Programming the VMware Cloud on AWS

Version 1.7

VMware Cloud on AWS

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

REST Programming the VMware Cloud 1

The VMware Cloud™ on AWS provides REST programming interfaces to control various operations for organizations in a software defined data center (SDDC) running on Amazon Web Services (AWS).

This chapter includes the following topics:

About REST Programming

Representational state transfer (REST) programming is a popular method for presenting and managing web services. For ease of use and security, REST builds on the standard web protocols HTTP and HTTPS, using the normal network ports 80 and 443, which are both open in most data centers.

REST interfaces fall into four categories: GET, PUT, POST, and DELETE. The first and last are self explanatory. PUT and POST are similar. POST creates an item; PUT modifies it. Unlike POST, PUT can be run multiple times with the same effect. Here are different ways to run REST commands:

Curl Commands

The `curl` command is always available on Linux and Mac OS X machines. On Windows you can install it with the Visual C++ redistributable package, or download it from various web sites such as https://curl.haxx.se.

The name cURL means command URL. It sends commands to a URL, in this case sending REST commands with header, body, and parameters. One downside for VMware Cloud programming is that each `curl` command must include a very long authorization token.

Python Program

Python programming is a good way to use the REST interfaces with VMware Cloud. The program can store the authorization token, minimizing copy and paste overhead. You'll need the `requests` package for REST transmission, and the `simplejson` package to form JSON headers.

A sample Python program is available on the https://code.vmware.com web site, in the code samples section. You can test the various APIs and make use of them to create your own Python programs.

PowerCLI or DCLI

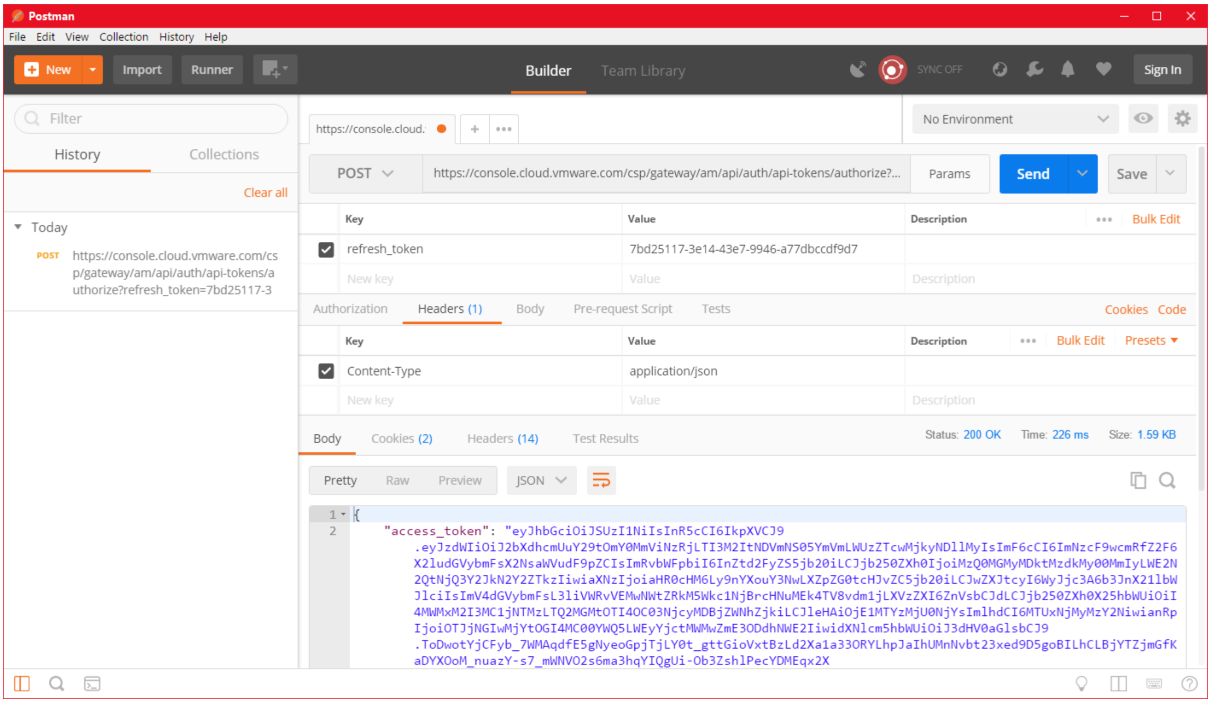
It is also possible to control VMC on AWS using PowerCLI `cmdlets` in the Windows PowerShell, or various namespaces in the vSphere Datacenter CLI (DCLI). For more information, go to the VMC Console and click **Developer Center > Downloads**.

Postman REST Client

The popular Postman REST client is now available as a free stand-alone application for Windows, Mac OS X, and Linux. It might be the easiest way to send REST commands to the VMware Cloud console. Postman started as a Chrome browser extension, like Firebug for Firefox. The Advanced REST Client is still available as a Chrome browser extension.

The figure below shows the `authorize` command, which is run against the cloud service provider (`csp`). Subsequent REST commands will use the resulting `access_token` when running against a software-defined data center in the VMC console.

Figure 1-1. Advanced REST Client



POST https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize?refresh_token=7bd25117-3

POST https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize?...

	Key	Value	Description
☑	refresh_token	7bd25117-3e14-43e7-9946-a77dbccdf9d7	
	New key	Value	Description

Headers (1)

	Key	Value	Description
☑	Content-Type	application/json	
	New key	Value	Description

Body Cookies (2) Headers (14) Test Results

Status: 200 OK Time: 226 ms Size: 1.59 KB

```
{
    "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9
        .eyJzdWIiOiJ2bXdhcmUuY29tOmY0MmViNzRjLTI3M2ItNDVmNS05YmVmLWUzZTcwMjkyNDllMyIsImF6cCI6ImNzcF9wcmRfZ2F6
        X2ludGVybmFsX2NsaWVudF9pZCIsImRvbWFpbiI6InZtd2FyZS5jb20iLCJjb250ZXh0IjoiMzQ0MGMyMDktMzdkMy00MmIyLWE2N
        2QtNjQ3Y2JkN2Y2ZTkzIiwiaXNzIjoiaHR0cHM6Ly9nYXouY3NwLXZpZG0tcHJvZC5jb20iLCJwZXJtcyI6WyJjc3A6b3JnX21lbW
        JlciIsImV4dGVybmFsL3liVWRvVEMwNWtZRkM5Wkc1NjBrcHNuMEk4TV8vdm1jLXVzZXI6ZnVsbCJdLCJjb250ZXh0X25hbWUiOiI
        4MWMxM2I3MC1jNTMzLTQ2MGMtOTI4OC03NjcyMDBjZWNhZjkiLCJleHAiOjE1MTYzMjU0NjYsImlhdCI6MTUxNjMyMzY2NiwianRp
        IjoiOTJjNGIwMjYtOGI4MC00YWQ5LWEyYjctMWMwZmE3ODdhNWE2IiwidXNlcm5hbWUiOiJ3dHV0aGlsbCJ9
        .ToDwotYjCFyb_7WMAqdfE5gNyeoGpjTjLY0t_gttGioVxtBzLd2Xa1a33ORYLhpJaIhUMnNvbt23xed9D5goBILhCLBjYTZjmGfK
        aDYXOoM_nuazY-s7_mWNVO2s6ma3hqYIQgUi-Ob3ZshlPecYDMEqx2X
```

In addition to `access_token`, the 200 OK response includes the passed-in token, expiry time, and your permissions scope. A bearer token allows anyone in possession of the token to execute a task like anyone else possessing the token.

VMware Cloud REST Interfaces

The table below lists the current REST interfaces, organized by command hierarchy.

Curly braces indicate substitutions, usually a GUID. For reference documentation about the REST interfaces, go to the VMC Console, sign in, and click **Developer Center > API Explorer**. The APIs are organized by expandable categories.

	URL	Description
get	/orgs	Get organizations associated with calling user
get	/orgs/{org}	Get details of organization
get	/orgs/{org}/providers	Get enabled cloud providers for an organization
delete	/orgs/{org}/subscriptions/{subscription}	Cancel a Subscription (discontinued)
get	/orgs/{org}/subscriptions/{subscription}	Get a subscription
get	/orgs/{org}/subscriptions	Get all subscriptions
post	/orgs/{org}/subscriptions	Create a subscription
get	/orgs/{org}/subscriptions/offer-instances	List all offers available for the specific product type in its region
get	/orgs/{org}/subscriptions/products	List the products that are available for purchase
get	/orgs/{org}/tasks	List all tasks for organization
get	/orgs/{org}/tasks/{taskId}	Get task details
post	/orgs/{org}/tasks/{taskId}	Modify an existing task
post	/orgs/{org}/sddcs/{sddc}/clusters	Add a cluster in the target SDDC
delete	/orgs/{org}/sddcs/{sddc}/clusters/{cluster}	Delete a cluster
post	/orgs/{org}/sddcs/{sddc}/esxs	Add/Remove one or more ESX hosts in the target cloud
get	/orgs/{org}/sddcs	List all the SDDCs of an organization
post	/orgs/{org}/sddcs	Provision SDDC
delete	/orgs/{org}/sddcs/{sddc}	Delete SDDC
get	/orgs/{org}/sddcs/{sddc}	Get SDDC
get	/orgs/{org}/sddcs/{sddc}/publicips	List all public IPs for an SDDC
post	/orgs/{org}/sddcs/{sddc}/publicips	Allocate public IPs for an SDDC
delete	/orgs/{org}/sddcs/{sddc}/publicips/{id}	Free one public IP for an SDDC
get	/orgs/{org}/sddcs/{sddc}/publicips/{id}	Get one public IP for an SDDC
patch	/orgs/{org}/sddcs/{sddc}/publicips/{id}	Attach or detach a public IP to workload VM for an SDDC
get	/orgs/{org}/sddcs/{sddc}/mgw/publicips/{id}	Get one public IP for the mgw of an SDDC (discontinued)
get	/orgs/{org}/sddcs/{sddc}/mgw/publicips	List all public IPs for the mgw of an SDDC (discontinued)
put	/orgs/{org}/sddcs/{sddc}/dns/private	Update DNS of management VMs to use private IP addresses
put	/orgs/{org}/sddcs/{sddc}/dns/public	Update DNS of management VMs to use public IP addresses
post	/orgs/{org}/sddcs/{sddc}/convert	Convert one host SDDC to minimum hosts for a default SDDC

	URL	Description
get	/orgs/{org}/sddc-templates	List available SDDC configuration templates in an organization
get	/orgs/{org}/sddcs/{sddc}sddc-template	Get configuration template for an SDDC
get	/orgs/{org}/sddc-templates/{templateId}	Get configuration template by given template ID
delete	/orgs/{org}/sddc-templates/{templateId}	Delete SDDC configuration template by given ID
get	/orgs/{org}/storage/cluster-constraints	Get constraints on storage size for EBS backed clusters
post	/orgs/{org}/tbrs/reservation	Retrieve reservations for all SDDCs in this organization
get	/orgs/{org}/tbrs/support-window	Get support windows for ticket based reservation service
put	/orgs/{org}/tbrs/support-window/{id}/{SddcId}	Move specified SDDC to the new support window ID
get	/orgs/{org}/account-link	Get a link for customer's account to start the linking process
get	/orgs/{org}/account-link/sddc-connections	Get a list of SDDC connections for the customer's organization
get	/orgs/{org}/account-link/compatible-subnets	Get a customer's compatible subnets for account linking
post	/orgs/{org}/account-link/compatible-subnets	Set which subnet to link accounts and finish the linking process
get	/orgs/{org}/account-link/compatible-subnets-async	Task to get customer's compatible subnets for account linking
post	/orgs/{org}/account-link/compatible-subnets-async	Task to set customer's compatible subnets for account linking
get	/orgs/{org}/account-link/connected-accounts	Get a list of connected accounts
delete	/orgs/{org}/account-link/connected-accounts/{pathId}	Delete a particular connected (linked) account.
post	/orgs/{org}/account-link/map-customer-zones	Create task to re-map customer's datacenters across zones
get	/orgs/{org}/sddcs/{sddc}/networking/connectivity-tests	Connection validation group result wrapper at task-params
post	/orgs/{org}/sddcs/{sddc}/networking/connectivity-tests	Retrieve metadata for connectivity tests
post	/locale	Set locale for the session

Finding API Reference Information

For more information about these REST interfaces, visit the VMware {Code} website at https://code.vmware.com and click API Explorer. On the left side, under **Language Bindings**, click the button for **REST**. VMC for AWS should appear as one of the categories. The API reference is in a common VMware REST API format.

VMware Cloud Networking APIs

The table below lists the REST interfaces for VMware Cloud Networking APIs (preview mode), used to set up a software defined network.

These VMware Cloud Networking APIs can be run from the public cloud. The public APIs are typically used for provisioning and initial connectivity (day 0).

Similar commands are available from your on-premises cloud as VMware NSX APIs. In this case, the URL starts as `/api/4.0/` instead of `/orgs/`... and continues as below. The direct from premises VMware NSX APIs are used for recurring operations (day 2).

These are available as "preview" APIs and may change in the future. Curly braces indicate substitutions, usually a GUID.

Table 1-1. VMware Cloud Networking APIs (preview mode)

	URL	Description
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/statistics/dashboard/firewall	Retrieve firewall dashboard statistics for a management or compute gateway (NSX Edge)
put	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/nat/config	Modify NAT configuration for a management or compute gateway (NSX Edge)
delete	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/nat/config	Delete all NAT configuration for the specified management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/nat/config	Retrieve NAT configuration for a management or compute gateway (NSX Edge)
put	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/firewall/config/rules/{ruleId}	Modify the specified firewall rule for a management or compute gateway (NSX Edge)
delete	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/firewall/config/rules/{ruleId}	Delete a specific firewall rule for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/firewall/config/rules/{ruleId}	Retrieve a specific firewall rule for a management or compute gateway (NSX Edge)
put	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/ipsec/config	Modify IPsec VPN configuration for a management or compute gateway (NSX Edge)
delete	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/ipsec/config	Delete IPsec VPN configuration for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/ipsec/config	Retrieve IPsec VPN configuration for a management or compute gateway (NSX Edge)
put	/orgs/{org}/sddcs/{sddc}/networks/4.0/ sddc/ cgws/{edgeId}/l2vpn/config	Modify SDDC L2 VPN configuration
delete	/orgs/{org}/sddcs/{sddc}/networks/4.0/ sddc/ cgws/{edgeId}/l2vpn/config	Delete SDDC L2 VPN configuration
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ sddc/ cgws/{edgeId}/l2vpn/config	Retrieve SDDC L2 VPN configuration
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/statistics/interfaces	Retrieve interface statistics for a management or compute gateway (NSX Edge)
put	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/nat/config/rules/{ruleId}	Update the specific NAT rule for a management or compute gateway (NSX Edge)
delete	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/nat/config/rules/{ruleId}	Delete the specific NAT rule for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/edges	Retrieve information about all management and compute gateways and other routers (NSX Edges)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/statistics/dashboard/interface	Retrieve interface dashboard statistics for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/firewall/statistics/{ruleId}	Retrieve statistics for a specific firewall rule for a management or compute gateway (NSX Edge)

Table 1-1. VMware Cloud Networking APIs (preview mode) (continued)

	URL	Description
post	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/firewall/config/rules	Append firewall rules for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/l2vpn/config/statistics	Retrieve L2 VPN statistics for a compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/status	Retrieve the status of the specified management or compute gateway (NSX Edge)
post	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/nat/config/rules	Append a NAT rule for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/statistics/interfaces/uplink	Retrieve uplink interface statistics for a management or compute gateway (NSX Edge)
put	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/dns/config	Configure DNS server configuration for a management or compute gateway (NSX Edge)
post	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/dns/config	Enable or disable DNS configuration for a management or compute gateway (NSX Edge)
delete	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/dns/config	Delete DNS server configuration for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/dns/config	Retrieve DNS server configuration for a management or compute gateway (NSX Edge)
put	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/firewall/config	Configure firewall for a management or compute gateway (NSX Edge)
delete	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/firewall/config	Delete firewall configuration for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/firewall/config	Retrieve the firewall configuration for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/statistics/dashboard/ipsec	Retrieve IPsec dashboard statistics for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/vnics	Retrieve all interfaces for the specified management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/dns/statistics	Retrieve DNS server statistics for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/statistics/interfaces/internal	Retrieve internal interface statistics for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/ipsec/statistics	Retrieve IPsec VPN statistics for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/peerconfig	Retrieve IPsec VPN peer configuration for a management or compute gateway (NSX Edge)
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ edges/ {edgeId}/dhcp/leaseInfo	Retrieve DHCP leaseinfo of a management or compute gateway (NSX Edge)
put	/orgs/{org}/sddcs/{sddc}/networks/4.0/ sddc/ networks/{networkId}	Modify a network in an SDDC

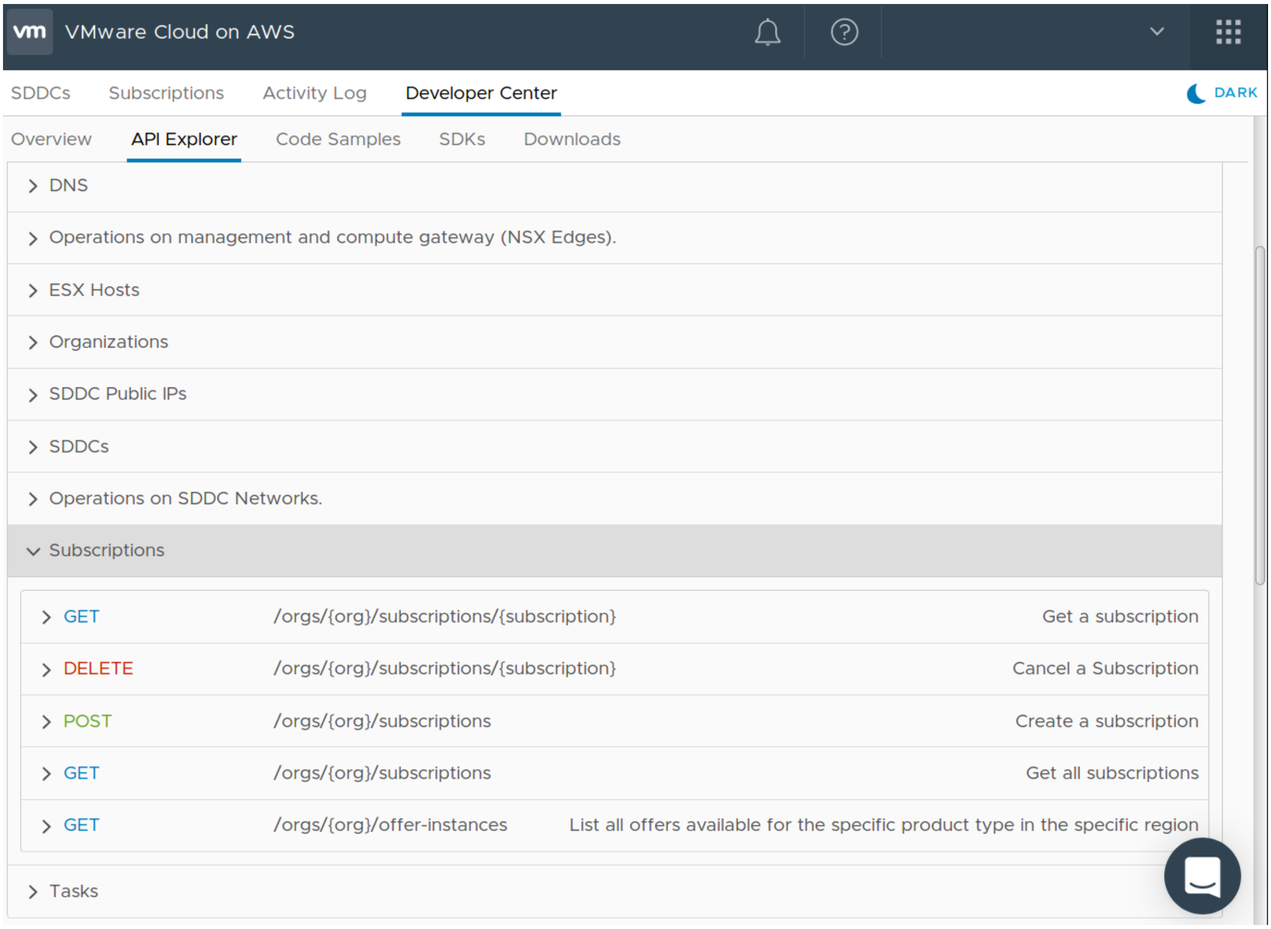
Table 1-1. VMware Cloud Networking APIs (preview mode) (continued)

	URL	Description
delete	/orgs/{org}/sddcs/{sddc}/networks/4.0/ sddc/ networks/{networkId}	Delete a network in an SDDC
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ sddc/ networks/{networkId}	Retrieve information about a network in an SDDC
post	/orgs/{org}/sddcs/{sddc}/networks/4.0/ sddc/ networks	Create a network in an SDDC
get	/orgs/{org}/sddcs/{sddc}/networks/4.0/ sddc/ networks	Retrieve all networks in an SDDC

VMC Console API Explorer

The VMC Console offers a Developer Center tab to help DevOps and administrators automate functions in the VMware Cloud on AWS.

Figure 1-2. API Explorer and reference



› DNS

› Operations on management and compute gateway (NSX Edges).

› ESX Hosts

› Organizations

› SDDC Public IPs

› SDDCs

› Operations on SDDC Networks.

⌄ Subscriptions

› GET	/orgs/{org}/subscriptions/{subscription}	Get a subscription
› DELETE	/orgs/{org}/subscriptions/{subscription}	Cancel a Subscription
› POST	/orgs/{org}/subscriptions	Create a subscription
› GET	/orgs/{org}/subscriptions	Get all subscriptions
› GET	/orgs/{org}/offer-instances	List all offers available for the specific product type in the specific region

› Tasks

The Developer Center tab appears to the right of the SDDCs, Subscriptions, and Activity Log tabs. After you click **Developer Center**, another set of tabs appears below.

- **Overview** gives an introduction to the VMC Console Developer Center.
- **API Explorer** provides reference information about the REST interfaces listed in Table 1 and Table 2.
- **Code Samples** shows many contributed programs in various languages to automate VMC operations.
- **SDKs** lists vSphere Automation SDKs with Github source and documentation on code.vmware.com.
- **Downloads** gives direct links to obtain the Datacenter CLI bundle and the PowerCLI for PowerShell.

In addition to providing reference information, API Explorer can also be used to execute REST commands within your SDDC. APIs are organized according to category. Click a category to show related APIs, as has been done for Subscriptions in the following figure.

At the top level, API Explorer is similar to the Swagger UI. When you click an item, it expands to show API description, possible responses, and a **Try it out** section with parameters and their value. Unlike some other interfaces, the API Explorer hides information in blue headings that expand when you click them. This makes it easy to browse long responses with unneeded data. Your organization ID is pre-filled so you don't need to provide it, and authentication is done automatically with `auth_token` fetched for you.

It might be possible to perform all your SDDC and Cloud automation from the API Explorer, although in the long run, repetitive tasks are easier to perform with a program coded in Python, PowerCLI, or DCLI.

Underneath the VMware Cloud on AWS interfaces is another section, showing REST commands for VMware Cloud Services, in case you need one of them, such as OAuth Client operations.

About Login and Authorization

After you login to your organization's SDDC, you can obtain an access key, an organization ID, and an API token.

If you are an organization member, you can login to your organization's SDDC as a user. Your user name is probably your login ID @ DNS domain name.

To see your account information, click the pull-down menu on upper right of the VMC console screen, and click **My Account**. The access key appears at the bottom of your profile.

To obtain an organization ID and SDDC ID, in the SDDCs tab, click VIEW DETAILS at bottom left of an SDDC, then click **Support**. The **Org ID** is listed under Support Information.

Generate an API Token

SDK applications use API tokens to make connections that are authorized for certain activities on the VMC Console. Previously called an OAuth Refresh token, an API token authorizes actions per organization.

You can generate more than one API token. A token is valid for six months, after which time you must regenerate it if you want to continue using APIs that rely on a token. If you believe an API token has been compromised, you can revoke the token to prevent unauthorized access. You generate a new API token to renew authorization.

A valid API token is required to access services of the cloud services platform (csp) and the VMware Cloud (vmc). The API token handles authorization more securely than an access key because it applies to only one organization, not across all organizations. The API token has the additional advantage of being connected to an SDK application, rather than an individual user.

To generate an API token:

1 On the VMware Cloud Services toolbar, click your user name and select **My Account > API Tokens**.

2 Click **New Token**.

3 Click **Copy to Clipboard**.

4 Paste the token into a safe place so you can retrieve it for use later on.

Authorize VMware Cloud APIs

After you generate an API token, you can use it to interact with VMware Cloud Service APIs by exchanging it for an authorization token.

1 Copy the API token from the safe place where you pasted it.

2 Exchange the API token for an authorization token by calling POST to `/am/api/auth/api-tokens/authorize`.

   You must set the content type of the POST to `application/x-www-form-urlencoded`.

3 Use the authentication token in the `csp-auth-token` header of your subsequent HTTP calls.

Interact with Single Sign-On

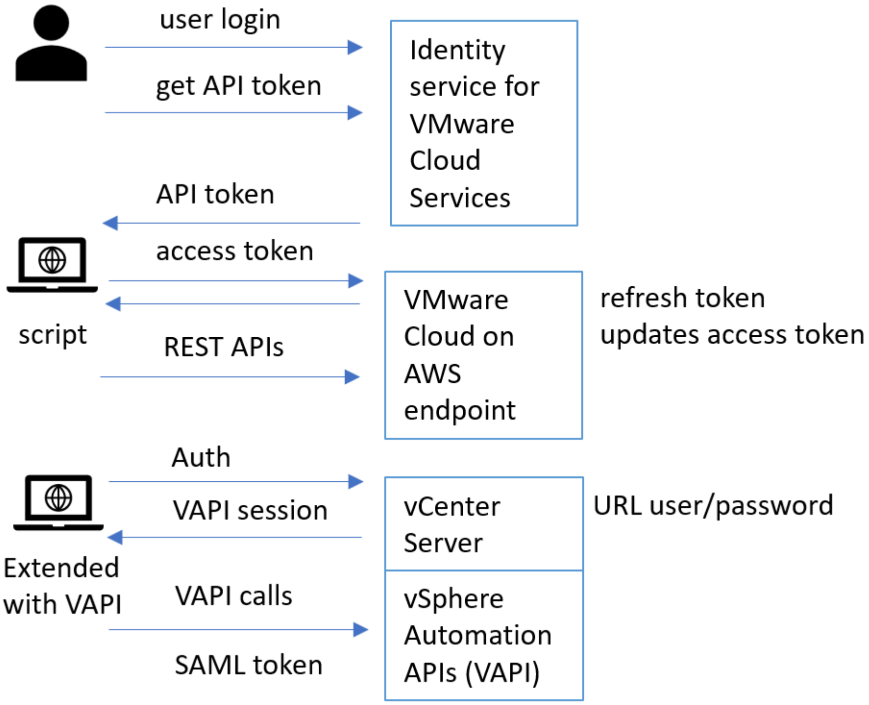
To interact with vSphere, you can use vCenter Single Sign-On (SSO) to send credentials to the SSO service and receive a SAML token that establishes an authenticated session with a vSphere Automation endpoint or a vCenter Server endpoint.

SAML tokens can be used instead of password-based authentication. Client applications present a SAML token to the endpoint, in exchange for a session identifier with which they area allowed to perform a series of authenticated operations. Token-based authentication is associated with a script or program, rather than with an individual user.

For details and code examples (Java, .NET, Python, Perl) see section "Retrieve a SAML Token" in the *VMware vSphere Automation SDKs Programming Guide*.

The VMC login and authorization flow is depicted below.

Figure 1-3. VMware Cloud (VMC) Authorization



Using Curl with VMware Cloud on AWS

2

You can use the VMware Cloud™ on AWS REST interfaces to automate tasks in your data center, and to perform some tasks that are not yet available in the VMC Console. Topic below show use of the `curl` command to send REST calls to the VMC Console.

This chapter includes the following topics:

Generate an Access Token

Before making a call to the VMware Cloud on AWS, you must request an API token, which authorizes your REST based programs to use the service.

Before you can generate the access token, you need to obtain an API token associated with your VMware Cloud on AWS account.

Procedure

1 Get an API Token.

   a Log in to http://vmc.vmware.com using your My VMware credentials.

   b On the VMware Cloud Services toolbar, click your user name and select **My Account > API Tokens**.

   c Click **New Token**.

   d Click **Copy to Clipboard**.

   e Paste the token into a safe place so you can retrieve it for later use.

2 To generate the access token, issue a POST command to the following URL, replacing `{token}` with the API token from step 1.

```
https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize?refresh_token={api-
token}
```

3 When the POST command returns results in the form `{"access-token": "token-string"}`, copy and save the access token string for later use. This string is over 900 characters long, so be careful to avoid line breaks.

Example: Generate an Access Token Using cURL

For example, to generate an authorization token, run the following command. The -X option sends a custom request (not GET). The -H option specifies that the HTTP header follows.

```
curl -X POST -H "Content-Type: application/json"
 https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize?refresh_token=api-token
```

What to do next

Pass the returned access token as part of the header in any subsequent REST calls you make. This is the only REST call run against the console.cloud cloud service provider . Subsequent calls are run against the `vmc` URL.

Get the Organization ID

Many calls to the VMware Cloud™ on AWS API require an organization ID.

Use the `/vmc/api/orgs` method to get the organization ID. For reference documentation about the REST interfaces, go to the VMC Console, sign in, and click **Developer Center > API Explorer**.

Prerequisites

You must have an authentication token to get the organization ID.

Procedure

1 Issue a GET to https://vmc.vmware.com/vmc/api/orgs

2 Paste in the `token-string` that you saved previously.

The value returned for the `id` key is the organization ID.

Example: Get the Organization ID Using cURL

You can also get the organization ID by browsing to your SDDC and clicking **View Details > Support**.

To get the organization ID, use the following command.

```
curl -X GET -H 'csp-auth-token: token-string' https://vmc.vmware.com/vmc/api/orgs
```

Get SDDC IDs

API calls that operate on an single SDDC require the SDDC ID as a parameter.

Use the `vmc/api/orgs/{org}/sddcs` method to get the organization ID. For reference documentation about the REST interfaces, go to the VMC Console, sign in, and click **Developer Center > API Explorer**.

Prerequisites

In order to get the SDDC ID, you must have an authentication token and an organization ID.

Procedure

- Issue a GET to https://vmc.vmware.com/vmc/api/orgs/%7Borg%7D/sddcs where *{org]* is replaced by the organization ID for the organization containing your SDDCs.

  The IDs for each SDDC are returned in the `sddc_id` key.

Example: Get SDDC IDs Using cURL

Use the following command to get SDDC IDs using cURL:

```
curl -X GET -H 'csp-auth-token: token-string' \
 -H 'Accept: application/json' 'https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs'
```

Add a Host Using the VMware Cloud™ on AWS API

If you have the capacity to add extra hosts to your SDDC, you can use the VMware Cloud™ on AWS API to add a host.

Use the `vmc/api/orgs/{org}/sddcs/{sddc}/esxs` method to add a host. For reference documentation about the REST interfaces, go to the VMC Console, sign in, and click **Developer Center > API Explorer**.

You can't add more hosts than the maximum number allowed in your SDDC.

Prerequisites

You need an authorization token, an organization ID, and an ID for the SDDC to which you want to add a host.

Procedure

- Issue a POST to https://vmc.vmware.com/vmc/api/orgs/%7Borg%7D/sddcs/%7Bsddc%7D/esxs where *{org]* is replaced by the organization ID for the organization and *{sddc}* is replaced by the ID for your SDDC. The body of the request should specify the number of hosts to create in the format `{"num_hosts": number}`

  A new host is provisioned and added to the SDDC cluster.

Example: Add a Host to an SDDC Using cURL

To provision a single host in your SDDC, use the following command.

```
curl -X POST -H 'csp-auth-token: token-string \
-H 'Accept: application/json' --header 'Content-Type: application/json' \
 -d '{ "num_hosts": 1}' 'https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}/esxs'
```

Remove a Host Using the VMware Cloud on AWS API

You can remove a host as long as you are above the minimum number of hosts for your SDDC.

Use the `vmc/api/orgs/{org}/sddcs/{sddc}/esxs/{esx}` method to remove a host. For reference documentation about the REST interfaces, go to the VMC Console, sign in, and click **Developer Center > API Explorer**.

Prerequisites

You need an authorization token, an organization ID, and an ID for the SDDC to which you want to add a host.

Procedure

- Issue a DELETE to https://vmc.vmware.com/vmc/api/orgs/%7Borg%7D/sddcs/%7Bsddc%7D/esxs/%7Besx%7D where *{org]* is replaced by the organization ID for the organization, *{sddc}* is replaced by the ID for your SDDC, and *{esx}* is replaced by the ID for the host.

  The specified host is removed from the SDDC.

Example: Remove a Host Using cURL

To remove a host in your SDDC, use the following command.

```
curl -X DELETE -H 'csp-auth-token: token-string \
-H'Accept: application/json' 'https://vmc.vmware.com/vmc/api/orgs/\
{org}/sddcs/{sddc}/esxs/{esx}'
```

Using a REST Client with VMware Cloud on AWS

3

You can use the VMware Cloud on AWS interfaces with a REST client such as Postman to automate setup and maintenance tasks in your datacenter.

This chapter includes the following topics:

Generate Access Token from API Token

Each user of VMware Cloud on AWS is assigned an API token, which can be used to authorize a short-term session and obtain an access token.

To obtain your API token, login to vmc.vmware.com where your SDDC is hosted. Click the pull-down menu on upper right of the VMC console screen, and click **My Account > API Token**. Its GUID appears near top of the list, and is valid for many months unless regenerated or revoked.

To obtain an access token, called a csp-auth-token in subsequent commands, supply these fields in Postman or similar browser based REST client. Under parameters (Params) type `refresh_token` for the key and your API Token for its value. Under Headers, type `Content-Type` for the key and `application/json` for its value.

```
POST
https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize

refresh_token   YourAPIToken

Content-Type    application/json
```

This pattern for Params and Headers will repeat in subsequent commands. POST and PUT commands also have a Body that will be supplied underneath Headers.

Click Send to run the REST command, and your `access_token` appears below. You will need to copy its (long) value as the `csp-auth-token` for subsequent commands. The returned Body text includes the `expires_in` field, expressed in seconds. For example, 1799 indicates that your `access_token` lasts a bit less than 30 minutes.

Note Keep the `authorize` tab open in Postman or other REST client, so you can update the `access_token` after it expires, for use in subsequent tabs.

Operations on Organizations

You can find the organizations you are associated with, get details about an organization, and determine the enabled cloud providers for an organization.

In Postman or another REST client, leave the tab open where you just ran the authorize command, and open a new tab. This makes it easier to copy and paste the `access-token` to provide as the value of `csp-auth-token` for subsequent commands.

To find the organization you are associated with, run the `/orgs` command. Click *Headers*, type `csp-auth-token` for the key, and as its value paste the `access-token` from the authorize command in the first tab.

```
GET
https://vmc.vmware.com/vmc/api/orgs

csp-auth-token   Paste-access-token-here

...
"id": "91c13b70-c533-460c-9288-767200cecaf9"
```

The "`id`" field is the GUID of the organization you are associated with. You can also find this value in the VMC Console under the Support tab for your SDDC. If you are associated with multiple organizations, they will appear as a separate JSON block in the returned body.

To get details about the organization, open a new tab and run the `/orgs` command again, pasting the GUID of your organization in place of {org} in the following command. Click *Headers*, type `csp-auth-token` for the key, and as its value paste the `access-token` from the authorize command in the first tab.

```
GET
https://vmc.vmware.com/vmc/api/orgs/{org}

csp-auth-token   Paste-access-token-here

...
"created": "2018-01-23T05:13:32.000277Z"
```

Among other information is the date when the organization was created, information about the cloud provider, host limit, and invitation code.

To determine the enabled cloud providers for the organization, open a new tab and run the `/orgs` command again, pasting the GUID of your organization in place of {org} in the following command, and adding `/providers` at the end. Click *Headers*, type `csp-auth-token` for the key, and as its value paste the `access-token` from the authorize command in the first tab.

```
GET
https://vmc.vmware.com/vmc/api/orgs/{org}/providers

csp-auth-token   Paste-access-token-here

[
    {
        "provider": "OURCLOUD",
        "regions": [
            "US_WEST_2",
            "US_EAST_1"
        ]
    }
]
```

Operations on Subscriptions

Subscriptions can save you money by committing to buy a certain amount of capacity for a defined period. A subscription is not required. Any use of service not covered by subscription is charged according to on-demand pricing.

If you run GET subscriptions command before creating a subscription, the subscription shows as empty. You can discover your subscription offers with the following interface:

```
GET
https://https://vmc.vmware.com/vmc/api/orgs/{org}/offer-instances
```

For that command and ones below, click Headers, type `csp-auth-token` for the key, and as its value paste the `access-token` from the authorize command in the initial tab.

Once you see the subscription offers, you can run a POST command to create a subscription according to offered terms. In the header, supply the access token and set content type to JSON. In the request body, choose the offer instance that you prefer, for example one shown below for 12 months.

```
POST
https://vmc.vmware.com/vmc/api/orgs/{org}/subscriptions

csp-auth-token  Paste-access-token-here
Content-Type    application/json

{
  "offer_version": "1.0",
  "product_type": "host",
  "region": "US_WEST_2",
  "commitment_term": "12",
  "offer_name": "VMware Cloud on AWS",
  "quantity": 1
}

...
    "id": "56193746-9d94-4839-bc6c-907754bc3d1f",
```

In the returned body, the `"id"` value is the GUID of your subscription. To verify your subscription, run the following command to see its terms.

```
GET
https://vmc.vmware.com/vmc/api/orgs/{org}/subscriptions/{subscriptionID}
```

To delete your subscription and return to on-demand pricing, use the DELETE command with the same URL.

```
DELETE
https://vmc.vmware.com/vmc/api/orgs/{org}/subscriptions/{subscriptionID}
```

Operations on Hosts and Clusters

For greater compute and storage capacity, you an add an ESXi host to a cluster in your SDDC, or for even greater capacity, you can add another cluster of four or more ESXi hosts. Each ESXi host has 2 CPUs, 512GB memory, and over 10TB storage. Each cluster contains four or more ESXi hosts.

Use the POST `esxs` command to add or remove and ESXi host. The choice is made by a query (?) string at the end of the URL, specifying an action to add or remove. In Headers, type `csp-auth-token` for the key, and as its value paste the `access-token` from the `authorize` command. In the Body, supply JSON text indicating the number of hosts to add, and the availability zone where it should be added.

```
POST
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}/esxs?action=add

csp-auth-token  Paste-access-token-here
Content-Type    application/json

{
  "num_hosts": 1,
  "availability_zone": "US-West"
}

...
   "id": "1d2bc925-4e4d-455a-ae22-350dca953676"
```

After you run the add action, the GUID of the new ESXi host appears in the returned body.

To remove an ESXi host for a cluster in your SDDC, use a similar POST command with the remove action. You only need to specify `num_hosts`, unless you have multiple clusters in your SDDC, then you need to specify the `clusterId` as well.

```
POST
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}/esxs?action=add

csp-auth-token  Paste-access-token-here
Content-Type    application/json

{
  "num_hosts": 1,
  "availability_zone": "US-West"
}


,,,
   "id": "1d2bc925-4e4d-455a-ae22-350dca953676",
```

The GUID of the removed ESXi host appears in the returned body, with other information.

Use the POST `cluster` command to add a cluster. In Headers, type `csp-auth-token` for the key, and as its value paste the `access-token` from the `authorize` command. In the Body, supply JSON text indicating the number of hosts the cluster should contain (4 or more).

```
POST
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}/clusters

csp-auth-token  Paste-access-token-here
Content-Type    application/json

{
  "num_hosts": 4
}

...
   "id": "9251d2bc-4e4d-455a-ae22-350dca953676"
```

The GUID of the added cluster appears in the returned body, with other information. You specify this GUID when you choose to delete the cluster.

Use the POST `cluster` command to add a cluster. In Headers, type `csp-auth-token` for the key, and as its value paste the `access-token` from the `authorize` command. In the URL, specify as {*cluster*} the GUID of the cluster to delete.

```
DELETE
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}/clusters/{cluster}

csp-auth-token  Paste-access-token-here
Content-Type    application/json
```

Operations on Tasks

You can get a list of recent tasks executed in your SDDC, with status started, finished, or failed. You can get the details of a specific task, and request to cancel it if possible.

To get a long list of recent tasks within your organization, run the `tasks` command. In Headers, type `csp-auth-token` for the key, and as its value paste the `access-token` from the `authorize` command. Also in headers, set Content-Type to application/json so the results body will be easy to read.

```
GET
https://vmc.vmware.com/vmc/api/orgs/{org}/tasks

csp-auth-token  Paste-access-token-here
Content-Type    application/json

...
   "id": "faa241ed-04cb-4685-b67e-d17f69f9bf67"
```

The list of recent tasks starts with general information about the SDDC. Following this is information about each separate task, enclosed in curly braces. The requesting user is listed, which may help you identify which task is which. Near the top of each task listing is an `"id"` line. This GUID the `taskId`, which can be used to get information about this task only, by pasting its value at the end of the URL. The `taskId` can also be used to request task cancellation, as in the following example. Cancel is the only action allowed currently.

```
POST
https://vmc.vmware.com/vmc/api/orgs/{org}/tasks/{taskId}?action=cancel

csp-auth-token  Paste-access-token-here
Content-Type    application/json

...
   "error_messages": [
      "Cannot cancel task: faa241ed-04cb-4685-b67e-d17f69f9bf67 in FINISHED state."
   ],
```

Operations on SDDCs

You can use the `sddcs` commands to provision a new SDDC, although this is something that might be easier to do from the VMC Console. You can get information about all SDDCs in your organization, or just one SDDC. You can delete an SDDC if you have permission to do so.

The `org/sddcs` command gets SDDC information for an entire organization, which might involve a lot of data. You can limit the information returned to an SDDC of interest. You can find your SDDC ID to substitute for `{sddc}` below by looking under the Support tab in VMC Console. In Headers, type `csp-auth-token` for the key, and as its value paste the `access-token` from the `authorize` command. Also in headers, set Content-Type to `application/json` so the results body will be easy to read.

```
GET
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}

csp-auth-token  Paste-access-token-here
Content-Type    application/json
```

In the returned body, the `"name"` of the SCCS corresponds with its name in the VMC Console. The four or more ESXi hosts that constitute the SDDC are listed as for the `esxs` command.

To provision a new SDDC, you must provide a certain amount of information in the request body, as in the example below. This is actually not enough information to create the SDDC without error, but it does create one with the message FAILED on the VMC Console.

```
POST
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs

csp-auth-token  Paste-access-token-here
Content-Type    application/json

{
  "name": "SDK SDDC",
  "account_link_sddc_config": [
    {
      "customer_subnet_ids": [
        "string"
      ],
      "connected_account_id": "c0c61e9d-23f4-3c0d-9472-ba8c6b182766"
    }
  ],
  "vxlan_subnet": "192.168.1.0/24",
  "vpc_cidr": "string",
  "provider": "ZEROCLOUD",
  "sso_domain": "vmc.local",
  "num_hosts": 4,
  "deployment_type": "SingleAZ",
  "region": "US_WEST_2"
}
```

To delete the SDDC, find the `"id"` in the returned body, and copy it for use in the delete command.

```
DELETE
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}

csp-auth-token  Paste-access-token-here
Content-Type    application/json
```

Before you delete an SDDC, make sure that no tasks are running on it, and that it does not contain any data you will need.

Operations on Public IP Addresses

Using the `publicips` commands, you can get the public IP addresses available to your SDDC, allocate a public IP address, attach it to a virtual machine, and free the IP address when no longer needed. The `publicips` commands are based on an AWS mechanism.

To list the public IP addresses available from AWS, run publicips command containing your organization's GUID and the GUID of your SDDC.

```
GET
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}/publicips
```

From the listed public IP addresses, allocate one for use by a virtual machine, as in this example.

```
GET
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}/publicips/{id}
```

To attach a public IP address to a virtual machine workload, use this unusual PATCH command.

```
PATCH
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}/publicips/{id}?action=attach

{
  "public_ip": "41.8.9.10",
  "name": "vm-name",
  "allocation_id": "string",
  "dnat_rule_id": "string",
  "associated_private_ip": "10.0.0.10",
  "snat_rule_id": "string"
}
```

To free a public IP from its association with a virtual machine workload and your SDDC, use the DELETE command.

```
DELETE
https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}/publicips/{id}
```

The `mgw/publicips` commands operate in a similar manner on the management gateway instead of the compute load.

The `dns/private` and `dns/public` commands update the DNS record of management VMs to use private IP addresses or public IP addresses, respectively.

Preview Mode Networking and Security

4

VMware Cloud customers can connect their on-premises data centers to AWS using the direct connect service with VMware Cloud networking APIs.

This chapter includes the following topics:

- REST for Preview Mode Networking and Security
- Learning More About Network and Security APIs

REST for Preview Mode Networking and Security

VMware Cloud on AWS provides public REST commands for setting up a cloud based datacenter, and direct mode REST commands for continuing networking and security operations.

These REST functions offer simplified access to control the management gateway (MGW), compute gateway (CGW), and logical networks. The REST functions pass JSON data back and forth. Sections below show the user of Curl commands.

Prerequisites

- Provisioned VMC SDDC
- For the public endpoint, VMC credentials with access token
- For the direct endpoint, NSX Manager credentials
- REST client such as `curl` or browser based tool

Authenticate API Endpoint to VMC

First obtain your `refresh-token` from the VMC Console. Click the **v** on upper right next to your name and organization. In the drop-down menu, click **My Account > API Tokens**. Copy and save the API Token, a 24 character alphanumeric string with hyphen separators.

Generate an Access Token

Use the API Token (`api-token` below) to generate an access token. Here you must connect to console.cloud instead of vmc.vmware.com.

```
curl -X POST -H "Content-Type: application/json" \
https://console.cloud.vmware.com/csp/gateway/am/api/auth/api-tokens/authorize?refresh_token=api-token
```

This command returns a long string with token, bearer, and expiration at the end. The access token is at the beginning, in double quotes, following `access_token` and colon. You will need this access token in subsequent REST commands, so copy and save the access token.

Get NSX Edges ID

For this REST command, you need your organization ID and the cloud SDDC ID. Both of these are available in the VMC Console, in your SDDC listing under the Support tab. They are also available with REST commands as shown in the previous chapter. To get the management gateway (MGW) and compute gateway (CGW), also called NSX Edges, run this command, where you replace *org* with the organization ID and *sddc* with the SDDC ID. Provide the `access_token` above as the `csp-auth-token`.

```
curl -X GET -H 'csp-auth-token:{access-token}' -H 'Accept: application/json' \
'https://vmc.vmware.com/vmc/api/orgs/org/sddcs/sddc/networks/4.0/edges
```

Here is an example of part of what might be returned by the command above.

```
{
            "objectId":"edge-2",
            "objectTypeName":"Edge",
            "vsmUuid":"421EF988-82A1-E9BF-60A3-ACDDC6018DBA",
            "nodeId":"a7be5498-9262-47c2-9dd6-dbfbbe8200fe",
            "revision":30,
            "type":{
               "name":"Edge"
            },
            "name":"SDDC-CGW-1-esg",
            ...
}
```

Configure vCenter Public Access

Create the management gateway (MGW) Firewall rule to enable vCenter access.

Request Public IP Address

Request additional public IP addresses for your VMC SDDC.

Configure VPN for Management Gateway

Configure IPsec VPN for secure connectivity to on-premises.

Validate Private API Endpoint

Authenticate to NSX API and retrieve edges.

The Networking and Security APIs are consistent between public and private endpoints. The differences in Authentication (Basic Auth versus OAuth) and API paths. You can use the same `cloudadmin` SSO user used to sign into vCenter Server and to authenticate with the NSX Private API endpoint.

1 Retrieve NSX Manager private IP.

2. Verify authentication through the Private Endpoint.
3. Retrieve Edges.

```
curl -X GET -H 'csp-auth-token:{auth-token}' -H 'Accept: application/json' \
   https://vmc.vmware.com/vmc/api/orgs/{org}/sddcs/{sddc}

curl -k -u cloudadmin:{nsxpassword} https://{nsxmanager-privateip}/api/versions

curl -k -u cloudadmin:{nsxpassword} -X GET -H 'content-type: application/xml' \
   https://{nsxmanager-privateip}/api/4.0/edges
```

Learning More About Network and Security APIs

The examples of Curl commands to control preview mode Networking and Security can be extended with further information available about VMware NSX APIs.

When you call preview mode Networking and Security APIs from VMware Cloud on AWS, you use the public endpoint. When you call the Networking and Security APIs from a private Cloud or data center, you are using the private endpoint. These endpoints are similar, with the following differences.

- Authentication of the public endpoint uses OAuth, while the private endpoint uses Basic Auth.
- API path names differ at the beginning, but not after these path name elements, public and private:

  ```
  https://vmc.vmware.com/vmc/api/
  https://nsx.mgr.IP.addr/api/4.0/
  ```

For more information about the individual preview mode Networking and Security APIs, you can search and find each of them in the *NSX for vSphere API Guide*, at the following URL:

https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.3/nsx_63_api.pdf