OnApp Cloud 6.4 Edge 1 vCenter Implementation Guide
Table of Contents

1.1 Technical Details And Requirements ................................................. 6
  1.1.1 vCenter Cloud Requirements .................................................. 6
  1.1.2 Networking .............................................................................. 7
  1.1.3 Supported Functionality ........................................................... 7
  1.1.4 OnApp Hardware Requirements ............................................... 10
  1.1.5 Implementation Details ........................................................... 11
1.2 Installation And Upgrade .................................................................. 12
  1.2.1 vCenter Installation ................................................................. 12
  1.2.2 Install Control Panel Server .................................................... 13
2.1 Control Panel Configuration ............................................................... 20
2.2 Create vCenter Compute Resource .................................................... 21
2.3 Edit vCenter Compute Resource ...................................................... 22
  2.3.1 Edit details of vCenter compute resource ................................. 22
  2.3.2 Manage vCenter compute resource data stores ......................... 23
2.4 Create vCenter Compute Zone ......................................................... 24
2.5 Manual IP Nets .............................................................................. 24
  2.5.1 View Manual IP Nets ............................................................... 25
  2.5.2 Delete Manual IP Net ............................................................... 25
2.6 Import vCenter Virtual Server ......................................................... 25
  2.6.1 Manual Import of vCenter VS ................................................. 26
  2.6.2 Resync vCenter VS ................................................................. 26
  2.6.3 Auto Import of vCenter VS .................................................... 27
  2.6.4 View Auto Import Rules ......................................................... 27
  2.6.5 Create Auto Import Rule ......................................................... 28
  2.6.6 Run Auto Import Rule ............................................................ 28
  2.6.7 Edit Auto Import Rule ............................................................ 28
  2.6.8 Delete Auto Import Rule ......................................................... 29
2.7 vCenter Virtual Servers ................................................................... 29
  2.7.1 Create vCenter Virtual Server .................................................. 31
  2.7.2 vCenter Virtual Server Wizard Beta ........................................ 36
  2.7.3 View vCenter Virtual Server Details ........................................ 48
  2.7.4 Edit vCenter Virtual Server ..................................................... 49
  2.7.5 Delete vCenter Virtual Server ................................................ 50
  2.7.6 Build vCenter Virtual Server Manually ................................... 50
  2.7.7 Clone vCenter Virtual Server .................................................. 51
  2.7.8 Migrate from vCenter to KVM .................................................. 51
  2.7.9 vCenter Virtual Server Power Options .................................... 54
  2.7.10 vCenter Virtual Server Administrative Options ..................... 55
  2.7.11 vCenter Virtual Server Transactions and Logs ....................... 55
  2.7.12 vCenter Virtual Server Networks .......................................... 56
  2.7.13 vCenter Virtual Server Disks .................................................. 58
  2.7.14 vCenter Virtual Server Statistics .......................................... 61
  2.7.15 Manage vCenter Virtual Server Recipes ............................... 63
  2.7.16 Manage vCenter Virtual Server Custom Variables ................. 64
  2.7.17 Manage Virtual Server Snapshots ........................................... 65
  2.7.18 vCenter Virtual Server Console ............................................. 65
2.8 OnApp OVA Import to vCenter ......................................................... 65
  2.8.1 Upload OVA ............................................................................ 66
  2.8.2 Convert OVA .......................................................................... 67
2.9 Import vCenter Templates ............................................................... 68
  2.9.1 Update template ..................................................................... 68
  2.9.2 Add template to Template Store ............................................. 68
2.10 Manage vCenter Templates ............................................................ 69
  2.10.1 Manage vCenter Template System Service Add-ons ............... 69
  2.10.2 Manage vCenter Template Recipes ....................................... 70
  2.10.3 Delete Recipe ........................................................................ 71
2.11 NSX Integration ............................................................................. 71
  2.11.1 NSX Managers in OnApp ........................................................ 72
  2.11.2 NSX Firewalls ........................................................................ 74
  2.11.3 NAT Rules for NSX Integration .............................................. 80
  2.11.4 NSX Load Balancers ............................................................... 84
  2.11.5 NSX IPSec VPN ................................................................. 95
2.11.6 NSX L2 VPN ................................................................. 102
2.12 Create and Manage vCenter Resource Pools ......................................................... 107
2.12.1 View vCenter Resource Pool ................................................................................. 107
2.12.2 Create vCenter Resource Pool .............................................................................. 108
2.12.3 Edit vCenter Resource Pool .................................................................................. 108
2.12.4 Delete vCenter Resource Pool ............................................................................... 108
2.13 vCenter Servers ........................................................................................................ 109
2.13.1 Edit vCenter Server Details .................................................................................. 109
2.13.2 Delete vCenter Server .......................................................................................... 110
2.14 vCenter Permissions .................................................................................................. 110
2.14.1 Default Permissions for vCenter User Role ............................................................ 110
2.14.2 Other vCenter Permissions ................................................................................... 111
3.1 Create vCenter Virtual Servers .................................................................................. 117
3.1.1 Step 1 of 6. Cloud Locations .................................................................................. 117
3.1.2 Step 2 of 6. Templates ......................................................................................... 118
3.1.3 Step 3 of 6. Properties ........................................................................................... 119
3.1.4 Step 4 of 6. Resources .......................................................................................... 120
3.1.5 Step 5 of 6. Recipes or Service Add-ons ................................................................. 121
3.1.6 Step 6. Confirmation ............................................................................................... 122
3.2 vCenter Virtual Server Beta Wizard ......................................................................... 123
3.2.1 Create Custom vCenter Virtual Servers Beta ......................................................... 124
3.2.2 Create Instance Package vCenter Virtual Servers Beta ........................................ 129
3.3 View vCenter Virtual Servers Details ..................................................................... 134
3.3.1 VS Properties ....................................................................................................... 134
3.3.2 Notes .................................................................................................................... 135
3.3.3 VS Management ................................................................................................. 135
3.4 Edit vCenter Virtual Servers ..................................................................................... 135
3.5 Delete vCenter Virtual Servers .................................................................................. 136
3.6 Build vCenter Virtual Servers Manually ................................................................... 136
3.7 Clone vCenter Virtual Servers .................................................................................. 137
3.8 Auto Import vCenter Virtual Server ......................................................................... 137
3.8.1 View Auto Import Rules ....................................................................................... 138
3.8.2 Create Auto Import Rule ....................................................................................... 138
3.8.3 Run Auto Import Rule ........................................................................................... 139
3.8.4 Edit Auto Import Rule ........................................................................................... 139
3.8.5 Delete Auto Import Rule ....................................................................................... 140
3.9 vCenter Virtual Servers Power Options ................................................................... 140
3.10 vCenter Virtual Servers Console ............................................................................ 140
3.11 vCenter Virtual Servers Transactions and Logs ....................................................... 141
3.12 vCenter Virtual Servers Networks ........................................................................ 141
3.12.1 Configure vCenter Virtual Servers Network Interface ....................................... 141
3.12.2 Rebuild vCenter Virtual Servers Network ............................................................ 142
3.12.3 Allocate/Remove vCenter Virtual Servers IP Addresses ...................................... 143
3.12.4 Display Network Speed for Network Interfaces on vCenter Virtual Servers Page ... 143
3.12.5 Edit vCenter Virtual Servers Network Speed ....................................................... 144
3.13 vCenter Virtual Servers Disks .................................................................................. 144
3.13.1 Edit vCenter Virtual Servers Disks ....................................................................... 144
3.13.2 Migrate vCenter Virtual Servers Disks .................................................................. 144
3.13.3 Delete vCenter Virtual Servers Disks ................................................................... 145
3.13.4 Add Disks to vCenter Virtual Server .................................................................... 145
3.14 vCenter Virtual Servers Statistics ........................................................................... 146
3.14.1 vCenter Virtual Servers CPU Utilization .............................................................. 146
3.14.2 vCenter Virtual Servers Billing Statistics .............................................................. 147
3.14.3 vCenter Virtual Servers Network Interface Statistics .......................................... 148
3.14.4 vCenter Virtual Servers Disk IOPS ...................................................................... 148
3.15 Manage vCenter Virtual Servers Recipes ................................................................ 148
3.16 Manage vCenter Virtual Servers Custom Variables .............................................. 150
3.17 VMware Virtual Servers Snapshots ......................................................................... 150
3.18 vCenter VS Console ................................................................................................. 151
3.19 vCenter Resource Pools ........................................................................................... 151
3.19.1 View vCenter Resource Pool ................................................................................. 152
3.19.2 Create vCenter Resource Pool ............................................................................. 152
3.19.3 Edit vCenter Resource Pool .................................................................................. 153
3.19.4 Delete vCenter Resource Pool ............................................................................ 153
4.1 Import vCenter VS ................................................................. 154
4.2 Resync vCenter VS ................................................................. 154
4.3 Auto Import Rules ................................................................. 158
  4.3.1 Get List of Auto Import Rules ......................................... 159
  4.3.2 Add Auto Import Rule ..................................................... 159
  4.3.3 Run Auto Import Rule .................................................... 160
  4.3.4 Edit Auto Import Rule ................................................... 161
  4.3.5 Delete Auto Import Rule ............................................... 161
4.4 Add vCenter VS ................................................................. 162
4.5 Clone vCenter VS ................................................................. 165
4.6 Add vCenter Compute Zone .................................................. 165
4.7 Add vCenter Compute Resources .......................................... 168
4.8 Edit vCenter Compute Resources ......................................... 169
4.9 vCenter Templates API ........................................................ 170
  4.9.1 Get List of vCenter Templates ........................................ 170
  4.9.2 Update vCenter Template .............................................. 172
4.10 NSX Integration API .......................................................... 173
  4.10.1 NSX Firewalls API ......................................................... 173
  4.10.2 NSX NAT API ............................................................. 181
  4.10.3 NSX Load Balancers API ................................................ 188
  4.10.4 NSX Managers API ....................................................... 217
  4.10.5 NSX IPSec VPN API ....................................................... 221
  4.10.6 NSX L2 VPN API ........................................................ 234
4.11 vCenter Resource Pool API ................................................ 244
  4.11.1 Get List of Resource Pools ............................................ 244
  4.11.2 Add vCenter Resource Pool .......................................... 245
  4.11.3 Edit vCenter Resource Pool ......................................... 246
  4.11.4 Delete vCenter Resource Pool ....................................... 247
4.12 vCenter Servers API .......................................................... 247
  4.12.1 Get List of vCenter Servers ......................................... 247
  4.12.2 Add vCenter Server ..................................................... 249
  4.12.3 Edit vCenter Server ................................................... 249
  4.12.4 Delete vCenter Server ................................................ 250
vCenter integration functionality is currently in beta.

This guide provides the info on how you can integrate vCenter into OnApp. VMware vCenter is a virtualization technology available for integration into OnApp. Use of the VMware vSphere 5 virtualization platform allows you to build a virtualized cloud infrastructure utilizing the highest standards of reliability and performance.

OnApp Cloud integration allows you to run and manage VMware ESXi compute resources alongside with Xen and KVM compute resources using the OnApp Control Panel.

In OnApp all the ESXi compute resources are displayed as a single combined compute resource with a sum of the CPU, RAM and Disk resources rather than individual compute resources.

The following diagram shows how the integration works:
1 Get Started

OnApp provides support for vCenter 6.7 starting from OnApp 6.0 Patch 3 (6.0.0-98).

OnApp Cloud integration allows you to run and manage VMware ESXi compute resources alongside with Xen and KVM compute resources using the OnApp Control Panel. In OnApp, all the ESXi compute resources are displayed as a single combined compute resource with a sum of the CPU, RAM, and Disk resources rather than individual compute resources.

The following diagram shows how the integration works:

This guide contains the information on how to configure your vCenter and OnApp integration. Refer to one of the following sections for details:

- Install Control Panel Server
- vCenter Installation

For information on how to manage vCenter related resources in OnApp UI, refer to the Administration or the User guide. For information on how to manage vCenter related resources via OnApp API, refer to the API guide.

1.1 Technical Details And Requirements

This chapter provides information on software and hardware requirements for OnApp to integrate with VMware vCenter. You may also find the information on architecture and networking models.

1.1.1 vCenter Cloud Requirements

If you are looking to run VMware ESXi servers through OnApp, then you will require an external installation of vCenter. These can be installed on virtual servers, if necessary, but should not be hosted inside OnApp.

The OnApp Control Panel server communicates with vCenter over the OnApp management network.

The following are the requirements for VMware integration with OnApp Control Panel:

- vCenter ESXi hosts must be organized into Clusters.
OnApp can only deploy and manage vCenter VSs connected to a dvPortGroup. All hosts in your cluster(s) must be connected to a DvSwitch or vSwitch.

Since VSS networks cannot be managed on OnApp side, it will not be possible to configure traffic shaping for them, so the Port speed field at the Edit NIC page and the Resources step of the VS Creation wizard will be disabled.

At least one data store on the ESXi hosts is required for the virtual server provisioning. Make sure that this data store is accessible to all ESXi hosts in a Cluster. NOTE: The data store name will be used on the Control Panel.

Ensure that the OnApp Control Panel server has admin access to vCenter and all of the ESXi hosts.

1.1.2 Networking

The OnApp Control Panel server communicates with vCenter over the OnApp management network. Below you can find a scheme, which shows network creation workflow in OnApp and in vCenter.

The following network mapping shows dependencies between vCenter and OnApp network components:

<table>
<thead>
<tr>
<th>vCenter</th>
<th>equals</th>
<th>OnApp</th>
</tr>
</thead>
<tbody>
<tr>
<td>dvPortGroup</td>
<td>Equals</td>
<td>Network Label</td>
</tr>
<tr>
<td>dvPortGroup VLAN</td>
<td>Equals</td>
<td>Network VLAN</td>
</tr>
<tr>
<td>dvPortGroup Name</td>
<td>Equals</td>
<td>Network Network</td>
</tr>
<tr>
<td>&lt;Nothing Here&gt;</td>
<td></td>
<td>Network IP Addresses</td>
</tr>
<tr>
<td>dvPortGroup MoRef</td>
<td></td>
<td>Network vCenter Identifier</td>
</tr>
</tbody>
</table>
1.1.2.1 Requirements
There is a set of requirements for managing vCenter networks, network zones and compute resources in OnApp Control Panel. Follow the requirements listed below to ensure the proper operation of your vCenter.

If you don't meet the requirements listed in this document, you won't be able to upgrade to OnApp 5.8. The upgrade will not be performed if any of the following network issues are detected in your vCenter.

1.1.2.1.1 Network Requirements
The following requirements are applicable to managing vCenter networks in OnApp CP:

- The network cannot be attached to a compute zone if this zone has more than one compute resource and one of them is vCenter-based.
- The network can be attached only to one vCenter compute resource.
- The network cannot be shared between vCenter compute resources.
- If any network in OnApp is already attached to a compute resource, it cannot be attached to a vCenter compute resource.

1.1.2.1.2 Network Zone Requirements
The following network zone requirements are applicable to vCenter:

- In one network zone, you can have networks that are assigned to vCenter and networks that are assigned to Xen/KVM compute resources.
- vCenter networks are imported into one network zone and you can move them to different zones.
1.1.2.1.3 Compute Resource Requirements
The following compute resource requirements are related to vCenter networks:

- The vCenter compute resource cannot be assigned to a compute zone if this zone already has any compute resources and attached networks.
- The compute resource that does not belong to vCenter cannot be assigned to a compute zone if this compute zone has vCenter compute resource and attached networks.

1.1.3 Supported Functionality
Here is the list of the current vCenter functions you can perform by means of OnApp Control Panel:

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Supported Actions</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Servers</td>
<td>view</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>import</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>create</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>edit</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>build manually</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>reboot</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>suspend</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>shut down</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>startup</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>rebuild network</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>change owner</td>
<td>5.5 and up</td>
</tr>
<tr>
<td></td>
<td>use VS console</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>back up by Veeam</td>
<td>5.9 and up</td>
</tr>
<tr>
<td></td>
<td>plugin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>migrate to KVM</td>
<td>5.10 and up</td>
</tr>
<tr>
<td>VS Disks</td>
<td>add</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>edit</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>migrate</td>
<td>5.4 and up</td>
</tr>
<tr>
<td>VS Network Interface</td>
<td>view</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>add</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>view network speed</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>edit network speed</td>
<td>5.4 and up</td>
</tr>
<tr>
<td>VS IP Addresses</td>
<td>allocate</td>
<td>5.4 and up</td>
</tr>
<tr>
<td>Functionality</td>
<td>Supported Actions</td>
<td>Version</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>VS Monitoring</td>
<td>remove</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>view CPU statistics</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>view billing statistics</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>view network interface statistics</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>view disk statistics</td>
<td>5.4 and up</td>
</tr>
<tr>
<td>VS Recipes</td>
<td>view</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>assign</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>remove</td>
<td>5.4 and up</td>
</tr>
<tr>
<td>VS Recipe Custom Variables</td>
<td>view</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>create</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>edit</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>5.4 and up</td>
</tr>
<tr>
<td>VS Snapshots</td>
<td>view</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>create</td>
<td>5.4 and up</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>5.4 and up</td>
</tr>
<tr>
<td>VS Templates</td>
<td>create</td>
<td>5.4 and up</td>
</tr>
<tr>
<td>OVA</td>
<td>upload</td>
<td>5.4 and up</td>
</tr>
</tbody>
</table>

**1.1.4 OnApp Hardware Requirements**

To integrate OnApp with vCenter you’ll need to configure an environment according to the following hardware requirements in order to host the OnApp platform:

- **Control Panel Server**

To use OnApp for vCenter you need to deploy a Control Panel server on which the OnApp software will be installed on.

You simply need to deploy an OnApp Control Panel Server with the following specs:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>4-8 Cores</td>
<td>8-16 Cores</td>
</tr>
<tr>
<td>Memory</td>
<td>16GB</td>
<td>32GB</td>
</tr>
<tr>
<td>Disk</td>
<td>100GB</td>
<td>250GB</td>
</tr>
<tr>
<td>Network Adapters</td>
<td>Dual port 1Gbps</td>
<td>Dual port 1Gbps</td>
</tr>
<tr>
<td>OS</td>
<td>CentOS 6 x64</td>
<td>CentOS 7 x64</td>
</tr>
</tbody>
</table>

- **Template Server (optional)**
If you wish to build a central template repo you need to deploy an additional template server, with the following specs:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2-4 Cores</td>
<td>4-8 Cores</td>
</tr>
<tr>
<td>Memory</td>
<td>8GB</td>
<td>16GB</td>
</tr>
<tr>
<td>Disk</td>
<td>100GB</td>
<td>250GB</td>
</tr>
<tr>
<td>Network Adapters</td>
<td>Dual port 1Gbps</td>
<td>Dual port 1Gbps</td>
</tr>
</tbody>
</table>

- **Network**

The diagram below shows an example of how you should set up your OnApp for vCenter integration:

1.1.5 Implementation Details

This diagram shows the relationship between OnApp and vCenter:
At the moment the following components are synchronized between vCenter and OnApp:

- Networks
- Data stores
- Compute resource changes
- Certain VS changes (amount of CPU, RAM, etc.)

Below you can find the compatibility matrix for vCenter and OnApp versions:

<table>
<thead>
<tr>
<th>Versions</th>
<th>vCenter 5.5</th>
<th>vCenter 6.0</th>
<th>vCenter 6.5</th>
<th>vCenter 6.7</th>
<th>vCenter 7.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnApp 6.3</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OnApp 6.2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>OnApp 6.1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OnApp 6.0</td>
<td>✓**</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓*</td>
</tr>
</tbody>
</table>

*Starting from the OnApp 6.0.0-98 update.
**OnApp 6.0.0-283 update is the last update that supports vCenter 5.5 in OnApp 6.0.

1.2 Installation And Upgrade

This chapter covers the topics on installation procedure and upgrade, as well as the changes in the OnApp Control Panel.

1.2.1 vCenter Installation

There is a set of requirements to vCenter networks, network zones and compute resources in OnApp Control Panel. If you don’t meet the requirements listed in the linked document, you won’t be able to upgrade to OnApp 6.0. The upgrade will not be performed if any of the network issues are detected in your vCenter.
Follow these guidelines to install and configure VMware vCenter:

- Install the VMware vCenter server by following VMware documentation instructions.
- Create an administrator account on the vCenter server or use the default administrator account.
- Create a new Datacenter.
- Create a new Cluster and keep DRS enabled.
- Install and add ESXi hosts to the Cluster.
- Create a vSphere Distributed Switch and add the ESXi hosts to the switch.
- Add a data store that is accessible to all ESXi hosts in the Cluster.
- Make sure the vCenter/ESXi TCP 443 port is open for incoming connections from the OnApp Control Panel.
- Use NTP for all environments for correct time synchronization.

### 1.2.2 Install Control Panel Server

- Use corresponding option of the Control Panel installer in case MySQL is already installed and configured.
- Installer output is redirected to ./onapp-cp-install.log
- All installer critical errors are in /var/log/messages
- This instruction is applicable for installing OnApp 6.0 Patch 2

To install Control Panel server, perform the following procedure:

1. Update your server:
   ```
   # yum update
   ```

2. Download OnApp YUM repository file:
   ```
   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-6.2.noarch.rpm
   ```

3. Install OnApp Control Panel installer package:
   ```
   #> yum install onapp-cp-install
   ```

4. *(Optional)* You can optionally apply the Control Panel custom configuration. It is important to set the custom values before the installer script runs.
   
   **Edit the /onapp/onapp-cp.conf file to set Control Panel custom values**
# Template server URL

```
TEMPLATE_SERVER_URL='http://templates-manager.onapp.com/
```

# IPs (separated with coma) list for the snmp to trap

```
SNMP_TRAP_IPS=
```

# OnApp Control Panel custom version

```
ONAPP_VERSION=
```

# OnApp MySQL/MariaDB connection data (database.yml)

```
ONAPP_CONN_WAIT_TIMEOUT=15
ONAPP_CONN_POOL=30
ONAPP_CONN_RECONNECT='true'
ONAPP_CONN_ENCODING='utf8'
ONAPP_CONN_SOCKET='/var/lib/mysql/mysql.sock'
```

# MySQL/MariaDB server configuration data (in case of local server)

```
MYSQL_WAIT_TIMEOUT=604800
MYSQL_MAX_CONNECTIONS=500
MYSQL_PORT=3306
```

# Use MariaDB instead of MySQL as OnApp database server

```
WITH_MARIADB=0
```

# Configure the database server relative amount of available RAM

```
TUNE_DB_SERVER=0
```

# The number of C data structures that can be allocated before triggering the garbage collector. It defaults to 8 million

```
RUBY_GC_MALLOC_LIMIT=16000000
```

# sysctl.conf net.core.somaxconn value

```
NET_CORE_SOMAXCONN=2048
```
# The root of OnApp database dump directory (on the Control Panel box)

    ONAPP_DB_DUMP_ROOT=

# Remote server's (to store database dumps) IP, user, path, openssh connection options and number of dumps to keep

    DB_DUMP_SERVER=
    DB_DUMP_USER=root
    DB_DUMP_SERVER_ROOT=/onapp/backups
    DB_DUMP_SERVER_SSH_OPT="-o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -o PasswordAuthentication=no"
    KEEP_DUMPS=168
    DB_DUMP_CRON='40 * * * *'

# Enable monit - tool for managing and monitoring Unix systems

    ENABLE_MONIT=1

# If enabled (the 1 value is set) - install (if local box) and configures RabbitMQ Server (messaging system) for the vCloud support.

    ENABLE_RABBITMQ=1

# Rotate transactions' log files created more than TRANS_LOGS_ROTATE_TIME day(s) ago

    TRANS_LOGS_ROTATE_TIME=30

# Maximum allowed for uploading file size in bytes, from 0 (meaning unlimited) to 2147483647 (2GB). Default is 0.

    MAX_UPLOAD_SIZE=1073741824

# Timeout before ping Redis Server to check if it is started. Default is 5 sec.

    REDIS_PING_TIMEOUT=5

# OnApp Control Panel SSL certificates (please do not change if you aren't familiar with SSL certificates)
# * The data below to generate self-signed PEM-encoded X.509 certificate

    SSL_CERT_COUNTRY_NAME=UK
    SSL_CERT_ORGANIZATION_NAME='OnApp Limited'
    SSL_CERT_ORGANIZATION_ALUNITNAME='OnApp Cloud'
    SSL_CERT_COMMON_NAME=`hostname --fqdn 2>/dev/null`
# SSLCertificateFile, SSLCertificateKeyFile Apache directives' values
# ssl_certificate, ssl_certificate_key Nginx directives' values

SSLCERTIFICATEFILE=/etc/pki/tls/certs/ca.crt
SSLCERTIFICATECSRFILE=/etc/pki/tls/private/ca.csr
SSLCERTIFICATEKEYFILE=/etc/pki/tls/private/ca.key

# * PEM-encoded CA Certificate (if custom one exists)
# SSLCACertificateFile, SSLCertificateChainFile Apache directives' values
# ssl_client_certificate Nginx directives' values

SSLCACERTIFICATEFILE=
SSLCERTIFICATECHAINFILE=

# SSLCipherSuite, SSLProtocol Apache directives' values
# ssl_ciphers, ssl_protocols Nginx directives' values

SSLCIPHERSUITE=
SSLPROTOCOL=

# vi /onapp/onapp-cp.conf

---

5. Run the Control Panel installer:

`#/onapp/onapp-cp-install/onapp-cp-install.sh -i SNMP_TRAP_IPS`

---

The full list of Control Panel installer options:

Usage:

```
```

Where:
### Usage:

```
```

#### MYSQL_ *

Options are useful if MySQL is already installed and configured.

- `-m` **MYSQL_HOST**
  - MySQL host

- `-p` **MYSQL_PASSWD**
  - MySQL password

- `-d` **MYSQL_DB**
  - OnApp MySQL database name

- `-u` **MYSQL_USER**
  - MySQL user

#### REDIS_*

Options are useful if Redis Server is already installed and configured.

- `--redis-host=REDIS_HOST`
  - IP address/FQDN where Redis Server runs. The Redis Server will be installed and configured on the current box if localhost/127.0.0.1 or box's public IP address (listed in SNMP_TRAP_IPS) is specified. If local Redis, it will serve as well on the unix socket '/tmp/redis.sock'. Default value is 127.0.0.1.

- `--redis-port=REDIS_PORT`
  - Redis Server listen port. Defaults are:
    - 0 - if local server
    - 6379 - if remote server

- `--redis-passwd=[=REDIS_PASSWD]`
  - Redis Server password to authenticate. Random password is generated if the option's argument isn't specified. By default no password is used for local Redis.

- `--redis-sock=REDIS_PATH`
  - Path to the Redis Server's socket. Used if local server only. Default is /tmp/redis.sock

#### ADMIN_*

Options are used to configure OnApp Control Panel administrator data. Please note, that these options are for NEW INSTALL only and not for upgrade.

- `-P` **ADMIN_PASSWD**
  - CP administrator password

- `-F` **ADMIN_FIRSTNAME**
  - CP administrator first name
Usage:

```
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-L ADMIN_LASTNAME</td>
<td>CP administrator last name</td>
</tr>
<tr>
<td>-E ADMIN_EMAIL</td>
<td>CP administrator e-mail</td>
</tr>
<tr>
<td>--rbhost RBT_HOST</td>
<td>IP address/FQDN where RabbitMQ Server runs.</td>
</tr>
<tr>
<td></td>
<td>The RabbitMQ will be installed and configured on the current box if localhost/127.0.0.1 or box's public IP address (enlisted in SNMP_TRAP_IPS) Default values are 127.0.0.1.</td>
</tr>
<tr>
<td>VCD_*</td>
<td>Options are usefull if vCloud/RabbitMQ are already installed and configured.</td>
</tr>
<tr>
<td>--vcdlogin VCD_LOGIN</td>
<td>RabbitMQ/vCloud user. Default value is 'rbtvcdd'.</td>
</tr>
<tr>
<td>--vcdpasswd VCD_PASSWD</td>
<td>RabbitMQ/vCloud user password. The random password is generated if isn't specified.</td>
</tr>
<tr>
<td>--vcdvhost VCD_VHOST</td>
<td>RabbitMQ/vCloud vhost. Default value is '/'</td>
</tr>
<tr>
<td>RBT_*</td>
<td>Options are used to configure RabbitMQ manager account.</td>
</tr>
<tr>
<td>--rbltlogin RBT_LOGIN</td>
<td>RabbitMQ manager login. The default value is 'rbtmgr'.</td>
</tr>
<tr>
<td>--rbtpassword RBT_PASSWD</td>
<td>RabbitMQ manager password. The random password is generated if isn't specified.</td>
</tr>
<tr>
<td>-v ONAPP_VERSION</td>
<td>Install custom OnApp CP version</td>
</tr>
<tr>
<td>-i SNMP_TRAP_IPS</td>
<td>IP addresses separated with coma for snmp to trap</td>
</tr>
<tr>
<td>-c CONFIG_FILE</td>
<td>Custom installer configuration file. Otherwise, preinstalled one is used.</td>
</tr>
<tr>
<td>-y</td>
<td>update OS packages (except of OnApp provided) on the box with 'yum update'.</td>
</tr>
<tr>
<td>-a</td>
<td>do not be interactive. Process with automatic installation.</td>
</tr>
<tr>
<td>-D</td>
<td>do not make database dump, and make sure it is disabled in the cron and not running at the moment</td>
</tr>
</tbody>
</table>
Usage:

```
```

-h  print this info

6. *(Optional)* Install CloudBoot dependencies:

```
#> yum install onapp-store-install
#> /onapp/onapp-store-install/onapp-store-install.sh
```

7. Install OnApp license to activate the Control Panel. Enter a valid license key via the Web UI (you'll be prompted to do so). Your default OnApp login is *admin/changeme*. The password can be changed via the Control Panel > *Cloud* > *Groups* menu in the Control Panel.

Once you have entered a license it can take up to 15 minutes to activate.

8. Restart the OnApp service:

```
#> service onapp restart
```
2 Administration Guide

This guide contains information on how administrators can manage vCenter related resources via OnApp UI. Refer to one of the following sections for detailed information:

- Control Panel Configuration
- Import vCenter Templates
- Manage vCenter Templates
- vCenter OVA Upload to OnApp
- Create vCenter Compute Resource
- Edit vCenter Compute Resource
- Create vCenter Compute Zone
- Manual IP Nets
- Import vCenter Virtual Server
- vCenter Virtual Servers
- vCenter Virtual Server Recipes
- NSX Integration
- Create and Manage vCenter Resource Pools
- vCenter Servers
- vCenter Permissions

For information on the vCenter related functionality available to users with the default role 'user' in OnApp, refer to the User Guide.

For information on the API requests, you can use to manage vCenter related resources, refer to the API Guide.

2.1 Control Panel Configuration

Read the steps described in this section carefully to get a common notion of the VMware vCenter configuration within the OnApp cloud.

To configure VMware vCenter on Control Panel:

1. Create new vCenter compute resource in the compute resource settings. See the Create vCenter Compute Resource section for details how to do that. A transaction will be launched to import all networks and data stores:

   a. Go to your Control Panel > Settings > Compute Resources > click the label of the necessary vCenter compute resource to see its details.

   b. On the page that appears, click Tools > Manage Networks > click the label of the newly created network (dvPortGroup Name).

   c. Click the New IP Net button to add the correct IP net for that network.

   d. Fill in the details of the new IP net:

      ▪ Label - the name of the IP net
      ▪ Network address - the network address of the IP net
      ▪ Network mask - the network mask. Must be less or equal 32.
- Default gateway - the default gateway to be added to the IP net automatically
- Allow gateway to be outside from IP net - tick this checkbox to allow gateway to be outside from the IP net.
- Add default IP range - tick this checkbox for the default IP range to be added to the IP net automatically. Otherwise, you'll need to add the required IP ranges after the IP net is created.

e. Click Submit to finish.

f. If required, specify a custom IP range.

Click here to see the instruction on adding an IP range.

i. Go to Control Panel > Settings > Compute Resources > click the label of the necessary vCenter compute resource to see its details.

ii. On the page that appears, click Tools > Manage Networks > click the label of the newly created network (dvPortGroup Name).

iii. Click the Actions icon next to the required IP net and select Add New IP Range.

iv. Fill in the start and end address and the default gateway of the new IP range; if necessary, tick the Allow gateway to be outside from IP net checkbox to allow gateway to be outside from the IP net.

v. Click Add to save the new IP range.

The Add New IP Range button is not displayed if there are no IP addresses that can be added to the IP net.

b. Data stores Cluster (PODs) are created as individual zones with their Cluster Name in the zone Name

c. Data stores not in a cluster are created under a single zone

2. Create a VS template by following the instructions in the Create Template for vCenter Virtual Server chapter. Also, you can upload templates using OVA import.

3. Create a new vCenter virtual server or import VS from vCenter.

- To import a VS from vCenter successfully, make sure vCenter resources for compute, network and datastore zones are added in your bucket in the Virtual section.

- In order for a vCenter VS console to work, the system_host parameter in /onapp/interface/config/on_app.yml file must be changed from its default value onapp.com to an appropriate FQDN or IP address of the Control Panel server.

2.2 Create vCenter Compute Resource

To add a vCenter compute resource to OnApp:

1. Go to your Control Panel > Admin > Settings menu.
2. Click the **Compute Resources** icon.

3. Press "+" button or click the **Add New Compute Resource** button underneath the list of **compute** resources.

4. On the screen that appears:
   - **Label** - enter a **compute** resource label
   - **Compute Resource Type** - choose the **vcenter** compute resource type
   - **vCenter server** - select the necessary **vCenter server** from the dropbox
   - **Cluster** - select the necessary cluster assigned to the specified vCenter server from the dropbox
   - **Compute Zone** - the compute zone to which the compute resource is assigned

5. Click the **Save** button. The compute resource will be added to the system. You can view it under the **Compute Resources** menu. The transaction will be launched to import all networks and data stores.

6. Click the compute resource **label** > **Tools** > **Import from vCenter** if it is necessary to rerun the transaction that will import all networks and data stores.

7. Go to **Admin** > **Settings** > **Compute Zones** and **create a compute zone**.

8. Attach the vCenter compute resource to the compute zone by selecting the resource from the list of unassigned compute resources.

- The vCenter compute resource cannot be assigned to a compute zone if this zone already has any compute resources and attached networks.
- The compute resource that does not belong to vCenter cannot be assigned to a compute zone if this compute zone has vCenter compute resource and attached networks.

### 2.3 Edit vCenter Compute Resource

This page provides information on how to edit vCenter compute resources and how to manage their data store joins.

#### 2.3.1 Edit details of vCenter compute resource

To edit details of a vCenter compute resource:

1. Go to your Control Panel > **Admin** > **Settings** menu.
2. Click the **Compute Resources** icon.
3. Click the **Actions** button next to the vCenter compute resource you want to edit and then click **Edit**.
4. On the screen that follows, change details as required:
   - **Label** - enter a compute resource label
   - **Compute Resource Type** - choose the vCenter compute resource type
Operating System Type - the operating system type of the virtual servers that can live on this compute resource

CPU Units - adjust the slider to set the desired amount of CPU units for this compute resource

Enabled - whether the compute resource is enabled or not (compute resources that are not enabled cannot be used to host VSs)

Collect Stats - move the slider to the right to collect statistics for this compute resource

Compute Zone - the compute zone to which the compute resource is assigned

API URL - set the vCenter API URL - e.g. https://example.com

Login - specify the vCenter login

Password - specify the vCenter password

5. Click the Save button to save your changes.

6. Go to compute resource label > Tools and click Resync vCenter to import all networks and datastore that are not currently synchronized in OnApp from vCenter.

On this page:

- Edit details of vCenter compute resource
- Manage vCenter compute resource data stores

2.3.2 Manage vCenter compute resource data stores

Data stores can easily be attached and removed from vCenter compute resources. This association between a compute resource and a data store is called a data store join.

You can add data stores to a compute resource only if they are assigned to the zones of the same type. For more information refer to Zone Types.

To add/remove data store joins:

1. Go to your Control Panel > Admin > Settings menu and click the Compute resources icon.
2. Click the label of the vCenter compute resource you want to manage data stores for.
3. On the screen that appears, click the Tools button, then click Manage Data Stores.
4. On the screen that follows, you’ll see a list of all data stores currently associated with this vCenter compute resource.

To remove a data store join, click the Delete icon next to it. You’ll be asked for confirmation before the store is removed.

To add a new data store join, choose a data store from the drop-down menu and click the Add Data Store button.
2.4 Create vCenter Compute Zone

To create a new vCenter compute zone:

1. Go to your Control Panel > Admin > Settings menu and click the Compute Zones icon.
2. Press "+" or click the Create Compute Zone button.
3. On the screen that follows give your compute zone a name (Label), choose Server Type (virtual) and select Location Group.

   Please do not proceed with other settings, since they will not be applicable after attaching a vCenter compute resource and converting into vCenter compute zone.

4. Click the Save button.
5. You will be redirected to the Compute Zone overview page. On this page, you will see Unassigned Compute Resources which can be added to this Compute Zone.
6. Click the "+" icon to assign a required vCenter compute resource(s).

   • The vCenter compute resource cannot be assigned to a compute zone if this zone already has any compute resources and attached networks.
   • The compute resource that does not belong to vCenter cannot be assigned to a compute zone if this compute zone has vCenter compute resource and attached networks.
   • Please do not assign data stores to vCenter compute zones. Instead, you may assign data stores to vCenter compute resources by using this instruction.

2.5 Manual IP Nets

The networking functionality available at Control Panel > Admin > Settings > Networks enables you to manage networks and work with IP nets. A network can contain several IP nets which include IP ranges with a default gateway. The network details page shows the list of IP nets in a network with their IP ranges which include the IPs assigned to virtual servers and/or users.

OnApp currently offers two types of IP nets: IP Pool and Manual IP. IP Pool nets are the regular type of IP net in OnApp, they contain IPs assigned to users/VSs and are available during server creation. When a VS is imported into OnApp and its IP is within one of the IP ranges from the vCenter networks, the IP is added to the IP net of the corresponding network.

If the IP of a vCenter VS that is being imported is not a part of an IP range in any of the vCenter networks, a special type of an IP net is created, Manual, and the IP of such a VS is added to it. Manual IP nets contain a single IP range which includes the whole space of IPv4 IP addresses. IPs from an Manual IP net are not available in the VS creation wizard. Manual IP nets can be viewed or deleted. A network can contain only one Manual IP net.

For information on IP Pool nets refer to Network Settings.
2.5.1 View Manual IP Nets

To view details of an IP net:

1. Go to your Control Panel > Admin > Settings menu.
2. Click the Networks icon. The page that loads shows the shared networks in your cloud.
3. Click the label of the network you are interested in. The screen will display the network's label, identifier, VLAN and network zone.
   This page also includes the IP nets in the selected network. Click an IP net of the Manual type net to view the list of IPs in it with the user and/or VS they are assigned to.

2.5.2 Delete Manual IP Net

You can delete only those IP nets that do not contain any IP ranges.

To delete an IP net:

1. Go to Control Panel > Admin > Settings > Networks. The page that loads shows the shared networks in your cloud.
2. Click the label of the network from which you want to remove an IP net.
3. Click the Actions icon next to the required IP net with the Manual type and select Delete.

2.6 Import vCenter Virtual Server

You can import one or more vCenter virtual servers at a time using vCenter compute resource menu. The VS(s) will be imported with limited functionality available. To gain access to the full functionality of the VS(s) you need to set vCenter credentials.

Prerequisites:

- Networks connected to Virtual Server(s) must be already imported to OnApp.
- Data stores containing Virtual Servers' disks must be already imported to OnApp.

On this page:

- Manual Import of vCenter VS
- Resync vCenter VS
- Auto Import of vCenter VS
- View Auto Import Rules
- Create Auto Import Rule
- Run Auto Import Rule
2.6.1 Manual Import of vCenter VS

To import vCenter virtual server(s):

1. Go to your Control Panel > Admin > Settings menu.
2. Click the Compute Resources icon.
3. Go to vCenter compute resource's label > Tools and click Import Virtual Server.
4. On the screen that follows, fill in the following:
   - VM name - choose the vCenter virtual server(s) from the drop-down list
   - Assign to User - choose a user from the drop-down list, who will be an owner of the virtual server(s)
5. Click Submit.

- You need to set your vCenter credentials to gain access to the full functionality of the VS at Control Panel > Cloud > Virtual Server > Label > Tools > Administrative Options > Set Credentials.
- The IPs of VSs imported from vCenter become a part of either IP Pool or Manual IP nets. For more information, refer to Manual IP Nets.

2.6.2 Resync vCenter VS

In case you apply any changes to the imported VS on the vCenter side, you may resync the VS to update all the VS's changes to match on both vCenter and OnApp sides. To resync vCenter VS:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the imported VS.
3. Click the Tools button on the VS's screen to expand the VS Tools menu.
4. Click the Resync VS button in the VS Options section to start the re-import transaction.
2.6.3 Auto Import of vCenter VS

If you need a quick import of multiple new VSs from vCenter to OnApp, use the auto import rules functionality. It allows you to apply the rule/rules to the already created but not yet imported virtual servers. After applying auto import rules, vCenter resources are recognized at OnApp side and can be billed immediately.

**Prerequisites**

- The auto import rule functionality is available on clouds that run OnApp 6.1 Edge 2 and subsequent versions.
- The *Manage auto import rules* permission should be enabled for a user who wants to view, create, run, edit or delete auto import rules.
- It only applies to the newly created vCenter virtual servers that are not yet imported to OnApp.

2.6.4 View Auto Import Rules

To view the list of auto import rules:

1. Go to your Control Panel > **Admin** > **Settings** menu.
2. Click the **Compute Resources** icon.
3. Go to vCenter compute resource's label > Tools and click **Auto Import Rules** to see a list of all rules and the following details:
   - *Label* - the name of the vCenter VS
   - *Source Type* - the type of vCenter source
   - *Source* - the vCenter resource
   - *Target Type* - the type of vCenter target user
   - *Target* - the vCenter user, who is the owner of the virtual server
4. Click the **Actions** button next to the auto import rule for quick access to the list of available actions.
5. To edit an auto import rule, click the **Edit** button.
6. To run an auto import rule, click the **Run** button.
2.6.5 Create Auto Import Rule

To create auto import rules:

1. Go to your Control Panel > Admin > Settings menu.
2. Click the Compute Resources icon.
3. Go to vCenter compute resource's label > Tools and click Auto Import Rules.
4. Click the Create Auto Import Rules button.
5. On the screen that follows, fill in the following:
   - Label - specify the name of the vCenter VS
   - Source Type - choose the type of vCenter source from the drop-down list
   - Source - choose the vCenter resource from the drop-down list
   - Target Type - choose the type of vCenter target user from the drop-down list
   - Target - choose the vCenter user from the drop-down list, who will be an owner of the virtual server
6. Click Submit.

2.6.6 Run Auto Import Rule

To run an auto import rule:

1. Go to your Control Panel > Admin > Settings menu.
2. Click the Compute Resources icon.
3. Go to vCenter compute resource's label > Tools and click Auto Import Rules.
4. Click the Actions button next to the auto import rule you want to run and click the Run button.

After you click the Run button, OnApp system receives the list of vCenter VSs suitable for this rule and schedules proper import transactions.

2.6.7 Edit Auto Import Rule

To edit an auto import rule:

1. Go to your Control Panel > Admin > Settings menu.
2. Click the Compute Resources icon.
3. Go to vCenter compute resource's label > Tools and click Auto Import Rules.
4. Click the Actions button next to the auto import rule you want to edit and click the Edit button.
5. Edit the following details:
   - **Label** - specify the name of the vCenter VS
   - **Source Type** - choose the type of vCenter source from the drop-down list
   - **Source** - choose the vCenter resource from the drop-down list
   - **Target Type** - choose the type of vCenter target user from the drop-down list
   - **Target** - choose the vCenter user from the drop-down list, who will be an owner of the virtual server

6. Click the **Submit** button.

### 2.6.8 Delete Auto Import Rule

**To delete an auto import rule:**

1. Go to your Control Panel > **Admin** > **Settings** menu.
2. Click the **Compute Resources** icon.
3. Go to vCenter compute resource's label > Tools and click **Auto Import Rules**.
4. Click the **Actions** button next to the auto import rule you want to delete and click the **Delete** button.
5. Click the **OK** button to confirm the deletion.

### 2.7 vCenter Virtual Servers

Virtual servers running on vCenter compute resources are managed almost the same as normal virtual servers. Also, the vCenter cluster is displayed as a pool of resources rather than per compute resource.

OnApp Cloud gives you high-end cloud management features including:

<table>
<thead>
<tr>
<th>vCenter Virtual Server Options</th>
<th>Power Options</th>
<th>Administrative Options</th>
<th>Networks</th>
<th>Disks</th>
<th>Snapshots</th>
<th>Statistics</th>
<th>Recipes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Edit</strong></td>
<td>Reboot</td>
<td>Create/Edit Administrator's note</td>
<td>Configure network interface</td>
<td>Create disks</td>
<td>Snapshots</td>
<td>CPU utilization</td>
<td>Recipes</td>
</tr>
<tr>
<td><strong>Rebuild manually</strong></td>
<td>Suspend</td>
<td>Transactions and logs</td>
<td>Rebuild network</td>
<td>Edit disks</td>
<td>Billing statistics</td>
<td>Custom variables</td>
<td></td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Shut down</td>
<td>Change Owner</td>
<td>Edit network speed</td>
<td>Migrate disks</td>
<td>Network interface statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Migrate to KVM</strong></td>
<td>Startup</td>
<td>Console</td>
<td>vCenter virtual server IP addresses</td>
<td>Delete disks</td>
<td>Disk IOPS statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resync VS</strong></td>
<td></td>
<td></td>
<td>Display network speed for</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Certain VS operations are unavailable in OnApp with vCenter:

- **Reboot in recovery**
- **Segregate**
- **VIP status**
- **Autoscaling**
- **Migrate VS.** vCenter utilizes vMotion to ensure that the VSs are optimally placed on the compute resources. However, you can migrate vCenter virtual servers to KVM.
- **Backups.** Backup process for vCenter virtual servers differs from the standard OnApp backup scheme. See vCenter VS Snapshots section for details.
- Use of IPv6 is not supported for vCenter virtual servers.

NOTE: Performing the following VS operations at vCenter may lead to problems with VMware infrastructure management. Please, do not execute the following actions in vCenter:

- Edit the Properties for any VS
- Create and delete Snapshots
- Make changes to the distributed vSwitch
- Remove templates from the data store
- Delete the services account on the virtual server
- Remove or stop VMware tools on the virtual server

Performing the following actions in vCenter will not affect OnApp:

- Migrate VSs between compute resources using vMotion
- Migrate VSs between data stores using Storage vMotion
- Place compute resources into maintenance mode
- Make changes to compute resources when in maintenance mode
- Back up VSs using third party tool (e.g. Veeam)
- Enable, Disable or make changes to DRS

Performing the following actions in vCenter will be synchronized with OnApp:

- Networks Created
2.7.1 Create vCenter Virtual Server

To create a vCenter virtual server:

Go to your Control Panel > Cloud > Virtual Servers menu and click the "✚" button or click the Create New Virtual Server button at the bottom of the page. Fill in the VS creation form step by step:

2.7.1.1 Step 1 of 6. Cloud Locations

On this page:

- Step 1 of 6. Cloud Locations
- Step 2 of 6. Templates
- Step 3 of 6. Properties
- Step 4 of 6. Resources
- Step 5 of 6. Add-ons
- Step 6. Confirmation

The Cloud Locations step applies to those users who have compute zones assigned to location groups in their bucket. This step will be present in the wizard if both of the following requirements are met:

- all compute resources available to the user are assigned to location groups
- compute resources are assigned to different locations

If the user's bucket has several compute zones, some of which are assigned to location groups, whereas others are not - the cloud locations screen will not be available in the wizard. Also if all compute zones are assigned to the same location this step will be skipped. In this case the wizard will start from the Templates step.

1. Indicate your virtual server's cloud location:
   - Country - choose the country, where the cloud is located, from the drop-down menu.
   - City - specify the city, where the cloud is located, from the drop-down menu.

2. Click Next to proceed to the following step of the wizard to specify the virtual server templates
2.7.1.2 Step 2 of 6. Templates

1. Click the required group icon on the right (vCenter) to expand the list of templates on the left. Every template contains the following info:
   - **Label**
   - **Min memory size** that is required to create a VS from this template
   - **Min disk size** that is required to create a VS from this template
   - **Virtualization type**
   - **Price per hour**

2. Select the template.

3. Click **Next**.

- You can use RHEL, Windows and Debian templates to create vCenter virtual servers. For details how to create vCenter templates, refer to [Create Template for vCenter Virtual Server](#) section.
- To be able to use Ubuntu templates later than 9 version for vCenter virtual server creation, you need to remove the absolute pathnames in `/etc/pam.d/vmtoolsd` file. For example: `/lib/security/pam_unix.so > pam_unix.so`
- Please make sure that the Windows password policy defined inside the template is compliant with the password policy set in the OnApp CP. This will ensure that there are no password related issues when provisioning Windows.
- OnApp supports templates with no more than one disk.
- Sometimes, vCenter VS creation may fail if it is based on OVA template with NVRAM file. For more details about the causes of the issue, refer to VMware article [Unable to deploy an OVF from a 6.7 environment](#). To check one of the possible solutions, refer to [vCenter 6.5 fails to boot OVA (Linux)](#). If the issue persists, make sure that you have equal version on vSphere and ESXi.

**Windows Licensing Type**

This option only appears if your bucket allows it, and if the relevant licensing options have been configured for the template group this template belongs to.

If this option is available, choose the license type you require:
- For the KMS type, choose the licensing server
- For your own license, type your license key

Please note that for the Windows templates imported from vCenter it is impossible to select the MAK license during the VS creation. Instead, select the **Your own license** option and manually indicate the License Key.
If you don’t specify the licensing type, MAK licensing will be set by default.

It is possible to deploy Windows virtual servers without running sysprep. To do so, you need to disable the Run Sysprep option for the compute zone the virtual server will be built on. See Create Compute Zone section for details.

It is not possible to set VS password when creating a Windows-based vCenter virtual server without running a sysprep.

2.7.1.3  Step 3 of 6. Properties
You can create a virtual server having specified only the required parameters and configure it later. Specify the following virtual server properties:

- **Label** - enter the label of the virtual server
- **Hostname** - enter the host name of the virtual server
  
  - Hostname may contain letters (A-Z), numbers (0-9) and hyphens (-) but no spaces or periods (.). The name may not consists entirely of digits.
  
  - For Windows-based VSs, the hostname length should be between 1 and 15 characters.
  
- **Domain** - enter the domain name of the virtual server
- **Password** - enter the password of the virtual server or leave black for the password to be auto generated
- **Password confirmation** - enter the password again to confirm it
- Click **Next**.

2.7.1.4  Step 4 of 6. Resources

**Compute Resources**

- **Compute Resource** - select the compute resource
- **vCenter Resource Pool** - select the resource pool

If you pick Resources from the dropdown menu, the virtual server will be placed into the default resource pool, so it will not be shown at any user resource pool, just under the cluster.

**Resources**

- **RAM** - set the amount of virtual server's RAM.
- **CPU Cores** - set the amount of virtual server's CPU cores.
- **CPU Priority (or CPU Units)** - set virtual server's CPU priority. If the CPU units are switched on in the bucket for this user, then CPU priority is replaced with CPU units. Refer to Billing Calculation section for details on CPU units and CPU priority.
The amount of CPU resource a VS is given is the CPU priority (you can think of this as its "share percentage") multiplied by the number of cores allocated to that VS. This is a minimum number – clients can exceed it, up to 100% multiplied by the number of cores. For example, on a compute resource with 3GHz CPU cores:

- 100% x 1 core = 3GHz (burstable to 3GHz)
- 10% x 2 cores = 600MHZ (burstable to 6GHz)
- 5% x 4 cores = 600MHz (burstable to 12GHz)

By default, OnApp allows overselling of cloud resources. For example, OnApp will allow users to create 5 VSs with 100% CPU priority/1 CPU core on a compute resource with a 4-core CPU. In this example, OnApp would reduce the guaranteed CPU for each VS.

If you build a VS on a KVM compute resource running CentOS5, the CPU priority settings will be disabled and CPU priority value will be 100 by default.

**Primary Disk**
- *Data Store Zone* - choose a data store zone for this VS's primary disk.
- *Primary data store* - select a primary data store for this VS's primary disk.
- *Primary disk size* - set the primary disk size.

**Swap Disk**
Select the following properties for a swap disk:

- *Size* - enter a size for a swap disk
- *Data Store Zone* - select a data store zone for a swap disk
- *Data Store* - select a data store for a swap disk
- *Disable* - select the checkbox to disable swap disk creation

Only enabled data stores will be available for selection at this step. You can enable or disable a data store at **Control Panel > Admin > Settings** menu by clicking the **Actions** button next to the data store you want to change, and then clicking **Edit**. Move the **Enabled** slider to the right to enable a data store.

**Network Configuration**

**Network Interface 1**

- *Network group* - select the network zone or leave Any
- *Network* - select the network from which the VS should get the IP address or leave Any
- *IP net* - select from the drop-down list the IP net from which the IP address should be assigned or leave Any
• IP range - select from the drop-down list the IP range from which the IP address should be assigned or leave Any
• IP address - select an IP address to be assigned from the drop-down box or leave Any
• Port Speed - set the port speed for this VS

Since VSS networks cannot be managed on OnApp side, it will not be possible to configure traffic shaping for them, so the Port speed field at the Edit NIC page and the Resources step of the VS Creation wizard will be disabled.

2.7.1.5 Step 5 of 6. Add-ons
During this step, you can assign service add-ons or recipes to your vCenter virtual server using Service Addons or Recipes sub-tabs.

You can create a vCenter virtual server either with Service Addons or Recipes, not with both at the same time. From which sub-tab you click Next, that option is applied. For example, if you select some recipes, then go to the Service Addons sub-tab and select some service add-ons and then click Next, service add-ons will be applied not recipes.

Recipes
The Recipes step is available in the wizard if Manage recipes joins for all virtual servers permission or Manage recipes joins for own virtual servers permission is enabled. To assign a recipe to your vCenter virtual server in the wizard, click Recipe under Add-ons and then follow the next steps:

1. Select a recipe that you want to assign to this virtual server by dragging the required recipe to the Assigned recipes pane.
2. To add a custom variable, click the "+" button next to the Custom recipe variables title bar, then specify variable details:
   - Specify the recipe name and its value.
   - Move the Enabled slider to the right to allow use of this variable.
3. Click Next to proceed to the next step of the wizard that completes the virtual server creation process.

The recipes step can be missing in the wizard if there are no recipes created in the cloud.

Service Add-ons
You can select the service add-ons that you want to assign to your virtual server. This step is optional. You can create a virtual server without choosing service add-ons and add them later if required.
Service add-ons are available if Manage Service Add-ons for all virtual servers permission or Manage Service Add-ons for own virtual servers permission is enabled.

1. Click the service add-on group icon on the left to expand the list of service add-ons on the right. Every service add-on contains the following info:
   - *Label*
   - *VS types* with which this service add-on is compatible
   - *Description* of the service add-on
   - *Price per hour*

2. Select the service add-on by clicking on it. You can select several add-ons from different service add-on groups. Click **View Selected Add-ons** to see the list of selected service add-ons. You can remove the selected service add-on from the list by clicking the button near the add-on.

3. Click **Next** to proceed to the next step of the wizard that completes the virtual server creation.

### 2.7.1.6 Step 6. Confirmation

- Move the **Enable Automated Backup** slider to the right if you want this VS to be backed up automatically (according to the backup settings configured in the Settings/Auto-backup Presets menu)

- Move the **Build Virtual Server** slider to the right, if you want the system to automatically build the VS. If you leave this box blank, you will have to build your server manually after it is created.

- Move the **Boot Virtual Server** slider to the right, if you want the virtual server to be started up automatically.

- Move the **Enable Autoscale** slider to the right to set autoscaling for this VS.

  - Until the **autoscaling rules** are configured the autoscaling itself will not start working.
  
  - If the **Enable Autoscale** slider is grayed out that means that you have reached the autoscaling limit in the bucket (or the max is set as 0).

- Move the **Acceleration allowed** slider to the right to enable accelerator for this VS. For more information, see **Edge Accelerator**.

At the Confirmation step you can find the configuration summary of VS, which will be created. You can view template's name, RAM size, number of networks, primary disk size, and number of cores.

After you set up all parameters, click the **Create Virtual Server** button to start the creation process.

### 2.7.2 vCenter Virtual Server Wizard Beta

OnApp 6.2 Edge 1 introduces a new beta version of the vCenter virtual server wizard. You can access the beta version of the wizard from the top bar on your Control Panel. To launch the wizard, click **Create Virtual Server > Add Virtual Server Beta**.
Note that a new beta version of the vCenter virtual server wizard is disabled by default. If you want to enable this version of the wizard, go to `on_app.yml` file and set the `show_new_wizard` parameter to `true`.

In this section you can find the procedures to create vCenter virtual servers in the new wizard, using one of the following methods:

- From Custom Set of Resources
- From Instance Package

2.7.2.1 Create Custom vCenter Virtual Server Beta

Virtual servers are created from templates and are deployed on compute, storage, and networking resources. To create a vCenter virtual server, you need to launch a wizard. The wizard walks you through several steps to get your virtual server up and running. You can create vCenter virtual servers from instance packages or custom set of resources. In this document, you can find a detailed guidance on how to create a custom vCenter virtual server but first take a look at the following section.

2.7.2.1.1 Infrastructure Mode

An infrastructure mode allows you to manage with OnApp only the infrastructure layer without any post actions (e.g. formatting disk after adding it, or assigning an IP address after adding a network interface). To create a vCenter virtual server in infrastructure mode, you need to have the Infrastructure mode permission enabled for your role and move the Infrastructure mode slider to the right at the Properties step in wizard.

To create a vCenter virtual server, follow the next procedure:

1. Go to your Control Panel and click Create Server on the top bar.
2. Click Create Virtual Server Beta to launch the wizard.
3. Follow the step-by-step instructions below to complete the wizard.
4. After you are finished, click the Create Virtual Server button.

On this page:
• **Infrastructure Mode**
• **Cloud Locations**
• **Templates**
• **Properties**
• **Compute Resources**
• **Storage Resources**
• **Network Resources**
• **Service Add-ons or Recipes**
  o **Service Add-ons**
  o **Recipes**
• **Confirmation**

### 2.7.2.1.2 Cloud Locations
The **Cloud Locations** step applies to those users who have compute zones assigned to location groups in their bucket. If Cloud Locations are not available, the wizard starts from the **Templates** step. This Cloud Locations step will be present in the wizard if both of the following requirements are met:

- All compute resources available to the user are assigned to location groups.
- Compute resources are assigned to different locations.

When you are at the **Cloud Locations** step, select a location for your virtual server:

- **Country** - choose the country, where the cloud is located, from the drop-down menu.
- **City** - specify the city, where the cloud is located, from the drop-down menu.

Click **Next** to proceed to the following step of the wizard.

### 2.7.2.1.3 Templates
To select a template, follow the next procedure:

1. Click the required group icon on the right (vCenter) to expand the list of templates on the left. Every template contains the following info:
   o **Label**
   o **Min memory size** that is required to create a VS from this template
   o **Min disk size** that is required to create a VS from this template
   o **Virtualization type**
   o **Price per hour**
2. Select the template.

### What template to choose

- You can use RHEL, Windows and Debian templates to create vCenter virtual servers. For details how to create vCenter templates, refer to [Create Template for vCenter Virtual Server](#) section.
- To be able to use Ubuntu templates later than 9 version for vCenter virtual server creation, you need to remove the absolute pathnames
in /etc/pam.d/vmtoolsd file. For example: /lib/security/pam_unix.so > pam_unix.so

- Please make sure that the Windows password policy defined inside the template is compliant with the password policy set in the OnApp CP. This will ensure that there are no password related issues when provisioning Windows.

3. Click **Next**.

### Additional Information for Windows Templates

The **Windows Licensing Type** box appears for Windows templates and includes license options that you configure for a corresponding template store. You can select one of the following license types:

- **MAK** - the default licensing type applicable to all Windows-based virtual servers. If you don't select the licensing type, MAK is set by default.

- **KMS** - the licensing type applicable to every virtual server since Windows 7, Windows Server 2008, and the following Windows versions. Click KMS and then select a licensing **Server**.

- **User license** - type your license key

When you create a virtual server from a Windows template, consider the following:

- You can create Windows-based vCenter virtual servers without running Sysprep. Disable the **Run Sysprep** option while creating or editing a destination compute zone.

- If multiple vCenter virtual servers are deployed from the same template without running Sysprep, they will have identical security identifiers (SIDs) that can result in the system conflict.

- You can't select KMS or your own license when you create a Windows vCenter virtual server from a custom template. As a workaround, you can create a vCenter VS from a template used for custom template creation.

- It is not possible to set VS password when creating a Windows-based vCenter virtual server without running a sysprep.

### 2.7.2.1.4 Properties

You can create a virtual server having specified only the required parameters and configure it later. Specify the following virtual server properties:

- **Infrastructure mode** - move the slider to the right to enable the **Infrastructure mode** for this virtual server

- **Label** - enter the label of the virtual server
• Hostname - enter the host name of the virtual server
  - Hostname may contain letters (A-Z), numbers (0-9) and hyphens (-) but no spaces or periods (.). The name may not consist entirely of digits.
  - For Windows-based VSs, the hostname length should be between 1 and 15 characters.

• Domain - enter the domain name of the virtual server

• Password - enter the password of the virtual server or leave blank for the password to be auto generated

• Password confirmation - enter the password again to confirm it

• Encrypt password - move the slider to the right to encrypt your password. For more information on the password encryption, see FAQ.

• Encryption passphrase - enter a passphrase for encryption

• Encryption passphrase confirmation - repeat the passphrase for encryption

• I want to create a VS with custom resources - move the slider to the right to create a virtual server based on a set of custom resources. If you don’t select the checkbox, you can create a virtual server from instance packages.

• Replace recipes - move the slider to the right to create a virtual server with service add-ons instead of recipes.

Click Next to proceed to the following step of the wizard where you select a custom set of resources.

---

2.7.2.1.5 Compute Resources

• RAM - set the amount of virtual server’s RAM.

• CPU Cores - set the amount of virtual server’s CPU cores.

• CPU Priority (or CPU Units) - set virtual server’s CPU priority. If the CPU units are switched on in the bucket for this user, then CPU priority is replaced with CPU units. Refer to Billing Calculation section for details on CPU units and CPU priority.

• Datacenter - select the data center for the data store.

• Cluster - select the cluster to import networks and data stores from.

2.7.2.1.6 Storage Resources

**Primary Disk**

• Size - set the primary disk size.

• Data Store Zone - choose a data store zone for this VS’s primary disk.

• Data Store - select a primary data store for this VS’s primary disk.

**Swap Disk**

Select the following properties for a swap disk:
- **Size** - enter a size for a swap disk
- **Data Store Zone** - select a data store zone for a swap disk
- **Data Store** - select a data store for a swap disk
- **Disable** - select the checkbox to disable swap disk creation

Only enabled data stores will be available for selection at this step. You can enable or disable a data store at **Control Panel > Admin > Settings** menu by clicking the **Actions** button next to the data store you want to change, and then clicking **Edit**. Move the **Enabled** slider to the right to enable a data store.

### 2.7.2.1.7 Network Resources
**Network Interface 1**

Selection of IP net, IP range, and IP address is not available for VSs in **Infrastructure mode**.

- **Network group** - select the network zone or leave **Any**
- **Network** - select the network from which the VS should get the IP address or leave **Any**
- **IP net** - select from the drop-down list the IP net from which the IP address should be assigned or leave **Any**
- **IP range** - select from the drop-down list the IP range from which the IP address should be assigned or leave **Any**
- **IP address** - select an IP address to be assigned from the drop-down box or leave **Any**
- **Port Speed** - set the port speed for this VS or select the **Unlimited** checkbox

Since **VSS networks** cannot be managed on OnApp side, it will not be possible to configure traffic shaping for them, so the **Port speed** field at the Edit NIC page and the Resources step of the VS Creation wizard will be disabled.

### 2.7.2.1.8 Service Add-ons or Recipes

This step is not available for VSs in **Infrastructure mode**.

During this step, you can assign **service add-ons** or **recipes** to your virtual server. The availability of service add-ons or recipes depends on the permissions **Manage Service Add-ons for all/own virtual servers** and **Manage Recipes for all/own virtual servers**. If you have only one of these permissions enabled, you will see only a corresponding tab in the wizard.
2.7.2.1.8.1 Service Add-ons
To create a virtual server with service add-ons instead of recipes, you should move the slider Replace recipes in the Properties step. If you do not move the slider, you will be able to create a virtual server with recipes.

Replace recipes slider is visible if Manage Service Add-ons for all virtual servers permission or Manage Service Add-ons for own virtual servers permissions are enabled.

Service add-ons are available under the following conditions:

- Manage Service Add-ons for all virtual servers permission or Manage Service Add-ons for own virtual servers permission is enabled
- Service add-on groups are available in your bucket
- The On Provisioning option is enabled for all or some of the service add-ons available to you within a bucket.

You can create a virtual server without service add-ons and add them later if required. To assign a service add-on to your virtual server in the wizard, follow the next steps:

1. Click the service add-on group icon on the left to expand the list of service add-ons on the right. Every service add-on contains the following info:
   - **Label**
   - **Description**
   - **Price per hour**
   - **Compatible with**, for example, Unix, Windows, etc

2. Click the service add-on to select it. You can select several add-ons from different service add-on groups. Click View Selected Add-ons to see the list of selected service add-ons.

   You can remove the selected service add-on from the list by clicking the \( \times \) button near the add-on.

3. Click **Next** to proceed to the next step of the wizard that completes the virtual server creation.

2.7.2.1.8.2 Recipes

The Recipes step is available only if you did not move the Replace recipes slider to the right in the Properties step.

To create a virtual server without a recipe and add them afterwards.

To assign a recipe to your virtual server in the wizard, follow the next steps:

1. Drag and drop a recipe from the Available recipes to Assigned for provisioning box.

2. To add a custom variable, click the "+" button next to the Custom recipe variables title bar, then specify variable details:
   - **Name & Value** - enter a name and value for the custom variable
   - **Enabled** - move the slider to the right to allow use of this variable

3. Click **Next** to proceed to the next step of the wizard that completes the virtual server creation process.

2.7.2.1.9 Confirmation

The Confirmation step allows you to apply the following settings:
• **Build Virtual Server** - move the slider to the right to automatically build the virtual server. If you don't select this checkbox, you have to build your server manually after it is created.

• **Boot Virtual Server** - move the slider to the right for the virtual server to be started up automatically.

The **Confirmation** step also provides the configuration summary of the virtual server, including information about the template, CPU cores, RAM, disks size, and network. When you are finished, click the **Create Virtual Server** button to start the creation process. After you click the button, several transactions are run to complete the process. You can check a status of each transaction in **Activity Log** of the virtual server.

### 2.7.2.2 Create Instance Package vCenter Virtual Server Beta

You can create a vCenter virtual server from a ready-made instance package. The **instance package** is a preconfigured environment with a specific compute, storage, and network capacity. For instance packages to be available in the wizard, you need to follow the next procedures:

- **Enable Permissions**
- **Add Instance Packages to CP**
- **Add Instance Packages to Bucket**

After you complete these steps, you can create vCenter virtual servers from instance packages in the wizard. The wizard walks you through several steps to get your virtual server up and running. In this document, you can find a detailed guidance on how to create a vCenter virtual server but first take a look at the following section.

#### 2.7.2.2.1 Before You Begin

On this page:

- **Before You Begin**
- **Infrastructure Mode**
- **Cloud Locations**
- **Templates**
- **Properties**
- **Instance Packages**
- **Service Add-Ons or Recipes**
- **Confirmation**

See also:

- **Instance Packages**
- **Create Custom Virtual Server**
- **Permissions**
- **Buckets**

Before you begin to create a virtual server from an instance package, take into consideration the following:

- You should have at least one **compute resource** configured and attached to a **compute zone**, a **data store** – to a **data store zone** and compute resource or zone, a **network** – to a **network zone** and compute resource, a **backup server** – to a **backup server zone** and compute resource or zone, and a **bucket** – to a user who creates a virtual server.
• If an instance package applies only to certain compute zones in a bucket, a virtual server is created on one of the compute resources within one of those zones. If an instance package is not limited to certain zones, the compute zone and compute resource are selected automatically from the ones available to a user.

• Instance package virtual servers can be created only in compute zones where all compute resources are assigned the same number of CPU units. If there are compute resources with different number of CPU units, it's not possible to create instance package virtual servers in such zones. The reason is that CPU priority for instance package virtual servers in this configuration cannot be set to 100%, which is the default value for such virtual servers.

• If there are no available IP addresses, all instance packages are dimmed in the wizard.

• Instance packages that have resources incompatible with the available compute zones are dimmed in the wizard.

• **Auto-scaling** and **Accelerator** are not supported for virtual servers created from instance packages.

To create Instance Package vCenter Virtual Server, follow the next procedure:

1. Go to your Control Panel and click **Create Server** on the top bar.

2. Click **Create Virtual Server Beta** to launch the wizard.

3. Follow the step-by-step instructions below to complete the wizard.

4. After you are finished, click the **Create Virtual Server** button.

### 2.7.2.2.2 Infrastructure Mode

An infrastructure mode allows you to manage with OnApp only the infrastructure layer without any post actions (e.g. formatting disk after adding it, or assigning an IP address after adding a network interface). To create the Instance Package vCenter virtual server in infrastructure mode, you need to have the **Infrastructure mode** permission enabled for your role and move the **Infrastructure mode** slider to the right at the **Properties** step in wizard.

### 2.7.2.2.3 Cloud Locations

The **Cloud Locations** step is available for users whose bucket includes compute zones assigned to location groups. If Cloud Locations are not available, the wizard starts from the **Templates** step. The **Cloud Locations** step is present in the wizard if the following requirements are satisfied:

- All compute zones that are added to a user's bucket are assigned to location groups.
- Compute zones that are added to a user's bucket are not assigned to the same location group.

When you are at the **Cloud Locations** step, select a location for your virtual server:

- **Country** - select a country where the cloud is located
- **City** - select a city from the country where the cloud is located

Click **Next** to proceed to the following steps of the wizard.

### 2.7.2.2.4 Templates

The **Templates** step allows you to select a template from which to build your virtual server.

To select a template, follow the next procedure:

1. Click a **Template Store** icon on the left to see templates that are available in this store. You can see the following details for each template:

   - **Label**
2. Click a template to select it.
3. Click Next to proceed.

**Additional Information for Windows Templates**

The **Windows Licensing Type** box appears for Windows templates and includes license options that you configure for a corresponding template store. You can select one of the following license types:

- **MAK** - the default licensing type applicable to all Windows-based virtual servers. If you don't select the licensing type, MAK is set by default.

- **KMS** - the licensing type applicable to every virtual server since Windows 7, Windows Server 2008, and the following Windows versions. Click KMS and then select a licensing Server.

- **User license** - type your license key

When you create a virtual server from a Windows template, consider the following:

- You can create Windows-based virtual servers without running Sysprep. Disable the **Run Sysprep** option while creating or editing a destination compute zone.

- If multiple virtual servers are deployed from the same template without running Sysprep, they will have identical security identifiers (SIDs) that can result in the system conflict.

- You can't select KMS or your own license when you create a Windows virtual server from a custom template. As a workaround, you can create a virtual server from a template used for custom template creation.

- You can build a **Windows 10/Windows Server 2016** virtual server on **KVM CentOS 6** and **CentOS 7** compute resources that run at least on the following processor:
  - Ivy Bridge Intel® Xeon® Processor E Series v2 Family
  - AMD Opteron G2, G3, G4, G5, and G6
  - The **fsgsbase** CPU flag is required for a destination compute zone. For more information on CPU flags, see **Manage Extended CPU Configuration for Compute Zone**.
There are some obligatory and optional properties that you can provide for your virtual server. The obligatory properties are marked with an asterisk on the list and the optional properties you can edit after creating a virtual server.

Enter the following properties for your virtual server:

- **Infrastructure mode** - move the slider to the right to enable the Infrastructure mode for this virtual server
- **Label*** - enter a label of the virtual server
- **Hostname*** - enter a hostname of the virtual server. The hostname can consist of letters [A-Z a-z], digits [0-9], and dash [-]. For more info on hostname validation, refer to RFC documentation.

**Additional Consideration for Windows**

- The hostname length should be between 1 and 15 characters.
- The following symbols are not allowed for Windows-based virtual servers:
  - percent sign [%]
  - double quotation marks [“]
  - brackets [<,>]
  - vertical bar [|]
  - caret [^]
  - ampersand [&]
  - parentheses [(,)]

- **Domain** - enter a domain of the virtual server. For example, in test.onapp.com the test is a hostname and onapp.com is a domain. If you don't enter a domain, the default value localdomain is used as follows test.localdomain. This parameter is not applicable to Windows virtual servers.

- **Time zone (Windows)** - select a time zone for a Windows virtual server. Most operating systems implies that the hardware clock is in UTC, however, Windows implies a localtime. Therefore, you need to select a time zone for it to be properly handled on a compute resource level.

- **Password** - enter a secure password for the virtual server. It can consist of 6-99 symbols, including letters [A-Z a-z], digits [0-9], dash [-], underscore [ _ ], and the following special characters: ~ ! @ # $ * _ - + = ` \ { } [ ] : ; ' , . ? / . You can use both lower and uppercase letters. If you don't enter a password, it will be generated automatically.

- **Password confirmation** - repeat the password to confirm it

- **Encrypt password** - move the slider to the right to encrypt your password. For more information on password encryption, see FAQ.

- **Encryption passphrase** - enter a passphrase for encryption

- **Encryption passphrase confirmation** - repeat the passphrase for encryption

- **I want to create a VS with custom resources** - move the slider to the right to create a virtual server based on a set of custom resources. The checkbox is displayed only if the Select resources manually on virtual server creation permission is enabled. See Create Custom vCenter Virtual Server for details.

- **Replace recipes** - move the slider to the right to create a virtual server with service add-ons instead of recipes.

Click **Next** to proceed to the following step of the wizard.
2.7.2.2.6 Instance Packages

To create a virtual server from an instance package, click a box for a corresponding package. The instance package box includes the following details:

- **CPUs** - the number of CPU cores available in this instance package
- **Memory** - the number of RAM in MB or GB available in the instance package
- **Disk Size** - the number of disk size in MB or GB available in this instance package
- **Bandwidth** - the number of bandwidth in MB or GB available in this instance package
- **Price per Hour**:
  - **Mode ON** - an estimated hourly price if the virtual server is powered on
  - **Mode OFF** - an estimated hourly price if the virtual server is powered off
- **Price per Month**:
  - **Mode ON** - an estimated monthly price if the virtual server is powered on
  - **Mode OFF** - an estimated monthly price if the virtual server is powered off

After you click an instance package box, it becomes highlighted in green. Click Next to proceed to the following step of the wizard.

2.7.2.2.7 Service Add-Ons or Recipes

During this step, you can assign service add-ons or recipes to your virtual server. The availability of service add-ons or recipes depends on the permissions Manage Service Add-ons for all/own virtual servers and Manage Recipes for all/own virtual servers. If you have only one of these permissions enabled, you will see only a corresponding tab in the wizard.

2.7.2.2.7.1 Service Add-ons

To create a virtual server with service add-ons instead of recipes, you should move the slider Replace recipes in the Properties step. If you do not move the slider, you will be able to create a virtual server with recipes.

*Replace recipes* slider is visible if Manage Service Add-ons for all virtual servers permission or Manage Service Add-ons for own virtual servers permissions are enabled.

Service add-ons are available under the following conditions:

- The Replace Recipes with Service Add-ons on VS Creation permission is enabled.
- Service add-on groups are available in a bucket.
- The On Provisioning option is enabled for all or some of the service add-ons available to you within a bucket.

If these conditions are not satisfied, you will see the Recipes step instead.

You can create a virtual server without service add-ons and add them afterwards. To assign a service add-on to your virtual server in the wizard, follow the next steps:
1. Click a service add-on group on the left to expand the list of service add-ons on the right. You can see the following details about each service add-on:
   o Label
   o Description
   o Price per hour
   o Compatible with, for example, Unix, Windows, etc

2. Click the service add-on to select it. You can select several add-ons from different service add-on groups. Click View Selected Add-ons to see the list of selected service add-ons. To remove the selected service add-on from the list, click the button.

3. Click Next to proceed to the final step of the wizard.

Recipes

Recipes step is available only if you did not more the Replace recipes slider to the right in the Properties step.

The Recipes step is available in the wizard if there are some recipes created in the cloud. You can create a virtual server without a recipe and add them afterwards. To assign a recipe to your virtual server in the wizard, follow the next steps:

1. Drag and drop a recipe from the Available recipes to Assigned for provisioning box.

2. To add a custom variable, click the "+" button next to Custom Recipe Variables and provide the following details:
   o Name & Value - enter a name and value for the custom variable
   o Enabled - move the slider to the right to allow use of this variable

3. Click Next to proceed to the final step of the wizard.

2.7.2.2.8 Confirmation

The Confirmation step provides the configuration summary of the virtual server, including information about CPU, memory, and disk size. Here you can also apply the following settings:

- Enable Automated Backup - move the slider to the right to create automatic backups of the virtual server based on the settings from Auto-Backup Presets.

- Build Virtual Server - move the slider to the to the right if you want the system to automatically build the virtual server. If you don't select this checkbox, you have to build your server manually after it is created.

- Boot Virtual Server - move the slider to the right if you want the virtual server to be started up automatically.

When you are finished, click the Create Virtual Server button to start the creation process. After you click the button, several transactions are run to complete the process. You can check a status of each transaction in Activity Log of the virtual server.

2.7.3 View vCenter Virtual Server Details

To view details of a specific vCenter virtual server:
1. Go to your Control Panel > Cloud > Virtual Servers menu.

2. Click the label of the virtual server you're interested in.

3. The screen that appears loads the VS properties, notes, activity log and tools for managing your virtual server.

2.7.3.1 VS Properties

VS properties page gives general overview of the VS details:

- Template this VS is built on
- Power status & On/Off/Reboot buttons.

Clicking the OFF button performs graceful shutdown and then powers off the virtual server after the timeout set in Configuration settings.

- Compute resource. Click the compute resource name to see its details
- Login credentials
- Owner. Click the owner name to see its details.
- Price per hour
- Memory
- CPU(s)/shares
- Disk Size
- Disk backups (irrelevant field)
- Network Speed
- IP Addresses. Only the first five IP addresses are displayed on the virtual server properties page. To view the list of all virtual server IP addresses, mouse over IP addresses area or go to the Networking > IP addresses tab.

If the automation options weren’t enabled during this virtual server creation, you’ll be redirected to the form where you can configure them.

2.7.3.2 Notes

The Notes section lists brief comments or reminders for a VS. You can add either admin’s or user’s notes. The admin’s note will be available to cloud administrators. Click the Actions button in the Notes section of the page to add admin’s or user’s note.

2.7.3.3 VS Management

- Click the Tools button to expand the Tools menu with the VS management options.
- Use the top menu to manage your virtual servers’ statistics/networking/storage options.

2.7.4 Edit vCenter Virtual Server

You can edit CPU and RAM resources for vCenter virtual servers built on Windows and Linux templates, as well as Windows and Linux OVA templates.

To edit CPU and RAM resources, follow the next steps:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click a label of the server you want to resize to display its details screen.
3. Click the Tools button and select the Edit Virtual Server link.
4. Change the label, CPU core/priority and RAM values, and click the Save button.
After you save the settings, the resize is completed automatically and you can see a message indicating the resize was successful.

2.7.5 Delete vCenter Virtual Server
Shut down the VS before destroying it. If you are deleting a VS that is running, the VS will be deleted after the time set in Timeout Before Shutting Down VSs configuration parameter.

To remove the virtual server from the cloud:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. On the screen that appears, you'll see the list of all virtual servers in the cloud. Click the label of the virtual server you want to delete.
3. On the VS's screen, click the Tools button, then select Delete Virtual Server.
4. Click the Destroy button.

You won't be able to restore a VS after deleting it.

2.7.6 Build vCenter Virtual Server Manually
To build/rebuild virtual server build/rebuild virtual server must be enabled. This is a new permission which manages build/rebuild functionality independently from update virtual server permission which used to regulate the build/rebuild options in the previous versions.

If you haven't checked the Build Virtual Server Automatically option during the VS creation process, you will have to do this manually after the VS has been created. Building a virtual server is the process of allocating physical resources to that VS.

To build a virtual server manually:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. On the screen that appears, click the Tools button and then click Rebuild Virtual Server.
4. On the screen that pops up, use the drop-down menu to choose a template with which to build the VS.
5. Tick the Required Start Up box to have your VS started automatically after it is built.
6. Click the Build Virtual Server button to finish.

2.7.7 Clone vCenter Virtual Server

You can create a clone of a virtual server based on the same resources as the origin virtual server. To be able to clone virtual servers, you need to have the Clone own virtual servers permission enabled. The cloned virtual server inherits resources from the origin as follows.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Cloned Virtual Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties - owner, hostname,</td>
<td>The same as the origin virtual server with Clone in the label, for example, Clone</td>
</tr>
<tr>
<td>password, and label.</td>
<td>Origin Label.</td>
</tr>
<tr>
<td>• Compute, data store, and</td>
<td>The same as the origin virtual server. If there are no available resources on the same</td>
</tr>
<tr>
<td>network resources &amp; zones</td>
<td>data store, network, and compute resource, you cannot clone a virtual server.</td>
</tr>
<tr>
<td>• Recipes, recipe variables,</td>
<td></td>
</tr>
<tr>
<td>and service add-ons</td>
<td></td>
</tr>
<tr>
<td>• Firewall rules</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>A random IP address is assigned from an IP range in the origin network.</td>
</tr>
<tr>
<td>Swap disk</td>
<td>A new swap disk is created on the cloned virtual server.</td>
</tr>
<tr>
<td>Backups</td>
<td>The backups of the origin virtual server are not cloned.</td>
</tr>
</tbody>
</table>

To clone a virtual server, follow the next procedure:

1. Go to your Control Panel > Cloud > Virtual Servers.
2. Click a label of the virtual server that you want to clone.
3. Click Tools and then click Clone Virtual Server.
4. In the pop-up box, click Clone Virtual Server to confirm the action.

After you confirm the action, several transactions are run to complete the cloning process. You can check a status of each transaction in Activity Log of the virtual server. After the virtual server is cloned, it is powered off until you start it.

2.7.8 Migrate from vCenter to KVM

OnApp enables you to migrate your vCenter virtual servers from VMware to KVM virtualization. You can initiate the migration from your OnApp Control Panel, using the procedure described in this document. The migration workflow includes several actions that are required to get your virtual servers up and running on KVM.

This workflow describes the basic steps that are run to migrate a virtual server from vCenter to KVM. You can enable some additional automation settings while initiating the migration in the wizard.

The Migration Workflow
1. You initiate the migration of a virtual server from your vCenter to a KVM compute resource.
2. The source virtual server is stopped and then exported from vCenter as a self-contained OVA package.
3. The OVA package is imported to the OVA List page in OnApp Control Panel.
4. The OVA package is converted to the KVM virtualization.
5. The virtual server is built from the OVA package.

Before you proceed to migrating your virtual server from vCenter to KVM, please take a look at the following section.

On this page:
Before You Begin
Migrate Virtual Server to KVM
Troubleshooting

See also:
Migration from vCloud to KVM
Buckets
Permissions
OVAs

2.7.8.1 Before You Begin

Before you proceed further, please note that:

- The migration from vCenter to KVM is available on clouds that run OnApp 5.10 and subsequent versions.
- You can migrate only virtual servers from your vCenter instance to KVM.
- vCenter virtual servers with XFS or LVM partitions/file systems cannot be migrated to KVM.
- The Migrate any/own virtual server permission should be enabled for a user who wants to migrate a virtual server.
- The destination KVM compute, data store, backup server, and network zones should be available in a bucket of a user who runs the migration.
- You can migrate a virtual server to the KVM compute, data store, backup server, and network zones that have enough resources to handle the virtual server.
  If there are not enough resources available in these zones, you cannot complete the wizard and initiate the migration.

If you experience any issues while migrating a virtual server from vCenter to KVM, see Troubleshooting.

2.7.8.2 Migrate Virtual Server to KVM

To migrate a virtual server from a vCenter instance to a KVM compute resource, follow the next procedure:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click a label of a virtual server that you want to migrate.
3. Click Tools and then click Migration to KVM.
4. Go through the following steps in the wizard to migrate the virtual server:
2.7.8.2.1 Step 1: Compute Resource
The first step enables you to select a KVM-based compute zone and resource to migrate your virtual server to.

- **Hypervisor group** - select a KVM hypervisor group (compute zone) where you want to migrate the VS
- **Hypervisor** - select a destination KVM hypervisor (compute resources) from the compute zone
- **Label** - edit a label of the VS if you want to keep the source VS after the migration
- **Hostname** - edit a hostname of the VS if you want to keep the source VS after the migration

- Hostname may contain letters (A-Z), numbers(0-9) and hyphens (-) but no spaces or periods (.). The name may not consists entirely of digits.
- For Windows-based VSs, the hostname length should be between 1 and 15 characters.

Click **Next**.

2.7.8.2.2 Step 2: Disks
The second step allows you to configure the logic of the disks migration to data stores associated with the KVM compute zone. You can migrate all disks to one data store or select a separate data store for each disk.

- **Allow Disk to One Data Store** - switch the option on/off to enable or disable the migration of disks to one data store. Depending on the selected option, one of the following boxes becomes available:
  - **All Disks to One Data Store** - select one data store to migrate all the disks to
  - **Select Data Store for Disk** - select a separate data store to migrate each disk to

Click **Next**.

2.7.8.2.3 Step 3: Networks
The third step enables you to apply the network configuration based on the networks available in the KVM compute zone. You assign each interface to a separate network from a destination network zone.

- **Network** - select a network for the interface or leave Any. If you select a specific network, you can also set the following network configurations.
- **IP net** - select an IP net that contains the IP address ranges of the network or leave Any
- **IP range** - select an IP range from an IP net that you selected in the previous step or leave Any
- **IP address** - select an IP address from an IP range that you selected in the previous step or leave Any

Click **Next**.

2.7.8.2.4 Step 4: Windows Licensing
If you migrate a Windows virtual server, the forth step of the wizard enables you to edit the licensing settings. You can select one of the following licensing options:

- **None** - select the checkbox to migrate a virtual server without license changes
• **MAK** - select the checkbox to migrate a virtual server with the MAK license and edit the following settings:
  - **Distribution** - select the Windows OS distribution of the virtual server
  - **R2** - select the checkbox to use an updated release of the Windows OS distribution
  - **Architecture** - select the architecture of the OS (x86 or x64)
  - **Edition** - select the edition of the Windows OS

• **Your own license** - select the checkbox and paste your own licensing key

Click **Next**.

2.7.8.2.5 Step 5: Confirmation
The final step allows you to configure the automation settings and initiate the migration.

• **Start VS after migrate** - enable the option to start the VS after the migration is finished. If you disable this option, you can start the VS via the **Power Options** after it is migrated.

• **Remove source VS after successful migration** - enable the option to delete the source VS after the migration is finished. If you disable this option, make sure that you edited **Label** and **Hostname** of the VS in the first step of the wizard.

Click **Submit** to initiate the migration.

After you submit the changes, several transactions are run to import your virtual server from vCenter to KVM. When the virtual server is built, you can see a log of the transactions in the **Activity Log** section of the destination VS. The migration process could take up to 15 minutes, depending on the virtual server configuration and the migration settings. If you cannot complete the wizard, see **Troubleshooting**.

2.7.8.3 Troubleshooting
You may face the following issues while initiating the migration of your virtual server from vCenter to KVM:

- **Not enough resources are available in a destination compute zone.**
  If there are not enough resources, such as RAM and CPU, select another compute zone or allocate more resources to the destination compute zone.

- **Not enough disk space is available in a destination data store zone.**
  If there is not enough disk space, select another data store zone or allocate more space to the destination data store zone.

- **Not enough IP addresses are available in a destination network zone.**
  If there are not enough IP addresses, select another network zone or allocate more IP addresses to the destination network zone.

2.7.9 vCenter Virtual Server Power Options
To manage vCenter virtual server power options:

1. Go to your Control Panel > **Cloud** > **Virtual Server** menu.
2. Click the label of the required virtual server.
3. Click the **Tools** button on the VS’s screen to expand the **VS Tools** menu.
4. The **Tools** menu enables you to perform the following power actions on VSS (the exact list shown depends on the VS status):
   - **Reboot Virtual Server** - powers off and then restarts the VS.
   - **Suspend Virtual Server** - stops a VS, changes its status to suspended and disables all the other actions on VS, unless unsuspended.
• *Shut Down Virtual Server* – pops up a dialogue box, where you can either *Shut Down VS* (terminates the VS gracefully), or *Power Off VS* (terminates the VS forcefully).

• *Startup Virtual Server* - queues a start-up action for a VS that's currently powered off.

### 2.7.10 vCenter Virtual Server Administrative Options

To manage a vCenter virtual server administrative options:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Click the label of the required vCenter VS.
3. Click the **Tools** button on the server’s screen to expand the Tools menu.
4. The **Tools** menu enables you to perform the following administrative actions:
   - **Set Root Password** - set current root/administrator password for a newly imported VS.
     - *Password confirmation* - repeat the password to confirm it.
     - *Encrypt password* - move the Encrypt Password slider to the right, to encrypt your password, then enter an encryption key in the field that appears.
   - **Change Owner** - pops up a dialogue box with a drop-down of all users on the system, enabling you to pass ownership of the vCenter VS to the user selected from the list. If you have any recipes for this server, you will be also prompted to confirm if the recipe should be moved to another user.
   - **Set Credentials** - The credentials are required for adding/editing disks and other operations. You need to set your vCenter credentials to gain access to the full functionality of the VS. For that click **Control Panel** > **Cloud** > **Virtual Server** > **Label** > **Tools** > **Administrative Options** > **Set Credentials**.

### 2.7.11 vCenter Virtual Server Transactions and Logs

The system records a detailed log of all the transactions happening to your virtual servers. The list of transactions logged by the system includes:

• Provision virtual server
• Startup virtual server
• Stop virtual server
• Resize virtual server without reboot
• Configure Operating System
• Build disk
• Resize disk
• Format disk
• Destroy disk
• Destroy virtual server
• Destroy template
• Download template
• Update firewall

To view transactions for a virtual server:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Click the label of the virtual server you're interested in.
3. The details screen for that virtual server shows recent transactions in the Activity Log section. To view more transactions, click the More Logs button.

To cancel pending tasks, click Cancel All Pending Tasks for this virtual server.

2.7.12 vCenter Virtual Server Networks

The Networking menu in the Virtual Servers menu enables you to manage network interfaces and allocate IP addresses.

2.7.12.1 Configure vCenter Virtual Server Network Interface

The Networking > Network Interfaces menu shows the virtual network interfaces allocated to this VS. Network interfaces join the physical network to the VS. When you create a VS a network interface is added automatically. This network interface will be assigned to the existing physical network using a spare IP (IPv4) and will be set primary by default.

OnApp supports IPv4 and IPv6. Since not every application supports IPv6, at least one IPv4 address must be allocated to a VS's primary network interface.

To see the list of all network interfaces allocated to the VS:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Networking tab, then click Network Interfaces.
4. On the page that follows you will see the following fields:
   - Interface – optional label of the network interface.
   - Network join – name of the network and a compute resource or compute zone this network is joined to.
   - Port speed – the speed set to the interface.
   - Primary interface – indication whether the interface is primary or not.

Here you can also view Interface Usage, Edit and Delete network interface (using icon controls) and Add a new network interface using the button at the bottom of the screen.

To add a network interface:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Networking tab, then click Network Interfaces.
4. Click the Add New Network Interface button at the bottom of the screen.
5. On the screen that appears, input values for the following parameters:
   - Label – a human-friendly name for the new interface.
   - Physical Network – choose a network join from the drop-down menu, which lists network joins assigned to the compute resource/compute zone on which the VS runs).
   - Port speed – set port speed in Mbps, or make it unlimited.
6. Click the Add Network Interface button.

To edit network interface label, port speed or set it as primary (if none is marked as primary), click Edit icon next to the appropriate network interface. After editing the port speed, the virtual server should be power cycled for the change to take effect.

To delete a network interface, click the Delete icon next to the interface you want to delete.

To allocate another physical network, add a new network interface.
2.7.12.2 Rebuild vCenter Virtual Server Network
To rebuild network join, added to the virtual server (required after allocating new IP addresses to a vCenter Windows-based VS):

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of a required VS.
3. On the screen that appears, click the Tools button, then click Rebuild Network.
4. In the pop-up window that appears, move the Force Reboot slider to the right, then select the VS shutdown type:
   - Power OFF virtual server
   - Shutdown virtual server
   - Gracefully shutdown virtual server
5. Move the Required Startup slider to the right to start up the VS automatically after the network is rebuilt.
6. Click the Rebuild Network button.

2.7.12.3 Allocate/Remove vCenter Virtual Server IP Addresses
In the Networking > IP Addresses tab you can find the list of assigned IP addresses, allocate new IP addresses and rebuild a network.
To allocate a new IP Address to the VS:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Networking tab, then click IP Addresses.
4. Click the Allocate New IP Assignment button.
5. Select a network interface from the drop-down menu (only the network interfaces you added to the VS will be available)
6. Select an IP address from the IP Pool associated with the network interface. You may select an IP address that's already assigned to a VS, but only one VS should be online at a time.
   Use Please show me used IP Pool, Show only my IPs and Show only IPv6 checkboxes to narrow the list of IP in the drop-down list.
7. Click the Add IP Address Assignment button.
8. Click Rebuild Network.
To remove an IP address from a VS:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Networking > IP Addresses tab.
4. Click the Delete icon next to the IP address you want to delete.
5. In the pop up window that appears:
   - Choose Delete with Reboot option if you want to reboot a VS and rebuild the network immediately after deleting the IP address. After choosing the Delete with Reboot option you will be redirected to the VS's Overview page.
   - Choose Delete without Reboot option if you don't want to reboot a VS. In this case to apply the changes, you will have to reboot the VS additionally.
2.7.12.4 Display Network Speed for Network Interfaces on vCenter Virtual Server Page

The main Virtual Servers screen displays the network speed of each VS's primary network interface. To see the speed of all interfaces assigned to a VS:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you are interested in.
3. Click the Networking > Network Interfaces tab.
4. On the screen that appears, the Port Speed column shows the network speed of the network interface.

2.7.12.5 Edit vCenter Virtual Server Network Speed

To edit a vCenter virtual server's network speed:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Select the virtual server you want to change.
3. Go to the Network > Network Interfaces, and edit the network speed accordingly.
4. Click the Save Network Interface button to save changes.

2.7.12.6 Import VSS Networks from vCenter

To use OnApp vCenter with basic licensing, you may import existing VSS from vCenter to OnApp so that they can be used instead of dvSwitches.

vSphere Standard Switches

In vCenter, you can create abstracted network devices called vSphere Standard Switches (VSS). You use standard switches to provide network connectivity to hosts and virtual machines. A standard switch can bridge traffic internally between virtual machines in the same VLAN and link to external networks.

You can add a VSS network for a VS imported from vCenter to OnApp. To successfully import VSS networks from vCenter to OnApp, do the following on the vCenter side:

- make sure that all VSS port group names are the same across ESXi hypervisors, otherwise, issues with migration may appear.
- manually create VSS on each ESXi host for the VSS to be shown in vCenter as one entry.

Once done, you may import your vCenter VS or resync it if the VS was imported previously.

Since VSS networks cannot be managed on OnApp side, it will not be possible to configure traffic shaping for them, so the Port speed field at the Edit NIC page and the Resources step of the VS Creation wizard will be disabled.

2.7.13 vCenter Virtual Server Disks

Virtual server storage is provided by disks. A disk is a partition of a data store that is allocated to a specific virtual server. Disk can be set as primary (that is, the disk from which an OS will boot).

Managing disks for the entire cloud is handled through the Control Panel's Settings menu. Disks
for individual virtual servers are managed through the Control Panel > **Cloud > Virtual Servers** menu, where you can:

- See the list of disks allocated to this VS
- Add a new disk
- Resize a disk
- Check disk usage statistics (IOPS)
- Delete a disk

### 2.7.13.1 Add Disks to vCenter Virtual Servers

Adding a disk to a virtual server will require that VS to be rebooted. If a VS is running when you try to add a new disk to it, you’ll be asked to confirm the reboot. To add a disk to a virtual server:

1. Go to your Control Panel > **Cloud > Virtual Servers** menu.
2. Click a VS’s label to open its details screen.
3. Click the **Storage** tab > **Disks**.
4. Click the **Create Disk** button.
5. Fill in the details:
   - **Data store** - select the data store to create a disk on from the drop-down list.
   - **Disk size**
   - **Swap Space** - move slider to the right if this disk is swap space.
   - **Require Format Disk** - move slider to the right if this disk requires formatting.

   For Linux-based vCenter VSs, if the **Require Format Disk** option is enabled, you’ll get a notification that VM will be rebooted. If the option is disabled, disk will not formatted, but will also not be visible without the VS rescan or reboot.

   - **Mounted** - move the slider to the right if the disk should be added to Linux FSTAB (for Linux application servers).
   - **Mount point** - the maximum length of a Mount Point is 256 characters. Spaces are not allowed. No more than one slash is allowed. If the mount point is not specified the default mount point will be used:

```
/mnt/onapp-disk-#{disk.identifier}
```

   - **Reboot Virtual Server** - move the slider to the right to reboot the VS after adding disk (applies only to Linux-based vCenter VSs)

6. Click the **Add Disk** button to finish.

When you add a new disk to a virtual server it will automatically become available to that server.
2.7.13.2 Edit vCenter Virtual Server Disks
You can easily resize disks when needed. The resize will fail if your current usage is greater than the new size you request.

To change disk size:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Make sure your virtual server is powered off, then click its label to open its details screen.
3. Click the Storage tab > Disks.
4. Click the Actions button next to the disk you want to change, then click the Edit link.
5. Enter a new disk label and size in GB in the fields provided.
6. Click the Save Disk button.

For Linux-based VSs, it is necessary to rescan or reboot a VS after increasing its disk size.

2.7.13.3 Migrate vCenter Virtual Server Disks
You can migrate disks of your virtual servers to other data stores, which are allocated to the same compute resource or compute zone. Unlike VS migration – disk migration requires reboot of the VS (despite the template it is based on).

To migrate a disk:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Make sure your virtual server is powered off, then click its label to open its details screen.
3. Click the Storage tab > Disks.
4. Click the Actions button next to the disk you want to move to another data store, then click the Import link.
5. On the screen that appears, select a target data store from a drop-down box.

You can only migrate disks to data stores in data store zones assigned to your billing plan.

6. Click Start Migrate.

You cannot migrate a disk to a data store with less capacity than the disk size!
If you move an 850GB disk between aggregates with 10GB actual usage, the 'dd' image of the local volume manager will take 850GB space, because the entire local volume manager is copied, including zero 'd space which may not be able to be recovered.
2.7.13.4 Delete vCenter Virtual Server Disks
To delete a disk:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Make sure your virtual server is powered off, then click its label to open its details screen.
3. Click the Storage > Disks tab.
4. Click the Actions button next to the disk you want to delete, then click Delete.

2.7.14 vCenter Virtual Server Statistics
For your convenience, the system tracks VS performance and generates statistics on:
- VS CPU Utilization
- VS Billing statistics
- Interface Usage
- Disk IOPS

2.7.14.1 vCenter Virtual Server CPU Utilization
OnApp tracks CPU usage for virtual servers and generates charts that help analyze VS performance.
The charts show the total CPU usage for all the cores of this particular VS for a specified time period. The vertical axis shows the CPU usage percentage (CPU percentage is the core-independent quantity). The horizontal axis defines a time period.

To see CPU usage statistics:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Overview > CPU Usage.
4. On the screen that appears, the top chart shows CPU usage for the last 24 hours. The bottom chart shows usage for the last three months (if there is enough data). If there less data available, the chart will show utilization for the time available.
5. Tick the Show in My Timezone box to show bandwidth statistics according to your profile's time zone settings.
6. To zoom into a time period, click and drag in a chart. Click the Reset Zoom button to zoom out again.

To see what percentage of compute resource's CPU resource a VS takes, go to your Control Panel > Cloud > Virtual Servers menu and click the label of the VS you're interested in. On the screen that appears, the CPU(s)/Shares parameter displays the amount of CPU resource given to this VS.

2.7.14.2 vCenter Virtual Server Billing Statistics
OnApp has a record of all the charges applied to your VSs for the last three month period. If a virtual server was created less than three months ago, statistics are recorded for the VS's existence to date. You can view all statistics available, or those for a shorter period by setting a Start and End time.
To view billing statistics for a virtual server:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Click the label of the virtual server you're interested in.
3. Click the **Overview** > **Billing Statistics** tab.
4. Set Start and End time. By default the statistics are generated for the last three months or the actual VS existence period.
5. Tick the **Show in my Timezone** box to show bandwidth statistics according to your profile's timezone settings.
6. On the page that appears:
   - **Date** – particular date and time for the generated statistics
   - **Users** – the virtual server owner. Click the owner name to see the User Profile (user details)
   - **Virtual Servers** – the virtual server name with the total due for VS resources (CPU priority, CPUs, memory and template resources) for the point of time specified in the Date column.
   - **Network Interfaces Usage** – the total due for the network interfaces used by this VS for the point of time specified in the Date column. Click the network interface name to see its details.
   - **Disks Usage**– the list of disks assigned to this VS with the total due for the disk space resources (disk size, data read/written, reads/writes completed) for the point of time specified in the Date column. Click the disk name to see its details.
   - **Costs** – the total due for the Virtual servers, Network Interfaces and Disks resources at the point of time specified in the Date column.

Scroll down to see Total Amount (the total due for the whole billing statistics period).

2.7.14.3 vCenter Virtual Server Network Interface Statistics

OnApp tracks network usage for virtual servers and generates charts that help analyze network performance. To see network utilization statistics for a virtual server:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Click the label of the virtual server you're interested in.
3. Click the **Networking** > **Network Interfaces** tab.
4. Click the **Statistics** (chart) icon next to the network you're interested in.
5. On the screen that appears, the top chart shows bandwidth usage for the last 24 hours. The bottom chart shows usage for the last three months.
6. To zoom into a time period, click and drag in a chart. Click the **Reset Zoom** button to zoom out again.

2.7.14.4 vCenter Virtual Server Disk IOPS

The system tracks IOPS (Input/Output Operations per Second) for virtual servers and generates charts that help analyze VS disk performance. The data presented in the chart are for the periods during which the statistics was gathered, typically 3 minutes. To see IOPS for a virtual server:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Click the label of the virtual server you're interested in.
3. Click the **Storage** > **Disks** tab.
4. Next to the necessary disk, click the **Actions** button and select the **IOPS** option.
5. There are four charts on the screen that appears:
   - Instant IOPS - summary of input/output operations per minute
6. To zoom into a time period, click and drag in a chart. Click the Reset zoom button to zoom out again.

The OnApp API allows you to limit the Hourly IOPS and Hourly data by setting the limit=N parameter, where the N variable is the number of hours for which the charts will display the info.

2.7.15 Manage vCenter Virtual Server Recipes

Established connection between vCenter and ESXi compute resources and having VMware tools pre-installed on virtual servers is required for running recipes on vCenter virtual servers

To manage virtual server recipes:
1. Go to your Control Panel > Virtual Servers menu.
2. Click the label of the server you're interested in.
3. Click the Overview tab, then choose Recipes.
4. The screen that follows shows details of all the recipes in the Control Panel:
   - The left pane shows the list of recipes available in the bucket organized into recipe groups.
   - The right pane displays the list of events to which the recipes can be assigned to. Click the arrow button next to event to expand the list of recipes assigned to it.

Assign recipe

Use drag and drop feature to assign a recipe to a desired event.

You can assign virtual server recipes to the following events:

- **VS provisioning** - run the recipe during the virtual server provisioning
- **VS network rebuild** - run the recipe while rebuilding a network
- **VS disk added** - run the recipe while adding a disk to the virtual server
- **VS network interface added** - run the recipe while adding a network interface to the virtual server
- **VS network interface removed** - run the recipe while deleting a network interface from the virtual server
- **VS disk resized** - run the recipe while resizing a virtual server disk
- **VS resize** - run the recipe while resizing the virtual server
- **VS IP address add** - run the recipe while adding an IP address the virtual server
- **VS IP address remove** - run the recipe while removing an IP address from the virtual server
- **VS start** - run the recipe while starting the virtual server
- **VS reboot** - run the recipe while rebooting the virtual server
- **VS hot migrate** - run the recipe during the hot migration of the virtual server
- **VS hot full migrate** - run the recipe during the hot migration of the virtual server with disk
- **VS failover** - run the recipe during the failover process

**To use drag and drop:**
1. Click the arrow button in front of the required event to unfold it.
2. Select the required recipe in the left pane and hold it down with the left mouse button.
3. Drag the recipe up to the right pane and release the mouse button to drop the recipe and add it to the required event.

**Remove recipe**

To remove recipe:

1. Click the arrow button in front of the required event to view the list of recipes assigned to it.
2. Click the **Delete** button next to the recipe you want to remove.

**2.7.16 Manage vCenter Virtual Server Custom Variables**

SSH connection between VS and Control Panel is required for running recipes on vCenter virtual servers.

You can define custom variables for particular virtual servers. Each custom variable is a name-value set that can be used during the virtual server recipe implementation. Custom variables are set on a per server basis. You can create custom variables during the virtual server creation or via the virtual server **Overview** menu.

**To create a new custom variable:**
1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. You'll see a list of all virtual servers in your cloud. Click the name of a virtual server for which you want to create a variable.
3. On the virtual server details screen, click the **Overview** tab, then choose **Recipes Variables**.
4. On the screen that appears, click the "+" button.
5. Specify the recipe name and its value.
6. Move the **Enabled** slider to the right to allow use of this recipe.
7. Click **Save**.

To edit a custom variable, click the **Edit** icon next to the required variable and change its details.

To delete a custom variable, click the **Delete** icon next to the variable you want to remove. You will be asked to confirm the deletion.

It is possible to set custom variables for image templates, as well as for virtual servers. Virtual server custom variables will always overlay template custom variables.
2.7.17 Manage Virtual Server Snapshots

VMware snapshot tools are used to perform snapshots by simply locking the filesystem disk (vmdk) and creating a new VMware disk with the changes made alongside, so the procedure for virtual servers running under VMware looks like: vmdk + vmdk(1) + vmdk(#).

To view the list of VS Snapshots:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the server you want to back up.
3. Click the Tools button > Snapshots.
4. On the screen that appears, you'll see the list of all VS snapshots.

To create a snapshot for vCenter VS:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the server you want to back up.
3. Click the Tools button > Snapshots.
4. Click the Create New Snapshot button.
5. Give your snapshot a name.
6. Click Create Snapshot button.

To delete a VS snapshot, click the Actions button next to the required snapshot, then click Delete.

2.7.18 vCenter Virtual Server Console

- To be able to use the MKS console on vCenter virtual servers, VSs must not be configured for VNC access in vCenter.
- In order for a vCenter VS console to work, the system_host parameter in /onapp/interface/config/on_app.yml file must be changed from its default value onapp.com to an appropriate FQDN or IP address of the Control Panel server.

You can use the virtual server console to manage your virtual servers in command line mode. To use the VS console:
1. Go to Control Panel > Cloud > Virtual Servers menu.
2. Click the Label of appropriate Virtual Server.
3. Go to Console tab and click MKS. The console window will appear.

2.8 OnApp OVA Import to vCenter

For more information on how to manage OVAs, refer to the Administration Guide.

OnApp OVA template store is used as a central repository to deploy templates into vCenter environments. These templates are stored on the OnApp CP server or backup server and are
uploaded to vCenter during deployment via the OVA import procedure. OVA is an archive containing files from the Open Virtualization Format (OVF) package. OVF is an open-source standard for packaging and distributing software applications for virtual servers.

The OVA import procedure involves the following steps:

1. **Uploading OVA to CP**
2. **Converting OVA into a vCenter template**
3. **Adding the template to the template store**
4. **Building a virtual server from the template**

- The template OVF hardware version should be equal to or lower than the version of vCenter compute resource.
- If the OVF template is exported from VirtualBox, the template hardware version should be changed from 'virtualbox-X' to 'vmx-X'.

### 2.8.1 Upload OVA

To upload OVAs to your cloud:

1. Go to your **Control Panel > Cloud > Templates** menu on the left navigation panel.
2. Click the **OVA List** link from the expanding menu.
3. On the page that loads, click the **Upload OVA** button at the bottom of the screen.
4. Fill in the following details:
   - **Label** - enter a name for OVA
   - **Backup server** - select the backup server where OVA will be stored
     
     It is required to select a backup server where the OVA template should be stored. If the backup server is not selected, it will not be possible to upload an OVA.
     
   - **Version** - fill in the version of the OVA
   - **Min memory size** - specify the minimum required RAM for the OVA (128 MB by default). If you set the RAM value that is smaller than in the OVA file, this amount will be overwritten by the real memory size from the OVA file after upload. If you set the value that is bigger than the RAM in the OVA file, the settings will be applied.

5. Click **Next**. On the page that appears, click **File** or **File URL** tab depending on the upload method:
   - **File** - click **Choose File** to select the required OVA file from your file system. The yellow infobox will show the maximum file size for OVAs. The maximum upload size is pre-configured at **Admin > Settings > Configuration** (the **Max upload size** field). Click the **Upload OVA** button.
   - **File URL** - select this tab if you want to upload OVA from URL and specify the link from which the OVA archive will be uploaded.
6. Click **Save** to upload the OVA archive.

If an operating system of OVA is Linux and incremental backups are activated on your CP, you will not be able to upload the OVA file. To solve this issue, go to your Control Panel > **Admin > Settings > Configuration > Backups/Templates** tab and enable the *Store extended attributes* slider.

After you upload OVA to the cloud, it can be found at **Cloud > Templates > OVA List > My OVAs** tab. The OVAs uploaded by your users are under the **User OVAs** tab. You can convert the uploaded OVA into a vCenter-based template by following steps from the next section.

### 2.8.2 Convert OVA

The initially-uploaded OVA file is saved without the attached virtualization so that you can convert it more than once into all supported virtualization formats. To convert the uploaded OVA archive into a vCenter-based template, follow the next steps:

1. Go to your **Control Panel > Cloud > Templates** menu from the left navigation pane.
2. Click **OVA List** on the menu.
3. Click the **Actions** icon > **Convert** next to the required OVA file.
4. In the open box, select the vCenter virtualization format and fill in the following details:
   - **Label** - enter a name for a new OVA file that will be created on the basis of the initially-uploaded one
   - **Operating system** - select the operating system of the OVA (Linux, Windows or Other). Choose the Other operating system if you want to upload an OVA with an operating system other than Windows or Linux.
   - **Operating system distro** - select the operating system distribution of the OVA
   - **Architecture** - select the architecture of the OVA (x86 or x64)
   - **Edition** - select the edition of the OVA (for Windows-based OVAs only)
   - **R2** - move the slider to the right if you want to use the updated release of Windows OS distribution (for Windows-based OVAs only)
   - **Initial username** - provide a username for the guest operating system
   - **Initial password** - provide a password for the guest operating system
   - **Make public** - move the slider to the right if you want to make the OVA available to all users in the cloud
5. Click **Save** to convert OVA into the vCenter virtualization format.

- The OVA file is locked for the time period while it is being converted. You can unlock the OVA file to make the following actions instantly available: edit OVA and delete OVA. To unlock OVA, click the **Actions** button and select the **Unlock** option.
The limits on the number of OVAs and disk space allocated for storing OVAs are bound to a user who uploaded an OVA file. Therefore, when the OVA file is being converted, the bucket limits are checked for the user who uploaded OVA and not for the user who converts it.

When the uploaded OVA file is converted into a template, you can proceed to add this template to the template store and then build a VS from this template.

2.9 Import vCenter Templates

As you add a vCenter compute resource to OnApp, the vCenter templates are also imported and stored at the vCenter Template List page in the Pending state. To finalize the import of the vCenter templates and be able to manage them, it is required to update the templates on the OnApp side by specifying the template's credentials.

Before importing templates from vCenter, make sure that the following conditions are met:
1. Install VMware tools inside the VS by following the VMware instructions.
2. Make sure that Perl is installed on this VS.
   Otherwise, the functionality of the imported templates may be limited.

2.9.1 Update template

To change the status of the vCenter templates to Active:
1. Go to your Control Panel > vCenter Template List.
2. Next to the required template, click the Actions button > select the Edit template option.
3. In the initial username and password fields, indicate the template credentials, set during the template's creation.
4. Click the Save button.
   The template's status will change to Active, and it will be possible to select this template while adding a vCenter template to the Template Store.

2.9.2 Add template to Template Store

To add a vCenter template to the Template Store:
1. Go to your Control Panel > Templates > Template Store.
2. Select the label of the Template Group you need to add the vCenter template to.
3. Click the ‘+’ button in the Actions column.
4. Select the Add vCenter Template option from the dropdown.
5. Select the vCenter template from the list of available vCenter templates in the dropdown.
6. Click the Save button to save the changes.
Once finished, the template will be available to select on the Templates step of the VS Creation wizard.

- Please note that for the Windows templates imported from vCenter it is impossible to select the MAK license during the VS creation. Instead, select the **Your own license** option and manually indicate the License Key.
- Windows 2008 and Windows 2008 R2 templates are not supported.

### 2.10 Manage vCenter Templates

After you [import a vCenter template](#) and update it's credentials on OnApp side, you can assign system service add-ons and recipes to this template.

Windows 2008 and Windows 2008 R2 templates are not supported.

#### 2.10.1 Manage vCenter Template System Service Add-ons

To assign system service add-ons to a vCenter template:

1. Go to your **Control Panel > Cloud > vCenter Template list**. You'll see a list of imported vCenter templates, available on your cloud.
2. Next to the template in question click the **Actions** button and select the **Manage Service Add-ons** option.
3. Click the '+' button.
4. The screen that follows shows the list of the available system service add-ons organized into groups. Click the arrow button next to a group to expand the list of add-ons assigned to it.
5. Click the label of the necessary system service add-on to see its details:
   - **Label**
   - **Type** - user or system
   - **Description**
   - **Price**
   - **Apply to existing Virtual Servers** - move the slider to the right to assign the system service add-on to all the VSs in your cloud built from this template
6. Click the **Assign** button to finish.
2.10.2 Manage vCenter Template Recipes

To assign system service add-ons to a vCenter template:

1. Go to your Control Panel > Cloud > vCenter Template list. You'll see a list of imported vCenter templates, available on your cloud.

2. Next to the template in question click the Actions button and select the Manage Recipes option.

Use drag and drop feature to assign a recipe to a desired event.

You can assign template recipes to the following events:

- **VS provisioning** - run the recipe during the virtual server provisioning
- **VS disk added** - run the recipe while adding a disk to the virtual server
- **VS network interface added** - run the recipe while adding a network interface to the virtual server
- **VS network interface removed** - run the recipe while deleting a network interface from the virtual server
- **VS disk resized** - run the recipe while resizing a virtual server disk
- **VS resize** - run the recipe while resizing the virtual server
- **VS IP address add** - run the recipe while adding an IP address the virtual server
- **VS IP address remove** - run the recipe while removing an IP address from the virtual server
- **VS start** - run the recipe while starting the virtual server
- **VS reboot** - run the recipe while rebooting the virtual server

To use recipes with own Windows templates, the templates must be version 3.1 or later.
Note that a VS related recipe is always executed first, for example:

1. You have two recipes, one assigned to a template and another assigned to a VS.
2. You assign both of them to a required event.
3. After the VS is built, the VS related recipe is run first.
4. Next, the template recipe is run.

This execution order is also relevant when the VS related recipe and template recipe are both assigned to the same event.

To use drag and drop:

1. Click the arrow button in front of the required event to unfold it.
2. Select the required recipe in the left pane and hold it down with the left mouse button.
3. Drag the recipe up to the right pane and release the mouse button to drop the recipe and add it to the required event.

2.10.3 Delete Recipe

To remove a recipe:

1. Click the arrow button in front of the required event to view the list of recipes assigned to it.
2. Click the Delete button next to the recipe you want to remove.

2.11 NSX Integration

OnApp integration with VMware NSX Data Center delivers a complete L2-L7 networking and security virtualization platform providing you with agility and automation. This feature allows you to configure Advanced Edge services within the OnApp UI. Also, you receive access to full end-to-end provisioning instead of a limited one.

- Please note that in order to use NSX for vCenter, the corresponding feature set has to be enabled in your license.
- In OnApp 6.2, limited NSX support is being added for vCenter in beta mode. Please speak to your account manager to discuss pricing and your plan for upgrading.

In this chapter, you can find the following information on how to manage NSX integration with vCenter:

- NSX Manager in OnApp
- NSX Firewalls
NAT Rules for NSX Integration
NSX Load Balancers
NSX IPSec VPN
NSX L2 VPN

2.11.1 NSX Managers in OnApp
The NSX Manager is used to deploy a universal controller cluster that provides the control plane for the NSX environment. At OnApp, you can import NSX manager with limited functionality available and set vCenter credentials to gain access to full functionality. Once imported, it allows you to view and edit imported vCenter edges in OnApp interface.

- This functionality is available for users with the OnApp Administrator role.
- For vCenter, NSX Manager is enabled by default but you have to import and sync it with NSX edge first.
- Ensure that Any action on NSX manager permission is on before starting using NSX integration. For more information about permissions refer to the permissions section of this guide.

On this page:

- View NSX Manager Details
- Import NSX Manager to OnApp
- View NSX Edges

See also:
- NSX Firewalls
- NAT Rules for NSX Integration
- NSX Load Balancers

2.11.1.1 View NSX Manager Details
To view the details of a particular NSX Manager:
1. Go to your Control Panel > Admin > Settings menu.
2. Click the SDN Managers icon, then click the vCenter/vCloud tab.
3. Click the label of an NSX manager to view its details:
   - Label - the name of the NSX manager
   - Resource - the hostname of the controller
   - Type - the type of manager, which is NSX
   - Version - build and version number of NSX manager
   - IP Address - the IP address of the controller
   - Uptime - the time the NSX manager has been working and available
   - Status - powered on/off status of NSX manager
2.11.1.2 Import NSX Manager to OnApp

Although NSX is enabled by default in OnApp, two steps are required to activate and start using this functionality. First, you need to set NSX credentials in order to communicate with NSX. Second, you need to import vCenter edges to OnApp.

To import NSX manager to OnApp:
1. Go to your Control Panel > Admin > Settings menu.
2. Click the SDN Managers icon, then click the vCenter/vCloud tab.
3. Click the Actions button next to the NSX manager to view its options.
4. First, click Set credentials.
5. In the dialogue box that pops up, enter login and password.
6. Next, click the Import option.

After the transaction is completed, all the NSX items will be imported to OnApp Control Panel. For instance, vCenter edges will be available at Control Panel > Cloud > Edges menu.

7. Click the Save button.

After NSX manager is successfully imported to OnApp interface, you can proceed to configuration of NSX firewalls and networks and start using edges created at the vCenter side in OnApp interface.
2.11.1.3 View NSX Edges

Edges work as vCloud Director Edge Gateways for vCenter instances, which serve as a perimeter virtual router. You can manage edge services (Firewall, NAT, Load Balancers etc.) via OnApp interface.

NSX Edges are imported from vCenter side.

To view the vCenter edge details:

1. Go to your Control Panel > Cloud > Edges.
2. Click the label of the necessary edge to see its details.
3. On the page that appears, you will see the following details of the edge:
   - **Label** - label of the vCenter edge
   - **vCenter** - hostname of the vCenter instance
   - **State** - deployed or undeployed
   - **Status** - power status, active or inactive

   **Network Interfaces**
   - **Label** - label of the network interface
   - **Type** - uplink or trunk
   - **Network** - label of the network

2.11.2 NSX Firewalls

NSX Firewall monitors the North-South traffic to provide perimeter security functionality including firewall, Network Address Translation (NAT), and site-to-site IPSec VPN functionality.

OnApp provides you with the possibility to manage NSX firewall service separately for each vCenter edge in your cloud. It is possible to enable and disable firewall for the entire edge or enable some of the rules on the list. You can configure the details of sources and destinations for each rule.

There are two major types of firewall rules in OnApp: internal (created on vCenter side and imported to OnApp) and user-defined (created on OnApp side).
NSX firewalls may be configured for an existing vCloud edge gateway or vCenter edge. For more information on creation and import of the aforementioned instances, see vCloud Edge Gateways and Edges sections of this guide.

On this page:

- Create Firewall Rule
- Edit Firewall Rule
- Delete Firewall Rule

See also:
- NSX integration
- Adding NSX Manager to OnApp
- NSX Load Balancers

2.11.2.1 Create Firewall Rule

To add a new firewall rule:

1. Go to your Control Panel > Cloud > Edges menu.
2. Click the label of the necessary Edge.
3. Click the Firewall tab to see the list of the firewall rules.
4. Click the button above the table. A new line will appear on the list.
5. In the line that appeared, specify the following parameters:
   - click to enable the rule.
   - Rule name - click to add the name of the rule.
   - Sources - as you hover over the Sources column space in the required line, the and buttons will appear:
     - Click the button to add a source IP address this firewall rule will be active for. This can be an IP address, CIDR, IP range, "any", "internal" or "external". This field is not case sensitive. Click the Apply IP button to save the changes.
     - Click the button to add the following types of destinations for this rule:
       - Network interfaces - select the necessary network interfaces from the list
       - Virtual machines - select the necessary virtual servers from the list
       - Networks - select the necessary networks from the list
       - IP sets - select the necessary options from the list of IP sets imported from vCenter side
       - Security groups - select the necessary options from the list of security groups imported from vCenter side
       - Click the Apply rules button to save the changes.
The **Toggle exclusion** button appears only if there are any sources already added to the list. Click this button to exclude all the specified sources, so that the rule will accept as a source all possible options, except the ones you included. Once this option is enabled, the **Any but** tag appears before the list of sources.

1. **Destinations** - as you hover over the Destinations column space in the required line, the ▼ and ▼ buttons will appear:
   - Click the ▼ button to add a destination IP addresses this firewall rule will be active for. This can be an IP address, CIDR, IP range, "any", "internal" or "external". This field is not case sensitive. Click the **Apply IP** button to save the changes.
   - Click the ▼ button to configure the following types of destinations for this rule:
     - **Network interfaces** - select the necessary network interfaces from the list.
     - **Virtual machines** - select the necessary virtual servers from the list.
     - **Networks** - select the necessary networks from the list.
     - **IP sets** - select the necessary options from the list of IP sets imported from vCenter side.
     - **Security groups** - select the necessary options from the list of security groups imported from vCenter side.
     - Click the **Apply rules** button to save the changes.

   The **Toggle exclusion** button appears only if there are any destinations already added to the list. Click this button to exclude all the specified destinations, so that the rule will accept as a destination all possible options, except the ones you included. Once this option is enabled, the **Any but** tag appears before the list of destinations.

   - **Services** - click the ▼ button to open up a pop up window. Once it appears, specify the following values:
     - **Protocol** - select TCP, UDP, ICMP, or Any.
     - **Source port** - insert the source port (from 1 to 65535).
     - **Destination port** - insert the destination port (from 1 to 65535).

**If you don't specify any source, destination, or service value, it will be displayed as "any" by default.**

1. **ACCEPT** – click to specify that the traffic from or to the specified source(s), destination(s), and service(s) that will be accepted by the firewall.

1. **DENY** – click to specify that the traffic from or to the specified source(s), destination(s), and service(s) that will be denied by the firewall.

1. **Logging** - move the slider to the right to enable logging for this rule.

6. Click the **Save** button above the table to apply the changes.
- You may filter the rules in the list by name, source, destination, and service.
- To select all firewall rules on the list, hover over the top left corner of the table, and tick the checkbox that appears.
- In case you want to revert the last changes applied, click the **Undo changes** button located above the table.
- To see the rules of the user-defined type only, click the icon above the table.
2.11.2 Edit Firewall Rule

To edit a firewall rule:

1. Go to your Control Panel > Cloud > Edges menu.
2. Click the label of the necessary Edge.
3. Click the Firewall tab.
4. On the page that appears, you will see the list of firewall rules for this edge. Find the necessary rule and make the necessary changes in the corresponding line.

**Click to view the description of parameters available for editing.**

- **X** - click to enable the rule. If the rule is enabled, click the button to disable it.
- **Rule name** - click to change the name of the rule.
- **Sources** - as you hover over the Sources column space in the required line, the , , and buttons will appear:
  - Click the button to add a source IP address this firewall rule will be active for. This can be an IP address, CIDR, IP range, "any", "internal" or "external". This field is not case sensitive. Click the Apply IP button to save the changes.
  - Click the button to configure the following types of destinations for this rule:
    - **Network interfaces** - select the necessary network interfaces from the list.
    - **Virtual machines** - select the necessary virtual servers from the list.
    - **Networks** - select the necessary networks from the list.
    - **IP sets** - select the necessary options from the list of IP sets imported from vCenter side.
    - **Security groups** - select the necessary options from the list of security groups imported from vCenter side. Click the Apply rules button to save the changes.
  - the Toggle exclusion button appears only if there are any sources already added to the list. Click this button to exclude all the sources except the ones added to the list. Once this option is enabled, the Any but tag appears before the list of sources.
a.  

- **Destinations** - as you hover over the Destinations column space in the required line, the ▲, ▼ and + buttons will appear:
  - Click the ▲ button to add a destination IP addresses this firewall rule will be active for. This can be an IP address, CIDR, IP range, "any", "internal" or "external". This field is not case sensitive. Click the Apply IP button to save the changes.
  - Click the + button to configure the following types of destinations for this rule:
    - Network interfaces - select the necessary network interfaces from the list.
    - Virtual machines - select the necessary virtual servers from the list.
    - Networks - select the necessary networks from the list.
    - IP sets - select the necessary options from the list of IP sets imported from vCenter side.
    - Security groups - select the necessary options from the list of security groups imported from vCenter side.
      Click the Apply rules button to save the changes.
  - The Toggle exclusion button appears only if there are any destinations already added to the list. Click this button to exclude all the destinations except the ones added to the list. Once this option is enabled, the Any but tag appears before the list of destinations.

- **Services** - click the + button to open up a pop up window. Once it appears, specify the following values:
  - **Protocol** - select TCP, UDP, ICMP, or Any.
  - **Source port** - insert the source port (from 1 to 65535).
  - **Destination port** - insert the destination port (from 1 to 65535).

If you don't specify any source, destination, or service value, it will be displayed as "any" by default.

a.  

- **ACCEPT** – click to specify that the traffic from or to the specified source(s), destination(s), and service(s) that will be accepted by the firewall.
- **DENY** – click to specify that the traffic from or to the specified source(s), destination(s), and service(s) that will be denied by the firewall.
- **Logging** - move the slider to the right to enable logging for this rule.

5. Click the Save button above the table to apply the changes.

**2.11.2.3 Delete Firewall Rule**
To delete a firewall rule:
1. Go to your Control Panel > **Cloud** > **Edges** menu.
2. Click the label of the necessary Edge.
3. Click the **Firewall** tab.
4. On the page that appears, you will see the list of firewall rules. Select a rule from the list, and then click the button above the table.
5. Click the **Save** button above the table to apply the changes.

2.11.3 **NAT Rules for NSX Integration**

vCenter NAT (Network Address Translation) service translates source or destination IP addresses and port numbers. In the most common case, you associate a NAT service with an uplink interface on an Edge so that addresses on organization VDC networks are not exposed on the external network.

You can view/create/edit/delete NAT rules using OnApp Control Panel.

---

### On this page:

- Create NAT Rules
- Edit NAT Rule
- Delete NAT Rules

See also:

- NSX Firewalls

---

2.11.3.1 **Create NAT Rules**

To add a new NAT rule for NSX integration:

1. Go to your Control Panel > **Cloud** > **Edges** > Edge label > **NAT** tab.
2. Click the "+" button.
3. On the page that appears specify the following parameters:

   For DNAT rules:
   
   - **Applied on** - select the vCloud Director external network where the rule will be applied
   - **Protocol** - select the type of protocol (TCP, UDP, ICMP or Any)
   - **Original IP** - specify the original IP address to apply this rule on
   - **Original port** - specify the port of original IP address
   - **Translated IP** - specify the IP address to translate the addresses of outgoing packets to
   - **Translated port** - specify the port of translated IP address
   - **Description** - add description if any

   For SNAT rules:

   1. **Applied on** - select the vCloud Director external network where the rule will be applied
- **Original IP** - specify original IP address to apply this rule on and click the "?" icon to configure IP nets and IP ranges
- **IP Net** - select an IP net from which the original IP address should be assigned
- **IP Range** - select an IP range from which the original IP address should be assigned
- **Translated IP** - specify the IP address to translate the addresses of outgoing packets to and click the "?" icon to configure IP nets and IP ranges
- **IP Net** - select an IP range from which the translated IP address should be assigned
- **IP Range** - select an IP range from which the translated IP address should be assigned
- **Description** - add description if any

4. Click the **Apply Rules** button to save the changes.
To edit a NAT rule:

1. Go to your Control Panel > Cloud > Edges > Edge label > NAT tab.
2. Click the icon next to the NAT rule, which you want to edit.
3. On the page that appears change the following parameters:
   For DNAT rules:
- **Applied on** - select the vCloud Director external network where the rule will be applied
- **Protocol** - select the type of protocol (TCP, UDP, ICMP or Any)
- **Original IP** - specify the original IP address to apply this rule on
- **Original port** - specify the port of original IP address
- **Translated IP** - specify the IP address to translate the addresses of outgoing packets to
- **Translated port** - the port of translated IP address
- **Description** - add description if any

For SNAT rules:

1. **Applied on** - select the vCloud Director external network where the rule will be applied
2. **Original IP** - specify original IP address to apply this rule on and click the "?" icon to configure IP nets and IP ranges
3. **IP Net** - select an IP net from which the original IP address should be assigned
4. **IP Range** - select an IP range from which the original IP address should be assigned
5. **Translated IP** - specify the IP address to translate the addresses of outgoing packets to and click the "?" icon to configure IP nets and IP ranges
6. **IP Net** - select an IP net from which the translated IP address should be assigned
7. **IP Range** - select an IP range from which the translated IP address should be assigned
8. **Description** - add description if any

4. Click the **Apply Rules** button to save the changes.
2.11.3.3 Delete NAT Rules

To delete a NAT rule:

1. Go to your Control Panel > Cloud > Edges > Edge label.
2. Click the NAT tab.
3. On the page that appears you will see the list of all NAT rules.
4. Select a rule from the list, and then click the button above the table.
5. Click the Save button to apply the changes.

2.11.4 NSX Load Balancers

The NSX Edge load balancer enables high-availability service and distributes the network traffic load among multiple servers. It 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.

You map an external, or public, IP address to a set of internal servers for load balancing. The load balancer accepts TCP, UDP, HTTP, or HTTPS requests on the external IP address and decides which internal server to use. Port 80 is the default port for HTTP and port 443 is the default port for HTTPTs.
2.11.4.1 Before you begin

- You must have a working NSX Edge instance before you can configure load balancing. For information on setting up NSX Edge, see NSX Edge Configuration, or vCloud Director edge gateways.
- For information on configuring an NSX Edge certificate, see Certificate Authentication.
- Select the layer of load balancing (L7 or L4) by clicking on the Type selection icon in the top right corner of the screen.
- Select the level of logging from the Log level drop-box in the top right corner of the screen. Note that Emergency is the least detailed level of logging, and Debug is the most detailed level of logging.

On this page:

- Before you begin
- Add Application Profiles
- Edit Application Profiles
- Add Service Monitors
- Edit Service Monitors
- Add Server Pools
- Edit Server Pools
- Add Application Rules
- Edit Application Rules
- Add Virtual Servers
- Edit Virtual Servers

2.11.4.2 Add Application Profiles

To add an application profile:

1. Go to Control Panel > vCenter > Edges > Edge label > Load Balancers tab.
2. Select Application Profiles tab.
3. Click the "+" button on the top of the page.
4. On the page that appears specify the following parameters:
   - Name - enter the name of the application profile
   - Type - select the type of traffic (TCP, HTTP, HTTPS or UDP). Depending on the type of traffic, specify the following parameters:

   **Click to view the list of parameters**

   For TCP or UDP
   - Persistence - select the persistence type (Source IP, MSRDP or none)
   - Expires - enter the persistence expiration time in seconds. The default value is 60 seconds.

   For HTTP
   - Persistence - select the persistence type (Source IP, Cookie or none)
- **HTTP Redirect URL** - enter the URL to which you want to redirect the HTTP traffic
- **Mode** - if you selected the Cookie persistence type, select the mode of inserting the cookie (insert, prefix or App session)
- **Cookie name** - if you selected the Cookie persistence type, enter the cookie name
- **Expires** - enter the persistence expiration time in seconds. The default value is 60 seconds.
- **Insert X-Forwarded-For HTTP header** - move the slider to the right to identify the originating IP address of a client connecting to a Web server through the load balancer

For HTTPS
- **Enable SSL Passthrough** - move the slider to the right to enable SSL passthrough
- **HTTP Redirect URL** - enter the URL to which you want to redirect the HTTP traffic
- **Persistence** - select the persistence type (Source IP, Cookie or none)
- **Mode** - if you selected the Cookie persistence type, select the mode of inserting the cookie (insert, prefix or App session)
- **Cookie name** - if you selected the Cookie persistence type, enter the cookie name
- **Expires** - enter the persistence expiration time in seconds. The default value is 60 seconds.
- **Enable pool side SSL** - move the slider to the right to enable the HTTPS communication between the load balancer and the back-end servers
- **Insert X-Forwarded-For HTTP header** - move the slider to the right to identify the originating IP address of a client connecting to a Web server through the load balancer
- **Cipher** - enter a cipher algorithm
- **Client Auth** - select whether to ignore or accept client authentication
- **Virtual server certificates** - select server certificates, CA certificates and CRLs certificates to authenticate the load balancer from the server side

5. Click the **Save** button.
2.11.4.3 Edit Application Profiles

To edit application profile:

1. Go to Control Panel > vCenter > Edges > Edge label > Load Balancers tab.
2. Select Application Profiles tab.
3. Click the icon next to the application profile you want to edit.
4. On the page that loads, edit the following parameters:
   o **Name** - enter the name of the application profile
   o **Type** - select the type of traffic (TCP, HTTP, HTTPS or UDP). Depending on the type of traffic, specify the following parameters:

   **Click to view the list of parameters**

   For TCP or UDP
   - **Persistence** - select the persistence type (Source IP, MSRDP or none)
   - **Expires** - enter the persistence expiration time in seconds. The default value is 60 seconds.

   For HTTP
   - **Persistence** - select the persistence type (Source IP, Cookie or none)
   - **HTTP Redirect URL** - enter the URL to which you want to redirect the HTTP traffic
   - **Mode** - if you selected the Cookie persistence type, select the mode of inserting the cookie (insert, prefix or App session)
   - **Cookie name** - if you selected the Cookie persistence type, enter the cookie name
Expires - enter the persistence expiration time in seconds. The default value is 60 seconds.

Insert X-Forwarded-For HTTP header - move the slider to the right to identify the originating IP address of a client connecting to a Web server through the load balancer.

For HTTPS

Enable SSL Passthrough - move the slider to the right to enable SSL passthrough.

HTTP Redirect URL - enter the URL to which you want to redirect the HTTP traffic.

Persistence - select the persistence type (Source IP, Cookie or none).

Mode - if you selected the Cookie persistence type, select the mode of inserting the cookie (insert, prefix or App session).

Cookie name - if you selected the Cookie persistence type, enter the cookie name.

Expires - enter the persistence expiration time in seconds. The default value is 60 seconds.

Enable pool side SSL - move the slider to the right to enable the HTTPS communication between the load balancer and the back-end servers.

Insert X-Forwarded-For HTTP header - move the slider to the right to identify the originating IP address of a client connecting to a Web server through the load balancer.

Cipher - enter a cipher algorithm.

Client Auth - select whether to ignore or accept client authentication.

Virtual server certificates - select server certificates, CA certificates and CRLs certificates to authenticate the load balancer from the server side.

5. Click the Save button.

2.11.4.4 Add Service Monitors

To add service monitors:

1. Go to Control Panel > vCenter > Edges > Edge label > Load Balancers tab.

2. Select Service Monitoring tab.

3. Click the "+" button on the top of the page.

4. On the page that appears specify the following parameters:

   - Name - enter a name for the service monitor
   - Interval - enter the interval in seconds in which a server is to be tested
   - Timeout - the maximum time in seconds within which a response from the server must be received
   - Max retries - enter the number of times the server is tested before it is declared DOWN
   - Method - select the method to detect server status from the drop-down menu: GET, OPTIONS, or POST.
   - URL - Enter the URL to GET or POST ("/") by default.)
- **Expected** - Enter the string that the monitor expects to match in the status line of HTTP response in the Expected section. This is a comma-separated list. For example, 200,301,302,401.
- **Send** - enter the string sent to the back-end server after a connection is established. The maximum permitted string length is 256 characters.
- **Receive** - enter the string to be matched. This string can be a header or in the body of the response. When the received string matches this definition, the server is considered UP.
- **Extension** - enter advanced monitor parameters as key=value pairs in the Extension section

5. Click the **Save** button.
2.11.4.5  Edit Service Monitors
To edit service monitors:
1. Go to Control Panel > vCenter > Edges > Edge label > Load Balancers tab.
2. Select Service Monitoring tab.
3. Click the ✏ icon next to the service monitor you want to edit.
4. On the page that loads, edit the following parameters:
   o Name - enter a name for the service monitor
   o Interval - enter the interval in seconds in which a server is to be tested
   o Timeout - the maximum time in seconds within which a response from the server must be received
   o Max retries - enter the number of times the server is tested before it is declared DOWN
   o Method - select the method to detect server status from the drop-down menu: GET, OPTIONS, or POST. (GET, OPTIONS or POST)
   o URL - enter the string that the monitor expects to match in the status line of HTTP response in the Expected section. This is a comma-separated list.
   o For example, 200,301,302,401.
   o Expected - enter the string that the monitor expects to match in the status line of HTTP response in the Expected section. This is a comma-separated list. For example, 200,301,302,401.
   o Send - enter the string sent to the back-end server after a connection is established. The maximum permitted string length is 256 characters.
   o Receive - enter the string to be matched. This string can be a header or in the body of the response. When the received string matches this definition, the server is considered UP.
   o Extension - enter advanced monitor parameters as key=value pairs in the Extension section
5. Click the Save button.

2.11.4.6  Add Server Pools
To add server pools to manage load balancer distribution:
1. Go to Control Panel > vCenter > Edges > Edge label > Load Balancers tab.
2. Select Pools tab.
3. Click the "+" button on the top of the page.
4. On the page that appears specify the following parameters:
   o Name - enter a name of the server pool
   o Description - additional description if any
   o Monitor - select an existing default or custom monitor from the Monitors drop-down menu
   o Transparent - move the slider to the right to make client IP addresses visible to the back-end servers
   o Members - enter the name and IP address of the server member
     ▪ Weight - enter the proportion of traffic this member can handle
- **Monitor port** - enter the monitor port where the member is to receive health monitor pings
- **Port** - enter the port where the member is to receive traffic
- **Min Conn.** - enter the minimum number of concurrent connections that a member must always accept
- **Max Conn.** - enter the maximum number of concurrent connections that the member can handle. If the incoming requests go higher than the maximum, they are queued and wait for a connection to be released.

5. Click the **Save** button.

---

### 2.11.4.7 Edit Server Pools

To edit load balancer pools:

1. Go to **Control Panel > vCenter > Edges > Edge label > Load Balancers** tab.
2. Select **Pools** tab.
3. Click the **edd** icon next to the service monitor you want to edit.
4. On the page that loads, edit the following parameters:
   - **Name** - enter a name of the server pool
   - **Description** - additional description if any
   - **Monitor** - select an existing default or custom monitor from the Monitors drop-down menu
o **Transparent** - move the slider to the right to make client IP addresses visible to the back-end servers

o **Members** - enter the name and IP address of the server member
  - **Weight** - enter the proportion of traffic this member can handle
  - **Monitor port** - enter the monitor port where the member is to receive health monitor pings
  - **Port** - enter the port where the member is to receive traffic
  - **Min Conn.** - enter the minimum number of concurrent connections that a member must always accept
  - **Max Conn.** - enter the maximum number of concurrent connections that the member can handle. If the incoming requests go higher than the maximum, they are queued and wait for a connection to be released.

5. Click the **Save** button.

### 2.11.4.8 Add Application Rules

To add application rules:

1. Go to **Control Panel > vCenter > Edges > Edge label > Load Balancers** tab.
2. Select **Application Rules** tab.
3. Click the "+" button on the top of the page.
4. On the page that appears specify the following parameters:
   - **Name** - enter a name for an application rule
   - **Script** - Type the name and script for the rule. For information about the application rule syntax, see [http://cbonte.github.io/haproxy-dconv/](http://cbonte.github.io/haproxy-dconv/).
5. Click the **Save** button.

### 2.11.4.9 Edit Application Rules

To edit application rules:

1. Go to **Control Panel > vCenter > Edges > Edge label > Load Balancers** tab.
2. Select **Application Rules** tab.
3. Click the icon next to the service monitor you want to edit.
4. On the page that loads, edit the following parameters:
   - **Name** - enter a name for an application rule
   - **Script** - type the name and script for the rule. For information about the application rule syntax, see [http://cbonte.github.io/haproxy-dconv/](http://cbonte.github.io/haproxy-dconv/).
5. Click the **Save** button.

### 2.11.4.10 Add Virtual Servers

To add an NSX Edge internal or uplink interface as a virtual server:

1. Go to **Control Panel > vCenter > Edges > Edge label > Load Balancers** tab.
2. Select **Virtual Servers** tab.

3. On the page that appears you will see the list of virtual servers together with their details:
   - **Name** - enter a name of a virtual server
   - **Application profile** - select application profile associated with this VS from the drop-down menu
   - **Enable virtual server** - move the slider to the right to make this virtual server available for use
   - **Enable acceleration** - move the slider to the right to enable acceleration for the load balancer to use the faster L4 load balancer engine rather than L7 load balancer engine
   - **Description** - add description if any
   - **IP Address** - enter an IP address that the load balancer is listening on
   - **Protocol** - select the protocol that the virtual server handles
   - **Port** - enter the port number that the load balancer listens on
   - **Default pool** - select the default VSs pool
   - **Conn limit** - enter the maximum concurrent connections that the virtual server can process
   - **Conn rate limit** - enter the maximum incoming new connection requests per second
   - **Selected rules** - add the application rule to associate it with the virtual server

4. Click the **Save** button.
To edit virtual servers:
1. Go to Control Panel > vCenter > Edges > Edge label > Load Balancers tab.
2. Select Virtual Servers tab.
3. On the page that appears, edit the following parameters:
- Name - enter a name of a virtual server
- Application profile - select application profile associated with this VS from the drop-down menu
- Enable virtual server - move the slider to the right to make this virtual server available for use
- Enable acceleration - move the slider to the right to enable acceleration for the load balancer to use the faster L4 load balancer engine rather than L7 load balancer engine
- Description - add description if any
- IP Address - enter an IP address that the load balancer is listening on
- Protocol - select the protocol that the virtual server handles
- Port - enter the port number that the load balancer listens on
- Default pool - select the default VSs pool
- Conn limit - enter the maximum concurrent connections that the virtual server can process
- Conn rate limit - enter the maximum incoming new connection requests per second section
- Selected rules - add the application rule to associate it with the virtual server

4. Click the Save button.

2.11.5 NSX IPSec VPN

Internet Protocol Security (IPSec) VPN ensures secure and private communications over Internet Protocol (IP) networks. It authenticates and encrypts IP packets between two end points. A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. The goal is to securely connect two or more LAN networks and allow full communication between them, without any restrictions.

On this page:

- Manage IPSec VPN Service
- Add IPSec VPN Site
- Edit IPSec VPN Site
- Certificate Authentication
- Delete IPSec VPN Site

See also:

- NSX L2 VPN
- NSX Managers in OnApp
- NSX Firewalls

2.11.5.1 Manage IPSec VPN Service

To manage IPSec VPN service for a specific edge:

1. Go to your Control Panel > Cloud > Edges.
2. Click the label of the necessary edge from the list of all edges in your cloud.
3. Go to the **IPSec VPN** tab.
4. You can manage the following options for the entire service for a specific edge:
   - **Service status** - move the slider to the right to enable IPSec VPN service for this edge
   - **Global shared key** - the global pre-shared key (PSK) that is shared by all the sites whose peer endpoint is set to **Any**

   If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting.

   - - click to edit the global shared key
   - - click to preview the global shared key
   - Log level - select one of the following options, where **Emergency** is the least detailed level of logging, and **Debug** is the most detailed level of logging)

2.11.5.2 Add IPSec VPN Site

OnApp IPSec VPN has two different session types: policy-based and route-based. With the policy-based IPSec VPN session type, you can connect multiple local subnets behind the NSX Edge with the peer subnets on the remote VPN site by using IPSec tunnels. Alternatively, if you select the route-based IPSec VPN session type, virtual tunnel interfaces (VTI) are created on the ESG appliance. Each VTI is associated with an IPSec tunnel. The encrypted traffic is routed from one site to another site through the VTI interfaces. IPSec processing happens only at the VTI interfaces.

To add an IPSec VPN site:
1. Go to your Control Panel > **Cloud** > **Edges**.
2. Select the necessary edge from the list of all edges in your cloud.
3. Go to the **IPSec VPN** tab > click the **IPSec VPN sites** tab below.
4. Click the button above the table.
5. In the window that appears, specify the following parameters:
   - **Name** - specify the name of the IPSec VPN site
   - **Enabled** - move the slider to the right to enable this IPSec VPN site
   - **Enabled PFS** - move the slider to the right to enable Perfect Forward Secrecy for this site
   - **Local ID** - enter the local ID to identify the local NSX Edge instance. This local ID is the peer ID on the remote site. Preferably, use the public IP address of the VPN or a fully qualified domain name (FQDN) for the VPN service as the local ID.
   - **Local Endpoint** - enter an IP address or an FQDN of the local endpoint. If you are adding an IP-to-IP tunnel using a pre-shared key, the local ID and local endpoint IP can be the same.
- **Local subnets** - enter the subnets to share between the IPSec VPN sites in the CIDR format. Use a comma separator to enter multiple subnets.

The local subnets behind an NSX Edge must have address ranges that do not overlap with the IP addresses on the peer VPN site. If the local and remote peer across an IPsec VPN tunnel have overlapping IP addresses, traffic forwarding across the tunnel might not be consistent.

- **Peer ID** - enter the Peer ID to identify the peer site:
  - For peers using certificate authentication, this ID must be the distinguished name (DN) in the peer’s certificate. Enter the DN of the certificate as a range of comma-separated values in the following order without spaces: C=xxx,ST=xxx,L=xxx,O=xxx,OU=xxx,CN=xxx,E=xxx.
  - For PSK peers, the peer ID can be any text value. Preferably, use the public IP address of the VPN or an FQDN for the VPN service as the peer ID.

- **Peer endpoint** - enter an IP address or an FQDN of the peer endpoint. The default value is **any**. If you retain the default value, you must configure the Global PSK.

- **Peer subnet** - enter the internal IP address of the peer subnet in the CIDR format. Use a comma separator to type multiple subnets.

- **Encryption algorithm** - select one of the following supported encryption algorithms from the dropbox:
  - AES (AES128-CBC)
  - AES256 (AES256-CBC)
  - Triple DES (3DES192-CBC)
  - AES-GCM (AES128-GCM)

- **Authentication** - select one of the following options:
  - **PSK (Pre Shared Key)** - indicates that the secret key shared between NSX Edge and the peer site is to be used for authentication. The secret key can be a string with a maximum length of 128 bytes. PSK authentication is disabled in FIPS mode.
  - **Certificate** - indicates that the certificate defined at the global level is to be used for authentication.

- **Shared key** - the global pre-shared key (PSK) is shared by all the sites whose peer endpoint is set to ‘any’. If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting.

- **Diffie-Hellman Group** - select one of the following cryptography schemes that allows the peer site and the NSX Edge to establish a shared secret over an insecure communications channel:
  - **DH-2** (not available when the FIPS mode is enabled)
  - **DH-5** (not available when the FIPS mode is enabled)
  - **DH-14** (a default selection for both FIPS and non-FIPS mode)
  - **DH-15**
  - **DH-16**

- **Extension** - type one of the following:
- securelocaltrafficbyip=IPAddress to redirect Edge local traffic over the IPSec VPN tunnel. IP address is the default value.
- passthroughSubnets=PeerSubnetIPAddress to support overlapping subnets.

- **Digest Algorithm** - select one of the following secure hashing algorithms:
  - SHA1
  - SHA_256

- **IKE Option** - select one of the following Internet Key Exchange (IKE) protocols to set up a security association (SA) in the IPSec protocol suite:
  - **IKEv1** - when you select this option, IPSec VPN initiates and responds to IKEv1 protocol only
  - **IKEv2** - when you select this option, IPSec VPN initiates and responds to IKEv2 protocol only
  - **IKE-Flex** - when you select this option, and if the tunnel establishment fails with IKEv2 protocol, the source site does not fall back and initiate a connection with the IKEv1 protocol. Instead, if the remote site initiates a connection with the IKEv1 protocol, then the connection is accepted

> If you configure multiple sites with the same local and remote endpoints, make sure that you select the same IKE version and PSK across all these IPSec VPN sites.

- **IKE Responder Only** - move the slider to the right to operate IPSec VPN in a responder-only mode. In this mode, IPSec VPN never initiates a connection.

- **Session Type** - select one of the possible options:
  - **policy based** - select to use the policy-based IPSec VPN
  - **route-based** - select to use the route-based IPSec VPN. If you select this session type, fill in the the following additional fields that will appear:
    - **Tunnel Interface IP CIDR**
    - **Tunnel Interface MTU** - default value is 1476. Valid values are in the range from 92 to 8976

4. Click the **Save** button above the table to apply the changes.
To edit the details of an IPSec VPN site:
1. Go to your Control Panel > Cloud > Edges.
2. Select the necessary edge from the list of all edges in your cloud.
3. Go to the IPSec VPN tab > click the IPSec VPN sites tab below.
4. Click the icon next to the required IPSec VPN site.
5. Make the necessary changes in the window that appears.

Click here to view the description of parameters available for editing.

- **Name** - specify the name of the IPSec VPN site
- **Enabled** - move the slider to the right to enable this IPSec VPN site
- **Enabled PFS** - move the slider to the right to enable Perfect Forward Secrecy for this site
- **Local ID** - enter the local ID to identify the local NSX Edge instance. This local ID is the peer ID on the remote site. Preferably, use the public IP address of the VPN or a fully qualified domain name (FQDN) for the VPN service as the local ID.
- **Local Endpoint** - enter an IP address or an FQDN of the local endpoint. If you are adding an IP-to-IP tunnel using a pre-shared key, the local ID and local endpoint IP can be the same.
- **Local subnets** - enter the subnets to share between the IPSec VPN sites in the CIDR format. Use a comma separator to enter multiple subnets.
- **Peer ID** - enter the Peer ID to identify the peer site:
  - For peers using certificate authentication, this ID must be the distinguished name (DN) in the peer's certificate. Enter the DN of the certificate as a range of comma-separated values in the following order without spaces:
    \[ C=xxx,ST=xxx,L=xxx,O=xxx,OU=xxx,CN=xxx,E=xxx \]
  - For PSK peers, the peer ID can be any text value. Preferably, use the public IP address of the VPN or an FQDN for the VPN service as the peer ID.
- **Peer endpoint** - enter an IP address or an FQDN of the peer endpoint. The default value is **any**. If you retain the default value, you must configure the Global PSK.

- **Peer subnet** - enter the internal IP address of the peer subnet in the CIDR format. Use a comma separator to type multiple subnets.

- **Encryption algorithm** - select one of the following supported encryption algorithms from the dropbox:
  - AES (AES128-CBC)
  - AES256 (AES256-CBC)
  - Triple DES (3DES192-CBC)
  - AES-GCM (AES128-GCM)

- **Authentication** - select one of the following options:
  - **PSK (Pre Shared Key)** - indicates that the secret key shared between NSX Edge and the peer site is to be used for authentication. The secret key can be a string with a maximum length of 128 bytes. PSK authentication is disabled in FIPS mode.
  - **Certificate** - indicates that the certificate defined at the global level is to be used for authentication.

- **Shared key** - the global pre-shared key (PSK) is shared by all the sites whose peer endpoint is set to 'any'. If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting.

- **Diffie-Hellman Group** - select one of the following cryptography schemes that allows the peer site and the NSX Edge to establish a shared secret over an insecure communications channel:
  - **DH-2** (not available when the FIPS mode is enabled)
  - **DH-5** (not available when the FIPS mode is enabled)
  - **DH-14** (a default selection for both FIPS and non-FIPS mode)
  - **DH-15**
  - **DH-16**

- **Extension** - type one of the following:
  - `securelocaltrafficbyip=IPAddress` to redirect Edge local traffic over the IPSec VPN tunnel. IP address is the default value.
  - `passthroughSubnets=PeerSubnetIPAddress` to support overlapping subnets.

- **Digest Algorithm** - select one of the following secure hashing algorithms:
  - SHA1
  - SHA_256

- **IKE Option** - select one of the following Internet Key Exchange (IKE) protocols to set up a security association (SA) in the IPSec protocol suite
  - **IKEv1** - when you select this option, IPSec VPN initiates and responds to IKEv1 protocol only.
  - **IKEv2** - when you select this option, IPSec VPN initiates and responds to IKEv2 protocol only.
  - **IKE-Flex** - when you select this option, and if the tunnel establishment fails with IKEv2 protocol, the source site does not fall back and initiate a connection with the IKEv1 protocol. Instead, if the remote site initiates a connection with the IKEv1 protocol, then the connection is accepted.
If you configure multiple sites with the same local and remote endpoints, make sure that you select the same IKE version and PSK across all these IPSec VPN sites.

- **IKE Responder Only** - move the slider to the right to operate IPSec VPN in a responder-only mode. In this mode, IPSec VPN never initiates a connection.
- **Session Type** - select one of the possible options:
  - *policy based* - select to use the policy-based IPSec VPN
  - *route-based* - select to use the route-based IPSec VPN. If you select this session type, the following additional fields will appear:
    - *Tunnel Interface IP CIDR*
    - *Tunnel Interface MTU* - default value is 1476. Valid values are in the range from 92 to 8976

6. Click the **Save** button above the table to apply the changes.

### 2.11.5.4 Certificate Authentication

If you select Certificate as an Authentication option for an IPSec VPN site, it is required to enable **Certificate Authentication** option. It is not possible to upload a certificate on OnApp side; the certificates are imported to OnApp from vCenter as you import the edge instance (if there were any assigned on the vCenter side).

Self-signed certificates cannot be used for IPSec VPN.

To configure certificate authentication for IPSec VPN:
1. Go to your Control Panel > **Cloud** > **Edges**.
2. Select the necessary edge from the list of all edges in your cloud.
3. Go to the **IPSec VPN** tab.
4. Move the **Enable Certificate Authentication** slider to the right to enable service authentication.
5. On the page that appears, select the necessary service certificates, CA certificates and CRLs certificates.

### 2.11.5.5 Delete IPSec VPN Site

To delete an IPSec VPN site:
1. Go to your Control Panel > **Cloud** > **Edges**.
2. Click the label of the edge the necessary IPSec VPN was added to.
3. Click the **IPSec VPN** tab.
4. Click the **IPSec VPN sites** tab below. On the page that appears, you will see the list of IPSec VPN sites added to this edge.
5. Click the line with the required IPSec VPN site to select it.
6. Once selected, click the button that appeared above the table to delete the IPSec VPN site.

7. Click the Save button above the table to apply the changes.

2.11.6 NSX L2 VPN

With L2 VPN, you can stretch multiple logical networks (both VLAN and VXLAN) between different physical sites. In addition, you can configure multiple sites on an L2 VPN server. L2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries. Virtual servers remain on the same subnet when they are moved between sites and their IP addresses do not change.

NSX L2 VPN configuration consists of three steps:

1. Configuration of your destination edge - L2 VPN server
2. Adding peer sites to the L2 VPN server
3. Configuration of your source edge - L2 VPN client

Before you proceed further, please note that:

- The Any action on L2 VPN service and Any action on L2 VPN peer site permissions should be enabled for a user who wants to use NSX L2 VPN.
- You must enable the L2 VPN service on both the server and the client. For that, use the L2 VPN slider located at the top left corner of the screen.

On this page:

- Edit L2 VPN Server
- Add Peer Sites to L2 VPN Server
- Edit Peer Sites
- Edit L2 VPN Client
- Edit Advanced Client Settings

See also:

- NSX Firewalls
- NSX IPSec VPN
- NSX Load Balancers

2.11.6.1 Edit L2 VPN Server

Configure L2 VPN Server which is the destination NSX Edge to which the client is to be connected.

To configure L2 VPN server:

1. Go to Dashboard > vCenter > Edges menu.
2. Click the label of the edge you want to configure the server for.

3. Click the L2 VPN tab, then click Server > Server Global tab.

4. On the page that follows edit the following fields:
   - **Listener IP** - enter the primary or secondary IP address of an external interface of the NSX Edge
   - **Listener Port** - edit the port number for the L2 VPN service
   - **Encryption algorithm** - select one or more encryption algorithms to encrypt the communication between the server and the client
   - **Validate server certificate** - move the slider to the right to enable the certificate to be bound to SSL VPN server, then select the certificate from the list that appears

5. Click the **Save** button at the top of the page.

Next, you can add and configure multiple sites on an L2 VPN server.

---

2.11.6.2  Add Peer Sites to L2 VPN Server

To add new peer sites:

1. Go to **Dashboard > vCenter > Edges** menu.
2. Click the label of the edge you want to configure the server for.
3. Click the L2 VPN tab, then click **Server > Server Sites** tab.

4. On the page that follows, edit the following details:
   - **Name** - enter a unique name for the peer site
   - **Enabled** - move the slider to the left to disable the newly added peer site
   - **Description** - add a description of your peer site
   - **User ID** - enter a user name with which the peer site is to be authenticated
   - **User password** - enter a password with which the peer site is to be authenticated
   - **Confirm password** - confirm the password
   - **Select sub-interfaces** - select the sub interfaces to be stretched with the client
   - **Egress optimization gateway address** - enter the gateway IP addresses for which the traffic is to be locally routed or for which the traffic is to be blocked over the tunnel
Can be used if the default gateway for virtual servers is the same across the two sites. Provide the list of IP addresses separated by comma, e.g. 191.1.1.1, 192.1.1.1

5. Click the **Save** button.
2.11.6.3 Edit Peer Sites

To edit peer sites:

1. Go to Dashboard > vCenter > Edges menu.
2. Click the label of the edge you want to configure the server for.
3. Click the L2 VPN tab, then click Server > Server Sites tab.
4. Click the icon next to the label of the peer site you want to edit.
5. On the page that loads, edit the following details:
   - **Name** - enter a unique name for the peer site
   - **Enabled** - move the slider to the left to disable the newly added peer site
   - **Description** - add a description of your peer site
   - **User ID** - enter a user name with which the peer site is to be authenticated
   - **User password** - enter a password with which the peer site is to be authenticated
   - **Confirm password** - confirm the password
   - **Select sub-interfaces** - select the sub interfaces to be stretched with the client
   - **Egress optimization gateway address** - enter the gateway IP addresses for which the traffic is to be locally routed or for which the traffic is to be blocked over the tunnel
6. Click the Save button.

Next, proceed to L2 VPN Client which is the source NSX Edge to which the client is connected.

2.11.6.4 Edit L2 VPN Client

To edit L2 VPN client:

1. Go to Dashboard > vCenter > Edges menu.
2. Click the label of the edge you want to configure the server for.
3. Click the L2 VPN tab, then click Client > Client Global tab.
4. On the page that loads, edit the following details:
   - **Server address** - enter the address of the L2 VPN server to which this client is to be connected
   - **Server port** - edit the default port to which the L2 VPN client must connect to, if necessary
   - **Encryption algorithm** - select the encryption algorithm for communicating with the server
   - **Select sub-interfaces** - to select the sub interfaces to be stretched to the server
   - **Egress optimization gateway address** - enter the gateway IP address of the sub interfaces or the IP addresses to which traffic should not flow over the tunnel
   - **User ID** - enter a user name with which the server is to be authenticated
   - **User password** - enter a password with which the peer site is to be authenticated
   - **Confirm password** - confirm the password
5. Click the Save button at the top of the page.
2.11.6.5  Edit Advanced Client Settings
When a client Edge does not have direct access to the Internet and must reach the source (server) NSX Edge through a proxy server, you must specify proxy server settings as follows:

1. Go to Dashboard > vCenter > Edges menu.
2. Click the label of the edge you want to configure the server for.
3. Click the L2 VPN tab, then click Client > Client Advanced tab.
4. On the page that loads, edit the following details:
   - Enable secure proxy - move the slider to the right to enable only secure proxy connections
     - Proxy address - enter the proxy server address
     - Proxy port - enter the proxy server port
     - Proxy user name - enter a user name with which the proxy server is to be authenticated
     - Proxy user password - enter a user password with which the proxy server is to be authenticated
   - Use system generated certificate - move the slider to the right to
5. Click the Save button at the top of the page.
2.12 Create and Manage vCenter Resource Pools

VMware vCenter resource pool determines how and when the provider virtual data center compute and memory resources are committed to the Org VDC. In other words, the resource pool allows you to delegate control over the resources of a host or a cluster. The benefits are evident when you use resource pools to divide into sections all resources in a cluster.

You can view, create, edit, and delete resource pools by using the VMware vCenter Control Panel.

On this page:

- View vCenter Resource Pool
- Create vCenter Resource Pool
- Edit vCenter Resource Pool
- Delete vCenter Resource Pool

2.12.1 View vCenter Resource Pool

To view the vCenter resource pools:

1. Go to your Control Panel > Cloud > Resource Pools menu to see an overview of all resource pools in the cloud.

2. The page that loads will show the list of resource pools with their details:

   - **Label** - the name of the resource pool
   - **Compute Zone** - compute zones which the resource pool is placed on
   - **Compute Resource** - compute resource which the resource pool is placed on
   - **Owner** - owner of resource pool
   - **Actions** - click the Actions button to edit or delete the resource pool

The search box at the top right corner of the page allows you to search a Resource Pool by its label.

To view vCenter resource pool details, click on the label of resource pool you are interested in.
2.12.2 Create vCenter Resource Pool

To create a vCenter resource pool:

Go to your Control Panel > Cloud > Resource Pools menu to see an overview of all resource pools in the cloud.
Click the New Resource Pool button just below the list of resource pools.

On the screen that appears, fill in the resource pool creation form:

- **Label** - specify a name for the resource pool
- **Compute Resource** - select the required compute resource from the dropdown menu

The CPU and RAM Limits of the new resource pool will be automatically unlimited, all other properties will be set to default.

Click the Submit button to save the changes.

2.12.3 Edit vCenter Resource Pool

To edit a vCenter resource pool:

Go to your Control Panel > Cloud > Resource Pools menu to see an overview of all resource pools in the cloud.
Click the Actions button next to the resource pool you want to edit, and click Edit.
On the screen that appears, edit the necessary parameters, and click Save.

You can also use the button at the resource pool details page.

2.12.4 Delete vCenter Resource Pool

To delete a vCenter resource pool:
1. Go to your Control Panel > **Cloud** > **Resource Pools** menu to see an overview of all resource pools in the cloud.

2. Click the **Actions** button next to the resource pool you want to delete and click **Delete**.

3. Click **OK** to confirm the deletion.

Please note that if you delete the resource pool that has a virtual server on it, the VS will be moved to the cluster default resource pool.

### 2.13 vCenter Servers

To connect to vCenter, you can create a vCenter server logical point on the OnApp side. This option will allow you to add each cluster from the vCenter side as a compute resource on the OnApp side separately.

When your vCenter server is imported, you will see all of your networks and data stores being imported and placed in separate zones. After that, you will be able to create compute resources using clusters that have been imported with the vCenter server. With this feature, you will be able to create your VS now based on the compute resource (cluster) and Resource Pool that you select on VS creation wizard. It brings more logic and comfort to your user experience.

You can also set up billing for each cluster separately in the corresponding bucket by specifying the necessary compute zone in the **Limits for compute zones** section.

**Add vCenter Server**

To add a vCenter server:

1. Go to your Control Panel > **Admin** > **Settings** > **vCenter Servers** menu.
2. Click the **Add** button.
3. On the page that appears, specify the following details:
   - **Label**
   - **IP / Hostname**
   - **Login**
   - **Password**
4. Click the **Save** button.

**2.13.1 Edit vCenter Server Details**

To edit vCenter server details:

1. Go to your Control Panel > **Admin** > **Settings** > **vCenter Servers** menu.
2. Next to the necessary VS, click the **Actions** button and select the **Edit** option.
3. Apply the required changes in the corresponding field(s):
   - **Label**
   - **Login**
4. Click the Save button.

## 2.13.2 Delete vCenter Server

To delete a vCenter virtual server:

1. Go to your Control Panel > Admin > Settings > vCenter Servers menu.
2. Next to the necessary VS, click the Actions button and select the Delete option.
3. Confirm the deletion.

## 2.14 vCenter Permissions

The list below includes the permissions related to vCenter Resources.

- Users with the Administrator role in OnApp have vCenter related permissions enabled by default. They can create and manage vCenter resources if there is a vCenter compute resource in the cloud.
- Users with vCenter User role have all OnApp User permissions, default permissions for vCenter User role, and two extra permissions necessary to create a vCenter VS:
  - Read all public OVAs
  - See Compute Resource during virtual server creation
- Users with OnApp User role have limited vCenter permissions enabled by default, and cannot create a vCenter VS.
- The vCenter permissions list is not updated in OnApp for custom roles imported from vCenter.

### 2.14.1 Default Permissions for vCenter User Role

#### 2.14.1.1 vCenter Clusters

OnApp administrators can control users’ ability to manage vCenter clusters through the Control Panel’s Roles menu. You can set the following cluster permissions for user roles:

- Any actions on vCenter Clusters - the user can take any action on vCenter clusters
- Show vCenter Clusters on Virtual Server creation - the user can see vCenter Clusters on Add New Virtual Server screen

#### 2.14.1.2 vCenter Datacenters

OnApp administrators can control users’ ability to manage vCenter datacenters. This is handled through the Control Panel’s Roles menu. You can set the following datacenters permissions for user roles:

- Any actions on vCenter Datacenters - the user can take any action on vCenter Datacenters
• Show vCenter Datacenters on Virtual Server creation - the user can see vCenter Datacenters on Add New Virtual Server screen

2.14.1.3 vCenter Servers
• Any actions on vCenter Servers - the user can take any action on vCenter servers
• Create a new vCenter Server - the user can create new vCenter servers
• Delete any vCenter Server - the user can delete any vCenter server
• Import any vCenter Server - the user can import any vCenter server to OnApp
• See any vCenter Server - the user can see the list of all vCenter servers in the cloud
• Update any vCenter Server - the user can edit any vCenter server within the cloud

For more details, refer to the vCenter Servers section of this guide.

2.14.1.4 vCenter Templates
• Any actions on vCenter Templates - the user can take any action on vCenter templates
• See any vCenter Templates - the user can see any vCenter templates
• Update any vCenter Templates - the user can edit any vCenter templates

2.14.1.5 vCenter Resource Pool
• Add a new vCenter Resource Pool - the user can add a vCenter Resource Pool
• Delete own vCenter Resource Pool - the user can delete own vCenter Resource Pool
• See own vCenter Resource Pool - the user can see own vCenter Resource Pool
• Update own vCenter Resource Pool - the user can update own vCenter Resource Pool

2.14.1.6 Virtual Servers
• Resync vCenter VS - the user can run the re-import vCenter VS transaction

2.14.2 Other vCenter Permissions

2.14.2.1 NSX Edges
OnApp administrators can control users’ ability to manage NSX edges through the Control Panel's Roles menu. You can set the following NSX edges permissions for user roles:
• Any action on edge - the user can take any action on NSX edges
• See any edge - the user can see any NSX edge

2.14.2.2 NSX Firewall Rules
OnApp administrators can control users’ ability to manage NSX firewall rules through the Control Panel's Roles menu. You can set the following firewall rules permissions for user roles:
• Any action on firewall rule - the user can take any action on NSX firewall rules
• Create any firewall rule - the user can create a new NSX firewall rule
• Delete any firewall rule - the user can delete any NSX firewall rule
• See any firewall rules - the user can see any NSx firewall rules
• Update any firewall rule - the user can edit any NSX firewall rule
2.14.2.3 NSX Firewall Services
OnApp administrators can control users’ ability to manage NSX firewall services through the Control Panel's Roles menu. You can set the following firewall services permissions for user roles:

- *Any action on firewall service* - the user can take any action on NSX firewall services
- *See any firewall service* - the user can see any NSX firewall service
- *Update any firewall service* - the user can edit any NSX firewall service

2.14.2.4 NSX IPSec Services
OnApp administrators can control users’ ability to manage NSX IPSec services through the Control Panel's Roles menu. You can set the following IPSec services permissions for user roles:

- *Any action on IPSec service* - the user can take any action on NSX IPSec services
- *See any IPSec service* - the user can see any NSX IPSec service
- *Update any IPSec service* - the user can edit any NSX IPSec service

2.14.2.5 NSX IPSec Sites
OnApp administrators can control users’ ability to manage NSX IPSec sites through the Control Panel's Roles menu. You can set the following IPSec sites permissions for user roles:

- *Any action on IPSec site* - the user can take any action on NSX IPSec sites
- *Create IPSec sites* - the user can create an NSX IPSec site
- *Delete any IPSec site* - the user can delete any NSX L2 VPN IPSec site
- *See any IPSec site* - the user can see any NSX IPSec sites
- *Update any IPSec site* - the user can edit any NSX IPSec site

2.14.2.6 NSX L2 VPN Peer Sites
OnApp administrators can control users’ ability to manage NSX L2 VPN peer sites through the Control Panel's Roles menu. You can set the following L2 VPN peer sites permissions for user roles:

- *Any action on L2 VPN peer site* - the user can take any action on NSX L2 VPN peer sites
- *Create L2 VPN peer sites* - the user can create an NSX L2 VPN peer site
- *Delete any L2 VPN peer site* - the user can delete any NSX L2 VPN peer site
- *See any L2 VPN peer site* - the user can see any NSX L2 VPN sites
- *Update any L2 VPN peer site* - the user can edit any NSX L2 VPN sites

2.14.2.7 NSX L2 VPN Services
OnApp administrators can control users’ ability to manage NSX L2 VPN services through the Control Panel's Roles menu. You can set the following L2 VPN services permissions for user roles:

- *Any action on L2 VPN service* - the user can take any action on NSC L2 VPN services
- *See any L2 VPN service* - the user can see any NSX L2 VPN service
- *Update any L2 VPN service* - the user can edit any NSX load balancer L2 VPN services

2.14.2.8 NSX Load Balancer Application Profiles
OnApp administrators can control users’ ability to manage NSX load balancer application profiles through the Control Panel's Roles menu. You can set the following load balancer application profiles permissions for user roles:
• **Any action on application profile** - the user can take any action on NSX load balancer application profiles

• **Create any application profile** - the user can create a new NSX load balancer application profile

• **Delete any application profile** - the user can delete any NSX load balancer application profile

• **See any application profile** - the user can see any NSX load balancer application profile

• **Update any application profile** - the user can edit any NSX load balancer application profile

2.14.2.9 NSX Load Balancer Application Rules

OnApp administrators can control users’ ability to manage NSX load balancer application rules through the Control Panel’s Roles menu. You can set the following load balancer application rules permissions for user roles:

• **Any action on application rules** - the user can take any action on NSX load balancer application rules

• **Create any application rule** - the user can create a new NSX load balancer application rule

• **Delete any application rule** - the user can delete any NSX load balancer application rule

• **See any application rule** - the user can see any NSX load balancer application rules

• **Update any application rule** - the user can edit any NSX load balancer application rules

2.14.2.10 NSX Load Balancer Monitors

OnApp administrators can control users’ ability to manage NSX load balancer monitors through the Control Panel’s Roles menu. You can set the following load balancer monitors permissions for user roles:

• **Any action on monitors** - the user can take any action on NSX load balancer monitors

• **Create any monitor** - the user can create a new NSX load balancer monitor

• **Delete any monitor** - the user can delete any NSX load balancer monitor

• **See any monitor** - the user can see any NSX load balancer monitors

• **Update any monitor** - the user can edit any NSX load balancer monitors

2.14.2.11 NSX Load Balancer Pools

OnApp administrators can control users’ ability to manage NSX load balancer pools through the Control Panel’s Roles menu. You can set the following load balancer pools permissions for user roles:

• **Any action on pool** - the user can take any action on NSX load balancer pools

• **Create any pool** - the user can create a new NSX load balancer pool

• **Delete any pool** - the user can delete any NSX load balancer pool

• **See any pool** - the user can see any NSX load balancer pools

• **Update any pool** - the user can edit any NSX load balancer pools

2.14.2.12 NSX Load Balancer Services

OnApp administrators can control users’ ability to manage NSX load balancer services through the Control Panel’s Roles menu. You can set the following load balancer services permissions for user roles:

• **Any action on load balancer service** - the user can take any action on NSX load balancer services

• **See any load balancer service** - the user can see any NSX load balancer service
• **Update any load balancer service** - the user can edit any NSX load balancer service

2.14.2.13 NSX Load Balancer Virtual Servers
OnApp administrators can control users' ability to manage NSX Edge internal or uplink interfaces as virtual servers through the Control Panel's Roles menu. You can set the following permissions for user roles:

- **Any action on virtual server** - the user can take any action on NSX load balancer virtual servers
- **Create any virtual server** - the user can create a new NSX load balancer virtual server
- **Delete any virtual server** - the user can delete any NSX load balancer virtual servers
- **See any virtual server** - the user can see any NSX load balancer virtual servers
- **Update any virtual server** - the user can edit any NSX load balancer virtual servers

2.14.2.14 NSX Managers
OnApp administrators can control users' ability to manage NSX managers through the Control Panel's Roles menu. You can set the following NSX managers permissions for user roles:

- **Any action on NSX manager** - the user can take any action on NSX manager
- **See any NSX manager** - the user can see any NSX manager
- **Update any NSX manager** - the user can edit any NSX manager

2.14.2.15 NSX NAT Rules
OnApp administrators can control users' ability to manage NSX NAT rules through the Control Panel's Roles menu. You can set the following NAT rules permissions for user roles:

- **Any action on nat rule** - the user can take any action on NSX NAT rules
- Create any nat rule - the user can create a new NSX NAT rule
- **Delete any nat rule** - the user can delete any NSX NAT rule
- **See any nat rule** - the user can see any NSX NAT rules
- **Update any nat rule** - the user can edit any NSX NAT rules

2.14.2.16 NSX NAT Services
OnApp administrators can control users' ability to manage NSX NAT services through the Control Panel's Roles menu. You can set the following NAT services permissions for user roles:

- **Any action on nat service** - the user can take any action on NSX NAT services
- **See any nat service** - the user can see any NSX NAT services
- **Update any nat service** - the user can edit any NSX NAT services

2.14.2.17 vCenter Resource Pools
OnApp administrators can manage vCenter resource pools. You can set the following permissions for user roles:

- **Any actions on vCenter Resource Pools** - the user can take any action on vCenter Resource Pool
- **Delete any vCenter Resource Pool** - the user can delete a vCenter Resource Pool
- **See any vCenter Resource Pool** - the user can see any vCenter Resource Pool
- **Update any vCenter Resource Pool** - the user can update any vCenter Resource Pool

2.14.2.18 Virtual Servers
• **Infrastructure Mode** - the user can build managed vCenter VSs
See [Create Custom vCenter VS](#) for more details.
On this page:

- Default permissions for vCenter User role
- Other vCenter permissions
3 User Guide

Virtual servers running on vCenter compute resources are managed almost the same as normal virtual servers. Also, the vCenter cluster is displayed as a pool of resources rather than per compute resource.

OnApp Cloud gives you high-end cloud management features including:

<table>
<thead>
<tr>
<th>vCenter Virtual Server Options</th>
<th>Power Options</th>
<th>Networks</th>
<th>Disks</th>
<th>Snapshots</th>
<th>Statistics</th>
<th>Recipes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>Reboot</td>
<td>Configure network interface</td>
<td>Create disks</td>
<td>Snapshots</td>
<td>CPU utilization</td>
<td>Recipes</td>
</tr>
<tr>
<td>Rebuild manually</td>
<td>Suspend</td>
<td>Rebuild network</td>
<td>Edit disks</td>
<td>Billing statistics</td>
<td>Custom variables</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Shut down</td>
<td>Edit network speed</td>
<td>Migrate disks</td>
<td>Network interface statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>vCenter virtual server IP addresses</td>
<td>Delete disks</td>
<td>Disk IOPS statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Display network speed for network interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Certain VS operations are unavailable in OnApp with vCenter:

- Reboot in recovery
- Segregate
- VIP status
- Autoscaling
- Migrate VS. vCenter utilizes vMotion to ensure that the VSs are optimally placed on the compute resources
- Use of IPv6 is not supported for vCenter virtual servers.

NOTE: Performing the following VS operations at vCenter may lead to problems with VMware infrastructure management. Please, do not execute the following actions in vCenter:

- Power On/Off or Suspend VSs
- Edit the Properties for any VS
- Create and delete Snapshots
- Make changes to the distributed vSwitch
• Remove templates from the data store
• Rename templates
• Delete the services account on the virtual server
• Remove or stop VMware tools on the virtual server

Performing the following actions in vCenter will not affect OnApp:
• Migrate VSs between compute resources using vMotion
• Migrate VSs between data stores using Storage vMotion
• Place compute resources into maintenance mode
• Make changes to compute resources when in maintenance mode
• Back up VSs using third party tool (e.g. Veeam)
• Enable, Disable or make changes to DRS

Performing the following actions in vCenter will be synchronized with OnApp:
• Networks Created
• Networks Deleted
• Datastores Created
• Datastores Deleted
• New Compute Added
• Compute Remove
• Updates to Imported VSs (Ex. Changed Resources, added NICs, add Disks)
• VS has been Deleted

### 3.1 Create vCenter Virtual Servers

To create a vCenter virtual server:

Go to your Control Panel > **Cloud** > **Virtual Servers** menu and click the "+" button or click the **Create New Virtual Server** button at the bottom of the page. Fill in the VS creation form step by step:

#### 3.1.1 Step 1 of 6. Cloud Locations

On this page:

• [Step 1 of 6. Cloud Locations](#)
• [Step 2 of 6. Templates](#)
• [Step 3 of 6. Properties](#)
Step 4 of 6. Resources

Step 5 of 6. Recipes or Service Add-ons

Step 6. Confirmation

The Cloud Locations step applies to those users who have compute zones assigned to location groups in their bucket. This step will be present in the wizard if both of the following requirements are met:

- all compute resources available to the user are assigned to location groups
- compute resources are assigned to different locations

If the user's bucket has several compute zones, some of which are assigned to location groups, whereas others are not - the cloud locations screen will not be available in the wizard. Also if all compute zones are assigned to the same location this step will be skipped. In this case the wizard will start from the Templates step.

1. Indicate your virtual server's cloud location:
   - Country - choose the country, where the cloud is located, from the drop-down menu.
   - City - specify the city, where the cloud is located, from the drop-down menu.

2. Click Next to proceed to the following step of the wizard to specify the virtual server templates

3.1.2 Step 2 of 6. Templates

1. Click the required group icon on the right (vCenter) to expand the list of templates on the left. Every template contains the following info:
   - Label
   - Min memory size that is required to create a VS from this template
   - Min disk size that is required to create a VS from this template
   - Virtualization type
   - Price per hour

2. Select the template.

3. Click Next.

1. You can use RHEL, Windows and Debian templates to create vCenter virtual servers. For details how to create vCenter templates, refer to Create Template for vCenter Virtual Server section.

2. To be able to use Ubuntu templates later than 9 version for vCenter virtual server creation, you need to remove the absolute pathnames in /etc/pam.d/vmtoolsd file. For example: /lib/security/pam_unix.so > pam_unix.so

3. Please make sure that the Windows password policy defined inside the template is compliant with the password policy set in the OnApp CP. This
will ensure that there are no password related issues when provisioning Windows.

4. OnApp supports templates with no more than one disk.

**Windows Licensing Type**

This option only appears if your bucket allows it, and if the relevant licensing options have been configured for the template group this template belongs to.

If this option is available, choose the license type you require:

- For the KMS type, choose the licensing server
- For your own license, type your license key

Please note that for the Windows templates imported from vCenter it is impossible to select the MAK license during the VS creation. It will be necessary to choose the **Your own license** option and manually indicate the License Key.

If you don't specify the licensing type, MAK licensing will be set by default.

It is possible to deploy Windows virtual servers without running sysprep. To do so, you need to disable the **Run Sysprep** option for the compute zone the virtual server will be built on. See **Create Compute Zone** section for details.

It is not possible to set VS password when creating a Windows-based vCenter virtual server without running a sysprep.

---

**3.1.3 Step 3 of 6. Properties**

You can create a virtual server having specified only the required parameters and configure it later. Specify the following virtual server properties:

- **Label** - enter the label of the virtual server
- **Hostname** - enter the host name of the virtual server

  - Hostname may contain letters (A-Z), numbers(0-9) and hyphens (-) but no spaces or periods (.). The name may not consists entirely of digits.
  - For Windows-based VSs, the hostname length should be between 1 and 15 characters.

- **Domain** - enter the domain name of the virtual server
- **Password** - enter the password of the virtual server or leave black for the password to be auto generated
- **Password confirmation** - enter the password again to confirm it
- Click **Next**.

3.1.4 Step 4 of 6. Resources

**Compute Resources**
- *Compute Resource* - select the compute resource
- *vCenter Resource Pool* - select the resource pool

If you pick **Resources** from the dropdown menu, the virtual server will be placed into the default resource pool, so it will not be shown at any user resource pool, just under the cluster.

**Resources**
- **RAM** - set the amount of virtual server's RAM.
- **CPU Cores** - set the amount of virtual server's CPU cores.
- **CPU Priority (or CPU Units)** - set virtual server's CPU priority. If the CPU units are switched on in the bucket for this user, then CPU priority is replaced with CPU units. Refer to Billing Calculation section for details on CPU units and CPU priority.

The amount of CPU resource a VS is given is the CPU priority (you can think of this as its "share percentage") multiplied by the number of cores allocated to that VS. This is a minimum number – clients can exceed it, up to 100% multiplied by the number of cores. For example, on a compute resource with 3GHz CPU cores:
- 100% x 1 core = 3GHz (burstable to 3GHz)
- 10% x 2 cores = 600MHZ (burstable to 6GHz)
- 5% x 4 cores = 600MHz (burstable to 12GHz)

By default, OnApp allows overselling of cloud resources. For example, OnApp will allow users to create 5 VSs with 100% CPU priority/1 CPU core on a compute resource with a 4-core CPU. In this example, OnApp would reduce the guaranteed CPU for each VS. If you build a VS on a KVM compute resource running CentOS5, the CPU priority settings will be disabled and CPU priority value will be 100 by default.

Note that CPU priority amount does not reflect the number of VMware CPU Resource Shares. It is calculated as follows: CPU Resource Shares (VMware) = CPU Priority (OnApp) *20. For example, 25% of CPU Priority (in OnApp) transforms into 500 CPU Resource shares (in VMware):
- 25% x 20 = 500 CPU Resource Shares (low)
- 50% x 20 = 1000 CPU Resource Shares (normal)
- 100% x 20 = 2000 CPU Resource Shares (high)

**Primary Disk**
- *Data Store Zone* - choose a data store zone for this VS's primary disk.
- *Primary data store* - select a primary data store for this VS's primary disk.
- *Primary disk size* - set the primary disk size.

**Swap Disk**
Select the following properties for a swap disk:
- *Size* - enter a size for a swap disk
- *Data Store Zone* - select a data store zone for a swap disk
- *Data Store* - select a data store for a swap disk
- *Disable* - select the checkbox to disable swap disk creation

**Network Configuration**

*Network Interface 1*
- *Network group* - select the network zone or leave *Any*
- *Network* - select the network from which the VS should get the IP address or leave *Any*
- *IP net* - select from the drop-down list the IP net from which the IP address should be assigned or leave *Any*
- *IP range* - select from the drop-down list the IP range from which the IP address should be assigned or leave *Any*
- *IP address* - select an IP address to be assigned from the drop-down box or leave *Any*
- *Port Speed* - set the port speed for this VS

Please note that it is possible to create a vCenter virtual server from a vCenter template with only one network interface added.

### 3.1.5 Step 5 of 6. Recipes or Service Add-ons

**Recipes**
You can select recipes that you want to assign to your virtual server. This step is optional. You can create a virtual server without choosing recipes and add them later if required.

1. Select a recipe that you want to assign to this virtual server by dragging the required recipe to the **Assigned recipes** pane.
2. To add a custom variable, click the "+" button next to the **Custom recipe variables** title bar, then specify variable details:
   - Specify the recipe name and its value.
Move the Enabled slider to the right to allow use of this variable.

3. Click Next to proceed to the next step of the wizard that completes the virtual server creation process.

The recipes step can be missing in the wizard if there are no recipes created in the cloud.

Service Add-ons

**Prerequisites**

Ensure that the following requirements are met to be able to assign service add-on to a VS:

- *Replace Recipes with Service Add-ons on VS creation* permission is enabled
- Service add-on groups are available in your bucket
- The *On Provisioning* option is enabled for all or some of the service add-ons available to you within a bucket.

In case there are no available service add-ons, this step of the wizard is not available.

You can select the service add-ons that you want to assign to your virtual server. This step is optional. You can create a virtual server without choosing service add-ons and add them later if required.

1. Click the service add-on group icon on the left to expand the list of service add-ons on the right. Every service add-on contains the following info:
   - *Label*
   - *VS types* with which this service add-on is compatible
   - *Description* of the service add-on
   - *Price per hour*

2. Select the service add-on by clicking on it. You can select several add-ons from different service add-on groups. Click View Selected Add-ons to see the list of selected service add-ons. You can remove the selected service add-on from the list by clicking the button near the add-on.

3. Click Next to proceed to the next step of the wizard that completes the virtual server creation.

### 3.1.6 Step 6. Confirmation

- Move the Enable Automated Backup slider to the right if you want this VS to be backed up automatically (according to the backup settings configured in the Settings/Auto-backup Presets menu)
• Move the Build Virtual Server slider to the right, if you want the system to automatically build the VS. If you leave this box blank, you will have to build your server manually after it is created.

• Move the Boot Virtual Server slider to the right, if you want the virtual server to be started up automatically.

• Move the Enable Autoscale slider to the right to set autoscaling for this VS.

  • Until the autoscaling rules are configured the autoscaling itself will not start working.
  • If the Enable Autoscale slider is grayed out that means that you have reached the autoscaling limit in the bucket (or the max is set as 0).

• Move the Acceleration allowed slider to the right to enable accelerator for this VS. For more information, see Edge Accelerator.

At the Confirmation step you can find the configuration summary of VS, which will be created. You can view template's name, RAM size, number of networks, primary disk size, and number of cores.

After you set up all parameters, click the Create Virtual Server button to start the creation process.

### 3.2 vCenter Virtual Server Beta Wizard

OnApp 6.2 Edge 1 introduces a new beta version of the vCenter virtual server wizard. You can access the beta version of the wizard from the top bar on your Control Panel. To launch the wizard, click Create Virtual Server > Add Virtual Server Beta.

Note that a new beta version of the vCenter virtual server wizard is disabled by default. If you want to enable this version of the wizard, go to on_app.yml file and set the show_new_wizard parameter to true.

In this section you can find the procedures to create vCenter virtual servers in the new wizard, using one of the following methods:

• From Custom Set of Resources

• From Instance Package
3.2.1 Create Custom vCenter Virtual Servers Beta

Virtual servers are created from templates and are deployed on compute, storage, and networking resources. To create a vCenter virtual server, you need to launch a wizard. The wizard walks you through several steps to get your virtual server up and running. You can create vCenter virtual servers from instance packages or custom set of resources. In this document, you can find a detailed guidance on how to create a custom vCenter virtual server but first take a look at the following section.

3.2.1.1 Infrastructure Mode

An infrastructure mode allows you to manage with OnApp only the infrastructure layer without any post actions (e.g. formatting disk after adding it, or assigning an IP address after adding a network interface). To create a vCenter virtual server in infrastructure mode, you need to have the infrastructure mode permission enabled for your role and move the Infrastructure mode slider to the right at the Properties step in wizard.

To create a vCenter virtual server, follow the next procedure:

1. Go to your Control Panel and click Create Server on the top bar.
2. Click Create Virtual Server Beta to launch the wizard.
3. Follow the step-by-step instructions below to complete the wizard.
4. After you are finished, click the Create Virtual Server button.

On this page:

- Infrastructure Mode
- Cloud Locations
- Templates
- Properties
- Compute Resources
- Storage Resources
- Network Resources
- Service Add-ons or Recipes
3.2.1.2 Cloud Locations

The **Cloud Locations** step applies to those users who have compute zones assigned to location groups in their bucket. If Cloud Locations are not available, the wizard starts from the **Templates** step. This Cloud Locations step will be present in the wizard if both of the following requirements are met:

- All compute resources available to the user are assigned to location groups.
- Compute resources are assigned to different locations.

When you are at the **Cloud Locations** step, select a location for your virtual server:

- **Country** - choose the country, where the cloud is located, from the drop-down menu.
- **City** - specify the city, where the cloud is located, from the drop-down menu.

Click **Next** to proceed to the following step of the wizard.

3.2.1.3 Templates

To select a template, follow the next procedure:

1. Click the required group icon on the right (vCenter) to expand the list of templates on the left. Every template contains the following info:
   - **Label**
   - **Min memory size** that is required to create a VS from this template
   - **Min disk size** that is required to create a VS from this template
   - **Virtualization type**
   - **Price per hour**

2. Select the template.

**What template to choose**

- You can use RHEL, Windows and Debian templates to create vCenter virtual servers. For details how to create vCenter templates, refer to [Create Template for vCenter Virtual Server](#) section.
- To be able to use Ubuntu templates later than 9 version for vCenter virtual server creation, you need to remove the absolute pathnames in `/etc/pam.d/vmtoolsd` file. For example: `/lib/security/pam_unix.so > pam_unix.so`
- Please make sure that the Windows password policy defined inside the template is compliant with the password policy set in the OnApp CP. This will ensure that there are no password related issues when provisioning Windows.

3. Click **Next**.
Additional Information for Windows Templates

The **Windows Licensing Type** box appears for Windows templates and includes license options that you configure for a corresponding template store. You can select one of the following license types:

- **MAK** - the default licensing type applicable to all Windows-based virtual servers. If you don't select the licensing type, **MAK** is set by default.

- **KMS** - the licensing type applicable to every virtual server since Windows 7, Windows Server 2008, and the following Windows versions. Click **KMS** and then select a licensing **Server**.

- **User license** - type your license key

When you create a virtual server from a Windows template, consider the following:

- You can create Windows-based vCenter virtual servers without running Sysprep. Disable the **Run Sysprep** option while creating or editing a destination **compute zone**.

- If multiple vCenter virtual servers are deployed from the same template without running Sysprep, they will have identical security identifiers (SIDs) that can result in the system conflict.

- You can't select KMS or your own license when you create a Windows vCenter virtual server from a custom template. As a workaround, you can create a vCenter VS from a template used for custom template **creation**.

- It is not possible to set VS password when creating a Windows-based vCenter virtual server without running a sysprep.

---

**3.2.1.4 Properties**

You can create a virtual server having specified only the required parameters and configure it later. Specify the following virtual server properties:

- **Infrastructure mode** - move the slider to the right to enable the **Infrastructure mode** for this virtual server

- **Label** - enter the label of the virtual server

- **Hostname** - enter the host name of the virtual server

  - **Hostname** may contain letters (A-Z), numbers (0-9) and hyphens (-) but no spaces or periods (.). The name may not consist entirely of digits.

  - For Windows-based VSS, the hostname length should be between 1 and 15 characters.

- **Domain** - enter the domain name of the virtual server
• **Password** - enter the password of the virtual server or leave black for the password to be auto generated

• **Password confirmation** - enter the password again to confirm it

• **Encrypt password** - move the slider to the right to encrypt your password. For more information on the password encryption, see FAQ.

• **Encryption passphrase** - enter a passphrase for encryption

• **Encryption passphrase confirmation** - repeat the passphrase for encryption

• **I want to create a VS with custom resources** - select the checkbox to create a virtual server based on a set of custom resources. If you don't select the checkbox, you can create a virtual server from instance packages.

Click **Next** to proceed to the following step of the wizard where you select a custom set of resources.

---

3.2.1.5  **Compute Resources**

- **RAM** - set the amount of virtual server's RAM.
- **CPU Cores** - set the amount of virtual server's CPU cores.
- **CPU Priority (or CPU Units)** - set virtual server's CPU priority. If the CPU units are switched on in the bucket for this user, then CPU priority is replaced with CPU units. Refer to **Billing Calculation** section for details on CPU units and CPU priority.
- **Datacenter** - select the data center for the data store.
- **Cluster** - select the cluster to import networks and data stores from.

3.2.1.6  **Storage Resources**

**Primary Disk**

- **Size** - set the primary disk size.
- **Data Store Zone** - choose a data store zone for this VS's primary disk.
- **Data Store** - select a primary data store for this VS's primary disk.

**Swap Disk**

Select the following properties for a swap disk:

- **Size** - enter a size for a swap disk
- **Data Store Zone** - select a data store zone for a swap disk
- **Data Store** - select a data store for a swap disk
- **Disable** - select the checkbox to disable swap disk creation

3.2.1.7  **Network Resources**

**Network Interface 1**

- **Network group** - select the network zone or leave **Any**
- **Network** - select the network from which the VS should get the IP address or leave **Any**
- **IP net** - select from the drop-down list the IP net from which the IP address should be assigned or leave **Any**
• *IP range* - select from the drop-down list the IP range from which the IP address should be assigned or leave *Any*

• *IP address* - select an IP address to be assigned from the drop-down box or leave *Any*

• *Port Speed* - set the port speed for this VS or select the *Unlimited* checkbox

### 3.2.1.8 Service Add-ons or Recipes

During this step, you can assign service add-ons or recipes to your virtual server. The availability of service add-ons or recipes depends on your cloud configuration.

#### 3.2.1.8.1 Service Add-ons

Service add-ons are available under the following conditions:

- The *Replace Recipes with Service Add-ons on VS creation* permission is enabled
- Service add-on groups are available in your bucket
- The *On Provisioning* option is enabled for all or some of the service add-ons available to you within a bucket.

If these conditions are not satisfied, you will see the *Recipes* step instead.

You can create a virtual server without service add-ons and add them later if required. To assign a service add-on to your virtual server in the wizard, follow the next steps:

1. Click the service add-on group icon on the left to expand the list of service add-ons on the right. Every service add-on contains the following info:
   - *Label*
   - *Description*
   - *Price per hour*
   - *Compatible with*, for example, Unix, Windows, etc

2. Click the service add-on to select it. You can select several add-ons from different service add-on groups. Click *View Selected Add-ons* to see the list of selected service add-ons.

   You can remove the selected service add-on from the list by clicking the button near the add-on.

3. Click *Next* to proceed to the next step of the wizard that completes the virtual server creation.

#### 3.2.1.8.2 Recipes

The *Recipes* step is available in the wizard if there are some recipes created in the cloud. You can create a virtual server without a recipe and add them afterwards. To assign a recipe to your virtual server in the wizard, follow the next steps:

1. Drag and drop a recipe from the *Available recipes* to *Assigned for provisioning* box.

2. To add a custom variable, click the "+" button next to the *Custom recipe variables* title bar, then specify variable details:
   - *Name & Value* - enter a name and value for the custom variable
   - *Enabled* - move the slider to the right to allow use of this variable

3. Click *Next* to proceed to the next step of the wizard that completes the virtual server creation process.

### 3.2.1.9 Confirmation

The *Confirmation* step allows you to apply the following settings:
• **Build Virtual Server** - move the slider to the right to automatically build the virtual server. If you don't select this checkbox, you have to build your server manually after it is created.

• **Boot Virtual Server** - move the slider to the right for the virtual server to be started up automatically.

The **Confirmation** step also provides the configuration summary of the virtual server, including information about the template, CPU cores, RAM, disks size, and network. When you are finished, click the **Create Virtual Server** button to start the creation process. After you click the button, several transactions are run to complete the process. You can check a status of each transaction in Activity Log of the virtual server.

### 3.2.2 Create Instance Package vCenter Virtual Servers Beta

You can create a vCenter virtual server from a ready-made instance package. The instance package is a preconfigured environment with a specific compute, storage, and network capacity. For instance packages to be available in the wizard, your Administrator needs to configure an environment where:

• Instance packages permissions are enabled
• Instance packages are added to your Control Panel
• Instance packages are added to your bucket

After you complete these steps, you can create vCenter virtual servers from instance packages in the wizard. The wizard walks you through several steps to get your virtual server up and running. In this document, you can find a detailed guidance on how to create a vCenter virtual server, but first take a look at the following section.

---

### 3.2.2.1 Before You Begin

**On this page:**

• [Before You Begin](#)
• [Infrastructure Mode](#)
• [Cloud Locations](#)
• [Templates](#)
• [Properties](#)
• [Instance Packages](#)
• [Service Add-Ons or Recipes](#)
• [Confirmation](#)

**See also:**

• [Create Custom Virtual Server](#)
• [Permissions](#)
• [Buckets](#)

Before you begin to create a virtual server from an instance package, take into consideration the following:

• You should have an environment properly configured by your Administrator. The environment must provide at least one compute resource configured and attached to a compute zone, a data store – to a data store zone and compute resource or zone,
a network – to a network zone and compute resource or zone, a backup server – to a backup server zone and compute resource or zone, and a **bucket** – to a user who creates a virtual server.

- If an instance package applies only to certain compute zones in a **bucket**, a virtual server is created on one of the compute resources within one of those zones. If an instance package is not limited to certain zones, the compute zone and compute resource are selected automatically from the ones available to a user.
- Instance package virtual servers can be created only in compute zones where all compute resources are assigned the same number of CPU units. If there are compute resources with different number of CPU units, it’s not possible to create instance package virtual servers in such zones. The reason is that CPU priority for instance package virtual servers in this configuration cannot be set to 100%, which is the default value for such virtual servers.
- If there are no available IP addresses, all instance packages are dimmed in the wizard.
- Instance packages that have resources incompatible with the available compute zones are dimmed in the wizard.
- **Auto-scaling** and **Accelerator** are not supported for virtual servers created from instance packages.

To create a virtual server, follow the next procedure:

1. Go to your Control Panel and click **Create Server** on the top bar.
2. Click **Create Virtual Server Beta** to launch the wizard.
3. Follow the step-by-step instructions below to complete the wizard.
4. After you are finished, click the **Create Virtual Server** button.

### 3.2.2.2 Infrastructure Mode

An infrastructure mode allows you to manage with OnApp only the infrastructure layer without any post actions (e.g. formatting disk after adding it, or assigning an IP address after adding a network interface). To create the Instance Package vCenter virtual server in infrastructure mode, you need to have the **Infrastructure mode permission** enabled for your role and move the **Infrastructure mode** slider to the right at the **Properties** step in the wizard.

### 3.2.2.3 Cloud Locations

The **Cloud Locations** step is available for users whose bucket includes compute zones assigned to **location groups**. If Cloud Locations are not available, the wizard starts from the **Templates** step. The **Cloud Locations** step is present in the wizard if the following requirements are satisfied:

- All compute zones that are added to a user’s bucket are assigned to location groups.
- Compute zones that are added to a user’s bucket are not assigned to the same location group.

When you are at the **Cloud Locations** step, select a location for your virtual server:

- **Country** - select a country where the cloud is located
- **City** - select a city from the country where the cloud is located

Click **Next** to proceed to the following steps of the wizard.
The Templates step allows you to select a template from which to build your virtual server.

To select a template, follow the next procedure:

1. Click a Template Store icon on the left to see templates that are available in this store. You can see the following details for each template:
   - **Label**
   - **Min memory size** that is required to create a VS from this template
   - **Min disk size** that is required to create a VS from this template
   - **Virtualization type** that is XEN or KVM
   - **Estimated Price per Hour** that is calculated for a VS in Mode ON and Mode OFF

2. Click a template to select it.
3. Click Next to proceed.

**Additional Information for Windows Templates**

The Windows Licensing Type box appears for Windows templates and includes license options that you configure for a corresponding template store. You can select one of the following license types:

- **MAK** - the default licensing type applicable to all Windows-based virtual servers. If you don't select the licensing type, MAK is set by default.
- **KMS** - the licensing type applicable to every virtual server since Windows 7, Windows Server 2008, and the following Windows versions. Click KMS and then select a licensing Server.
- **User license** - type your license key

When you create a virtual server from a Windows template, consider the following:

- You can create Windows-based virtual servers without running Sysprep. Disable the Run Sysprep option while creating or editing a destination compute zone.
- If multiple virtual servers are deployed from the same template without running Sysprep, they will have identical security identifiers (SIDs) that can result in the system conflict.
- You can't select KMS or your own license when you create a Windows virtual server from a custom template. As a workaround, you can create a virtual server from a template used for custom template creation.
- You can build a Windows 10/Windows Server 2016 virtual server on KVM CentOS 6 and CentOS 7 compute resources that run at least on the following processor:
  - Ivy Bridge Intel® Xeon® Processor E Series v2 Family
  - AMD Opteron G2, G3, G4, G5, and G6
3.2.2.5 Properties

There are some obligatory and optional properties that you can provide for your virtual server. The obligatory properties are marked with an asterisk on the list and the optional properties you can edit after creating a virtual server.

Enter the following properties for your virtual server:

- **Infrastructure mode** - move the slider to the right to enable the **Infrastructure mode** for this virtual server
- **Label** - enter a label of the virtual server
- **Hostname** - enter a hostname of the virtual server. The hostname can consist of letters [A-Z a-z], digits [0-9], and dash [-]. For more info on hostname validation, refer to [RFC documentation](https://tools.ietf.org/html/rfc1123).

**Additional Consideration for Windows**

- The hostname length should be between 1 and 15 characters.
- The following symbols are not allowed for Windows-based virtual servers:
  - percent sign [%]
  - double quotation marks [“]
  - brackets [<>]
  - vertical bar [|]
  - caret [^]
  - ampersand [&]
  - parentheses [(,)]
- **Domain** - enter a domain of the virtual server. For example, in `test.onapp.com` the `test` is a hostname and `onapp.com` is a domain. If you don't enter a domain, the default value `localdomain` is used as follows `test.localdomain`. This parameter is not applicable to Windows virtual servers.
- **Time zone** (Windows) - select a time zone for a Windows virtual server. Most operating systems implies that the hardware clock is in UTC, however, Windows implies a `localtime`. Therefore, you need to select a time zone for it to be properly handled on a compute resource level.
- **Password** - enter a secure password for the virtual server. It can consist of 6-99 symbols, including letters [A-Z a-z], digits [0-9], dash [-], underscore [ _ ], and the following special characters: ~ ! @ # $ * _ + = \ { } [ ] : ; ' , . ? / You can use both lower and uppercase letters. If you don't enter a password, it will be generated automatically.
- **Password confirmation** - repeat the password to confirm it
- **Encrypt password** - move the slider to the right to encrypt your password. For more information on password encryption, see [FAQ](https://www.onapp.com/support/faq).
- **Encryption passphrase** - enter a passphrase for encryption
- **Encryption passphrase confirmation** - repeat the passphrase for encryption
- **I want to create a VS with custom resources** - select the checkbox to create a virtual server based on a set of custom resources. The checkbox is displayed only if the Select resources manually on virtual server creation permission is enabled. See Create Custom vCenter Virtual Server for details.

Click **Next** to proceed to the following step of the wizard.

### 3.2.2.6 Instance Packages

To create a virtual server from an instance package, click a box for a corresponding package. The instance package box includes the following details:

- **CPUs** - the number of CPU cores available in this instance package
- **Memory** - the number of RAM in MB or GB available in the instance package
- **Disk Size** - the number of disk size in MB or GB available in this instance package
- **Bandwidth** - the number of bandwidth in MB or GB available in this instance package
- **Price per Hour:**
  - **Mode ON** - an estimated hourly price if the virtual server is powered on
  - **Mode OFF** - an estimated hourly price if the virtual server is powered off
- **Price per Month:**
  - **Mode ON** - an estimated monthly price if the virtual server is powered on
  - **Mode OFF** - an estimated monthly price if the virtual server is powered off

After you click an instance package box, it becomes highlighted in green. Click **Next** to proceed to the following step of the wizard.

### 3.2.2.7 Service Add-Ons or Recipes

During this step, you can assign service add-ons or recipes to your virtual server. The availability of service add-ons or recipes depends on your cloud configuration.

#### 3.2.2.7.1 Service Add-ons

Service add-ons are available under the following conditions:

- The Replace Recipes with Service Add-ons on VS Creation permission is enabled.
- Service add-on groups are available in a bucket.
- The On Provisioning option is enabled for all or some of the service add-ons available to you within a bucket.

If these conditions are not satisfied, you will see the **Recipes** step instead.

You can create a virtual server without service add-ons and add them afterwards. To assign a service add-on to your virtual server in the wizard, follow the next steps:

1. Click a service add-on group on the left to expand the list of service add-ons on the right. You can see the following details about each service add-on:
   - **Label**
   - **Description**
2. Click the service add-on to select it. You can select several add-ons from different service add-on groups. Click View Selected Add-ons to see the list of selected service add-ons.

To remove the selected service add-on from the list, click the button.

3. Click Next to proceed to the final step of the wizard.

Recipes
The Recipes step is available in the wizard if there are some recipes created in the cloud. You can create a virtual server without a recipe and add them afterwards. To assign a recipe to your virtual server in the wizard, follow the next steps:

1. Drag and drop a recipe from the Available recipes to Assigned for provisioning box.

2. To add a custom variable, click the "+" button next to Custom Recipe Variables and provide the following details:
   - Name & Value - enter a name and value for the custom variable
   - Enabled - move the slider to the right to allow use of this variable

3. Click Next to proceed to the final step of the wizard.

3.2.2.8 Confirmation

The Confirmation step provides the configuration summary of the virtual server, including information about CPU, memory, and disk size. Here you can also apply the following settings:

- **Enable Automated Backup** - move the slider to the right to create automatic backups of the virtual server based on the settings from Auto-Backup Presets.
- **Build Virtual Server** - move the slider to the to the right if you want the system to automatically build the virtual server. If you don't select this checkbox, you have to build your server manually after it is created.
- **Boot Virtual Server** - move the slider to the right if you want the virtual server to be started up automatically.

When you are finished, click the Create Virtual Server button to start the creation process. After you click the button, several transactions are run to complete the process. You can check a status of each transaction in Activity Log of the virtual server.

3.3 View vCenter Virtual Servers Details

To view details of a specific vCenter virtual server:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. The screen that appears loads the VS properties, notes, activity log and tools for managing your virtual server.

3.3.1 VS Properties

VS properties page gives the general overview of the VS details:
• Template this VS is built on
• Power status & On/Off/Reboot buttons.

Clicking the OFF button performs graceful shutdown and then powers off the virtual server after the timeout set in Configuration settings.

• Compute resource. Click the compute resource name to see its details
• Login credentials
• Owner. Click the owner name to see its details.
• Price per hour
• Memory
• CPU(s)/shares
• Disk Size
• Disk backups (irrelevant field)
• Network Speed
• IP Addresses. Only the first five IP addresses are displayed on the virtual server properties page. To view the list of all virtual server IP addresses, mouse over IP addresses area or go to the Networking > IP addresses tab.

If the automation options weren’t enabled during this virtual server creation, you’ll be redirected to the form where you can configure them.

3.3.2 Notes

The Notes section lists brief comments or reminders for a VS. You can add either admin's or user's notes. The admin's note will be available to cloud administrators. Click the Actions button in the Notes section of the page to add admin's or user's note.

3.3.3 VS Management

• Click the Tools button to expand the Tools menu with the VS management options.
• Use the top menu to manage your virtual servers' statistics/networking/storage options.

3.4 Edit vCenter Virtual Servers

You can edit CPU and RAM resources for vCenter virtual servers built on Windows and Linux templates, as well as Windows and Linux OVA templates.

To edit CPU and RAM resources, follow the next steps:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click a label of the server you want to resize to display its details screen.
3. Click the Tools button and select the Edit Virtual Server link.
4. Change the label, CPU core/priority and RAM values, and click the Save button. After you save the settings, the resize is completed automatically and you can see a message indicating the resize was successful.

3.5 Delete vCenter Virtual Servers

Shut down the VS before destroying it. If you are deleting a VS that is running, the VS will be deleted after the time set in Timeout Before Shutting Down VSs configuration parameter.

To remove the virtual server from the cloud:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. On the screen that appears, you'll see the list of all virtual servers in the cloud. Click the label of the virtual server you want to delete.
3. On the VS's screen, click the Tools button, then select Delete Virtual Server.
4. Click the Destroy button.

You won't be able to restore a VS after deleting it.

3.6 Build vCenter Virtual Servers Manually

To build/rebuild virtual server build/rebuild virtual server must be enabled. This is a new permission which manages build/rebuild functionality independently from update virtual server permission which used to regulate the build/rebuild options in the previous versions.

If you haven't checked the Build Virtual Server Automatically option during the VS creation process, you will have to do this manually after the VS has been created. Building a virtual server is the process of allocating physical resources to that VS.

To build a virtual server manually:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. On the screen that appears, click the Tools button and then click Rebuild Virtual Server.
4. On the screen that pops up, use the drop-down menu to choose a template with which to build the VS.
5. Tick the Required Start Up box to have your VS started automatically after it is built.
6. Click the Build Virtual Server button to finish.
3.7 Clone vCenter Virtual Servers

You can create a clone of a virtual server based on the same resources as the origin virtual server. To be able to clone virtual servers, you need to have the *Clone own virtual servers* permission enabled. The cloned virtual server inherits resources from the origin as follows.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Cloned Virtual Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties - owner, hostname, password, and label.</td>
<td>The same as the origin virtual server with <em>Clone</em> in the label, for example, <em>Clone Origin Label</em>.</td>
</tr>
<tr>
<td>Compute, data store, and network resources &amp; zones</td>
<td>The same as the origin virtual server. If there are no available resources on the same data store, network, and compute resource, you cannot clone a virtual server.</td>
</tr>
<tr>
<td>Recipes, recipe variables, and service add-ons</td>
<td>The same as the origin virtual server.</td>
</tr>
<tr>
<td>Firewall rules</td>
<td>A random IP address is assigned from an IP range in the origin network.</td>
</tr>
<tr>
<td>Swap disk</td>
<td>A new swap disk is created on the cloned virtual server.</td>
</tr>
<tr>
<td>Backups</td>
<td>The backups of the origin virtual server are not cloned.</td>
</tr>
</tbody>
</table>

To clone a virtual server, follow the next procedure:

1. Go to your Control Panel > **Cloud** > **Virtual Servers**.
2. Click a label of the virtual server that you want to clone.
3. Click **Tools** and then click **Clone Virtual Server**.
4. In the pop-up box, click **Clone Virtual Server** to confirm the action.

After you confirm the action, several transactions are run to complete the cloning process. You can check a status of each transaction in **Activity Log** of the virtual server. After the virtual server is cloned, it is powered off until you start it.

3.8 Auto Import vCenter Virtual Server

If you need a quick import of multiple new VSs from vCenter to OnApp, use the auto import rules functionality. It allows you to apply the rule/rules to the already created but not yet imported virtual servers. After applying auto import rules, vCenter resources are recognized at OnApp side and can be billed immediately.

**Prerequisites**

- The auto import rule functionality is available on clouds that run OnApp 6.1 Edge 2 and subsequent versions.
• The **Manage auto import rules** permission should be enabled for a user who wants to view, create, run, edit or delete auto import rules.

• It only applies to the newly created vCenter virtual servers that are not yet imported to OnApp.

On this page:

• **View Auto Import Rules**
• **Create Auto Import Rule**
• **Run Auto Import Rule**
• **Edit Auto Import Rule**
• **Delete Auto Import Rule**

### 3.8.1 View Auto Import Rules

To view the list of auto import rules:

1. Go to your Control Panel > **Admin** > **Settings** menu.
2. Click the **Compute Resources** icon.
3. Go to vCenter compute resource's label > Tools and click **Auto Import Rules** to see a list of all rules and the following details:
   - **Label** - the name of the vCenter VS
   - **Source Type** - the type of vCenter source
   - **Source** - the vCenter resource
   - **Target Type** - the type of vCenter target user
   - **Target** - the vCenter user, who is an owner of the virtual server
4. Click the **Actions** button next to the auto import rule for quick access to the list of available actions.
5. To edit an auto import rule, click the **Edit** button.
6. To run an auto import rule, click the **Run** button.

### 3.8.2 Create Auto Import Rule

To create auto import rules:

1. Go to your Control Panel > **Admin** > **Settings** menu.
2. Click the **Compute Resources** icon.
3. Go to vCenter compute resource's label > Tools and click **Auto Import Rules**.

![Auto Import Rules screen](image-url)
4. Click the **Create Auto Import Rules** button.

5. On the screen that follows, fill in the following:
   - **Label** - specify the name of the vCenter VS
   - **Source Type** - choose the type of vCenter source from the drop-down list
   - **Source** - choose the vCenter resource from the drop-down list
   - **Target Type** - choose the type of vCenter target user from the drop-down list
   - **Target** - choose the vCenter user from the drop-down list, who will be an owner of the virtual server

6. Click **Submit**.

### 3.8.3 Run Auto Import Rule

To run an auto import rule:

1. Go to your Control Panel > **Admin** > **Settings** menu.
2. Click the **Compute Resources** icon.
3. Go to vCenter compute resource's label > Tools and click **Auto Import Rules**.
4. Click the **Actions** button next to the auto import rule you want to run and click the **Run** button.

After you click the **Run** button, OnApp system receives the list of vCenter VSs suitable for this rule and schedules proper import transactions.

### 3.8.4 Edit Auto Import Rule

To edit an auto import rule:

1. Go to your Control Panel > **Admin** > **Settings** menu.
2. Click the **Compute Resources** icon.
3. Go to vCenter compute resource's label > Tools and click **Auto Import Rules**.
4. Click the **Actions** button next to the auto import rule you want to edit and click the **Edit** button.
5. Edit the following details:
   - **Label** - specify the name of the vCenter VS
   - **Source Type** - choose the type of vCenter source from the drop-down list
   - **Source** - choose the vCenter resource from the drop-down list
   - **Target Type** - choose the type of vCenter target user from the drop-down list
Target - choose the vCenter user from the drop-down list, who will be an owner of the virtual server

6. Click the Submit button.

3.8.5 Delete Auto Import Rule

To delete an auto import rule:
1. Go to your Control Panel > Admin > Settings menu.
2. Click the Compute Resources icon.
3. Go to vCenter compute resource's label > Tools and click Auto Import Rules.
4. Click the Actions button next to the auto import rule you want to delete and click the Delete button.
5. Click the OK button to confirm the deletion.

3.9 vCenter Virtual Servers Power Options

To manage vCenter virtual server power options:
1. Go to your Control Panel > Cloud > Virtual Server menu.
2. Click the label of the required virtual server.
3. Click the Tools button on the VS's screen to expand the VS Tools menu.
4. The Tools menu enables you to perform the following power actions on VSs (the exact list shown depends on the VS status):
   - Reboot Virtual Server - powers off and then restarts the VS.
   - Suspend Virtual Server - stops a VS, changes its status to suspended and disables all the other actions on VS, unless unsuspended.
   - Shut Down Virtual Server – pops up a dialogue box, where you can either Shut Down VS (terminates the VS gracefully), or Power Off VS (terminates the VS forcefully).
   - Startup Virtual Server - queues a start-up action for a VS that's currently powered off.

3.10 vCenter Virtual Servers Console

Currently, vCenter virtual server console is not available if you are using vCenter version 6.0 update 3 or later.

You can use the virtual server console to manage your virtual servers in command line mode.
To use the VS console:
1. Go to Control Panel > Cloud > Virtual Servers menu.
2. Click the Label of appropriate Virtual Server.
3. Go to Console tab and click MKS. The console window will appear.
3.11 vCenter Virtual Servers Transactions and Logs

The system records a detailed log of all the transactions happening to your virtual servers. The list of transactions logged by the system includes:

- Provision virtual server
- Startup virtual server
- Stop virtual server
- Resize virtual server without reboot
- Configure Operating System
- Build disk
- Resize disk
- Format disk
- Destroy disk
- Destroy virtual server
- Destroy template
- Download template
- Update firewall

To view transactions for a virtual server:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. The details screen for that virtual server shows recent transactions in the Activity Log section. To view more transactions, click the More Logs button.

To cancel pending tasks, click Cancel All Pending Tasks for this virtual server.

3.12 vCenter Virtual Servers Networks

The Networking menu in the Virtual Servers menu enables you to manage network interfaces and allocate IP addresses.

3.12.1 Configure vCenter Virtual Servers Network Interface

The Networking > Network Interfaces menu shows the virtual network interfaces allocated to this VS. Network interfaces join the physical network to the VS. When you create a VS a network interface is added automatically. This network interface will be assigned to the existing physical network using a spare IP (IPv4) and will be set primary by default. OnApp supports IPv4 and IPv6. Since not every application supports IPv6, at least one IPv4 address must be allocated to a VS's primary network interface.

To see the list of all network interfaces allocated to the VS:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Networking tab, then click Network Interfaces.
4. On the page that follows you will see the following fields:

- Interface – optional label of the network interface.
- **Network join** – name of the network and a compute resource or compute zone this network is joined to.
- **Port speed** – the speed set to the interface.
- **Primary interface** – indication whether the interface is primary or not.

Here you can also view Interface Usage, Edit and Delete network interface (using icon controls) and Add a new network interface using the button at the bottom of the screen.

To add a network interface:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Click the label of the virtual server you’re interested in.
3. Click the **Networking** tab, then click **Network Interfaces**.
4. Click the **Add New Network** Interface button at the bottom of the screen.
5. On the screen that appears, input values for the following parameters:
   - **Label** – a human-friendly name for the new interface.
   - **Physical Network** – choose a network join from the drop-down menu, which lists network joins assigned to the compute resource/compute zone on which the VS runs).
   - **Port speed** – set port speed in Mbps, or make it unlimited.
6. Click the **Add Network Interface** button.

To edit network interface label, port speed or set it as primary (if none is marked as primary), click **Edit** icon next to the appropriate network interface. After editing the port speed, the virtual server should be power cycled for the change to take effect.

To delete a network interface, click the **Delete** icon next to the interface you want to delete.

To run the VS, at least one network interface with an assigned IP address (or addresses) is required!
To allocate another physical network, add a new network interface.

### 3.12.2 Rebuild vCenter Virtual Servers Network

To rebuild network join, added to the virtual server (required after allocating new IP addresses):

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Click the label of a required VS.
3. On the screen that appears, click the **Tools** button, then click **Rebuild Network**.
4. In the pop-up window that appears, move the **Force Reboot** slider to the right, then select the VS shutdown type:
   - Power OFF virtual server
   - Shutdown virtual server
   - Gracefully shutdown virtual server
5. Move the **Required Startup** slider to the right to start up the VS automatically after the network is rebuilt.
6. Click the **Rebuild Network** button.
3.12.3 Allocate/Remove vCenter Virtual Servers IP Addresses

In the Networking > IP Addresses tab you can find the list of assigned IP addresses, allocate new IP addresses and rebuild a network.

To allocate a new IP Address to the VS:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Networking tab, then click IP Addresses.
4. Click the Allocate New IP Assignment button.
5. Select a network interface from the drop-down menu (only the network interfaces you added to the VS will be available)
6. Select an IP address from the IP Pool associated with the network interface. You may select an IP address that's already assigned to a VS, but only one VS should be online at a time.
   Use Please show me used IP Pool, Show only my IPs and Show only IPv6 checkboxes to narrow the list of IP in the drop-down list.
7. Click the Add IP Address Assignment button.
8. Click the Rebuild Network button to rebuild the network.

You must rebuild the network after making changes to IP address allocations.

To remove an IP address from a VS:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Networking > IP Addresses tab.
4. Click the Delete icon next to the IP address you want to delete.
5. In the pop up window that appears:
   - Choose Delete with Reboot option if you want to reboot a VS and rebuild the network immediately after deleting the IP address. After choosing the Delete with Reboot option you will be redirected to the VS's Overview page.
   - Choose Delete without Reboot option if you don't want to reboot a VS. In this case to apply the changes, you will have to the reboot the VS additionally.

You can't delete an IP address that is in use.

3.12.4 Display Network Speed for Network Interfaces on vCenter Virtual Servers Page

The main Virtual Servers screen displays the network speed of each VS's primary network interface. To see the speed of all interfaces assigned to a VS:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you are interested in.
3. Click the Networking > Network Interfaces tab.
4. On the screen that appears, the **Port Speed** column shows the network speed of the network interface.

### 3.12.5 Edit vCenter Virtual Servers Network Speed

To edit a vCenter virtual server's network speed:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Select the virtual server you want to change.
3. Go to the **Network** > **Network Interfaces**, and edit the network speed accordingly.
4. Click the **Save Network Interface** button to save changes.

### 3.13 vCenter Virtual Servers Disks

Virtual server storage is provided by disks. A disk is a partition of a data store that is allocated to a specific virtual server. Disk can be set as primary (that is, the disk from which an OS will boot).

Managing disks for the entire cloud is handled through the Control Panel's Settings menu. Disks for individual virtual servers are managed through the Control Panel > **Cloud** > **Virtual Servers** menu, where you can:

- See the list of disks allocated to this VS
- **Add a new disk**
- **Resize a disk**
- **Check disk usage statistics (IOPS)**
- **Delete a disk**

#### 3.13.1 Edit vCenter Virtual Servers Disks

You can easily resize disks when needed. The resize will fail if your current usage is greater than the new size you request.

To change disk size:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Make sure your virtual server is powered off, then click its label to open its details screen.
3. Click the **Storage** tab > **Disks**.
4. Click the **Actions** button next to the disk you want to change, then click the **Edit** link.
5. Enter a new disk label and size in GB in the fields provided.
6. Click the **Save Disk** button.

For Linux-based VSs, it is necessary to rescan or **reboot** a VS after increasing its disk size.

#### 3.13.2 Migrate vCenter Virtual Servers Disks

You can migrate disks of your virtual servers to other data stores, which are allocated to the same compute resource or compute zone. Unlike **VS migration** – disk migration requires reboot
To migrate a disk:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Make sure your virtual server is powered off, then click its label to open its details screen.
3. Click the **Storage > Disks**.
4. Click the **Actions** button next to the disk you want to move to another data store, then click the **Import** link.
5. On the screen that appears, select a target data store from a drop-down box.

You can only migrate disks to data stores in data store zones assigned to your bucket.

6. Click **Start Migrate**.

You cannot migrate a disk to a data store with less capacity than the disk size!
If you move an 850GB disk between aggregates with 10GB actual usage, the 'dd' image of the local volume manager will take 850GB space, because the entire local volume manager is copied, including zero 'd space which may not be able to be recovered.

---

### 3.13.3 Delete vCenter Virtual Servers Disks

To delete a disk:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Make sure your virtual server is powered off, then click its label to open its details screen.
3. Click the **Storage > Disks** tab.
4. Click the **Actions** button next to the disk you want to delete, then click **Delete**.

### 3.13.4 Add Disks to vCenter Virtual Server

Adding a disk to a virtual server will require VS to be rebooted. If a VS is running when you try to add a new disk to it, you'll be asked to confirm the reboot. To add a disk to a virtual server:

1. Go to your Control Panel > **Cloud** > **Virtual Servers** menu.
2. Click a VS's label to open its details screen.
3. Click the **Storage > Disks**.
4. Click the **Create Disk** button.

5. Fill in the details:
   - **Data store** - select the data store to create a disk on from the drop-down list.
   - **Disk size**
   - **Swap Space** - move slider to the right if this disk is swap space.
   - **Require Format Disk** - move slider to the right if this disk requires formatting.

   For Linux-based vCenter VSs, if the **Require Format Disk** option is enabled, you'll get a notification that VM will be rebooted. If the option is disabled, disk will not be formatted, but will also not be visible without the VS rescan or reboot.

   - **Mounted** - move slider to the right if the disk should be added to Linux FSTAB (for Linux application servers).
   - **Mount point** - the maximum length of a Mount Point is 256 characters. Spaces are not allowed. No more than one slash is allowed. If the mount point is not specified the default mount point will be used:

     ```
     /mnt/onapp-disk-#{disk.identifier}
     ```

   - **Reboot Virtual Server** - move the slider to the right to reboot the VS after adding the disk (applies only to Linux-based vCenter VSs)

6. Click the **Add Disk** button to finish.

When you add a new disk to a virtual server it will automatically become available to that server.

### 3.14 vCenter Virtual Servers Statistics

For your convenience, the system tracks VS performance and generates statistics on:

- **VS CPU Utilization**
- **VS Billing statistics**
- **Interface Usage**
- **Disk IOPS**

#### 3.14.1 vCenter Virtual Servers CPU Utilization

OnApp tracks CPU usage for virtual servers and generates charts that help analyze VS performance.

The charts show the total CPU usage for all the cores of this particular VS for a specified time period. The vertical axis shows the CPU usage percentage (CPU percentage is the core-independent quantity). The horizontal axis defines a time period.

To see CPU usage statistics:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Overview > CPU Usage.
4. On the screen that appears, the top chart shows CPU usage for the last 24 hours. The bottom chart shows usage for the last three months (if there is enough data). If there less data available, the chart will show utilization for the time available.
5. Tick the Show in My Timezone box to show bandwidth statistics according to your profile's time zone settings.
6. To zoom into a time period, click and drag in a chart. Click the Reset Zoom button to zoom out again.

To see what percentage of compute resource's CPU resource a VS takes, go to your Control Panel > Cloud > Virtual Servers menu and click the label of the VS you're interested in. On the screen that appears, the CPU(s)/Shares parameter displays the amount of CPU resource given to this VS.

3.14.2 vCenter Virtual Servers Billing Statistics

OnApp has a record of all the charges applied to your VSs for the last three month period. If a virtual server was created less than three months ago, statistics are recorded for the VS's existence to date. You can view all statistics available, or those for a shorter period by setting a Start and End time.

To view billing statistics for a virtual server:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Overview > Billing Statistics tab.
4. Set Start and End time. By default the statistics are generated for the last three months or the actual VS existence period.
5. Tick the Show in My Timezone box to show bandwidth statistics according to your profile's time zone settings.
6. On the page that appears:
   - Date – particular date and time for the generated statistics
   - Users – the virtual server owner. Click the owner name to see the User Profile (user details)
   - Virtual Servers – the virtual server name with the total due for VS resources (CPU priority, CPUs, memory and template resources) for the point of time specified in the Date column.
   - Network Interfaces Usage – the total due for the network interfaces used by this VS for the point of time specified in the Date column. Click the network interface name to see its details.
   - Disks Usage – the list of disks assigned to this VS with the total due for the disk space resources (disk size, data read/written, reads/writes completed) for the point of time specified in the Date column. Click the disk name to see its details.
   - Costs – the total due for the Virtual servers, Network Interfaces and Disks resources at the point of time specified in the Date column.

Scroll down to see Total Amount (the total due for the whole billing statistics period).
3.14.3 vCenter Virtual Servers Network Interface Statistics

OnApp tracks network usage for virtual servers and generates charts that help analyze network performance. To see network utilization statistics for a virtual server:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Networking > Network Interfaces tab.
4. Click the Statistics (chart) icon next to the network you're interested in.
5. On the screen that appears, the top chart shows bandwidth usage for the last 24 hours. The bottom chart shows usage for the last three months.
6. To zoom into a time period, click and drag in a chart. Click the Reset zoom button to zoom out again.

3.14.4 vCenter Virtual Servers Disk IOPS

The system tracks IOPS (Input/Output Operations per Second) for virtual servers and generates charts that help analyze VS disk performance. The data presented in the chart are for the periods during which the statistics was gathered, typically 3 minutes. To see IOPS for a virtual server:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the Storage > Disks tab.
4. Next to the necessary disk, click the Actions button and select the IOPS option.
5. There are four charts on the screen that appears:
   - Instant IOPS - summary of input/output operations per minute
   - Hourly IOPS - summary of input/output operations per hour
   - Instant Data Written/Read - summary of written and read data for the last 24 hours
6. To zoom into a time period, click and drag in a chart. Click the Reset zoom button to zoom out again.

The OnApp API allows you to limit the Hourly IOPS and Hourly data by setting the limit=N parameter, where the N variable is the number of hours for which the charts will display the info.

3.15 Manage vCenter Virtual Servers Recipes

SSH connection between VS and Control Panel is required for running recipes on vCenter virtual servers.

To manage virtual server recipes:

1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the virtual server you're interested in.
3. Click the **Overview** tab, then choose **Recipes**.

4. The screen that follows shows details of all the recipes in the cloud:
   - The left pane shows the list of available recipes organized into recipe groups.
   - The right pane displays the list of events to which the recipes can be assigned to. Click the arrow button next to event to expand the list of recipes assigned to it.

**Assign recipe**

Use drag and drop feature to assign recipe to assign a recipe to a desired event.

You can assign virtual server recipes to the following events:

- **VS provisioning** - run the recipe during the virtual server provisioning
- **VS network rebuild** - run the recipe while rebuilding a network
- **VS disk added** - run the recipe while adding a disk to the virtual server
- **IP address allocated for VS** - run the recipe when adding an IP address to the VS network interface
- **IP address revoked from VS** - run the recipe when removing an IP address from the VS network interface
- **VS network interface added** - run the recipe while adding a network interface to the virtual server
- **VS network interface removed** - run the recipe while deleting a network interface from the virtual server
- **VS disk resized** - run the recipe while resizing a virtual server disk
- **VS resize** - run the recipe while resizing the virtual server
- **VS IP address add** - run the recipe while adding an IP address the virtual server
- **VS IP address remove** - run the recipe while removing an IP address from the virtual server
- **VS start** - run the recipe while starting the virtual server
- **VS reboot** - run the recipe while rebooting the virtual server
- **VS hot migrate** - run the recipe during the hot migration of the virtual server
- **VS hot full migrate** - run the recipe during the hot migration of the virtual server with disk
- **VS failover** - run the recipe during the failover process

**To use drag and drop:**

1. Click the arrow button in front of the required event to unfold it.
2. Select the required recipe in the right pane and hold it down with the left mouse button.
3. Drag the recipe up to the left pane and release the mouse button to drop the recipe and add it to the required event.

**Remove recipe**

To remove recipe:

1. Click the arrow button in front of the required event to view the list of recipes assigned to it.
2. Click the **Delete** button next to the recipe you want to remove.
3.16 Manage vCenter Virtual Servers Custom Variables

SSH connection between VS and Control Panel is required for running recipes on vCenter virtual servers.

You can define custom variables for particular virtual servers. Each custom variable is a name-value set that can be used during the virtual server recipe implementation. Custom variables are set on a per server basis. You can create custom variables during the virtual server creation or via the virtual server Overview menu.

To create a new custom variable:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. You'll see a list of all virtual servers in your cloud. Click the name of a virtual server for which you want to create a variable.
3. On the virtual server details screen, click the Overview tab, then choose Recipes Variables.
4. On the screen that appears, click the "+" button.
5. Specify the recipe name and its value.
6. Move the Enabled slider to the right to allow use of this recipe.
7. Click Save.

To edit a custom variable, click the Edit icon next to the required variable and change its details.

To delete a custom variable, click the Delete icon next to the variable you want to remove. You will be asked to confirm the deletion.

It is possible to set custom variables for image templates, as well as for virtual servers. Virtual server custom variables will always overlay template custom variables.

3.17 VMware Virtual Servers Snapshots

VMware snapshot tools are used to perform snapshots by simply locking the filesystem disk (vmdk) and creating a new VMware disk with the changes made alongside, so the procedure for virtual servers running under VMware looks like: vmdk + vmdk(1) + vmdk(#).

To view the list of VS Snapshots:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the server you want to back up.
3. Click the Tools button > Snapshots.
4. On the screen that appears, you'll see the list of all VS snapshots.

To create a snapshot for vCenter VS:
1. Go to your Control Panel > Cloud > Virtual Servers menu.
2. Click the label of the server you want to back up.
3. Click the **Tools** button > **Snapshots**.
4. Click the **Create New Snapshot** button.
5. Give your snapshot a name.
6. Click **Create Snapshot** button.

To delete a VS snapshot, click the **Actions** button next to the required snapshot, then click **Delete**.

### 3.18 vCenter VS Console

- Currently, vCenter virtual server console is not available if you are using vCenter version 6.0 update 3 or later.
- To be able to use the MKS console on vCenter virtual servers, VSs must not be configured for VNC access in vCenter.

You can use the virtual server console to manage your virtual servers in command line mode. To use the VS console:
1. Go to **Control Panel** > **Cloud** > **Virtual Servers** menu.
2. Click the **Label** of appropriate Virtual Server.
3. Go to **Console** tab and click **MKS**. The console window will appear.

### 3.19 vCenter Resource Pools

VMware vCenter resource pool determines how and when the provider virtual data center compute and memory resources are committed to the Org VDC. Resource pool allows you to delegate control over the resources of a host or a cluster. For instance, you may use it to divide all resources in a cluster into sections.

Below you can find instructions on how to manage the vCenter resource pools.

This functionality is available for users with the following permissions enabled:
- Any actions on vCenter Resource Pools - the user can take any action on vCenter Resource Pool
- Add a new vCenter Resource Pool - the user can add a vCenter Resource Pool
- Delete any vCenter Resource Pool - the user can delete a vCenter Resource Pool
- Delete own vCenter Resource Pool - the user can delete own vCenter Resource Pool
- See any vCenter Resource Pool - the user can see any vCenter Resource Pool
3.19.1 View vCenter Resource Pool

To view the vCenter resource pools:

1. Go to your Control Panel > Cloud > Resource Pools menu to see an overview of all resource pools in the cloud.
2. The page that loads will show the list of resource pools with their details:
   - **Label** - the name of the resource pool
   - **Compute Zone** - compute zone on which the resource pool is placed
   - **Compute Resource** - compute resource on which the resource pool is placed
   - **Owner** - the resource pool owner
   - **Actions** - click the Actions button to edit or delete the resource pool

   The search box at the top right corner of the page allows you to search a resource pool by its label.

   To view vCenter resource pool details, click on the label of resource pool are interested in.

3.19.2 Create vCenter Resource Pool

To create a vCenter resource pool:

Go to your Control Panel > Cloud > Resource Pools menu to see an overview of all resource pools in the cloud.
Click the New Resource Pool button just below the list of resource pools.

On the screen that appears, fill in the resource pool creation form:

- **Label** - specify a name for the resource pool
- **Compute Resource** - select the required compute resource from the dropdown menu

   The CPU and RAM Limits of the new resource pool will be automatically unlimited, all other properties will be set to default.

Click the Submit button to save the changes.
3.19.3 Edit vCenter Resource Pool

To edit a vCenter resource pool:

Go to your Control Panel > Cloud > Resource Pools menu to see an overview of all resource pools in the cloud.
Click the Actions button next to the resource pool you want to edit, then click Edit.
On the screen that appears, edit the necessary parameters, then click Save.

You can also use the pencil button at the resource pool details page.

3.19.4 Delete vCenter Resource Pool

To delete a vCenter resource pool:

1. Go to your Control Panel > Cloud > Resource Pools menu to see an overview of all resource pools in the cloud.
2. Click the Actions button next to the resource pool you want to delete and click Delete.
3. Click OK to confirm the deletion.

Please note that if you delete the resource pool that has a virtual server on it, the VS will be moved to the cluster default resource pool.
4 API

The following sections provide the list of API requests to manage the vCenter components in OnApp. Refer to one of the following sections for details:

- Import vCenter VS
- Resync vCenter VS
- Auto Import Rules
- Add vCenter Compute Zone
- Add vCenter Compute Resource
- Edit vCenter Compute Resource
- Add vCenter VS
- Clone vCenter VS
- vCenter Templates
- vCenter Servers API
- vCenter Resource Pool API

For information on how to manage vCenter related resources in OnApp UI, refer to the Administration or the User guide.

4.1 Import vCenter VS

To import a vCenter virtual server into OnApp, use the following request:

```
POST /settings/hypervisors/:hypervisor_id/virtual_machines.xml
POST /settings/hypervisors/:hypervisor_id/virtual_machines.json
```

XML Request Example

```
```

JSON Request Example

```
```

Where:

- `vm_moref` - moref of the virtual server on vCenter
- `user_id` - the ID of a new owner in OnApp

4.2 Resync vCenter VS

To resync a vCenter virtual server into OnApp, use the following request:
POST /virtual_machines/:id/resync.xml
POST /virtual_machines/:id/resync.json

**XML Request Example**


**JSON Request Example**


**XML Output Example**
<virtual_machine>
  <id type="integer">2022</id>
  <hypervisor_id type="integer">156</hypervisor_id>
  <template_id nil="true"/>
  <identifier>bohpzakuuvzrwu</identifier>
  <hostname>mscentossnap</hostname>
  <memory type="integer">384</memory>
  <cpus type="integer">1</cpus>
  <cpu_shares type="integer">20</cpu_shares>
  <created_at type="dateTime">2019-09-03T11:41:52+03:00</created_at>
  <updated_at type="dateTime">2019-09-03T11:44:38+03:00</updated_at>
  <built type="boolean">true</built>
  <locked type="boolean">false</locked>
  <booted type="boolean">false</booted>
  <xen_id nil="true"/>
  <remote_access_password nil="true"/>
  <local_remote_access_port nil="true"/>
  <label>ms.centossnapfu</label>
  <recovery_mode nil="true"/>
  <user_id type="integer">376</user_id>
  <operating_system>linux</operating_system>
  <operating_system_distro>centos64Guest</operating_system_distro>
  <allowed_swap type="boolean">true</allowed_swap>
  <template_label nil="true"/>
  <min_disk_size nil="true"/>
  <allowed_hot_migrate nil="true"/>
  <note nil="true"/>
  <admin_note nil="true"/>
  <suspended type="boolean">false</suspended>
  <strict_virtual_machine_id nil="true"/>
  <enable_autoscale type="boolean">false</enable_autoscale>
  <add_to_marketplace nil="true"/>
  <state>delivered</state>
  <initial_root_password_encrypted type="boolean">false</initial_root_password_encrypted>
  <edge_server_type nil="true"/>
  <storage_server_type nil="true"/>
  <firewall_notrack type="boolean">false</firewall_notrack>
  <service_password nil="true"/>
  <preferred_hvs type="array"/>
  <local_remote_access_ip_address nil="true"/>
  <cpu_units type="integer">200</cpu_units>
  <cpu_sockets nil="true"/>
  <draas_keys type="array"/>
  <iso_id nil="true"/>
  <cores_per_socket type="integer">0</cores_per_socket>
  <instance_package_id nil="true"/>
  <hot_add_cpu type="boolean">false</hot_add_cpu>
  <hot_add_memory type="boolean">false</hot_add_memory>
  <time_zone nil="true"/>
  <autoscale_service nil="true"/>
  <cdboot type="boolean">false</cdboot>
  <draas_mode type="integer">0</draas_mode>
  <vapp_id nil="true"/>
  <vmware_tools nil="true"/>
  <vcenter_moref>vm-4532</vcenter_moref>
  <template_version nil="true"/>
  <openstack_id nil="true"/>
  <domain>localdomain</domain>
  <vcenter_reserved_memory type="integer">0</vcenter_reserved_memory>
  <deleted_at nil="true"/>
</virtual_machine>
<ip_addresses type="array"/>
<montly_bandwidth_used type="decimal">0.0</monthly_bandwidth_used>
<total_disk_size type="integer">3</total_disk_size>
<support_incremental_backups type="boolean">false</support_incremental_backups>
<cpu_priority type="integer">20</cpu_priority>
<built_from_iso type="boolean">false</built_from_iso>
<built_from_ova type="boolean">false</built_from_ova>
<acceleration type="boolean">false</acceleration>
<hypervisor_type>vcenter</hypervisor_type>
</virtual_machine>

Where:

id - id of the virtual server
hypervisor_id - id of the compute resource
template_id - id of the template
identifier - the VS identifier in the DB
hostname - the VS's host name
memory - the amount of RAM allocated to this VS
cpus - the number of CPU cores assigned to the VS
cpu_shares - the CPU priority value
created_at - the date, when the VS was created in the [YYYY][MM][DD][hh][mm][ss]Z format
updated_at - the date, when the VS was updated in the [YYYY][MM][DD][hh][mm][ss]Z format
built - true if the virtual server is built, otherwise false
locked - true if the virtual server is locked, otherwise false
booted - true if the virtual server is booted, otherwise false
xen_id - this parameter is not applicable to vCenter VS
remote_access_password - the password for remote access
local_remote_access_port - the port ID used for console access
label - label of the VS
recovery_mode - true if recovery mode is allowed, otherwise false
user_id - the ID of a new owner in OnApp
operating_system - the OS on which the virtual server is based
operating_system_distro - the distribution of the OS
allowed_swap - true, if swap is allowed; otherwise, false
template_label - label of the template
allowed_hot_migrate - true, if hot migration for the VS is allowed; otherwise, false
note - optional text, added as a note
admin_note - optional text note
suspended - true, if the VS is suspended; otherwise, false
enable_autoscale - true, if autoscale is enabled for the VS; otherwise, false
add_to_marketplace - this parameter is not applicable to vCenter VS
Initial root password encrypted - true, if root password for the VS is encrypted on the vCenter side; otherwise, false

Edge server type - this parameter is not applicable to vCenter VS

Storage server type - this parameter is not applicable to vCenter VS

Firewall notrack - true if the NOTRACK rule is set in iptables

Service password - service account password

Preferred hvs - the array of preferable compute resources based on compute zone that meet some virtual server configuration settings

Local remote access ip address - IP address used for remote access

Cpu units - the amount of CPU units per core if the CPU priority is replaced with CPU units in the user bucket

Cpu sockets - the amount of CPU sockets per core

Cores per socket - the number of CPU cores per socket

Instance package id - id of the instance package

Hot add cpu - true, if the CPU parameter can be changed without rebooting the VS; otherwise, false

Hot add memory - true, if the memory parameter can be changed without rebooting the VS; otherwise, false

Time zone - the time zone of the user

Autoscale service - this parameter is not applicable to vCenter VS

Vapp id - this parameter is not applicable to vCenter VS

Vcenter moref - moref of the virtual server on vCenter

Template version - the version of the template

Deleted at - time when the VS was deleted in the [YYYY][MM][DD][T][hh][mm][ss]Z format

Acceleration allowed - true, if acceleration is allowed for the VS; otherwise, false

Vcenter cluster id - ID of the vCenter cluster

Virsh console - true, if Virsh console is enabled for the VS, otherwise, false

Ip addresses - an array of IP addresses assigned to this virtual server

Monthly bandwidth used - VS's monthly bandwidth

Total disk size - the total disk size in GB of all disks assigned to the VS

Support incremental backups - true, if incremental backups are supported; otherwise, false

Cpu priority - it has the same value as cpu shares parameter

Built from iso - true, if the VS was built from an ISO template; otherwise, false

Built from ova - true, if the VS was built from an OVA template; otherwise, false

Acceleration - true, if acceleration is allowed for the VS; otherwise, false

Hypervisor type - the type of the compute resource (vCenter)

4.3 Auto Import Rules

If you need a quick import of multiple new VSs from vCenter to OnApp, use the auto import rules functionality. This section contains requests for management of auto import rules.
4.3.1 Get List of Auto Import Rules

To get the list of all available auto import rules, use the following request:

GET /settings/hypervisors/:hypervisor_id/auto_import_rules.xml
GET /settings/hypervisors/:hypervisor_id/auto_import_rules.json

XML Request Example

```
```

JSON Request Example

```
```

XML Output Example

```
<auto_import_rules type="array">
  <auto_import_rule>
    <id type="integer">18</id>
    <event_type>vm_created</event_type>
    <label>All DC machines</label>
    <source_type>VCenter::Datacenter</source_type>
    <source_id type="integer">452</source_id>
    <target_type>User</target_type>
    <target_id type="integer">513</target_id>
    <hypervisor_id type="integer">862</hypervisor_id>
  </auto_import_rule>
  <auto_import_rule>
    <id type="integer">20</id>
    <event_type>vm_created</event_type>
    <label>test_rule</label>
    <source_type>VCenter::ResourcePool</source_type>
    <source_id type="integer">184</source_id>
    <target_type>User</target_type>
    <target_id type="integer">1</target_id>
    <hypervisor_id type="integer">862</hypervisor_id>
  </auto_import_rule>
</auto_import_rules>
```

Where:

- **id** - the ID of an auto import rule
- **event_type** - the type of event with which this rule will be associated
- **label** - the label of auto import rule specified by the user
- **source_type** - the type of vCenter source
- **source_id** - the ID of the vCenter source
- **target_type** - the type of target user
- **target_id** - the ID of the user
- **hypervisor_id** - the ID of the compute resource

4.3.2 Add Auto Import Rule

To add an auto import rule, use the following request:
POST /settings/hypervisors/:hypervisor_id/auto_import_rules.xml
POST /settings/hypervisors/:hypervisor_id/auto_import_rules.json

XML Request Example

curl -i -X POST
http://onapp.test/settings/hypervisors/152/auto_import_rules.xml -d
' <auto_import_rule><label>Test auto import label</label><source_type>VCenter::Cluster</source_type><source_id type="integer">1</source_id><target_type>User</target_type><target_id type="integer">1</target_id></auto_import_rule>' -u user:userpass -H 'Accept: application/xml' -H 'Content-type: application/xml'

JSON Request Example

curl -i -X POST
http://onapp.test/settings/hypervisors/152/auto_import_rules.json -d
' {"label": "Test auto import label", "source_type": "VCenter::Cluster", "source_id": 1, "target_type": "User", "target_id": 1}' -u user:userpass -H 'Accept: application/json' -H 'Content-type: application/json'

Where:

* **label** - the label of auto import rule specified by the user
* **source_type** - the type of vCenter source
* **source_id** - the ID of the vCenter source
* **target_type** - the type of target user
* **target_id** - the ID of the user

4.3.3 Run Auto Import Rule

To run an auto import rule, use the following request:

POST
/settings/hypervisors/:hypervisor_id/auto_import_rules/:rule_id/run.xml

POST
/settings/hypervisors/:hypervisor_id/auto_import_rules/:rule_id/run.json

XML Request Example

curl -i -X POST

JSON Request Example
4.3.4 Edit Auto Import Rule

To edit an auto import rule, use the following request:

PUT
/settings/hypervisors/:hypervisor_id/auto_import_rules/:rule_id.xml
PUT
/settings/hypervisors/:hypervisor_id/auto_import_rules/:rule_id.json

**XML Request Example**

```bash
curl -i -X PUT
http://onapp.test/settings/hypervisors/12/auto_import_rules/3.xml
-d
'Outer XML Element for auto import rule
  <auto_import_rule>
    <label>Test auto import label EDITED</label>
    <source_type>VCenter::Cluster</source_type>
    <source_id type="integer">1</source_id>
    <target_type>User</target_type>
    <target_id type="integer">1</target_id>
  </auto_import_rule>"
-u user:userpass
-H 'Accept: application/xml'
-H 'Content-type: application/xml'
```

**JSON Request Example**

```bash
curl -i -X PUT
http://onapp.test/settings/hypervisors/12/auto_import_rules/3.json
-d
'Outer JSON Element for auto import rule
  {"label": "Test auto import label EDITED", "source_type": "VCenter::Cluster", "source_id": 1, "target_type": "User", "target_id": 1}"
-u user:userpass
-H 'Accept: application/json'
-H 'Content-type: application/json'
```

**Where:**

- **label** - the label of auto import rule specified by the user
- **source_type** - the type of vCenter source
- **source_id** - the ID of the vCenter source
- **target_type** - the type of target user
- **target_id** - the ID of the user

4.3.5 Delete Auto Import Rule

To delete an auto import rule, use the following request:

DELETE
/settings/hypervisors/:hypervisor_id/auto_import_rules/:rule_id.xml
DELETE
/settings/hypervisors/:hypervisor_id/auto_import_rules/:rule_id.json

**XML Request Example**

```bash
curl -i -X POST
-u user:userpass
-H 'Accept: application/json'
-H 'Content-type: application/json'
```
4.4 Add vCenter VS

Virtual servers running on vCenter compute resources are managed exactly the same as normal virtual servers. The only difference is the creation process.

Currently, the use of IPv6 is not supported for vCenter virtual servers.

To create a vCenter virtual server, use the following request:

POST /virtual_machines.xml
POST /virtual_machines.json

**XML Request Example**

```
curl -i -X POST -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -d
'<virtual_machine><template_id>267</template_id><infrastructure_mode>false
</infrastructure_mode><label>new_vs</label><hostname>new_hostname</hostname>
<initial_root_password>qwaszx</initial_root_password><initial_root_password_confirmation>qwaszx</initial_root_password_confirmation><hypervisor_id>29</hypervisor_id><vcenter_resource_pool_id>14</vcenter_resource_pool_id>
<datacenter_id>56</datacenter_id><memory>128</memory><cpus>1</cpus><cpu_shares>1</cpu_shares>
<data_store_group_primary_id>84</data_store_group_primary_id><primary_data_store_id>7</primary_data_store_id><primary_disk_size>256</primary_disk_size><network_group_id>2</network_group_id><network_id>7</network_id><ip_net_id>1</ip_net_id><ip_range_id>4</ip_range_id><ip_address>11.111.111.111</ip_address><rate_limit>200</rate_limit><recipe_joins_attributes type="array"><recipe_id>11</recipe_id></recipe_joins_attributes><custom_recipe_variable><enabled>true</enabled><id>62</id><name>custom_variable</name><value>custom_script</value></custom_recipe_variable><service_addon_ids type="array"><service_addon_id>273</service_addon_id></service_addon_ids><required_virtual_machine_build>true</required_virtual_machine_build><required_virtual_machine_startup>true</required_virtual_machine_startup></virtual_machine>'
```

**JSON Request Example**

```
curl -i -X POST -u user:userpass -H 'Accept: application/json' -H 'Content-type: application/json'
```

```
```

```
```
curl -i -X POST -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -d
'{"virtual_machine":{"template_id":"267","infrastructure_mode":"0","label":"new_vs","hostname":"new_hostname","initial_root_password":"qwazx","initial_root_password_confirmation":"qwazx","hypervisor_id":"29","vcenter_resource_pool_id":"14","datacenter_id":"56","memory":"128","cpus":"1","cpu_shares":1,"data_store_group_primary_id":84,"primary_data_store_id":7,"network_group_id":2,"network_id":7,"ip_net_id":3,"ip_range_id":4,"ip_address":"11.111.111.111","rate_limit":200,"required_virtual_machine_build":"1","required_virtual_machine_startup":"1","custom_recipe_variables":{"custom_recipe_variable":{"name":"varname","value":"var_value","enabled":1}}}}' --url http://onapp.test/virtual_machines.json

Where:

- **template_id** - the ID of a template from which the VS should be built
- **infrastructure_mode** - true, if Infrastructure mode should be enabled for this VS; otherwise, false
- **label** - the label of the VS

- **hostname** - set the host name for the VS
- **domain** - specify the domain for the VS. The default value is localdomain. You can edit the default value for domain in /onapp/interface/config/on_app.yml. This parameter is not applicable for Windows virtual servers.

- **initial_root_password** - the root password for a VS. Optional, if none specified, the system will provide a random password. It can consist of 6-32 characters, letters [A-Za-z], digits [0-9], dash [-] and lower dash [ _ ]. You can use both lower- and uppercase letters.

**NOTE:** It is not possible to set VS password when creating a Windows-based vCenter virtual server without running a sysprep.

- **initial_root_password_confirmation** - confirm the root password for the VS

- **hypervisor_id** - the ID of a compute resource where the VS will be built. Optional: if no compute resource ID is specified, the VS will be built on the compute resource with the least available RAM (but sufficient RAM for the VS).

- **vcenter_resource_pool_id** - ID of the vCenter Resource Pool

- **datacenter_id** - the ID of a data center for the data store. Optional: if no data center is set, the VS will be built in any available compute zone.

- **memory** - the amount of RAM assigned to the VS

- **cpus** - the number of CPU cores assigned to the VS

- **cpu_shares** - the CPU priority value

- **cpu_units** - the amount of CPU units per core if the CPU priority is replaced with CPU units in the user bucket

- **data_store_group_primary_id** - set the ID of the data store zone to which this primary disk is allocated
**primary_data_store_id*** - the ID of a primary data store for the VS primary disk

**primary_disk_size*** - set the disk space for the VS

**network_group_id** - the ID of the network zone. Optional parameter.

**network_id** - the ID of the network. Optional parameter that can be used only if it is assigned to the network zone.

💡 **ip_net_id** - the ID of the IP net from which the IP address should be assigned

💡 **ip_range_id** - the ID of the IP range from which the IP address should be assigned

💡 **ip_address** - the ID of an IP address for the VS

**rate_limit** - set the max port speed in Mbps or set 0 to get maximum port speed allowed by your bucket. If this parameter is omitted or sent without value, the default port speed will be configured for the VS. The default port speed depends on the maximum port speed set in your bucket and the Max network interface port speed parameter at Control Panel > Settings > Configuration. The system identifies which of the two values (in the bucket or in the configuration) is lower and sets it as the default port speed during VS creation.

**recipe_joins_attributes** - an array of the recipe IDs that you want to run on the virtual server provisioning

**recipe_id** - the ID of the recipe that you want to assign to the VS

**custom_recipe_variable** - the array of custom variables with the following details:

- **enabled** - true, if the variable is enabled, otherwise false
- **id** - variable ID
- **name** - variable name
- **value** - variable value script

**service_addon_ids** - the array of service add-on IDs that you want to add to VS. You can assign service add-on only if they are enabled on your license.

**service_addon_id** - the ID of the service add-on that you want to add to VS

**required_virtual_machine_build*** - set 1 to build VS automatically

**required_virtual_machine_startup** - set 1 to start up the VS automatically, otherwise, set 0 (default state is "1")

**licensing_server_id** - the ID of a template group where the KMS server details are indicated and to which the template belongs (either directly or through the child group). This parameter is for Windows virtual machines with KMS licensing type only.

**licensing_type** - the type of a license: *mak*, *kms*, or user *own* license. This parameter is required for Windows virtual machines only.

**licensing_key** - the key of a license, required if you have selected *own* licensing type, and not required for MAK and KMS licensing types. This parameter is required for Windows virtual machines only.

---

**Page History**

- **v.6.4 Edge 1**
  - added the *vcenter_resource_pool_id* parameter
  - removed the *hypervisor_group_id* and *cluster_id* parameters

- **v.6.3 Edge 2**
• added the `infrastructure_mode` parameter

v.6.0

• added the following parameters:
  o `ip_net_id`
  o `ip_range_id`
  o `ip_address`

v.5.9

• added the following parameters:
  o `datacenter_id`
  o `cluster_id`
  o `primary_data_store_id`

v.3.1

• added the following parameters:
  o `custom_variables`
  o `enabled`
  o `id`
  o `name`
  o `value`

4.5 Clone vCenter VS

To clone a virtual server, use the following request:

POST /virtual_machines/:virtual_machine_id/clone.xml

POST /virtual_machines/:virtual_machine_id/clone.json

XML Request Example

```bash
```

JSON Request Example

```bash
```

4.6 Add vCenter Compute Zone

To add a new compute zone, use the following request:
POST /settings/hypervisor_zones.xml
POST /settings/hypervisor_zones.json

**XML Request Example**

curl -i -X POST http://onapp.test/settings/hypervisor_zones.xml -d '
'<pack><label>zaza</label><server_type>virtual</server_type><location_group_id>38</location_group_id><release_resource_type>memory_guarantee</release_resource_type><max_vms_start_at_once>5</max_vms_start_at_once><recovery_type>roundrobin</recovery_type><failover_timeout>15</failover_timeout><run_sysprep>1</run_sysprep><default_gateway></default_gateway><cpu_units>1000</cpu_units></pack>' -u user:userpass -H 'Accept: application/xml' -H 'Content-type: application/xml'

**JSON Request Example**

curl -i -X POST http://onapp.test/settings/hypervisor_zones.json -d '{"pack":{"label":"zaza","server_type":"virtual","location_group_id":"38","release_resource_type":"memory_guarantee","max_vms_start_at_once":"5","recovery_type":"roundrobin","failover_timeout":"15","run_sysprep":"1","default_gateway":null,"cpu_units":"1000"}}' -u user:userpass -H 'Accept: application/json' -H 'Content-type: application/json'

Where:

* **label** - title of a new compute zone

* **server_type** - specify the type of servers that will reside within this compute zone:
  - **virtual** - choose the virtual type to create a Xen, KVM, VMware or CloudBoot zone
  - **smart** - choose the smart server type to create a smart server zone
  - **baremetal** - choose the baremetal server type to create a baremetal server zone

* **location_group** - specify the location group to which the compute zone will be assigned

* **release_resource_type** - specify the release resource type. Release resource option allows to free up compute resources by over-committing RAM, CPU and CPU shares of virtual servers that are shut down. By default, the compute zone is created with the Memory Guarantee option enabled. In this case the release resources option is not used. Then, to enable resource over-committing you should choose either the Ballooning or Only Started VS option.
  - **memory_guarantee** - the actual free compute memory is calculated. All virtual servers residing on the compute resource will be able to start.
  - **ballooning** - free compute memory is calculated with the ability to use memory over-committing. The ballooning option is only available for KVM compute resources. NOTE: Virtual server may be migrated to another compute resource if there is not enough memory for it to start up on the compute resource with the ballooning option enabled.

Do not use the ballooning option if there is at least one edge or storage server within the compute zone.
• **only_started_vms** - only the memory of running virtual servers is calculated.

**max_vms_start_at_once** - the maximum number of virtual servers that can be started simultaneously within this compute zone

**recovery_type** - specify the compute resource selection algorithm, which will be used on virtual server provisioning and recovery, per compute zone:

• **roundrobin** - set the *roundrobin* type to select the compute resource with maximum free RAM during the VS recovery

Note: this option behaves in different ways, depending on the event:

• On provisioning, the round-robin algorithm will be used on compute resource selection.

• On recovery, the compute resource with maximum free RAM will be selected.

• **fillnext** - select the fillnext type to select the compute resource with minimum required free RAM. This option allows to fill compute resource as tightly as possible before starting to use next appliance in the zone

**failover_timeout** - time period for which the iterations will run during the failover if the compute resource does not respond

**prefer_local_reads** - set 1 to minimise the network throughput dependency for read heavy workloads. When this option is enabled, reads go over the local software bridge to a local replica of the data rather than traverse a physical NIC + switch.

**run_sysprep** - set 1 to enable Windows virtual server deployment without running sysprep

**NOTE:** It is not possible to set VS password when creating a Windows-based VMware virtual server without running a sysprep.

cpu_units - set the number of cpu units for applied to each compute resource in this compute zone

**VMware parameters:**

default_gateway - external gateway IP address. All virtual servers within the compute zone will be rerouted to this gateway.

**Page History**

v. 3.3:

• added *cpu_units* parameters

v. 3.1:

• added the following parameters:
  o **server_type**
  o **release_resource_type**
  o **recovery_type**
  o **run_sysprep**
4.7 Add vCenter Compute Resources

To add a vCenter compute resource, use the following request:

POST /settings/hypervisors.xml
POST /settings/hypervisors.json

XML Request Example

curl -i -X POST http://onapp.test/settings/hypervisors.xml -d
  '<hypervisor><label>vcenter_compute_resource</label><hypervisor_type>vcenter</hypervisor_type><vcenter_server_id>1</vcenter_server_id><vcenter_cluster_id>1</vcenter_cluster_id><hypervisor_group_id>3</hypervisor_group_id></hypervisor>'
  -u user:userpass -H 'Accept:application/xml' -H 'Content-type:application/xml'

JSON Request Example

curl -i -X POST http://onapp.test/settings/hypervisors.json -d
  '{"hypervisor": {"label": "cluster_label", "hypervisor_type": "vcenter", "vcenter_server_id": 1,"vcenter_cluster_id": 1, "hypervisor_group_id": 3}}'
  -u user:userpass -H 'Accept: application/json' -H 'Content-type: application/json'

Where:

* label* - the name of the compute resource
* hypervisor_type* - specify compute resource type (vcenter)
* vcenter_server_id* - the ID of the vCenter server logical point
* vcenter_cluster_id* - the ID of the necessary vCenter cluster
* hypervisor_group_id* - the ID of the necessary compute zone

Page History

v. 6.4 Edge 1

* added the following parameters:
  - vcenter_server_id
  - vcenter_cluster_id
  - hypervisor_group_id

* removed the following parameters:
  - enabled
  - collect_stats
  - cpu_units
  - disable_failover
  - connection_options
  - login
password
api_url

v 6.0

- removed the following parameters:
  - ip_address
  - backup_ip_address
- added the api_url parameter

### 4.8 Edit vCenter Compute Resources

To edit a vCenter compute resource, use the following request:

**PATCH** /settings/hypervisors/:hypervisor_id.xml

**PATCH** /settings/hypervisors/:hypervisor_id.json

**XML Request Example**

```
curl -i -X PATCH http://onapp.test/settings/hypervisors/:hypervisor_id.xml
  -d '<hypervisor><label>vcenter_compute_resource_label</label><hypervisor_group_id>41</hypervisor_group_id></hypervisor>'
  -u user:userpass
  -H 'Accept:application/xml'
  -H 'Content-type:application/xml'
```

**JSON Request Example**

```
curl -i -X PATCH http://onapp.test/settings/hypervisors/:hypervisor_id.json
  -d '{"hypervisor": {"label": "vcenter_compute_resource_label", "hypervisor_group_id": 41}}'
  -u user:userpass
  -H 'Accept:application/json'
  -H 'Content-type:application/json'
```

Where:

- **label** - the name of the compute resource
- **compute zone** - the name of the compute zone

Please, note that an ability to edit a compute zone is available only if no virtual server is imported.

**Page History**

v. 6.4 Edge 1

- removed the following parameters:
  - enabled
  - collect_stats
  - cpu_units
  - disable_failover
170

- connection options: (login, password, api_url)

v.6.0
- removed the following parameters:
  - ip_address
  - backup_ip_address
- added the api_url parameter

4.9 vCenter Templates API

As you add a vCenter compute resource to OnApp, the vCenter templates are also imported. To finalize the import of the vCenter templates and be able to manage them, it is required to update the templates on the OnApp side. This section contains requests to view and update vCenter templates.

4.9.1 Get List of vCenter Templates

To get the list of vCenter templates in your cloud, use the following request:

GET /vcenter/templates.xml
GET /vcenter/templates.json

XML Request example

```
```

JSON Request Example

```
```

XML Output Example
<vcenter_image_templates type="array">
    <vcenter_image_template>
        <id type="integer">538</id>
        <label>win2016</label>
        <created_at type="dateTime">2019-10-18T12:39:27+03:00</created_at>
        <updated_at type="dateTime">2019-10-18T12:39:27+03:00</updated_at>
        <version>1.0</version>
        <file_name>win2016</file_name>
        <operating_system>windows</operating_system>
        <operating_system_distro>2016</operating_system_distro>
        <allowed_swap type="boolean">true</allowed_swap>
        <state>pending</state>
        <checksum nil="true"/>
        <allow_resize_without_reboot nil="true"/>
        <min_disk_size type="integer">1</min_disk_size>
        <user_id nil="true"/>
        <template_size type="integer">0</template_size>
        <allowed_hot_migrate type="boolean">false</allowed_hot_migrate>
        <operating_system_arch nil="true"/>
        <operating_system_edition nil="true"/>
        <operating_system_tail nil="true"/>
        <parent_template_id nil="true"/>
        <virtualization type="array">
            <virtualization>vcenter</virtualization>
        </virtualization>
        <min_memory_size type="integer">8192</min_memory_size>
        <disk_target_device nil="true"/>
        <cdn type="boolean">false</cdn>
        <backup_server_id nil="true"/>
        <ext4 type="boolean">false</ext4>
        <baremetal_server type="boolean">false</baremetal_server>
        <initial_password nil="true"/>
        <initial_username nil="true"/>
        <remote_id nil="true"/>
        <resize_without_reboot_policy nil="true"/>
        <application_server type="boolean">false</application_server>
        <draas type="boolean">false</draas>
        <properties>
            <nics type="integer">1</nics>
        </properties>
        <locked type="boolean">false</locked>
        <openstack_id nil="true"/>
        <datacenter_id type="integer">489</datacenter_id>
        <identifier>vm-2374</identifier>
        <type>VCenter::ImageTemplate</type>
    </vcenter_image_template>
</vcenter_image_templates>

Where:

id - the ID of the vCenter template
label - the label of the vCenter template
created_at - the date, when the VS was created in the [YYYY][MM][DD][hh][mm][ss]Z format
updated_at - the date, when the VS was updated in the [YYYY][MM][DD][hh][mm][ss]Z format
version - version of the template file
file_name - the name of the template file
operating_system - the operating system's name
operating_system_distro - the operating system's distribution

allowed_swap – true, if swap is allowed; otherwise, false

state - state of the template (active, inactive, pending)

checksum - file checksum

allow_resize_without_reboot - true if resize without reboot is allowed, otherwise false

min_disk_size - minimum disk size required to build a VS on this template (GB)

user_id - the ID of a template's user in OnApp

template_size - the size of the template

allowed_hot_migrate - true, if hot migration for the VS is allowed; otherwise, false

operating_system_arch - architecture of the operating system

operating_system_edition - edition of the OS

operating_system_tail - tail of the OS

parent_template_id - the ID of the target template group

virtualization - type of virtualization (xen, kvm or kvm_virtio) which is compatible with this template

min_memory_size - minimum memory size required to build a VS on this template (MB)

disk_target_device - the prefix indicating the method of translating the disk to a VS by compute resource

cdn - true if this template can be used for building edge servers; otherwise, false

backup_server_id - the ID of the backup server

ext4 - true if ext4 file system is supported; otherwise, false

smart_server - true if a smart server can be built from this template; otherwise, false

baremetal_server - true if a baremetal server can be built from this template; otherwise, false

initial_password - the initial password for the template on the vCenter side

initial_username - the initial username for the template on the vCenter side

remote_id - ID of the template on the vCenter side

manager_id - ID of the template on the template server

resize_without_reboot_policy - the hot resize possibility for a particular template considering its OS version and virtualization type

application_server - true if an application server can be built from this template; otherwise, false

draas - true if DRaaS is allowed; otherwise, false

properties - the attributes of template

nics - the array of parameters associated with the NICs

locked - true if the template is locked; otherwise, false

4.9.2 Update vCenter Template

To update a vCenter template's initial credentials, use the following request:

PUT /vcenter/templates/template_id.xml
PUT /vcenter/templates/template_id.json

XML Request Example
4.10 NSX Integration API

This section provides the API calls you can use to manage NSX items imported from vCenter.

4.10.1 NSX Firewalls API

Edge Firewall monitors the North-South traffic to provide perimeter security functionality including firewall, Network Address Translation (NAT), and site-to-site IPSec and SSL VPN functionality. You may set up specifications of the accepted or denied data and its paths to ensure a secure connection between the internal and external networks. This section contains the API requests you can use to manage NSX firewalls:

- Get NSX Firewall Service Details
- Edit NSX Firewall Service
- Get List of NSX Firewall Rules
- Get NSX Firewall Rule Details
- Add NSX Firewall Rule
- Edit NSX Firewall Rule
- Delete NSX Firewall Rule

4.10.1.1 Get NSX Firewall Service Details
To get an NSX firewall service details, use the following request:

GET /nsx/edges/:edge_id/firewall/service.xml
GET /nsx/edges/:edge_id/firewall/service.json

XML Request Example


JSON Request Example

Where:

- **initial_password** - the password for vCenter templates set during the template's creation
- **initial_username** - the username for vCenter templates set during the template's creation

XML Output Example

```
<nsx_firewall_service>
    <id type="integer">3</id>
    <enabled type="boolean">true</enabled>
    <edge_id type="integer">3</edge_id>
    <created_at type="dateTime">2019-11-06T10:16:49Z</created_at>
    <updated_at type="dateTime">2019-11-06T10:35:59Z</updated_at>
    <locked type="boolean">false</locked>
</nsx_firewall_service>
```

Where:

- **id** - ID of the firewall service
- **enabled** - true, if the service is enabled; otherwise, false
- **edge_id** - ID of the edge the firewall service is assigned to
- **created_at** - the date when the firewall service was created in the [YYYY][MM][DD][T][hh][mm][ss]Z format
- **updated_at** - the date when the firewall service was updated in the [YYYY][MM][DD][T][hh][mm][ss]Z format
- **locked** - true, if the firewall service is locked; otherwise, false

4.10.1.2 Edit NSX Firewall Service

To edit an NSX firewall service, use the following request:

PUT /nsx/edges/:edge_id/firewall/service.xml
PUT /nsx/edges/:edge_id/firewall/service.json

XML Request Example

```
curl -i -X PUT http://onapp.test/nsx/edges/4/firewall/service.xml -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -d '<nsx_firewall_service><enabled type="boolean">true</enabled><firewall_rules type="array"><firewall_rule><enabled type="boolean">true</enabled><label>Rule 2</label><source_excluded type="boolean">false</source_excluded><destination_excluded type="boolean">true</destination_excluded><action>deny</action><logging type="boolean">false</logging><sources type="array"><source><target_type>Nsx::Firewall::Rules::IpAddress</target_type><value>192.168.0.1</value></source><source><target_type>Nsx::NetworkInterface</target_type><value>vnic-0</value></source></sources><destinations type="array"><destination><target_type>Nsx::Firewall::Rules::IpAddress</target_type><value>192.168.1.1</value></destination></destinations><services type="array"><service><protocol>tcp</protocol><source_port>3333</source_port><destination_port>4444</destination_port></service><service><protocol>icmp</protocol></service></services></firewall_rule></firewall_rules></nsx_firewall_service>''
```
JSON Request Example

```bash
curl -i -X PUT http://onapp.test/nx/edges/4/firewall/service.json -H 'Accept: application/json' -H 'Content-type: application/json' -u user:password -d '{"nsx_firewall_service": {"enabled": true,"firewall_rules": [{"enabled": true, "label": "Rule 2", "rule_type": "user", "source_excluded": false, "destination_excluded": true, "action": "deny", "logging": false, "sources": [{"target_type": "Nsx::Firewall::Rules::IpAddress", "value": "192.168.0.1"}, {"target_type": "Nsx::NetworkInterface", "value": "vnic-0"}], "destinations": [{"target_type": "Nsx::Firewall::Rules::IpAddress", "value": "192.168.1.1"}, {"target_type": "Nsx::NetworkInterface", "value": "vnic-0"}], "services": [{"protocol": "tcp", "source_port": "3333"}, {"protocol": "icmp"}]}}}
```

Where:
- `enabled` - true, if firewall service is enabled; otherwise, false

**firewall_rules:**
- `enabled` - true, if a firewall rule is enabled; otherwise, false
- `label` - label of a firewall rule
- `rule_type` - user
- `source_excluded` - true, if toggle exclusion for this source is enabled; otherwise, false
- `destination_excluded` - true, if toggle exclusion for this destination is enabled; otherwise, false
- `action` - accept or deny
- `logging` - true, if logging for this rule is enabled; otherwise, false
- `sources`:
  - `target_type` - Nsx::Network, Nsx::VirtualMachine, Nsx::IpSet, Nsx::SecurityGroup, Nsx::Firewall::Rules::IpAddress or Nsx::NetworkInterface
  - `value` - moref of the selected target (depending on the chosen target type)
- `destinations`:
  - `target_type` - Nsx::Network, Nsx::VirtualMachine, Nsx::IpSet, Nsx::SecurityGroup, Nsx::Firewall::Rules::IpAddress or Nsx::NetworkInterface
  - `value` - moref of the selected target (depending on the chosen target type)
- `services`:
  - `protocol` - any, tcp, udp or icmp
  - `source_port` - the source port
  - `destination_port` - the destination port

4.10.1.3 Get List of NSX Firewall Rules

To get the list of firewall rules assigned to a specific edge in your cloud, use the following request:

GET /nsx/edges/:edge_id/firewall/service/rules.xml
GET /nsx/edges/:edge_id/firewall/service/rules.json

XML Request Example

JSON Request Example


XML Output Example

```xml
<nsx_firewall_rules type="array">
  <nsx_firewall_rule>
    <id type="integer">14</id>
    <identifier>131074</identifier>
    <enabled type="boolean">true</enabled>
    <label>firewall</label>
    <rule_type>internal_high</rule_type>
    <action>accept</action>
    <logging type="boolean">false</logging>
    <firewall_service_id type="integer">3</firewall_service_id>
    <created_at type="dateTime">2019-11-06T10:16:49Z</created_at>
    <updated_at type="dateTime">2019-11-06T10:16:49Z</updated_at>
    <source_excluded type="boolean">false</source_excluded>
    <destination_excluded type="boolean">false</destination_excluded>
  </nsx_firewall_rule>
  <nsx_firewall_rule>
    <id type="integer">15</id>
    <identifier>133138</identifier>
    <enabled type="boolean">true</enabled>
    <label>New Rule</label>
    <rule_type>user</rule_type>
    <action>accept</action>
    <logging type="boolean">false</logging>
    <firewall_service_id type="integer">3</firewall_service_id>
    <created_at type="dateTime">2019-11-06T10:16:49Z</created_at>
    <updated_at type="dateTime">2019-11-06T10:16:49Z</updated_at>
    <source_excluded type="boolean">false</source_excluded>
    <destination_excluded type="boolean">false</destination_excluded>
  </nsx_firewall_rule>
</nsx_firewall_rules>
```

Where:
- **id** - ID of the firewall rule
- **identifier** - identifier of the firewall rule
- **enabled** - true, if the rule is enabled; otherwise, false
- **label** - label of the firewall rule
- **rule_type** - internal_high, user or default_policy
- **action** - accept or deny
- **logging** - true, if logging for this firewall rule is enabled; otherwise, false
- **firewall_service_id** - ID of the firewall service the rule is assigned to
created_at - the date when the firewall rule was created in the [YYYY][MM][DD][hh][mm][ss]Z format
updated_at - the date when the firewall rule was updated in the [YYYY][MM][DD][hh][mm][ss]Z format
source_excluded - true, if toggle exclusion for this source is enabled; otherwise, false
destination_excluded - true, if toggle exclusion for this destination is enabled; otherwise, false

4.10.1.4 Get NSX Firewall Rule Details
To get NSX firewall rule details, use the following request:
GET /nsx/edges/:edge_id/firewall/service/rules/:rule_id.xml
GET /nsx/edges/:edge_id/firewall/service/rules/:rule_id.json

XML Request Example
```bash
```

JSON Request Example
```bash
```

XML Output Example
```xml
<nvx_firewall_rule>
  <id type="integer">15</id>
  <identifier>133138</identifier>
  <enabled type="boolean">true</enabled>
  <label>New Rule</label>
  <rule_type>user</rule_type>
  <action>accept</action>
  <logging type="boolean">false</logging>
  <firewall_service_id type="integer">3</firewall_service_id>
  <created_at type="dateTime">2019-11-06T16:49Z</created_at>
  <updated_at type="dateTime">2019-11-06T16:49Z</updated_at>
  <source_excluded type="boolean">false</source_excluded>
  <destination_excluded type="boolean">false</destination_excluded>
</nvx_firewall_rule>
```

Where:
- id - ID of the firewall rule
- identifier - identifier of the firewall rule
- enabled - true, if the rule is enabled; otherwise, false
- label - label of the firewall rule
- rule_type - internal_high, user or default_policy
- action - accept or deny
- logging - true, if logging for this firewall rule is enabled; otherwise, false
firewall_service_id - ID of the firewall service the rule is assigned to

created_at - the date when the firewall rule was created in the [YYYY][MM][DD][hh][mm][ss]Z format

updated_at - the date when the firewall rule was updated in the [YYYY][MM][DD][hh][mm][ss]Z format

source_excluded - true, if toggle exclusion for this source is enabled; otherwise, false
destination_excluded - true, if toggle exclusion for this destination is enabled; otherwise, false

4.10.1.5 Add NSX Firewall Rule
To add an NSX firewall rule, use the following request:

POST /nsx/edges/:edge_id/firewall/service/rules.xml
POST /nsx/edges/:edge_id/firewall/service/rules.json

XML Request Example

curl -i -X POST --header 'Accept: application/xml' --header 'Content-type: application/xml' -u user:userpass -d '"<nsx_firewall_rule><enabled type="boolean">true</enabled><label>Rule 2</label><source_excluded type="boolean">false</source_excluded><destination_excluded type="boolean">false</destination_excluded><action>deny</action><logging type="boolean">false</logging><sources type="array"><source><target_type>Nsx::Firewall::Rules::IpAddress</target_type><value>192.168.0.1</value></source><source><target_type>Nsx::NetworkInterface</target_type><value>vnic-0</value></source></sources><destinations type="array"><destination><target_type>Nsx::Firewall::Rules::IpAddress</target_type><value>192.168.1.1</value></destination><destination><target_type>Nsx::NetworkInterface</target_type><value>vnic-0</value></destination></destinations><services type="array"><service><protocol>tcp</protocol><source_port>3333</source_port><destination_port>4444</destination_port></service><service><protocol>icmp</protocol></service></services></nsx_firewall_rule>"'

JSON Request Example

curl -i -X POST --header 'Accept: application/json' --header 'Content-type: application/json' -u user:userpass -d '"{"nsx_firewall_rule": {"enabled": true, "label": "Rule 2", "rule_type": "user", "source_excluded": false, "destination_excluded": true, "action": "deny", "logging": false, "sources": [{"target_type": "Nsx::Firewall::Rules::IpAddress", "value": "192.168.0.1"}, {"target_type": "Nsx::NetworkInterface", "value": "vnic-0"}], "destinations": [{"target_type": "Nsx::Firewall::Rules::IpAddress", "value": "192.168.1.1"}, {"target_type": "Nsx::NetworkInterface", "value": "vnic-0"}], "services": [{"protocol": "udp", "source_port": "1111", "destination_port": "2222"}, {"protocol": "icmp"}]}}"'

Where:

enabled - true, if IPSec VPN site is enabled; otherwise, false

label - the label of the firewall rule

rule_type - user

source_excluded - true, if toggle exclusion for this source is enabled; otherwise, false
destination_excluded - true, if toggle exclusion for this destination is enabled; otherwise, false
action - accept or deny
logging - true, if logging for this rule is enabled; otherwise, false

sources:
• target_type - Nsx::Network, Nsx::VirtualMachine, Nsx::IpSet, Nsx::SecurityGroup, Nsx::Firewall::Rules::IpAddress or Nsx::NetworkInterface
• value - moref of the selected target (depending on the chosen target type)

destinations:
• target_type - Nsx::Network, Nsx::VirtualMachine, Nsx::IpSet, Nsx::SecurityGroup, Nsx::Firewall::Rules::IpAddress or Nsx::NetworkInterface
• value - moref of the selected target (depending on the chosen target type)

services:
• protocol - any, tcp, udp or icpm
• source_port - the source port
• destination_port - the destination port

4.10.1.6 Edit NSX Firewall Rule
To edit an NSX firewall rule, use the following request:

PUT /nsx/edges/:edge_id/firewall/service/rules/:rule_id.xml
PUT /nsx/edges/:edge_id/firewall/service/rules/:rule_id.json

XML Request Example

curl -i -X PUT
http://onapp.test/nsx/edges/45/firewall/service/rules/56.xml
-H 'Accept: application/xml'
-H 'Content-type: application/xml'
-u user:userpass
-d '<nsx_firewall_rule><enabled type="boolean">true</enabled><label>Rule 2</label><source_excluded type="boolean">false</source_excluded><destination_excluded type="boolean">true</destination_excluded><action>deny</action><logging type="boolean">false</logging><sources type="array"><source><target_type>Nsx::Firewall::Rules::IpAddress</target_type><value>192.168.0.1</value></source><source><target_type>Nsx::NetworkInterface</target_type><value>vnic-0</value></source></sources><destinations type="array"><destination><target_type>Nsx::Firewall::Rules::IpAddress</target_type><value>192.168.1.1</value></destination><destination><target_type>Nsx::NetworkInterface</target_type><value>vnic-0</value></destination></destinations><services type="array"><service><protocol>tcp</protocol><source_port>3333</source_port><destination_port>4444</destination_port></service><service><protocol>icmp</protocol></service></services></nsx_firewall_rule>'

JSON Request Example

curl -i -X PUT
-H 'Accept: application/json'
-H 'Content-type: application/json'
-u user:userpass
-d '{
  "nsx_firewall_rule": {
    "enabled": true,
    "label": "Rule 2",
    "source_excluded": false,
    "destination_excluded": true,
    "action": "deny",
    "logging": false,
    "sources": [
      {
        "target_type": "IpAddress",
        "value": "192.168.0.1"
      },
      {
        "target_type": "NetworkInterface",
        "value": "vnic-0"
      }
    ],
    "destinations": [
      {
        "target_type": "IpAddress",
        "value": "192.168.1.1"
      },
      {
        "target_type": "NetworkInterface",
        "value": "vnic-0"
      }
    ],
    "services": [
      {
        "protocol": "tcp",
        "source_port": 3333,
        "destination_port": 4444
      }
    ]
  }
}'
curl -i -X PUT http://onapp.test/nsx/edges/45/firewall/service/rules/56.json -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -d '{"nsx_firewall_rule": {"enabled": true, "label": "Rule 2", "rule_type": "user", "source_excluded": false, "destination_excluded": true, "action": "deny", "logging": false, "sources": [{"target_type": "Nsx::Firewall::Rules::IpAddress", "value": "192.168.0.1"}], "destinations": [{"target_type": "Nsx::Firewall::Rules::IpAddress", "value": "192.168.1.1"}, {"target_type": "Nsx::NetworkInterface", "value": "vnic-0"}], "services": [{"protocol": "tcp", "source_port": "3333", "destination_port": "4444"}, {"protocol": "icmp"}]}}'

**Where:**

- **enabled** - true, if firewall rule is enabled; otherwise, false
- **label** - the label of the firewall rule
- **rule_type** - user
- **source_excluded** - true, if toggle exclusion for this source is enabled; otherwise, false
- **destination_excluded** - true, if toggle exclusion for this destination is enabled; otherwise, false
- **action** - accept or deny
- **logging** - true, if logging for this rule is enabled; otherwise, false

**sources:**
- **target_type** - Nsx::Network, Nsx::VirtualMachine, Nsx::IpSet, Nsx::SecurityGroup, Nsx::Firewall::Rules::IpAddress or Nsx::NetworkInterface
- **value** - moref of the selected target (depending on the chosen target type)

**destinations:**
- **target_type** - Nsx::Network, Nsx::VirtualMachine, Nsx::IpSet, Nsx::SecurityGroup, Nsx::Firewall::Rules::IpAddress or Nsx::NetworkInterface
- **value** - moref of the selected target (depending on the chosen target type)

**services:**
- **protocol** - any, tcp, udp, icmp
- **source_port** - the source port
- **destination_port** - the destination port

4.10.1.7 Delete NSX Firewall Rule

To delete an NSX firewall rule, use the following request:

```
DELETE /nsx/edges/:edge_id/firewall/service/rules/:rule_id.xml
DELETE /nsx/edges/:edge_id/firewall/service/rules/:rule_id.json
```

**XML Request example**

```
```

**JSON Request Example**
Returns HTTP 204 response on successful deletion, or HTTP 404 when a firewall with the ID specified is not found.

4.10.2 NSX NAT API

NAT (Network Address Translation) service translates source or destination IP addresses and port numbers. Below you can find the list of operations applicable for NSX NAT services and rules:

- Get NAT Service Details
- Edit NAT Service
- Get List of NAT Rules
- Get NAT Rule Details
- Add NAT Rule
- Edit NAT Rule
- Delete NAT Rule

4.10.2.1 Get NAT Service Details

To view the details of a particular NAT service, use the following request:

GET /nsx/edges/:edge_id/nat/service.xml
GET /nsx/edges/:edge_id/nat/service.json

**XML Request Example**

```bash
curl -i -X GET -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass --url
http://onapp.test/nsx/edges/3/nat/service.xml
```

**JSON Request Example**

```bash
curl -i -X GET -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass --url
http://onapp.test/nsx/edges/3/nat/service.json
```

**XML Output Example**

```xml
<nsx_nat_service>
  <id type="integer">3</id>
  <enabled type="boolean">true</enabled>
  <edge_id type="integer">3</edge_id>
  <created_at type="dateTime">2019-11-06T10:16:49Z</created_at>
  <updated_at type="dateTime">2019-11-06T10:16:49Z</updated_at>
  <locked type="boolean">false</locked>
</nsx_nat_service>
```

Where:
id - ID of the NAT service

enabled - true if the NAT service is enabled; otherwise, false

edge_id - the ID of the edge

created_at - the date when the NAT service was created in the [YYYY][MM][DD][T][hh][mm][ss]Z format

updated_at - the date when the NAT service was updated in the [YYYY][MM][DD][T][hh][mm][ss]Z format

locked - true, if NAT service is locked; otherwise, false

4.10.2.2 Edit NAT Service

To edit NAT service, use the following request:

PUT /nsx/edges/:edge_id/nat/service.xml

PUT /nsx/edges/:edge_id/nat/service.json

XML Request Example

curl -i -X PUT -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -d '<nsx_nat_service><enabled type="boolean">true</enabled><nat_rules type="array"><nat_rule><original_port>1</original_port><translated_port>2</translated_port><protocol>tcp</protocol><enabled type="boolean">true</enabled><logging type="boolean">true</logging><type>rule</type><rule_type>user</rule_type><interface type="integer">2</interface><action>dnat</action><original_ip>1.1.1.1</original_ip><translated_ip>2.2.2.2</translated_ip><description>desc</description></nat_rule></nat_rules></nsx_nat_service>'

JSON Request Example

curl -i -X PUT -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -d '{"nsx_nat_service": {"enabled": true,"nat_rules": [{"original_port": "1","translated_port": "2","protocol": "tcp","enabled": true,"logging": true,"type": "rule","rule_type": "user","interface": 2,"action": "dnat","original_ip": "1.1.1.1","translated_ip": "2.2.2.2","description": "desc"}]}}'}

Where:

enabled - true if the NAT service is enabled; otherwise, false

nat_rules - an array of the NSX NAT rules with the following details:

- original_port - the port of original IP address
- translated_port - the port of translated IP address
- protocol - any, tcp, udp or icpm
- enabled - true if the rule is enabled; otherwise, false
- logging - true if logging is enabled; otherwise, false
- type - user
- rule_type - user
- interface - vnic's or sub-interface's index
• action - DNAT or SNAT
• original_ip - the original IP address to apply this rule on
• translated_ip - the IP address to translate the addresses of outgoing packets to
• description - description of a rule

4.10.2.3 Get List of NAT Rules
To get list of NAT rules, use the following request:

GET /nsx/edges/:edge_id/nat/service/rules.xml
GET /nsx/edges/:edge_id/nat/service/rules.json

XML Request Example

```
```

JSON Request Example

```
```

XML Output Example

```
<nsx_nat_rules type="array">
  <nsx_nat_rule>
    <id type="integer">23</id>
    <action>dnat</action>
    <enabled type="boolean">true</enabled>
    <interface_id type="integer">9</interface_id>
    <identifier>200723</identifier>
    <logging type="boolean">false</logging>
    <nat_service_id type="integer">3</nat_service_id>
    <original_ip>1.1.1.1</original_ip>
    <rule_type>user</rule_type>
    <translated_ip>1.1.1.1</translated_ip>
    <original_port>any</original_port>
    <protocol>any</protocol>
    <translated_port>any</translated_port>
    <icmp_type nil="true"/>
    <description nil="true"/>
    <created_at type="dateTime">2019-11-06T12:45:29Z</created_at>
    <updated_at type="dateTime">2019-11-06T12:45:29Z</updated_at>
    <interface_type>Nsx::NetworkInterface</interface_type>
  </nsx_nat_rule>
<nsx_nat_rule>...</nsx_nat_rule>
</nsx_nat_rules>
```

Where:

action - DNAT or SNAT
created_at - the date when the NAT rule was created in the [YYYY][MM][DD][hh][mm][ss]Z format
description - description of a rule
enabled - true if the rule is enabled; otherwise, false
icmp_type - any, address-mask-request, address-mask-reply, destination-unreachable, echo-request, echo-reply, parameter-problem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-request and timestamp-reply
id - the ID of the edge
identifier - the identifier of the rule
logging - true if logging is enabled, otherwise, false
nat_service_id - the ID of a NAT service
interface_id - the ID of the network interface
original_ip - the original IP address to apply this rule on
original_port - the port of original IP address
protocol - any, tcp, udp or icpm
rule_type - user or internal_high
translated_ip - the IP address to translate the addresses of outgoing packets to
translated_port - the port of translated IP address
updated_at - the date when the NAT rule was updated in the [YYYY][MM][DD][hh][mm][ss]Z format
interface_type - Nx::NetworkInterface or Nx::SubInterface

4.10.2.4 Get NAT Rule Details
To get details of a particular NAT rule, use the following request:
GET /nsx/edges/edge_id/nat/service/rules/:rule_id.xml
GET /nsx/edges/edge_id/nat/service/rules/:rule_id.json

XML Request Example
```
```

JSON Request Example
```
```

XML Output Example
Where:

- **id** - the ID of the rule
- **action** - DNAT or SNAT
- **enabled** - true if the rule is enabled; otherwise, false
- **interface_id** - the ID of the network interface
- **identifier** - the identifier of the rule
- **logging** - true if logging is enabled; otherwise, false
- **nat_service_id** - the ID of the NAT service
- **original_ip** - the original IP address to apply this rule on
- **rule_type** - user or internal_high
- **translated_ip** - the IP address to translate the addresses of outgoing packets to
- **original_port** - the port of original IP address
- **protocol** - any, tcp, udp or icpm
- **translated_port** - the port of translated IP address
- **icmp_type** - any, address-mask-request, address-mask-reply, destination-unreachable, echo-request, echo-reply, parameter-problem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-request and timestamp-reply
- **description** - description of the rule
- **created_at** - the date when the NAT rule was created in the [YYYY][MM][DD][hh][mm][ss][Z] format
- **updated_at** - the date when the NAT rule was updated in the [YYYY][MM][DD][hh][mm][ss][Z] format
- **interface_type** - Nsx::NetworkInterface or Nsx::SubInterface

4.10.2.5 Add NAT Rule

To create a new NAT rule, use the following request:

POST /nsx/edges/:edge_id/nat/service/rules.xml
POST /nsx/edges/:edge_id/nat/service/rules.json
XML Request Example

```bash
curl -i -X POST -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass --url http://onapp.test/nsx/edges/3/nat/service/rules.xml -d '<nsx_nat_rule><original_port>1</original_port><translated_port>2</translated_port><protocol>tcp</protocol><enabled type="boolean">true</enabled><logging type="boolean">true</logging><rule_type>user</rule_type><interface type="integer">2</interface><action>dnat</action><original_ip>1.1.1.1</original_ip><translated_ip>2.2.2.2</translated_ip><description>desc</description></nsx_nat_rule>"
```

JSON Request Example

```bash
curl -i -X POST -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass --url http://onapp.test/nsx/edges/3/nat/service/rules.json -d '{"nsx_nat_rule": {"original_port": "1","translated_port": "2","protocol": "tcp","enabled": "true","logging": true,"rule_type": "user","interface": 2,"action": "dnat","original_ip": "1.1.1.1","translated_ip": "2.2.2.2","description": "desc"}}'
```

Where:

- **original_port** - the port of original IP address
- **translated_port** - the port of translated IP address
- **protocol** - any, tcp, udp or icpm
- **enabled** - true if the rule is enabled; otherwise, false
- **logging** - true if logging is enabled, otherwise, false
- **rule_type** - user
- **interface** - vnic's or sub-interface's index
- **action** - DNAT or SNAT
- **original_ip** - the original IP address to apply this rule on
- **translated_ip** - the IP address to translate the addresses of outgoing packets to
- **description** - the description of a NAT rule

4.10.2.6 Edit NAT Rule

To edit a NAT rule, use the following request:

```bash
PUT /nsx/edges/:edge_id/nat/service/rules/:rule_id.xml
PUT /nsx/edges/:edge_id/nat/service/rules/:rule_id.json
```

XML Request Example
JSON Request Example

```bash
curl -i -X PUT -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -d
'http://onapp.test/nsx/edges/3/nat/service/rules/11.xml' -d
'\t<nsx_nat_rule><original_port>any</original_port><translated_port>any</translated_port><protocol>any</protocol><enabled
type="boolean">true</enabled><logging
type="boolean">true</logging><rule_type>user</rule_type><interface
type="integer">2</interface><action>snat</action><description>
desc</description></nsx_nat_rule>'
```

Where:
- `original_port` - the port of original IP address
- `translated_port` - the port of translated IP address
- `protocol` - any, tcp, udp or icmp
- `enabled` - true if the rule is enabled; otherwise, false
- `logging` - true if logging is enabled, otherwise, false
- `rule_type` - user
- `interface` - the ID of the network interface
- `action` - DNAT or SNAT
- `description` - the description of the NAT rule

4.10.2.7 Delete NAT Rule
To delete a NAT rule, use the following request:

DELETE /nsx/edges/:edge_id/nat/service/rules/:rule_id.xml
DELETE /nsx/edges/:edge_id/nat/service/rules/:rule_id.json

XML Request Example

```bash
curl -i -X DELETE -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -d
'url http://onapp.test/nsx/edges/3/nat/service/rules/11.xml'
```

JSON Request Example

```bash
curl -i -X DELETE -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -d
```
Returns HTTP 204 response on successful deletion, or HTTP 404 when a NAT rule with the ID specified is not found.

4.10.3 NSX Load Balancers API

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. This section contains the following API requests you can use to manage NSX load balancers:

- Get NSX Load Balancer Service Details
- Edit NSX Load Balancer Service
- Application Profiles
- Pools
- Virtual Servers
- Service Monitors
- Application Rules

4.10.3.1 Get NSX Load Balancer Service Details

To get the details of load balancer service, use the following request:

GET /nsx/edges/:edge_id/load_balancer/service.xml
GET /nsx/edges/:edge_id/load_balancer/service.json

XML Request Example

curl -i -X GET -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass --url
http://onapp.test/nsx/edges/3/load_balancer/service.xml

XML Output Example

```xml
<nsx_load_balancer_service>
  <id type="integer">3</id>
  <enabled type="boolean">false</enabled>
  <acceleration type="boolean">true</acceleration>
  <logging type="boolean">true</logging>
  <log_level>info</log_level>
  <edge_id type="integer">3</edge_id>
  <created_at type="dateTime">2019-11-06T10:16:50Z</created_at>
  <updated_at type="dateTime">2019-11-06T10:16:50Z</updated_at>
  <locked type="boolean">false</locked>
</nsx_load_balancer_service>
```

Where:

- id - the ID of the NSX load balancer service
- enabled - true if NSX load balancer service is enabled, otherwise, false
acceleration - true if acceleration is enabled; otherwise, false

logging - true if logging is enabled; otherwise, false

log_level - emergency, alert, critical, error, warning, notice, info or debug

data

edge_id - the ID of the edge

created_at - the date when the load balancer service was created in the [YYYY][MM][DD][hh][mm][ss]Z format

updated_at - the date when the load balancer service was updated in the [YYYY][MM][DD][hh][mm][ss]Z format

locked - true, if load balancer service is locked; otherwise, false

4.10.3.2 Edit NSX Load Balancer Service

To edit NSX load balancer service, use the following request:

PUT /nsx/edges/:edge_id/load_balancer/service.xml

PUT /nsx/edges/:edge_id/load_balancer/service.json

XML Request Example

curl -i -X PUT -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -d '...

<nsx_load_balancer_service><enabled type="boolean">true</enabled><acceleration type="boolean">false</acceleration><logging type="boolean">false</logging><log_level>info</log_level><application_profiles type="array"><application_profile><identifier>applicationProfile-5</identifier><cookie_name>qwe</cookie_name><cipher>qwe</cipher><client_auth>required</client_auth><mode>insert</mode><persistence>sourceIp</persistence><type>HTTPS</type><expires>123</expires><insert_x_forwarded type="boolean">true</insert_x_forwarded><ssl_passthrough type="boolean">true</ssl_passthrough><server_ssl type="boolean">false</server_ssl><service_certificate>certificate-52</service_certificate><ca_certificates type="array"><ca_certificate>certificate-54</ca_certificate></ca_certificates><crl_certificates type="array"><crl_certificate>crl-4</crl_certificate></crl_certificates></application_profile></application_profiles><monitors type="array"><monitor><identifier>monitor-2</identifier><url>a ds</url><expected>ads</expected><send_data>ads</send_data><receive_data>ads</receive_data><extension>ads</extension><type>GET</type><method_data>GET</method_data><interval>1</interval><timeout>2</timeout><max_retries>3</max_retries></monitor></monitors><pools type="array"><pool><identifier>pool-4</identifier><description>ads</description><algorithm>ip-hash</algorithm><transparent>1</transparent><monitor>monitor-2</monitor><members type="array"><member><identifier>member-2</identifier><ip_address>192.168.0.1</ip_address><monitor_port>1111</monitor_port><port>2222</port><enabled type="boolean">true</enabled><weight>1</weight><max_conn>3</max_conn><min_conn>4</min_conn></member></members></pool></pools><application_rules type="array"><application_rule><identifier>applicationRule-6</identifier><script>asfd</script></application_rule></application_rules><virtual_servers type="array"><virtual_server><identifier>virtualServer-1</identifier><description>ads</description><ip_address>192.168.0.1</ip_address><port>1111</port><protocol>http</protocol><connection_limit>1234</connection_limit><connection_rate_limit>1234</connection_rate_limit><enabled type="boolean">true</enabled><acceleration type="boolean">true</acceleration></virtual_server></virtual_servers>
JSON Request Example


Where:

- **enabled** - true, if this load balancer service is enabled; otherwise, false
- **acceleration** - true, if acceleration is enabled; otherwise, false
- **logging** - true, if logging for load balancer service is enabled; otherwise, false
- **log_level** - emergency, alert, critical, error, warning, notice, info or debug

**application_profiles**:

- **identifier** - identifier of the application profile
- **label** - label of the application profile
- **http_redirect_url** - HTTP redirect URL
- **cookie_name** - Cookie's label
- **cipher** - a cipher algorithm
- **client_auth** - required or ignored
- **mode** - insert, prefix or app
• **persistence** - sourceip, msrdp, cookie or ssl_sessionid
• **type** - the type of traffic (TCP, HTTP, HTTPS or UDP)
• **expires** - the persistence expiration time in seconds. The default value is 60 seconds.
• **insert_x_forwarded** - true or false
• **ssl_passthrough** - true if SSL passthrough is enabled; otherwise, false
• **server_ssl** - true if poolside SSL is enabled; otherwise, false
• **service_certificate** - service certificate’s identifier
• **ca_certificates** - CA certificates’ identifiers
• **crl_certificates** - CRL certificates’ identifiers

monitors:
• **identifier** - identifier of the monitor
• **label** - label of the monitor
• **url** - the URL to GET or POST
• **expected** - the string that the monitor expects to match in the status line of HTTP response in the Expected section
• **send_data** - the string sent to the back-end server after a connection is established
• **receive_data** - the string to be matched
• **extension** - advanced monitor parameters as key=value pairs
• **type** - http, https, tcp, icmp or udp
• **method_data** - GET, OPTIONS or POST
• **interval** - the interval in seconds in which a server is to be tested
• **timeout** - the maximum time in seconds within which a response from the server must be received
• **max_retries** - the number of times the server is tested before it is declared DOWN

pools:
• **identifier** - identifier of the pool
• **label** - label of the pool
• **description** - description of the pool
• **algorithm** - round-robin, ip-hash, leastconn, uri, httpheader or url
• **transparent** - true if client IP addresses are visible to the back-end servers; otherwise, false
• **monitor** - the ID of the existing default or custom monitor
• **members** - an array of the server members with the following details:
  o **label** - the name of the server member
  o **ip_address** - the IP address of the server member
  o **monitor_port** - the monitor port where the member is to receive health monitor pings
  o **port** - the port where the member is to receive traffic
  o **enabled** - true if this member is enabled; otherwise, false
  o **weight** - the proportion of traffic this member can handle
**max_conn** - the maximum number of concurrent connections that the member can handle. If the incoming requests go higher than the maximum, they are queued and wait for a connection to be released.

**min_conn** - the minimum number of concurrent connections that a member must always accept

**application_rules:**
- *identifier* - identifier of the application rule
- *label* - label of the application rule
- *script* - application rule's script

**virtual_servers:**
- *identifier* - identifier of the virtual server
- *label* - label of the VS
- *description* - description of the VS
- *ip_address* - IP address of the VS
- *port* - the port number that the load balancer listens on
- *protocol* - *http*, *https*, *tcp* or *udp*
- *connection_limit* - the maximum concurrent connections that the virtual server can process
- *connection_rate_limit* - the maximum incoming new connection requests per second section
- *enabled* - *true* if this virtual server is available for use; otherwise, *false*
- *acceleration* - *true* if acceleration is enabled for this VS; otherwise, *false*
- *application_profile* - the label of the application profile associated with this VS
- *default_pool* - identifier of the default pool
- *application_rules* - an array of application rules' identifiers

### 4.10.3.3 Application Profiles

You create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. This section contains the following API requests:

- **Get List of Application Profiles**
- **Get Application Profile Details**
- **Add Application Profile**
- **Edit Application Profile**
- **Delete Application Profile**

#### 4.10.3.3.1 Get List of Application Profiles

To get a list of application profiles, use the following request:

GET `/nsx/edges/:edge_id/load_balancer/service/application_profiles.xml`

GET `/nsx/edges/:edge_id/load_balancer/service/application_profiles.json`

**XML Request Example**
JSON Request Example

```bash
```

XML Output Example

```xml
<nsx_load_balancer_application_profiles type="array">
  <nsx_load_balancer_application_profile>
    <cipher null="true" />
    <client_auth null="true" />
    <cookie_name null="true" />
    <created_at>2019-10-03T10:31:00.000Z</created_at>
    <expires>123</expires>
    <http_redirect_url null="true" />
    <id>4</id>
    <identifier>applicationProfile-3</identifier>
    <insert_x_forwarded>false</insert_x_forwarded>
    <label>1</label>
    <load_balancer_service_id>9</load_balancer_service_id>
    <mode null="true" />
    <persistence>sourceip</persistence>
    <server_ssl>false</server_ssl>
    <ssl_passthrough>false</ssl_passthrough>
    <type>TCP</type>
    <updated_at>2019-10-03T10:31:00.000Z</updated_at>
  </nsx_load_balancer_application_profile>
...
</nsx_load_balancer_application_profiles>
```

Where:

cipher - DEFAULT, ECDEHE-RSA-AES128-GCM-SHA256, ECDEHE-RSA-AES256-GCM-SHA384, ECDEHE-RSA-AES256-SHA, ECDHE-ECDSA-AES256-SHA, ECDHE-ECDSA-AES256-SHA, ECDH-RSA-AES256-SHA AES256-SHA AES128-SHA, or DES-CBC3-SHA

client_auth - ignored or required

cookie_name - the Cookie's identifier

created_at - the date in the [YYYY][MM][DD][T][hh][mm][ss]Z format

expires - the persistence expiration time in seconds. The default value is 60 seconds.

http_redirect_url - the HTTP redirect URL

id - the ID of the application profile

identifier - the identifier of an application profile

insert_x_forwarded - true or false

label - the label of the application profile

load_balancer_service_id - the ID of the load balancer service

193
mode - insert, prefix or app

persistence - sourceip, msrdp, cookie or ssl_sessionid

server_ssl - true if poolside SSL is enabled; otherwise, false

ssl_passthrough - true if SSL passthrough is enabled; otherwise, false

type - the type of traffic (TCP, HTTP, HTTPS or UDP)

updated_at - the date when the application profile was updated in the [YYYY][MM][DD][hh][mm][ss]Z format

4.10.3.2 Get Application Profile Details

To get details of a particular application profile, use the following request:

GET /nsx/edges/:edge_id/load_balancer/service/application_profiles/:application_profile_id.xml

GET /nsx/edges/:edge_id/load_balancer/service/application_profiles/:application_profile_id.json

XML Request Example


JSON Request Example


XML Output Example

<nsx_load_balancer_application_profile>
  <cipher>DEFAULT</cipher>
  <client_auth>required</client_auth>
  <cookie_name null="true" />
  <created_at>2019-10-04T08:17:34.000Z</created_at>
  <http_redirect_url null="true" />
  <id>4</id>
  <identifier>applicationProfile-3</identifier>
  <insert_x_forwarded>true</insert_x_forwarded>
  <label>1111</label>
  <load_balancer_service_id>9</load_balancer_service_id>
  <mode null="true" />
  <persistence>sourceip</persistence>
  <server_ssl>true</server_ssl>
  <ssl_passthrough>false</ssl_passthrough>
  <type>HTTPS</type>
  <updated_at>2019-10-04T08:17:34.000Z</updated_at>
</nsx_load_balancer_application_profile>

Where:
cipher - DEFAULT, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, ECDHE-ECDSA-AES256-SHA, ECDH-ECDSA-AES256-SHA, ECDH-RSA-AES256-SHA, AES256-SHA AES128-SHA, or DES-CBC3-SHA

client_auth - whether client authentication is required or ignored

cookie_name - true for the Cookie persistence type; otherwise, false

created_at - the date when the application profile was created in the [YYYY][MM][DD][hh][mm][ss]Z format

expires - the persistence expiration time in seconds. The default value is 60 seconds.

http_redirect_url - true for HTTP or HTTPs type of traffic; false for TCP or UDP

id - the ID of an application profile

identifier - the identifier of an application profile

insert_x_forwarded - true or false

label - the label of a load balancer

load_balancer_service_id - the ID of the load balancer service

mode - true for Cookie persistence type; otherwise, false

persistence - the persistence type (sourceip, cookie or none)

server_ssl - true if poolside SSL is enabled; otherwise, false

ssl_passthrough - true if SSL passthrough is enabled; otherwise, false

type - the type of traffic (TCP, HTTP, HTTPS or UDP)

updated_at - the date when the application profile was updated in the [YYYY][MM][DD][hh][mm][ss]Z format

4.10.3.3 Add Application Profile

To create an application profile, use the following request:

POST /nsx/edges/:edge_id/load_balancer/service/application_profiles.xml

POST /nsx/edges/:edge_id/load_balancer/service/application_profiles.json

XML Request Example


'<nsx_application_profile><label>new</label><cipher>DEFAULT</cipher><client_auth>required</client_auth><persistence>sourceip</persistence><type>HTTP</type><expires type="integer">123</expires><insert_x_forwarded type="boolean">true</insert_x_forwarded><ssl_passthrough type="boolean">false</ssl_passthrough><server_ssl type="boolean">true</server_ssl><ca_certificates type="array"><ca_certificate>certificate-52</ca_certificate></ca_certificates><crl_certificates type="array"><crl_certificate>crl-4</crl_certificate><crl_certificate>crl-6</crl_certificate></crl_certificates><service_certificate>certificate-54</service_certificate></nsx_application_profile>"

Where:

- **label** - the label of an application profile
- **cipher** - DEFAULT, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, ECDHE-ECDSA-AES128-SHA, ECDHE-ECDSA-AES256-SHA, ECDH-ECDSA-AES256-SHA, AES256-SHA AES128-SHA, or DES-CBC3-SHA
- **client_auth** - select whether to ignore or accept client authentication (ignore or required)
- **persistence** - the persistence type (sourceip, cookie or none)
- **type** - the type of traffic (TCP, HTTP, HTTPS or UDP)
- **expires** - the persistence expiration time in seconds. The default value is 60 seconds.
- **insert_x_forwarded** - true or false
- **ssl_passthrough** - true if SSL passthrough is enabled; otherwise, false
- **server_ssl** - true if poolside SSL is enabled; otherwise, false
- **ca_certificates** - CA certificates' identifiers
- **crl_certificates** - CRL certificates' identifiers
- **service_certificate** - server certificates to authenticate the load balancer from the server side

4.10.3.3.4 Edit Application Profile

To edit a particular application profile, use the following request:

```
PUT /nsx/edges/:edge_id/load_balancer/service/application_profiles/:application_profile_id.xml
```

```
PUT /nsx/edges/:edge_id/load_balancer/service/application_profiles/:application_profile_id.json
```

**XML Request Example**

```bash
curl -i -X PUT -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass --url http://onapp.test/nsx/edges/9/load_balancer/service/application_profiles/4.xml -d '<nsx_application_profile><label>new</label><cipher>DEFAULT</cipher><client_auth>required</client_auth><persistence>sourceip</persistence><type>HTTP</type><expires type="integer">123</expires><insert_x_forwarded type="boolean">true</insert_x_forwarded><ssl_passthrough type="boolean">false</ssl_passthrough><server_ssl type="boolean">true</server_ssl><ca_certificates type="array">><ca_certificate>certificate-52</ca_certificate></ca_certificates><crl_certificates type="array">><crl_certificate>crl-4</crl_certificate></crl_certificates><service_certificate>certificate-54</service_certificate></nsx_application_profile>'
```
JSON Request Example

```bash
```

Where:

**label** - label of the application profile

**cipher** - DEFAULT, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, ECDHE-ECDSA-AES256-SHA, ECDH-ECDSA-AES256-SHA, ECDH-RSA-AES256-SHA, AES256-SHA AES128-SHA, or DES-CBC3-SHA

**client_auth** - select whether to ignore or accept client authentication (ignore or required)

**persistence** - the persistence type (sourceip, cookie or none)

**type** - the type of traffic (TCP, HTTP, HTTPS or UDP)

**expires** - the persistence expiration time in seconds. The default value is 60 seconds.

**insert_x_forwarded** - true or false

**ssl_passthrough** - true if SSL passthrough is enabled; otherwise, false

**server_ssl** - true if poolside SSL is enabled; otherwise, false

**ca_certificates** - CA certificates' identifiers

**crl_certificates** - CRL certificates' identifiers

**service_certificate** - server certificate's identifier to authenticate the load balancer from the server side

4.10.3.3.5 Delete Application Profile

To delete an application profile, use the following request:

DELETE /nsx/edges/:edge_id/load_balancer/service/application_profiles/:service_application_id.xml

DELETE /nsx/edges/:edge_id/load_balancer/service/application_profiles/:service_application_id.json

XML Request Example

```bash
```

JSON Request Example
Returns HTTP 204 response on successful deletion, or HTTP 404 when an application profile with the ID specified is not found.

4.10.3.4 Service Monitors
A service monitor defines health check parameters for the load balancer. After you create a service monitor and associate it with a server pool, you can update the existing service monitor or delete it to save system resources. Below you can find the list of operations applicable for NSX service monitors:

- Get List of Service Monitors
- Get Service Monitor Details
- Add Service Monitor
- Edit Service Monitor
- Delete Service Monitor

4.10.3.4.1 Get List of Service Monitors
To get the list of service monitors, use the following request:
GET /nsx/edges/:edge_id/load_balancer/service/monitors.xml
GET /nsx/edges/:edge_id/load_balancer/service/monitors.json

XML Request Example


JSON Request Example


XML Output Example
<nsx_load_balancer_monitors type="array">
  <nsx_load_balancer_monitor>
    <id type="integer">2</id>
    <identifier>monitor-1</identifier>
    <label>default_tcp_monitor</label>
    <url nil="true"/>
    <expected nil="true"/>
    <send_data nil="true"/>
    <receive_data nil="true"/>
    <type>tcp</type>
    <method_data nil="true"/>
    <interval type="integer">5</interval>
    <timeout type="integer">15</timeout>
    <max_retries type="integer">3</max_retries>
    <load_balancer_service_id type="integer">3</load_balancer_service_id>
    <created_at type="dateTime">2019-11-06T10:16:50Z</created_at>
    <updated_at type="dateTime">2019-11-06T10:16:50Z</updated_at>
  </nsx_load_balancer_monitor>
  <nsx_load_balancer_monitor>
    <id type="integer">9</id>
    <identifier>monitor-5</identifier>
    <label>m1</label>
    <url>/</url>
    <expected nil="true"/>
    <send_data>qwe</send_data>
    <receive_data>qwe</receive_data>
    <extension nil="true"/>
    <type>http</type>
    <method_data>GET</method_data>
    <interval type="integer">0</interval>
    <timeout type="integer">0</timeout>
    <max_retries type="integer">0</max_retries>
    <load_balancer_service_id type="integer">3</load_balancer_service_id>
    <created_at type="dateTime">2019-11-06T10:16:50Z</created_at>
    <updated_at type="dateTime">2019-11-06T10:16:50Z</updated_at>
  </nsx_load_balancer_monitor>
</nsx_load_balancer_monitors>

Where:

id - ID of the service monitor
identifier - identifier of the service monitor
label - label of the service monitor
url - the URL to GET or POST
expected - the string that the monitor expects to match in the status line of HTTP response in the Expected section
send_data - the string sent to the back-end server after a connection is established
receive_data - the string to be matched
extension - advanced monitor parameters as key=value pairs
type - http, https, tcp, icmp or udp
method_data - GET, OPTIONS or POST
interval - the interval in seconds in which a server is to be tested
timeout - the maximum time in seconds within which a response from the server must be received
**max_retries** - the number of times the server is tested before it is declared DOWN

**load_balancer_service_id** - ID of the load balancer service

**created_at** - the date when the service monitor was created in the [YYYY][MM][DD][hh][mm][ss]Z format

**updated_at** - the date when the service monitor was updated in the [YYYY][MM][DD][hh][mm][ss]Z format

### 4.10.3.4.2 Get Service Monitor Details

To get a service monitor details, use the following request:

GET /nsx/edges/:edge_id/load_balancer/service/monitors/:monitor_id.xml
GET /nsx/edges/:edge_id/load_balancer/service/monitors/:monitor_id.json

**XML Request Example**

```bash
```

**JSON Request Example**

```bash
```

**XML Output Example**

```xml
<nsx_load_balancer_monitor>
  <id type="integer">9</id>
  <identifier>monitor-5</identifier>
  <label>m1</label>
  <url></url>
  <expected nil="true"/>
  <send_data>qwe</send_data>
  <receive_data>qwe</receive_data>
  <extension nil="true"/>
  <type>http</type>
  <method_data>GET</method_data>
  <interval type="integer">0</interval>
  <timeout type="integer">0</timeout>
  <max_retries type="integer">0</max_retries>
  <load_balancer_service_id type="integer">3</load_balancer_service_id>
  <created_at type="dateTime">2019-11-06T16:50Z</created_at>
  <updated_at type="dateTime">2019-11-06T16:50Z</updated_at>
</nsx_load_balancer_monitor>
```

**Where:**

- **id** - ID of the service monitor
- **identifier** - identifier of the service monitor
- **label** - label of the service monitor
- **url** - the URL to GET or POST
**expected** - the string that the monitor expects to match in the status line of HTTP response in the Expected section

**send_data** - the string sent to the back-end server after a connection is established

**receive_data** - the string to be matched

**extension** - advanced monitor parameters as key=value pairs

**type** - http, https, tcp, icmp or udp

**method_data** - GET, OPTIONS or POST

**interval** - the interval in seconds in which a server is to be tested

**timeout** - the maximum time in seconds within which a response from the server must be received

**max_retries** - the number of times the server is tested before it is declared DOWN

**load_balancer_service_id** - ID of the load balancer service

**created_at** - the date when the service monitor was created in the [YYYY][MM][DD][T][hh][mm][ss]Z format

**updated_at** - the date when the service monitor was updated in the [YYYY][MM][DD][T][hh][mm][ss]Z format

### 4.10.3.4.3 Add Service Monitor

To add a service monitor, use the following request:

**POST** /nsx/edges/:edge_id/load_balancer/service/monitors.xml

**POST** /nsx/edges/:edge_id/load_balancer/service/monitors.json

**XML Request Example**

```
```

**JSON Request Example**

```
```

**Where:**

**label** - label of the service monitor

**interval** - the interval in seconds in which a server is to be tested

**timeout** - the maximum time in seconds within which a response from the server must be received

**max_retries** - the number of times the server is tested before it is declared DOWN
type - http, https, tcp, icmp or udp

method_data - GET, OPTIONS or POST

url - the URL to GET or POST

expected - the string that the monitor expects to match in the status line of HTTP response in the Expected section

send_data - the string sent to the back-end server after a connection is established

receive_data - the string to be matched

extension - advanced monitor parameters as key=value pairs

4.10.3.4 Edit Service Monitor

To edit a service monitor, use the following request:

PUT /nsx/edges/:edge_id/load_balancer/service/monitors/:monitor_id.xml

PUT /nsx/edges/:edge_id/load_balancer/service/monitors/:monitor_id.json

XML Request Example

```
curl -i -X PUT
http://onapp.test/edges/45/load_balancer/service/monitors/56.xml
-H 'Accept: application/xml' -H 'Content-type: application/xml' -u
user:userpass -d '<nsx_monitor><label>TEST</label><interval
type="integer">5</interval><timeout
type="integer">15</timeout><max_retries
type="integer">3</max_retries><type>https</type><method_data>GET</method_data>
<url>/</url><expected>asd</expected><send_data>asd</send_data><receive_data>asd</receive_data><extension>asd</extension></nsx_monitor>'
```

JSON Request Example

```
curl -i -X PUT
http://onapp.test/edges/45/load_balancer/service/monitors/56.json
-H 'Accept: application/json' -H 'Content-type: application/json' -u
user:userpass -d '{"nsx_monitor": {"label": "TEST", "interval": 5,
"timeout": 15, "max_retries": 3, "type": "https", "method_data": "GET",
"url": "/", "expected": "asd", "send_data": "asd", "receive_data": "asd",
"extension": "asd"}}'
```

Where:

- **label** - label of the service monitor
- **interval** - the interval in seconds in which a server is to be tested
- **timeout** - the maximum time in seconds within which a response from the server must be received
- **max_retries** - the number of times the server is tested before it is declared DOWN
- **type** - http, https, tcp, icmp or udp
- **method_data** - GET, OPTIONS or POST
- **url** - the URL to GET or POST
- **expected** - the string that the monitor expects to match in the status line of HTTP response in the Expected section
- **send_data** - the string sent to the back-end server after a connection is established
**receive_data** - the string to be matched

**extension** - advanced monitor parameters as key=value pairs

### 4.10.3.4.5 Delete Service Monitor

To delete a service monitor, use the following request:

```
DELETE /nsx/edges/:edge_id/load_balancer/service/monitors/:monitor_id.xml
DELETE /nsx/edges/:edge_id/load_balancer/service/monitors/:monitor_id.json
```

**XML Request Example**

```
curl -i -X DELETE -u user:userpass
```

**JSON Request Example**

```
curl -i -X DELETE -u user:userpass
```

Returns HTTP 204 response on successful deletion, or HTTP 404 when a service monitor with the ID specified is not found.

### 4.10.3.5 Pools

After you add a server pool to manage load balancer distribution, you can update the existing pool or delete it to save system resources. This following API requests are applicable for NSX load balancer virtual server pools:

- **Get List of Pools**
- **Get Pool Details**
- **Add Pool**
- **Edit Pool**
- **Delete Pool**

### 4.10.3.5.1 Get List of Pools

To view a list of the pools, use the following request:

```
GET /nsx/edges/:edge_id/load_balancer/service/pools.xml
GET /nsx/edges/:edge_id/load_balancer/service/pools.json
```

**XML Request Example**

```
```

**JSON Request Example**

XML Output Example

<nsx_load_balancer_pools type="array">
<nsx_load_balancer_pool>
  <algorithm>ip-hash</algorithm>
  <algorithm_params null="true"/>
  <created_at>2019-10-07T09:45:07.000Z</created_at>
  <description>2</description>
  <id>2</id>
  <identifier>pool-6</identifier>
  <label>p2</label>
  <load_balancer_service_id>9</load_balancer_service_id>
  <monitor_id>26</monitor_id>
  <transparent>false</transparent>
  <updated_at>2019-10-07T09:45:07.000Z</updated_at>
</nsx_load_balancer_pool>
...
</nsx_load_balancer_pools>

Where:

- **algorithm** - round-robin, ip-hash, leastconn, uri, httpheader or url
- **algorithm_params** - algorithm parameters for httpheader, url
- **created_at** - the date when the VS pool was created in the [YYYY][MM][DD][T][hh][mm][ss]Z format
- **description** - the description of the VS pool
- **id** - the edge gateway ID
- **identifier** - the identifier of the pool
- **label** - the label of the pool
- **load_balancer_service_id** - the ID of the load balancer service
- **monitor_id** - the ID of the default or custom monitor
- **transparent** - true if client IP addresses are visible to the back-end servers; otherwise, false
- **updated_at** - the date when the VS pool was created in the [YYYY][MM][DD][T][hh][mm][ss]Z format

4.10.3.5.2 Get Pool Details

To view the details of a particular pool, use the following request:

GET /nsx/edges/:edge_id/load_balancer/service/pools/:pool_id.xml
GET /nsx/edges/:edge_id/load_balancer/service/pools/:pool_id.json

XML Request Example

```bash
```

JSON Request Example

**XML Output Example**

```xml
<nsx_load_balancer_pool>
  <algorithm>ip-hash</algorithm>
  <algorithm_params null="true" />
  <created_at>2019-10-07T09:45:07.000Z</created_at>
  <description>2</description>
  <id>2</id>
  <identifier>pool-6</identifier>
  <label>p2</label>
  <load_balancer_service_id>9</load_balancer_service_id>
  <monitor_id>26</monitor_id>
  <transparent>false</transparent>
  <updated_at>2019-10-07T09:45:07.000Z</updated_at>
</nsx_load_balancer_pool>
```

**Where:**

- **algorithm** - round-robin, ip-hash, leastconn, uri, httpheader or url
- **algorithm_params** - algorithm parameters for httpheader, url
- **created_at** - the date when the VS pool was created in the [YYYY][MM][DD][hh][mm][ss]Z format
- **description** - the description of the VS pool
- **id** - the edge gateway ID
- **identifier** - the identifier of the VS pool
- **label** - the label of the VS pool
- **load_balancer_service_id** - the ID of the load balancer service
- **monitor_id** - the ID of the default or custom monitor
- **transparent** - true if client IP addresses are visible to the back-end servers; otherwise, false
- **updated_at** - the date when the VS pool was created in the [YYYY][MM][DD][hh][mm][ss]Z format

**4.10.3.5.3 Add Pool**

To create a pool, use the following request:

- POST /nsx/edges/:edge_id/load_balancer/service/pools.xml
- POST /nsx/edges/:edge_id/load_balancer/service/pools.json

**XML Request Example**

JSON Request Example

curl -i -X POST -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -url http://onapp.test/nsx/edges/9/load_balancer/service/pools.json -d '{"nsx_pool": {"label": "ads","description": "ads","algorithm": "ip-hash","transparent": "true","monitor": "monitor-2","members": [{"label": "ads","ip_address": "192.168.0.1"},"monitor_port": "1111","port": "2222","enabled": true,"weight": "1","max_conn": "3","min_conn": "4"}]}'

Where:

- **label** - the label of the VS pool
- **description** - the description of the VS pool
- **algorithm** - round-robin, ip-hash, leastconn, uri, httpheader or url
- **transparent** - true if client IP addresses are visible to the back-end servers; otherwise, false
- **monitor** - the identifier of the existing default or custom monitor
- **members** - an array of the server members with the following details:
  - **label** - the name of the server member
  - **ip_address** - the IP address of the server member
  - **monitor_port** - the monitor port where the member is to receive health monitor pings
  - **port** - the port where the member is to receive traffic
  - **enabled** - true if this member is enabled; otherwise, false
  - **weight** - the proportion of traffic this member can handle
  - **max_conn** - the maximum number of concurrent connections that the member can handle. If the incoming requests go higher than the maximum, they are queued and wait for a connection to be released.
  - **min_conn** - the minimum number of concurrent connections that a member must always accept

4.10.3.5.4 Edit Pool

To edit a particular pool, use the following request:

PUT /nsx/edges/:edge_id/load_balancer/service/pools/:pool_id.xml
PUT /nsx/edges/:edge_id/load_balancer/service/pools/:pool_id.json

XML Request Example
JSON Request Example

```
curl -i -X PUT -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -url
http://onapp.test/nsx/edges/9/load_balancer/service/pools/9.json -d
'{"nsx_pool": {
"label": "ads",
"description": "ads",
"algorithm": "ip-hash",
"algorithm_params": "",
"transparent": "true",
"monitor": "monitor-2",
"members": []}}'
```

Where:

- **label** - the label of the pool
- **description** - the description of the pool
- **algorithm** - round-robin, ip-hash, leastconn, uri, httpheader or url
- **algorithm_params** - algorithm parameters for httpheader, url
- **transparent** - true if client IP addresses visible to the back-end servers; otherwise, false
- **monitor** - the identifier of the service monitor

Optional parameters:

- **members** - an array of the server members with the following parameters:
  - **enabled** - set to 1 to enable load balancers service
  - **ip_address** - the IP address of the server member
  - **label** - a name of the server member
  - **max_conn** - enter the maximum number of concurrent connections that the member can handle. If the incoming requests go higher than the maximum, they are queued and wait for a connection to be released.
  - **min_conn** - enter the minimum number of concurrent connections that a member must always accept
  - **port** - enter the monitor port where the member is to receive health monitor pings
  - **weight** - enter the proportion of traffic this member can handle

4.10.3.5.5 Delete Pool

To delete a pool, use the following request:

```
DELETE /nsx/edges/:edge_id/load_balancer/service/pools/:pool_id.xml
DELETE /nsx/edges/:edge_id/load_balancer/service/pools/:pool_id.json
```

XML Request Example

```
curl -i -X PUT -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -url
'<?xml version="1.0"?>
<nsx_pool><label>ads</label><description>ads</description>
<algorithm>ip-hash</algorithm><algorithm_params></algorithm_params><transparent type="boolean">true</transparent><monitor>monitor-2</monitor><members type="array"/></nsx_pool>'
```
4.10.3.6 Application Rules
You can write an application rule to directly manipulate and manage application traffic. Below you can find the list of operations for application rules:

- Get List of Application Rules
- Get Application Rule Details
- Add Application Rule
- Edit Application Rule
- Delete Application Rule

4.10.3.6.1 Get List of Application Rules
To get the list of application rules, use the following request:

GET /nsx/edges/:edge_id/load_balancer/service/application_rules.xml
GET /nsx/edges/:edge_id/load_balancer/service/application_rules.json

XML Request Example

```
```

JSON Request Example

```
```

XML Output Example
<nsx_load_balancer_application_rules type="array">
  <nsx_load_balancer_application_rule>
    <id type="integer">3</id>
    <identifier>applicationRule-1</identifier>
    <label>ar1</label>
    <script>acl block ACME path_beg -i /cloud/org/acme block if block_ACME</script>
    <load_balancer_service_id type="integer">3</load_balancer_service_id>
    <created_at type="dateTime">2019-11-06T10:16:58Z</created_at>
    <updated_at type="dateTime">2019-11-06T10:16:58Z</updated_at>
  </nsx_load_balancer_application_rule>
  <nsx_load_balancer_application_rule>
    <id type="integer">4</id>
    <identifier>applicationRule-2</identifier>
    <label>ar2</label>
    <script>acl block ACME path_beg -i /cloud/org/acme</script>
    <load_balancer_service_id type="integer">3</load_balancer_service_id>
    <created_at type="dateTime">2019-11-06T10:16:58Z</created_at>
    <updated_at type="dateTime">2019-11-06T10:16:58Z</updated_at>
  </nsx_load_balancer_application_rule>
</nsx_load_balancer_application_rules>

Where:

- **id** - ID of the application rule
- **identifier** - identifier of the application rule
- **label** - label of the application rule
- **script** - script of the application rule
- **load_balancer_service_id** - ID of the load balancer service

**created_at** - the date when the firewall rule was created in the [YYYY][MM][DD][hh][mm][ss]Z format

**updated_at** - the date when the firewall rule was updated in the [YYYY][MM][DD][hh][mm][ss]Z format

4.10.3.6.2 Get Application Rule Details
To get the details of an application rule, use the following request

GET /nsx/edges/:edge_id/load_balancer/service/application_rules/:rule_id.xml
GET /nsx/edges/:edge_id/load_balancer/service/application_rules/:rule_id.json

**XML Request Example**


**JSON Request Example**
XML Output Example

```xml
<nsx_load_balancer_application_rule>
  <id type="integer">4</id>
  <identifier>applicationRule-2</identifier>
  <label>ar2</label>
  <script>acl block_ACME path_beg -i /cloud/org/acme</script>
  <load_balancer_service_id type="integer">3</load_balancer_service_id>
  <created_at type="dateTime">2019-11-06T10:16:58Z</created_at>
  <updated_at type="dateTime">2019-11-06T10:16:58Z</updated_at>
</nsx_load_balancer_application_rule>
```

Where:

- **id** - ID of the application rule
- **identifier** - identifier of the application rule
- **label** - label of the application rule
- **script** - script of the application rule
- **load_balancer_service_id** - ID of the load balancer service
- **created_at** - the date when the firewall rule was created in the [YYYY][MM][DD]T[hh][mm][ss]Z format
- **updated_at** - the date when the firewall rule was updated in the [YYYY][MM][DD]T[hh][mm][ss]Z format

4.10.3.6.3 Add Application Rule

To add a new application rule, use the following request:

**XML Request Example**

```bash
```

**JSON Request Example**

```bash
```
Where:

`label` - label of the application rule

`script` - application rule script

4.10.3.6.4 Edit Application Rule

To edit an application rule, use the following request:

PUT /nsx/edges/:edge_id/load_balancer/service/application_rules/:rule_id.xml

PUT /nsx/edges/:edge_id/load_balancer/service/application_rules/:rule_id.json

XML Request Example

curl -i -X PUT -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -url
http://onapp.test/nsx/edges/9/load_balancer/service/application
rules/9.xml -d '<nsx_application_rule><label>TEST</label><script>script.sh
-r -avga</script></nsx_application_rule>'

JSON Request Example

curl -i -X PUT -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -url
http://onapp.test/nsx/edges/9/load_balancer/service/pools/9.json -d
'{"nsx_application_rule": {"label": "TEST", "script": "script.sh -r -asf"}}'

Where:

`label` - label of the application rule

`script` - application rule script

4.10.3.6.5 Delete Application Rule

To delete an application rule, use the following request:

DELETE /nsx/edges/:edge_id/load_balancer/service/application_rules/:ru
le_id.xml

DELETE /nsx/edges/:edge_id/load_balancer/service/application_rules/:ru
le_id.json

XML Request Example

curl -i -X DELETE -u user:userpass
http://onapp.test/nsx/edges/3/load_balancer/service/application_rules/13.x
ml -H 'Accept: application/xml' -H 'Content-type: application/xml'

JSON Request Example

curl -i -X DELETE -u user:userpass
13.json -H 'Accept: application/json' -H 'Content-type: application/json'

Returns HTTP 204 response on successful deletion, or HTTP 404 when an application rule with the ID specified is not found.
4.10.3.7 Virtual Servers

After you add virtual servers, you can update the existing virtual server configuration or delete it. This section contains the following API requests:

- Get List of Virtual Servers
- Get Virtual Server Details
- Add Virtual Server
- Edit Virtual Server
- Delete Virtual Server

4.10.3.7.1 Get List of Virtual Servers

To view the list of virtual servers, use the following request:

GET /nsx/edges/:edge_id/load_balancer/service/virtual_servers.xml
GET /nsx/edges/:edge_id/load_balancer/service/virtual_servers.json

**XML Request Example**


**JSON Request Example**


**XML Output Example**

```
<nsx_load_balancer_virtual_servers type="array">
  <nsx_load_balancer_virtual_server>
    <id type="integer">6</id>
    <identifier>virtualServer-24</identifier>
    <label>vs1</label>
    <description nil="true"/>
    <ip_address>69.168.237.214</ip_address>
    <port>2222</port>
    <protocol>tcp</protocol>
    <connection_limit type="integer">0</connection_limit>
    <connection_rate_limit type="integer">0</connection_rate_limit>
    <enabled type="boolean">false</enabled>
    <acceleration type="boolean">false</acceleration>
    <default_pool_id type="integer">2</default_pool_id>
    <load_balancer_service_id type="integer">3</load_balancer_service_id>
    <created_at type="dateTime">2019-11-07T11:44:20Z</created_at>
    <updated_at type="dateTime">2019-11-07T11:44:20Z</updated_at>
  </nsx_load_balancer_virtual_server>
</nsx_load_balancer_virtual_servers>
```

**Where:**

id - the ID of the virtual server
identifier - the identifier of the VS
label - the name of a virtual server
description - the description of the VS
ip_address - an IP address that the load balancer is listening on
port - the port number that the load balancer listens on
protocol - http, https, tcp or udp
connection_limit - the maximum concurrent connections that the virtual server can process
connection_rate_limit - the maximum incoming new connection requests per second section
enabled - true if this virtual server is available for use; otherwise, false
acceleration - true if acceleration is enabled for this VS; otherwise, false
default_pool_id - the identifier of the default VSs pool
load_balancer_service_id - the ID of the load balancer service
created_at - the date when the VS was created in the [YYYY][MM][DD][hh][mm][ss]Z format
updated_at - the date when the VS was updated in the [YYYY][MM][DD][hh][mm][ss]Z format
application_profile_id - the ID of the application profile associated with this VS

4.10.3.7.2 Get Virtual Server Details
To view the details of a particular virtual server, use the following request:

GET /nsx/edges/:edge_id/load_balancer/service/virtual_servers/:virtual_server_id.xml
GET /nsx/edges/:edge_id/load_balancer/service/virtual_servers/:virtual_server_id.json

XML Request Example


JSON Request Example


XML Output Example
<nsx_load_balancer_virtual_server>
  <id type="integer">6</id>
  <identifier>virtualServer-24</identifier>
  <label>vs1</label>
  <description nil="true"/>
  <ip_address>69.168.237.214</ip_address>
  <port>222</port>
  <protocol>tcp</protocol>
  <connection_limit type="integer">0</connection_limit>
  <connection_rate_limit type="integer">0</connection_rate_limit>
  <enabled type="boolean">false</enabled>
  <acceleration type="boolean">false</acceleration>
  <default_pool_id type="integer">2</default_pool_id>
  <load_balancer_service_id type="integer">3</load_balancer_service_id>
  <created_at type="dateTime">2019-11-07T11:44:20Z</created_at>
  <updated_at type="dateTime">2019-11-07T11:44:20Z</updated_at>
  <application_profile_id type="integer">6</application_profile_id>
</nsx_load_balancer_virtual_server>

Where:

id - ID of the VS
identifier- the identifier of the VS
label- the name of a virtual server
description - the description of the VS
ip_address - an IP address that the load balancer is listening on
port - the port number that the load balancer listens on
protocol - http, https, tcp or udp
connection_limit - the maximum concurrent connections that the virtual server can process
connection_rate_limit - the maximum incoming new connection requests per second section
enabled - true if this virtual server is available for use; otherwise, false
acceleration - true if acceleration is enabled for this VS; otherwise, false
default_pool_id- the ID of the default VSs pool
load_balancer_service_id - the identifier of the load balancer service
created_at- the date when the VS was created in the [YYYY][MM][DD][hh][mm][ss]Z format
updated_at- the date when the VS was updated in the [YYYY][MM][DD][hh][mm][ss]Z format
application_profile_id - the ID of the application profile associated with this VS

4.10.3.7.3 Add Virtual Server
To create a virtual server, use the following request:
POST /nsx/edges/:edge_id/load_balancer/service/virtual_servers.xml
POST /nsx/edges/:edge_id/load_balancer/service/virtual_servers.json

XML Request Example
curl -i -X POST -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -url
http://onapp.test/nsx/edges/9/load_balancer/service/virtual_servers.xml -d '<nsx_virtual_server><label>New</label><description>New</description><ip_address>10.0.0.138</ip_address><port>4321</port><protocol>tcp</protocol><connection_limit>1</connection_limit><connection_rate_limit>2</connection_rate_limit><enabled type="boolean">true</enabled><acceleration type="boolean">false</acceleration><application_profile>applicationProfile-3</application_profile><default_pool>pool-7</default_pool><application_rules type="array">applicationRule-1</application_rule><application_rule>applicationRule-2</application_rule></nsx_virtual_server>'

JSON Request Example

curl -i -X POST -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -url
http://onapp.test/nsx/edges/9/load_balancer/service/virtual_servers.json -d '{"nsx_virtual_server": {"label": "New","description": "New","ip_address": "10.0.0.138","port": "4321","protocol": "tcp","connection_limit": "1","connection_rate_limit": "2","enabled": true,"acceleration": false,"application_profile": "applicationProfile-3","default_pool": "pool-7","application_rules": ["applicationRule-1","applicationRule-2"]}}'

Where:

- **label** - the name of a virtual server
- **description** - the description of the VS
- **ip_address** - an IP address that the load balancer is listening on
- **port** - the port number that the load balancer listens on
- **protocol** - http, https, tcp or udp
- **connection_limit** - the maximum concurrent connections that the virtual server can process
- **connection_rate_limit** - the maximum incoming new connection requests per second section
- **enabled** - true if this virtual server is available for use; otherwise, false
- **acceleration** - true if acceleration is enabled for this VS; otherwise, false
- **application_profile** - the label of the application profile associated with this VS
- **default_pool** - identifier of the default pool
- **application_rules** - an array of application rules associated with the virtual server

4.10.3.7.4 Edit Virtual Server

To edit virtual servers, use the following request:

PUT /nsx/edges/:edge_id/load_balancer/service/virtual_servers/:virtual_server_id.xml
PUT /nsx/edges/:edge_id/load_balancer/service/virtual_servers/:virtual_server_id.json

XML Request Example

'\n<nxs\_virtual\_server><label>New</label><description>New</description><ip\_address>10.0.0.138</ip\_address><port>4321</port><protocol>tcp</protocol><connection\_limit>1</connection\_limit><connection\_rate\_limit>2</connection\_rate\_limit><enabled type="boolean">true</enabled><acceleration type="boolean">false</acceleration><application\_profile>applicationProfile-3</application\_profile><default_pool>pool-7</default_pool><application\_rules type="array"></application\_rules></nxs\_virtual\_server>'

JSON Request Example

```
curl -i -X PUT -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -d '{"nsx\_virtual\_server": {"label": "NEWEST","description": "New","ip\_address": "10.0.0.138", "port": "4321","protocol": "tcp","connection\_limit": "1","connection\_rate\_limit": "2","enabled": "1","acceleration": "0","application\_profile": "applicationProfile-3","default_pool": "pool-7","application\_rules": []}}}'
```

Where:

- **label** - the name of a virtual server
- **description** - the description of the VS
- **ip\_address** - an IP address that the load balancer is listening on
- **port** - the port number that the load balancer listens on
- **protocol** - http, https, tcp or udp
- **connection\_limit** - the maximum concurrent connections that the virtual server can process
- **connection\_rate\_limit** - the maximum incoming new connection requests per second section
- **enabled** - true, if this virtual server is available for use; otherwise, false
- **acceleration** - true, if acceleration is enabled for this VS; otherwise, false
- **application\_profile** - the label of the application profile associated with this VS
- **default\_pool** - the identifier of the default pool
- **application\_rules** - an array of application rules associated with the virtual server

4.10.3.7.5 Delete Virtual Server

To delete a virtual server, use the following request:

```
DELETE /nsx/edges/:edge_id/load_balancer/service/virtual_servers/:virtual_server_id.xml
DELETE /nsx/edges/:edge_id/load_balancer/service/virtual_servers/:virtual_server_id.json
```

XML Request Example
JSON Request Example

```
curl -i -X DELETE -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -
```

Returns HTTP 204 response on successful deletion, or HTTP 404 when a VS with the ID specified is not found.

### 4.10.4 NSX Managers API

The NSX Manager is used to deploy a universal controller cluster that provides the control plane for the NSX environment. At OnApp, you can import NSX manager with limited functionality available and set vCloud credentials to gain access to full functionality. Once imported, it allows you to view and edit imported vCloud edge gateways in OnApp interface.

Below you can find the list of operations applicable for NSX managers:

- Get List of NSX Managers
- Get NSX Manager Details
- Import NSX Manager
- Update NSX Manager Credentials

#### 4.10.4.1 Get List of NSX Managers

To get the list of NSX managers in your cloud, use the following request:

GET /settings/nsx/managers.xml
GET /settings/nsx/managers.json

**XML Request Example**

```
curl -i -X GET -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -
url http://onapp.test/settings/nsx/managers.xml
```

**JSON Request Example**

```
curl -i -X GET -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -
url http://onapp.test/settings/nsx/managers.json
```

**XML Output Example**
<nsx_managers type="array">  
  <nsx_manager>  
    <id type="integer">1</id>  
    <label>NSX manager for vc-c.onappdev.host</label>  
    <api_url>https://nsx-c.onappdev.host:443</api_url>  
    <login>admin</login>  
    <password>P@ssword1!</password>  
    <vcenter_type>Nsx::VCloud::VCenter</vcenter_type>  
    <vcenter_id type="integer">1</vcenter_id>  
    <created_at type="dateTime">2019-11-11T08:00:51Z</created_at>  
    <updated_at type="dateTime">2019-11-11T08:28:36Z</updated_at>  
    <version>6.4.5 Build 13282012</version>  
    <host>nsx-c.onappdev.host</host>  
    <status>RUNNING</status>  
    <uptime>8 days, 16 hours, 33 minutes</uptime>  
  </nsx_manager>  
  <nsx_manager>  
    <id type="integer">2</id>  
    <label>NSX manager for vc-d.onappdev.host</label>  
    <api_url>https://nsx-d.onappdev.host:443</api_url>  
    <login>admin</login>  
    <password nil="true"/>  
    <vcenter_type>Nsx::VCloud::VCenter</vcenter_type>  
    <vcenter_id type="integer">2</vcenter_id>  
    <created_at type="dateTime">2019-11-11T08:00:52Z</created_at>  
    <updated_at type="dateTime">2019-11-11T08:00:52Z</updated_at>  
    <host nil="true"/>  
    <status nil="true"/>  
    <uptime nil="true"/>  
  </nsx_manager>  
</nsx_managers>  

**Where:**  
- **id** - the ID of the NSX manager  
- **label** - the label of the NSX manager  
- **api_url** - the URL used to connect to NSX  
- **login** - login of the NSX manager  
- **password** - password of the NSX manager  
- **vcenter_type** - Nsx::VCloud::VCenter or Nsx::Hypervisor  
- **vcenter_id** - ID of the vCenter VS  
- **created_at** - the date when the NSX manager was created in the [YYYY][MM][DD][hh][mm][ss]Z format  
- **updated_at** - the date when the NSX manager was updated in the [YYYY][MM][DD][hh][mm][ss]Z format  
- **version** - NSX version  
- **host** - hostname of the vCenter VS  
- **status** - STARTING, RUNNING, STOPPING, or STOPPED  
- **uptime** - duration of the uptime  

**Page History**  
v.6.3 Edge 1
• removed last_seen_event parameter

4.10.4.2 Get NSX Manager Details
To get an NSX manager details, use the following request:

GET /settings/nsx/managers/:manager_id.xml
GET /settings/nsx/managers/:manager_id.json

XML Request Example


JSON Request Example


XML Output Example

```xml
<nsx_manager>
  <id type="integer">1</id>
  <label>NSX manager for vc-c.onappdev.lviv</label>
  <api_url>https://nsx-c.onappdev.lviv:443</api_url>
  <login>admin</login>
  <password>Password1!</password>
  <vcenter_type>Nsx::VCloud::VCenter</vcenter_type>
  <vcenter_id type="integer">1</vcenter_id>
  <created_at type="dateTime">2019-11-11T08:00:51Z</created_at>
  <updated_at type="dateTime">2019-11-11T08:28:36Z</updated_at>
  <version>6.4.5 Build 13282012</version>
  <host>nsx-c.onappdev.lviv</host>
  <status>RUNNING</status>
  <uptime>8 days, 16 hours, 33 minutes</uptime>
</nsx_manager>
```

Where:

- `api_url` - the URL used to connect to NSX
- `created_at` - the date when the NSX manager was created in the [YYYY][MM][DD][hh][mm][ss]Z format
- `updated_at` - the date when the NSX manager was updated in the [YYYY][MM][DD][hh][mm][ss]Z format
- `id` - the ID of the NSX manager
- `label` - the label of the NSX manager
- `login` - login of the NSX manager
- `password` - password of the NSX manager
- `vcenter_id` - ID of the vCenter VS
- `vcenter_type` - Nsx::VCloud::VCenter or Nsx::Hypervisor
- `version` - NSX version
host - hostname of the vCenter VS
status - STARTING, RUNNING, STOPPING, or STOPPED
uptime - duration of the uptime

Page History
v.6.3 Edge 1
- removed last_seen_event parameter

4.10.4.3 Import NSX Manager
To import an NSX manager, use the following request:
POST /settings/nsx/managers/:manager_id/import.xml
POST /settings/nsx/managers/:manager_id/import.json

XML Request Example
```
```

JSON Request Example
```
```

4.10.4.4 Update NSX Manager Credentials
To update the NSX manager’s credentials, use the following request:
PUT /settings/nsx/managers/:manager_id/credentials.xml
PUT /settings/nsx/managers/:manager_id/credentials.json

XML Request Example
```
```

JSON Request Example
```
curl -i -X PUT -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -d --url http://onapp.test/settings/nsx/managers/4/credentials.json -d '{"nsx_manager_credentials": {"login": "admin", "password": "P@ssword1!"}}'
```

Where:
login - login for this NSX manager
password - the password for this NSX manager
4.10.5 NSX IPSec VPN API

Internet Protocol Security (IPSec) VPN ensures secure and private communications over Internet Protocol (IP) networks. It authenticates and encrypts IP packets between two end points. This section contains the API requests you can use to manage NSX IPSec VPN service and IPSec VPN sites.

4.10.5.1 NSX IPSec VPN Service

Below you can find the list of operations applicable for NSX IPSec VPN services:

- Get IPSec VPN Service Details
- Edit IPSec VPN Service

4.10.5.1.1 Get IPSec VPN Service Details

To get IPSec VPN service details, use the following request:

GET /nsx/edges/:edge_id/vpn/ipsec/service.xml
GET /nsx/edges/:edge_id/vpn/ipsec/service.json

XML Request Example


JSON Request Example


XML Output Example

```xml
<nsx_ipsec_service>
  <id type="integer">116</id>
  <enabled type="boolean">true</enabled>
  <logging type="boolean">true</logging>
  <edge_id type="integer">126</edge_id>
  <service_certificate_id type="integer">205</service_certificate_id>
  <psk>testkey</psk>
  <log_level>info</log_level>
  <created_at type="dateTime">2019-11-06T13:01:09Z</created_at>
  <updated_at type="dateTime">2019-11-06T13:01:09Z</updated_at>
  <locked type="boolean">false</locked>
</nsx_ipsec_service>
```

Where:

- **id** - ID of the IPSec VPN service
- **enabled** - true, if IPSec VPN service is enabled; otherwise, false
- **logging** - true, if logging for this IPSec VPN service is enabled; otherwise, false
- **edge_id** - ID of the edge this IPSec VPN service was created for
- **service_certificate_id** - ID of the service certificate
- **psk** - the value of the pre-shared key
log_level - emergency, alert, critical, error, warning, notice, info or debug

created_at - the date when the IPSec VPN service was created in the [YYYY][MM][DD][hh][mm][ss]Z format

updated_at - the date when the IPSec VPN service was updated in the [YYYY][MM][DD][hh][mm][ss]Z format

locked - true, if IPSec VPN service is locked; otherwise, false

4.10.5.1.2 Edit IPSec VPN Service

To edit IPSec VPN service, use the following request:

PUT /nsx/edges/:edge_id/vpn/ipsec/service.xml
PUT /nsx/edges/:edge_id/vpn/ipsec/service.json

XML Request Example

curl -i -X PUT -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -d
"<nsx_ipsec_service><certificate_auth_enabled>true</certificate_auth_enabled><enabled>true</enabled><ipsec_sites>
  <ipsec_site><authentication_mode>psk</authentication_mode><compliance_suite>none</compliance_suite><dh_group>dh5</dh_group><digest_algorithm>sha1</digest_algorithm><enable_pfs>false</enable_pfs><enabled>false</enabled><encryption_algorithm>aes</encryption_algorithm><ike_option>ikev1</ike_option><ipsec_session_type>policybasedsession</ipsec_session_type><label>Alpha</label><local_id>10.0.0.133</local_id><local_ip>10.0.0.133</local_ip><local_subnets>
  <local_subnet>0.0.0.0/0</local_subnet></local_subnets><peer_id>123.23.3.3</peer_id><peer_ip>123.23.3.3</peer_ip><peer_subnets>
  <peer_subnet>0.0.0.0/0</peer_subnet></peer_subnets><psk>:testkey</psk><responder_only>false</responder_only></ipsec_site></ipsec_sites><log_level>info</log_level><logging>true</logging><psk>testkey</psk><service_certificate>certificate-45</service_certificate></nsx_ipsec_service>"

JSON Request Example

curl -i -X PUT -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -d
'{"nsx_ipsec_service": {"enabled":true, "logging":true, "log_level":"info", "psk":"testkey", "service_certificate":"certificate-45", "certificate_auth_enabled":true, "ipsec_sites":[{"enabled":false, "label":"Alpha", "local_id":"10.0.0.133", "local_ip":"10.0.0.133", "peer_id":"123.23.3.3", "peer_ip":"123.23.3.3", "ipsec_session_type":"policybasedsession", "encryption_algorithm":"aes", "enable_pfs":false, "dh_group":"dh5", "psk":"testkey", "authentication_mode":"psk", "digest_algorithm":"sha1", "responder_only":false, "compliance_suite":null, "ike_option":"ikev1", "local_subnets":null, "peer_subnets":null}}}}

Where:

enabled* - true, if IPSec VPN service is enabled; otherwise, false

logging* - true, if logging for IPSec VPN service is enabled; otherwise, false

log_level* - emergency, alert, critical, error, warning, notice, info or debug

psk - the value of the pre-shared key
service_certificate - identifier of the service certificate (optional; required if any IPSec site uses certificate authentication)

certificate_auth_enabled* - true, if certificate authentication is enabled; otherwise, false

ipsec_sites:
  • enabled* - true, if IPSec VPN site is enabled; otherwise, false (local IP must be assigned to an Edge's Uplink vNIC)
  • label - label of an IPSec VPN site
  • local_id* - ID of the local site
  • local_ip* - IP of the local site (local IP must be assigned to an Edge's Uplink vNIC)
  • peer_id* - ID of a peer site (for certificate authentication must be a valid Distinguished Name)
  • peer_ip* - IP or FQDN of a peer site
  • ipsec_session_type - policybasedsession or routebasedsession. If routebasedsession is selected:
    o tunnel_interface_ip* - tunnel interface IP in CIDR notation
    o tunnel_interface_mtu* - MTU, allowed values 152 - 8916 (inclusively)
  • encryption_algorithm* - aes, aes256, aes-gsm, or 3des
  • enable_pfs* - true, if PFS is enabled; otherwise, false
  • dh_group* - dh2, dh5, dh14, dh15, or dh16
  • psk - the value of the pre-shared key
  • authentication_mode* - psk or x.509 (for Certificate mode; available only if service_certificate for a service is set)
  • digest_algorithm* - sha1 or sha-256
  • responder_only* - true, if IKE Responder Only option is enabled; otherwise, false
  • compliance_suite - none, cnsa, prime, suite-b-gcm-128, suite-b-gcm-256, suite-b-gmac-128, suite-b-gmac-256, or foundation
  • ike_option* - ikev1, ikev2, or ike-flex
  • local_subnets* - an array of local subnets in CIDR format (If routebasedsession is set for ipsec_session_type, local_subnets value should be "[0.0.0.0/0]")
  • peer_subnets* - an array of peer subnets in CIDR format (If routebasedsession is set for ipsec_session_type, peer_subnets value should be "[0.0.0.0/0]"

4.10.5.2 NSX IPSec VPN Sites
Below you can find the list of operations applicable for NSX IPSec VPN sites:

  • Get List of IPSec VPN Sites
  • Get IPSec VPN Site Details
  • Add IPSec VPN Site
  • Edit IPSec VPN Site
  • Delete IPSec VPN Site

4.10.5.2.1 Get List of IPSec VPN Sites
To get list of IPSec VPN sites, use the following request:
GET /nsx/edges/:edge_id/vpn/ipsec/service/sites.xml
GET /nsx/edges/:edge_id/vpn/ipsec/service/sites.json

**XML Request Example**

```
```

**JSON Request Example**

```
```

**XML Output Example**
<nsx_ipsec_sites type="array">
    <nsx_ipsec_site>
        <id type="integer">735</id>
        <enabled type="boolean">false</enabled>
        <label>Alpha</label>
        <identifier>ipsecsite-170</identifier>
        <ipsec_service_id type="integer">116</ipsec_service_id>
        <local_id>123123213123123123</local_id>
        <local_ip>10.0.0.133</local_ip>
        <peer_id>123123213123123123</peer_id>
        <peer_ip>123.23.3.3</peer_ip>
        <ipsec_session_type>policybasedsession</ipsec_session_type>
        <encryption_algorithm>aes</encryption_algorithm>
        <enable_pfs type="boolean">false</enable_pfs>
        <dh_group>dh5</dh_group>
        <tunnel_interface_ip_address nil="true"/>
        <tunnel_interface_mtu nil="true"/>
        <ipsec_session_type>policybasedsession</ipsec_session_type>
        <encryption_algorithm>aes</encryption_algorithm>
        <enable_pfs type="boolean">false</enable_pfs>
        <dh_group>dh5</dh_group>
        <tunnel_interface_ip_address nil="true"/>
        <tunnel_interface_mtu nil="true"/>
    </nsx_ipsec_site>
    <nsx_ipsec_site>
        <id type="integer">736</id>
        <enabled type="boolean">false</enabled>
        <label>Subnet</label>
        <identifier>ipsecsite-171</identifier>
        <ipsec_service_id type="integer">116</ipsec_service_id>
        <local_id>10.0.0.133</local_id>
        <local_ip>10.0.0.133</local_ip>
        <peer_id>123.32.3.3</peer_id>
        <peer_ip>123.32.3.3</peer_ip>
        <ipsec_session_type>policybasedsession</ipsec_session_type>
        <encryption_algorithm>aes-gcm</encryption_algorithm>
        <enable_pfs type="boolean">false</enable_pfs>
        <dh_group>dh15</dh_group>
        <tunnel_interface_ip_address nil="true"/>
        <tunnel_interface_mtu nil="true"/>
    </nsx_ipsec_site>
    <nsx_ipsec_site>
        <id type="integer">737</id>
        <enabled type="boolean">false</enabled>
        <label>Subnet</label>
        <identifier>ipsecsite-172</identifier>
        <ipsec_service_id type="integer">116</ipsec_service_id>
        <local_id>122.123.23.128/32</local_id>
        <local_ip>122.123.23.128/32</local_ip>
        <peer_id>123.32.3.3</peer_id>
        <peer_ip>123.32.3.3</peer_ip>
        <ipsec_session_type>policybasedsession</ipsec_session_type>
        <encryption_algorithm>aes-gcm</encryption_algorithm>
        <enable_pfs type="boolean">false</enable_pfs>
        <dh_group>dh15</dh_group>
        <tunnel_interface_ip_address nil="true"/>
        <tunnel_interface_mtu nil="true"/>
    </nsx_ipsec_site>
    <nsx_ipsec_site>
        <id type="integer">738</id>
        <enabled type="boolean">false</enabled>
        <label>Subnet</label>
        <identifier>ipsecsite-173</identifier>
        <ipsec_service_id type="integer">116</ipsec_service_id>
        <local_id>122.123.23.128/32</local_id>
        <local_ip>122.123.23.128/32</local_ip>
        <peer_id>123.32.3.3</peer_id>
        <peer_ip>123.32.3.3</peer_ip>
        <ipsec_session_type>policybasedsession</ipsec_session_type>
        <encryption_algorithm>aes-gcm</encryption_algorithm>
        <enable_pfs type="boolean">false</enable_pfs>
        <dh_group>dh15</dh_group>
        <tunnel_interface_ip_address nil="true"/>
        <tunnel_interface_mtu nil="true"/>
    </nsx_ipsec_site>
</nsx_ipsec_sites>
Where:

- **id** - ID of the IPSec VPN site
- **enabled** - true, if IPSec VPN site is enabled; otherwise, false
- **label** - the label of the IPSec VPN site
- **identifier** - identifier of the IPSec VPN site
- **ipsec_service_id** - ID of the IPSec VPN service
- **local_id** - ID of the local site
- **local_ip** - IP of the local site
- **peer_id** - ID of a peer site
- **peer_ip** - IP of a peer site
- **ipsec_session_type** - policybasedsession or routebasedsession. If **ipsec_session_type** is set to routebasedsession:
  - **tunnel_interface_ip** - tunnel interface IP in CIDR notation
  - **tunnel_interface_mtu** - MTU, allowed values 152 - 8916 (inclusively)
- **encryption_algorithm** - aes, aes256, aes-gsm, or 3des
- **enable_pfs** - true, if PFS is enabled; otherwise, false
- **dh_group** - dh2, dh5, dh14, dh15, or dh16
- **local_subnets** - an array of local subnets in CIDR format
- **peer_subnets** - an array of peer subnets in CIDR format
- **psk** - the value of the pre-shared key
- **authentication_mode** - psk or x.509 (for Certificate mode)
- **extension** - securelocaltrafficbyip=IPAddress or passthroughSubnets=PeerSubnetIPAddress
- **digest_algorithm** - sha1 or sha-256
- **responder_only** - true, if IKE Responder Only option is enabled; otherwise, false
- **compliance_suite** - none, cnca, prime, suite-b-gcm-128, suite-b-gcm-256, suite-b-gmac-128, suite-b-gmac-256, or foundation
- **ike_option** - ikev1, ikev2, or ike-flex
- **certificate_id** - identifier of the certificate

4.10.5.2.2 Get IPSec VPN Site Details

To get the IPSec VPN site details, use the following request:

GET /nsx/edges/:edge_id/vpn/ipsec/service/sites/:site_id.xml
GET /nsx/edges/:edge_id/vpn/ipsec/service/sites/:site_id.json

**XML request Example**

```bash
```

**JSON Request Example**

XML Output Example
<nsx_ipsec_site>
  <id type="integer">735</id>
  <enabled type="boolean">false</enabled>
  <label>Alpha</label>
  <identifier>ipsecsite-170</identifier>
  <ipsec_service_id type="integer">116</ipsec_service_id>
  <local_id>123123213123123123</local_id>
  <local_ip>10.0.0.133</local_ip>
  <peer_id>123123123123123123</peer_id>
  <peer_ip>123.23.3.3</peer_ip>
  <ipsec_session_type>policybasedsession</ipsec_session_type>
  <encryption_algorithm>aes</encryption_algorithm>
  <enable_pfs type="boolean">false</enable_pfs>
  <dh_group>dh5</dh_group>
  <tunnel_interface_ip nil="true"/>
  <tunnel_interface_mtu nil="true"/>
  <local_subnets type="array">
    <local_subnet>0.0.0.0</local_subnet>
  </local_subnets>
  <peer_subnets type="array">
    <peer_subnet>0.0.0.0</peer_subnet>
  </peer_subnets>
  <psk>:SLEFPSKLFEP{SEKFSEP{KFSP<SEF<SEF<SEF</psk>
  <authentication_mode>psk</authentication_mode>
  <digest_algorithm>sha1</digest_algorithm>
  <responder_only type="boolean">false</responder_only>
  <ike_option>ikev1</ike_option>
  <certificate_id nil="true"/>
</nsx_ipsec_site>

Where:

- **id** - ID of the IPSec VPN site
- **enabled** - true, if IPSec VPN site is enabled; otherwise, false
- **label** - label of the IPSec VPN site
- **identifier** - identifier of the IPSec VPN site
- **ipsec_service_id** - ID of the IPSec VPN service
- **local_id** - ID of the local site
- **local_ip** - IP of the local site
- **peer_id** - ID of a peer site
- **peer_ip** - IP of a peer site
- **ipsec_session_type** - policybasedsession or routebasedsession. If **ipsec_session_type** is set to routebasedsession:
  - **tunnel_interface_ip** - tunnel interface IP in CIDR notation
  - **tunnel_interface_mtu** - MTU, allowed values 152 - 8916 (inclusively)
encryption_algorithm - aes, aes256, aes-gsm, or 3des
enable_pfs - true, if PFS is enabled; otherwise, false
dh_group - dh2, dh5, dh14, dh15, or dh16
local_subnets - an array of local subnets in CIDR format
peer_subnets - an array of peer subnets in CIDR format
psk - the value of the pre-shared key
authentication_mode - psk or x.509 (for Certificate mode)
extension - securelocaltrafficbyip=IPAddress or passthroughSubnets=PeerSubnetIPAddress
digest_algorithm - sha1 or sha-256
responder_only - true, if IKE Responder Only option is enabled; otherwise, false
compliance_suite - none, cnsa, prime, suite-b-gcm-128, suite-b-gcm-256, suite-b-gmac-128, suite-b-gmac-256, or foundation
ike_option - ikev1, ikev2, or ike-flex
certificate_id - identifier of the certificate

4.10.5.2.3 Add IPSec VPN Site
To add an IPSec VPN site, use the following request:

POST /nsx/edges/:edge_id/vpn/ipsec/service/sites/:site_id.xml
POST /nsx/edges/:edge_id/vpn/ipsec/service/sites/:site_id.json

XML Request Example

ike_option<i-ike-flex</ike_option><ipsec_session_type>routebasedsession</ipsec_session_type><label>Bravo</label><local_id>10.0.0.133</local_id><local_ip>10.0.0.133</local_ip><local_subnets type="array"><local_subnet>0.0.0.0/0</local_subnet></local_subnets><peer_i
C=Test, L=host peer_ip>123.32.4.32</peer_ip><peer_subnets type="array"><peer_subnet>0.0.0.0/0</peer_subnet> responder
only>false</responder_only><tunnel_interface_ip_address>23.23.21.23/24</tunnel_interface_ip_address><tunnel_interface_mtu>1500</tunnel_interface_mtu></nsx_ipsec_site>'

JSON Request Example
curl -i -X POST -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass --url http://onapp.test/nsx/edges/113/vpn/ipsec/service/sites/3.json -d '{"nsx_ipsec_site": {"enabled": false, "label": "Bravo", "local_id": "10.0.0.133", "local_ip": "10.0.0.133", "peer_id": "C=Test, L=host", "peer_ip": "123.32.4.32", "ipsec_session_type": "routebasedsession", "encryption_algorithm": "aes-gcm", "enable_pfs": false, "dh_group": "dh5", "tunnel_interface_ip_address": "23.23.21.23/24", "tunnel_interface_mtu": 1500, "local_subnets": ["0.0.0.0/0"], "peer_subnets": ["0.0.0.0/0"], "authentication_mode": "x.509", "extension": ",", "digest_algorithm": "sha-256", "responder_only": false, "compliance_suite": "none", "ike_option": "ike-flex", "certificate": "certificate-45"}}'

Where:

enabled* - true, if IPSec VPN site is enabled; otherwise, false (local IP must be assigned to an Edge's Uplink vNIC)

label - label of an IPSec VPN site

local_id* - ID of the local site

local_ip* - IP of the local site (local IP must be assigned to an Edge’s Uplink vNIC)

peer_id* - ID of a peer site (for certificate authentication must be a valid Distinguished Name)

peer_ip* - IP or FQDN of a peer site

ipsec_session_type - policybasedsession or routebasedsession. If routebasedsession is selected:
  • tunnel_interface_ip* - tunnel interface IP in CIDR notation
  • tunnel_interface_mtu* - MTU, allowed values 152 - 8916 (inclusively)

encryption_algorithm* - aes, aes256, aes-gsm, or 3des

enable_pfs* - true, if PFS is enabled; otherwise, false

dh_group* - dh2, dh5, dh14, dh15, or dh16

local_subnets* - an array of local subnets in CIDR format (If routebasedsession is set for ipsec_session_type, local_subnets value should be ["0.0.0.0/0"]) 

peer_subnets* - an array of peer subnets in CIDR format (If routebasedsession is set for ipsec_session_type, peer_subnets value should be ["0.0.0.0/0"]) 

authentication_mode* - psk or x.509 (for Certificate mode; available only if service_certificate for a service is set)

extension - securelocaltrafficbyip=IPAddress or passthroughSubnets=PeerSubnetIPAddress

digest_algorithm* - sha1 or sha-256

responder_only* - true, if IKE Responder Only option is enabled; otherwise, false

compliance_suite - none, cnsa, prime, suite-b-gcm-128, suite-b-gcm-256, suite-b-gmac-128, suite-b-gmac-256, or foundation

ike_option* - ikev1, ikev2, or ike-flex

certificate* - identifier of the certificate

4.10.5.2.4 Edit IPSec VPN Site

To edit an IPSec VPN site, use the following request:

PUT /nsx/edges/:edge_id/vpn/ipsec/service/sites/:site_id.xml

PUT /nsx/edges/:edge_id/vpn/ipsec/service/sites/:site_id.json
XML Request Example

```bash
<iike_option>ike-flex</ike_option><ipsec_session_type>routebasedsession</ipsec_session_type><label>Bravo</label><local_id>10.0.0.133</local_id><local_ip>10.0.0.133</local_ip><local_subnets><element>0.0.0.0/0</element></local_subnets><peer_id>C=Test, L=host</peer_id><peer_ip>123.32.4.32</peer_ip><peer_subnets><element>0.0.0.0/0</element></peer_subnets><responder_only>false</responder_only><tunnel_interface_ip_address>23.23.21.23/24</tunnel_interface_ip_address><tunnel_interface_mtu>1500</tunnel_interface_mtu></nsx_ipsec_site>'
```

JSON Request Example

```bash
curl -i -X PUT -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass --url http://onapp.test/nx/edges/13/vpn/ipsec/service/sites/3.json -d '{"nsx_ipsec_site": {"enabled": false, "label": "Bravo", "local_id": "10.0.0.133", "local_ip": "10.0.0.133", "peer_id": "C=Test, L=host", "peer_ip": "123.32.4.32", "ipsec_session_type": "routebasedsession", "encryption_algorithm": "aes-gcm", "enable_pfs": false, "dh_group": "dh5", "tunnel_interface_ip_address": "23.23.21.23/24", "tunnel_interface_mtu": 1500, "local_subnets": ["0.0.0.0/0"], "peer_subnets": ["0.0.0.0/0"], "authentication_mode": "x.509", "extension": ",", "digest_algorithm": "sha-256", "responder_only": false, "compliance_suite": "none", "ike_option": "ike-flex", "certificate": "certificate-45"}}'
```

Where:

- `enabled*` - true, if IPSec VPN site is enabled; otherwise, `false`
- `label` - label of the IPSec VPN site
- `identifier` - identifier of the IPSec VPN site
- `ipsec_service_id` - ID of the IPSec VPN service
- `local_id*` - ID of the local site
- `local_ip*` - IP of the local site (local IP must be assigned to an Edge's Uplink vNIC)
- `peer_id*` - ID of a peer site (for certificate authentication must be a valid Distinguished Name)
- `peer_ip*` - IP or FQDN of a peer site
- `ipsec_session_type` - `policybasedsession` or `routebasedsession`. If `routebasedsession` is selected:
  - `tunnel_interface_ip*` - tunnel interface IP in CIDR notation
  - `tunnel_interface_mtu*` - MTU, allowed values 152 - 8916 (inclusively)
- `encryption_algorithm*` - aes, aes256, aes-gsm, or 3des
- `enable_pfs*` - true, if PFS is enabled; otherwise, `false`
**dh_group** - dh2, dh5, dh14, dh15, or dh16

**local_subnets** - an array of local subnets in CIDR format (If routebasedsession is set for ipsec_session_type, local_subnets value should be ["0.0.0.0/0"])  

**peer_subnets** - an array of peer subnets in CIDR format (If routebasedsession is set for ipsec_session_type, peer_subnets value should be ["0.0.0.0/0"])  

**authentication_mode** - psk or x.509 (for Certificate mode; available only if service_certificate for a service is set)

**psk** - the value of the pre-shared key

**extension** - securelocaltrafficbyip=IPAddress or passthroughSubnets=PeerSubnetIPAddress

**digest_algorithm** - sha1 or sha-256

**responder_only** - true, if IKE Responder Only option is enabled; otherwise, false

**compliance_suite** - none, cnsa, prime, suite-b-gcm-128, suite-b-gcm-256, suite-b-gmac-128, suite-b-gmac-256, or foundation

**ike_option** - ikev1, ikev2, or ike-flex

**certificate_id** - identifier of the certificate

4.10.5.2.5 Delete IPSec VPN Site
To delete IPSec VPN site, use the following request:

DELETE /nsx/edges/:edge_id/vpn/ipsec/service/sites/:site_id.xml
DELETE /nsx/edges/:edge_id/vpn/ipsec/service/sites/:site_id.json

**XML Request Example**

curl -i -X DELETE -u user:userpass  

**JSON Request Example**

curl -i -X DELETE -u user:userpass  

Returns HTTP 204 response on successful deletion, or HTTP 404 when an IPSec VPN site with the ID specified is not found.

4.10.5.3 NSX Certificates API
Service certificates are required in case you select Certificate authentication option while configuring an IPSec VPN site for your vCloud edge gateway. This section contains the API requests you can use to manage NSX certificates and CRL certificates.

4.10.5.3.1 Get List of NSX Certificates
To get the list of NSX certificates imported from vCloud, use the following request:

GET /nsx/edges/:edge_id/certificates.xml
GET /nsx/edges/:edge_id/certificates.json

**XML Request Example**

JSON Request Example


XML Output Example

```xml
<nsx_certificates type="array">
  <nsx_certificate>
    <id type="integer">10</id>
    <identifier>certificate-54</identifier>
    <label>adfs.onappdev.lviv</label>
    <common_name>adfs.onappdev.lviv</common_name>
    <issuer_common_name>adfs.onappdev.lviv</issuer_common_name>
    <certificate_type>certificate_self_signed</certificate_type>
    <edge_id type="integer">3</edge_id>
    <valid_from type="dateTime">2018-05-07T08:08:43Z</valid_from>
    <not_after type="dateTime">2023-05-07T08:08:43Z</not_after>
    <created_at type="dateTime">2019-11-11T08:26:41Z</created_at>
    <updated_at type="dateTime">2019-11-11T08:26:41Z</updated_at>
    <signature_algorithm>SHA256WITHRSA</signature_algorithm>
    <public_key_algorithm>RSA</public_key_algorithm>
    <public_key_length type="integer">2048</public_key_length>
  </nsx_certificate>
  <nsx_certificate>
    <id type="integer">13</id>
    <identifier>certificate-51</identifier>
    <label>GlobalSign Domain Validation CA - SHA256 - G2</label>
    <common_name>GlobalSign Domain Validation CA - SHA256 - G2</common_name>
    <issuer_common_name>GlobalSign Root CA</issuer_common_name>
    <certificate_type>certificate_ca</certificate_type>
    <edge_id type="integer">3</edge_id>
    <valid_from type="dateTime">2014-02-20T10:00:00Z</valid_from>
    <not_after type="dateTime">2024-02-20T10:00:00Z</not_after>
    <created_at type="dateTime">2019-11-11T08:26:41Z</created_at>
    <updated_at type="dateTime">2019-11-11T08:26:41Z</updated_at>
    <signature_algorithm>SHA256WITHRSA</signature_algorithm>
    <public_key_algorithm>RSA</public_key_algorithm>
    <public_key_length type="integer">2048</public_key_length>
  </nsx_certificate>
</nsx_certificates>

Where:

id - the ID number of the certificate
identifier - the identifier of the certificate
label - the label of the certificate
common_name - the certificate's common name
issuer_common_name - common name of the certificate's issuer
certificate_type - certificate_ca, certificate_self_signed, or certificate_signed

232
edge_id - the ID of the edge the certificate is assigned to
valid_from - the date when the certificate started to be valid
not_after - final end-date, until the certificate is valid
created_at - the date when the certificate was created in the [YYYY][MM][DD][TH][hh][mm][ss]Z format
updated_at - the date when the certificate was updated in the [YYYY][MM][DD][TH][hh][mm][ss]Z format
signature_algorithm - the certificate's signature algorithm
public_key_algorithm - RSA or DSA
public_key_length - the key size in bits. The minimum is 2048 bits

4.10.5.3.2 Get List of CRL Certificates
To get the list of CRL certificates, use the following request:
GET /nsx/edges/:edge_id/crls.xml
GET /nsx/edges/:edge_id/crls.json

XML Request Example
```
```

JSON Request Example
```
```

XML Output Example
Where:

id - ID of the CRL certificate
label - label of the CRL certificate
identifier - identifier of the CRL certificate
issuer_common_name - common name of the issuer
define_id - ID of the corresponding edge
next_update - date of the next update scheduled in the [YYYY][MM][DD]T[hh][mm][ss]Z format
created_at - the date when the CRL certificate was created in the [YYYY][MM][DD]T[hh][mm][ss]Z format
updated_at - the date when the CRL certificate was updated in the [YYYY][MM][DD]T[hh][mm][ss]Z format

4.10.6 NSX L2 VPN API

This section provides the API calls you can use to manage NSX L2 VPN. With L2 VPN, you can stretch multiple logical networks (both VLAN and VXLAN) between different physical sites.

4.10.6.1 NSX L2 VPN Server

L2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries. Virtual servers remain on the same subnet when they are moved between sites and their IP addresses do not change. This section contains the API requests you can use to manage L2 VPN server:

- Edit NSX L2 VPN Server
- Get List of L2 VPN Peer Sites
- Get NSX L2 VPN Peer Site Details
- Add NSX L2 VPN Peer Site
- Edit NSX L2 VPN Peer Site
- Delete NSX L2 VPN Peer Site

4.10.6.1.1 Edit NSX L2 VPN Server
To edit L2 VPN server, use the following request:

PUT /nsx/edges/:edge_id/vpn/l2_vpn/service.xml
PUT /nsx/edges/:edge_id/vpn/l2_vpn/service.json

XML Request Example

curl -i -X PUT http://onapp.test/nsx/edges/126/vpn/l2_vpn/service.xml -H 'Accept: application/xml' -H 'Content-Type: application/xml' -d '<nsx_l2_vpn_service><certificate_auth_enabled>true</certificate_auth_enabled><enabled>false</enabled><encryption_algorithm type="array"><encryption_algorithm>ECDHE-RSA-AES128-GCM-SHA256</encryption_algorithm><encryption_algorithm>ECDHE-RSA-AES256-GCM-SHA384</encryption_algorithm></encryption_algorithm><l2_vpn_peer_sites type="array"><l2_vpn_peer_site><description>1</description><egress_optimization type="array"><egress_optimization>123.43.21.3</egress_optimization></egress_optimization><enabled>true</enabled><identifier>l2vpnpeersite-83</identifier><label>Alpha</label><sub_interfaces type="array"><sub_interface>10</sub_interface><sub_interface>11</sub_interface></sub_interfaces><user_id>newusername</user_id><user_password>%b5u`=8G[GK#vHe`</user_password></l2_vpn_peer_site></l2_vpn_peer_sites><listener_ip>10.0.0.133</listener_ip><listener_port>443</listener_port><mode>server</mode><service_certificate>certificate-46</service_certificate></nsx_l2_vpn_service>"

JSON Request Example


Where:

enabled* - true if L2 VPN service is enabled; otherwise, false
mode* - server
**listener_ip** - the primary or secondary IP address of an external interface of the NSX Edge

**listener_port** - the port number for the L2 VPN service

**encryption_algorithm** - ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, NULL-SHA256, AES128-GCM-SHA256, or NULL-MD5

**service_certificate** - the identifier of the service certificate

**certificate_auth_enabled** - **true** if the certificate to be bound to SSL VPN server is enabled; otherwise, **false**

**l2_vpn_peer_sites** - an array of L2 VPN peer sites added to this server with their details:

- **description** - the description of the peer site
- **egress_optimization** - the gateway IP addresses for which the traffic is to be locally routed or for which the traffic is to be blocked over the tunnel; array of IP addresses(["192.168.1.1", "192.168.1.2"]) or comma-separated string("192.168.1.1, 192.168.1.2")
- **enabled** - **true** if the newly added peer site is enabled; otherwise, **false**
- **identifier** - the identifier of the peer site
- **label** - the name of the peer site
- **routed_remote_subnets_enabled** - **true** if the sub interfaces to be stretched with the client are enabled; otherwise, **false**
- **sub_interfaces** - the indexes of the sub interfaces
- **user_id** - a user name with which the peer site is to be authenticated
- **user_password** - a password with which the peer site is to be authenticated

### 4.10.6.1.2 Get List of L2 VPN Peer Sites

To view the list of L2 VPN peer sites on your cloud, use the following request:

GET /nsx/edges/:edge_id/vpn/l2_vpn/service/peer_sites.xml
GET /nsx/edges/:edge_id/vpn/l2_vpn/service/peer_sites.json

**XML Request Example**

```bash
```

**JSON Request Example**

```bash
```

**XML Request Output**
<nsx_L2_VPN_Peer_Sites type="array">
  <nsx_L2_VPN_Peer_Site>
    <id type="integer">732</id>
    <label>Alpha</label>
    <identifier>l2vpnpeersite-83</identifier>
    <description>1</description>
    <egress_optimization type="array">
      <egress_optimization>123.43.21.3</egress_optimization>
    </egress_optimization>
  </nsx_L2_VPN_Peer_Site>
  ...
</nsx_L2VPN_Peer_Sites>

Where:

id - the ID of the peer site
label - the name of the peer site
identifier - identifier of the peer site
description - the description of a peer site
egress_optimization - the gateway IP addresses for which the traffic is to be locally routed or for which the traffic is to be blocked over the tunnel
enabled - true if the newly added peer site is enabled; otherwise, false
user_id - the ID of a user of a peer site
user_password - the password with which the peer site is to be authenticated
routed_remote_subnets_enabled - true if the sub interfaces to be stretched with the client are enabled; otherwise, false
l2_vpn_service_id - the ID of the VPN service attached
certificate_id - the ID of the CA certificate attached
created_at - the date when the peer site was created in the [YYYY][MM][DD][hh][mm][ss]Z format
updated_at - the date when the peer site was edited in the [YYYY][MM][DD][hh][mm][ss]Z format

4.10.6.1.3 Get NSX L2 VPN Peer Site Details
To get the details of a particular L2 VPN peer site, use the following request:
GET /nsx/edges/:edge_id/vpn/l2_vpn/service/peer_sites/:peer_site_id.xml
GET /nsx/edges/:edge_id/vpn/l2_vpn/service/peer_sites/:peer_site_id.js

XML Request Example

JSON Request Example


XML Output Example

```xml
<nsx_l2_vpn_peer_site>
  <id type="integer">732</id>
  <label>Alpha</label>
  <identifier>l2vpnpeersite-83</identifier>
  <description></description>
  <egress_optimization type="array">
    <egress_optimization>123.43.21.3</egress_optimization>
  </egress_optimization>
  <enabled type="boolean">true</enabled>
  <user_id>newusername</user_id>
  <user_password>%b5u`=8G[ GK#vHe</user_password>
  <routed_remote_subnets_enabled type="boolean">false</routed_remote_subnets_enabled>
  <l2_vpn_service_id type="integer">100</l2_vpn_service_id>
  <ca_certificate_id nil="true"/>
  <created_at type="dateTime">2019-11-06T13:01:10Z</created_at>
  <updated_at type="dateTime">2019-11-06T13:01:10Z</updated_at>
</nsx_l2_vpn_peer_site>
```

Where:

- **id** - the ID of the peer site
- **label** - the name of the peer site
- **identifier** - identifier of the peer site
- **description** - the description of a peer site
- **egress_optimization** - the gateway IP addresses for which the traffic is to be locally routed or for which the traffic is to be blocked over the tunnel
- **enabled** - true if the newly added peer site is enabled; otherwise, false
- **user_id** - the ID of a user of a peer site
- **user_password** - the password with which the peer site is to be authenticated
- **routed_remote_subnets_enabled** - true if the sub interfaces to be stretched with the client are enabled; otherwise, false
- **l2_vpn_service_id** - the ID of the VPN service attached
- **ca_certificate_id** - the ID of the CA certificate attached
- **created_at** - the date when the peer site was created in the [YYYY][MM][DD][hh][mm][ss]Z format
- **updated_at** - the date when the peer site was edited in the [YYYY][MM][DD][hh][mm][ss]Z format
4.10.6.1.4 Add NSX L2 VPN Peer Site
To create an L2 VPN peer site, use the following request:

POST /nsx/edges/:edge_id/vpn/12_vpn/service/peer_sites.xml
POST /nsx/edges/:edge_id/vpn/12_vpn/service/peer_sites.json

XML Request Example

curl -i -X POST
-H 'Content-Type: application/xml'
-d '<?xml version="1.0" encoding="UTF-8"?>
<nsx_l2_vpn_peer_site>
  <label>Alpha</label>
  <description>1</description>
  <egress_optimization>
    <ip_address>123.43.21.3</ip_address>
  </egress_optimization>
  <enabled>true</enabled>
  <l2_vpn_service_id>87</l2_vpn_service_id>
  <label>Alpha</label>
  <sub_interfaces>
    <sub_interface>10</sub_interface>
    <sub_interface>11</sub_interface>
  </sub_interfaces>
  <user_id>newusername</user_id>
  <user_password>%b5u`=8G[GK#vHe`
</nsx_l2_vpn_peer_site>'

JSON Request Example

curl -i -X POST
http://onapp.test/nsx/edges/113/vpn/l2_vpn/service/peer_sites.json -H 'Accept: application/json'
-H 'Content-Type: application/json'
-d '{"nsx_l2_vpn_peer_site":
  "label": "New rule",
  "description": "desc",
  "egress_optimization": ["123.43.21.3"],
  "enabled": true,
  "user_id": "someuser",
  "user_password": "%b5u`=8G[GK#vHe`
, "routed_remote_subnets_enabled": false,
  "sub_interfaces": ["10", "11"]}'

Where:

- **label** - the label of a new peer site
- **description** - description of the peer site
- **egress_optimization** - the gateway IP addresses for which the traffic is to be locally routed or for which the traffic is to be blocked over the tunnel; array of IP addresses(["192.168.1.1", "192.168.1.2"]) or comma-separated string("192.168.1.1, 192.168.1.2")
- **enabled** - true if the newly added peer site is enabled; otherwise, false
- **user_id** - the ID of a user with which the peer site is to be authenticated
- **user_password** - a password with which the peer site is to be authenticated
- **routed_remote_subnets_enabled** - true if the sub interfaces to be stretched with the client are enabled; otherwise, false
- **sub_interfaces** - the indexes of the sub interfaces

4.10.6.1.5 Edit NSX L2 VPN Peer Site
To edit L2 VPN peer service, use the following request:

PUT /nsx/edges/:edge_id/vpn/12_vpn/service/peer_sites/:peer_site_id.xml
PUT /nsx/edges/:edge_id/vpn/12_vpn/service/peer_sites/:peer_site_id.json

XML Request Example

```xml
<nsx_l2_vpn_peer_site>
  <label>Alpha</label>
  <description>1</description>
  <egress_optimization>
    <ip_address>123.43.21.3</ip_address>
  </egress_optimization>
  <enabled>true</enabled>
  <l2_vpn_service_id>87</l2_vpn_service_id>
  <label>Alpha</label>
  <sub_interfaces>
    <sub_interface>10</sub_interface>
    <sub_interface>11</sub_interface>
  </sub_interfaces>
  <user_id>newusername</user_id>
  <user_password>%b5u`=8G[GK#vHe`
</nsx_l2_vpn_peer_site>
```

JSON Request Example

```json
{"nsx_l2_vpn_peer_site":
  "label": "New rule",
  "description": "desc",
  "egress_optimization": ["123.43.21.3"],
  "enabled": true,
  "user_id": "someuser",
  "user_password": "%b5u`=8G[GK#vHe`
, "routed_remote_subnets_enabled": false,
  "sub_interfaces": ["10", "11"]}
```
curl -i -X PUT
http://onapp.test/edges/126/vpn/l2_vpn/service/peer_sites/732.xml -H 'Accept: application/json' -H 'Content-Type: application/xml' -d '<nsx_l2_vpn_peer_site><description>1</description><egress_optimization type="array"><egress_optimization>123.43.21.3</egress_optimization></egress_optimization><enabled>true</enabled><l2_vpn_service_id>87</l2_vpn_service_id><sub_interfaces_enabled><sub_interfaces type="array"><sub_interface>10</sub_interface><sub_interface>11</sub_interface></sub_interfaces><user_id>newusername</user_id><user_password>%b5u`=8G[ GK#vHe`</user_password></nsx_l2_vpn_peer_site>'

JSON Request Example

curl -i -X PUT
http://onapp.test/edges/113/vpn/l2_vpn/service/peer_sites/678.json -H 'Accept: application/json' -H 'Content-Type: application/json' -d '{"nsx_l2_vpn_peer_site": {"label":"Alpha","description": "1","egress_optimization": ["123.43.21.3"],"enabled": true,"user_id":"newusername","user_password":"%b5u`=8G[ GK#vHe`","routed_remote_subnets_enabled": false,"l2_vpn_service_id": 87,"sub_interfaces": ["10","11"]}}'

Where:

- **label** - the label of a new peer site
- **description** - description of the peer site
- **egress_optimization** - the gateway IP addresses for which the traffic is to be locally routed or for which the traffic is to be blocked over the tunnel; array of IP addresses(["192.168.1.1", "192.168.1.2"]) or comma-separated string("192.168.1.1, 192.168.1.2")
- **enabled** - true if the newly added peer site is enabled; otherwise, false
- **user_id** - the ID of a user with which the peer site is to be authenticated
- **user_password** - a password with which the peer site is to be authenticated
- **routed_remote_subnets_enabled** - true if the sub interfaces to be stretched with the client are enabled; otherwise, false
- **l2_vpn_service_id** - the ID of the VPN service associated
- **sub_interfaces** - the indexes of the sub interfaces

4.10.6.1.6 Delete NSX L2 VPN Peer Site

To delete an L2 VPN peer site, use the following request:

DELETE
/nsx/edges/:edge_id/vpn/l2_vpn/service/peer_sites/:peer_site_id.xml
DELETE
/nsx/edges/:edge_id/vpn/l2_vpn/service/peer_sites/:peer_site_id.json

XML Request Example

curl -i -X DELETE -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass --url
http://nsx/edges/113/vpn/l2_vpn/service/peer_sites/730.xml

JSON Request Example

Returns HTTP 204 response on successful deletion, or HTTP 404 when a peer site with the ID specified is not found.

4.10.6.2 NSX L2 VPN Client
In this section you can find the list of operations applicable for NSX managers:

- Get NSX L2 VPN Client Details
- Edit L2 VPN Client

4.10.6.2.1 Get NSX L2 VPN Client Details
To view the details of a particular L2 VPN client, use the following request:
GET /nsx/edges/:edge_id/vpn/l2_vpn/service.xml
GET /nsx/edges/:edge_id/vpn/l2_vpn/service.json

XML Request Example


JSON Request Example


XML Request Output
<nsx_l2_vpn_service>
   <id type="integer">102</id>
   <enabled type="boolean">false</enabled>
   <logging type="boolean">true</logging>
   <log_level>debug</log_level>
   <edge_id type="integer">128</edge_id>
   <routed_remote_subnets_enabled type="boolean">false</routed_remote_subnets_enabled>
   <mode>client</mode>
   <listener_ip nil="true"/>
   <listener_port nil="true"/>
   <server_address>123.3.23.3</server_address>
   <server_port type="integer">433</server_port>
   <service_certificate_id nil="true"/>
   <ca_certificate_id type="integer">217</ca_certificate_id>
   <encryption_algorithm type="array">
      <encryption_algorithm>AES128-GCM-SHA256</encryption_algorithm>
   </encryption_algorithm>
   <egress_optimization type="array">
      <egress_optimization>32.23.3.3</egress_optimization>
   </egress_optimization>
   <user_id>user</user_id>
   <user_password>@{5BChTJn`~3-f</user_password>
   <proxy_type>https</proxy_type>
   <proxy_address>123.3.33.4</proxy_address>
   <proxy_port type="integer">433</proxy_port>
   <proxy_user_name>user</proxy_user_name>
   <proxy_user_password nil="true"/>
   <created_at type="dateTime">2019-11-06T13:01:22Z</created_at>
   <updated_at type="dateTime">2019-11-06T13:01:22Z</updated_at>
   <locked type="boolean">false</locked>
</nsx_l2_vpn_service>

Where:

* id - the ID of the L2 VPN client
  * enabled - true if the L2 VPN service in enabled; otherwise, false
  * logging - true, if logging for this L2 VPN client is enabled; otherwise, false
  * log_level - emergency, alert, critical, error, warning, notice, info or debug
  * edge_id - the ID of the edge the L2 VPN client is associated with
  * routed_remote_subnets_enabled - true if the routed remote subnets are enabled; otherwise, false
  * mode - the mode of L2 VPN (server or client)
  * listener_ip - the primary or secondary IP address of an external interface of the NSX Edge
  * listener_port - the port number for the L2 VPN client
  * server_address - the address of the L2 VPN server to which this client is to be connected
  * server_port - the default port to which the L2 VPN client must connect to
  * service_certificate_id - the ID of the service certificate
  * ca_certificate_id - the ID of the CA certificate
  * encryption_algorithm - the encryption algorithm for communicating with the server
  * egress_optimization - the gateway IP address of the sub interfaces or the IP addresses to which traffic should not flow over the tunnel
  * user_id - a user name with which the server is to be authenticated
**user_password** - a password with which the peer site is to be authenticated

**proxy_type** - the type of traffic (TCP, HTTP, HTTPS or UDP)

**proxy_address** - the proxy server address

**proxy_port** - the proxy server port

**proxy_user_name** - a user name with which the proxy server is to be authenticated

**proxy_user_password** - a user password with which the proxy server is to be authenticated

**created_at** - the date when the L2 VPN client was created in the [YYYY][MM][DD]T[hh][mm][ss]Z format

**updated_at** - the date when the L2 VPN client was updated in the [YYYY][MM][DD]T[hh][mm][ss]Z format

**locked** - true if this L2 VPN client is locked; otherwise, false

4.10.6.2.2 Edit L2 VPN Client

To edit L2 VPN client, use the following request:

PUT /nsx/edges/:edge_id/vpn/l2_vpn/service.xml

PUT /nsx/edges/:edge_id/vpn/l2_vpn/service.json

**XML Request Example**

```
curl -i -X PUT http://onapp.test/nsx/edges/128/vpn/l2_vpn/service.xml -H 'Accept: application/xml' -H 'Content-Type: application/xml' -d <nsx_l2_vpn_service><ca_certificate>certificate-38</ca_certificate><certificate_auth_enabled>true</certificate_auth_enabled><egress_optimization type="array"><egress_optimization>32.23.3.3</egress_optimization></egress_optimization><enabled>true</enabled><encryption_algorithm type="array"><encryption_algorithm>AES128-GCM-SHA256</encryption_algorithm></encryption_algorithm><mode>client</mode><proxy_address>123.3.33.4</proxy_address><proxy_port>2722</proxy_port><proxy_user_name>user</proxy_user_name><proxy_user_password>%b5u`=8G\[GK#vHe`</proxy_user_password><secure_proxy_enabled>true</secure_proxy_enabled><server_address>123.3.23.3</server_address><server_port>433</server_port><sub_interfaces type="array"><sub_interface>10</sub_interface><sub_interface>11</sub_interface></sub_interfaces><user_id>user</user_id><user_password>%b5u`=8G\[GK#vHe`</user_password></nsx_l2_vpn_service>
```

**JSON Request Example**

```
url -i -X PUT http://onapp.test/nsx/edges/115/vpn/l2_vpn/service.json -H 'Accept: application/json' -H 'Content-Type: application/json' -d '{"nsx_l2_vpn_service":{"enabled":true,"mode":"client","server_address":"123.3.23.3","server_port":"433","encryption_algorithm":["AES128-GCM-SHA256"],"egress_optimization":["32.23.3.3"],"user_id":"user","user_password":"%b5u`=8G\[GK#vHe`","proxy_address":"123.3.33.4","proxy_port":"2722","proxy_user_name":"user","proxy_user_password":"%b5u`=8G\[GK#vHe`","ca_certificate":"certificate-38","sub_interfaces":["10","11"],"certificate_auth_enabled":true,"secure_proxy_enabled":true}}
```

**Where:**

enabled* - true if L2 VPN service is enabled; otherwise, false

mode* - client
**server_address** - the address of the L2 VPN server to which this client is to be connected

**server_port** - the default port to which the L2 VPN client must connect to

**encryption_algorithm** - the encryption algorithm for communicating with the server

**egress_optimization** - the gateway IP address of the sub interfaces or the IP addresses to which traffic should not flow over the tunnel

**user_id** - a user name with which the server is to be authenticated

**user_password** - a password with which the peer site is to be authenticated

**proxy_address** - the proxy server address; required if **secure_proxy_enabled** is true

**proxy_port** - the proxy server port; required if **secure_proxy_enabled** is true

**proxy_user_name** - a user name with which the proxy server is to be authenticated; required if **secure_proxy_enabled** is true

**proxy_user_password** - a user password with which the proxy server is to be authenticated; required if **secure_proxy_enabled** is true

**ca_certificate** - the identifier of the CA certificate for this client

**sub_interfaces** - the indexes of the sub interfaces

**certificate_auth_enabled** - true if certificate client authentication is enabled; otherwise, false

**secure_proxy_enabled** - true if only secure proxy connections are enabled; otherwise, false

### 4.11 vCenter Resource Pool API

This section provides the API calls you can use to manage vCenter Resource Pool.

#### 4.11.1 Get List of Resource Pools

To get the list of vCenter resource pools in your cloud, use the following request:

GET /vcenter/resource_pools.xml
GET /vcenter/resource_pools.json

**XML Request Example**

```
```

**JSON Request Example**

```
```

**XML Output Example**
<vcenter_resource_pools type="array">
<vcenter_resource_pool>
  <id type="integer">2</id>
  <label>RP1</label>
  <identifier>resgroup-2357</identifier>
  <cluster_id type="integer">1</cluster_id>
  <parent_id type="integer">1</parent_id>
  <user_id nil="true"/>
</vcenter_resource_pool>
<vcenter_resource_pool>
  <id type="integer">3</id>
  <label>RP2</label>
  <identifier>resgroup-2358</identifier>
  <cluster_id type="integer">1</cluster_id>
  <parent_id type="integer">1</parent_id>
  <user_id nil="true"/>
</vcenter_resource_pool>
<vcenter_resource_pool>
  <id type="integer">21</id>
  <label>RD-vcd-c.onappdev.com-resource-pool</label>
  <identifier>resgroup-11092</identifier>
  <cluster_id type="integer">4</cluster_id>
  <parent_id type="integer">17</parent_id>
  <user_id nil="true"/>
</vcenter_resource_pool>
</vcenter_resource_pools>

Where:

id - ID of the vCenter resource pool
label - the name of the vCenter resource pool
identifier - the resource pool identifier
cluster_id - ID of the cluster the resource pool is based in
parent_id - ID of the default resource pool
user_id - equal to nil if resource pool is imported into CP or equal to user_id if created by the user via CP

4.11.2 Add vCenter Resource Pool

To create a new resource pool, use the following request:

POST /vcenter/resource_pools.xml
POST /vcenter/resource_pools.json

XML Request Example


JSON Request Example

**XML Output Example**

```
<vcenter_resource_pool>
  <id type="integer">43</id>
  <label>new_resource_pool_via_api</label>
  <identifier>yfbbqriebulai</identifier>
  <cluster_id type="integer">4</cluster_id>
  <parent_id type="integer">17</parent_id>
  <user_id type="integer">1</user_id>
</vcenter_resource_pool>
```

Where:
- **id** - the resource pool ID
- **label** - the name of a new resource pool
- **identifier** - the resource pool identifier
- **cluster_id** - ID of the cluster the resource pool is based on
- **parent_id** - ID of the default resource pool
- **user_id** - user ID in Control Panel

### 4.11.3 Edit vCenter Resource Pool

To edit vCenter Resource Pool, use the following request:

**XML Request Example**

```
```

**JSON Request Example**

```
```

Where:
- **label** - the resource pool name
4.11.4 Delete vCenter Resource Pool

To delete a vCenter resource pool, use the following request:

```
DELETE /vcenter/resource_pools/:resource_pool_id.xml
DELETE /vcenter/resource_pools/:resource_pool_id.json
```

**XML Request Example**

```
curl -i -X DELETE -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -url 
http://onapp.test/vcenter/resource_pools/:resource_pool_id.xml
```

**JSON Request Example**

```
curl -i -X DELETE
```

Returns HTTP 204 response on successful deletion, or HTTP 404 when a vCenter resource pool with the ID specified is not found.

4.12 vCenter Servers API

This section contains requests for management of vCenter servers.

4.12.1 Get List of vCenter Servers

To get the list of vCenter servers in your cloud, use the following request:

```
GET /settings/vcenter_servers.xml
GET /settings/vcenter_servers.json
```

**XML Request Example**

```
curl -i -X GET -H 'Accept: application/xml' -H 'Content-type: application/xml' -u user:userpass -url 
http://onapp.test/settings/vcenter_servers.xml
```

**JSON Request Example**

```
curl -i -X GET -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -url 
http://onapp.test/settings/vcenter_servers.json
```

**XML Output Example**
Where:

- **id** - the ID of the vCenter server
- **label** - the label of the vCenter server
- **api_url** - the API URL of the vCenter server on the vCenter side
**login** - vCenter login

**online** - true, if the server is online; otherwise, false

**host** - the hostname of the vCenter server

**machine** - operation system type of vCenter server

**release** - the vCenter version

**instance_uuid** - universally unique identifier of an instance

**cpu_mhz** - cpu frequency

**cpus** - number of CPUs for this vCenter server

**threads_per_core** - threads per core

**cpu_cores** - number of CPU cores for this vCenter server

**total_mem** - the total amount of RAM for this vCenter server

**free_mem** - the amount of free RAM for this vCenter server

**public_key_hash** - hash of a public key

### 4.12.2 Add vCenter Server

To add a new vCenter server, use the following request:

```
POST /settings/vcenter_servers.xml
POST /settings/vcenter_servers.json
```

**XML Request Example**

```
```

**JSON Request Example**

```
curl -i -X POST -H 'Accept: application/json' -H 'Content-type: application/json' -u user:userpass -u url http://onapp.test/settings/vcenter_servers.json -d '{"vcenter_server": {"label": "vcenter_server_label", "api_url": "vc-b.onappdev.lviv", "login": "administrator@vsphere.local", "password": "vsphere_pass"}}'
```

**Where:**

- **label** - the label of the vCenter server
- **api_url** - the API URL of the vCenter server on the vCenter side
- **login** - your vCenter login
- **password** - your vCenter password

### 4.12.3 Edit vCenter Server

To edit a vCenter server, use the following request:

```
PUT /settings/vcenter_servers/:vcenter_server_id.xml
PUT /settings/vcenter_servers/:vcenter_server_id.json
```

**XML Request Example**

```
```
### JSON Request Example

```bash
```

Where:
- **label** - the label of the vCenter server
- **login** - your vCenter login
- **password** - your vCenter password

### 4.12.4 Delete vCenter Server

To remove a vCenter server, use the following request:

**DELETE** /settings/vcenter_servers/:vcenter_server_id.xml
**DELETE** /settings/vcenter_servers/:vcenter_server_id.json

### XML Request Example

```bash
```

### JSON Request Example

```bash
```

Returns HTTP 204 response on successful deletion, or HTTP 404 when a vCenter server with the ID specified is not found.