vCenter Server Appliance Configuration

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Contents

About vCenter Server Appliance Configuration

vCenter Server Appliance Configuration provides information about configuring the VMware vCenter® Server Appliance™.

Intended Audience

This information is intended for anyone who wants to use the vCenter Server Appliance to run VMware vCenter Server® and VMware Platform Services Controller®. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

vSphere Web Client and vSphere Client

Task instructions in this guide are based on the vSphere Web Client. You can also perform most of the tasks in this guide by using the new vSphere Client. The new vSphere Client user interface terminology, topology, and workflow are closely aligned with the same aspects and elements of the vSphere Web Client user interface. You can apply the vSphere Web Client instructions to the new vSphere Client unless otherwise instructed.

NOTE   Not all functionality in the vSphere Web Client has been implemented for the vSphere Client in the vSphere 6.5 release. For an up-to-date list of unsupported functionality, see *Functionality Updates for the vSphere Client Guide* at http://www.vmware.com/info?id=1413.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Updated Information

This *vCenter Server Appliance Configuration* is updated with each release of the product or when necessary.

This table provides the update history of the *vCenter Server Appliance Configuration*.

Revision	Description
04 OCT 2017	■ Updated log in information in "Join the vCenter Server Appliance to an Active Directory Domain," on page 21
EN-002607-00	Initial release.

vCenter Server Appliance Overview 1

The vCenter Server Appliance is a preconfigured Linux virtual machine, which is optimized for running VMware vCenter Server® and the associated services on Linux.

During the deployment of the appliance, you select a deployment type of vCenter Server with an embedded Platform Services Controller, Platform Services Controller, or vCenter Server with an external Platform Services Controller. When you deploy a Platform Services Controller appliance, you can create a VMware vCenter® Single Sign-On™ domain or join an existing domain. For information about the vCenter Server and Platform Services Controller deployment types and the deployment topologies with external Platform Services Controller instances, see *vSphere Installation and Setup*.

The vCenter Server Appliance is supported on VMware ESXi™ 5.5 and later. The appliance package contains the following software:

- Project Photon OS® 1.0

- PostgreSQL database

- vCenter Server 6.5 and vCenter Server 6.5 components

- Platform Services Controller that contains all the necessary services for running vCenter Server such as vCenter Single Sign-On, License service, and VMware Certificate Authority

  For detailed information about the Platform Services Controller, see *Platform Services Controller Administration*.

Customization of the vCenter Server Appliance is unsupported except for adding memory, CPU, and disk space.

The vCenter Server Appliance 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 Appliance Management Interface and to the appliance Linux operating system.

  IMPORTANT The password for the root account of the vCenter Server Appliance expires after 365 days by default. For information about how to change the root password and configure the password expiration settings, see "Change the Password and Password Expiration Settings of the Root User," on page 16.

- 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.

  In vSphere 5.5, this user is administrator@vsphere.local. In vSphere 6.0, when you install vCenter Server or deploy the vCenter Server Appliance with a new Platform Services Controller, 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 in the vCenter Server Appliance. 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 access the vCenter Server Appliance and edit the vCenter Server Appliance settings in four ways:

■   Use the vCenter Server Appliance Management Interface.

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

■   Use the VMware vSphere® Web Client.

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

■   Use the appliance shell.

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

■   Use the Direct Console User Interface.

You can use TTY2 to log in to the vCenter Server Appliance 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.

Starting with vSphere 6.5, the vCenter Server Appliance supports high availability. For information about configuring vCenter Server Appliance in a vCenter High Availability cluster, see *vSphere Availability*.

Starting with vSphere 6.5, the vCenter Server Appliance and Platform Services Controller appliance support file-based backup and restore. For information about backing up and restoring, see *vSphere Installation and Setup*.

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

After you deploy the vCenter Server Appliance that contains vCenter Server with an embedded Platform Services Controller, vCenter Server with an external Platform Services Controller, or a Platform Services Controller, you can log in to the vCenter Server Appliance Management Interface and edit the appliance settings.

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

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

This chapter includes the following topics:

Log In to the vCenter Server Appliance Management Interface

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

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

Prerequisites

- Verify that the vCenter Server Appliance is successfully deployed and running.

■ If you are using Internet Explorer, verify that TLS 1.0, TLS 1.1, and TLS 1.2 are enabled in the security settings.

Procedure

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

2 Log in as root.

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

View the vCenter Server Appliance Health Status

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

The overall health status of the vCenter Server Appliance is based on the status of the hardware components such as memory, CPU, storage, and network. 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 Appliance patches and enable automatic checks for vCenter Server Appliance patches, see *vSphere Upgrade*.

For information about how to view the individual status, see "Monitor Health Status and Statistics in the vCenter Server Appliance," on page 52.

Prerequisites

Log in to the vCenter Server Appliance Management Interface as root.

Procedure

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

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

Table 2-1. Health Status

Badge Icon	Description
🟢	Good. All components in the appliance are healthy.
🟡	Warning. One or more components in the appliance might become overloaded soon. View the details in the Health Messages pane.
🟠	Alert. One or more components in the appliance might be degraded. Nonsecurity patches might be available. View the details in the Health Messages pane.
🔴	Critical. One or more components in the appliance might be in an unusable status and the appliance 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 the vCenter Server Appliance

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

Prerequisites

Log in to the vCenter Server Appliance Management Interface as root.

Procedure

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

2 Click **Reboot** or **Shutdown** to restart or power off the virtual machine.

3 In the confirmation dialog box, click **Yes** to confirm the operation.

Export a Support Bundle

You can export 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 Appliance Management Interface as root.

Procedure

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

2 Click **Create Support Bundle**, and save the bundle on your local machine.

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

Enable or Disable SSH and Bash Shell Access

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

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

Prerequisites

Log in to the vCenter Server Appliance Management Interface as root.

Procedure

1 In the vCenter Server Appliance Management Interface, click **Access**, and click **Edit**.

2 Edit the access settings for the vCenter Server Appliance.

Option	Description
Enable SSH login	Enables SSH access to the vCenter Server Appliance.
Enable Bash shell	Enables Bash shell access to the vCenter Server Appliance 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 assign static IPv4 and IPv6 addresses, edit the DNS settings, and define the proxy settings for the vCenter Server Appliance.

Prerequisites

■ To change the IP address of the appliance, 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 change the IP address after the deployment, because the system name is used as a primary network identifier.

> **NOTE** You cannot change the primary network identifier after you deploy the vCenter Server Appliance.

■ Log in to the vCenter Server Appliance Management Interface as root.

Procedure

1 In the vCenter Server Appliance Management Interface, click **Networking** and click **Manage**.

2 In the Hostname, Name Servers, and Gateways pane, click **Edit**.

3 In the Name Servers section, configure the DNS settings.

Option	Description
Obtain DNS settings automatically	Obtains the DNS settings automatically from the network.
Enter settings manually	Lets you set the DNS address settings manually. If you select this option, you must provide the following information: ■ The IP address of the preferred DNS server. ■ (Optional) The IP address of the alternative DNS server.

4 In the Default Gateways section, enter an IPv4 or IPv6 gateway address.

5 In the Networking Interfaces pane, click **Edit**.

6 Expand the network interface name to edit the IP address settings.

7 Edit the IPv4 address settings.

Option	Description
Disable IPv4 settings	Disables the IPv4 address. The appliance uses only an IPv6 address.
Obtain IPv4 settings automatically	Obtains the IPv4 address for the appliance automatically from the network .
Use the following IPv4 settings	Uses an IPv4 address that you set manually. You must enter the IP address, subnet prefix length, and the default gateway.

8   Edit the IPv6 settings.

Option	Description
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.
Static IPv6 addresses	Uses static IPv6 addresses that you set up manually. 1 Click the **Add** icon. 2 Enter the IPv6 address and the subnet prefix length. 3 Click **OK**. 4 (Optional) Edit the default gateway.

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.

9   To configure a proxy server, in the Proxy Settings pane, click **Edit**.

10   Select **Use a Proxy Server**, enter the proxy server settings, and click **OK**.

Configure the System Time Zone and Time Synchronization Settings

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

When you deploy the vCenter Server Appliance, you either use the time settings of the ESXi host on which the appliance 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.

IMPORTANT   If the vCenter Server Appliance is using an external Platform Services Controller, you must configure both the vCenter Server Appliance and the Platform Services Controller to use the same time synchronization source. Otherwise, authentication with vCenter Single Sign-On might fail.

Prerequisites

Log in to the vCenter Server Appliance Management Interface as root.

Procedure

1   In the vCenter Server Appliance 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 **OK**.

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 **OK**.

Change the Password and Password Expiration Settings of the Root User

When you deploy the vCenter Server Appliance, you set the initial password of the root user, which expires after 365 days by default. For security reasons, you can change the root password and the password expiration settings.

Prerequisites

Log in to the vCenter Server Appliance Management Interface as root.

Procedure

1   In the vCenter Server Appliance Management Interface, click **Administration**.

2   In the Change root password pane, change the root password and click **Submit**.

3   Configure the password expiration settings for the root user.

a   In the Root password expires section, set the password expiration policy.

Option	Description
Yes	The password of the root user expires after a particular number of days. You must provide the following information: ■ **Root password validity (days)** The number of days after which the password expires. ■ **Email for expiration warning** The email address to which the vCenter Server Appliance sends a warning message before the expiration date.
No	The password of the root user never expires.

b   In the Password expiry settings pane, click **Submit** to apply the new password expiry settings.

In the Password expires on text box, you can see the new expiration date.

Redirect vCenter Server Appliance Log Files to Another Machine

You can redirect the vCenter Server Appliance log files to another machine, for example, if you want to preserve storage space on the vCenter Server Appliance.

Prerequisites

Log in to the vCenter Server Appliance Management Interface as root.

Procedure

1 In the vCenter Server Appliance Management Interface, select **Syslog Configuration**.

2 Click **Edit**.

3 From the **Common Log Level** drop-down menu, select the log files to redirect.

Option	Description
*	All log files are redirected to the remote machine.
info	Only informational log files are redirected to the remote machine.
notice	Only notices are redirected to the remote machine. Notice indicates normal but significant condition.
warn	Only warnings are redirected to the remote machine.
error	Only error messages are redirected to the remote machine.
crit	Only critical log files are redirected to the remote machine.
alert	Only alerts are redirected to the remote machine. Alert indicates that action must be taken immediately.
emerg	Only emergency log files are redirected to the remote machine. Emergency indicates that the system stopped responding and cannot be used.

4 In the **Remote Syslog Host** text box, enter the FQDN or IP address of the machine on which you want to export the log files.

5 In the **Remote Syslog Port** text box, enter the port number to use for communication with the machine on which you want to export the log files.

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

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

7 Click **OK**.

The new configuration settings are shown in the Remote Syslog Configuration pane.

8 (Optional) To stop redirecting log files to another machine, click **Reset**.

Monitor Network Use

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

Prerequisites

Log in to the vCenter Server Appliance Management Interface as root.

Procedure

1 In the vCenter Server Appliance Management Interface, click **Networking**.

2 From the **Network Utilization** drop-down menu, select the time period for generating the network utilization graph.

3   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.

4   Point to the network utilization graph to see the network use data for a particular date and time.

Monitor CPU and Memory Use

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

Prerequisites

Log in to the vCenter Server Appliance Management Interface as root.

Procedure

1   In the vCenter Server Appliance Management Interface, click **CPU and Memory**.

2   From the **Overall CPU Utilization Trending** drop-down menu, select the time period for which you want to generate a CPU utilization trending graph.

3   Point to the CPU graph to see the CPU use for a particular date and time.

4   From the **Overall Memory Utilization Trending** drop-down menu, select the time period for which you want to generate a memory utilization trending graph.

5   Point to the memory graph to see the memory use for a particular date and time.

Monitor Database Use

You can use the vCenter Server Appliance Management Interface to monitor the use of the embedded database of the vCenter Server Appliance 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 Appliance Management Interface as root.

Procedure

1   In the vCenter Server Appliance Management Interface, click **Database**.

2   In the **Current Utilization** pane, you can monitor the consumed and free space for the vCenter Server Appliance database.

Data File System	Description
VC DB SEAT	Stats, events, alarms, and tasks data that is generated for the hosts and virtual machines managed by the vCenter Server instance running in the vCenter Server Appliance.
Transaction Log	Internal database transaction logging data that is used for recovery from failures and other purposes.
VC Inventory	Inventory data that describes the hosts and virtual machines managed by the vCenter Server instance running in the vCenter Server Appliance.

3   From the **Overall current space utilization trending** drop-down menu, select the time period for which you want to generate the space utilization trending graphs.

4   Click the colored radio button of a particular database component to include or exclude that component from the graph.

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

Using the vSphere Web Client to Configure the vCenter Server Appliance

3

After you deploy the vCenter Server Appliance, you can perform some configuration operations from the vSphere Web Client such as joining the appliance to an Active Directory domain, managing the services that are running in the vCenter Server Appliance, networking, and other settings.

This chapter includes the following topics:

Join the vCenter Server Appliance to an Active Directory Domain

You can join a Platform Services Controller appliance or a vCenter Server Appliance with an embedded Platform Services Controller to an Active Directory domain. You can attach the users and groups from this Active Directory domain to your vCenter Single Sign-On domain.

IMPORTANT Joining a Platform Services Controller appliance or a vCenter Server Appliance with an embedded Platform Services Controller to an Active Directory domain with a read-only domain controller (RODC) is unsupported. You can join a Platform Services Controller or a vCenter Server Appliance with an embedded Platform Services Controller only to an Active Directory domain with a writable domain controller.

If you want to configure permissions for users and groups from an Active Directory domain to access the vCenter Server components, you must join its associated embedded or external Platform Services Controller instance to the Active Directory domain.

For example, to enable an Active Directory user to log in to the vCenter Server instance in a vCenter Server Appliance with an embedded Platform Services Controller by using the vSphere Web Client with Windows session authentication (SSPI), you must join the vCenter Server Appliance to the Active Directory domain and assign the Administrator role to this user. To enable an Active Directory user to log in to a vCenter Server instance that uses an external Platform Services Controller appliance by using the vSphere Web Client with SSPI, you must join the Platform Services Controller appliance 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 in the vCenter Server Appliance 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 the vCenter Server Appliance to an Active Directory domain.

Procedure

1 Use the vSphere Web Client to log in as administrator@*your_domain_name* to the vCenter Server instance in the vCenter Server Appliance.

2 On the vSphere Web Client main page, hover over the **Home** icon, click **Home**, and select **System Configuration**.

3 Under Deployment, click **System Configuration**.

4 Under System Configuration, click **Nodes**.

5 Under Nodes, select a node and click the **Manage** tab.

6 Under Advanced, select **Active Directory**, and click **Join**.

7 Enter the Active Directory details.

Option	Description
Domain	Active Directory domain name, for example, mydomain.com. Do not provide an IP address in this text box.
Organizational unit	Optional. The full OU LDAP FQDN, for example, OU=Engineering,DC=mydomain,DC=com. **IMPORTANT** Use this text box only if you are familiar with LDAP.
User name	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.

8 Click **OK** to join the vCenter Server Appliance to the Active Directory domain.

The operation silently succeeds and you can see the Join button turned to Leave.

9 Right-click the node you edited and select **Reboot** to restart the appliance so that the changes are applied.

IMPORTANT If you do not restart the appliance, you might encounter problems when using the vSphere Web Client.

10 Navigate to **Administration > Single Sign-On > Configuration**.

11 On the **Identity Sources** tab, click the **Add Identity Source** icon.

12   Select **Active Directory (Integrated Windows Authentication)**, enter the identity source settings of the joined Active Directory domain, and click **OK**.

Table 3-1. 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.
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 (SPN)	SPN that helps Kerberos to identify the Active Directory service. Include the domain in the name, for example, STS/example.com.
	You might have to run `setspn -S` to add the user you want to use. See the Microsoft documentation for information on `setspn`.
	The SPN must be unique across the domain. Running `setspn -S` checks that no duplicate is created.
User Principal Name (UPN)	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.

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

What to do next

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

Leave an Active Directory Domain

After you joined the vCenter Server Appliance, you can log in to the vSphere Web Client and set up the vCenter Server Appliance to leave the Active Directory domain.

Prerequisites

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

Procedure

1   Use the vSphere Web Client to log in as administrator@*your_domain_name* to the vCenter Server instance in the vCenter Server Appliance.

The address is of the type http://*appliance-IP-address-or-FQDN*/vsphere-client.

2   On the vSphere Web Client main page, hover over the **Home** icon, click **Home**, and select **System Configuration**.

3   Under System Configuration, click **Nodes**.

4   Under Nodes, select a node and click the **Manage** tab.

5   Under Advanced, select **Active Directory** and click **Leave**.

6   Type the Active Directory user name and password.

7   Click **OK** to leave the Active Directory domain.

8   Click the **Actions** menu, and select **Reboot** to restart the appliance so that the changes are applied.

Add a User to the SystemConfiguration.BashShellAdministrators Group

To enable access to the vCenter Server Appliance Bash shell by using the vSphere Web 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 Web Client to log in as administrator@*your_domain_name* to the vCenter Server instance in the vCenter Server Appliance.

    The address is of the type http://*appliance-IP-address-or-FQDN*/vsphere-client.

2   Click **Administration**.

3   Under Single Sign-On, click **Users and Groups**.

4   On the **Groups** tab, select the **SystemConfiguration.BashShellAdministrators** group.

5   In the **Group Members** pane, click the **Add member** icon.

6   Double-click users from the list or type names in the **Users** text box.

7   Click **OK**.

Edit Access Settings to the vCenter Server Appliance

You can use the vSphere Web Client to enable local and remote access to the appliance.

Prerequisites

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

To enable access to the vCenter Server Appliance Bash shell, verify that the user name you use to log in to the vCenter Server instance in the vCenter Server Appliance is a member of the SystemConfiguration.BashShellAdministrators group. For information about adding a user to the SystemConfiguration.BashShellAdministrators group, see "Add a User to the SystemConfiguration.BashShellAdministrators Group," on page 24.

Procedure

1   Use the vSphere Web Client to log in as administrator@*your_domain_name* to the vCenter Server instance in the vCenter Server Appliance.

    The address is of the type http://*appliance-IP-address-or-FQDN*/vsphere-client.

2   On the vSphere Web Client main page, hover over the **Home** icon, click **Home**, and select **System Configuration**.

3   Under System Configuration, click **Nodes**.

4   Under Nodes, select a node and click the **Manage** tab.

5   Under Common, select **Access** and click **Edit**.

6   Select how you can access the vCenter Server Appliance.

Option	Description
Enable local login	Enables local login to the vCenter Server Appliance console.
Enable SSH login	Enables SSH access to the vCenter Server Appliance.
Enable Bash shell access	Enables Bash shell access to the vCenter Server Appliance for the number of minutes that you enter.
	This option is available only when the user name you use to log in to the vCenter Server instance in the vCenter Server Appliance is a member of the SystemConfiguration.BashShellAdministrators group.

7   Click **OK** to save the settings.

Edit the DNS and IP Address Settings of the vCenter Server Appliance

After you deploy the vCenter Server Appliance, you can edit the DNS settings and specify which DNS server to use. You can edit the IP address settings of the vCenter Server Appliance. You can also specify whether to use IPv4 and IPv6 or only IPv6, and how the appliance obtains the IP address.

You can edit these settings by using the vSphere Web Client.

Prerequisites

■   To change the IP address of the appliance, 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 change the IP address after the deployment. The system name is always used as a primary network identifier.

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

Procedure

1   Use the vSphere Web Client to log in as administrator@*your_domain_name* to the vCenter Server instance in the vCenter Server Appliance.

    The address is of the type http://*appliance-IP-address-or-FQDN*/vsphere-client.

2   On the vSphere Web Client main page, hover over the **Home** icon, click **Home**, and select **System Configuration**.

3   Under System Configuration, click **Nodes**.

4   Under Nodes, select a node and click the **Manage** tab.

5   Under **Common**, select **Networking**, and click **Edit**.

6   Expand **DNS** and edit the settings.

Option	Description
Obtain DNS server address automatically	Obtains the DNS settings automatically from the network.
Enter settings manually	Lets you specify the DNS address settings manually. If you select this option, you must provide: ■ **Hostname** Name of the vCenter Server Appliance machine. ■ **Preferred DNS server** IP address of the preferred DNS server. ■ **Alternate DNS server** IP address of the alternate DNS server. ■ **Search domains** Restricts the domain when looking up an address. Domains that you type, are searched in the order you list them, and the search stops when a valid name is found.

7   Expand the network interface name to edit the IP address settings.

8   Edit the IPv4 address settings.

Option	Description
No IPv4 settings	Disables the IPv4 address. The appliance uses only an IPv6 address.
Obtain IPv4 settings automatically	Obtains the IPv4 address for the appliance automatically from the network.
Use the following IPv4 settings	Uses an IPv4 address that you set manually. You must enter the IP address, subnet prefix length, and the default gateway.

9   Edit the IPv6 settings.

Option	Description
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.
Static IPv6 addresses	Uses static IPv6 addresses that you set up manually. 1 Click the **Add** icon. 2 Enter the IPv6 address and the subnet prefix length. 3 Click **OK**. 4 (Optional) Edit the default gateway.

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.

10   (Optional) Delete a dynamic IPv6 address.

a   Click **Remove addresses**.

b   Select the IP address to delete and click the **Delete** icon (✖).

c   Click **OK**.

11   Click **OK** to save your edits.

Edit the Firewall Settings of the vCenter Server Appliance

After you deploy the vCenter Server Appliance, you can edit the firewall settings of the vCenter Server Appliance and can create firewall rules. You can edit the firewall settings by using the vSphere Web Client.

By using the firewall rules, you can allow or block the traffic between the vCenter Server Appliance and specific servers, hosts, or virtual machines. You cannot block specific ports, you block all of the traffic.

Prerequisites

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

Procedure

1   Use the vSphere Web Client to log in as administrator@*your_domain_name* to the vCenter Server instance in the vCenter Server Appliance.

    The address is of the type http://*appliance-IP-address-or-FQDN*/vsphere-client.

2   On the vSphere Web Client main page, hover over the **Home** icon, click **Home**, and select **System Configuration**.

3   Under System Configuration, click **Nodes**.

4   Under Nodes, select a node and click the **Manage** tab.

5   Under Advanced, select **Firewall** and click **Edit**.

6   Edit the firewall settings.

Option	Action
Add a firewall rule	a Click the **Add** icon (✚) to create a new firewall rule. b Select a network interface of the virtual machine . c Type an IP address of the network to apply this rule on. The IP address can be IPv4 and IPv6 address. d Type a subnet prefix length. e From the **Action** drop-down menu, select whether to block or to allow the connection between the vCenter Server Appliance and the network that you specified. f Click **OK**.
Edit a firewall rule	a Click the **Edit** icon (✏) to edit a firewall rule. b Edit the settings of the rule. c Click **OK**.
Prioritize the rules	a Click the down or up arrows to move a rule downwards or upwards in the list of rules.
Delete a firewall rule	a Select a rule from the list, and click the **Delete** icon (✖). b Click **OK**.

7   Click **OK** to save your edits.

Edit the Startup Settings of a Service

The Message Bus Configuration, ESXi Dump Collector, and Auto Deploy services are optional services in the vCenter Server Appliance and they are not running by default. You can edit the startup settings of these services in the vCenter Server Appliance.

Prerequisites

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

Procedure

1   Use the vSphere Web Client to log in as administrator@*your_domain_name* to the vCenter Server instance in the vCenter Server Appliance.

     The address is of the type http://*appliance-IP-address-or-FQDN*/vsphere-client.

2   On the vSphere Web Client main page, hover over the **Home** icon, click **Home**, and select **System Configuration**.

3   Under System Configuration, click **Nodes** and select a node from the list.

4   Click the **Related Objects** tab.

     You see the list of services running in the node you selected.

5   Right-click a service, such as **Auto Deploy**, **ESXi Dump Collector**, or **Message Bus Configuration Service**, and select **Edit Startup Type**.

6   Select how you want the service to start.

Option	Description
Automatic	The service starts automatically when the Operating System starts.
Manual	You start the service manually after the Operating System starts.
Disabled	The service is disabled.

7   Click **OK**.

Start, Stop, or Restart Services in the vCenter Server Appliance

In the vSphere Web Client, you can start, stop, or restart the services that are running in the vCenter Server Appliance.

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   Log in as administrator@*your_domain_name* to the vCenter Server instance in the vCenter Server Appliance by using the vSphere Web Client.

2   On the vSphere Web Client Home page, click **System Configuration**.

3   Under System Configuration, click **Nodes** and select a node from the list.

4   Click the **Related Objects** tab.

     You see a list of services running in the node you selected.

5   From the **Actions** menu, select an operation.

You can start, stop, and restart the service.

View the Health Status of Services and Nodes

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

vCenter Server instances and machines that run vCenter Server services are considered nodes. Graphical badges represent the health status of services and 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   Log in as administrator@*your_domain_name* to the vCenter Server instance by using the vSphere Web Client.

2   On the vSphere Web Client Home page, click **System Configuration**.

You can view the health status badges for the services and nodes.

Table 3-2. 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.

3   (Optional) In the Services Health and Nodes Health panes, click the hyperlink next to the health badge to view all services and nodes in this health state.

For example, in the Services Health pane, click the hyperlink of the Warning health status. In the dialog box that pops up, select a service to view more information about the service and attempt to resolve the health issues of the service.

Edit the Settings of Services

The vSphere Web Client lists all manageable services running on vCenter Server. You can edit the settings for some of the services.

The vSphere Web Client displays information about all manageable services running in vCenter Server and the vCenter Server Appliance. A list of the default services is available for each vCenter Server instance.

NOTE   Starting with vSphere 6.5, all vCenter Server services and some Platform Services Controller services run as child processes of the VMware Service Lifecycle Manager service.

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   Log in as administrator@*your_domain_name* to the vCenter Server instance by using the vSphere Web Client.

2   On the vSphere Web Client Home page, under Administration, click **System Configuration**.

3   Under System Configuration, click **Nodes** and select a node from the list.

4   Click the **Related Objects** tab.

    You see the list of services running in the node you selected. Editable settings are not available for all manageable services.

5   Right-click a service from the list and click **Settings**.

    Editable settings are not available for all manageable services.

6   On the Manage tab, click the **Edit** button.

7   Edit the service configuration properties.

8   Click **OK** to save the settings.

9   (Optional) From the **Actions** menu, select **Restart**.

    Restart the service only if a restart is required to apply the configuration changes.

Export a Support Bundle

If you have deployed the vCenter Server Appliance with an embedded Platform Services Controller, you can export a support bundle containing the log files for a specific product included in the vCenter Server Appliance or for a specific service in the Platform Services Controller. If you have deployed the vCenter Server Appliance with an external Platform Services Controller, you can export support bundles for specific services or for specific products, depending on the node that you select in the vSphere Web Client.

Prerequisites

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

Procedure

1   Use the vSphere Web Client to log in as administrator@*your_domain_name* to the vCenter Server instance in the vCenter Server Appliance.

    The address is of the type http://*appliance-IP-address-or-FQDN*/vsphere-client.

2   On the vSphere Web Client main page, hover over the **Home** icon, click **Home**, and select **System Configuration**.

3   Under System Configuration, click **Nodes**.

4   Select a node from the list.

5   Click the **Actions** menu and select **Export Support Bundle**.

6   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.

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

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

Using the Appliance Shell to Configure the vCenter Server Appliance 4

You can access all of the vCenter Server Appliance 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

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.

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.
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.

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

Keyboard Shortcut	Details
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 Appliance 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 Appliance Shell

The plug-ins in the vCenter Server Appliance 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 Appliance

Plug-In	Description
`com.vmware.clear`	A plug-in that you can use to clear the terminal screen.
`com.vmware.cmsso-util`	A plug-in that you use for orchestrating changes to PNID, Machine Certificate, unregistering a node from Component Manager, vCenter Single Sign-On, reconfiguring vCenter Server with an embedded Platform Services Controller, and repointing vCenter Server to an external Platform Services Controller.
`com.vmware.dcli`	vAPI based CLI client.

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

Plug-In	Description
`com.vmware.nslookup`	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.
`com.vmware.pgrep`	A plug-in that you can use to search for all named processes.
`com.vmware.pgtop`	A plug-in that you can use to monitor the PostgreSQL database.
`com.vmware.ping`	A plug-in that you can use to ping a remote host. Accepts the same arguments as bin/ping.
`com.vmware.ping6`	A plug-in that you can use to ping a remote host. Accepts the same arguments as bin/ping6.
`com.vmware.portaccess`	A plug-in that you can use to troubleshoot the port access of a host.
`com.vmware.ps`	A plug-in that you can use to see statistics on running processes.
`com.vmware.rvc`	Ruby vSphere Console
`com.vmware.service-control`	A plug-in that you can use to manage VMware services.
`com.vmware.shell`	A plug-in that allows access to the appliance Bash shell.
`com.vmware.showlog`	A plug-in that you can use to browse the log files.
`com.vmware.shutdown`	A plug-in that you can use to restart or power off the appliance.
`com.vmware.software-packages`	A plug-in that you can use to update the software packages in the appliance.
`com.vmware.support-bundle`	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 `stream` command, the support bundle is not created on the local file system, but is directly exported to the remote Linux system.
`com.vmware.top`	A plug-in that displays process information. Accepts the same arguments as /usr/bin/top/.
`com.vmware.tracepath`	A plug-in that traces path to a network host. Accepts the same arguments as /sbin/tracepath.
`com.vmware.tracepath6`	A plug-in that traces path to a network host. Accepts the same arguments as /sbin/tracepath6.
`com.vmware.updatemgr-util`	A plug-in that you can use to configure VMware Update Manager.
`com.vmware.vcenter-restore`	A plug-in that you can use to restore vCenter Server.
`com.vmware.vimtop`	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 the vCenter Server Appliance 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 of the vCenter Server Appliance.

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

API Commands in the vCenter Server Appliance Shell

The API commands in the vCenter Server Appliance let you perform various administrative tasks in the vCenter Server Appliance. The API commands are provided by appliance management service in the vCenter Server Appliance. 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 the vCenter Server Appliance

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

Table 4-3. API Commands Available in the vCenter Server Appliance (Continued)

API Command	Description
com.vmware.appliance.version1.access.consolecli.get	Get information about the state of the console-based controlled CLI (TTY1).
com.vmware.appliance.version1.access.consolecli.set	Set enabled state of console-based controlled CLI (TTY1).
com.vmware.appliance.version1.access.dcui.get	Get information about the state of the Direct Console User Interface (DCUI TTY2).
com.vmware.appliance.version1.access.dcui.set	Set enabled state of the Direct Console User Interface (DCUI TTY2).
com.vmware.appliance.version1.access.shell.get	Get information about the state of Bash shell, that is, access to Bash shell from within the controlled CLI.
com.vmware.appliance.version1.access.shell.set	Set enabled state of Bash shell, that is, access to Bash shell from within the controlled CLI.
com.vmware.appliance.version1.access.ssh.get	Get enabled state of the SSH-based controlled CLI.
com.vmware.appliance.version1.access.ssh.set	Set enabled state of the SSH-based controlled CLI.
com.vmware.appliance.version1.localaccounts.user.add	Create a new local user account.
com.vmware.appliance.version1.localaccounts.user.delete	Delete a local user account.
com.vmware.appliance.version1.localaccounts.user.get	Get the local user account information.
com.vmware.appliance.version1.localaccounts.user.list	List local user accounts.
com.vmware.appliance.version1.localaccounts.user.password.update	Update the password of a logged in user or of the user that you specify in the username parameter.
com.vmware.appliance.version1.localaccounts.user.set	Update local user account properties, such as role, full name, enabled status, and password.
com.vmware.appliance.version1.monitoring.snmp.disable	Stop an enabled SNMP agent.
com.vmware.appliance.version1.monitoring.snmp.enable	Start a disabled SNMP agent.
com.vmware.appliance.version1.monitoring.snmp.get	Return an SNMP agent configuration.
com.vmware.appliance.version1.monitoring.snmp.hash	Generate localized keys for secure SNMPv3 communications.
com.vmware.appliance.version1.monitoring.snmp.limits	Get SNMP limits information.
com.vmware.appliance.version1.monitoring.snmp.reset	Restore settings to factory defaults.
com.vmware.appliance.version1.monitoring.snmp.set	Set SNMP configuration.
com.vmware.appliance.version1.monitoring.snmp.stats	Generate diagnostics report for SNMP agent.
com.vmware.appliance.version1.networking.dns.domains.add	Add domains to DNS search domains.
com.vmware.appliance.version1.networking.dns.domains.list	Get a list of DNS search domains.
com.vmware.appliance.version1.networking.dns.domains.set	Set DNS search domains.
com.vmware.appliance.version1.networking.dns.hostname.get	Get the Fully Qualified Domain Name.
com.vmware.appliance.version1.networking.dns.hostname.set	Set the Fully Qualified Domain Name.
com.vmware.appliance.version1.networking.dns.servers.add	Add a DNS server. This method fails if you use DHCP.

Table 4-3. API Commands Available in the vCenter Server Appliance (Continued)

API Command	Description
com.vmware.appliance.version1.networking.dns.servers.get	Get DNS server configuration.
com.vmware.appliance.version1.networking.dns.servers.set	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.
com.vmware.appliance.version1.networking.firewall.addr.inbound.add	Add a firewall rule to allow or deny access from an incoming IP address.
com.vmware.appliance.version1.networking.firewall.addr.inbound.delete	Delete a specific rule at a given position or delete all rules.
com.vmware.appliance.version1.networking.firewall.addr.inbound.list	Get an ordered list of inbound IP addresses that are allowed or denied by a firewall rule.
com.vmware.appliance.version1.networking.interfaces.get	Get information about a particular network interface.
com.vmware.appliance.version1.networking.interfaces.list	Get a list of available network interfaces, including interfaces that are not yet configured.
com.vmware.appliance.version1.networking.ipv4.get	Get IPv4 network configuration for interfaces.
com.vmware.appliance.version1.networking.ipv4.list	Get IPv4 network configuration for all configured interfaces.
com.vmware.appliance.version1.networking.ipv4.renew	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.
com.vmware.appliance.version1.networking.ipv4.set	Set IPv4 network configuration for an interface.
com.vmware.appliance.version1.networking.ipv6.get	Get IPv6 network configuration for interfaces.
com.vmware.appliance.version1.networking.ipv6.list	Get IPv6 network configuration for all configured interfaces.
com.vmware.appliance.version1.networking.ipv6.set	Set IPv6 network configuration for an interface.
com.vmware.appliance.version1.networking.routes.add	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.
com.vmware.appliance.version1.networking.routes.delete	Delete static routing rules.
com.vmware.appliance.version1.networking.routes.list	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.
com.vmware.appliance.version1.networking.proxy.delete	Delete the proxy configuration for a protocol that you provide as input.
com.vmware.appliance.version1.networking.proxy.get	Get proxy configuration information for all protocols.
com.vmware.appliance.version1.networking.proxy.set	Set proxy configuration for a protocol that you provide as input.

Table 4-3. API Commands Available in the vCenter Server Appliance (Continued)

API Command	Description
com.vmware.appliance.version1.ntp.get	Get NTP configuration settings. If you run the `tymesync.get` command, you can retrieve the current time synchronization method (by using NTP or VMware Tools). The `ntp.get` 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.
com.vmware.appliance.version1.ntp.server.add	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.
com.vmware.appliance.version1.ntp.server.delete	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.
com.vmware.appliance.version1.ntp.server.set	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.
com.vmware.appliance.version1.resources.cpu.stats.get	Get CPU statistics.
com.vmware.appliance.version1.resources.load.health.get	Get load health.
com.vmware.appliance.version1.resources.load.stats.get	Get load averages (over 1, 5, and 15-minute intervals).
com.vmware.appliance.version1.resources.mem.health.get	Get memory health.
com.vmware.appliance.version1.resources.mem.stats.get	Get memory statistics.
com.vmware.appliance.version1.resources.net.stats.get	Get network statistics.
com.vmware.appliance.version1.resources.net.stats.list	Get network statistics for all interfaces that are up and running.
com.vmware.appliance.version1.resources.processes.stats.list	Get statistics on all processes.
com.vmware.appliance.version1.resources.softwarepackages.health.get	Get the health of the update component.
com.vmware.appliance.version1.resources.storage.health.get	Get storage health statistics.
com.vmware.appliance.version1.resources.storage.stats.list	Get storage statistics for each logical disk.
com.vmware.appliance.version1.resources.swap.health.get	Get swap health.

Table 4-3. API Commands Available in the vCenter Server Appliance (Continued)

API Command	Description
`com.vmware.appliance.version1.resources.swap.stats.get`	Get swap statistics.
`com.vmware.appliance.version1.resources.system.health.get`	Get the overall health of the system.
`com.vmware.appliance.version1.resources.system.stats.get`	Get the system status.
`com.vmware.appliance.version1.services.list`	Get the list of all known services.
`com.vmware.appliance.version1.services.restart`	Restart a service.
`com.vmware.appliance.version1.services.status.get`	Get the status of a service.
`com.vmware.appliance.version1.services.stop`	Stop a service.
`com.vmware.appliance.version1.system.storage.list`	Gets disk to partition mapping.
`com.vmware.appliance.version1.system.storage.resize`	Resizes all partitions to 100 percent of disk size.
`com.vmware.appliance.version1.system.time.get`	Gets system time.
`com.vmware.appliance.version1.system.update.get`	Get the URL-based patching configuration.
`com.vmware.appliance.version1.system.update.set`	Set the URL-based patching configuration.
`com.vmware.appliance.version1.system.version.get`	Get the version of the appliance.
`com.vmware.appliance.version1.timesync.get`	Get the time synchronization configuration.
`com.vmware.appliance.version1.timesync.set`	Set the time synchronization configuration.

Configuring SNMP for the vCenter Server Appliance

The vCenter Server Appliance 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 Appliance SNMP agent. You configure the agent differently depending on whether you want to use SNMP v1/v2c or SNMP v3.

In vSphere 6.0, SNMP v3 informs are not supported. The vCenter Server Appliance 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 Appliance 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 the vCenter Server Appliance for SNMP v1 and v2c

When you configure the vCenter Server Appliance 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

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

2

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

Configure SNMP Communities

To enable the vCenter Server Appliance 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 Server Appliance SNMP 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 Appliance 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.

In vSphere 6.0, SNMP v3 informs are not supported. The vCenter Server Appliance supports only notifications such as v1/v2c traps and v3 traps with all security levels.

Procedure

1 Configure the SNMP Engine ID on page 44

   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 on page 44

   SNMP v3 optionally supports authentication and privacy protocols.

3 Configure SNMP Users on page 45

   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 on page 45

   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 seven 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 specify the passwords directly on the command line.

   The authentication and privacy hash values are displayed.

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

   For example, run the following command:

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

   The parameters in the command are as follows.

Parameter	Description
userid	Replace with the user name.
authhash	Replace with the authentication hash value.
privhash	Replace with the privacy hash value.
security	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
hostname	Replace with the host name or IP address of the management system that receives the traps.
port	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.
userid	Replace with the user name.
secLevel	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 Appliance 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.

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 the vCenter Server Appliance 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 the VMware website:
http://communities.vmware.com/community/developer/managementapi.

Procedure

1   In your management software, specify the vCenter Server Appliance 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 the vCenter Server Appliance.

3   If you are using SNMP v3, configure users and authentication and privacy protocols to match the protocols configured on the vCenter Server Appliance.

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 Appliance 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`

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

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 the vCenter Server Appliance

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

When you deploy the vCenter Server Appliance, 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 Appliance 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 the vCenter Server Appliance. If you decide to use native time synchronization software, vCenter Server Appliance VMware Tools periodic time synchronization is disabled, and the reverse.

Use VMware Tools Time Synchronization

You can set up the vCenter Server Appliance 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.

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

Add or Replace NTP Servers in the vCenter Server Appliance Configuration

To set up the vCenter Server Appliance to use NTP-based time synchronization, you must add the NTP servers to the vCenter Server Appliance 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 Appliance 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 just 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 Appliance 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 just 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 Appliance to be based on an NTP server. See "Synchronize the Time in the vCenter Server Appliance with an NTP Server," on page 49.

Synchronize the Time in the vCenter Server Appliance with an NTP Server

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

Prerequisites

Set up one or more Network Time Protocol (NTP) servers in the vCenter Server Appliance configuration. See "Add or Replace NTP Servers in the vCenter Server Appliance Configuration," on page 48.

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 the vCenter Server Appliance

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

User Roles in the vCenter Server Appliance

There are three main user roles in the vCenter Server Appliance.

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

Operator	Local users with the operator user role can read the appliance configuration.
Administrator	Local users with the administrator user role can configure the appliance.
Super Administrator	Local users with the super administrator user role can configure the appliance, manage the local accounts, and use the Bash shell.

Get a List of the Local User Accounts in the vCenter Server Appliance

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 the vCenter Server Appliance

You can create a new local user account in the vCenter Server Appliance.

For information about the user roles, see .

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`

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.

You created a new local user in the appliance.

Update the Password of a Local User in the vCenter Server Appliance

You can update the password of a local user in the vCenter Server Appliance 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 the vCenter Server Appliance

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

For information about the user roles, see "User Roles in the vCenter Server Appliance," on page 50.

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 the vCenter Server Appliance

You can delete a local user account in the vCenter Server Appliance.

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 the vCenter Server Appliance

You can monitor the hardware health status of the vCenter Server Appliance 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 the vCenter Server Appliance Health Status," on page 12.

For a complete list of the API commands that you can use for monitoring statistics and health of the vCenter Server Appliance system, see "API Commands in the vCenter Server Appliance Shell," on page 37.

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 the vCenter Server Appliance, run the `mem.health.get` command.

■ To view the health of the storage in the vCenter Server Appliance, run the `storage.health.get` command.

■ To view the health of the swap in the vCenter Server Appliance, run the `swap.health.get` command.

■ To view the health of the update component in the vCenter Server Appliance, 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 Appliance patches and enabling automatic checks for vCenter Server Appliance patches, see *vSphere Upgrade*.

■ To view the overall health of the vCenter Server Appliance 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 Appliance.

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

■ Monitor Services By Using vimtop in Interactive Mode on page 53

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

■ Interactive Mode Command-Line Options on page 53

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 on page 54

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 Appliance 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 `vimtop` command-line options.
–v	Prints the `vimtop` version number.
–c *filename*	Loads a user-defined `vimtop` configuration file. If the –c option is not used, the default configuration file is `/root/vimtop/vimtop.xml`. You can create your own configuration file, specifying a different filename and path by using the W single-key interactive command.

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

Option	Description
–n *number*	Sets the number of performed iterations before the vimtop exits interactive mode. vimtop updates the display *number* number of times and exits. The default value is 10000.
–p / –d *seconds*	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
h	Show a help menu for the current panel, giving a brief summary of commands, and the status of secure mode.
i	Show or hide the top line view of the overview panel of the vimtop plug-in.
t	Show or hide the Tasks section, which displays information in the overview panel about the tasks currently running on the vCenter Server instance.
m	Show or hide the Memory section in the overview panel.
f	Show or hide the CPU section which displays information in the overview panel about all available CPUs.
g	Show or hide the CPUs section which displays information in the overview panel about the top 4 physical CPUs.
spacebar	Immediately refreshes the current pane.
p	Pause the displayed information about the services resource use in the current panels.
r	Refresh the displayed information about the services resource use in the current panels.
s	Set refresh period.
q	Exit the interactive mode of the vimtop plug-in.
k	Displays the Disks view of the main panel.
o	Switch the main panel to Network view.
Esc	Clear selection or return to the Processes view of the main panel.
Enter	Select a service to view additional details.
n	Show or hide names of the headers in the main panel.
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.

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

Key Names	Description
x	Return the column widths to their default values.
+	Expand selected item.
-	Collapse selected item.
w	Write the current setup to a `vimtop` configuration file. The default file name is the one specified by `–c` option, or `/root/vimtop/vimtop.xml` if the `–c` option is not used. You can also specify a different file name on the prompt generated by the `w` command.

Using the Direct Console User Interface to Configure the vCenter Server Appliance

5

After you deploy the vCenter Server Appliance, 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 Appliance. 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

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

Procedure

1   Browse to the vCenter Server Appliance in the vSphere Web Client or the VMware Host Client inventory.

2   Open the vCenter Server Appliance console.

- From the vSphere Web Client, on the **Summary** tab, click **Launch Console**.

- From the VMware Host Client, click **Console** and select an option from the drop-down menu.

3   Click inside the console window and press F2 to customize the system.

4   Type the password for the root user of the appliance and press Enter.

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

You logged in to the Direct Console User Interface. You can change the password of the root user of the vCenter Server Appliance, 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 Appliance Direct Console User Interface, you can change the password of the root user.

The default root password for the vCenter Server Appliance is the password you enter during deployment of the virtual appliance.

IMPORTANT The password for the root account of the vCenter Server Appliance expires after 365 days. You can change the expiry time for an account by logging as root to the vCenter Server Appliance 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   Browse to the vCenter Server Appliance in the vSphere Web Client or the VMware Host Client inventory.

2   Open the vCenter Server Appliance console.

   ■   From the vSphere Web Client, on the **Summary** tab, click **Launch Console**.

   ■   From the VMware Host Client, click **Console** and select an option from the drop-down menu.

3   Click inside the console window and press F2 to customize the system.

4   To log in to the Direct Console User Interface, type the current password of the root user and press Enter.

5   Select **Configure Root Password** and press Enter.

6   Type the old password of the root user, and press Enter.

7   Set up the new password and press Enter.

8   Press Esc until you return to the main menu of the Direct Console User Interface.

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

Configure the Management Network of the vCenter Server Appliance

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

Prerequisites

To change the IP address of the appliance, 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 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 the vCenter Server Appliance.

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 on the appliance
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 of the appliance 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 the vCenter Server Appliance

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

Procedure

1   Log in to the Direct Console User Interface of the vCenter Server Appliance.

2   Select **Restart Management Network** and press Enter.

3   Press F11.

Enable Access to the Appliance Bash Shell

You can use the appliance Direct Console User Interface to enable local and remote access to the appliance 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 the vCenter Server Appliance.

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 Appliance Bash shell for troubleshooting.

Access the Appliance Bash Shell for Troubleshooting

Log in to the vCenter Server Appliance shell for troubleshooting purposes only.

Procedure

1   Access the appliance shell using one of the following methods.

    ■   If you have direct access to the appliance, 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.

3   In the appliance 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 vCenter Server 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`

Index