VMware vCenter Server Appliance Management Programming Guide

VMware vSphere 6.5
vCenter Server 6.5
VMware ESXi 6.5

vmware
by Broadcom

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

https://docs.vmware.com/

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

Contents

About the vCenter Server Appliance Management Programming Guide

The *vCenter Server Appliance Management Programming Guide* provides information about using APIs to work with the vCenter Server Appliance, a turnkey solution for managing data centers featuring VMware® vCenter Server and VMware ESXi.

Intended Audience

This information is intended for anyone who wants to develop software to configure, monitor, and manage the vCenter Server Appliance. The information is written for developers who have some experience with REST APIs, JavaScript, Java, or Python.

VMware Glossary

VMware Information Experience 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.

Introduction to Programming the vCenter Server Appliance

1

This programming guide explains how to use the APIs available to manage the vCenter Server Appliance.

The vCenter Server Appliance provides a fully packaged solution for data center management in a vSphere installation. The vCenter Server Appliance delivers complete life cycle management, including:

- Large-scale data center management capability
- Rapid deployment
- Comprehensive appliance monitoring
- Appliance backup and restore
- Enterprise-level high availability
- Low total cost of ownership, with no licensing cost for guest operating system or applications

Read the following topics next:

About vSphere

vSphere is the VMware software stack that implements private-cloud data center management, as well as the on-premises component of hybrid-cloud deployments. A vSphere installation includes one or more instances of vCenter Server configured to manage one or more virtual data centers. Each virtual data center includes one or more instances of VMware ESXi.

The vCenter Server Appliance contains an instance of vCenter Server. The Appliance Management API gives you programmatic access to manage the management elements of your data center.

About ESXi

Each instance of ESXi includes management agents and the VMware hypervisor layer, which runs several virtual machines. Each virtual machine contains a guest operating system, such as Windows or Linux, capable of running IT or user applications.

The vCenter Server Appliance runs as a virtual machine on an ESXi instance. The Appliance provides an independent endpoint capable of handling API requests both for vCenter Server and for the Appliance Management API .

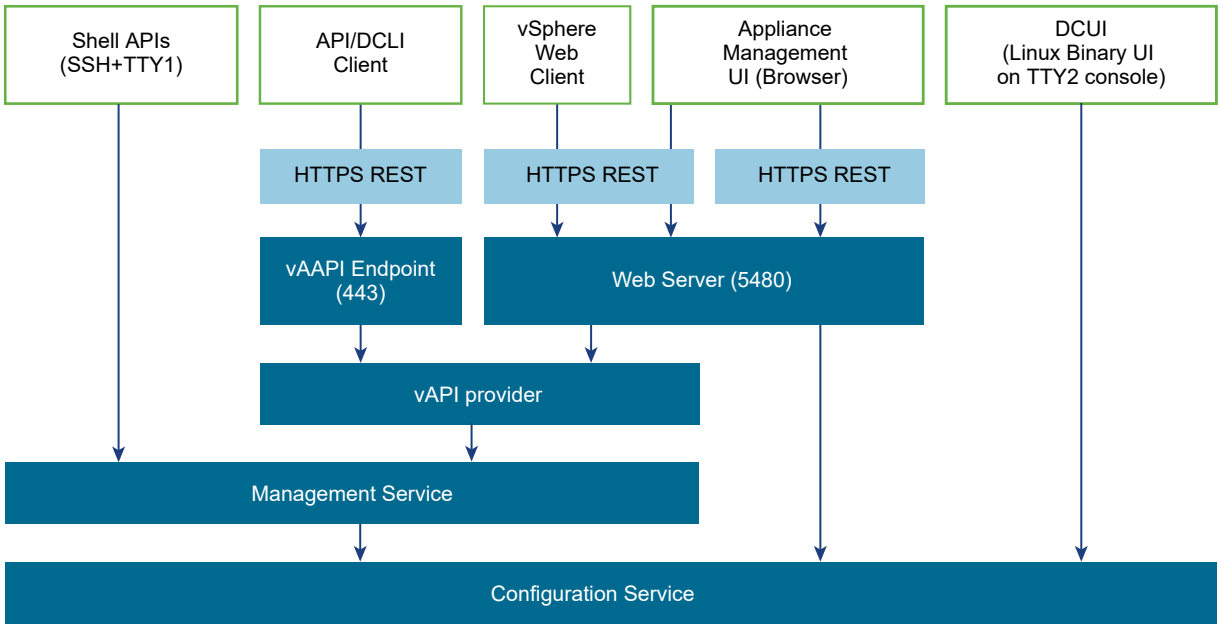
vCenter Server Appliance Management Overview

The vCenter Server Appliance is an instance of vCenter Server running in a Linux guest operating system.

vCenter Server is a collection of services designed for managing and monitoring vSphere installations. The vCenter Server Appliance responds to CLI commands, requests from the vSphere Web Client, and API requests from custom clients. API clients can be written in a choice of several software languages.

The vCenter Server Appliance is managed by CLI, web interfaces, or API requests. These requests help you manage appliance configuration, monitor resource usage, or backup and restore the vCenter Server instance. You can also use API requests to check the health of the vCenter Server installed in the appliance. This programming guide explains how to use the APIs that are available to manage the appliance.

Figure 1-1. vCenter Server Appliance Management Connections



For more information about the capabilities of the vCenter Server Appliance, see *vCenter Server Appliance Configuration*.

Limitations of Programming for the vCenter Server Appliance

The vCenter Server Appliance supports several programming interfaces for monitoring appliance health and performance, managing network configuration, security hardening, and other functions. The vCenter Server Appliance also supports several user interfaces, which offer overlapping sets of functionality.

You can perform many operations with the vSphere Web Client. But some operations in the vSphere Web Client do not allow you to specify every detail of the operation. To access more completely the capabilities of such operations, you must use the API.

However, the API cannot access all the capabilities. A few special features require direct shell access or special user interfaces. See Supplementing the vCenter Server Appliance API.

API Endpoints for Managing the vCenter Server Appliance

The vCenter Server Appliance integrates with the vSphere Automation API endpoint that provides a common surface for exposing several vSphere services. When you use the vSphere Automation API endpoint, you establish a single session that provides access to virtual machine management, search and filter, Content Library, and other services for working with vSphere objects.

Other endpoints associated with the vCenter Server Appliance include the Lookup Service and the vCenter Single Sign-On Service. For more information about using the Lookup Service, see Chapter 3 Retrieving Service Endpoints. For more information about using the vCenter Single Sign-On Service, see vCenter Single Sign-On Token Authentication for the vCenter Server Appliance.

Supplementing the vCenter Server Appliance API

Some less common features of the vCenter Server Appliance are not accessible by API. These features require direct shell access or specific user interfaces.

Direct Console User Interface to the vCenter Server Appliance

The vCenter Server Appliance provides a Direct Console User Interface (DCUI) for operator access to basic appliance functions.

The DCUI provides access to a subset of management functions. It provides direct access to the appliance should the vSphere Web Client and the Virtual Appliance Management UI become unavailable.

For an illustration showing Appliance connections, see the block diagram Figure 1-1. vCenter Server Appliance Management Connections.

After the vCenter Server Appliance startup is complete, the DCUI displays basic CPU, memory, and network information on the operator console. The operator can use the DCUI screen to configure network interfaces, DNS, SuperAdministrator password, and troubleshooting options.

Virtual Appliance Management UI

The Virtual Appliance Management UI is an HTML client specifically designed to configure the system-level options of the vCenter Server Appliance.

The Virtual Appliance Management UI runs in a browser that connects to port 5480 of the appliance, and is used during the initial configuration of the appliance. The Virtual Appliance Management UI provides access to all the service APIs of the appliance.

For an illustration showing Appliance connections, see the block diagram Figure 1-1. vCenter Server Appliance Management Connections.

Appliance Shell and the vCenter Server Appliance

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

For an illustration showing Appliance connections, see the block diagram Figure 1-1. vCenter Server Appliance Management Connections.

For more information about the appliance shell, see *vCenter Server Appliance Configuration*.

vSphere Web Client and the vCenter Server Appliance

The vSphere Web Client is the preferred user interface for general management tasks. You can access the vCenter Server Appliance from the vSphere Web Client by using the **Administration > System Configuration** screen.

For an illustration showing Appliance connections, see the block diagram Figure 1-1. vCenter Server Appliance Management Connections.

DCLI and the vCenter Server Appliance

The Datacenter CLI (DCLI) is a CLI client of the VMware vSphere® Automation™ SDK. Almost all methods that are available in the vSphere Automation SDKs are available as DCLI commands.

You can run the DCLI from the VMware vSphere® Command-Line Interface (vCLI) package or from the appliance shell.

For an illustration showing Appliance connections, see the block diagram Figure 1-1. vCenter Server Appliance Management Connections.

For more information about the DCLI, see *Getting Started with vSphere Command-Line Interfaces*.

Quick Start with vCenter Server Appliance APIs

You can start using the vCenter Server Appliance APIs without accessing the Lookup Service Endpoint or the vCenter Single Sign-On Endpoint. In a production environment, you might instead use centralized service registration and token authentication.

To use the vCenter Server Appliance APIs without the Lookup Service or token authentication, see vCenter Single Sign-On User Name and Password Authentication for the vCenter Server Appliance.

vCenter Server Appliance Programming Environment

2

The vCenter Server Appliance is a key component in your vSphere environment, providing several services for data center management, as well as its own management.

Read the following topics next:

- Platform Services Controller Services
- Platform Services in the vCenter Server Appliance Environment
- vSphere Deployment Configurations

Platform Services Controller Services

With Platform Services Controller, all VMware products within the same environment can share the authentication domain and other services. Services include certificate management, authentication, and licensing.

Platform Services Controller includes the following core infrastructure services.

Table 2-1. Platform Services Controller Services

Service	Description
`applmgmt` (VMware Appliance Management Service)	Handles appliance configuration and provides public API endpoints for appliance lifecylce management. Included on the Platform Services Controller appliance.
`vmware-cis-license` (VMware License Service)	Each Platform Services Controller includes VMware License Service, which delivers centralized license management and reporting functionality to VMware products in your environment. The license service inventory replicates across all Platform Services Controller in the domain at 30-second intervals.
`vmware-cm` (VMware Component Manager)	Component manager provides service registration and lookup functionalities.
`vmware-psc-client` (VMware Platform Services Controller Client)	Back end to the Platform Services Controller Web interface.

Table 2-1. Platform Services Controller Services (continued)

Service	Description

`vmware-sts-idmd`
(VMware Identity Management Service)
`vmware-stsd`
(VMware Security Token Service)
	Services behind the vCenter Single Sign-On feature, which provide secure authentication services to VMware software components and users.
	By using vCenter Single Sign-On, the VMware components communicate using a secure SAML token exchange mechanism. vCenter Single Sign-On constructs an internal security domain (vsphere.local by default) where the VMware software components are registered during installation or upgrade.

`vmware-rhttpproxy` (VMware HTTP Reverse Proxy)	The reverse proxy runs on each Platform Services Controller node and each vCenter Server system. It is a single entry point into the node and enables services that run on the node to communicate securely.
`vmware-sca` (VMware Service Control Agent)	Manages service configurations. You can use the `service-control` CLI to manage individual service configurations.
`vmware-statsmonitor` (VMware Appliance Monitoring Service)	Monitor the vCenter Server Appliance guest operating system resource consumption.
`vmware-vapi-endpoint` (VMware vAPI Endpoint)	The vSphere Automation API endpoint provides a single point of access to vAAPI services. You can change the properties of the vAAPI Endpoint service from the vSphere Web Client. See the *VMware vCloud Suite SDKs Programming Guide* for details on vAAPI endpoints.
`vmafdd` VMware Authentication Framework	Service that provides a client-side framework for vmdir authentication and serves the VMware Endpoint Certificate Store (VECS).
`vmcad` VMware Certificate Service	Provisions each VMware software component that has the vmafd client libraries and each ESXi host with a signed certificate that has VMCA as the root certificate authority. You can change the default certificates by using the Certificate Manager utility or Platform Services Controller Web interface. VMware Certificate Service uses the VMware Endpoint Certificate Store (VECS) to serve as a local repository for certificates on every Platform Services Controller instance. Although you can decide not to use VMCA and instead can use custom certificates, you must add the certificates to VECS.
`vmdird` VMware Directory Service	Provides a multitenant, multimastered LDAP directory service that stores authentication, certificate, lookup, and license information. Do not update data in `vmdird` by using an LDAP browser. If your domain contains more than one Platform Services Controller instance, an update of vmdir content in one vmdir instance is propagated to all other instances of vmdir.

Table 2-1. Platform Services Controller Services (continued)

Service	Description
`vmdnsd` VMware Domain Name Service	Not used in vSphere 6.x.

`vmonapi`
VMware Lifecycle Manager API
`vmware-vmon`
VMware Service Lifecycle Manager
	Start and stop vCenter Server services and monitor service API health. The `vmware-vmon` service is a centralized platform-independent service that manages the life cycle of Platform Services Controller and vCenter Server. Exposes APIs and CLIs to third-party applications.

`lwsmd` Likewise Service Manager	Likewise facilitates joining the host to an Active Directory domain and subsequent user authentication.

Platform Services in the vCenter Server Appliance Environment

The vCenter Server Appliance registers its services with the Platform Services Controller, but in some situations you might be unable to use the Lookup Service registration. In those situations, you must access an appliance endpoint directly.

A direct connection to the vCenter Server Appliance can become necessary in configurations where the Platform Services Controller is embedded in the appliance. When the appliance vCenter Server is being restored from a backup, or when the embedded Lookup Service is restarting, you might be unable to look up the appliance's service registration.

For more information about embedded or external Platform Services Controller configurations, see vSphere Deployment Configurations.

For more information about backup and restore operations, see Chapter 6 Maintenance of the vCenter Server Appliance.

vSphere Deployment Configurations

vSphere Automation client applications communicate with services on the Platform Services Controller and vCenter Server components of the virtual environment. vCenter Server can be deployed with an embedded or external Platform Services Controller.

vCenter Server with an Embedded Platform Services Controller

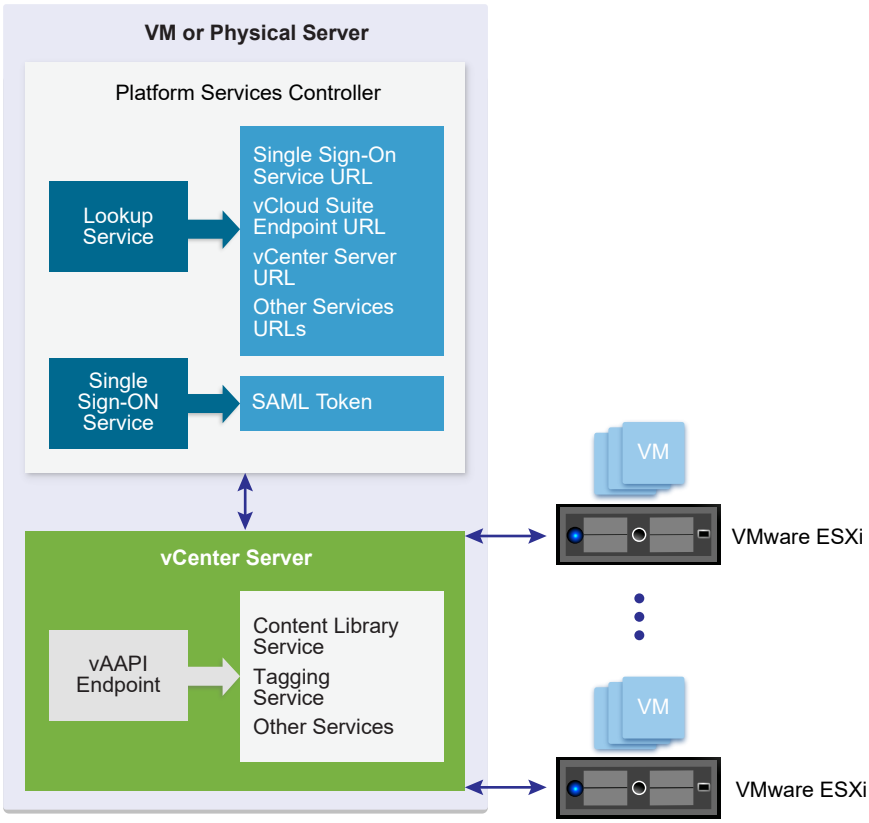
vCenter Server and Platform Services Controller reside on the same virtual machine or physical server. This deployment is most suitable for small environments such as development or test beds.

You can use the Platform Services Controller in two ways to establish secure, authenticated sessions for your client application, by making requests to the Lookup Service and the vCenter Single Sign-On Service.

One way to use the Platform Services Controller is to request an authentication token that can be used to authenticate requests across services. The client connects to the Lookup Service and retrieves the vCenter Single Sign-On Service endpoint and the vSphere Automation API endpoint. The client then uses the vCenter Single Sign-On endpoint to authenticate with user credentials and receive a token that securely verifies the client's credentials. This allows the client to authenticate with a number of service endpoints without sending user credentials over the network repeatedly.

Alternatively, if the client connects directly to the vSphere Automation API endpoint, there is no need for the client to interact with the vCenter Single Sign-On Service. The client sends user credentials to the vSphere Automation API endpoint, which creates a session identifier that persists across requests.

Figure 2-1. vCenter Server with Embedded Platform Services Controller

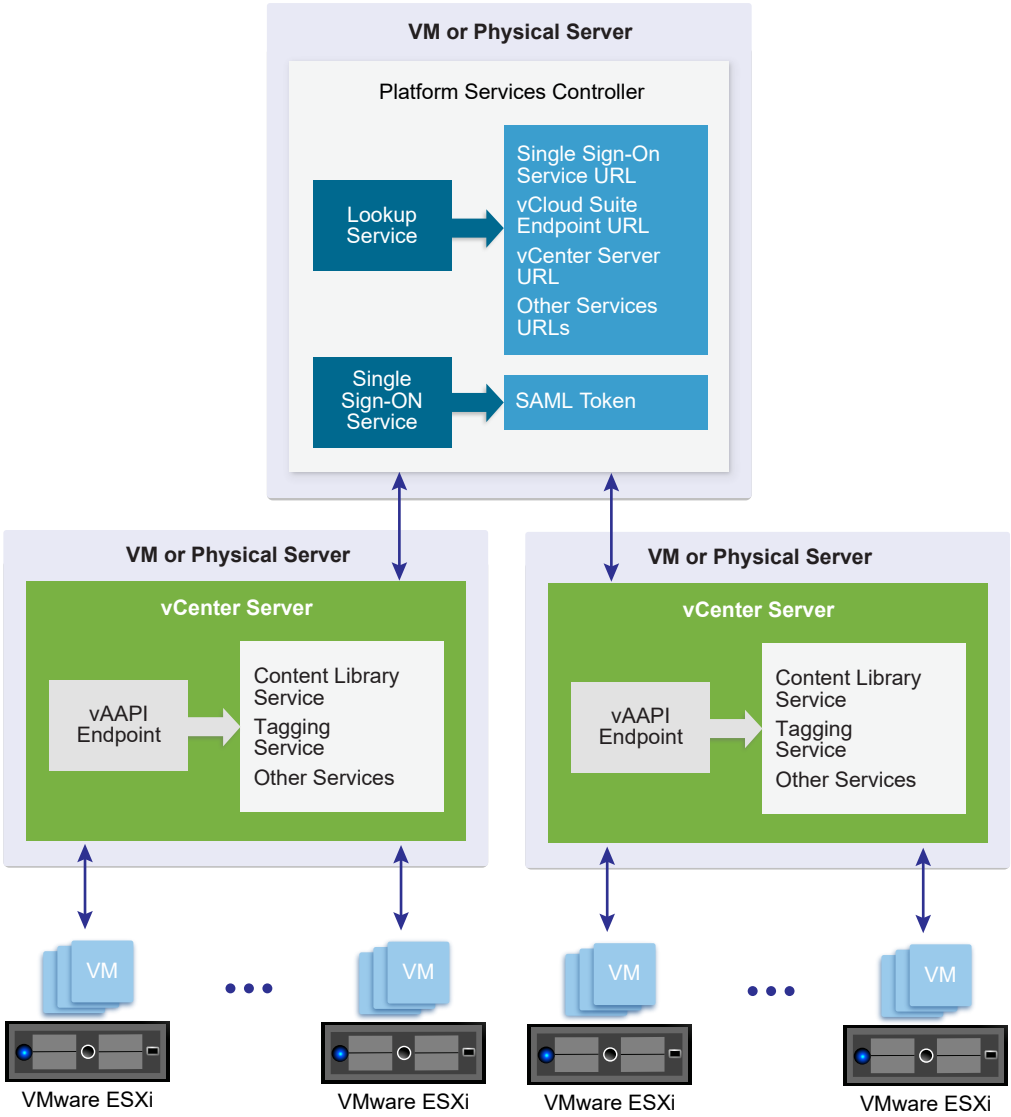


vCenter Server with an External Platform Services Controller

In the case of an external Platform Services Controller, the vCenter Server and the Platform Services Controller are deployed on separate virtual machines or physical servers. The Platform Services Controller can be shared across several vCenter Server instances. For larger deployments or to provide better availability, more than one Platform Services Controller can be deployed. When configured as replication partners within a single vCenter Single Sign-On domain, Platform Services Controller instances replicate all user and system data within the cluster.

A client application functions in a similar way as in a Platform Services Controller with embedded vCenter Server deployment. The only difference is that the client application can access services on multiple vCenter Server instances, or services only on a particular vCenter Server instance.

Figure 2-2. vCenter Server with External Platform Services Controller



Retrieving Service Endpoints

3

To access services and resources in the virtual environment, vSphere Automation API client applications must know the endpoints of vSphere Automation and vSphere services. Client applications retrieve service endpoints from the Lookup Service that runs on the Platform Services Controller.

The Lookup Service provides service registration and discovery by using a Web services API. By using the Lookup Service, you can retrieve endpoints of services on the Platform Services Controller and vCenter Server. The following endpoints are available from the Lookup Service.

- The vCenter Single Sign-On endpoint on the Platform Services Controller. You use the vCenter Single Sign-On service to get a SAML token and establish an authenticated session with a vSphere Automation endpoint or a vCenter Server endpoint.
- The vSphere Automation Endpoint on vCenter Server. Through the vSphere Automation Endpoint, you can make requests to vSphere Automation API services such as virtual machine management, Content Library, and Tagging.
- The vCenter Server endpoint. In an environment with external Platform Services Controller instances, you can use the vCenter Server endpoint to get the node ID of a particular vCenter Server instance. By using the node ID , you can retrieve service endpoints on that vCenter Server instance.
- The vSphere API endpoint and endpoints of other vSphere services that run on vCenter Server.

Workflow for Retrieving Service Endpoints

The workflow that you use to retrieve service endpoints from the Lookup Service might vary depending on the endpoints that you need and their number. Follow this general workflow for retrieving service endpoints.

1 Connect to the Lookup Service on the Platform Services Controller and service registration object so that you can query for registered services.

2 Create a service registration filter for the endpoints that you want to retrieve.

3 Use the filter to retrieve registration information for services from the Lookup Service.

4 Extract one or more endpoint URLs from the array of registration information that you receive from the Lookup Service.

Read the following topics next:

- Filtering for Predefined Service Endpoints
- Filter Parameters for Predefined Service Endpoints
- Connect to the Lookup Service and Retrieve the Service Registration Object
- Retrieve Service Endpoints on vCenter Server Instances
- Retrieve a vCenter Server ID by Using the Lookup Service
- Retrieve a vSphere Automation Endpoint on a vCenter Server Instance

Filtering for Predefined Service Endpoints

The Lookup Service maintains a registration list of vSphere services. You can use the Lookup Service to retrieve registration information for any service by setting a registration filter that you pass to the `List()` function on the Lookup Service. The functions and objects that you can use with the Lookup Service are defined in the `lookup.wsdl` file that is part of the SDK.

Lookup Service Registration Filters

You can query for service endpoints through a service registration object that you obtain from the Lookup Service. You invoke the `List()` function on the Lookup Service to list the endpoints that you need by passing `LookupServiceRegistrationFilter`. `LookupServiceRegistrationFilter` identifies the service and the endpoint type that you can retrieve.

Optionally, you can include the node ID parameter in the filter to identify the vCenter Server instance where the endpoint is hosted. When the node ID is omitted, the `List()` function returns the set of endpoint URLs for all instances of the service that are hosted on different vCenter Server instances in the environment.

For example, a `LookupServiceRegistrationFilter` for queering the vSphere Automation service has these service endpoint elements.

Table 3-1. Service Registration Filter Parameters

Filter Types	Value	Description
`LookupServiceRegistrationServiceType`	`product= "com.vmware.cis"`	vSphere Automation namespace.
	`type="cs.vapi"`	Identifies the vSphere Automation service.

Table 3-1. Service Registration Filter Parameters (continued)

Filter Types	Value	Description
`LookupServiceRegistrationEndpointType`	`type="com.vmware.vapi.endpoint"`	Specifies the endpoint path for the service.
	`protocol="vapi.json.https.public"`	Identifies the protocol that will be used for communication with the endpoint .

For information about the filter parameter of the available predefined service endpoints, see Filter Parameters for Predefined Service Endpoints.

Filter Parameters for Predefined Service Endpoints

Depending on the service endpoint that you want to retrieve, you provide different parameters to the `LookupServiceRegistrationFilter` that you pass to the `List()` function on the Lookup Service. To search for services on a particular vCenter Server instance, set the node ID parameter to the filter.

Table 3-2. Input Data for URL Retrieval for the Lookup Service Registration Filter

Service	Input Data	Value
vCenter Single Sign-On	product namespace	`com.vmware.cis`
	service type	`cs.identity`
	protocol	`wsTrust`
	endpoint type	`com.vmware.cis.cs.identity.sso`
vSphere Automation Endpoint	product namespace	`com.vmware.cis`
	service type	`cs.vapi`
	protocol	`vapi.json.https.public`
	endpoint type	`com.vmware.vapi.endpoint`
vCenter Server	product namespace	`com.vmware.cis`
	service type	`vcenterserver`
	protocol	`vmomi`
	endpoint type	`com.vmware.vim`
vCenter Storage Monitoring Service	product namespace	`com.vmware.vim.sms`
	service type	`sms`
	protocol	`https`
	endpoint type	`com.vmware.vim.sms`

Table 3-2. Input Data for URL Retrieval for the Lookup Service Registration Filter (continued)

Service	Input Data	Value
vCenter Storage Policy-Based Management	product namespace	`com.vmware.vim.sms`
	service type	`sms`
	protocol	`https`
	endpoint type	`com.vmware.vim.pbm`
vSphere ESX Agent Manager	product namespace	`com.vmware.vim.sms`
	service type	`cs.eam`
	protocol	`vmomi`
	endpoint type	`com.vmware.cis.cs.eam.sdk`

Connect to the Lookup Service and Retrieve the Service Registration Object

You must connect to the Lookup Service to gain access to its operations. After you connect to the Lookup Service, you must retrieve the service registration object to make registration queries.

Procedure

1. Connect to the Lookup Service.
   a. Configure a connection stub for the Lookup Service endpoint, which uses SOAP bindings, by using the HTTPS protocol.
   b. Create a connection object to communicate with the Lookup Service.
2. Retrieve the Service Registration Object.
   a. Create a managed object reference.
   b. Retrieve the `ServiceContent` managed object.
   c. Retrieve the service registration object.

      With the service registration object, you can make registration queries.

Retrieve Service Endpoints on vCenter Server Instances

You can create a function that obtains the endpoint URLs of a service on all vCenter Server instances in the environment. You can modify that function to obtain the endpoint URL of a service on a particular vCenter Server instance.

Prerequisites

- Establish a connection with the Lookup Service.
- Retrieve a service registration object.

Procedure

1. Create a filter criterion for service information.
2. Create a filter criterion for endpoint information.
3. Create the registration filter object.

Option	Description
Omit the node ID parameter	Retrieves the endpoint URLs of the service on all vCenter Server instances.
Include the node ID parameter	Retrieves the endpoint URL of the service on a particular vCenter Server instance.

4. Retrieve the specified service information by using the `List()` function.

Results

Depending on whether you included the node ID parameter, the `List()` function returns on eof the following results:

- A list of endpoint URLs for a service that is hosted on all vCenter Server instances in the environment.
- An endpoint URL of a service that runs on a particular vCenter Server instance.

What to do next

Call the function that you implemented to retrieve service endpoints. You can pass different filter parameters depending on the service endpoints that you need. For more information, see Filter Parameters for Predefined Service Endpoints.

To retrieve a service endpoint on a particular vCenter Server instance, you must retrieve the node ID of that instance and pass it to the function. For information about how to retrieve the ID of a vCenter Server instance, see Retrieve a vCenter Server ID by Using the Lookup Service.

Retrieve a vCenter Server ID by Using the Lookup Service

You use the node ID of a vCenter Server instance to retrieve the endpoint URL of a service on that vCenter Server instance. You specify the node ID in the service registration filter that you pass to the `List()` function on the Lookup Service.

Managed services are registered with the instance name of the vCenter Server instance where they run. The instance name maps to a unique vCenter Server ID. The instance name of a vCenter Server system is specified during installation and might be an FQDN or an IP address.

Prerequisites

- Establish a connection with the Lookup Service.
- Retrieve a service registration object.

Procedure

1. List the vCenter Server instances.
2. Find the matching node name of the vCenter Server instance and save the ID.

Results

Use the node ID of the vCenter Server instance to filter subsequent endpoint requests. You can use the node ID in a function that retrieves the endpoint URL of a service on a vCenter Server instance. For information about implementing such a function, see Retrieve Service Endpoints on vCenter Server Instances.

Retrieve a vSphere Automation Endpoint on a vCenter Server Instance

Through the vSphere Automation Endpoint, you can access other vSphere Automation services that run on vCenter Server, such as Content Library and Tagging. To use a vSphere Automation service, you must retrieve the vSphere Automation Endpoint.

Prerequisites

- Establish a connection with the Lookup Service.
- Retrieve a service registration object.
- Determine the node ID of the vCenter Server instance where the vSphere Automation service runs.
- Implement a function that retrieves the endpoint URL of a service on a vCenter Server instance.

Procedure

1. Invoke the function for retrieving the endpoint URL of a service on a vCenter Server instance by passing filter strings that are specific to the vSphere Automation endpoint.
2. Save the URL from the resulting single-element list.

Authentication Mechanisms

4

The vCenter Server Appliance accepts several authentication methods. The authentication method that you choose depends on whether you choose token authentication, and on the state of the appliance.

During normal operation, the vCenter Server Appliance enables you to authenticate with vCenter Single Sign-On credentials. You have the option to use either token authentication or user name and password authentication. The user name and password must be recognized within the vCenter Single Sign-On domain.

However, during the process of restoring the Appliance from a backup image, you must use a different authentication protocol. For more information, see Restoring the vCenter Server Appliance.

Read the following topics next:

- vCenter Single Sign-On User Name and Password Authentication for the vCenter Server Appliance
- vCenter Single Sign-On Token Authentication for the vCenter Server Appliance

vCenter Single Sign-On User Name and Password Authentication for the vCenter Server Appliance

You can authenticate with the vCenter Server Appliance by using a user name and password known to the vCenter Single Sign-On Service.

If you prefer to delegate the process of requesting a SAML token for your API client, you can present your SSO domain credentials to the vSphere Automation API endpoint and request a session ID. The endpoint process forwards your credentials to the vCenter Single Sign-On Service and requests a SAML token on your behalf. In this case, you never deal with the token.

Authenticate with vCenter Single Sign-OnCredentials and Create a Session

To establish a session with the vSphere Automation API Endpoint in the vCenter Server Appliance, you create a connection to the endpoint and authenticate with vCenter Single Sign-On credentials to receive a session ID.

Prerequisites

To perform this task, you must have the following items in place:

- The DNS name or IP address of the vCenter Server Appliance
- A vCenter Single Sign-On domain account that has the requisite permissions for the operation that you intend to invoke

Procedure

1. Create a connection context by specifying the vSphere Automation API Endpoint URL and the message protocol to be used for the connection.
2. Create the request options or stub configuration and set the specific security context to be used.

   The security context contains the vCenter Single Sign-On user name and password that are used for authenticating to the vSphere Automation API Endpoint.
3. Create an interface stub or a REST path that uses the stub configuration.

   The interface stub corresponds to the interface containing the method to be invoked.
4. Invoke the session `create` method.

   The service creates an authenticated session and returns a session identification cookie to the client.
5. Add the cookie to your request headers or to a security context for your client stub configuration.
6. Remove the basic authentication from your request headers or the security context of your client stub configuration.

Results

Subsequent method calls authenticate with the session cookie instead of the user name and password.

What to do next

Use the updated stub configuration with the session ID to create a stub for the interface that you want to use. Method calls on the new stub use the session ID to authenticate.

vCenter Single Sign-On Token Authentication for the vCenter Server Appliance

You can authenticate with the vCenter Server Appliance by using a SAML token from the vCenter Single Sign-On Service. The token can be either a bearer token or a holder-of-key token.

To use SAML token authentication, you issue a request to the vCenter Single Sign-On Service, specifying the token type (bearer or holder-of-key), expected token lifetime, renewability, and other parameters. You also supply a user name and password combination that is valid in the SSO domain. These credentials must have an associated role with sufficient privilege for the operations that you intend to invoke with the Management API.

If the vCenter Single Sign-On Service accepts your credentials, it responds with an XML message. The message contains a SAML assertion that your client can extract and present as an `Authorization` header in an HTTP request to the vSphere Automation API endpoint.

Retrieve a SAML Token

The vCenter Single Sign-On service provides authentication mechanisms for securing the operations that your client application performs in the virtual environment. Client applications use SAML security tokens for authentication.

Client applications use the vCenter Single Sign-On service to retrieve SAML tokens. For more information about how to acquire a SAML security token, see the *vCenter Single Sign-On Programming Guide* documentation.

Prerequisites

Verify that you have the vCenter Single Sign-On URL. You can use the Lookup Service on the Platform Services Controller to obtain the endpoint URL. For information about retrieving service endpoints, see Chapter 3 Retrieving Service Endpoints.

Procedure

1. Create a connection object to communicate with the vCenter Single Sign-On service.

   Pass the vCenter Single Sign-On endpoint URL, which you can get from the Lookup Service.
2. Issue a security token request by sending valid user credentials to the vCenter Single Sign-On service on the Platform Services Controller.

Results

The vCenter Single Sign-On service returns a SAML token.

What to do next

You can present the SAML token to the vSphere Automation API Endpoint or other endpoints, such as the vSphere Web Services Endpoint. The endpoint returns a session ID and establishes a persistent session with that endpoint. Each endpoint that you connect to uses your SAML token to create its own session.

Create a vSphere Automation Session with a SAML Token

To establish a vSphere Automation session, you create a connection to the vSphere Automation API Endpoint and then you authenticate with a SAML token to create a session for the connection.

Prerequisites

- Retrieve the vSphere Automation Endpoint URL from the Lookup Service.
- Obtain a SAML token from the vCenter Single Sign-On service.

Procedure

1. Create a connection by specifying the vSphere Automation API Endpoint URL and the message protocol to be used for the connection.

   Note To transmit your requests securely, use **`https`** for the vSphere Automation API Endpoint URL.

2. Create the request options or stub configuration and set the security context to be used.

   The security context object contains the SAML token retrieved from the vCenter Single Sign-On service. Optionally, the security context might contain the private key of the client application.

3. Create an interface stub or a REST path that uses the stub configuration instance.

   The interface stub corresponds to the interface containing the method to be invoked.

4. Invoke the session `create` method.

   The service creates an authenticated session and returns a session identification cookie to the client.

5. Create a security context instance and add the session ID to it.
6. Update the stub configuration instance with the session security context.

What to do next

Use the updated stub configuration with the session ID to create a stub for the interface that you want to use. Method calls on the new stub use the session ID to authenticate.

Authorization Model for Administration of the vCenter Server Appliance

5

The vCenter Server Appliance supports three levels of authorization for users administering the appliance.

The authorization level with the least capability is the **operator** role. A user having the **operator** role has read access to appliance configuration settings.

A user having the **administrator** role has read and write access to appliance configuration settings, but cannot manage user accounts.

A user having the **superAdministrator** role has all the capabilities of the other roles, and has the additional capabilities of creating local user accounts and accessing the local Bash shell.

This model applies to the API and all other interfaces to the vCenter Server Appliance except when you use SSH and log in using a local account.

Read the following topics next:

- Authorization Model Mapping to the vCenter Single Sign-On Domain
- Using the ApplianceOperator Role
- Using the ApplianceAdmin Role
- Using the ApplianceSuperAdmin Role

Authorization Model Mapping to the vCenter Single Sign-On Domain

The three-level authorization model of the vCenter Server Appliance maps to local roles and to SSO groups, depending on how the user authenticated. This model allows consistent security control regardless of operational context.

The authorization levels map to group and role.

Table 5-1. Authorization Mapping

Authorization Level	vCenter Single Sign-On Group	Appliance Local Role
operator	ComponentManager.Administrator	operator
administrator	ComponentManager.Administrator	admin
superAdministrator	SysConfig.BashShellAdministrator	superAdmin

When an administrator adds user accounts, the options available include a choice of the role to assign to the new user.

Using the ApplianceOperator Role

The **operator** role is the most restricted of the authorization levels available to users who work with the vCenter Server Appliance.

Appliance operators are allowed to view information about the appliance. They are not allowed to alter its characteristics. The **operator** role is suited for monitoring and reporting functions. For example, the **operator** role allows access to these methods:

- resources.system.health.get
- resources.storage.stats.list
- services.status.get

Using the ApplianceAdmin Role

The **administrator** role provides an intermediate authorization level for users who manage the vCenter Server Appliance.

An **administrator** role is required for users who alter the appliance configuration, exercise control functions, or other operations that can affect appliance users.

For example, use the **administrator** role for these methods:

- networking.ip4v.renew
- networking.firewall.addr.inbound.add
- services.control
- shutdown.reboot

Using the ApplianceSuperAdmin Role

The **superAdministrator** role is the most expansive authorization level for users who manage the vCenter Server Appliance.

The **superAdministrator** role allows unrestricted access to appliance operations. This role is required for adding or altering user accounts and to enable access to the Bash shell for the other user accounts.

Maintenance of the vCenter Server Appliance

6

The vCenter Server Appliance Management API facilitates backup and restore operations. You can create a backup image that includes the database and configuration of the vCenter Server instance. You can also use the API to restore the backup image into a freshly deployed Appliance.

Read the following topics next:

- Backing Up the vCenter Server Appliance
- Restoring the vCenter Server Appliance

Backing Up the vCenter Server Appliance

The vCenter Server Appliance Management API supports backing up key parts of the Appliance. This allows you to protect vCenter Server data and to minimize the time required to restore data center operations.

The backup process collects key files into a tar bundle and compresses the bundle to reduce network load. To minimize storage impact, the transmission is streamed without caching in the Appliance. To reduce total time required to complete the backup operation, the backup process handles the different components in parallel.

You have the option to encrypt the compressed file before transmission to the backup storage location. When you choose encryption, you must supply a password which can be used to decrypt the file during restoration.

The backup operation always includes the vCenter Server database and system configuration files, so that a restore operation has all the data needed to re-create an operational Appliance. Current Alarms are included as well. You also have the option to specify additional data sets, called parts. In this release, you can specify a data set that includes Statistics, Events, and Tasks.

Backup and Restore Protocols for the vCenter Server Appliance

The vCenter Server Appliance backup and restore feature supports a number of plug-in communication protocols. Choose one of these protocols as the backup location type when you invoke the operation.

- FTP

- FTPS
- SCP
- HTTP
- HTTPS

The value `PATH` for the location type field indicates a locally mounted volume.

Note If you specify the `SCP` protocol, you must specify an absolute path as the value of the location type field when you create the backup job.

Back Up a vCenter Server Appliance Using the API

You can use the Management API of the vCenter Server Appliance to create a backup of the vCenter Server database and key operational elements of the Appliance.

This procedure explains the sequence of operations you use to create a backup image of the vCenter Server instance in the Appliance. You can do this as part of a regular maintenance schedule.

Prerequisites

- The vCenter Server instance must be in a ready state. All processes with start-up type automatic must be running.
- No other backup or restore job may be running concurrently.
- The destination storage location must be accessible to the Appliance backup process.
- The path to the destination directory must already exist, as far as the parent directory.
- If the destination directory does not exist, the backup process will create it. If the directory does exist, it must be empty.
- The destination storage device must have sufficient space for the backup image. For information about how to calculate the space needed for the backup image, see Calculate the Size Needed To Store the Backup File.

Procedure

1. Authenticate to the vSphere Automation API endpoint and establish a session.
2. Create a backup request object to describe the backup operation.

   The request specifies several attributes, especially the backup location, the protocol used to communicate with the storage server, the necessary authorization, and which optional parts of the database you want to back up. The core inventory data and Alarms are always backed up, but you can choose whether or not to back up Statistics, Events, and Tasks. Collectively, this optional part of the backup is referred to as `seat`.
3. Issue a request to start the backup operation.
4. From the response, save the unique job identifier of the backup operation.

5 Monitor progress of the job until it is complete.

6 Report job completion.

Calculate the Size Needed To Store the Backup File

When you prepare to do a backup of a vCenter Server instance, you can use the API to calculate the storage space needed for the backup file.

You can do this task when you are choosing a backup storage location or whenever your existing storage location might be approaching full capacity.

Prerequisites

- Verify that you have a vCenter Server instance running.
- Verify that you are familiar with authentication methods. See #unique_43.

Procedure

1 Authenticate to the vSphere Automation API endpoint and establish a session.

2 Request a list of backup parts available.

3 For each available backup part, request the size of the backup file.

The backup process calculates the compressed size of each backup part.

4 Choose which parts to include in the backup, and sum their sizes.

The backup storage server must have sufficient space to contain the chosen parts.

What to do next

After you choose which backup parts you will store, and verify that the backup storage server has sufficient free space, you can launch a backup job. For information, see Back Up a vCenter Server Appliance Using the API.

Restoring the vCenter Server Appliance

The vCenter Server Appliance Management API supports restoring the Appliance from a backup copy. The API simplifies the process by unifying the handling of various components of the vCenter Server in a single operation.

The process of restoring a vCenter Server Appliance from a backup has two phases.

1 Deploy an unconfigured Appliance from an OVF file. OVF deployment is described in the vSphere Automation SDK programming guide.

2 Invoke the `restore` operation from the Management API to apply configuration settings and load the vCenter Server database from the backup image.

Note You cannot specify optional parts for the restore operation. The restore operation includes all optional parts, such as Events and Tasks, that were specified at the time when the backup image was created.

Authentication When Restoring the vCenter Server Appliance

During the process of restoring the vCenter Server Appliance from a backup image, you cannot use vCenter Single Sign-On authentication. You must use local authentication until the Appliance is fully configured.

When you restore your vCenter Server Appliance from a backup image, it begins in an unconfigured state. During this time, you must use local authentication to access the Management API . When you use local authentication, do not use the vSphere Automation API endpoint. Instead you must connect your client to port 5480 of the appliance.

When you use local authentication you must pass user name and password credentials with each method invocation. Use credentials that are known to the guest operating system of the Appliance.

Availability of Services While Restoring a vCenter Server Instance

During the process of restoring the vCenter Server backup file, services in the vCenter Server instance must restart. While they are restarting, your API client receives an error message.

You can write your client to trap the error, but you have no way to know when the vCenter Server services are running again. To determine when the restore process is complete, you must retry the API connection until it succeeds, then request the status of the job.

Restore the vCenter Server Appliance Using the API

You can use the Management API of the vCenter Server Appliance to restore the Appliance from a backup image containing the vCenter Server database and key operational elements of the Appliance.

This procedure explains the sequence of operations you use to restore the vCenter Server instance from a backup image.

Prerequisites

- The old vCenter Server Appliance, from which the backup image came, must be powered off before you start the restore operation.
- A new vCenter Server Appliance must be deployed in an unconfigured state, except that it must have a fully qualified domain name or IP address that matches the old one.
- The new vCenter Server Appliance must have the same build number as the one in the backup image.

- The new vCenter Server Appliance must have a size equal to or greater than the old one. If the old vCenter Server Appliance was customized to exceed the largest template size, the new one must be customized to the same size.
- If the old vCenter Server Appliance was deployed with an external Platform Services Controller, the new one must be also. If the old one was deployed in an embedded configuration, the new one must be also.
- No other backup or restore job may be running concurrently.
- The destination storage location must be accessible to the Appliance restore process.

Procedure

1. Create a restore request object to describe the restore operation.
2. Issue a request to start the restore operation.
3. Monitor progress of the job until it is complete.
4. Report job completion.

What to do next

After the vCenter Server Appliance is fully configured by the restore operation, you can resume using the vSphere Automation API endpoint for subsequent operations.