

vCenter Server Configuration

Update 3

VMware vSphere 7.0

VMware ESXi 7.0

vCenter Server 7.0

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

About vCenter Server Configuration 6

1 vCenter Server Configuration Overview 7

What Happened to the Platform Services Controller 8

2 Using the vCenter Server Management Interface to Configure vCenter Server 10

Log In to the vCenter Server Management Interface 11

View vCenter ServerHealth Status 11

Reboot or Shut Down vCenter Server 12

Create a Support Bundle 12

Monitor CPU and Memory Use 13

Monitor Disk Use 13

Monitor Network Use 14

Monitor Database Use 14

Enable or Disable SSH and Bash Shell Access 15

Configure the DNS, IP Address, and Proxy Settings 15

Reconfigure the Primary Network Identifier 17

Edit the Firewall Settings 18

Configure the System Time Zone and Time Synchronization Settings 19

Start, Stop, and Restart Services 20

Configure Update Settings 21

Change the Password and Password Expiration Settings of the Root User 21

Forward vCenter Server Log Files to Remote Syslog Server 22

Configure and Schedule Backups 23

3 Using the vSphere Client to Configure vCenter Server 25

Configuring vCenter Server 25

Configure License Settings for vCenter Server 25

Configuring Statistics Settings 26

Configure Runtime Settings for vCenter Server 29

Configure User Directory Settings 29

Configure Mail Sender Settings 30

Configure SNMP Settings 32

View Port Settings 32

Configure Timeout Settings 33

Configure Logging Options 33

Configure Database Settings 34

- Verifying SSL Certificates for Legacy Hosts 35
- Configure Advanced Settings 36
- Send a Message to Other Logged In Users 37
- Join or Leave an Active Directory Domain 37
- Add a User to the SystemConfiguration.BashShellAdministrators Group 39
- Reboot a Node 40
- View the Health Status of Nodes 40
- Export a Support Bundle 41

4 Using the Appliance Shell to Configure vCenter Server 43

- Access the Appliance Shell 43
- Enable and Access the Bash Shell from the Appliance Shell 44
- Keyboard Shortcuts for Editing Commands 44
- Get Help About the Plug-Ins and API Commands in the Appliance 45
- Plug-Ins in the vCenter Server Shell 46
- Browse the Log Files By Using the showlog Plug-In 47
- API Commands in the Appliance Shell 48
- Configuring SNMP for vCenter Server 53
 - Configure the SNMP Agent for Polling 53
 - Configure vCenter Server for SNMP v1 and v2c 54
 - Configure vCenter Server for SNMP v3 56
 - Configure the SNMP Agent to Filter Notifications 59
 - Configure SNMP Management Client Software 60
 - Reset SNMP Settings to Factory Defaults 61
- Configuring Time Synchronization Settings in vCenter Server 61
 - Use VMware Tools Time Synchronization 62
 - Add or Replace NTP Servers in the vCenter Server Configuration 62
 - Synchronize the Time in vCenter Server with an NTP Server 63
- Managing Local User Accounts in vCenter Server 64
 - User Roles in vCenter Server 64
 - Get a List of the Local User Accounts in vCenter Server 64
 - Create a Local User Account in vCenter Server 65
 - Update the Password of a Local User in vCenter Server 65
 - Update a Local User Account in vCenter Server 66
 - Delete a Local User Account in vCenter Server 66
- Monitor Health Status and Statistics in vCenter Server 67
- Using the vimtop Plug-In to Monitor the Resource Use of Services 68
 - Monitor Services By Using vimtop in Interactive Mode 68
 - Interactive Mode Command-Line Options 68
 - Interactive Mode Single-Key Commands for vimtop 69

5 Using the Direct Console User Interface to Configure vCenter Server 71

Log In to the Direct Console User Interface 71

Change the Password of the Root User 72

Configure the Management Network of vCenter Server 72

Restart the Management Network of vCenter Server 73

Enable Access to the Bash Shell 74

Access the Bash Shell for Troubleshooting 74

Export a vCenter Server Support Bundle for Troubleshooting 74

About vCenter Server Configuration

vCenter Server Configuration provides information about configuring VMware vCenter[®] Server[™].

Intended Audience

This information is intended for anyone who wants to configure VMware vCenter Server[®]. The information is written for experienced system administrators who are familiar with virtual machine technology and data center operations.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

vSphere Client and vCenter Server Management Interface

Instructions in this guide reflect the vSphere Client, an HTML5-based GUI, and the vCenter Server Management Interface. Some additional functions can be performed using the vCenter Server appliance shell and the Direct Console User Interface.

vCenter Server Configuration Overview

1

vCenter Server is deployed using a preconfigured virtual machine, which is optimized for running VMware vCenter Server[®] and the associated services.

During the deployment of vCenter Server, you can create a VMware vCenter[®] Single Sign-On[™] domain or join an existing domain. For information about the vCenter Server deployment, see *vCenter Server Installation and Setup*.

vCenter Server is supported on VMware ESXi[™] 6.0 and later. The package contains the following software:

- Project Photon OS[®] 3.0
- PostgreSQL database
- vCenter Server 7.0 and vCenter Server 7.0 components
- Necessary services for running vCenter Server such as vCenter Single Sign-On, License service, and VMware Certificate Authority

For detailed information about authentication, see *vSphere Authentication*.

Customization of the preconfigured virtual machine is unsupported except for adding memory, CPU, and disk space.

vCenter Server has the following default user names:

- root user with the password that you set during the deployment of the virtual appliance. You use the root user to log in to the vCenter Server Management Interface and to the preconfigured virtual machine operating system.

Important The password for the root account of vCenter Server expires after 365 days by default. For information about changing the root password and configuring the password expiration settings, see [Change the Password and Password Expiration Settings of the Root User](#).

- administrator@your_domain_name which is the vCenter Single Sign-On user with the password and domain name that you set during the deployment of the appliance.

When you install vCenter Server, you can change the vSphere domain. Do not use the same domain name as the domain name of your Microsoft Active Directory or OpenLDAP domain name.

Initially, only the user `administrator@your_domain_name` has the privileges to log in to the vCenter Server system. By default, the `administrator@your_domain_name` user is a member of the `SystemConfiguration.Administrators` group. This user can add an identity source in which additional users and groups are defined to vCenter Single Sign-On or give permissions to the users and groups. For more information, see *vSphere Security*.

You can configure vCenter Server settings in four ways:

- Use the vCenter Server Management Interface.

You can edit the system settings such as access, network, time synchronization, and the root password settings. This is the preferred way for configuring vCenter Server.

- Use the vSphere Client.

You can navigate to the system configuration settings of vCenter Server and join the deployment to an Active Directory domain. You can manage the services that are running in vCenter Server and modify various settings such as access, network, and firewall settings.

- Use the Bash shell.

You can use TTY1 to log in to the console or can use SSH and run configuration, monitoring, and troubleshooting commands in vCenter Server.

- Use the Direct Console User Interface.

You can use TTY2 to log in to the vCenter Server Direct Console User Interface to change the password of the root user, configure the network settings, or enable access to the Bash shell or SSH.

This chapter includes the following topics:

- [What Happened to the Platform Services Controller](#)

What Happened to the Platform Services Controller

In vSphere 7.0, all Platform Services Controller services are consolidated into vCenter Server.

Beginning in vSphere 7.0, deploying or upgrading vCenter Server in vSphere 7.0 requires the use of vCenter Server Appliance, a preconfigured virtual machine optimized for running vCenter Server. The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into vCenter Server, and deployment and administration are simplified.

As these services are now part of vCenter Server, they are no longer described as a part of Platform Services Controller. In vSphere 7.0, the *vSphere Authentication* publication replaces the *Platform Services Controller Administration* publication. The new publication contains complete information about authentication and certificate management. For information about upgrading or migrating from vSphere 6.5 and 6.7 deployments using an existing external Platform Services Controller to vSphere 7.0 using vCenter Server Appliance, see the *vSphere Upgrade* documentation.

Using the vCenter Server Management Interface to Configure vCenter Server

2

After you deploy vCenter Server, you can log in to the vCenter Server Management Interface and edit the settings.

For information about patching vCenter Server and enabling automatic checks for vCenter Server patches, see the *vSphere Upgrade* documentation.

For information backing up and restoring vCenter Server, see *vCenter Server Installation and Setup*.

This chapter includes the following topics:

- Log In to the vCenter Server Management Interface
- View vCenter ServerHealth Status
- Reboot or Shut Down vCenter Server
- Create a Support Bundle
- Monitor CPU and Memory Use
- Monitor Disk Use
- Monitor Network Use
- Monitor Database Use
- Enable or Disable SSH and Bash Shell Access
- Configure the DNS, IP Address, and Proxy Settings
- Reconfigure the Primary Network Identifier
- Edit the Firewall Settings
- Configure the System Time Zone and Time Synchronization Settings
- Start, Stop, and Restart Services
- Configure Update Settings
- Change the Password and Password Expiration Settings of the Root User
- Forward vCenter Server Log Files to Remote Syslog Server
- Configure and Schedule Backups

Log In to the vCenter Server Management Interface

Log in to the vCenter Server Management Interface to access the vCenter Server configuration settings.

Note The login session expires if you leave the vCenter Server Management Interface idle for 10 minutes.

Prerequisites

Verify that the vCenter Server is successfully deployed and running.

Procedure

1 In a Web browser, go to the vCenter Server Management Interface, <https://appliance-IP-address-or-FQDN:5480>.

2 Log in as root.

The default root password is the password that you set while deploying vCenter Server.

View vCenter ServerHealth Status

You can use the vCenter Server Management Interface to view the overall health status of vCenter Server and health messages.

The overall health status of vCenter Server is based on the status of the hardware components such as CPU, memory, database, and storage. It is also based on the update component, which shows whether the software packages are up to date according to the last check for available patches.

Important If you do not perform regular checks for available patches, the health status of the update component might become out-of-date. For information about how to check for vCenter Server patches and enable automatic checks for vCenter Server patches, see *vSphere Upgrade*.

Prerequisites






Log in to the vCenter Server Management Interface as root.

Procedure

1 In the vCenter Server Management Interface, click **Summary**.

- In the Health Status pane, view the Overall Health badge.

Table 2-1. Health Status

Badge Icon	Description
	Good. All components are healthy.
	Warning. One or more components might become overloaded soon. View the details in the Health Messages pane.
	Alert. One or more components might be degraded. Nonsecurity patches might be available. View the details in the Health Messages pane.
	Critical. One or more components might be in an unusable status and vCenter Server might become unresponsive soon. Security patches might be available. View the details in the Health Messages pane.
	Unknown. No data is available.

Reboot or Shut Down vCenter Server

You can use the vCenter Server Management Interface to restart or power off the virtual machine running.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- In the vCenter Server Management Interface, click **Summary**.
- From the top menu pane, click the **Actions** drop-down menu.
- Click **Reboot** or **Shutdown** to restart or power off the virtual machine.
- In the confirmation dialog box, click **Yes** to confirm the operation.

Create a Support Bundle

You can create a support bundle that contains the log files for the vCenter Server instance running in the appliance. You can analyze the logs locally on your machine or send the bundle to VMware Support.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Summary**.
- 2 From the top menu pane, click the **Actions** drop-down menu.
- 3 Click **Create Support Bundle** and save the bundle on your local machine.

Results

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

Monitor CPU and Memory Use

You can use the vCenter Server Management Interface to monitor the overall CPU and memory use of vCenter Server.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Monitor**.
- 2 On the Monitor page, click the **CPU & Memory** tab.
- 3 From the **date range** drop-down menu, select the time period for which you want to generate a CPU utilization trending graph and a memory utilization trending graph.
- 4 Point to the graphs to see the CPU and memory use for a particular date and time.

Monitor Disk Use

You can use the vCenter Server Management Interface to monitor the disk use of vCenter Server.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Monitor**.
- 2 On the Monitor page, click the **Disks** tab.

Results

The Monitor Disks pane shows a disk, sortable by name, partition, or utilization.

Monitor Network Use

You can use the vCenter Server Management Interface to monitor the network use of vCenter Server in the last day, week, month, or quarter.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Monitor**.
- 2 On the Monitor page, click the **Network** tab.
- 3 From the **date range** drop-down menu, select the time period for generating the network utilization graph.
- 4 From the table below the graph grid, select a packet or transmit byte rate to monitor.
The options vary depending on your network settings.
The network utilization graph refreshes to display the use of the item you select.
- 5 Point to the network utilization graph to see the network use data for a particular date and time.

Monitor Database Use

You can use the vCenter Server Management Interface to monitor the use of the embedded database of the vCenter Server by data type. You can also monitor space use trending graphs and filter any of the largest data types.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Monitor**.
- 2 On the Monitor page, click the **Database** tab to monitor the consumed and free space for the vCenter Server database.
- 3 From the **date range** drop-down menu, select the time period for which you want to generate the space utilization trending graphs.
- 4 At the base of the graph, click the title a particular database component to include or exclude that component from the graph.

Option	Description
Seat space utilization trend graph	Allows you to select and view alarm, event, task, and stat trendlines.
Overall space utilization trend graph	Allows you to select and view SEAT, DB Log, and core trendlines.

- 5 Point to the space utilization graph to see the database use value for a particular date and time.

Enable or Disable SSH and Bash Shell Access

You can use the vCenter Server Management Interface to edit the access settings for the appliance.

You can enable or disable an SSH administrator login to the appliance. You can also enable access to the vCenter Server Bash shell for a specific time interval.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Access**, and click **Edit**.
- 2 Edit the access settings for vCenter Server.

Option	Description
Enable SSH login	Enables SSH access to vCenter Server.
Enable DCUI	Enables DCUI access to vCenter Server.
Enable Console CLI	Enables console CLI access to vCenter Server.
Enable Bash Shell	Enables Bash shell access to vCenter Server for the number of minutes that you enter.

- 3 Click **OK** to save the settings.

Configure the DNS, IP Address, and Proxy Settings

You can set the combination of static and DHCP, IPv4 and IPv6 addresses, edit the DNS settings, and define the proxy settings for vCenter Server.

Prerequisites

- To change the IP address of the appliance, verify that the system name of the appliance is an FQDN. The system name is used as a primary network identifier. If you set an IP address as a system name during the deployment of the appliance, you can later change the PNID to an FQDN.

Note You can set only IPv4 IP address as system name. The IPv4 IP address must be enabled before this setting.

- To restore a dual stack VC, the base VC after stage 1 deployment should be configured as:
 - If PNID of backed up VC resolves to IPv4 and IPv4 is configured static, the base VC during stage1 should have static or DHCP IPv4 configured.

- If PNID of backed up VC resolves to IPv4 and IPv4 is configured DHCP, the base VC during stage1 should have DHCP IPv4 configured.
 - If PNID of backed up VC resolves to IPv6 and IPv6 is configured static, the base VC during stage1 should have static or DHCP IPv6 configured.
 - If PNID of backed up VC resolves to IPv6 and IPv6 is configured DHCP, the base VC during stage1 should have DHCP IPv6 configured.
- Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Networking**.
- 2 From the Network Settings page, click **Edit**.
- 3 Expand the Hostname and DNS section to configure the DNS settings.

Note Valid value for Hostname is either FQDN resolving to enabled IP address or IPv4 IP address.

Option	Description
Obtain DNS settings automatically	Obtains the DNS settings automatically from the network.
Enter DNS settings manually	Lets you set the DNS address settings manually. If you select this option, you must provide the following information: <ul style="list-style-type: none"> ■ The IP address of the preferred DNS server. ■ (Optional) The IP address of the alternate DNS server.

- 4 From the Network Settings page, click **Edit**.
- 5 Expand the NICO section to configure the gateway settings.

Note PNID and network APIs support only NICO as primary NIC.

- 6 Edit the IPv4 address settings.

Option	Description
Enable or Disable IPv4 settings	Enables or Disables the IPv4 address based on the toggle switch option.
Obtain IPv4 settings automatically	Obtains the IPv4 address for the appliance automatically from the network.
Enter IPv4 settings manually	Uses an IPv4 address that you set manually. You must enter the IP address, subnet prefix length, and the default gateway.

Note For static IPv4 or IPv6 addresses, DNS server must be set manually.

Note Second and third party solutions need to re-register, when there is a change in the IPv4 and IPv6 IP addresses.

7 Edit the IPv6 address settings.

Option	Description
Enable or Disable IPv6 settings	Enables or disables the IPv6 address based on the toggle switch option.
Obtain IPv6 settings automatically through DHCP	Assigns IPv6 addresses to the appliance automatically from the network by using DHCP.
Obtain IPv6 settings automatically through router advertisement	Assigns IPv6 addresses to the appliance automatically from the network by using router advertisement.
Use static IPv6 addresses	<p>Uses static IPv6 addresses that you set up manually.</p> <ol style="list-style-type: none"> 1 Click the checkbox. 2 Enter the IPv6 address and the subnet prefix length. 3 Click Add to enter additional IPv6 addresses. 4 Click Save.

Note For static IPv4 or IPv6 addresses, DNS server must be set manually.

You can configure the appliance to obtain the IPv6 settings automatically through both DHCP and router advertisement. You can assign static a IPv6 address at the same time.

Note Second and third party solutions need to re-register, when there is a change in the IPv4 and IPv6 IP addresses.

8 To configure a proxy server, in the Proxy Settings section, click **Edit**.

9 Select the proxy setting to enable

Option	Description
HTTPS	Enable to configure the HTTPS proxy settings.
FTP	Enable to configure the FTP proxy settings.
	Note Ensure that the ICMP is enabled on the proxy server.
HTTP	Enable to configure the HTTP proxy settings.

10 Enter the server hostname or IP address.

11 Enter the port.

12 Enter the username (optional).

13 Enter the password (optional).

14 Click **Save**.

Reconfigure the Primary Network Identifier

You can change the FQDN, IP, or PNID of the management network of vCenter Server.

Prerequisites

The system name is used as a primary network identifier. If you set an IP address as a system name during the deployment of the appliance, you can later change the PNID to an FQDN.

If vCenter High Availability (HA) is enabled, you must disable the vCenter HA setup before reconfiguring the PNID.

Procedure

- 1 Log in to the vCenter Server Management Interface using your administrator SSO credentials.
- 2 In the vCenter Server Management Interface, navigate to the **Networking** page and click **Edit**.
- 3 Select the NIC to be modified and click **Next**.
- 4 In the **Edit Settings** pane, change the host name and provide the new IP address. Click **Next**.
- 5 In the **SSO Credentials** pane, provide the administrator SSO credentials. You must use **administrator@<domain_name>** credentials.
- 6 In the **Ready to Complete** pane, review your new settings and check the backup acknowledgement box. Click **Finish**.

A taskbar shows the status of the network update. To cancel the update, click **Cancel Network Update**. When the network reconfiguration is complete, the UI redirects to the new IP address.

- 7 To finish the reconfiguration process and restart services, log in using your administrator SSO credentials.
- 8 On the **Networking** page, verify the new host name and IP address.

What to do next

- Re-register all deployed plug-ins.
- Regenerate all custom certificates.
- If vCenter HA was enabled, reconfigure vCenter HA.
- If Active Domain was enabled, reconfigure Active Domain.
- If Hybrid Link mode was enabled, reconfigure Hybrid Link with the Cloud vCenter Server.

Edit the Firewall Settings

After you deploy vCenter Server, you can edit its firewall settings and create firewall rules using the Management Interface.

You can set up firewall rules to accept or block traffic between vCenter Server and specific servers, hosts, or virtual machines. You cannot block specific ports, you block all the traffic.

Prerequisites

Verify that the user who logs in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in vCenter Single Sign-On.

Procedure

- 1 In the vCenter Server Management Interface, click **Firewall**.
- 2 Edit the firewall settings.

Command	Action
Add	<ol style="list-style-type: none"> a To create a firewall rule, click Add. b Select a network interface of the virtual machine. c Enter the IP address of the network to apply this rule to. The IP address can be IPv4 and IPv6 address. d Enter a subnet prefix length. e From the Action drop-down menu, select whether to Accept, Ignore, Reject, or Return the connection between vCenter Server and the network that you entered. f Click Save.
Edit	<ol style="list-style-type: none"> a Select a rule and click Edit. b Edit the settings of the rule. c Click Save.
Delete	<ol style="list-style-type: none"> a Select a rule and click Delete. b At the prompt, click Delete again.
Reorder	<ol style="list-style-type: none"> a Select a rule and click Reorder. b In the Reorder pane, select the rule to move. c Click Move Up or Move Down. d Click Save.

Configure the System Time Zone and Time Synchronization Settings

After you deploy vCenter Server, you can change the system time zone and time synchronization settings from the vCenter Server Management Interface.

When you deploy vCenter Server, you either use the time settings of the ESXi host on which vCenter Server is running or you configure the time synchronization based on an NTP server. If the time settings in your vSphere network change, you can edit the time zone and time synchronization settings in the appliance.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Time**.
- 2 Configure the system time zone settings.
 - a In the Time zone pane, click **Edit**.
 - b From the **Time zone** drop-down menu, select a location or time zone and click **Save**.
- 3 Configure the time synchronization settings.
 - a In the Time synchronization pane, click **Edit**.
 - b From the **Mode** drop-down menu, configure the time synchronization method.

Option	Description
Disabled	No time synchronization. Uses the system time zone settings.
Host	Enables VMware Tools time synchronization. Uses VMware Tools to synchronize the time of the appliance with the time of the ESXi host.
NTP	Enables NTP synchronization. You must enter the IP address or FQDN of one or more NTP servers.

- c Click **Save**.

Start, Stop, and Restart Services

You can use the vCenter Server Management Interface to view the status of vCenter Server components and to start, stop, and restart services.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Services**.
The Services page displays a table of the installed services that can be sorted by name, startup type, health, and state.
- 2 Select a service and click **SET STARTUP TYPE** to configure either Manual or Automatic start of a service.
- 3 Select a service and click **START** to start a service.
- 4 Select a service and click **STOP** to stop, or **RESTART** to restart a service, then click **OK**.

Warning Stopping or Restarting some services may lead to functionality becoming temporarily unavailable.

Configure Update Settings

You can use the vCenter Server Management Interface to configure your update settings and check for new updates.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Update**.
- 2 To configure your update settings, click **Settings**.
 - a To check for updates automatically, select the checkbox.
 - b Select to use a default or custom repository.
 - c If you selected a custom repository, enter the repository URL, username (optional), and password (optional). Click **Save**.

For the URL, HTTPS and FTPS protocols are supported.
- 3 To manually check for updates, click the **Check Updates** drop-down menu.
 - a Select to check a **CD-ROM** or a **CD-ROM + URL** for updates.

Results

The Available Updates table displays available updates sortable by version, type, release date, reboot requirement, and severity.

Change the Password and Password Expiration Settings of the Root User

When you deploy vCenter Server, you set the initial password of the root user, which expires after 90 days by default. You can change the root password and the password expiration settings from the vCenter Server Management Interface.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, click **Administration**.
- 2 In the Password section, click **Change**.
- 3 Enter the current password and the new password, then click **Save**.

- 4 Configure the password expiration settings for the root user.
 - a In the Password expiration settings section, click **Edit** and select the password expiration policy.

Option	Description
Yes	<p>The password of the root user expires after a specified number of days. You must provide the following information:</p> <ul style="list-style-type: none"> ■ Root password validity (days) <p>The number of days after which the password expires.</p> ■ Email for expiration warning <p>The email address to which vCenter Server sends a warning message before the expiration date.</p>
No	The password of the root user never expires.

- b In the Password expiration settings pane, click **Save** to apply the new password expiration settings.

The Password expiration settings section displays the new expiration date.

Forward vCenter Server Log Files to Remote Syslog Server

You can forward the vCenter Server log files to a remote syslog server to conduct an analysis of your logs.

Note ESXi can be configured to send log files to a vCenter Server rather than storing them to a local disk. The recommended maximum numbers of supported hosts to collect logs from is 30. See <http://kb.vmware.com/s/article/2003322> for information on how to configure ESXi log forwarding. This feature is intended for smaller environments with stateless ESXi hosts. For all other cases, use a dedicated log server. Using vCenter Server to receive ESXi log files might impact vCenter Server performance.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- 1 In the vCenter Server Management Interface, select **Syslog**.
- 2 In the Forwarding Configuration section, click **Configure** if you have not configured any remote syslog hosts. Click **Edit** if you already have configured hosts.
- 3 In the Create Forwarding Configuration pane, enter the server address of the destination host. The maximum number of supported destination hosts is three.

- From the **Protocol** drop-down menu, select the protocol to use.

Menu Item	Description
TLS	Transport Layer Security
TCP	Transmission Control Protocol
RELP	Reliable Event Logging Protocol
UDP	User Datagram Protocol

- In the **Port** text box, enter the port number to use for communication with the destination host.
- In the Create Forwarding Configuration pane, click **Add** to enter another remote syslog server.
- Click **Save**.
- Verify that the remote syslog server is receiving messages.
- In the Forwarding Configuration section, click **Send Test Message**.
- Verify on the remote syslog server that the test message was received.

The new configuration settings are shown in the Forwarding Configuration section.

Configure and Schedule Backups

You can use the vCenter Server Management Interface to set a backup location, create a backup schedule, and monitor backup activity.

Prerequisites

Log in to the vCenter Server Management Interface as root.

Procedure

- In the vCenter Server Management Interface, click **Backup**.
- To create a backup schedule, click **Configure**. To edit an existing backup schedule, click **Edit**.
 - In the **Backup Schedule** pane, enter the backup location using the format **protocol://server-address[:port-number]/folder/subfolder**.
Supported protocols for backup are FTPS, HTTPS, SFTP, FTP, NFS, SMB, and HTTP.
 - Enter the username and password for the backup server.
 - Enter the time and frequency for the backup to occur.
 - (Optional) Enter an encryption password for the backup.
 - Indicate the number of backups to retain.
 - Indicate the types of data to be backed up.

3 To initiate a manual backup, click **Backup Now**.

Results

Information for scheduled and manual backups is displayed in the **Activity** table.

Using the vSphere Client to Configure vCenter Server

3

You can perform some configuration operations from the vSphere Client such as joining the appliance to an Active Directory domain, networking, and other settings.

This chapter includes the following topics:

- [Configuring vCenter Server](#)
- [Join or Leave an Active Directory Domain](#)
- [Add a User to the SystemConfiguration.BashShellAdministrators Group](#)
- [Reboot a Node](#)
- [View the Health Status of Nodes](#)
- [Export a Support Bundle](#)

Configuring vCenter Server

You can configure vCenter Server from the vSphere Client and from the vCenter Server Management Interface.

What you can do depends on your deployment.

On-premises vCenter Server

You can change many of the vCenter Server settings, including licensing, statistics collection, logging, and more.

vCenter Server in VMware Cloud on AWS

VMware preconfigures vCenter Server instances when you create an SDDC. You can view configuration settings and advanced settings, and you can set a Message of the Day.

For detailed information on how to configure vCenter Server, see the *vCenter Server Configuration* guide.

Configure License Settings for vCenter Server

You must assign a license to a vCenter Server system before its evaluation period expires or its currently assigned license expires. If you upgrade, combine, or divide vCenter Server licenses in

Customer Connect, you must assign the new licenses to vCenter Server systems and remove the old licenses.

Prerequisites

- To view and manage licenses in the vSphere environment, you must have the **Global.Licenses** privilege on the vCenter Server system, where the vSphere Client runs.

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Select the **Configure** tab.
- 3 Under **Settings**, select **Licensing**.
- 4 Click **Assign License**.
- 5 In the **Assign License** dialog box, select the task that you want to perform.
 - ◆ In the vSphere Client, select an existing license or select a newly created license.

Task	Steps
Select an existing license	Select an existing license from the list and click OK .
Select a newly created license	<ol style="list-style-type: none"> a Click the New License tab. b In the Assign License dialog box, type or copy and paste a license key and click OK. c Enter a name for the new license and click OK. Details about the product, product features, capacity, and expiration period appear on the page. d Click OK. e In the Assign License dialog box, select the newly created license, and click OK.

Results

The license is assigned to the vCenter Server system, and one instance from the license capacity is allocated for the vCenter Server system.

Configuring Statistics Settings

To set up how statistical data is recorded, you configure collection intervals for statistics. You can access the stored statistical information through command-line monitoring utilities or by viewing performance charts in the vSphere Client.

Configure Statistics Collection Intervals in the vSphere Client

Statistic collection intervals determine the frequency at which statistic queries occur, the length of time statistical data is stored in the database, and the type of statistical data that is collected.

You can view the collected statistics through the performance charts in the vSphere Client or through command-line monitoring utilities.

Note Not all interval attributes are configurable.

Prerequisites

Required privilege: **Performance.ModifyIntervals**

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Select the **Configure** tab.
- 3 Under **Settings**, select **General**.
- 4 Click **Edit**.
- 5 To enable or disable a statistics interval, check the box for that interval.
- 6 To change a statistics interval attribute value, select a value from the drop-down menu.
 - a In **Interval Duration**, select the time interval in which statistics data is collected.
 - b In **Save For**, select for how long the archived statistics are kept in the database.
 - c In **Statistics Level**, select a new level for collecting statistics.

The lower the level is, the fewer number of statistic counters are used. Level 4 uses all statistics counters. Use it only for debugging purposes.

The statistics level must be less than or equal to the statistics level that is set for the preceding statistics interval. This requirement is a vCenter Server dependency.

- 7 (Optional) In Database Size, estimate the effect of the statistics settings on the database.
 - a Enter the number of **Physical Hosts**.
 - b Enter the number of **Virtual Machines**.

The estimated space required and number of database rows required are calculated and displayed.

- c If necessary, make changes to your statistics collection settings.
- 8 Click **Save**.

Example: Relationships Between the Default Settings for Statistics Intervals

- Samples that are collected every 5 minutes are stored for 1 day.
- Samples that are collected every 30 minutes are stored for 1 week.
- Samples that are collected every 2 hours are stored for 1 month.
- Samples that are collected on 1 day are stored for 1 year.

For all statistics intervals, the default level is 1. It uses the Cluster Services, CPU, Disk, Memory, Network, System, and Virtual Machine Operations counters.

Data Collection Levels

Each collection interval has a default collection level that determines the amount of data gathered and which counters are available for display in the charts. Collection levels are also referred to as statistics levels.

Table 3-1. Statistics Levels

Level	Metrics	Best Practice
Level 1	<ul style="list-style-type: none"> ■ Cluster Services (VMware Distributed Resource Scheduler) – all metrics ■ CPU – cpuintitlement, totalmhz, usage (average), usagemhz ■ Disk – capacity, maxTotalLatency, provisioned, unshared, usage (average), used ■ Memory – consumed, mementitlement, overhead, swapinRate, swapoutRate, swapused, totalmb, usage (average), vmmemctl (balloon) ■ Network – usage (average), IPv6 ■ System – heartbeat, uptime ■ Virtual Machine Operations – numChangeDS, numChangeHost, numChangeHostDS 	<p>Use for long-term performance monitoring when device statistics are not required.</p> <p>Level 1 is the default Collection Level for all Collection Intervals.</p>
Level 2	<ul style="list-style-type: none"> ■ Level 1 metrics ■ CPU – idle, reservedCapacity ■ Disk – All metrics, excluding numberRead and numberWrite. ■ Memory – All metrics, excluding memUsed and maximum and minimum rollup values. ■ Virtual Machine Operations – All metrics 	<p>Use for long-term performance monitoring when device statistics are not required but you want to monitor more than the basic statistics.</p>
Level 3	<ul style="list-style-type: none"> ■ Level 1 and Level 2 metrics ■ Metrics for all counters, excluding minimum and maximum rollup values. ■ Device metrics 	<p>Use for short-term performance monitoring after encountering problems or when device statistics are required.</p>
Level 4	All metrics supported by the vCenter Server, including minimum and maximum rollup values.	<p>Use for short-term performance monitoring after encountering problems or when device statistics are required.</p>

Note When the statistics levels, level 3 or level 4 are used beyond the default value, it may cause one particular process, vpxd, to sustain memory growth, if it cannot save the statistics information to the database as quickly as required. If the usage limit of these statistics levels is not monitored closely, it may cause vpxd to grow out of memory and eventually crash.

So, in case the administrator decides to elevate any of these levels, it is necessary for the administrator to monitor the size of the vpxd process to make sure that is not growing boundlessly after the change.

Configure Runtime Settings for vCenter Server

You can change the vCenter Server ID, managed address, and name. You might need to make changes if you run multiple vCenter Server systems in the same environment.

Prerequisites

Required privilege: **Global.Settings**

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Select the **Configure** tab.
- 3 Under **Settings**, select **General**.
- 4 Click **Edit**.
- 5 In the Edit vCenter Server Settings dialog box, select **Runtime Settings**.
- 6 In **vCenter Server unique ID**, enter a unique ID.

You can change this value to a number from 0 through 63 to identify each vCenter Server system running in a common environment. By default, an ID value is generated randomly.

- 7 In **vCenter Server managed address**, enter the vCenter Server system address.

The address can be IPv4, IPv6, a fully qualified domain name, an IP address, or another address format.

- 8 In **vCenter Server name**, enter the name of the vCenter Server system.

If you change the DNS name of the vCenter Server, you can use this text box to modify the vCenter Server name to match.

- 9 Click **Save**.

What to do next

If you made changes to the vCenter Server system unique ID, you must restart the vCenter Server system for these changes to take effect.

Configure User Directory Settings

You can configure some of the ways vCenter Server interacts with the user directory server that is configured as an identity source.

For vCenter Server versions before vCenter Server 5.0, these settings apply to an Active Directory associated with vCenter Server. For vCenter Server 5.0 and later, these settings apply to vCenter Single Sign-On identity sources.

Prerequisites

Required privilege: **Global.Settings**

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Select the **Configure** tab.
- 3 Under **Settings**, select **General**.
- 4 Click **Edit**.
- 5 In the Edit vCenter general settings window, select **User directory**.
- 6 In **User directory timeout**, type the timeout interval in seconds for connecting to the directory server.
- 7 Enable the **Query Limit** box to set a query limit size.
- 8 In **Query Limit Size**, enter the number of users and groups for which you can associate permissions on the child inventory objects of the vCenter Server system.

Note You can associate permissions with users and groups from the Add Permissions dialog box that displays when you click **Add permissions** in **Manage > Permissions** for a vSphere inventory object.

- 9 Click **SAVE**.

Configure Mail Sender Settings

You must configure the email address of the sender account to use vCenter Server operations, such as sending email notifications as alarm actions. You can send email alerts and alarms using either anonymous or authentication mode.

Prerequisites

Required privilege: **Global.Settings**

SMTP authentication is available for:

- vSphere 7.0 Update 1 and later versions only.
- Office 365 mailbox users only.
- SMTP mail sender should meet the basic requirements for SMTP Authentication as mentioned in Microsoft's document [Requirement for SMTP AUTH client submission](#).

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Select the **Configure** tab.
- 3 Under **Settings**, select **General**.
- 4 Click **Edit**.
- 5 Select **Mail** and enter the settings that vCenter Server uses to send email alerts.

6 In **Mail server** text box, enter the SMTP server information.

The SMTP server is the DNS name or IP address of the SMTP gateway to use for sending email messages.

- For sending mails anonymously, you can enter any SMTP server information as the mail server name.
- For SMTP authentication, you must enter the mail server name as `smtp.office365.com`, unless you have some customized configuration. Do not use IP address as mail server as IP address is not supported for SMTP authentication.

7 In **Mail sender** text box, enter the sender account information.

The sender account is the email address of the sender.

For SMTP authentication, you must enter a valid SMTP account name in the **Mail sender** text box.

Note You must enter the full email address, including the domain name.

For example, `mail_server@example.com`

8 Click **SAVE**.**9** This step is applicable only for SMTP authentication.

You must configure the SMTP user settings as below:

- a Select the **Configure** tab.
- b Select **Advanced Settings**.
- c Click **EDIT SETTINGS** and enter the following values for the configuration parameters:

Name	Value
<code>mail.smtp.username</code>	Valid SMTP account name. Note This account name must be same as the account name provided in Mail sender text box for sending mails using SMTP authentication in Step 7.
<code>mail.smtp.password</code>	Valid SMTP account password. Note Currently, the account password is not masked and is visible. You must use a dedicated SMTP mail user until the masking is available in upcoming releases.
<code>mail.smtp.port</code>	587

- d Click **SAVE**.

What to do next

You can perform the following steps to test the mail settings:

- 1 Create an alarm that is triggered by a user action.

For example, the user action can be powering off a virtual machine.

- 2 Verify that you receive an email, when the alarm is triggered.

Configure SNMP Settings

You can configure up to four receivers to receive SNMP traps from vCenter Server. For each receiver, specify a host name, port, and community.

Prerequisites

Required privilege: **Global.Settings**

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Select the **Configure** tab.
- 3 Under **Settings**, select **General**.
- 4 Click **Edit**.
- 5 Select **SNMP receivers**.
- 6 Select the **Enable receiver 1** box.
- 7 In **Primary Receiver URL**, enter the host name or IP address of the SNMP receiver.
- 8 In **Receiver port**, enter the port number of the receiver.
The port number must be a value between 1 and 65535.
- 9 In **Community string**, enter the community identifier.
- 10 To send alarms to multiple receivers, select the additional **Enable receiver** boxes and enter the host name, port number, and community identifier for those receivers.
- 11 Click **Save**.

View Port Settings

You can view the ports used by the Web service to communicate with other applications. You cannot configure these port settings.

The Web service is installed as part of the VMware vCenter Server installation. The Web service is a required component for third-party applications that use the VMware SDK application programming interface (API). For information about installing the Web service, see the *vCenter Server Installation and Setup* documentation.

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Select the **Configure** tab.
- 3 Under **Settings**, select **General**.

4 Click **Edit**.

5 Select **Ports**.

The ports used by the Web service are displayed.

6 Click **Save**.

Configure Timeout Settings

You can configure the timeout intervals for vCenter Server operations. These intervals specify the amount of time after which the vSphere Client times out.

Prerequisites

Required privilege: **Global.Settings**

Procedure

1 In the vSphere Client, navigate to the vCenter Server instance.

2 Select the **Configure** tab.

3 Under **Settings**, select **General**.

4 Click **Edit**.

5 Select **Timeout settings**.

6 In **Normal**, type the timeout interval in seconds for normal operations.

Do not set the value to zero (0).

7 In **Long**, enter the timeout interval in minutes for long operations.

Do not set the value to zero (0).

8 Click **Save**.

9 Restart the vCenter Server system for the changes to take effect.

Configure Logging Options

You can configure the amount of detail that vCenter Server collects in log files.

Prerequisites

Required privilege: **Global.Settings**

Procedure

1 In the vSphere Client, navigate to the vCenter Server instance.

2 Select the **Configure** tab.

3 Under **Settings**, select **General**.

4 Click **Edit**.

- 5 Select **Logging settings**.
- 6 Select the logging options.

Option	Description
None	Turns off logging
Error	Displays only error log entries
Warning	Displays warning and error log entries
Info	Displays information, error, and warning log entries
Verbose	Displays information, error, warning, and verbose log entries
Trivia	Displays information, error, warning, verbose, and trivia log entries

- 7 Click **SAVE**.

Results

Changes to the logging settings take effect immediately. You do not need to restart the vCenter Server system.

Configure Database Settings

You can configure the maximum number of database connections that can occur simultaneously. To limit the growth of the vCenter Server database and save storage space, you can configure the database to discard information about tasks or events periodically.

Note Do not use the database retention options, if you want to keep a complete history of tasks and events for your vCenter Server.

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Select the **Configure** tab.
- 3 Under **Settings**, select **General**.
- 4 Click **Edit**.
- 5 In Edit vCenter general settings window, click **Database**.
- 6 In **Maximum connections** field, enter the required number of connections.

Note Do not change this value unless one of these issues exists in your system.

- If your vCenter Server system performs many operations frequently and performance is critical, increase the number of connections.
 - If the database is shared and connections to the database are costly, decrease the number of connections.
-

- 7 Enable **Task cleanup** option for vCenter Server to delete the retained tasks periodically.

- 8** (Optional) In **Task retention (days)** field, enter a value (in days).

Information about tasks that are performed on this vCenter Server system is discarded after the specified number of days.

- 9** Enable **Event cleanup** option for vCenter Server to clean up the retained events periodically.

- 10** (Optional) In **Event retention (days)** field, enter a value (in days).

Information about events for this vCenter Server system is discarded after the specified number of days.

Note Monitor vCenter Server database consumption and disk partition in the vCenter Server Management Interface.

Warning Increasing the events retention to more than 30 days results in significant increase of vCenter database size and can shutdown the vCenter Server. Ensure that you increase the vCenter database accordingly.

- 11** Restart the vCenter Server to apply changes manually.

- 12** Click **SAVE**.

Verifying SSL Certificates for Legacy Hosts

You can configure vCenter Server to check the SSL certificates of hosts to which it connects. If you configure this setting, vCenter Server and the vSphere Client check for valid SSL certificates before connecting to a host for operations such as adding a host or making a remote console connection to a virtual machine.

vCenter Server 5.1 and vCenter Server 5.5 always connect to ESXi hosts using SSL thumbprint certificates. Starting with vCenter Server 6.0, the SSL certificates are signed by VMware Certificate Authority by default. You can instead use certificates from a third-party CA. Thumbprint mode is supported only for legacy hosts.

Procedure

- 1** In the vSphere Client, navigate to the vCenter Server instance.
- 2** Select the **Configure** tab.
- 3** Under **Settings**, select **General**.
- 4** Click **Edit**.
- 5** Select **SSL settings**.
- 6** Determine the host thumbprint for each legacy host that requires validation.
 - a Log in to the direct console.
 - b Select **View Support Information** on the **System Customization** menu.

The thumbprint is displayed in the column on the right.

- 7 Compare the thumbprint you obtained from the host with the thumbprint listed in the vCenter Server SSL settings dialog box.
- 8 If the thumbprints match, select the check box for the host.
Hosts that are not selected will be disconnected after you click **Save**.
- 9 Click **Save**.

Configure Advanced Settings

In **Advanced Settings**, you can modify the vCenter Server configuration file, `vpzd.cfg`.

You can use **Advanced Settings** to add entries to the `vpzd.cfg` file, but not to edit or delete them. VMware recommends that you change these settings only when instructed to do so by VMware technical support or when you are following specific instructions in VMware documentation.

Prerequisites

Required privilege: **Global.Settings**

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Select the **Configure** tab.
- 3 Select **Advanced Settings**.
- 4 Click **Edit Settings**.
- 5 In the **Name** field, type a name for the setting. Names must start with 'config.' For example: **config.log**.
- 6 In the **Value** field, type the value for the specified setting.
- 7 Click **Add**.
- 8 Click **Save**.

Results

Newly added advanced settings have `config.` appended to the setting keys in the `vpzd.cfg` file. For example:

```
config.example.setting = exampleValue
```

What to do next

Many advanced settings changes require you to restart the vCenter Server system. Consult VMware technical support to determine if your changes require a restart.

Send a Message to Other Logged In Users

Administrators can send messages to users who are currently logged in to a vCenter Server system. The message might announce maintenance or ask users to log out temporarily.

Procedure

- 1 In the vSphere Client, navigate to the vCenter Server instance.
- 2 Click **Configure**.
- 3 Select **Settings > Message of the Day** and click **Edit**.
- 4 Enter a message and click **OK**.

Results

The message appears at the top of the vSphere Client in each active user session.

Join or Leave an Active Directory Domain

You can join vCenter Server to an Active Directory domain. You can attach the users and groups from this Active Directory domain to your vCenter Single Sign-On domain. You can leave the Active Directory domain.

Important Joining vCenter Server to an Active Directory domain with a read-only domain controller (RODC) is not supported. You can join vCenter Server only to an Active Directory domain with a writable domain controller.

If you want to configure permissions so that users and groups from an Active Directory can access the vCenter Server components, you must join the vCenter Server instance to the Active Directory domain.

For example, to enable an Active Directory user to log in to the vCenter Server instance by using the vSphere Client, you must join the vCenter Server instance to the Active Directory domain and assign the Administrator role to this user.

Prerequisites

- Verify that the user who logs in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in vCenter Single Sign-On.
- Verify that the system name of the appliance is an FQDN. If, during the deployment of the appliance, you set an IP address as a system name, you cannot join vCenter Server to an Active Directory domain.

Procedure

- 1 Use the vSphere Client to log in as `administrator@your_domain_name` to the vCenter Server instance.
- 2 From the vSphere Client menu, select **Administration**.

- 3 Select **Single Sign On > Configuration**.
- 4 Click on the **Identity Provider** tab, and select **Active Directory Domain** as the identity provide type.
- 5 Click **JOIN AD**.
- 6 In the Join Active Directory Domain window, provide the following details.

Option	Description
Domain	Active Directory domain name, for example, mydomain.com. Do not provide an IP address in this text box.
Organization Unit (optional)	The full Organization Unit (OU) LDAP FQDN, for example, OU=Engineering,DC=mydomain,DC=com. Important Use this text box only if you are familiar with LDAP.
Username	User name in User Principal Name (UPN) format, for example, jchin@mydomain.com. Important Down-level login name format, for example, DOMAIN\UserName, is unsupported.
Password	Password of the user.

Note Reboot the node to apply changes.

- 7 Click **JOIN** to join the vCenter Server to the Active Directory domain.
The operation silently succeeds and you can see the Join AD option turned to Leave AD.
- 8 (Optional) To leave the Active Directory Domain, click **LEAVE AD**.
- 9 Restart the vCenter Server to apply the changes.

Important If you do not restart the vCenter Server, you might encounter problems when using the vSphere Client.

- 10 Select **Identity Sources** tab, and click the **ADD**.
 - a In the Add Identity Source window, select **Active Directory (Integrated Windows Authentication)** as the Identity Source Type.
 - b Enter the identity source settings of the joined Active Directory domain, and click **ADD**.

Table 3-2. Add Identity Source Settings

Text Box	Description
Domain name	FDQN of the domain. Do not provide an IP address in this text box.
Use machine account	Select this option to use the local machine account as the SPN. When you select this option, you specify only the domain name. Do not select this option if you expect to rename this machine.

Table 3-2. Add Identity Source Settings (continued)

Text Box	Description
Use Service Principal Name (SPN)	Select this option if you expect to rename the local machine. You must specify an SPN, a user who can authenticate with the identity source, and a password for the user.
Service principal name	<p>SPN that helps Kerberos to identify the Active Directory service. Include the domain in the name, for example, STS/example.com.</p> <p>You might have to run <code>setspn -S</code> to add the user you want to use. See the Microsoft documentation for information on <code>setspn</code>.</p> <p>The SPN must be unique across the domain. Running <code>setspn -S</code> checks that no duplicate is created.</p>
Username	Name of a user who can authenticate with this identity source. Use the email address format, for example, jchin@mydomain.com. You can verify the User Principal Name with the Active Directory Service Interfaces Editor (ADSI Edit).
Password	Password for the user who is used to authenticate with this identity source, which is the user who is specified in User Principal Name. Include the domain name, for example, jdoe@example.com.

Results

On the **Identity Sources** tab, you can see the joined Active Directory domain.

What to do next

You can configure permissions so that users and groups from the joined Active Directory domain can access the vCenter Server components. For information about managing permissions, see the *vSphere Security* documentation.

Add a User to the SystemConfiguration.BashShellAdministrators Group

To enable access to the appliance Bash shell by using the vSphere Client, the user you use to log in must be a member of the SystemConfiguration.BashShellAdministrators group. By default, this group is empty and you must add a user to the group manually.

Prerequisites

Verify that the user you use to log in to the vCenter Server instance is a member of the SystemConfiguration.Administrators group in the vCenter Single Sign-On domain.

Procedure

- 1 Use the vSphere Client to log in as `administrator@your_domain_name` to the vCenter Server instance.

The address is of the type `http://appliance-IP-address-or-FQDN/ui`.

- 2 From the vSphere Client menu, select **Administration**.
- 3 Select **Single Sign On > Users and Groups**.
- 4 Click on the **Groups** tab, select **SystemConfiguration.BashShellAdministrators** from the options available in the Group Name column.
- 5 Click **EDIT**.
- 6 In the **Edit Group** window, to add members, select the domain from the dropdown menu and then search for the required users.
- 7 Click **SAVE**.

Reboot a Node

In the vSphere Client, you can reboot a node in vCenter Server.

Prerequisites

Verify that the user you use to log in to the vCenter Server instance is a member of the `SystemConfiguration.Administrators` group in the vCenter Single Sign-On domain.

Procedure

- 1 Use the vSphere Client to log in as `administrator@your_domain_name` to the vCenter Server instance.
- 2 On the vSphere Client main page, click **Administration > Deployment > System Configuration**.
- 3 Under System Configuration, select a node from the list.
- 4 Click **REBOOT NODE**.

View the Health Status of Nodes

In the vSphere Client, you can view the health status of vCenter Server nodes.

vCenter Server instances and machines that run vCenter Server services are considered nodes. Graphical badges represent the health status of nodes.

Prerequisites

Verify that the user you use to log in to the vCenter Server instance is a member of the `SystemConfiguration.Administrators` group in the vCenter Single Sign-On domain.





Procedure

- 1 Use the vSphere Client to log in as `administrator@your_domain_name` to the vCenter Server instance.

The address is of the type `http://appliance-IP-address-or-FQDN/ui`.

- 2 From the vSphere Client menu, select **Administration**.
- 3 Select **Deployment > System Configuration**.
- 4 Select a node to view its health status.

Table 3-3. Health States

Badge Icon	Description
	Good. The health of the object is normal.
	Warning. The object is experiencing some problems.
	Critical. The object is either not functioning properly or will stop functioning soon.
	Unknown. No data is available for this object.

Export a Support Bundle

You can export a support bundle containing the log files for a specific product included in vCenter Server.

Prerequisites

Verify that the user who logs in to the vCenter Server instance is a member of the `SystemConfiguration.Administrators` group in vCenter Single Sign-On.

Procedure

- 1 Use the vSphere Client to log in as `administrator@your_domain_name` to the vCenter Server instance.

The address is of the type `http://appliance-IP-address-or-FQDN/ui`.

- 2 On the vSphere Client home page, click **Administration > Deployment > System Configuration**.
- 3 Select a node from the list and click **Export Support Bundle**.

- 4 In the **Export Support Bundle** window, expand the trees to view the services running in the appliance and deselect the services for which you do not want to export log files.

All the services are selected by default. If you want to export the support bundle and send it to VMware Support, leave all check boxes selected. The services are separated in two categories: a Cloud infrastructure category, which contains the services of specific products in the appliance, and a Virtual appliance category, which contains the services specific for the appliance and the vCenter Server product.

- 5 Click **Export Support Bundle** and save the bundle on your local machine.

Results

You saved the support bundle to your machine and can explore it.

Using the Appliance Shell to Configure vCenter Server

4

You can access all of the vCenter Server API commands and plug-ins that you can use for monitoring, troubleshooting, and configuring the appliance by using the appliance shell.

You can run all commands in the appliance shell with or without the `pi` keyword.

This chapter includes the following topics:

- Access the Appliance Shell
- Enable and Access the Bash Shell from the Appliance Shell
- Keyboard Shortcuts for Editing Commands
- Get Help About the Plug-Ins and API Commands in the Appliance
- Plug-Ins in the vCenter Server Shell
- Browse the Log Files By Using the `showlog` Plug-In
- API Commands in the Appliance Shell
- Configuring SNMP for vCenter Server
- Configuring Time Synchronization Settings in vCenter Server
- Managing Local User Accounts in vCenter Server
- Monitor Health Status and Statistics in vCenter Server
- Using the `vimtop` Plug-In to Monitor the Resource Use of Services

Access the Appliance Shell

To access the plug-ins included in the appliance shell and to be able to see and use the API commands, first access the appliance shell.

Procedure

- 1 Access the appliance shell.
 - If you have direct access to the appliance console, press `Alt+F1`.
 - If you want to connect remotely, use SSH or another remote console connection to start a session to the appliance.

- 2 Enter a user name and password recognized by the appliance.

Results

You are logged in to the appliance shell and can see the welcome message.

Enable and Access the Bash Shell from the Appliance Shell

If you log in to the appliance shell as a user who has a super administrator role, you can enable access to the Bash shell of the appliance for other users. The root user has access to the appliance Bash shell by default.

The appliance Bash shell is enabled by default for the root

Procedure

- 1 Access the appliance shell and log in as a user who has a super administrator role.
The default user with a super administrator role is root.
- 2 If you want to enable the Bash shell access for other users, run the following command.

```
shell.set --enabled true
```

- 3 To access the Bash shell run `shell` or `pi shell`.

Keyboard Shortcuts for Editing Commands

You can use various keyboard shortcuts to enter and edit commands in the appliance Bash shell.

Table 4-1. Keyboard Shortcuts and Function

Keyboard Shortcut	Details
Tab	Completes the current command. If you enter a part of the command name and press the Tab key, the system completes the command name. To view the commands that match a set of characters that you enter, type a character and press the Tab key.
Enter (at the command line)	Runs the command that you entered.
Enter (at the More prompt)	Displays the next page of output.
Delete or Backspace	Deletes the character that is on the left of the cursor.
Left arrow or Ctrl+B	Moves the cursor one character to the left. When you enter a command that extends beyond a single line, you can press the Left Arrow or Ctrl-B keys to go back to the beginning of the command.
Right arrow or Ctrl+F	Moves the cursor one character to the right.
Esc, B	Moves the cursor one word back.
Esc, F	Moves the cursor one word forward.

Table 4-1. Keyboard Shortcuts and Function (continued)

Keyboard Shortcut	Details
Ctrl+A	Moves the cursor to the beginning of the command line.
Ctrl+E	Moves the cursor to the end of the command line.
Ctrl+D	Deletes the character selected by the cursor.
Ctrl+W	Deletes the word next to the cursor.
Ctrl+K	Deletes the line forward. When you press Ctrl+K, everything that you entered starting from the cursor location to the end of the command line is deleted.
Ctrl+U or Ctrl+X	Deletes the line backward. When you press Ctrl+U, everything from the beginning of the command line to the cursor location is deleted.
Ctrl+T	Changes the places of the character to the left of the cursor with the character selected by the cursor.
Ctrl+R or Ctrl+L	Displays the system prompt and command line.
Ctrl+V or Esc, Q	Inserts a code to indicate to the system that the following keystroke must be treated as a command entry, not as an editing key.
Up arrow, or Ctrl+P	Recalls commands in the history buffer, beginning with the most recent command.
Down arrow or Ctrl+N	Returns to more recent commands in the history buffer after you use the Up arrow or Ctrl+P to recall commands.
Ctrl+Y	Recalls the most recent entry in the delete buffer. The delete buffer contains the last 10 items you have cut or deleted.
Esc, Y	Recalls the next entry in the delete buffer. The delete buffer contains the last 10 items you have cut or deleted. Press Ctrl+Y first to recall the most recent entry, and then press Esc, Y up to nine times to recall the remaining entries in the buffer.
Esc, C	Capitalizes the character selected by the cursor.
Esc, U	Changes the casing for all characters in the word selected by the cursor, up to the next space, to uppercase.
Esc, L	Changes the capitalized letters in a word from the character selected by the cursor to the end of the word to lowercase.

Get Help About the Plug-Ins and API Commands in the Appliance

You can access the vCenter Server plug-ins and API commands from the appliance shell. You can use the plug-ins and commands for monitoring, troubleshooting, and configuring the appliance.

You can use the Tab key to autocomplete API commands, plug-in names, and API parameters. Plug-in parameters do not support autocompletion.

Procedure

- 1 Access the appliance shell and log in.

- 2 To get help about the plug-ins, run the `help pi list` or the `? pi list` command.
You receive a list with all the plug-ins in the appliance.
- 3 To get help about the API commands, run the `help api list` or the `? api list` command.
You receive a list with all the API commands in the appliance.
- 4 To get help about a particular API command, run the `help api api_name` or the `? api api_name` command.
For example, to receive help about the `com.vmware.appliance.version1.timesync.set` command, run `help api timesync.set` or `? api timesync.set`.

Plug-Ins in the vCenter Server Shell

The plug-ins in vCenter Server provide you with access to various administrative tools. The plug-ins reside in the CLI itself. The plug-ins are standalone Linux or VMware utilities, which do not depend on any VMware service.

Table 4-2. Plug-Ins Available in the vCenter Server

Plug-In	Description
<code>com.vmware.clear</code>	A plug-in that you can use to clear the terminal screen.
<code>com.vmware.cmsso-util</code>	A plug-in that you use for orchestrating changes to PNID, Machine Certificate, unregistering a node from Component Manager, vCenter Single Sign-On, and reconfiguring vCenter Server.
<code>com.vmware.dcli</code>	vAPI based CLI client.
<code>com.vmware.nslookup</code>	A plug-in that you can use to query the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.
<code>com.vmware.pgrep</code>	A plug-in that you can use to search for all named processes.
<code>com.vmware.pgtop</code>	A plug-in that you can use to monitor the PostgreSQL database.
<code>com.vmware.ping</code>	A plug-in that you can use to ping a remote host. Accepts the same arguments as <code>bin/ping</code> .
<code>com.vmware.ping6</code>	A plug-in that you can use to ping a remote host. Accepts the same arguments as <code>bin/ping6</code> .
<code>com.vmware.portaccess</code>	A plug-in that you can use to troubleshoot the port access of a host.
<code>com.vmware.ps</code>	A plug-in that you can use to see statistics on running processes.
<code>com.vmware.rvc</code>	Ruby vSphere Console
<code>com.vmware.service-control</code>	A plug-in that you can use to manage VMware services.

Table 4-2. Plug-Ins Available in the vCenter Server (continued)

Plug-In	Description
<code>com.vmware.shell</code>	A plug-in that allows access to the appliance Bash shell.
<code>com.vmware.showlog</code>	A plug-in that you can use to browse the log files.
<code>com.vmware.shutdown</code>	A plug-in that you can use to restart or power off the appliance.
<code>com.vmware.software-packages</code>	A plug-in that you can use to update the software packages in the appliance.
<code>com.vmware.support-bundle</code>	A plug-in that you can use to create a bundle on the local file system and export it to a remote Linux system. If you use the plug-in with the <code>stream</code> command, the support bundle is not created on the local file system, but is directly exported to the remote Linux system.
<code>com.vmware.top</code>	A plug-in that displays process information. Accepts the same arguments as <code>/usr/bin/top/</code> .
<code>com.vmware.tracepath</code>	A plug-in that traces the path to a network host. Accepts the same arguments as <code>/sbin/tracepath</code> .
<code>com.vmware.tracepath6</code>	A plug-in that traces the path to a network host. Accepts the same arguments as <code>/sbin/tracepath6</code> .
<code>com.vmware.updatemgr-util</code>	A plug-in that you can use to configure VMware Update Manager.
<code>com.vmware.vcenter-restore</code>	A plug-in that you can use to restore vCenter Server.
<code>com.vmware.vimtop</code>	A plug-in that you can use to view a list of vSphere services and their resource use.

Browse the Log Files By Using the showlog Plug-In

You can browse the log files in vCenter Server to examine them for errors.

Procedure

- 1 Access the appliance shell and log in.
- 2 Type the `showlog` command, add a space, and press the Tab key to view all the contents of the `/var/log` folder.
- 3 Run the command for viewing the firstboot log files.

```
showlog /var/log/firstboot/cloudvm.log
```

API Commands in the Appliance Shell

The API commands in vCenter Server let you perform various administrative tasks. The API commands are provided by appliance management service. You can edit time synchronization settings, monitor processes and services, set up the SNMP settings, and so on.

Table 4-3. API Commands Available in vCenter Server

API Command	Description
<code>com.vmware.appliance.health.applmgmt.get</code>	Get the health of the applmgmt service.
<code>com.vmware.appliance.health.databasestorage.get</code>	Get the health of the database storage.
<code>com.vmware.appliance.health.load.get</code>	Get the CPU load health.
<code>com.vmware.appliance.health.mem.get</code>	Get the memory health.
<code>com.vmware.appliance.health.softwarepackages.get</code>	Get the health of the system update.
<code>com.vmware.appliance.health.storage.get</code>	Get the overall storage health.
<code>com.vmware.appliance.health.swap.get</code>	Get the swap health.
<code>com.vmware.appliance.health.system.get</code>	Get the system health.
<code>com.vmware.appliance.health.system.lastcheck</code>	Get the time of the last check of the health status.
<code>com.vmware.appliance.monitoring.list</code>	Get a list of monitored items.
<code>com.vmware.appliance.monitoring.get</code>	Get monitored item information.
<code>com.vmware.appliance.monitoring.query</code>	Query a range of values for the monitored items.
<code>com.vmware.appliance.recovery.backup.job.cancel</code>	Cancel a backup job by id.
<code>com.vmware.appliance.recovery.backup.job.create</code>	Start a backup job.
<code>com.vmware.appliance.recovery.backup.job.get</code>	Get a status of the backup job by id.
<code>com.vmware.appliance.recovery.backup.job.list</code>	Get a list of backup jobs.
<code>com.vmware.appliance.recovery.backup.parts.list</code>	Get a list of the vCenter Server components that can be included in a backup job.
<code>com.vmware.appliance.recovery.backup.parts.get</code>	Get detailed info for a backup part.
<code>com.vmware.appliance.recovery.backup.validate</code>	Validate parameters for a backup job without starting the job.
<code>com.vmware.appliance.recovery.restore.job.cancel</code>	Cancel a restore job.
<code>com.vmware.appliance.recovery.restore.job.create</code>	Start a restore job.
<code>com.vmware.appliance.recovery.restore.job.get</code>	Get status of the restore job.

Table 4-3. API Commands Available in vCenter Server (continued)

API Command	Description
<code>com.vmware.appliance.recovery.restore.validate</code>	Validate restore parameters of a restore job without starting the job.
<code>com.vmware.appliance.system.uptime.get</code>	Gets the system uptime.
<code>com.vmware.appliance.version1.access.consolecli.get</code>	Get information about the state of the console-based controlled CLI (TTY1).
<code>com.vmware.appliance.version1.access.consolecli.set</code>	Set enabled state of console-based controlled CLI (TTY1).
<code>com.vmware.appliance.version1.access.dcu.get</code>	Get information about the state of the Direct Console User Interface (DCUI TTY2).
<code>com.vmware.appliance.version1.access.dcu.set</code>	Set enabled state of the Direct Console User Interface (DCUI TTY2).
<code>com.vmware.appliance.version1.access.shell.get</code>	Get information about the state of Bash shell, that is, access to Bash shell from within the controlled CLI.
<code>com.vmware.appliance.version1.access.shell.set</code>	Set enabled state of Bash shell, that is, access to Bash shell from within the controlled CLI.
<code>com.vmware.appliance.version1.access.ssh.get</code>	Get enabled state of the SSH-based controlled CLI.
<code>com.vmware.appliance.version1.access.ssh.set</code>	Set enabled state of the SSH-based controlled CLI.
<code>com.vmware.appliance.version1.localaccounts.user.add</code>	Create a new local user account.
<code>com.vmware.appliance.version1.localaccounts.user.delete</code>	Delete a local user account.
<code>com.vmware.appliance.version1.localaccounts.user.get</code>	Get the local user account information.
<code>com.vmware.appliance.version1.localaccounts.user.list</code>	List local user accounts.
<code>com.vmware.appliance.version1.localaccounts.user.password.update</code>	Update the password of a logged in user or of the user that you specify in the <code>username</code> parameter.
<code>com.vmware.appliance.version1.localaccounts.user.set</code>	Update local user account properties, such as role, full name, enabled status, and password.
<code>com.vmware.appliance.version1.monitoring.snmp.disable</code>	Stop an enabled SNMP agent.
<code>com.vmware.appliance.version1.monitoring.snmp.enable</code>	Start a disabled SNMP agent.
<code>com.vmware.appliance.version1.monitoring.snmp.get</code>	Return an SNMP agent configuration.
<code>com.vmware.appliance.version1.monitoring.snmp.hash</code>	Generate localized keys for secure SNMPv3 communications.

Table 4-3. API Commands Available in vCenter Server (continued)

API Command	Description
<code>com.vmware.appliance.version1.monitoring.snmp.limits</code>	Get SNMP limits information.
<code>com.vmware.appliance.version1.monitoring.snmp.reset</code>	Restore settings to factory defaults.
<code>com.vmware.appliance.version1.monitoring.snmp.set</code>	Set SNMP configuration.
<code>com.vmware.appliance.version1.monitoring.snmp.stats</code>	Generate diagnostics report for SNMP agent.
<code>com.vmware.appliance.version1.networking.dns.domains.add</code>	Add domains to DNS search domains.
<code>com.vmware.appliance.version1.networking.dns.domains.list</code>	Get a list of DNS search domains.
<code>com.vmware.appliance.version1.networking.dns.domains.set</code>	Set DNS search domains.
<code>com.vmware.appliance.version1.networking.dns.hostname.get</code>	Get the Fully Qualified Domain Name.
<code>com.vmware.appliance.version1.networking.dns.hostname.set</code>	Set the Fully Qualified Domain Name.
<code>com.vmware.appliance.version1.networking.dns.servers.add</code>	Add a DNS server. This method fails if you use DHCP.
<code>com.vmware.appliance.version1.networking.dns.servers.get</code>	Get DNS server configuration.
<code>com.vmware.appliance.version1.networking.dns.servers.set</code>	Set the DNS server configuration. If the host is configured to acquire DNS servers and host name by using DHCP, a DHCP refresh is forced.
<code>com.vmware.appliance.version1.networking.firewall.addr.inbound.add</code>	Add a firewall rule to allow or deny access from an incoming IP address.
<code>com.vmware.appliance.version1.networking.firewall.addr.inbound.delete</code>	Delete a specific rule at a given position or delete all rules.
<code>com.vmware.appliance.version1.networking.firewall.addr.inbound.list</code>	Get an ordered list of inbound IP addresses that are allowed or denied by a firewall rule.
<code>com.vmware.appliance.version1.networking.interfaces.get</code>	Get information about a particular network interface.
<code>com.vmware.appliance.version1.networking.interfaces.list</code>	Get a list of available network interfaces, including interfaces that are not yet configured.
<code>com.vmware.appliance.version1.networking.ipv4.get</code>	Get IPv4 network configuration for interfaces.
<code>com.vmware.appliance.version1.networking.ipv4.list</code>	Get IPv4 network configuration for all configured interfaces.
<code>com.vmware.appliance.version1.networking.ipv4.renew</code>	Renew IPv4 network configuration on interfaces. If the interface is configured to use DHCP for IP address assignment, the lease of the interface is renewed.

Table 4-3. API Commands Available in vCenter Server (continued)

API Command	Description
<code>com.vmware.appliance.version1.networking.ipv4.set</code>	Set IPv4 network configuration for an interface.
<code>com.vmware.appliance.version1.networking.ipv6.get</code>	Get IPv6 network configuration for interfaces.
<code>com.vmware.appliance.version1.networking.ipv6.list</code>	Get IPv6 network configuration for all configured interfaces.
<code>com.vmware.appliance.version1.networking.ipv6.set</code>	Set IPv6 network configuration for an interface.
<code>com.vmware.appliance.version1.networking.routes.add</code>	Add static routing rules. A destination/prefix of the type 0.0.0.0/0 (for IPv4) or ::/0 (for IPv6) refers to the default gateway.
<code>com.vmware.appliance.version1.networking.routes.delete</code>	Delete static routing rules.
<code>com.vmware.appliance.version1.networking.routes.list</code>	Get routing table. A destination/prefix of the type 0.0.0.0/0 (for IPv4) or ::/0 (for IPv6) refers to the default gateway.
<code>com.vmware.appliance.version1.ntp.get</code>	Get NTP configuration settings. If you run the <code>timesync.get</code> command, you can retrieve the current time synchronization method (by using NTP or VMware Tools). The <code>ntp.get</code> command always returns the NTP server information, even when the time synchronization method is not set to NTP. If time synchronization method is not set by using NTP, the NTP status is displayed as down.
<code>com.vmware.appliance.version1.ntp.server.add</code>	Add NTP servers. This command adds NTP servers to the configuration. If the time synchronization is NTP-based, then NTP daemon is restarted to reload the new NTP servers. Otherwise, this command just adds servers to the NTP configuration.
<code>com.vmware.appliance.version1.ntp.server.delete</code>	Delete NTP servers. This command deletes NTP servers from the configuration. If the time synchronization mode is NTP-based, the NTP daemon is restarted to reload the new NTP configuration. Otherwise, this command just deletes servers from the NTP configuration.

Table 4-3. API Commands Available in vCenter Server (continued)

API Command	Description
<code>com.vmware.appliance.version1.ntp.server.set</code>	Set NTP servers. This command deletes old NTP servers from the configuration and sets the input NTP servers in the configuration. If the time synchronization is set by using NTP, the NTP daemon is restarted to reload the new NTP configuration. Otherwise, this command just replaces the servers in NTP configuration with the NTP servers that you provide as input.
<code>com.vmware.appliance.version1.resources.cpu.stats.get</code>	Get CPU statistics.
<code>com.vmware.appliance.version1.resources.load.health.get</code>	Get load health.
<code>com.vmware.appliance.version1.resources.load.stats.get</code>	Get load averages (over 1, 5, and 15-minute intervals).
<code>com.vmware.appliance.version1.resources.mem.health.get</code>	Get memory health.
<code>com.vmware.appliance.version1.resources.mem.stats.get</code>	Get memory statistics.
<code>com.vmware.appliance.version1.resources.net.stats.get</code>	Get network statistics.
<code>com.vmware.appliance.version1.resources.net.stats.list</code>	Get network statistics for all interfaces that are up and running.
<code>com.vmware.appliance.version1.resources.processes.stats.list</code>	Get statistics on all processes.
<code>com.vmware.appliance.version1.resources.softwarepackages.health.get</code>	Get the health of the update component.
<code>com.vmware.appliance.version1.resources.storage.health.get</code>	Get storage health statistics.
<code>com.vmware.appliance.version1.resources.storage.stats.list</code>	Get storage statistics for each logical disk.
<code>com.vmware.appliance.version1.resources.swap.health.get</code>	Get swap health.
<code>com.vmware.appliance.version1.resources.swap.stats.get</code>	Get swap statistics.
<code>com.vmware.appliance.version1.resources.system.health.get</code>	Get the overall health of the system.
<code>com.vmware.appliance.version1.resources.system.stats.get</code>	Get the system status.
<code>com.vmware.appliance.version1.services.list</code>	Get the list of all known services.
<code>com.vmware.appliance.version1.services.restart</code>	Restart a service.
<code>com.vmware.appliance.version1.services.status.get</code>	Get the status of a service.
<code>com.vmware.appliance.version1.services.stop</code>	Stop a service.
<code>com.vmware.appliance.version1.system.storage.list</code>	Gets disk to partition mapping.

Table 4-3. API Commands Available in vCenter Server (continued)

API Command	Description
<code>com.vmware.appliance.version1.system.storage.resize</code>	Resizes all partitions to 100 percent of disk size.
<code>com.vmware.appliance.version1.system.time.get</code>	Gets system time.
<code>com.vmware.appliance.version1.system.update.get</code>	Get the URL-based patching configuration.
<code>com.vmware.appliance.version1.system.update.set</code>	Set the URL-based patching configuration.
<code>com.vmware.appliance.version1.system.version.get</code>	Get the version of the appliance.
<code>com.vmware.appliance.version1.timesync.get</code>	Get the time synchronization configuration.
<code>com.vmware.appliance.version1.timesync.set</code>	Set the time synchronization configuration.

Configuring SNMP for vCenter Server

vCenter Server includes an SNMP agent that can send trap notifications and receive `GET`, `GETBULK`, and `GETNEXT` requests.

You can use the appliance shell API commands to enable and configure the vCenter Server SNMP agent. You configure the agent differently depending on whether you want to use SNMP v1/v2c or SNMP v3.

SNMP v3 informs are not supported. vCenter Server supports only notifications such as v1 and v2c traps, and v3 traps with all security levels.

Configure the SNMP Agent for Polling

If you configure the vCenter Server SNMP agent for polling, it can listen for and respond to requests from SNMP management client systems, such as `GET`, `GETNEXT`, and `GETBULK` requests.

By default, the embedded SNMP agent listens on UDP port 161 for polling requests from management systems. You can use the `snmp.set --port` command to configure an alternative port. To avoid conflicts between the port for the SNMP agent and the ports of other services, use a UDP port that is not defined in `/etc/services`.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is `root`.

- 2 Run the `snmp.set --port` command to configure the port.

For example, run the following command:

```
snmp.set --port port
```

Here *port* is the port for the SNMP agent to use for listening for polling requests.

Important The port you specify must not be already in use by other services. Use IP addresses from the dynamic range, port 49152 and up.

- 3 (Optional) If the SNMP agent is not enabled, enable it by running the `snmp.enable` command.

Configure vCenter Server for SNMP v1 and v2c

When you configure the vCenter Server SNMP agent for SNMP v1 and v2c, the agent supports sending notifications and receiving `GET` requests.

In SNMP v1 and v2c, community strings are namespaces that contain one or more managed objects. Namespaces can act as a form for authentication, but this does not secure the communication. To secure the communication, use SNMP v3.

Procedure

- 1 [Configure SNMP Communities](#)

To enable the vCenter Server SNMP agent to send and receive SNMP v1 and v2c messages, you must configure at least one community for the agent.

- 2 [Configure the SNMP Agent to Send v1 or v2c Notifications](#)

You can use the vCenter Server SNMP agent to send virtual machine and environmental notifications to management systems.

Configure SNMP Communities

To enable the vCenter Server SNMP agent to send and receive SNMP v1 and v2c messages, you must configure at least one community for the agent.

An SNMP community defines a group of devices and management systems. Only devices and management systems that are members of the same community can exchange SNMP messages. A device or management system can be a member of multiple communities.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 Run the `snmp.set --communities` command to configure an SNMP community.

For example, to configure public, east, and west network operation center communities, run the following command:

```
snmp.set --communities public,eastnoc,westnoc
```

Each time you specify a community with this command, the settings you specify overwrite the previous configuration.

To specify multiple communities, separate the community names with a comma.

Configure the SNMP Agent to Send v1 or v2c Notifications

You can use the vCenter ServerSNMP agent to send virtual machine and environmental notifications to management systems.

To send SNMP v1 and v2c notifications with the SNMP agent, you must configure the target, that is the receiver, unicast address, community, and an optional port. If you do not specify a port, the SNMP agent sends notifications to UDP port 162 on the target management system by default.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 Run the `snmp.set --targets` command:

```
snmp.set --targets target_address@port/community
```

Here *target_address*, *port*, and *community* are the address of the target system, the port number to send the notifications to, and the community name, respectively. The port value is optional. If you do not specify a port, the default port,161, is used.

Each time you specify a target with this command, the settings you specify overwrite all previously specified settings. To specify multiple targets, separate them with a comma.

For example, run the following command for configuring the targets 192.0.2.1@678/targetcommunity and 2001:db8::1/anothercom:

```
snmp.set --targets 192.0.2.1@678/targetcommunity,2001:db8::1/anothercom
```

- 3 (Optional) If the SNMP agent is not enabled, enable it by running the `snmp.enable` command.
- 4 (Optional) To send a test trap to verify that the agent is configured correctly, run the `snmp.test` command.

The agent sends a `warmStart` trap to the configured target.

Configure vCenter Server for SNMP v3

When you configure the SNMP agent for SNMP v3, the agent supports sending traps. SNMP v3 also provides stronger security than v1 or v2c, including cryptographic authentication and encryption.

SNMP v3 informs are not supported. vCenter Server supports only notifications such as v1/v2c traps and v3 traps with all security levels.

Procedure

1 Configure the SNMP Engine ID

Every SNMP v3 agent has an engine ID, which serves as a unique identifier for the agent. The engine ID is used with a hashing function to generate localized keys for authentication and encryption of SNMP v3 messages.

2 Configure SNMP Authentication and Privacy Protocols

SNMP v3 optionally supports authentication and privacy protocols.

3 Configure SNMP Users

You can configure up to five users who can access SNMP v3 information. User names must be no more than 32 characters long.

4 Configure SNMP v3 Targets

Configure SNMP v3 targets to allow the SNMP agent to send SNMP v3 traps.

Configure the SNMP Engine ID

Every SNMP v3 agent has an engine ID, which serves as a unique identifier for the agent. The engine ID is used with a hashing function to generate localized keys for authentication and encryption of SNMP v3 messages.

If you do not specify an engine ID before you enable the SNMP agent, when you enable the standalone SNMP agent, an engine ID is generated.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 Run the `snmp.set --engineid` command to configure the target.

For example, run the following command:

```
snmp.set --engineid 80001adc802417e202b8613f5400000000
```

Here, 80001adc802417e202b8613f5400000000 is the ID, a hexadecimal string between 5 and 32 characters in length.

Configure SNMP Authentication and Privacy Protocols

SNMP v3 optionally supports authentication and privacy protocols.

Authentication is used to ensure the identity of users. Privacy allows for encryption of SNMP v3 messages to ensure confidentiality of data. The privacy protocols provide a higher level of security than is available in SNMP v1 and v2c, which use community strings for security.

Both authentication and privacy are optional. However, you must enable authentication if you plan to enable privacy.

The SNMP v3 authentication and privacy protocols are licensed vSphere features and might not be available in some vSphere editions.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 (Optional) Run the `snmp.set --authentication` command to configure authentication.

For example, run the following command:

```
snmp.set --authentication protocol
```

Here, *protocol* must be either **none**, for no authentication, **SHA1**, or **MD5**.

- 3 (Optional) Run the `snmp.set --privacy` command to configure privacy protocol.

For example, run the following command:

```
snmp.set --privacy protocol
```

Here, *protocol* must be either **none**, for no privacy, or **AES128**.

Configure SNMP Users

You can configure up to five users who can access SNMP v3 information. User names must be no more than 32 characters long.

While configuring a user, you generate authentication and privacy hash values based on the user's authentication and privacy passwords and on the SNMP agent's engine ID. After configuring users, if you change the engine ID, the authentication protocol, or the privacy protocol, the users are no longer valid and must be reconfigured.

Prerequisites

- Verify that you have configured the authentication and privacy protocols before configuring users.

- Verify that you know the authentication and privacy passwords for each user that you plan to configure. Passwords must be at least eight characters long. Store these passwords in files on the host system.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 If you are using authentication or privacy, get the authentication and privacy hash values for the user by the running `snmp.hash --auth_hash --priv_hash` command.

For example, run the following command:

```
snmp.hash --auth_hash secret1 --priv_hash secret2
```

Here, *secret1* is the path to the file containing the user's authentication password and *secret2* is the path to the file containing the user's privacy password. Alternatively, you can specify the flag `--raw_secret` and set the boolean parameter to *true*.

The authentication and privacy hash values are displayed.

- 3 Configure the user by running `snmp.set --user`.

For example, run the following command:

```
snmp.set --user userid/authhash/privhash/security
```

The parameters in the command are as follows.

Parameter	Description
<i>userid</i>	Replace with the user name.
<i>authhash</i>	Replace with the authentication hash value.
<i>privhash</i>	Replace with the privacy hash value.
<i>security</i>	Replace with the level of security enabled for that user, which can be auth , for authentication only, priv , for authentication and privacy, or none , for no authentication or privacy.

Configure SNMP v3 Targets

Configure SNMP v3 targets to allow the SNMP agent to send SNMP v3 traps.

You can configure a maximum of three SNMP v3 targets, in addition to a maximum of three SNMP v1 or v2c targets.

To configure a target, you must specify a host name or IP address of the system that receives the traps, a user name, a security level, and whether to send traps. The security level can be either **none**, for no security, **auth**, for authentication only, or **priv**, for authentication and privacy.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 Run the `snmp.set --v3targets` command to set up the SNMP v3 target.

For example, run the following command:

```
snmp.set --v3targets hostname@port/userid/secLevel/trap
```

The parameters in the command are as follows.

Parameter	Description
<i>hostname</i>	Replace with the host name or IP address of the management system that receives the traps.
<i>port</i>	Replace with the port on the management system that receives the traps. If you do not specify a port, the default port, 161, is used.
<i>userid</i>	Replace with the user name.
<i>secLevel</i>	Replace with either none , auth , or priv to indicate the level of authentication and privacy you have configured. Use auth if you have configured authentication only, priv if you have configured both authentication and privacy, and none if you have configured neither.

- 3 (Optional) If the SNMP agent is not enabled, enable it by running the `snmp.enable` command.
- 4 (Optional) To send a test trap to verify that the agent is configured correctly, run the `snmp.test` command.

The agent sends a `warmStart` trap to the configured target.

Configure the SNMP Agent to Filter Notifications

You can configure the vCenter Server SNMP agent to filter out notifications if you do not want your SNMP management software to receive those notifications.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 Run the `snmp.set --notraps` command to filter traps.

- To filter specific traps, run the following command:

```
snmp.set --notraps oid_list
```

Here, *oid_list* is a list of object IDs for the traps to filter, separated by commas. This list replaces any object IDs that were previously specified using this command.

- To clear all trap filters, run the following command:

```
snmp.set --notraps reset
```

- 3 (Optional) If the SNMP agent is not enabled, enable it by running the `snmp.enable` command.

Results

The traps identified by the specified object IDs are filtered out of the output of the SNMP agent, and are not sent to SNMP management software.

Configure SNMP Management Client Software

After you have configured vCenter Server to send traps, you must configure your management client software to receive and interpret those traps.

To configure your management client software, specify the communities for the managed device, configure the port settings, and load the VMware MIB files. See the documentation for your management system for specific instructions for these steps.

Prerequisites

Download the VMware MIB files from <https://kb.vmware.com/s/article/1013445>.

Procedure

- 1 In your management software, specify the vCenter Server instance as an SNMP-based managed device.
- 2 If you are using SNMP v1 or v2c, set up appropriate community names in the management software.

These names must correspond to the communities set for the SNMP agent on vCenter Server.
- 3 If you are using SNMP v3, configure users and authentication and privacy protocols to match the protocols configured on vCenter Server.
- 4 If you configured the SNMP agent to send traps to a port on the management system other than the default UDP port 162, configure the management client software to listen on the port you configured.
- 5 Load the VMware MIBs into the management software to view the symbolic names for the vCenter Server variables.

To prevent lookup errors, load these MIB files in the following order before loading other MIB files:

- a `VMWARE-ROOT-MIB.mib`
- b `VMWARE-TC-MIB.mib`
- c `VMWARE-PRODUCTS-MIB.mib`

Results

The management software can now receive and interpret traps from vCenter Server.

Reset SNMP Settings to Factory Defaults

You can reset SNMP settings to factory defaults. You can also reset the value of a specific argument to the factory default.

You can reset a specific argument, such as the communities or targets. You can also reset the SNMP configuration to the factory defaults.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 To reset specific arguments, run the command `snmp.set --arguments reset`.

For example, to reset the communities that you configured, run the following command:

```
snmp.set --communities reset
```

- 3 To reset the whole SNMP configuration to the factory defaults, run the command `snmp.reset`.

Configuring Time Synchronization Settings in vCenter Server

You can change the time synchronization settings in vCenter Server after deployment.

When you deploy vCenter Server, you can choose the time synchronization method to be either by using an NTP server or by using VMware Tools. In case the time settings in your vSphere network change, you can edit the vCenter Server and configure the time synchronization settings by using the commands in the appliance shell.

When you enable periodic time synchronization, VMware Tools sets the time of the guest operating system to be the same as the time of the host.

After time synchronization occurs, VMware Tools checks once every minute to determine whether the clocks on the guest operating system and the host still match. If not, the clock on the guest operating system is synchronized to match the clock on the host.

Native time synchronization software, such as Network Time Protocol (NTP), is typically more accurate than VMware Tools periodic time synchronization and is therefore preferred. You can use only one form of periodic time synchronization in vCenter Server. If you decide to use native time synchronization software, vCenter Server VMware Tools periodic time synchronization is disabled, and the reverse.

Use VMware Tools Time Synchronization

You can set up vCenter Server to use VMware Tools time synchronization.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 Run the command to enable VMware Tools time synchronization.

```
timesync.set --mode host
```

- 3 (Optional) Run the command to verify that you successfully applied the VMware Tools time synchronization.

```
timesync.get
```

The command returns that the time synchronization is in host mode.

Results

The time of the appliance is synchronized with the time of the ESXi host.

Add or Replace NTP Servers in the vCenter Server Configuration

To set up the vCenter Server to use NTP-based time synchronization, you must add the NTP servers to the vCenter Server configuration.

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 Add NTP servers to the vCenter Server configuration by running the `ntp.server.add` command.

For example, run the following command:

```
ntp.server.add --servers IP-addresses-or-host-names
```

Here *IP-addresses-or-host-names* is a comma-separated list of IP addresses or host names of the NTP servers.

This command adds NTP servers to the configuration. If the time synchronization is based on an NTP server, then the NTP daemon is restarted to reload the new NTP servers. Otherwise, this command adds the new NTP servers to the existing NTP configuration.

- 3 (Optional) To delete old NTP servers and add new ones to the vCenter Server configuration, run the `ntp.server.set` command.

For example, run the following command:

```
ntp.server.set --servers IP-addresses-or-host-names
```

Here *IP-addresses-or-host-names* is a comma-separated list of IP addresses or host names of the NTP servers.

This command deletes old NTP servers from the configuration and sets the input NTP servers in the configuration. If the time synchronization is based on an NTP server, the NTP daemon is restarted to reload the new NTP configuration. Otherwise, this command replaces the servers in NTP configuration with the servers that you provide as input.

- 4 (Optional) Run the command to verify that you successfully applied the new NTP configuration settings.

```
ntp.get
```

The command returns a space-separated list of the servers configured for NTP synchronization. If the NTP synchronization is enabled, the command returns that the NTP configuration is in Up status. If the NTP synchronization is disabled, the command returns that the NTP configuration is in Down status.

What to do next

If the NTP synchronization is disabled, you can configure the time synchronization settings in the vCenter Server to be based on an NTP server. See [Synchronize the Time in vCenter Server with an NTP Server](#).

Synchronize the Time in vCenter Server with an NTP Server

You can configure the time synchronization settings in the vCenter Server to be based on an NTP server.

Prerequisites

Set up one or more Network Time Protocol (NTP) servers in the vCenter Server configuration. See [Add or Replace NTP Servers in the vCenter Server Configuration](#).

Procedure

- 1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

- 2 Run the command to enable NTP-based time synchronization.

```
timesync.set --mode NTP
```

- 3 (Optional) Run the command to verify that you successfully applied the NTP synchronization.

```
timesync.get
```

The command returns that the time synchronization is in NTP mode.

Managing Local User Accounts in vCenter Server

If you log in to the appliance shell as a super administrator, you can manage the local user accounts in vCenter Server by running commands in the appliance shell. The default user with a super administrator role is root.

User Roles in vCenter Server

There are three main user roles in vCenter Server.

The local users of vCenter Server have the rights to perform various tasks. Three user roles are available in vCenter Server:

Operator

Local users with the operator user role can read vCenter Server configuration.

Administrator

Local users with the administrator user role can configure vCenter Server.

Super Administrator

Local users with the super administrator user role can configure vCenter Server, manage the local accounts, and use the Bash shell.

Get a List of the Local User Accounts in vCenter Server

You can see the list of the local user accounts so that you can decide which user account to manage from the appliance shell.

Procedure

- 1 Access the appliance shell and log in as a user who has a super administrator role.

The default user with a super administrator role is root.

- 2 Run the `localaccounts.user.list` command.

You can see a list of the local users. The information about a user includes the user name, status, role, status of the password, full name, and email.

Note The list of local users includes only the local users who have their default shell as appliance shell.

Create a Local User Account in vCenter Server

You can create a new local user account.

For information about the user roles, see [User Roles in vCenter Server](#).

Procedure

- 1 Access the appliance shell and log in as a user who has a super administrator role.

The default user with a super administrator role is root.

- 2 Run the `localaccounts.user.add --role --username --password` command.

For example, to add the local user account test with the operator user role, run the following command:

```
localaccounts.user.add --role operator --username test --password
```

The role can be **operator**, **admin**, or **superAdmin**.

You can also set up a new local user account and specify an email and the full name of the user. For example, to add the local user account test1 with the operator user role, full name TestName and the email address test1@mymail.com, run the following command:

```
localaccounts.user.add --role operator --username test1 --password --fullname TestName --email test1@mymail.com
```

You cannot use spaces in full names.

- 3 Enter and confirm the password of the new local user when prompted.

Results

You created a new local user in the appliance.

Update the Password of a Local User in vCenter Server

You can update the password of a local user in vCenter Server for security reasons.

Procedure

- 1 Access the appliance shell and log in as a user who has a super administrator role.

The default user with a super administrator role is root.

- 2 Run the `localaccounts.user.password.update --username user name --password` command.

For example, to change the password of a user with user name test, run the following command:

```
localaccounts.user.password.update --username test --password
```

- 3 Enter and confirm the new password when prompted.

Update a Local User Account in vCenter Server

You can update an existing local user account in vCenter Server.

For information about the user roles, see [User Roles in vCenter Server](#).

Procedure

- 1 Access the appliance shell and log in as a user who has a super administrator role.

The default user with a super administrator role is root.

- 2 Run the `localaccounts.user.set --username` command to update an existing local user.

- To update the role of the local user, run the following command:

```
localaccounts.user.set --username user name --role new role
```

Here, *user name* is the name of the user that you want to edit and *new role* is the new role. The role can be **operator**, **admin**, or **superAdmin**.

- To update the email of the local user, run the following command:

```
localaccounts.user.set --username user name --email new email address
```

Here, *user name* is the name of the user that you want to edit and *new email address* is the new email address.

- To update the full name of the local user, run the following command:

```
localaccounts.user.set --username user name --fullname new full name
```

Here, *user name* is the name of the user that you want to edit and *new full name* is the new full name of the user.

- To update the status of the local user, run the following command:

```
localaccounts.user.set --username user name --status new status
```

Here, *user name* is the name of the user that you want to edit and *status* is the new status of the local user. The status can be either **disabled** or **enabled**.

Delete a Local User Account in vCenter Server

You can delete a local user account in vCenter Server.

Procedure

- 1 Access the appliance shell and log in as a user who has a super administrator role.

The default user with a super administrator role is root.

- 2 Run the `localaccounts.user.delete --username` command.

For example, to delete the user with user name test, run the following command:

```
localaccounts.user.delete --username test
```

The user is deleted.

Monitor Health Status and Statistics in vCenter Server

You can monitor the hardware health status of vCenter Server by using the API commands in the appliance shell. You can also monitor the health status of the update component for information about available patches.

You can view the status of the hardware components such as memory, CPU, storage, and network, as well as the update component that shows if the software packages are up to date according to the last check for available patches.

A particular health status can be green, yellow, orange, red, or gray. For more information, see [View vCenter Server Health Status](#).

For a complete list of the API commands that you can use for monitoring statistics and health of the vCenter Server system, see [API Commands in the Appliance Shell](#).

Procedure

- 1 Access the appliance shell and log in.

The user name that you use to log in can be of a user with an operator, administrator, or super administrator user role.

- 2 View the health status of a particular component.

- To view the health of the memory in vCenter Server, run the `mem.health.get` command.
- To view the health of the storage in vCenter Server, run the `storage.health.get` command.
- To view the health of the swap in vCenter Server, run the `swap.health.get` command.
- To view the health of the update component in vCenter Server, run the `softwarepackages.health.get` command.

Important If you do not perform regular checks for available patches, the health status of the update component might become out-of-date. For information about checking for vCenter Server patches and enabling automatic checks for vCenter Server patches, see [vSphere Upgrade](#).

- To view the overall health of the vCenter Server system, run the `system.health.get` command.

- 3 To view statistics about a particular hardware component, run the respective command.

For example, to view storage statistics for each logical disk, run the `storage.stats.list` command.

Using the vimtop Plug-In to Monitor the Resource Use of Services

You can use the `vimtop` utility plug-in to monitor vSphere services that run in the vCenter Server.

`vimtop` is a tool similar to `esxtop`, which runs in the environment of the vCenter Server. By using the text-based interface of `vimtop` in the appliance shell, you can view overall information about the vCenter Server, and a list of vSphere services and their resource use.

- [Monitor Services By Using vimtop in Interactive Mode](#)

You can use the `vimtop` plug-in to monitor services in real time.

- [Interactive Mode Command-Line Options](#)

You can use various command-line options when you run the `vimtop` command to enter the plug-in interactive mode.

- [Interactive Mode Single-Key Commands for vimtop](#)

When running in interactive mode, `vimtop` recognizes several single-key commands.

Monitor Services By Using vimtop in Interactive Mode

You can use the `vimtop` plug-in to monitor services in real time.

The default view of the `vimtop` interactive mode consists of the overview tables and the main table. You can use single-key commands in interactive mode to switch the view from processes to disks or network.

Procedure

- 1 From an SSH client application, log in to the vCenter Server shell.
- 2 Run the `vimtop` command to access the plug-in in interactive mode.

Interactive Mode Command-Line Options

You can use various command-line options when you run the `vimtop` command to enter the plug-in interactive mode.

Table 4-4. Interactive Mode Command-Line Options

Option	Description
-h	Prints help for the <code>vimtop</code> command-line options.
-v	Prints the <code>vimtop</code> version number.

Table 4-4. Interactive Mode Command-Line Options (continued)

Option	Description
<code>-c filename</code>	Loads a user-defined <code>vimtop</code> configuration file. If the <code>-c</code> option is not used, the default configuration file is <code>/root/vimtop/vimtop.xml</code> . You can create your own configuration file, specifying a different filename and path by using the <code>w</code> single-key interactive command.
<code>-n number</code>	Sets the number of performed iterations before the <code>vimtop</code> exits interactive mode. <code>vimtop</code> updates the display <code>number</code> number of times and exits. The default value is 10000.
<code>-p / -d seconds</code>	Sets the update period in seconds.

Interactive Mode Single-Key Commands for vimtop

When running in interactive mode, `vimtop` recognizes several single-key commands.

All interactive mode panels recognize the commands listed in the following table.

Table 4-5. Interactive Mode Single-Key Commands

Key Names	Description
<code>h</code>	Show a help menu for the current panel, giving a brief summary of commands, and the status of secure mode.
<code>i</code>	Show or hide the top line view of the overview panel of the <code>vimtop</code> plug-in.
<code>t</code>	Show or hide the Tasks section, which displays information in the overview panel about the tasks currently running on the vCenter Server instance.
<code>m</code>	Show or hide the Memory section in the overview panel.
<code>f</code>	Show or hide the CPU section which displays information in the overview panel about all available CPUs.
<code>g</code>	Show or hide the CPUs section which displays information in the overview panel about the top 4 physical CPUs.
<code>spacebar</code>	Immediately refreshes the current pane.
<code>p</code>	Pause the displayed information about the services resource use in the current panels.
<code>r</code>	Refresh the displayed information about the services resource use in the current panels.
<code>s</code>	Set refresh period.
<code>q</code>	Exit the interactive mode of the <code>vimtop</code> plug-in.
<code>k</code>	Displays the Disks view of the main panel.
<code>o</code>	Switch the main panel to Network view.
<code>Esc</code>	Clear selection or return to the Processes view of the main panel.
<code>Enter</code>	Select a service to view additional details.
<code>n</code>	Show or hide names of the headers in the main panel.

Table 4-5. Interactive Mode Single-Key Commands (continued)

Key Names	Description
u	Show or hide the measurement units in the headers in the main panel.
left, right arrows	Select columns.
up, down arrows	Select rows.
<, >	Move a selected column.
Delete	Remove selected column.
c	Add a column to the current view of the main panel. Use spacebar to add or remove columns from the displayed list.
a	Sort the selected column in ascending order.
d	Sort the selected column in descending order.
z	Clear the sort order for all columns.
l	Set width for the selected column.
x	Return the column widths to their default values.
+	Expand selected item.
-	Collapse selected item.
w	Write the current setup to a <code>vimtop</code> configuration file. The default file name is the one specified by <code>-c</code> option, or <code>/root/vimtop/vimtop.xml</code> if the <code>-c</code> option is not used. You can also specify a different file name on the prompt generated by the <code>w</code> command.

Using the Direct Console User Interface to Configure vCenter Server

5

After you deploy vCenter Server, you can reconfigure the network settings and enable access to the Bash shell for troubleshooting. To access the Direct Console User Interface, you must log in as root.

The home page of the Direct Console User Interface contains a link to the support bundle of the vCenter Server. The link to the support bundle is of the type `https://appliance-host-name:443/appliance/support-bundle`.

This chapter includes the following topics:

- [Log In to the Direct Console User Interface](#)
- [Change the Password of the Root User](#)
- [Configure the Management Network of vCenter Server](#)
- [Restart the Management Network of vCenter Server](#)
- [Enable Access to the Bash Shell](#)
- [Access the Bash Shell for Troubleshooting](#)
- [Export a vCenter Server Support Bundle for Troubleshooting](#)

Log In to the Direct Console User Interface

The Direct Console User Interface lets you interact with vCenter Server locally by using text-based menus.

Procedure

- 1 From the vSphere Client, navigate to the host and click **Configure > Services**. Confirm that the SSH and Direct Console User Interface services are running.
- 2 Open an SSH client and connect to the vCenter Server.
- 3 Log in with the root account.
- 4 Enter **DCUI** to start the Direct Console User Interface.
- 5 Click inside the console window and press F2 to customize the system.

- 6 Type the password for the root user and press Enter.

Important If you enter invalid credentials thrice, the root account is locked for five minutes.

Results

You logged in to the Direct Console User Interface. You can change the password of the root user, edit the network settings, and enable access to the vCenter Server appliance Bash shell.

Change the Password of the Root User

To prevent unauthorized access to the vCenter Server Direct Console User Interface, you can change the password of the root user.

The default root password for the vCenter Server instance is the password you enter during deployment.

Important The password for the root account of vCenter Server expires after 90 days. You can change the expiry time for an account by logging as root to the vCenter Server Bash shell, and running `chage -M number_of_days -W warning_until_expiration user_name`. To increase the expiration time of the root password to infinity, run the `chage -M -1 -E -1 root` command.

Procedure

- 1 Log in to the Direct Console User Interface.
- 2 Select **Configure Password** and press Enter.
- 3 Type the old password of the root user, and press Enter.
- 4 Set up the new password and press Enter.
- 5 Press Esc until you return to the main menu of the Direct Console User Interface.

Results

You changed the password of the root user of the appliance.

Configure the Management Network of vCenter Server

The vCenter Server instance can obtain networking settings from a DHCP server, or use static IP addresses. You can change the networking settings of vCenter Server from the Direct Console User Interface. You can change the IPv4, IPv6, and DNS configuration.

Prerequisites

To change the IP address of the vCenter Server instance, verify that the system name is an FQDN. If, during deployment you set an IP address as a system name, you cannot change the IP address after the deployment. The system name is always used as a primary network identifier.

Procedure

- 1 Log in to the Direct Console User Interface of vCenter Server
- 2 Select **Configure Management Network** and press Enter.
- 3 Change the IPv4 settings from **IP Configuration**.

Option	Description
Use dynamic IP address and network configuration	Obtains networking settings from a DHCP server if one is available on your network
Set static IP address and network configuration	Sets static networking configuration

- 4 Change the IPv6 settings from **IPv6 Configuration**.

Option	Description
Enable IPv6	Enables or disables IPv6
Use DHCP stateful configuration	Uses a DHCP server to obtain IPv6 addresses and networking settings
Use ICMP stateless configuration	Uses a Stateless Address Autoconfiguration (SLAAC) to obtain IPv6 addresses and network settings

- 5 Change the DNS settings from **DNS Configuration**.

Option	Description
Obtain DNS server address and hostname automatically	Obtains the DNS server address and host name automatically. Use this option if the IP settings are obtained automatically from a DHCP server.
Use the following DNS server address and hostname	Sets the static IP address and host name for the DNS server.

- 6 Set custom DNS suffixes from **Custom DNS Suffixes**.
If you do not specify any suffixes, a default suffix list is derived from the local domain name.
- 7 Press Esc until you return to the main menu of the Direct Console User Interface.

Restart the Management Network of vCenter Server

Restart the management network of vCenter Server to restore the network connection.

Procedure

- 1 Log in to the Direct Console User Interface of vCenter Server.
- 2 Select **Restart Management Network** and press Enter.
- 3 Press F11.

Enable Access to the Bash Shell

You can use the Direct Console User Interface to enable local and remote access to the Bash shell. Bash shell access enabled through Direct Console User Interface remains enabled for 3600 seconds.

Procedure

- 1 Log in to the Direct Console User Interface of vCenter Server.
- 2 Select **Troubleshooting Options** and press Enter.
- 3 From the Troubleshooting Mode Options menu, select to enable either Bash shell or SSH.
- 4 Press Enter to enable the service.
- 5 Press Esc until you return to the main menu of the Direct Console User Interface.

What to do next

Access the vCenter Server Bash shell for troubleshooting.

Access the Bash Shell for Troubleshooting

Log in to the Bash shell for troubleshooting purposes only.

Procedure

- 1 Access the shell using one of the following methods.
 - If you have direct access to the vCenter Server instance, press Alt+F1.
 - If you want to connect remotely, use SSH or another remote console connection to start a session.
- 2 Enter a user name and password.
- 3 In the shell, enter the command `pi shell` or `shell` to access the Bash shell.

Export a vCenter Server Support Bundle for Troubleshooting

You can export the support bundle of the vCenter Server instance in the appliance for troubleshooting using the URL displayed on the DCUI home screen.

You can also collect the support bundle from the vCenter Server appliance Bash shell by running the `vc-support.sh` script.

The support bundle is exported in `.tgz` format.

Procedure

- 1 Log in to the Windows host machine on which you want to download the bundle.

- 2 Open a Web browser and enter the URL to the support bundle displayed in the DCUI.

`https://appliance-fully-qualified-domain-name:443/appliance/support-bundle`

- 3 Enter the user name and password of the root user.

- 4 Click **Enter**.

The support bundle is downloaded as `.tgz` file on your Windows machine.

- 5 (Optional) To determine which firstboot script failed, examine the `firstbootStatus.json` file.

If you ran the `vc-support.sh` script in the vCenter Server appliance Bash shell, to examine the `firstbootStatus.json` file, run

```
cat /var/log/firstboot/firstbootStatus.json
```