VMware Cloud Director API for NSX Programming Guide

API Version 36.0

VMware Cloud Director 10.3

vmware®

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

https://docs.vmware.com/

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

Contents

About the VMware Cloud Director API for NSX

1

The VMware Cloud Director API for NSX is a proxy API that enables VMware Cloud Director API clients to make requests to the NSX API.

Use this document as a supplement to the *NSX vSphere API Guide* (NSX version 6.3 or later). This document lists the subset of NSX API requests supported by the VMware Cloud Director API for NSX and provides information about differences between those requests as they are described in the NSX API documentation and how you must make them when using the VMware Cloud Director API for NSX.

Relationship to the NSX API

The VMware Cloud Director API for NSX supports a subset of the operations and objects defined in the *NSX vSphere API Guide*. The API supports NSX 6.3 and 6.4. You can download the *NSX vSphere API Guide* from https://pubs.vmware.com/nsx-63/topic/com.vmware.ICbase/PDF/nsx_63_api.pdf (NSX 6.3) or https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/nsx_64_api.pdf (NSX 6.4). Requests listed in this document, with related examples documented in the *NSX vSphere API Guide*, can be used by callers of the VMware Cloud Director API for NSX with a few modifications and some additional constraints.

Relationship to the VMware Cloud Director API

The VMware Cloud Director API for NSX is not part of the VMware Cloud Director API. It uses a proxy facility to allow clients that have authenticated to the VMware Cloud Director API to make NSX API requests through the VMware Cloud Director secure public URL with a `network` suffix. Examples in this document represent this URL as `https://vcloud.example.com/network`.

Note The cross-virtual data center networking feature is available through the VMware Cloud Director OpenAPI. For information about VMware Cloud Director OpenAPI, see *Getting Started with vCloud OpenAPI* at https://code.vmware.com.

Multi-Tenant Support

The NSX API addresses NSX objects in a global scope like that of a VMware® vCenter™ data center. The NSX Proxy API addresses NSX objects within the scope of a VMware Cloud Director tenant organization.

Where the NSX API uses internal edge identifiers such as `edge-1` (typically shown as *edgeId* in the *NSX vSphere API Guide*) to identify an edge, the VMware Cloud Director API for NSX uses the identifier that VMware Cloud Director assigns to the edge. This is a unique identifier in the form of a UUID, as defined by RFC 4122. Use of this identifier allows the API to restrict access to an edge to members of the organization that owns the edge. Organization members' access to an edge is also governed by their role in the organization and the rights associated with that role. The VMware Cloud Director API for NSX uses this edge UUID only to identify the edge, locate the NSX Manager responsible for the edge, and retrieve its internal NSX edge ID, which it uses in subsequent NSX API operations on the edge.

Operations on other NSX objects such as certificates and grouping objects typically require a VMware Cloud Director organization or VDC UUID in the request to limit access to tenants with rights to the VMware Cloud Director object.

VMware Cloud Director system administrators can view or update all edges in the system.

Security

HTTP communications between a VMware Cloud Director API client and server are secured with SSL. API clients must also complete a login request to receive an authorization token that must be included in all subsequent requests.

Request Headers

The following HTTP headers are typically included in requests:

Accept

All requests must include an HTTP `Accept` header that designates the VMware Cloud Director API for NSX version that the client is using.

```
Accept: application/*+xml;version=api-version
```

For example, the following header indicates that the request is from a VMware Cloud Director API for NSX version 29.0 client.

```
Accept: application/*+xml;version=29.0
```

Accept-Encoding

By default, the system returns response content as uncompressed XML. Compressing the response can improve performance, especially when the response is large and network bandwidth is a factor. (Requests cannot be compressed.) To request a response to be returned as compressed XML, include the following header:

```
Accept-Encoding: gzip
```

The response is encoded using `gzip` encoding as described in RFC 1952, and includes the following header:

```
Content-Encoding: gzip
```

In the default configuration, responses smaller than 64 KB are never compressed.

Accept-Language

Message strings in `ErrorType` responses are localized. To specify the language desired in responses, use the `Accept-Language` request header. To request a response with message strings localized to French, use the following header:

```
Accept-Language: fr
```

Authorization

All requests to create a VMware Cloud Director API session must include an `Authorization` header of the form prescribed by the identity provider that your organization uses. See the *vCloud API Programming Guide for Service Providers*.

Content-Type

Requests that include a body must include the following HTTP `Content-Type` header.

```
Content-type: application/xml
```

x-vcloud-authorization

This header, which is returned with the `Session` response after a successful log-in, must be included in all subsequent requests from clients that authenticate to the integrated identity provider or the SAML identity provider. See the *vCloud API Programming Guide for Service Providers*.

X-VMWARE-VCLOUD-CLIENT-REQUEST-ID

The value of this header is used to build a request ID returned in the value of the X-VMWARE-VCLOUD-REQUEST-ID header. The value of this header cannot contain more than 128 characters drawn from the set of letters, numbers, and the hyphen (-). Values with invalid characters are ignored. Values with more than 128 characters are truncated.

NSX Edge Gateway Management 2

Each NSX Edge Gateway provides network edge security and gateway services to isolate a virtualized network.

This chapter includes the following topics:

Query or Upgrade an Edge Gateway

You can use the VMware Cloud Director API for NSX to query all edges, query a specific edge, or upgrade an edge.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 2-1. Summary of NSX Edge Gateway Query and Upgrade Requests

Operation	Request	Request Body	Response
List all edges in the system.	GET *API-URL*/edges	None	`pagedEdgeList`
List the edge with identifier *id*.	GET *API-URL*/edges/*id*	None	`edge`

Table 2-1. Summary of NSX Edge Gateway Query and Upgrade Requests (continued)

Operation	Request	Request Body	Response
Get the status of the edge with identifier *id*.	GET *API-URL*/edges/*id* /status	None	`edgeStatus`
Get the summary of the edge with identifier *id*.	GET *API-URL*/edges/*id* /summary	None	`edgeSummary`
Get the list of all jobs for the edge with identifier *id*.	GET *API-URL*/edges/*id*/jobs	None	`edgeJobs`
Get the list of active jobs for the edge with identifier *id*.	GET *API-URL*/edges/*id*/jobs?status=active	None	`edgeJobs`
Upgrade the edge with identifier *id*.	POST *API-URL*/edges/*id* /?action=upgrade	None	204 No Content
List the edges contained by VMware Cloud Director organization VDC with id *id*.	GET *API-URL*/edges/?orgVdc=*id*	None	`edgeSummaries`
Configure the edge with identifier *id* to use NSX FIPS mode. Requires NSX 6.3 or later. **Note** This option is available only if the system administrator has allowed enablement of FIPS mode on Edge Gateways. For more information about FIPS mode, see FIPS Mode in the *VMware NSX for vSphere* documentation.	POST *API-URL*/edges/*id* /fips?enable=[true | false]	None	204 No Content

Edge DHCP Services

An NSX edge gateway capabilities include IP address pooling, one-to-one static IP address allocation, and external DNS server configuration. Static IP address binding is based on the managed object ID and interface ID of the requesting client virtual machine.

The DHCP relay capability provided by NSX in your VMware Cloud Director environment enables you to leverage your existing DHCP infrastructure from within your vCloud Director environment without any interruption to the IP address management in your existing DHCP infrastructure. DHCP messages are relayed from virtual machines to the designated DHCP servers in your physical DHCP infrastructure, which allows IP addresses controlled by the NSX software to continue to be in synch with IP addresses in the rest of your DHCP-controlled environments.

Note

- DHCP relay does not support overlapping IP address spaces.
- DHCP relay and DHCP service cannot run on the same vNIC at the same time. If a relay agent is configured on a vNIC, a DHCP pool cannot be configured on the subnets of that vNIC. See the *NSX Administration Guide* for details.

In the table below:

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 2-2. Summary of NSX Edge DHCP Requests

Operation	Request	Request Body	Response
Retrieve DHCP configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/dhcp/config	None	`dhcp`
Update DHCP configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/dhcp/config	`dhcp`	204 No Content
Reset DHCP configuration for the edge with identifier *id* to factory defaults.	DELETE *API-URL*/edges/*id*/dhcp/config	None	204 No Content
Append an IP address pool to the set of DHCP pools configured for the edge with identifier *id*.	POST *API-URL*/edges/*id*/dhcp/config/ippools	`ipPool`	204 No Content
Delete the IP address pool identified by `ippool-#` from the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/config/ippools/ippool-*#*	None	204 No Content
Retrieve the DHCP relay configuration from the edge with identifier *id*.	GET *API-URL*/edges/*id*/dhcp/config/relay	None	`relay`
Update the DHCP relay configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/dhcp/config/relay	`relay`	204 No Content

Table 2-2. Summary of NSX Edge DHCP Requests (continued)

Operation	Request	Request Body	Response
Reset DHCP relay configuration for the edge with identifier *id*.to factory defaults.	DELETE *API-URL*/edges/*id*/dhcp/config/relay	None	204 No Content
Retrieve DHCP lease information from the edge with identifier *id*.	GET *API-URL*/edges/*id*/dhcp/leaseInfo	None	`dhcpLeases`

Edge Firewall Services

Edge Firewall provides perimeter security for organization VDC networks.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 2-3. Summary of NSX Edge Firewall Requests

Operation	Request	Request Body	Response
Retrieve firewall configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/firewall/config	None	`firewall`
Update firewall configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/firewall/config	`firewall`	204 No Content
Reset firewall configuration for the edge with identifier *id* to factory defaults.	DELETE *API-URL*/edges/*id*/firewall/config	None	204 No Content
Append an edge firewall rule for the edge with identifier *id*.	POST *API-URL*/edges/*id*/firewall/config/rules	`firewallRules`	201 Created
Add an edge firewall rule for the edge with identifier *id* above the rule identified by *#*	POST *API-URL*/edges/*id*/firewall/config/rules?aboveRuleId=*#*	`firewallRules`	201 Created
Retrieve the edge firewall rule identified by *#* . (Cannot retrieve internal rules or the default_policy rule.)	GET *API-URL*/edges/*id*/firewall/config/rules/*#*	None	`firewallRule`
Update the edge firewall rule identified by *#* . (Cannot update internal rules or the default_policy rule.)	PUT *API-URL*/edges/*id*/firewall/config/rules/*#*	`firewallRule`	204 No Content

Table 2-3. Summary of NSX Edge Firewall Requests (continued)

Operation	Request	Request Body	Response
Delete the edge firewall rule identified by # . (Cannot delete internal rules or the default policy rule.)	Delete *API-URL*/edges/*id*/firewall/config/rules/#	None	204 No Content
Retrieve statistics for the edge firewall rule identified by # . (Cannot retrieve statistics for internal rules or the default policy rule.)	GET *API-URL*/edges/*id*/firewall/statistics/#	None	`dashboardStatistics`

Edge NAT Services

NSX Edge provides network address translation (NAT) service to assign a public address to a computer or group of computers in a private network. Using this technology limits the number of public IP addresses that an organization requires. You must configure NAT rules to provide access to services running on privately addressed virtual machines.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 2-4. Summary of NSX Edge NAT Requests

Operation	Request	Request Body	Response
Retrieve edge NAT configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/nat/config	None	`nat`
Update edge NAT configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/nat/config	`nat`	204 No Content
Reset edge NAT configuration for the edge with identifier *id* to factory defaults.	DELETE *API-URL*/edges/*id*/nat/config	None	204 No Content
Append a NAT rule to NAT rules on the edge with identifier *id*.	POST *API-URL*/edges/*id*/nat/config/rules	`natRules`	201 Created
Add an edge NAT rule above the rule with identifier# on the edge with identifier *id*.	POST *API-URL*/edges/*id*/nat/config/rules/?aboveRuleId=#	`natRule`	201 Created

Table 2-4. Summary of NSX Edge NAT Requests (continued)

Operation	Request	Request Body	Response
Update edge NAT rule with identifier# on the edge with identifier *id*.	PUT *API-URL*/edges/*id*/nat/config/rules/#	`natRule`	204 No Content
Delete edge NAT rule with the identifier# from the edge with identifier *id*.	Delete *API-URL*/edges/*id*/nat/config/rules/#	None	204 No Content

Note Every external IP address associated with a NAT rule must be registered as a secondary address on the Edge Gateway's uplink interface. The VMware Cloud Director API for NSX handles this registration automatically. Administrators using the NSX API must register those external IP addresses manually.

Edge Routing Services

Dynamic routing protocols such as OSPF and BGP provide forwarding information between layer 2 broadcast domains.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- # is a small integer used in an NSX object identifier.

Table 2-5. Summary of NSX Edge Routing Requests

Operation	Request	Request Body	Response
Retrieve the routing configuration for the edge with identifier *id*	GET *API-URL*/edges/*id*/routing/config	None	`routing`
Update the routing configuration for the edge with identifier *id*	PUT *API-URL*/edges/*id*/routing/config	`routing`	204 No Content
Delete the routing configuration for the edge with identifier *id*	DELETE *API-URL*/edges/*id*/routing/config	None	204 No Content
Retrieve the global routing configuration for the edge with identifier *id*	GET *API-URL*/edges/*id*/routing/config/global	None	`routingGlobalConfig`
Update the global routing configuration for the edge with identifier *id*	PUT *API-URL*/edges/*id*/routing/config/global	`routingGlobalConfig`	204 No Content
Retrieve the static routing configuration for the edge with identifier *id*	GET *API-URL*/edges/*id*/routing/config/static	None	`staticRouting`

Table 2-5. Summary of NSX Edge Routing Requests (continued)

Operation	Request	Request Body	Response
Update the static routing configuration for the edge with identifier *id*	PUT *API-URL*/edges/*id*/routing/config/static	`staticRouting`	204 No Content
Delete static and default routing configuration for the edge with identifier *id*	DELETE *API-URL*/edges/*id*/routing/config/static	None	204 No Content
Retrieve the OSPF routing configuration for the edge with identifier *id*	GET *API-URL*/edges/*id*/routing/config/ospf	None	`ospf`
Update the OSPF routing configuration for the edge with identifier *id*	PUT *API-URL*/edges/*id*/routing/config/ospf	`ospf`	204 No Content
Delete OSPF routing configuration for the edge with identifier *id*	DELETE *API-URL*/edges/*id*/routing/config/ospf	None	204 No Content
Retrieve the BGP routing configuration for the edge with identifier *id*	GET *API-URL*/edges/*id*/routing/config/bgp	None	`bgp`
Update the BGP routing configuration for the edge with identifier *id*	PUT *API-URL*/edges/*id*/routing/config/bgp	`bgp`	204 No Content
Delete BGP routing configuration for the edge with identifier *id*	DELETE *API-URL*/edges/*id*/routing/config/bgp	None	204 No Content

Edge Load Balancer Services

The NSX Edge load balancer distributes incoming service requests evenly among multiple servers in such a way that the load distribution is transparent to users. Load balancing thus helps in achieving optimal resource utilization, maximizing throughput, minimizing response time, and avoiding overload. NSX Edge provides load balancing up to Layer 7.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 2-6. Summary of NSX Edge Load Balancer Requests

Operation	Request	Request Body	Response
Retrieve the load balancer configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/loadbalancer/config	None	`loadBalancer`
Update the load balancer configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/loadbalancer/config	`loadBalancer`	204 No Content
Delete the load balancer configuration for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/loadbalancer/config	None	204 No Content
Retrieve the load balancer virtual server configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/loadbalancer/config/virtualservers	None	`loadBalancer`
Update the load balancer virtual server configuration for the edge with identifier *id*. by appending the virtual server defined in the request body.	POST *API-URL*/edges/*id*/loadbalancer/config/virtualservers	`virtualServer`	201 Created
Delete the load balancer virtual server configuration for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/loadbalancer/config/virtualservers	None	204 No Content
Retrieve the configuration of the load balancer virtual server with identifier `virtualServer-#` for the edge with identifier *id*.	GET *API-URL*/edges/*id*/loadbalancer/config/virtualservers/virtualServer-*#*	None	`virtualServer`
Update the configuration of the load balancer virtual server with identifier `virtualServer-#` for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/loadbalancer/config/virtualservers/virtualServer-*#*	`virtualServer`	204 No Content
Delete the configuration of the load balancer virtual server with identifier `virtualServer-#` for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/loadbalancer/config/virtualservers /virtualServer-*#*	None	204 No Content
Retrieve the load balancer pool configuration for the edge with identifier *id*	GET *API-URL*/edges/*id*/loadbalancer/config/pools	None	`loadBalancer`

Table 2-6. Summary of NSX Edge Load Balancer Requests (continued)

Operation	Request	Request Body	Response
Update the load balancer pool configuration for the edge with identifier *id* by appending the pool defined in the request body.	POST *API-URL*/edges/*id*/loadbalancer/config/pools	`pool`	201 Created
Delete the load balancer pool configuration for the edge with identifier *id*	DELETE *API-URL*/edges/*id*/loadbalancer/config/pools	None	204 No Content
Retrieve the load balancer pool with id `pool-#` for the edge with identifier *id*	GET *API-URL*/edges/*id*/loadbalancer/config/pools/pool-*#*	None	`pool`
Update the load balancer pool with id `pool-#` for the edge with identifier *id*	PUT *API-URL*/edges/*id*/loadbalancer/config/pools/pool-*#*	`pool`	204 No Content
Delete the load balancer pool with id `pool-#` for the edge with identifier *id*	DELETE *API-URL*/edges/*id*/loadbalancer/config/pools/pool-*#*	None	204 No Content
Retrieve the load balancer application profile configuration for the edge with identifier *id*	GET *API-URL*/edges/*id*/loadbalancer/config/applicationprofiles	None	`loadBalancer`
Update the load balancer application profile configuration for the edge with identifier *id* to append the application profile defined in the request body.	POST *API-URL*/edges/*id*/loadbalancer/config/applicationprofiles	`applicationProfile`	201 Created
Delete the load balancer application profile configuration for the edge with identifier *id*	DELETE *API-URL*/edges/*id*/loadbalancer/config/applicationprofiles	None	204 No Content
Retrieve the load balancer application profile with id `applicationProfile-#` for the edge with identifier *id*	GET *API-URL*/edges/*id*/loadbalancer/config/applicationprofiles/applicationProfile-*#*	None	`applicationProfile`
Update the load balancer application profile with id for the edge with identifier `applicationProfile-#` *id*	PUT *API-URL*/edges/*id*/loadbalancer/config/applicationprofiles/applicationProfile-*#*	`applicationProfile`	204 No Content
Delete the load balancer application profile with id `applicationProfile-#` for the edge with identifier *id*	DELETE *API-URL*/edges/*id*/loadbalancer/config/applicationprofiles/applicationProfile-*#*	None	204 No Content

Table 2-6. Summary of NSX Edge Load Balancer Requests (continued)

Operation	Request	Request Body	Response
Retrieve the load balancer application rule configuration for the edge with identifier *id*	GET *API-URL*/edges/*id*/loadbalancer/config/applicationrules	None	`loadBalancer`
Update the load balancer application rule configuration for the edge with identifier *id* to append the application rule defined in the request body.	POST *API-URL*/edges/*id*/loadbalancer/config/applicationrules	`applicationRule`	201 Created
Delete the load balancer application rule configuration for the edge with identifier *id*	DELETE *API-URL*/edges/*id*/loadbalancer/config/applicationrules	None	204 No Content
Retrieve the load balancer application rule with id `applicationRule-#` for the edge with identifier *id*	GET *API-URL*/edges/*id*/loadbalancer/config/application rules/applicationRule-*#*	None	`applicationRule`
Update the load balancer application rule with id `applicationRule-#` for the edge with identifier *id*	PUT *API-URL*/edges/*id*/loadbalancer/config/applicationrules/applicationRule-*#*	`applicationRule`	204 No Content
Delete the load balancer application rule with id `applicationRule-#` for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/loadbalancer/config/applicationrules/applicationRule-*#*	None	204 No Content
Retrieve the load balancer monitor configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/loadbalancer/config/monitors	None	`loadBalancer`
Update the load balancer monitor configuration for the edge with identifier *id* to append the monitor defined in the request body.	POST *API-URL*/edges/*id*/loadbalancer/config/monitors	`monitor`	201 Created
Delete the load balancer monitor configuration for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/loadbalancer/config/monitors	None	204 No Content
Retrieve the load balancer monitor with id `monitor-#` for the edge with identifier *id*.	GET *API-URL*/edges/*id*/loadbalancer/config/monitors/monitor-*#*	None	`monitor`
Update the load balancer monitor with id `monitor-#` for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/loadbalancer/config/monitors/monitor-*#*	`monitor`	204 No Content

Table 2-6. Summary of NSX Edge Load Balancer Requests (continued)

Operation	Request	Request Body	Response
Delete the load balancer monitor with id `monitor-#` for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/loadbalancer/config/monitors/monitor-*#*	None	204 No Content
Retrieve load balancer status and statistics for the edge with identifier *id*.	GET *API-URL*/edges/*id*/loadbalancer/statistics	None	`loadBalancerStatusAndStats`
Enable load balancer pool member identified by `member-` *#* on the edge with identifier *id*.	POST *API-URL*/edges/*id*/loadbalancer/config/members/member-*#*?enable=true	None	204 No Content

Edge SSL VPN Services

NSX Edge SSL VPN services enable remote users to connect securely to private networks behind an Edge Gateway.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 2-7. Summary of NSX Edge SSL VPN Requests

Operation	Request	Request Body	Response
Retrieve the SSL VPN configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config	None	`sslvpnConfig`
Update the SSL VPN configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config	`sslvpnConfig`	204 No Content
Enable or disable the SSL VPN configuration for the edge with identifier *id*.	POST *API-URL*/edges/*id*/sslvpn/config?enableService=[true | false]	None	204 No Content
Delete the SSL VPN configuration for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config	None	204 No Content
Retrieve the SSL VPN authentication configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/auth/settings	None	`authenticationConfig`
Update the SSL VPN authentication configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/auth/settings	`authenticationConfig`	204 No Content

Table 2-7. Summary of NSX Edge SSL VPN Requests (continued)

Operation	Request	Request Body	Response
Retrieve all locally-defined SSL VPN users for the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/auth/localserver/users	None	`usersInfo`
Create locally-defined SSL VPN users for the edge with identifier *id*.	POST *API-URL*/edges/*id*/sslvpn/config/auth/localserver/users	`usersInfo`	201 Created
Update locally-defined SSL VPN users for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/auth/localserver/users	`usersInfo`	204 No Content
Delete all locally-defined SSL VPN users for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config/auth/localserver/users	None	204 No Content
Retrieve locally-defined SSL VPN user with identifier `user-`*#* from the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/auth/localserver/users/user-*#*	None	`user`
Update locally-defined SSL VPN user with identifier `user-`*#* on the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/auth/localserver/users/user-*#*	`user`	204 No Content
Delete locally-defined SSL VPN user with identifier `user-`*#* from the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config/auth/localserver/users/user-*#*	None	204 No Content
Retrieve all SSL VPN private networks for the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/client/networkextension/privatenetworks	None	`privateNetworks`
Configure one or more SSL VPN private networks for the edge with identifier *id*.	POST *API-URL*/edges/*id*/sslvpn/config/client/networkextension/privatenetworks	`privateNetworks`	201 Created
Update all SSL VPN private networks for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/client/networkextension/privatenetworks	`privateNetworks`	204 No Content
Delete all SSL VPN private networks for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config/client/networkextension/privatenetworks	None	204 No Content
Retrieve SSL VPN private network with identifier `privateNetwork-`*#* from the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/client/networkextension/privatenetworks/privateNetwork-*#*	None	`privateNetwork`
Update SSL VPN private network with identifier `privateNetwork-`*#* on the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/client/networkextension/privatenetworks/privateNetwork-*#*	`privateNetwork`	204 No Content

Table 2-7. Summary of NSX Edge SSL VPN Requests (continued)

Operation	Request	Request Body	Response
Delete SSL VPN private network with identifier `privateNetwork-#` from the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config/client/networkextension/privatenetworks/privateNetwork-#	None	204 No Content
Retrieve the SSL VPN server configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/server	None	`serverSettings`
Update the SSL VPN server configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/server	`serverSettings`	204 No Content
Retrieve all SSL VPN IP pools from the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/client/networkextension/ippools	None	`ipAddressPools`
Configure an SSL VPN IP pool for the edge with identifier *id*.	POST *API-URL*/edges/*id*/sslvpn/config/client/networkextension/ippools	`ipAddressPool`	201 Created
Update an SSL VPN IP pool for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/client/networkextension/ippools	`ipAddressPool`	204 No Content
Delete all SSL VPN IP pools from the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config/client/networkextension/ippools	None	204 No Content
Retrieve SSL VPN IP pool with identifier *pool-id* from the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/client/networkextension/ippools/*pool-id*	None	`ipAddressPool`
Update SSL VPN IP pool with identifier *pool-id* on the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/client/networkextension/ippools/*pool-id*	`ipAddressPool`	204 No Content
Delete SSL VPN IP pool with identifier *pool-id* from the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config/client/networkextension/ippools/*pool-id*	None	204 No Content
Retrieve all SSL VPN client install packages from the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/client/networkextension/installpackages	None	`clientInstallPackages`
Configure an SSL VPN client install package on the edge with identifier *id*.	POST *API-URL*/edges/*id*/sslvpn/config/client/networkextension/installpackages	`clientInstallPackages`	201 Created
Update an SSL VPN client install package on the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/client/networkextension/installpackages	`clientInstallPackages`	204 No Content
Delete all SSL VPN client install packages on the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config/client/networkextension/installpackages	None	204 No Content

Table 2-7. Summary of NSX Edge SSL VPN Requests (continued)

Operation	Request	Request Body	Response
Retrieve SSL VPN client install package with identifier `clientinstallpackage-#` from the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/client/networkextension/installpackages/clientinstallpackage-#	None	`clientInstallPackages`
Update SSL VPN client install package with identifier `clientinstallpackage-#` on the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/client/networkextension/installpackages/clientinstallpackage-#	`clientInstallPackages`	204 No Content
Delete SSL VPN client install package with identifier `clientinstallpackage-#` from the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config/client/networkextension/installpackages/clientinstallpackage-#	None	204 No Content
Retrieve the SSL VPN client configuration parameters for the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/client/networkextension/clientconfig	None	`clientConfiguration`
Update the SSL VPN client configuration parameters for the edge with identifier *id*.	PUT *API-URL*/edges/<id>/sslvpn/config/client/networkextension/clientconfig	`clientConfiguration`	204 No Content
Retrieve the SSL VPN advanced configuration parameters for the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/advancedconfig	None	`advancedConfig`
Update the SSL VPN advanced configuration parameters for the edge with identifier *id* .	PUT *API-URL*/edges/*id*/sslvpn/config/advancedconfig	`advancedConfig`	204 No Content
Retrieve active SSL VPN sessions for the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/activesessions	None	`activeSessions`
Disconnect active SSL VPN session with identifier *session-id* from the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/activesessions/*session-id*	None	204 No Content
Upload an SSL VPN login script to the edge with identifier *id*.	POST *API-URL*/edges/*id*/sslvpn/config/script/file		`scriptFileId`
Retrieve an SSL VPN login script with identifier# from the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/script/file/#	None	`logonLogoffScripts`
Configure parameters for uploaded SSL VPN login script on the edge with identifier *id*.	POST *API-URL*/edges/*id*/sslvpn/config/script		
Retrieve all SSL VPN login scripts from the edge with identifier *id*.	GET *API-URL*/edges/*id*/sslvpn/config/script		

Table 2-7. Summary of NSX Edge SSL VPN Requests (continued)

Operation	Request	Request Body	Response
Update parameters uploaded SSL VPN login scripts on the edge with identifier *id*.	PUT *API-URL*/edges/*id*/sslvpn/config/script		
Delete all SSL VPN login scripts from the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/sslvpn/config/script	None	200 OK

Edge L2 VPN Services

L2 VPN allows you to configure a tunnel between two sites. Virtual machines remain on the same subnet in spite of being moved between these sites, which enables you to extend your datacenter. An NSX Edge at one site can provide all services to virtual machines on the other site. To create the L2 VPN tunnel, you configure an L2 VPN server and L2 VPN client.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 2-8. Summary of NSX Edge L2 VPN Requests

Operation	Request	Request Body	Response
Retrieve the L2 VPN configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/l2vpn/config	None	`l2Vpn`
Retrieve the L2 VPN statistics for the edge with identifier *id*.	GET *API-URL*/edges/*id*/l2vpn/config/statistics	None	`l2vpnStatusAndStats`
Update the L2 VPN configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/l2vpn/config	`l2Vpn`	204 No Content
Enable or disable the L2 VPN configuration for the edge with identifier *id*.	POST *API-URL*/edges/*id*/l2vpn/config?enableService=[true | false]	None	204 No Content
Delete the L2 VPN configuration for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/l2vpn/config	None	204 No Content

Edge IPSec VPN Services

NSX Edge supports site-to-site IPSec VPN between an NSX Edge instance and remote sites. NSX Edge supports certificate authentication, preshared key mode, IP unicast traffic, and no dynamic routing protocol between the NSX Edge instance and remote VPN routers. Behind each remote VPN router, you can configure multiple subnets to connect to the internal network behind an

NSX Edge through IPSec tunnels. These subnets and the internal network behind a NSX Edge must have address ranges that do not overlap.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 2-9. Summary of NSX Edge IPSec VPN Requests

Operation	Request	Request Body	Response
Retrieve the IPSec VPN configuration for the edge with identifier *id*.	GET *API-URL*/edges/*id*/ipsec/config	None	`ipsec`
Update the IPSec VPN configuration for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/ipsec/config	`ipsec`	204 No Content
Delete the IPSec VPN configuration for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/ipsec/config	None	204 No Content
Retrieve IPSec VPN statistics for the edge with identifier *id*.	GET *API-URL*/edges/*id*/ipsec/statistics	None	`ipsecStatusAndStats`

Edge Interfaces, Logging, Statistics, and Remote Access Properties

These requests retrieve statistics and other information from an edge and configure properties for remote access and logging via syslog.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 2-10. Summary of NSX Edge Interface, Remote Access, Logging, and Statistics Properties Requests

Operation	Request	Request Body	Response
Retrieve vNIC details for the edge with identifier *id*.	GET *API-URL*/edges/*id*/vdcNetworks	None	`edgeInterfaces`
Retrieve syslog settings for the edge with identifier *id*.	GET *API-URL*/edges/*id*/syslog/config	None	`syslog`
Update syslog settings for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/syslog/config	`syslog`	204 No Content
Delete syslog settings for the edge with identifier *id*.	DELETE *API-URL*/edges/*id*/syslog/config	None	204 No Content

Table 2-10. Summary of NSX Edge Interface, Remote Access, Logging, and Statistics Properties Requests (continued)

Operation	Request	Request Body	Response
Retrieve statistics for all interfaces from the edge with identifier *id*.	GET *API-URL*/edges/*id*/statistics/interfaces	None	`statistics`
Retrieve statistics for all uplink interfaces from the edge with identifier *id*.	GET *API-URL*/edges/*id*/statistics/interfaces/uplink	None	`statistics`
Retrieve statistics for all internal interfaces from the edge with identifier *id*.	GET *API-URL*/edges/*id*/statistics/interfaces/internal	None	`statistics`
Retrieve dashboard interface statistics from the edge with identifier *id*.	GET *API-URL*/edges/*id*/statistics/dashboard/interface	None	`dashboardstatistics`
Retrieve dashboard firewall statistics from the edge with identifier *id*.	GET *API-URL*/edges/*id*/statistics/dashboard/firewall	None	`dashboardstatistics`
Retrieve dashboard sslvpn statistics from the edge with identifier *id*.	GET *API-URL*/edges/*id*/statistics/dashboard/sslvpn	None	`dashboardstatistics`
Retrieve dashboard IPsec VPN statistics from the edge with identifier *id*.	GET *API-URL*/edges/*id*/statistics/dashboard/ipsec	None	`dashboardstatistics`
Retrieve the L2 VPN statistics for the edge with identifier *id*.	GET *API-URL*/edges/*id*/l2vpn/config/statistics	None	`l2vpnStatusAndStats`
Update command line (SSH) access settings for the edge with identifier *id*.	PUT *API-URL*/edges/*id*/clisettings	`clisettings`	204 No Content
Enable command line (SSH) access to the edge with identifier *id*.	POST *API-URL*/edges/*id*/cliremoteaccess?enable=true	None	204 No Content
Retrieve support logs from the edge with identifier *id*.	GET *API-URL*/edges/*id*/techsupportlogs	None	`org.springframework.core.io.ByteArrayResource`

NSX Distributed Firewall Service

3

NSX Distributed Firewall can enforce firewall functionality directly at a Virtual Machine's vNIC, and supports a micro-segmentation security model where East-West traffic can be inspected at near line rate processing.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 3-1. Summary of NSX Distributed Firewall Requests

Operation	Request	Request Body	Response
Enable distributed firewall service for organization VDC with identifier *id*.	POST *API-URL*/firewall/vdc/*id*	None	204 No Content
Delete global distributed firewall configuration	DELETE *API-URL*/firewall/globalroot-0/config	None	204 No Content
Retrieve distributed firewall configuration for organization VDC with identifier *id*.	GET *API-URL*/firewall/globalroot-0/config?vdc=*id*	None	`firewallConfiguration`
Retrieve distributed firewall configuration for all organization VDCs in the organization with identifier *org-id*.	GET *API-URL*/firewall/globalroot-0/config?org=*org-id*	None	`firewallConfiguration`
Retrieve distributed firewall configuration at layer 2 for organization VDC with identifier *id*.	GET *API-URL*/firewall/globalroot-0/config/layer2sections/*id*	None	`section`
Retrieve distributed firewall configuration at layer 3 for organization VDC with identifier *id*.	GET *API-URL*/firewall/globalroot-0/config/layer3sections/*id*	None	`section`
Retrieve distributed firewall rule with identifier `rule-#` at layer 2 for organization VDC with identifier *id*.	GET *API-URL*/firewall/globalroot-0/config/layer2sections/*id*/rules/rule-*#*	None	`rule`

Table 3-1. Summary of NSX Distributed Firewall Requests (continued)

Operation	Request	Request Body	Response
Retrieve distributed firewall rule with identifier `rule-#` at layer 3 for organization VDC with identifier *id*.	GET *API-URL*/firewall/globalroot-0/config/layer3sections/*id*/rules/rule-#	None	`rule`
Update distributed firewall configuration at layer 2 for organization VDC with identifier *id*.	PUT *API-URL*/firewall/globalroot-0/config/layer2sections/*id*	`section`	204 No Content
Update distributed firewall configuration at layer 3 for organization VDC with identifier *id*.	PUT *API-URL*/firewall/globalroot-0/config/layer3sections/*id*	`section`	204 No Content
Update distributed firewall rule with identifier `rule-#` at layer 2 for organization VDC with identifier *id*.	PUT *API-URL*/firewall/globalroot-0/config/layer2sections/*id*/rules/rule-#	`rule`	204 No Content
Update distributed firewall rule with identifier `rule-#` at layer 3 for organization VDC with identifier *id*.	PUT *API-URL*/firewall/globalroot-0/config/layer3sections/*id*/rules/rule-#	`rule`	204 No Content
Append a new rule to distributed firewall rules at layer 2 for organization VDC with identifier *id*.	POST *API-URL*/firewall/globalroot-0/config/layer2sections/*id*/rules/rule-#	`rule`	201 Created
Append a new rule to distributed firewall rules at layer 3 for organization VDC with identifier *id*.	POST *API-URL*/firewall/globalroot-0/config/layer3sections/*id*/rules/rule-#	`rule`	201 Created
Delete distributed firewall rule with identifier `rule-#` at layer 2 for organization VDC with identifier *id*.	DELETE *API-URL*/firewall/globalroot-0/config/layer2sections/*id*/rules/rule-#	None	204 No Content
Delete distributed firewall rule with identifier `rule-#` at layer 3 for organization VDC with identifier *id*.	DELETE *API-URL*/firewall/globalroot-0/config/layer3sections/*id*/rules/rule-#	None	204 No Content
Delete distributed firewall from organization VDC with identifier *id*.	DELETE *API-URL*/firewall/*id*	None	204 No Content

Authorization

Three rights control access to distributed firewall configuration:

- ORG_VDC_DISTRIBUTED_FIREWALL_ENABLE

- ORG_VDC_DISTRIBUTED_FIREWALL_CONFIGURE
- ORG_VDC_DISTRIBUTED_FIREWALL_VIEW

An organization administrator role has ORG_VDC_DISTRIBUTED_FIREWALL_VIEW and ORG_VDC_DISTRIBUTED_FIREWALL_CONFIGURE rights by default. Only the system administrator has ORG_VDC_DISTRIBUTED_FIREWALL_ENABLE right by default.

Example: Add a Distributed Firewall Rules

The VMware Cloud Director API for NSX makes use of `etag` headers in responses. Requests that modify an object returned in a response must include the `etag` value from that response in an `if-match` header. For example, this request to retrieve a section of a firewall rule returns the requested section and includes an `etag` in the response header.

Request:

```
GET https://10.17.124.244/network/firewall/globalroot-0/config/layer3sections/c02d1603-
af97-4310-80b9-4f3beaa456c4
```

Response:

```
Content-Type:application/xml
Date:...
ETag:1487090590214
Expires: ...

<?xml version="1.0" encoding="UTF-8"?>
<sections>
   <section
      id="1048"
      name="vdc-01(c02d1603-af97-4310-80b9-4f3beaa456c4)"
      generationNumber="1474037046864"
      timestamp="1474037046864">
      <rule
         id="1020"
         disabled="false"
         logged="false">
         <name>testrule3</name>
         <action>allow</action>
         <appliedToList>
            <appliedTo>
               <name>vdc-01(c02d1603-af97-4310-80b9-4f3beaa456c4)
               </name>
               <value>securitygroup-28</value>
               <type>SecurityGroup</type>
               <isValid>true</isValid>
            </appliedTo>
         </appliedToList>
         <sectionId>1048</sectionId>
         <direction>inout</direction>
```

```
         <packetType>any</packetType>
      </rule>
   </section>
</sections>
```

A subsequent request to modify the section by adding a rule must include the `etag` as the value of an `if-match` request header.

Request:

```
POST https://10.17.124.244/network/firewall/globalroot-0/config/layer3sections/c02d1603-
af97-4310-80b9-4f3beaa456c4/rules
...
if-match:1487090590214
...
<?xml version="1.0" encoding="UTF-8"?>
<rule
   disabled="false"
   logged="false">
   <name>testrule3</name>
   <action>allow</action>
   <appliedToList>
      <appliedTo>
         <name>testrule3</name>
         <value>securitygroup-28</value>
         <type>SecurityGroup</type>
         <isValid>true</isValid>
      </appliedTo>
   </appliedToList>
   <direction>inout</direction>
   <packetType>any</packetType>
</rule>
```

NSX Services

4

Requests documented in this section manage global NSX objects such as certificates and grouping objects.

This chapter includes the following topics:

Certificate Management

NSX supports self-signed certificates, certificates signed by a Certification Authority (CA), and certificates generated and signed by a CA.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

To preserve tenant isolation, globally scoped NSX objects such as certificates, CSRs, and certificate revocation lists, are referenced with a tuple comprising the edge UUID and the NSX ID for the object. For example, where the NSX API references a certificate with identifier `certificate-1` with a URL of the form

```
.../services/truststore/certificate/certificate-1
```

the vCloud Director API for NSX prepends the edge URL (*id*) and a colon to the NSX object identifier, as shown in this example:

```
.../services/truststore/certificate/id:certificate-1
```

Table 4-1. Summary of NSX Certificate Management Requests

Operation	Request	Request Body	Response
Create a certificate for the edge with identifier *id*.	POST *API-URL*/services/truststore/certificate/*id*	`trustObject`	201 Created
Import a certificate or certificate chain against the certificate signing request with identifier `csr-#` .	POST *API-URL*/services/truststore/certificate/csr-*#*	`trustObject`	204 No Content
Retrieve all certificates for the edge with identifier *id*.	GET *API-URL*/services/truststore/certificate/scope/*id*	None	`certificates`
Retrieve the certificate with identifier `certificate-#` from the edge with identifier *id*.	GET *API-URL*/services/truststore/certificate/*id*:certificate-*#*	None	`certificate`
Delete the certificate with identifier certificate-*#* from the edge with identifier *id*.	DELETE *API-URL*/services/truststore/certificate/*id*:certificate-*#*	None	204 No Content
Create a certificate signing request for the edge with identifier *id*.	POST *API-URL*/services/truststore/csr/*id*	`csr`	201 Created
Retrieve all certificate signing requests for the edge with identifier *id*.	GET *API-URL*/services/truststore/csr/scope/*id*	None	`csrs`
Retrieve the certificate signing request with identifier `csr-#` from the edge with identifier *id*.	GET *API-URL*/services/truststore/certificate/*id*:csr-*#*	None	`csr`
Delete the certificate signing request with identifier `csr-#` from the edge with identifier *id*.	DELETE *API-URL*/services/truststore/certificate/*id*:csr-*#*	None	204 No Content
Create a certificate revocation list for the edge with identifier *id*.	POST *API-URL*/services/truststore/crl/*id*	`trustObject`	204 No Content
Retrieve all certificate revocation lists for the edge with identifier *id*.	GET *API-URL*/services/truststore/crl/scope/*id*	None	`crls`
Retrieve the certificate revocation list with identifier `crl-#` from the edge with identifier *id*.	GET *API-URL*/services/truststore/certificate/*id*:crl-*#*	None	`crl`
Delete the certificate revocation list with identifier `crl-#` from the edge with identifier *id*.	DELETE *API-URL*/services/truststore/certificate/*id*:crl-*#*	None	204 No Content

Applications and Application Groups

NSX application and application group requests provide the capability for defining sets and groups of certain entities, which you can then use when specifying other network-related configurations, such as in firewall rules.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 4-2. Summary of NSX Application and Application Group Requests

Operation	Request	Request Body	Response
Retrieve all application groups defined in the organization VDC with identifier *id*.	GET *API-URL*/services/applicationgroup/scope/*id*	None	`list`
Retrieve the application group with identifier `application-group-`*#* defined in the organization VDC with identifier *id*.	GET *API-URL*/services/application/*id*:application-group-*#*	None	`applicationGroup`
Retrieve all applications defined in the organization VDC with identifier *id*.	GET *API-URL*/services/application/scope/*id*	None	`list`
Retrieve the application with identifier `application-`*#* defined in the organization VDC with identifier *id*.	GET *API-URL*/services/application/*id*:application-*#*	None	`application`

Security Groups

A security group is a collection of assets or grouping objects from your VMware Cloud Director inventory

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 4-3. Summary of NSX Security Group Requests

Operation	Request	Request Body	Response
Retrieve all security groups defined in the organization VDC with identifier *id*.	GET *API-URL*/services/securitygroup/scope/*id*	None	`list`
Retrieve the security group with identifier *id*:securitygroup-# .	GET *API-URL*/services/securitygroup/*id*:securitygroup-#	None	`securityGroup`
Create a new security group in the organization VDC with identifier *id*:securitygroup-# . The group has no membership information specified.	POST *API-URL*/services/securitygroup/*id*:securitygroup-#	`securitygroup`	200 OK
Update the security group with identifier *id*:securitygroup-# . The update specifies no membership information.	PUT *API-URL*/services/securitygroup/*id*:securitygroup-#	`securitygroup`	
Delete the security group with identifier *id*:securitygroup-# .	DELETE *API-URL*/services/securitygroup/*id*:securitygroup-#	None	204 No Content
Create a new security group in the organization VDC with identifier *id*. The group includes membership information.	POST *API-URL*/network/services/securitygroup/bulk/*id*	`securitygroup`	200 OK
Add members to the security group with identifier *id*:securitygroup-# .	PUT *API-URL*/network/services/securitygroup/bulk/*id*:securitygroup-#	`securitygroup`	
Add member with identifier # to the security group with identifier *id*:securitygroup-# .	PUT *API-URL*/network/services/securitygroup/# /members/ #	None	
Delete member with identifier # from the security group with identifier *id*:securitygroup-# .	DELETE *API-URL*/network/services/securitygroup/*id*:securitygroup-# /members/ #	None	204 No Content

Security Tags

You can use the VMware Cloud Director API for NSX to manage NSX security tags and their virtual machine assignments. For example, you can create a user-defined security tag, assign

tags to a virtual machine, view tags assigned to virtual machines, and view virtual machines that have a specific tag assigned.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

Table 4-4. Summary of NSX Security Tag Requests

Operation	Request	Request Body	Response
Retrieve all security tags defined in the organization VDC with identifier *id*.	GET *API-URL*/services/securitytags/*id*/tag/	None	`list`
Retrieve all security tags with tag id *id*:securitytag-*#* defined in the organization VDC with identifier *id*.	GET *API-URL*/services/securitytags/*id*/tag/*id*:securitytag-*#*	None	`list`
Create a security tag in the organization VDC with identifier *id*.	POST *API-URL*/network/services/securitytags/*id*/tag	`securityTag`	200 OK
Delete the security tag with tag id *id*:securitytag-*#* defined in the organization VDC with identifier *id*.	DELETE *API-URL*/network/services/securitytags/*id*/tag/*id*:securitytag-*#*	None	204 No Content
Retrieve the list of VMs in the organization VDC with identifier *id* that have the security tag with tag id *id*:securitytag-*#* attached.	GET *API-URL*/network/services/securitytags/*id*/tag/vm/*id*:securitytag-*#*		
(Requires NSX 6.3.)	POST *API-URL*/network/services/securitytags/*id*/vm/*id*:securitytag-*#*		
(Requires NSX 6.3.)	DELETE *API-URL*/network/services/securitytags/*id*/vm/*id*:securitytag-*#*		204 No Content

Grouping Objects

You can use the VMware Cloud Director API for NSX to create and manage IP address groups and MAC address groups in an organization virtual data center.

- *API-URL* is a URL of the form `https://vcloud.example.com/network`.
- *id* is a VMware Cloud Director unique identifier in the form of a UUID, as defined by RFC 4122.
- *#* is a small integer used in an NSX object identifier.

See Get an IP Set in an Organization VDC.

Table 4-5. Summary of NSX IP and MAC Sets Requests

Operation	Request	Request Body	Response
Create an IP set in the organization VDC with identifier *id*.	POST *API-URL*/services/ipset/*id*	`ipset`	None
Retrieve all IP sets defined in the organization VDC with identifier *id*.	GET *API-URL*/services/ipset/scope/*id*	None	`list`
Get the IP set with identifier # defined in the organization VDC with identifier *id*.	GET *API-URL*/services/ipset/*id*:ipset-*#*	None	`ipset`
Update the IP set with identifier # defined in the organization VDC with identifier *id*.	PUT *API-URL*/services/ipset/*id*:ipset-*#*	`ipset`	None
Delete the IP set with identifier # defined in the organization VDC with identifier *id*.	DELETE *API-URL*/services/ipset/*id*:ipset-*#*	None	None
Create a MAC set in the organization VDC with identifier *id*.	POST *API-URL*/services/macset/*id*	`macset`	None
Retrieve all MAC sets defined in the organization VDC with identifier *id*.	GET *API-URL*/services/macset/scope/*id*	None	`list`
Get the MAC set with identifier # defined in the organization VDC with identifier *id*.	GET *API-URL*/services/macset/*id*:macset-*#*	None	`macset`
Update the MAC set with identifier # defined in the organization VDC with identifier *id*.	PUT *API-URL*/services/macset/*id*:macset-*#*	`macset`	None
Delete the MAC set with identifier # defined in the organization VDC with identifier *id*.	DELETE *API-URL*/services/macset/*id*:macset-*#*	None	None

Example: Get an IP Set in an Organization VDC

To get the IP set with identifier *2* defined in the organization VDC with identifier *78229ccd-2bf2-466d-8444-03d0bb46caaf*, use the following request:

```
GET https://vcloud.example.com/network/services/ipset/
78229ccd-2bf2-466d-8444-03d0bb46caaf:ipset-2
```