<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Users &amp; Groups Overview</td>
<td>115</td>
</tr>
<tr>
<td>6.2 Managing Users</td>
<td>116</td>
</tr>
<tr>
<td>6.3 Managing Groups</td>
<td>122</td>
</tr>
<tr>
<td>6.4 Managing VDCs</td>
<td>127</td>
</tr>
<tr>
<td>6.5 Managing Permissions</td>
<td>130</td>
</tr>
<tr>
<td>6.6 Accounting Client</td>
<td>133</td>
</tr>
<tr>
<td>6.7 Showback</td>
<td>139</td>
</tr>
<tr>
<td>6.8 Managing ACL Rules</td>
<td>143</td>
</tr>
<tr>
<td>6.9 Managing Quotas</td>
<td>148</td>
</tr>
<tr>
<td>7 Authentication</td>
<td>155</td>
</tr>
<tr>
<td>7.1 Authentication Overview</td>
<td>155</td>
</tr>
<tr>
<td>7.2 SSH Auth</td>
<td>156</td>
</tr>
<tr>
<td>7.3 x509 Authentication</td>
<td>157</td>
</tr>
<tr>
<td>7.4 LDAP Authentication</td>
<td>160</td>
</tr>
<tr>
<td>8 Sunstone GUI</td>
<td>165</td>
</tr>
<tr>
<td>8.1 OpenNebula Sunstone: The Cloud Operations Center</td>
<td>165</td>
</tr>
<tr>
<td>8.2 Sunstone Views</td>
<td>171</td>
</tr>
<tr>
<td>8.3 Self-service Cloud View</td>
<td>182</td>
</tr>
<tr>
<td>8.4 Group Admin View</td>
<td>204</td>
</tr>
<tr>
<td>8.5 User Security and Authentication</td>
<td>215</td>
</tr>
<tr>
<td>8.6 Cloud Servers Authentication</td>
<td>219</td>
</tr>
<tr>
<td>9 Other Subsystems</td>
<td>223</td>
</tr>
<tr>
<td>9.1 MySQL Backend</td>
<td>223</td>
</tr>
<tr>
<td>10 References</td>
<td>225</td>
</tr>
<tr>
<td>10.1 ONED Configuration</td>
<td>225</td>
</tr>
<tr>
<td>10.2 Scheduler</td>
<td>236</td>
</tr>
<tr>
<td>10.3 Logging &amp; Debugging</td>
<td>240</td>
</tr>
<tr>
<td>10.4 Onedb Tool</td>
<td>243</td>
</tr>
</tbody>
</table>
1.1 Hosts & Clusters Overview

A **Host** is a server that has the ability to run Virtual Machines and that is connected to OpenNebula’s Frontend server. OpenNebula can work with Hosts with a heterogeneous configuration, i.e. you can connect Hosts to the same OpenNebula with different hypervisors or Linux distributions as long as these requirements are fulfilled:

- Every Host need to have a **oneadmin** account.
- OpenNebula’s Frontend and all the Hosts need to be able to resolve, either by DNS or by /etc/hosts the names of all the other Hosts and Frontend.
- The **oneadmin** account in any Host or the Frontend should be able to ssh passwordlessly to any other Host or Frontend. This is achieved either by sharing the $HOME of oneadmin accross all the servers with NFS or by manually copying the ~/.ssh directory.
- It needs to have a hypervisor supported by OpenNebula installed and properly configured. The correct way to achieve this is to follow the specific guide for each hypervisor.
- **ruby** >= 1.8.7
- OpenNebula node packages installed. For CentOS/RHEL these are opennebula-node-kvm or opennebula-common for kvm or xen. For Debian based distros install opennebula-node.

**Clusters** are pools of hosts that share datastores and virtual networks. Clusters are used for load balancing, high availability, and high performance computing.

1.1.1 Overview of Components

There are three components regarding Hosts:

- **Host Management**: Host management is achieved through the onehost CLI command or through the Sunstone GUI. You can read about Host Management in more detail in the Managing Hosts guide.

- **Host Monitorization**: In order to keep track of the available resources in the Hosts, OpenNebula launches a Host Monitoring driver, called IM (Information Driver), which gathers all the required information and submits it to the Core. The default IM driver executes ssh commands in the host, but other mechanism are possible. There is further information on this topic in the Monitoring Subsystem guide.

- **Cluster Management**: Hosts can be grouped in Clusters. These Clusters are managed with the onecluster CLI command, or through the Sunstone GUI. You can read about Cluster Management in more detail in the Managing Clusters guide.
1.2 Managing Hosts

In order to use your existing physical nodes, you have to add them to the system as OpenNebula hosts. You need the following information:

- **Hostname** of the host or IP
- **Information Driver** to be used to monitor the host, e.g. `kvm`. These should match the Virtualization Drivers installed and more info about them can be found at the Virtualization Subsystem guide.
- **Virtualization Driver** to boot, stop, resume or migrate VMs in the host, e.g. `kvm`. Information about these drivers can be found in its guide.
- **Networking Driver** to isolate virtual networks and apply firewalling rules, e.g. `802.1Q`. Information about these drivers can be found in its guide.
- **Cluster** where to place this host. The Cluster assignment is optional, you can read more about it in the Managing Clusters guide.

**Warning:** Before adding a host check that you can ssh to it without being prompt for a password

1.2.1 onehost Command

The following sections show the basics of the `onehost` command with simple usage examples. A complete reference for these commands can be found here.

This command enables Host management. Actions offered are:

- **create**: Creates a new Host
- **delete**: Deletes the given Host
- **enable**: Enables the given Host
- **disable**: Disables the given Host
- **update**: Update the template contents.
- **sync**: Synchronizes probes in all the hosts.
- **list**: Lists Hosts in the pool
- **show**: Shows information for the given Host
- **top**: Lists Hosts continuously
- **flush**: Disables the host and reschedules all the running VMs it.

Create and Delete

Hosts, also known as physical nodes, are the servers managed by OpenNebula responsible for Virtual Machine execution. To use these hosts in OpenNebula you need to register them so they are monitored and well-known to the scheduler.

Creating a host:

```
$ onehost create host01 --im dummy --vm dummy --net dummy
ID: 0
```

The parameters are:
• **--im/-i**: Information Manager driver. Valid options: kvm, xen, vmware, ec2, ganglia, dummy.

• **--vm/-v**: Virtual Machine Manager driver. Valid options: kvm, xen, vmware, ec2, dummy.

• **--net/-n**: Network manager driver. Valid options: 802.1Q, dummy, ebtables, fw, ovswitch, vmware.

To remove a host, just like with other OpenNebula commands, you can either specify it by ID or by name. The following commands are equivalent:

```bash
$ onehost delete host01
$ onehost delete 0
```

### Show, List and Top

To display information about a single host the **show** command is used:

```bash
$ onehost show 0
HOST 0 INFORMATION
    ID : 0
    NAME : host01
    CLUSTER : -
    STATE : MONITORED
    IM_MAD : dummy
    VM_MAD : dummy
    VN_MAD : dummy
    LAST MONITORING TIME : 07/06 17:40:41

HOST SHARES
    TOTAL MEM : 16G
    USED MEM (REAL) : 857.9M
    USED MEM (ALLOCATED) : 0K
    TOTAL CPU : 800
    USED CPU (REAL) : 299
    USED CPU (ALLOCATED) : 0
    RUNNING VMS : 0

MONITORING INFORMATION
    CPUSPEED="2.2GHz"
    FREECPU="501"
    FREEMEMORY="15898723"
    HOSTNAME="host01"
    HYPERVISOR="dummy"
    TOTALCPU="800"
    TOTALMEMORY="16777216"
    USEDCPU="299"
    USEDMEMORY="878493"

We can instead display this information in XML format with the **-x** parameter:

```bash
$ onehost show -x 0
<HOST>
  <ID>0</ID>
  <NAME>host01</NAME>
  <STATE>2</STATE>
  <IM_MAD>dummy</IM_MAD>
  <VM_MAD>dummy</VM_MAD>
  <VN_MAD>dummy</VN_MAD>
  <LAST_MON_TIME>1341589306</LAST_MON_TIME>
  <CLUSTER_ID>-1</CLUSTER_ID>
</HOST>
```

1.2. Managing Hosts
To see a list of all the hosts:

```
$ onehost list
```

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>RVM</th>
<th>TCPU</th>
<th>FCPU</th>
<th>ACPU</th>
<th>TMEM</th>
<th>FMEM</th>
<th>AMEM</th>
<th>STAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>host01</td>
<td>-</td>
<td>0</td>
<td>800</td>
<td>198</td>
<td>800</td>
<td>16G</td>
<td>10.9G</td>
<td>16G</td>
<td>on</td>
</tr>
<tr>
<td>1</td>
<td>host02</td>
<td>-</td>
<td>0</td>
<td>800</td>
<td>677</td>
<td>800</td>
<td>16G</td>
<td>3.7G</td>
<td>16G</td>
<td>on</td>
</tr>
</tbody>
</table>

It can also be displayed in XML format using `-x`:

```
$ onehost list -x
```

```
<HOST_POOL>

<HOST>

  ...

</HOST>

...</HOST_POOL>
```

The `top` command is similar to the `list` command, except that the output is refreshed until the user presses `CTRL-C`.

### Enable, Disable and Flush

The `disable` command disables a host, which means that no further monitorization is performed on this host and no Virtual Machines are deployed in it. It won’t however affect the running VMs in the host.

```
$ onehost disable 0
```

To re-enable the host use the `enable` command:

```
$ onehost enable 0
```
$ onehost enable 0

The `flush` command will mark all the running VMs in the specified host as to be rescheduled, which means that they will be migrated to another server with enough capacity. At the same time, the specified host will be disabled, so no more Virtual Machines are deployed in it. This command is useful to clean a host of running VMs.

$ onehost flush host02

$ onehost list

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>RVM</th>
<th>TCPU</th>
<th>FCPU</th>
<th>ACPU</th>
<th>TMEM</th>
<th>FMEM</th>
<th>AMEM</th>
<th>STAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>host01</td>
<td>-</td>
<td>3</td>
<td>800</td>
<td>96</td>
<td>500</td>
<td>16G</td>
<td>11.1G</td>
<td>14.5G</td>
<td>on</td>
</tr>
<tr>
<td>1</td>
<td>host02</td>
<td>-</td>
<td>0</td>
<td>800</td>
<td>640</td>
<td>800</td>
<td>16G</td>
<td>8.5G</td>
<td>16G</td>
<td>on</td>
</tr>
<tr>
<td>2</td>
<td>host03</td>
<td>-</td>
<td>3</td>
<td>800</td>
<td>721</td>
<td>500</td>
<td>16G</td>
<td>8.6G</td>
<td>14.5G</td>
<td>on</td>
</tr>
</tbody>
</table>

$ onevm list

<table>
<thead>
<tr>
<th>ID</th>
<th>USER</th>
<th>GROUP</th>
<th>NAME</th>
<th>STAT</th>
<th>UCPU</th>
<th>UMEM</th>
<th>HOST</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>vm01</td>
<td>runn</td>
<td>54</td>
<td>102.4M</td>
<td>host03</td>
<td>0d 00h01</td>
</tr>
<tr>
<td>1</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>vm02</td>
<td>runn</td>
<td>91</td>
<td>276.5M</td>
<td>host02</td>
<td>0d 00h01</td>
</tr>
<tr>
<td>2</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>vm03</td>
<td>runn</td>
<td>13</td>
<td>174.1M</td>
<td>host01</td>
<td>0d 00h01</td>
</tr>
<tr>
<td>3</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>vm04</td>
<td>runn</td>
<td>72</td>
<td>204.8M</td>
<td>host03</td>
<td>0d 00h00</td>
</tr>
<tr>
<td>4</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>vm05</td>
<td>runn</td>
<td>49</td>
<td>112.6M</td>
<td>host02</td>
<td>0d 00h00</td>
</tr>
<tr>
<td>5</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>vm06</td>
<td>runn</td>
<td>87</td>
<td>414.7M</td>
<td>host01</td>
<td>0d 00h00</td>
</tr>
</tbody>
</table>

Update

It’s sometimes useful to store information in the host’s template. To do so, the `update` command is used.

An example use case is to add the following line to the host’s template:

```
TYPE="production"
```

Which can be used at a later time for scheduling purposes by adding the following section in a VM template:

```
SCHED_REQUIREMENTS="TYPE="production"
```

That will restrict the Virtual Machine to be deployed in `TYPE=production` hosts.

The host drivers can be also changed with the host template attributes `_MAD`. Please note that this change will only apply to new deployments. If the `im_mad` is changed, make sure to run the `onehost sync` command explained below.

```
IM_MAD="kvm"
VM_MAD="kvm"
VN_MAD="dummy"
```
Sync

When OpenNebula monitors a host, it copies a certain amount of files to /var/tmp/one. When the administrator changes these files, they can be copied again to the hosts with the sync command. When executed this command will copy the probes to the nodes and will return the prompt after it has finished telling which nodes it could not update.

To keep track of the probes version there’s a new file in /var/lib/one/remotes/VERSION. By default this holds the OpenNebula version (ex. ‘4.4.0’). This version can be seen in he hosts with a onehost show <host>:

```
$ onehost show 0
HOST 0 INFORMATION
ID: 0
[...]
MONITORING INFORMATION
VERSION="4.4.0"
[...]
```

The command onehost sync only updates the hosts with VERSION lower than the one in the file /var/lib/one/remotes/VERSION. In case you modify the probes this VERSION file should be modified with a greater value, for example 4.4.0.01.

In case you want to force upgrade, that is, no VERSION checking you can do that adding --force option:

```
$ onehost sync --force
```

You can also select which hosts you want to upgrade naming them or selecting a cluster:

```
$ onehost sync host01,host02,host03
$ onehost sync -c myCluster
```

onehost sync command can alternatively use rsync as the method of upgrade. To do this you need to have installed rsync command in the frontend and the nodes. This method is faster that the standard one and also has the benefit of deleting remote files no longer existing in the frontend. To use it add the parameter --rsync:

```
$ onehost sync --rsync
```

1.2.2 Host Information

Hosts include the following monitoring information. You can use this variables to create custom RANK and REQUIREMENTS expressions for scheduling. Note also that you can manually add any tag and use it also for RANK and REQUIREMENTS
<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HYPERVISOR</td>
<td>Name of the hypervisor of the host, useful for selecting the hosts with an specific technology.</td>
</tr>
<tr>
<td>ARCH</td>
<td>Architecture of the host CPUs, e.g. x86_64.</td>
</tr>
<tr>
<td>MODEL-NAME</td>
<td>Model name of the host CPU, e.g. Intel(R) Core(TM) i7-2620M CPU @ 2.70GHz.</td>
</tr>
<tr>
<td>CPUSPEED</td>
<td>Speed in Mhz of the CPUs.</td>
</tr>
<tr>
<td>HOSTNAME</td>
<td>As returned by the hostname command.</td>
</tr>
<tr>
<td>VERSION</td>
<td>This is the version of the monitoring probes. Used to control local changes and the update process</td>
</tr>
<tr>
<td>MAX_CPU</td>
<td>Number of CPUs multiplied by 100. For example, a 16 cores machine will have a value of 1600. The value of RESERVED_CPU will be substracted from the information reported by the monitoring system. This value is displayed as TOTAL CPU by the onehost show command under HOST SHARE section.</td>
</tr>
<tr>
<td>MAX_MEM</td>
<td>Maximum memory that could be used for VMs. It is advised to take out the memory used by the hypervisor using RESERVED_MEM. This values is substracted from the memory amount reported. This value is displayed as TOTAL MEM by the onehost show command under HOST SHARE section.</td>
</tr>
<tr>
<td>MAX_DISK</td>
<td>Total space in megabytes in the DATASTORE LOCATION.</td>
</tr>
<tr>
<td>USED_CPU</td>
<td>Percentage of used CPU multiplied by the number of cores. This value is displayed as USED CPU (REAL) by the onehost show command under HOST SHARE section.</td>
</tr>
<tr>
<td>USED_MEM</td>
<td>Memory used, in kilobytes. This value is displayed as USED MEM (REAL) by the onehost show command under HOST SHARE section.</td>
</tr>
<tr>
<td>USED_DISK</td>
<td>Used space in megabytes in the DATASTORE LOCATION.</td>
</tr>
<tr>
<td>FREE_CPU</td>
<td>Percentage of idling CPU multiplied by the number of cores. For example, if 50% of the CPU is idling in a 4 core machine the value will be 200.</td>
</tr>
<tr>
<td>FREE_MEM</td>
<td>Available memory for VMs at that moment, in kilobytes.</td>
</tr>
<tr>
<td>FREE_DISK</td>
<td>Free space in megabytes in the DATASTORE LOCATION.</td>
</tr>
<tr>
<td>CPU_USAGE</td>
<td>Total CPU allocated to VMs running on the host as requested in CPU in each VM template. This value is displayed as USED CPU (ALLOCATED) by the onehost show command under HOST SHARE section.</td>
</tr>
<tr>
<td>MEM_USAGE</td>
<td>Total MEM allocated to VMs running on the host as requested in MEMORY in each VM template. This value is displayed as USED MEM (ALLOCATED) by the onehost show command under HOST SHARE section.</td>
</tr>
<tr>
<td>DISK_USAGE</td>
<td>Total size allocated to disk images of VMs running on the host computed using the SIZE attribute of each image and considering the datastore characteristics.</td>
</tr>
<tr>
<td>NETRX</td>
<td>Received bytes from the network.</td>
</tr>
<tr>
<td>NETTX</td>
<td>Transferred bytes to the network.</td>
</tr>
<tr>
<td>WILD</td>
<td>Comma separated list of VMs running in the host that were not launched and are not currently controlled by OpenNebula</td>
</tr>
<tr>
<td>ZOMBIES</td>
<td>Comma separated list of VMs running in the host that were launched by OpenNebula but are not currently controlled by it.</td>
</tr>
</tbody>
</table>
1.2.3 Host Life-cycle

<table>
<thead>
<tr>
<th>Short state</th>
<th>State</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>init</td>
<td>INIT</td>
<td>Initial state for enabled hosts.</td>
</tr>
<tr>
<td>update</td>
<td>MONITORING_MONITORED</td>
<td>Monitoring a healthy Host.</td>
</tr>
<tr>
<td>on</td>
<td>MONITORED</td>
<td>The host has been successfully monitored.</td>
</tr>
<tr>
<td>err</td>
<td>ERROR</td>
<td>An error occurred while monitoring the host. See the Host information with onehost show for an error message.</td>
</tr>
<tr>
<td>off</td>
<td>DISABLED</td>
<td>The host is disabled, and won’t be monitored. The scheduler ignores Hosts in this state.</td>
</tr>
<tr>
<td>retry</td>
<td>MONITORING_ERROR</td>
<td>Monitoring a host in error state.</td>
</tr>
</tbody>
</table>

1.2.4 Scheduler Policies

You can define global Scheduler Policies for all VMs in the sched.conf file, follow the Scheduler Guide for more information. Additionally, users can require their virtual machines to be deployed in a host that meets certain constrains. These constrains can be defined using any attribute reported by onehost show, like the architecture (ARCH).

The attributes and values for a host are inserted by the monitoring probes that run from time to time on the nodes to get information. The administrator can add custom attributes either creating a probe in the host, or updating the host information with: onehost update <HOST_ID>. Calling this command will fire up an editor (the one specified in the EDITOR environment variable) and you will be able to add, delete or modify some of those values.

```bash
$ onehost show 3
[...
MONITORING INFORMATION
CPUSPEED=2.2GHz
FREECPU=800
FREEMEMORY=16777216
HOSTNAME=ursa06
HYPERVISOR=dummy
TOTALCPU=800
TOTALMEMORY=16777216
USEDCPU=0
USEDMEMORY=0

$ onehost update 3

[in editor, add CUSTOM_ATTRIBUTE=VALUE]

$onehost show 3
[...
MONITORING INFORMATION
CPUSPEED=2.2GHz
FREECPU=800
FREEMEMORY=16777216
HOSTNAME=ursa06
HYPERVISOR=dummy
TOTALCPU=800
TOTALMEMORY=16777216
USEDCPU=0
USEDMEMORY=0
CUSTOM_ATTRIBUTE=VALUE
```

This feature is useful when we want to separate a series of hosts or marking some special features of different hosts.
These values can then be used for scheduling the same as the ones added by the monitoring probes, as a placement requirement:

```
SCHED_REQUIREMENTS = "CUSTOM_ATTRIBUTE = "SOME_VALUE"
```

### 1.2.5 A Sample Session

Hosts can be added to the system anytime with the `onehost` command. You can add the hosts to be used by OpenNebula like this:

```
$ onehost create host01 --im kvm --vm kvm --net dummy
$ onehost create host02 --im kvm --vm kvm --net dummy
```

The status of the hosts can be checked with the `onehost list` command:

```
$ onehost list

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>RVM</th>
<th>TCPU</th>
<th>FCPU</th>
<th>ACPU</th>
<th>TMEM</th>
<th>FMEM</th>
<th>AMEM</th>
<th>STAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>host01</td>
<td>-</td>
<td>7</td>
<td>400</td>
<td>290</td>
<td>400</td>
<td>3.7G</td>
<td>2.2G</td>
<td>3.7G</td>
<td>on</td>
</tr>
<tr>
<td>1</td>
<td>host02</td>
<td>-</td>
<td>2</td>
<td>400</td>
<td>294</td>
<td>400</td>
<td>3.7G</td>
<td>2.2G</td>
<td>3.7G</td>
<td>on</td>
</tr>
<tr>
<td>2</td>
<td>host03</td>
<td>-</td>
<td>0</td>
<td>400</td>
<td>312</td>
<td>400</td>
<td>3.7G</td>
<td>2.2G</td>
<td>3.7G</td>
<td>off</td>
</tr>
</tbody>
</table>
```

And specific information about a host with `show`:

```
$ onehost show host01

HOST 0 INFORMATION

ID : 0
NAME : host01
CLUSTER : -
STATE : MONITORED
IM_MAD : kvm
VM_MAD : kvm
VN_MAD : dummy
LAST MONITORING TIME : 1332756227

HOST SHARES
MAX MEM : 3921416
USED MEM (REAL) : 1596540
USED MEM (ALLOCATED) : 0
MAX CPU : 400
USED CPU (REAL) : 74
USED CPU (ALLOCATED) : 0
RUNNING VMS : 7

MONITORING INFORMATION
ARCH=x86_64
CPUSPEED=2393
FREECPU=326.0
FREEMEMORY=2324876
HOSTNAME=rama
HYPERVERSOR=kvm
MODELNAME="Intel(R) Core(TM) i5 CPU M 450 @ 2.40GHz"
NETRX=0
NETTX=0
TOTALCPU=400
TOTALMEMORY=3921416
USEDCPU=74.0
USEDMEMORY=1596540
```
If you want not to use a given host you can temporarily disable it:

\$ onehost disable host01

A disabled host should be listed with \texttt{STAT off} by \texttt{onehost list}. You can also remove a host permanently with:

\$ onehost delete host01

\textbf{Warning:} Detailed information of the \texttt{onehost} utility can be found in the Command Line Reference

### 1.2.6 Importing Wild VMs

The monitoring mechanism in OpenNebula reports all VMs found in a hypervisor, even those not launched through OpenNebula. These VMs are referred to as Wild VMs, and can be imported to be managed through OpenNebula. This includes all supported hypervisors, even the hybrid ones.

The Wild VMs can be spotted through the \texttt{onehost show} command:

\$ onehost show 3

\begin{verbatim}
HOST 3 INFORMATION
ID : 3
NAME : MyvCenterHost
CLUSTER : -
STATE : MONITORED
[...]
WILD VIRTUAL MACHINES

NAME IMPORT_ID CPU MEMORY
Ubuntu14.04VM 4223f951-243a-b31a-018f-390a02ff5c96 1 2048
CentOS7 422375e7-7fc7-4ed1-e0f0-fb778fe66e60 1 2048
\end{verbatim}

And imported through the \texttt{onehost importvm} command:

\$ onehost importvm 0 CentOS7
\$ onevm list

\begin{verbatim}
ID USER GROUP NAME STAT UCPU UMEM HOST TIME
3 oneadmin oneadmin CentOS7 runn 0 590M MyvCenterHost 0d 01h02
\end{verbatim}

After a Virtual Machine is imported, their lifecycle (including creation of snapshots) can be controlled through OpenNebula. The following operations \textbf{cannot} be performed on an imported VM:

- Delete –recreate
- Undeploy (and Undeploy –hard)
- Migrate (and Migrate –live)
- Stop

\textbf{Note:} For kvm and xen hosts the poweroff action will leave VMs in a state that cannot be resumed through OpenNebula. Those VMs need to be resumed manually with the same method they were created in the first place.

The same import mechanism is available graphically through Sunstone. Running and Powered Off VMs can be imported through the WILDS tab in the Host info tab.
1.2.7 Using Sunstone to Manage Hosts

You can also manage your hosts using Sunstone. Select the Host tab, and there, you will be able to create, enable, disable, delete and see information about your hosts in a user friendly way.

1.3 Managing Clusters

A Cluster is a group of Hosts. Clusters can have associated Datastores and Virtual Networks, this is how the administrator sets which Hosts have the underlying requirements for each Datastore and Virtual Network configured.

1.3.1 Cluster Management

Clusters are managed with the “onecluster” command. To create new Clusters, use onecluster create <name>. Existing Clusters can be inspected with the onecluster list and show commands.
$ onecluster create production
ID: 100

$ onecluster list

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>HOSTS</th>
<th>NETS</th>
<th>DATASTORES</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>production</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

$ onecluster show production
CLUSTER 100 INFORMATION
ID : 100
NAME : production

HOSTS

VNETS

DATASTORES

Add Hosts to Clusters

Hosts can be created directly in a Cluster, using the \(-cluster\) option of onehost create, or be added at any moment using the command onecluster addhost. Hosts can be in only one Cluster at a time.

To delete a Host from a Cluster, the command onecluster delhost must be used. When a Host is removed from a Cluster, it is seen as part of the Cluster ‘none’, more about this below.

In the following example, we will add Host 0 to the Cluster we created before. You will notice that the onecluster show command will list the Host ID 0 as part of the Cluster.

$ onehost list

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>RVM</th>
<th>TCPU</th>
<th>FCPUS</th>
<th>ACPU</th>
<th>TMEM</th>
<th>FMEM</th>
<th>AMEM</th>
<th>STAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>host01</td>
<td>-</td>
<td>7</td>
<td>400</td>
<td>290</td>
<td>400</td>
<td>3.7G</td>
<td>2.2G</td>
<td>3.7G</td>
<td>on</td>
</tr>
</tbody>
</table>

$ onecluster addhost production host01

$ onehost list

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>RVM</th>
<th>TCPU</th>
<th>FCPUS</th>
<th>ACPU</th>
<th>TMEM</th>
<th>FMEM</th>
<th>AMEM</th>
<th>STAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>host01</td>
<td>production</td>
<td>7</td>
<td>400</td>
<td>290</td>
<td>400</td>
<td>3.7G</td>
<td>2.2G</td>
<td>3.7G</td>
<td>on</td>
</tr>
</tbody>
</table>

$ onecluster show production
CLUSTER 100 INFORMATION
ID : 100
NAME : production

HOSTS
0

VNETS

DATASTORES

Add Resources to Clusters

Datastores and Virtual Networks can be added to one Cluster. This means that any Host in that Cluster is properly configured to run VMs using Images from the Datastores, or is using leases from the Virtual Networks.
For instance, if you have several Hosts configured to use Open vSwitch networks, you would group them in the same Cluster. The Scheduler will know that VMs using these resources can be deployed in any of the Hosts of the Cluster. These operations can be done with the `onecluster addvnet/delvnet` and `adddatastore/deldatastore`:

```
$ onecluster addvnet production priv-ovswitch

$ onecluster adddatastore production iscsi
```

```
$ onecluster list
  ID  NAME    HOSTS  NETS  DATASTORES
  100 production 1 1 1

$ onecluster show 100
CLUSTER 100 INFORMATION
  ID : 100
  NAME : production

CLUSTER TEMPLATE

  HOSTS
  0

  VNETS
  1

  DATASTORES
  100
```

The System Datastore for a Cluster

You can associate an specific System DS to a cluster to improve its performance (e.g. balance VM I/O between different servers) or to use different system DS types (e.g. shared and ssh).

To use a specific System DS with your cluster, instead of the default one, just create it (with TYPE=SYSTEM_DS in its template), and associate it just like any other datastore (onecluster adddatastore). Check the System DS guide for more information.

Cluster Properties

Each cluster includes a generic template where cluster configuration properties or attributes can be defined. The following list of attributes are recognized by OpenNebula:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATASTORE_LOCATION</td>
<td><em>Default</em> path for datastores in the cluster hosts. It is the same for all the hosts in the cluster. Note that DATASTORE_LOCATION is only for the cluster hosts and not for the front-end. It defaults to /var/lib/one/datastores</td>
</tr>
</tbody>
</table>

You can easily update these values with the `onecluster` command:

```
$ onecluster update production
-----8<------ editor session ----8<------
DATASTORE_LOCATION="/mnt/nas/datastores"
```

1.3. Managing Clusters
$ oneluster show production
CLUSTER 100 INFORMATION
ID : 100
NAME : production
SYSTEM DATASTORE : 100

CLUSTER TEMPLATE
DATASTORE_LOCATION="/mnt/nas/datastores"

HOSTS
0

VNETS
1

DATASTORES
100

You can add as many variables as you want, following the standard template syntax. These variables will be used for now only for informational purposes.

### 1.3.2 The Default Cluster ‘None’

Hosts, Datastores and Virtual Networks can be grouped into clusters, but this is optional. By default, these resources are created outside of any Cluster, what can be seen as a special Cluster named ‘none’ in Sunstone. In the CLI, this Cluster name is shown as ‘-‘.

Virtual Machines using resources from image Datastores or Virtual Networks in the Cluster ‘none’ can be deployed in any Host, which must be properly configured.

Hosts in the Cluster ‘none’ will only run VMs using resources without a Cluster.

**Warning:** System Datastores in cluster default are not shared across clusters and can only be used by hosts in the default cluster.

### 1.3.3 Scheduling and Clusters

**Automatic Requirements**

When a Virtual Machine uses resources (Images or Virtual Networks) from a Cluster, OpenNebula adds the following requirement to the template:

```bash
$ onevm show 0
[...]
AUTOMATIC_REQUIREMENTS="CLUSTER_ID = 100"
```

Because of this, if you try to use resources from more than one Cluster, the Virtual Machine creation will fail with a message similar to this one:

```bash
$ onetemplate instantiate 0
```
DISK [0]: IMAGE [0] from DATASTORE [1] requires CLUSTER [101]
NIC [0]: NETWORK [1] requires CLUSTER [100]

**Manual Requirements and Rank**

The placement attributes SCHED_REQUIREMENTS and SCHED_RANK can use attributes from the Cluster template. Let’s say you have the following scenario:

```bash
$ onehost list
ID  NAME  CLUSTER  RVM  ALLOCATED_CPU  ALLOCATED_MEM  STAT
1  host01  cluster_a  0  0 / 200 (0%)  0K / 3.6G (0%)  on
2  host02  cluster_a  0  0 / 200 (0%)  0K / 3.6G (0%)  on
3  host03  cluster_b  0  0 / 200 (0%)  0K / 3.6G (0%)  on

$ onecluster show cluster_a
CLUSTER TEMPLATE
QOS="GOLD"

$ onecluster show cluster_b
CLUSTER TEMPLATE
QOS="SILVER"
```

You can use these expressions:

- `SCHED_REQUIREMENTS = "QOS = GOLD"`
- `SCHED_REQUIREMENTS = "QOS != GOLD & Hypervisor = kvm"`

### 1.3.4 System Storage

The system datastore holds files for running VMs. Each cluster can use a different system datastore, read more in the [system datastore guide](#).

### 1.3.5 Managing Clusters in Sunstone

The **Sunstone UI interface** offers an easy way to manage clusters and the resources within them. You will find the cluster submenu under the infrastructure menu. From there, you will be able to:

- Create new clusters selecting the resources you want to include in this cluster:
Create Cluster

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Cluster</th>
<th>RVMs</th>
<th>Allocated CPU</th>
<th>Allocated MEM</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dev2</td>
<td>-</td>
<td>8</td>
<td>800 / 800 (100%)</td>
<td>8GB / 16GB (50%)</td>
<td>ON</td>
</tr>
<tr>
<td>0</td>
<td>dev1</td>
<td>-</td>
<td>7</td>
<td>800 / 800 (100%)</td>
<td>6.5GB / 16GB (41%)</td>
<td>ON</td>
</tr>
</tbody>
</table>

You selected the following hosts: dev2.

- See the list of current clusters, from which you can update the template of existing ones, or delete them.
2.1 Storage Overview

A Datastore is any storage medium used to store disk images for VMs, previous versions of OpenNebula refer to this concept as Image Repository. Typically, a datastore will be backed by SAN/NAS servers.

An OpenNebula installation can have multiple datastores of several types to store disk images. OpenNebula also uses a special datastore, the system datastore, to hold images of running VMs.

2.1.1 What Datastore Types Are Available?

OpenNebula is shipped with 3 different datastore classes:

- **System**, to hold images for running VMs, depending on the storage technology used these temporal images can be complete copies of the original image, qcow deltas or simple filesystem links.
• **Images**, stores the disk images repository. Disk images are moved, or cloned to/from the System datastore when the VMs are deployed or shutdown; or when disks are attached or snapshoted.

• **Files**, This is a special datastore used to store plain files and not disk images. The plain files can be used as kernels, ramdisks or context files.

Image datastores can be of different type depending on the underlying storage technology:

• **File-system**, to store disk images in a file form. The files are stored in a directory mounted from a SAN/NAS server.

• **vmfs**, a datastore specialized in VMFS format to be used with VMware hypervisors. Cannot be mounted in the OpenNebula front-end since VMFS is not *nix compatible.

• **LVM**, The LVM datastore driver provides OpenNebula with the possibility of using LVM volumes instead of plain files to hold the Virtual Images. This reduces the overhead of having a file-system in place and thus increases performance.

• **Ceph**, to store disk images using Ceph block devices.

• **Dev**, to attach already existent block devices in the nodes in the virtual machines

As usual in OpenNebula the system has been architected to be highly modular, so you can easily adapt the base types to your deployment.

### 2.1.2 How Are the Images Transferred to the Hosts?

The Disk images registered in a datastore are transferred to the hosts by the transfer manager (TM) drivers. These drivers are specialized pieces of software that perform low-level storage operations.

The transfer mechanism is defined for each datastore. In this way a single host can simultaneously access multiple datastores that uses different transfer drivers. Note that the hosts must be configured to properly access each data-store type (e.g. mount FS shares).

OpenNebula includes 6 different ways to distribute datastore images to the hosts:

• **shared**, the datastore is exported in a shared filesystem to the hosts.

• **ssh**, datastore images are copied to the remote hosts using the ssh protocol

• **qcow2**, a driver specialized to handle qemu-qcow format and take advantage of its snapshotting capabilities

• **vmfs**, image copies are done using the vmkfstools (VMware filesystem tools)

• **ceph**, a driver that delegates to libvirt/KVM the management of Ceph RBDs.

• **lvm**, images are stored as LVs in a cLVM volume.

• **fs_lvm**, images are in a file system and are dumped to a new LV in a cLVM volume.

• **dev**, attaches existing block devices directly to the VMs

### 2.1.3 Planning your Storage

You can take advantage of the multiple datastore features of OpenNebula to better scale the storage for your VMs, in particular:

• Balancing I/O operations between storage servers

• Different VM types or users can use datastores with different performance features

• Different SLA policies (e.g. backup) can be applied to different VM types or users
Easily add new storage to the cloud

There are some limitations and features depending on the transfer mechanism you choose for your system and image datastores (check each datastore guide for more information). The following table summarizes the valid combinations of Datastore and transfer drivers:

<table>
<thead>
<tr>
<th>Datastore</th>
<th>shared</th>
<th>ssh</th>
<th>qcow2</th>
<th>vmfs</th>
<th>ceph</th>
<th>lvm</th>
<th>fs_lvm</th>
<th>dev</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File-System</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vmfs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ceph</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>lvm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>dev</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following table reflects the compatibility of disk snapshotting and disk live snapshotting (ie, snapshotting with the VM in running state) for the different transfer manager drivers. This only applies for the kvm hypervisor.

<table>
<thead>
<tr>
<th>Datastore</th>
<th>shared</th>
<th>ssh</th>
<th>qcow2</th>
<th>vmfs</th>
<th>ceph</th>
<th>lvm</th>
<th>fs_lvm</th>
<th>dev</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshotting</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Live Snapshotting</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.1.4 Datastore Attributes

When defining a datastore there are a set of global attributes that can be used in any datastore. Please note that this list must be extended with the specific attributes for each datastore type, which can be found in the specific guide for each datastore driver.

**Common attributes:**

- **DS_MAD (mandatory)**: The DS type. Possible values: fs, lvm, vmfs, ceph, dev
- **TM_MAD (mandatory)**: Transfer drivers for the datastore. Possible values: shared, ssh, qcow2, lvm, fs_lvm, vmfs, ceph, dev
- **BASE_PATH**: Base path to build the path of the Datastore Images. This path is used to store the images when they are created in the datastores. Defaults to /var/lib/one/datastores.
- **RESTRICTED_DIRS**: Paths that cannot be used to register images. A space separated list of paths.
- **SAFE_DIRS**: If you need to un-block a directory under one of the RESTRICTED_DIRS. A space separated list of paths.
- **NO_DECOMPRESS**: Do not try to untar or decompress the file to be registered. Useful for specialized Transfer Managers
- **LIMIT_TRANSFER**: Specify the maximum transfer rate in bytes/second when downloading images from a http/https URL. Suffixes K, M or G can be used.
- **DATASTORE_CAPACITY_CHECK**: If yes, the available capacity of the datastore is checked before creating a new image.
- **LIMIT_MB**: The maximum capacity allowed for the datastore in MB.

### 2.1.5 Tuning and Extending

Drivers can be easily customized please refer to the specific guide for each datastore driver or to the Storage subsystem developer’s guide.

However you may find the files you need to modify here:

- `/var/lib/one/remotes/datastore/<DS_DRIVER>
- `/var/lib/one/remotes/tm/<TM_DRIVER>`
2.2 The System Datastore

The system datastore is a special Datastore class that holds images for running VMs. As opposed to the regular images datastores you cannot register new images into a system datastore.

**Warning:** System DS size of 0 is normal for first time installations.

To accommodate different System Datastore types, they are monitored using the host probes. The System DS size and usage will be reported as 0 till you add to OpenNebula a host configured to use that System DS. You may also need to wait for the first VM to be deployed to get size and usage information reported back.

2.2.1 Types of System Datastore

For each running VM in the datastore there is a directory containing the disk images and additional configuration files. For example, the structure of the system datastore 0 with 3 VMs (VM 0 and 2 running, and VM 7 stopped) could be:

```plaintext
datastores
|-- 0/
 | |-- 0/
 | | |-- disk.0
 | |-- 1/
 | | |-- disk.0
 | `-- 7/
   | |-- checkpoint
   | `-- disk.0
```

There are three system datastore types, based on the TM_MAD driver used:

- **shared**, the storage area for the system datastore is a shared directory across the hosts.
- **vmfs**, a specialized version of the shared one to use the vmfs file system. The infrastructure notes explained here for ‘shared’ apply to vmfs. Then please follow to the specific [VMFS storage guide here](#).
- **ssh**, uses a local storage area from each host for the system datastore

The Shared System Datastore

The shared transfer driver requires the hosts to share the system datastore directory (it does not need to be shared with the front-end). Typically these storage areas are shared using a distributed FS like NFS, GlusterFS, Lustre, etc.

A shared system datastore usually reduces VM deployment times and **enables live-migration**, but it can also become a bottleneck in your infrastructure and degrade your VMs performance if the virtualized services perform disk-intensive workloads. Usually this limitation may be overcome by:

- Using different filesystem servers for the images datastores, so the actual I/O bandwith is balanced
- Using an ssh system datastore instead, the images are copied locally to each host
- Tuning or improving the filesystem servers
**The SSH System Datastore**

In this case the system datastore is distributed among the hosts. The ssh transfer driver uses the hosts’ local storage to place the images of running VMs (as opposed to a shared FS in the shared driver). All the operations are then performed locally but images have to be copied always to the hosts, which in turn can be a very resource demanding operation. Also this driver prevents the use of live-migrations between hosts.
The System and Image Datastores

OpenNebula will automatically transfer VM disk images to/from the system datastore when a VM is booted or shut-down. The actual transfer operations and the space taken from the system datastore depends on both the image configuration (persistent vs non-persistent) as well as the drivers used by the images datastore. The following table summarizes the actions performed by each transfer manager driver type.

<table>
<thead>
<tr>
<th>Image Type</th>
<th>shared</th>
<th>ssh</th>
<th>qcow2</th>
<th>vmfs</th>
<th>ceph</th>
<th>lvm</th>
<th>shared lvm</th>
<th>dev</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent</td>
<td>link</td>
<td>copy</td>
<td>link</td>
<td>link</td>
<td>link</td>
<td>link</td>
<td>lv copy</td>
<td></td>
</tr>
<tr>
<td>Non-persistent</td>
<td>copy</td>
<td>copy</td>
<td>snapshot</td>
<td>cp</td>
<td>rdb copy+</td>
<td>lv copy+</td>
<td>lv copy</td>
<td>link</td>
</tr>
<tr>
<td>Volatile</td>
<td>new</td>
<td>new</td>
<td>new</td>
<td>new</td>
<td>new</td>
<td>new</td>
<td>new</td>
<td>new</td>
</tr>
</tbody>
</table>

In the table above:

- **link** is the equivalent to a symbolic link operation that will not take any significant amount of storage from the system datastore.
- **copy, rbd copy and lv copy**, are copy operations as in regular cp file operations, that may involve creation of special devices like a logical volume. This will take the same size as the original image.
- **snapshot**, qcow2 snapshot operation.
- **new**, a new image file is created on the system datastore of the specified size.

**Important Note, operations with +**, are performed on the original image datastore; an so those operations take storage from the image datastore and not from the system one.

Once the disk images are transferred from the image datastore to the system datastore using the operations described above, the system datastore (and its drivers) is responsible for managing the images, mainly to:

- Move the images across hosts, e.g. when the VM is stopped or migrated
- Delete any copy from the hosts when the VM is shut-down

### 2.2.2 Configuration Overview

You need to configure one or more system datastores for each of your clusters. In this way you can better plan the storage requirements, in terms of total capacity assigned, performance requirements and load balancing across system datastores. Note that hosts not assigned to a cluster can still use system datastores that are neither assigned to a cluster.

To configure the system datastores for your OpenNebula cloud you need to:

- Create as many system datastores as needed (you can add more later if you need them)
- Assign the system datastores to a given cluster
- Configure the cluster hosts to access the system datastores

### 2.2.3 Step 1. Create a New System Datastore

To create a new system datastore you need to specify its type as system either in Sunstone (system) or through the CLI (adding TYPE = SYSTEM_DS to the datastore template). And you need to select the system datastore drivers, as discussed above: shared, vmfs and ssh.

For example to create a system datastore using the shared drivers simply:
2.2.4 Step 2. Assign the System Datastores

Hosts can only use a system datastore if they are in the same cluster, so once created you need to add the system datastores to the cluster. You can add more than one system datastore to a cluster, the actual system DS used to deploy the VM will be selected based on storage scheduling policies, see below.

```
$ cat system.ds
NAME    = nfs_ds
TM_MAD  = shared
TYPE    = SYSTEM_DS

$ onedatastore create system.ds
ID: 100
```

**Warning:** Host not associated to a cluster will also use system datastores not associated to a cluster. If you are not using clusters you can skip this section.

To associate this system datastore to the cluster, add it:

```
$ onecluster adddatastore production_cluster nfs_ds
```

As we’ll see shortly, hosts need to be configured to access the systems datastore through a well-known location, that defaults to /var/lib/one/datastores. You can also override this setting for the hosts of a cluster using the DATASTORE_LOCATION attribute. It can be changed with the onecluster update command.

```
$ onecluster update production_cluster
#Edit the file to read as:
DATASTORE_LOCATION=/path/to/datastores/
```

**Warning:** DATASTORE_LOCATION defines the path to access the datastores in the hosts. It can be defined for each cluster, or if not defined for the cluster the default in oned.conf will be used.

**Warning:** When needed, the front-end will access the datastores at /var/lib/one/datastores, this path cannot be changed, you can link each datastore directory to a suitable location.

2.2.5 Step 3. Configure the Hosts

The specific configuration for the hosts depends on the system datastore type (shared or ssh). Before continuing check that SSH is configured to enable oneadmin passwordless access in every host.

**Configure the Hosts for the Shared System Datastore**

A NAS has to be configured to export a directory to the hosts, this directory will be used as the storage area for the system datastore. Each host has to mount this directory under $DATASTORE_LOCATION/<ds_id>. In small installations the front-end can be also used to export the system datastore directory to the hosts. Although this deployment is not recommended for medium-large size deployments.

**Warning:** It is not needed to mount the system datastore in the OpenNebula front-end as /var/lib/one/datastores/<ds_id>
Configure the Hosts for the SSH System Datastore

There is no special configuration needed to take place to use the ssh drivers for the system datastore. Just be sure that there is enough space under `$DATASTORE_LOCATION` to hold the images of the VMs that will run in each particular host.

Also be sure that there is space in the frontend under `/var/lib/one/datastores/<ds_id>` to hold the images of the stopped or undeployed VMs.

2.2.6 Multiple System Datastore Setups

In order to distribute efficiently the I/O of the VMs across different disks, LUNs or several storage backends, OpenNebula is able to define multiple system datastores per cluster. Scheduling algorithms take into account disk requirements of a particular VM, so OpenNebula is able to pick the best execution host based on capacity and storage metrics.

Admin Perspective

For an admin, it means that she would be able to decide which storage policy to apply for the whole cloud she is administering, that will then be used to chose which system datastore is more suitable for a certain VM.

When more than one system datastore is added to a cluster, all of them can be taken into account by the scheduler to place VMs into.

System scheduling policies are defined in `/etc/one/sched.conf`. These are the defaults the scheduler would use if the VM template doesn’t state otherwise. The possibilities are described here:

- **Packing**. Tries to optimize storage usage by selecting the datastore with less free space.
- **Striping**. Tries to optimize I/O by distributing the VMs across datastores.
- **Custom**. Based on any of the attributes present in the datastore template.

To activate for instance the Stripping storage policy, `/etc/one/sched.conf` must contain:

```plaintext
DEFAULT_DS_SCHED = 
  [ 
    policy = 1 
  ]
```

After a VM is deployed in a system datastore, the admin can migrate it to another system datastore. To do that, the VM must be first powered-off. The command `onevm migrate` accepts both a new host and datastore id, that must have the same TM_MAD drivers as the source datastore.

**Warning:** Any host belonging to a given cluster must be able to access any system or image datastore defined in that cluster.

**Warning:** System Datastores in cluster default are not shared across clusters and can only be used by hosts in the default cluster.

User Perspective

For a user, OpenNebula’s ability to handle multiples datastore means that she would be able to require for its VMs to be run on a system datastore backed by a fast storage cabin, or run on the host with a datastore with the most free space available. This choice is obviously limited to the underlying hardware and the administrator configuration.

This control can be exerted within the VM template, with two attributes:
### Attribute | Description | Examples
--- | --- | ---
SCHED_DS_REQUIREMENTS | Boolean expression that rules out entries from the pool of datastores suitable to run this VM. | `SCHED_DS_REQUIREMENTS="ID=100"`
| | | `SCHED_DS_REQUIREMENTS="NAME=GoldenCephDS"`
| | | `SCHED_DS_REQUIREMENTS=FREE_MB > 250000)`
SCHED_DS_RANK | States which attribute will be used to sort the suitable datastores for this VM. Basically, it defines which datastores are more suitable than others. | `SCHED_DS_RANK=FREE_MB`
| | | `SCHED_DS_RANK=-FREE_MB`

**Warning:** Admins and user with admins rights can force the deployment to a certain datastore, using `onevm deploy` command.

## 2.2.7 Disable a System Datastore

System Datastores can be disabled to prevent the scheduler from deploying new Virtual Machines in them. Datastores in the `disabled` state and monitored as usual, and the existing VMs will continue to run in them.

```
$ onedatastore disable system -v
DATASTORE 0: disabled

$ onedatastore show system
DATASTORE 0 INFORMATION
ID : 0
NAME : system
...
STATE : DISABLED
```

## 2.2.8 Tuning and Extending

Drivers can be easily customized. Please refer to the specific guide for each datastore driver or to the Storage subsystem developer’s guide.

However you may find the files you need to modify here:
- `/var/lib/one/remotes/datastore/<DS_DRIVER>`
- `/var/lib/one/remotes/tm/<TM_DRIVER>`

## 2.3 The Filesystem Datastore

The Filesystem datastore lets you store VM images in a file form. The datastore is format agnostic, so you can store any file-type depending on the target hypervisor. The use of file-based disk images presents several benefits over device backed disks (e.g. easily backup images, or use of shared FS) although it may less performing in some cases.

Usually it is a good idea to have multiple filesystem datastores to:
- Group images of the same type, so you can have a qcow datastore for KVM hosts and a raw one for Xen
- Balance I/O operations, as the datastores can be in different servers
- Use different datastores for different cluster hosts
2.3.1 Requirements

There are no special requirements or software dependencies to use the filesystem datastore. The drivers make use of standard filesystem utils (cp, ln, mv, tar, mkfs...) that should be installed in your system.

2.3.2 Configuration

Configuring the System Datastore

Filesystem datastores can work with a system datastore that uses either the shared or the SSH transfer drivers, note that:

- Shared drivers for the system datastore enables live-migrations, but it could demand a high-performance SAN.
- SSH drivers for the system datastore may increase deployment/shutdown times but all the operations are performed locally, so improving performance in general.

See more details on the System Datastore Guide

Configuring the FileSystem Datastores

The first step to create a filesystem datastore is to set up a template file for it. In the following table you can see the valid configuration attributes for a filesystem datastore. The datastore type is set by its drivers, in this case be sure to add DS_MAD=fs.

The other important attribute to configure the datastore is the transfer drivers. These drivers determine how the images are accessed in the hosts. The Filesystem datastore can use shared, ssh and qcow2. See below for more details.

The specific attributes for this datastore driver are listed in the following table, you will also need to complete with the common datastore attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS_MAD</td>
<td>The DS type, use fs for the Filesystem datastore</td>
</tr>
<tr>
<td>TM_MAD</td>
<td>Transfer drivers for the datastore: shared, ssh or qcow2, see below</td>
</tr>
</tbody>
</table>

For example, the following illustrates the creation of a filesystem datastore using the shared transfer drivers.

```bash
> cat ds.conf
NAME = production
DS_MAD = fs
TM_MAD = shared

> onedatastore create ds.conf
ID: 100

> onedatastore list
<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>IMAGES</th>
<th>TYPE</th>
<th>TM</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>system</td>
<td>none</td>
<td>0</td>
<td>fs</td>
<td>shared</td>
</tr>
<tr>
<td>1</td>
<td>default</td>
<td>none</td>
<td>3</td>
<td>fs</td>
<td>shared</td>
</tr>
<tr>
<td>100</td>
<td>production</td>
<td>none</td>
<td>0</td>
<td>fs</td>
<td>shared</td>
</tr>
</tbody>
</table>
```

The DS and TM MAD can be changed later using the onedatastore update command. You can check more details of the datastore by issuing the onedatastore show command.
Finally, you have to prepare the storage for the datastore and configure the hosts to access it. This depends on the transfer mechanism you have chosen for your datastore.

After creating a new datastore the LN_TARGET and CLONE_TARGET parameters will be added to the template. These values should not be changed since they define the datastore behaviour. The default values for these parameters are defined in oned.conf for each driver.

**Warning:** Note that datastores are not associated to any cluster by default, and their are supposed to be accessible by every single host. If you need to configure datastores for just a subset of the hosts take a look to the Cluster guide.

### Frontend Access to the Storage

By default, it is implied that the Frontend has direct access to the storage. Let’s say we are configuring datastore DS_ID = 100. It is implied that the frontend can write directly to /var/lib/one/datastores/100. When an image is first downloaded and registered into the datastore, only the frontend is involved in this operation.

However, in some scenarios this not ideal, and therefore it can be configured. If the underlying storage is GlusterFS, GFS2 or any other shared storage system, and we do not want the frontend to be part of this storage cluster we can use these attributes to configure the behaviour:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRIDGE_LIST</td>
<td><em>(Optional)</em> Space separated list of hosts that have access to the storage. This can be all the hosts in the storage cluster, or a subset of them, which will carry out the write operations to the datastore. For each operation only one of the host will be chosen, using a round-robin algorithm.</td>
</tr>
<tr>
<td>STAGING_DIR</td>
<td><em>(Optional)</em> Images are first downloaded to the frontend and then scp’d over to the chosen host from the BRIDGE_LIST list. They are scp’d to the STAGING_DIR, and then moved to the final destination. If empty, it defaults to /var/tmp.</td>
</tr>
</tbody>
</table>

**Warning:** When using a BRIDGE_LIST the front-end will not interact with the datastore therefore the BASE_PATH of the datastore needs to be set to the DATASTORE_LOCATION value. This is the default behavior and only needs to be adjusted if the DATASTORE_LOCATION attribute has been changed.

### 2.3.3 Using the Shared Transfer Driver

The shared transfer driver assumes that the datastore is mounted in all the hosts of the cluster. When a VM is created, its disks (the disk.i files) are copied or linked in the corresponding directory of the system datastore. These file operations are always performed remotely on the target host.
Persistent & Non Persistent Images

If the VM uses a persistent image, a symbolic link to the datastore is created in the corresponding directory of the system datastore. Non-persistent images are copied instead. For persistent images, this allows an immediate deployment, and no extra time is needed to save the disk back to the datastore when the VM is shut down.

On the other hand, the original file is used directly, and if for some reason the VM fails and the image data is corrupted or lost, there is no way to cancel the persistence.

Finally images created using the ‘onevm disk-snapshot’ command will be moved to the datastore only after the VM is successfully shut down. This means that the VM has to be shutdown using the ‘onevm shutdown’ command, and not ‘onevm delete’. Suspending or stopping a running VM won’t copy the disk file to the datastore either.

Host Configuration

Each host has to mount the datastore under `$DATASTORE_LOCATION/<datastore_id>`. You also have to mount the datastore in the front-end in `/var/lib/one/datastores/<datastore_id>`.

If you are using NFS to share the filesystem between nodes some sensible mount options are `soft,intr,rsize=32768,wsize=32768`. For example:

```
server:/storage/datastore0 /var/lib/one/datastores/0 nfs soft,intr,rsize=32768,wsize=32768,rw 0 0
```

With the documented configuration of libvirt/kvm the image files are accessed as `oneadmin` user. In case the files must be read by `root` the option `no_root_squash` must be added.

**Warning:** `$DATASTORE_LOCATION` defines the path to access the datastores in the hosts. It can be defined for each cluster, or if not defined for the cluster the default in `oned.conf` will be used.
2.3.4 Using the SSH Transfer Driver

In this case the datastore is only directly accessed by the front-end. VM images are copied from/to the datastore using the SSH protocol. This may impose high VM deployment times depending on your infrastructure network connectivity.

Persistent & Non Persistent Images

In either case (persistent and non-persistent) images are always copied from the datastore to the corresponding directory of the system datastore in the target host.

If an image is persistent (or for the matter of fact, created with the ‘onevm disk-snapshot’ command), it is transferred back to the Datastore only after the VM is successfully shut down. This means that the VM has to be shut down using the ‘onevm shutdown’ command, and not ‘onevm delete’. Note that no modification to the image registered in the datastore occurs till that moment. Suspending or stopping a running VM won’t copy/modify the disk file registered in the datastore either.

Host Configuration

There is no special configuration for the hosts in this case. Just make sure that there is enough space under $DATASTORE_LOCATION to hold the images of the VMs running in that host.

2.3.5 Using the qcow2 Transfer driver

The qcow2 drivers are a specialization of the shared drivers to work with the qcow2 format for disk images. The same features/restrictions and configuration applies so be sure to read the shared driver section.

The following list details the differences:

- Persistent images are created with the `qemu-img` command using the original image as backing file
• When an image has to be copied back to the datastore the `qemu-img convert` command is used instead of a direct copy

### 2.3.6 Tuning and Extending

Drivers can be easily customized please refer to the specific guide for each datastore driver or to the Storage subsystem developer’s guide.

However you may find the files you need to modify here:

• `/var/lib/one/remotes/datastore/<DS_DRIVER>`
• `/var/lib/one/remotes/tm/<TM_DRIVER>`

### 2.4 The VMFS Datastore

In order to use VMware hypervisors in your OpenNebula cloud you will need to use **VMFS Datastores**. To configure them, it is important to keep in mind that there are (at least) two datastores to define, the system datastore (where the running VMs and their images reside, only need transfer manager drivers) and the images datastore (where the images are stored, needs both datastore and transfer manager drivers).

#### 2.4.1 Requirements

• In order to use the VMFS datastore, the ESX servers need to have the SSH access configured for the oneadmin account.

• If the VMFS volumes are exported through a SAN, it should be accesible and configured so the ESX server can mount the iSCSI export.

#### 2.4.2 Description

This storage model implies that all the volumes involved in the image staging are purely VMFS volumes, taking full advantage of the VMware filesystem (VM image locking and improved performance).
2.4.3 Infrastructure Configuration

- The OpenNebula front-end doesn’t need to mount any datastore.
- The ESX servers needs to present or mount (as iSCSI, NFS or local storage) both the system datastore and the image datastore (naming them with just the <datastore-id>, for instance 0 for the system datastore and 1 for the image datastore).

**Warning:** The system datastore can be other than the default one (0). In this case, the ESX will need to mount the datastore with the same id as the datastores has in OpenNebula. More details in the System Datastore Guide.

2.4.4 OpenNebula Configuration

The datastore location on ESX hypervisors is ”/vmfs/volumes”. There are two choices:

- In homogeneous clouds (all the hosts are ESX) set the following in /etc/one/oned.conf:

```ini
DATASTORE_LOCATION=/vmfs/volumes
```

2.4. The VMFS Datastore
• In heterogeneous clouds (mix of ESX and other hypervisor hosts) put all the ESX hosts in clusters with the following attribute in their template (e.g. oneclass update):

```
DATASTORE_LOCATION=/vmfs/volumes
```

**Warning:** You need also to set the BASE_PATH attribute in the template when the Datastore is created.

## Datastore Configuration

The **system** and **images** datastores needs to be configured with the following drivers:

<table>
<thead>
<tr>
<th>Datastore</th>
<th>DS Drivers</th>
<th>TM Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>.</td>
<td>vmfs</td>
</tr>
<tr>
<td>Images</td>
<td>vmfs</td>
<td>vmfs</td>
</tr>
</tbody>
</table>

### System Datastore

*vmfs* drivers: the **system** datastore needs to be updated in OpenNebula (onidatastore update <ds_id>) to set the TM_MAD drivers to *vmfs*. There is no need to configure datastore drivers for the system datastore.

OpenNebula expects the system datastore to have the ID=0, but a system datastore with different ID can be defined per cluster. See the **system datastore guide** for more details.

### Images Datastore

The **image** datastore needs to be updated to use *vmfs* drivers for the datastore drivers, and *vmfs* drivers for the transfer manager drivers. The default datastore can be updated as:

```
$ onidatastore update 1
DS_MAD=vmfs
TM_MAD=vmfs
BRIDGE_LIST=<space-separated list of ESXi host>
```

The specific attributes for this datastore driver are listed in the following table, you will also need to complete with the **common datastore attributes**:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS_MAD</td>
<td>The DS type, use <em>vmfs</em></td>
</tr>
<tr>
<td>TM_MAD</td>
<td>Must be <em>vmfs</em></td>
</tr>
<tr>
<td>BRIDGE_LIST</td>
<td>Space separated list of ESX servers that are going to be used as proxies to stage images into the datastore (<em>vmfs</em> datastores only)</td>
</tr>
<tr>
<td>DS_TMP_DIR</td>
<td>Path in the OpenNebula front-end to be used as a buffer to stage in files in <em>vmfs</em> datastores. Defaults to the value in <code>/var/lib/one/remotes/datastore/vmfs/vmfs.conf</code>.</td>
</tr>
<tr>
<td>BASE_PATH</td>
<td>This variable must be set to <em>vmfs</em>/volumes for VMFS datastores.</td>
</tr>
</tbody>
</table>

After creating a new datastore the LN_TARGET and CLONE_TARGET parameters will be added to the template. These values should not be changed since they define the datastore behaviour. The default values for these parameters are defined in *oned.conf* for each driver.
Driver Configuration

Transfer Manager Drivers

These drivers trigger the events remotely through an ssh channel. The \texttt{vmfs} drivers are a specialization of the shared drivers to work with the VMware vmdk filesystem tools using the \texttt{vmkfstool} command. This comes with a number of advantages, like FS locking, easier VMDK cloning, format management, etc.

Datastore Drivers

The \texttt{vmfs} datastore drivers allows the use of the VMware VM filesystem, which handles VM file locks and also boosts I/O performance.

- To correctly configure a \texttt{vmfs} datastore set of drivers there is the need to chose the ESX bridges, i.e., the ESX serves that are going to be used as proxies to stage images into the \texttt{vmfs} datastore. A list of bridges must be defined with the \texttt{BRIDGE\_LIST} attribute of the datastore template (see the table below). The drivers will pick one ESX server from that list in a round robin fashion.
- The \texttt{vmfs} datastore needs to use the front-end as a buffer for the image staging in some cases, this buffer can be set in the \texttt{DS\_TMP\_DIR} attribute.

2.4.5 Tuning and Extending

Drivers can be easily customized please refer to the specific guide for each datastore driver or to the Storage subsystem developer’s guide.

However you may find the files you need to modify here:

- \texttt{/var/lib/one/remotes/datastore/\texttt{<DS\_DRIVER>}}
- \texttt{/var/lib/one/remotes/tm/\texttt{<TM\_DRIVER>}}

2.5 LVM Drivers

The LVM datastore driver provides OpenNebula with the possibility of using LVM volumes instead of plain files to hold the Virtual Images. This reduces the overhead of having a file-system in place and thus increases performance.

2.5.1 Overview

OpenNebula ships with two sets of LVM drivers:

- \texttt{FS LVM}, file based VM disk images with Logical Volumes (LV), using the \texttt{fs\_lvm} drivers
- \texttt{Block LVM}, pure Logical Volume (LV), using the \texttt{lvm} drivers

In both cases Virtual Machine will run from Logical Volumes in the host, and they both require cLVM in order to provide live-migration.

However there are some differences, in particular the way non active images are stored, and the name of the Volume Group where they are executed.

This is a brief description of both drivers:
2.5.2 FS LVM

In a FS LVM datastore using the fs_lvm drivers (the now recommended LVM drivers), images are registered as files in a shared FS volume, under the usual path: /var/lib/one/datastores/<id>.

This directory needs to be accessible in the worker nodes, using NFS or any other shared/distributed file-system.

When a Virtual Machine is instantiated OpenNebula will dynamically select the system datastore. Let’s assume for instance the selected datastore is 104. The virtual disk image will be copied from the stored image file under the datastores directory and dumped into a LV under the Volume Group: vg-one-104. It follows that each node must have a cluster-aware LVM Volume Group for every possible system datastore it may execute.

This set of drivers brings precisely the advantage of dynamic selection of the system datastore, allowing therefore more granular control of the performance of the storage backend.

Read more

2.5.3 Block LVM

The Block LVM datastore use the lvm drivers with the classical approach to using LVM in OpenNebula.

When a new datastore that uses this set of drivers is created, it requires the VG_NAME parameter, which will tie the images to that Volume Group. Images will be registered directly as Logical Volumes in that Volume Group (as opposed to being registered as files in the frontend), and when they are instantiated the new cloned Logical Volume will also be created in that very same Volume Group.
2.6 The FS LVM Datastore

2.6.1 Overview

The FS LVM datastore driver provides OpenNebula with the possibility of using LVM volumes instead of plain files to hold the Virtual Images.

It is assumed that the OpenNebula hosts using this datastore will be configured with CLVM, therefore modifying the OpenNebula Volume Group in one host will reflect in the others.
2.6.2 Requirements

OpenNebula Front-end

- Password-less ssh access to an OpenNebula LVM-enabled host.

OpenNebula LVM Hosts

LVM must be available in the Hosts. The oneadmin user should be able to execute several LVM related commands with sudo passwordlessly.

- Password-less sudo permission for: lvremove, lvcreate, lvs, vgdisplay and dd.
- LVM2
  - oneadmin needs to belong to the disk group (for KVM).

2.6.3 Configuration

Configuring the System Datastore

To use LVM drivers, the system datastore must be shared. This system datastore will hold only the symbolic links to the block devices, so it will not take much space. See more details on the System Datastore Guide.

It will also be used to hold context images and Disks created on the fly, they will be created as regular files.

It is worth noting that running virtual disk images will be created in Volume Groups that are hardcoded to be vg-one-<system_ds_id>. Therefore the nodes must have those Volume Groups pre-created and available for all possible system datastores.

Configuring LVM Datastores

The first step to create a LVM datastore is to set up a template file for it.

The specific attributes for this datastore driver are listed in the following table, you will also need to complete with the common datastore attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS_MAD</td>
<td>Must be fs</td>
</tr>
<tr>
<td>TM_MAD</td>
<td>Must be fs_lvm</td>
</tr>
<tr>
<td>DISK_TYPE</td>
<td>Must be block</td>
</tr>
</tbody>
</table>

For example, the following examples illustrates the creation of an LVM datastore using a configuration file. In this case we will use the host host01 as one of our OpenNebula LVM-enabled hosts.

```
> cat ds.conf
NAME = production
DS_MAD = fs
TM_MAD = fs_lvm

> onedatastore create ds.conf
ID: 100

> onedatastore list
   ID  NAME  CLUSTER  IMAGES  TYPE  TM
     0  system  none  0   fs  shared
```
1 default none 3 fs shared
100 production none 0 fs fs_lvm

**Note:** Datastores are not associated to any cluster by default, and they are supposed to be accessible by every single host. If you need to configure datastores for just a subset of the hosts take a look to the *Cluster guide.*

After creating a new datastore the LN_TARGET and CLONE_TARGET parameters will be added to the template. These values should not be changed since they define the datastore behaviour. The default values for these parameters are defined in `oned.conf` for each driver.

**Host Configuration**

The hosts must have LVM2 and **must** have a Volume-Group for every possible system-datastore that can run in the host. CLVM must also be installed and active across all the hosts that use this datastore.

It’s also required to have password-less sudo permission for: `lvremove, lvcreate, lvs` and `dd`.

**2.6.4 Tuning & Extending**

System administrators and integrators are encouraged to modify these drivers in order to integrate them with their datacenter:

Under `/var/lib/one/remotes/`:

- `tm/fs_lvm/ln`: Links to the LVM logical volume.
- `tm/fs_lvm/clone`: Clones the image by creating a snapshot.
- `tm/fs_lvm/mvds`: Saves the image in a new LV for SAVE_AS.
- `tm/fs_lvm/cpds`: Saves the image in a new LV for SAVE_AS while VM is running.

**2.7 The Block LVM Datastore**

**2.7.1 Overview**

The Block LVM datastore driver provides OpenNebula with the possibility of using LVM volumes instead of plain files to hold the Virtual Images.

It is assumed that the OpenNebula hosts using this datastore will be configured with CLVM, therefore modifying the OpenNebula Volume Group in one host will reflect in the others. There is a special list of hosts (BRIDGE_LIST) which belong to the LVM cluster, that will be the ones OpenNebula uses to speak to when doing LVM operations.
2.7.2 Requirements

OpenNebula Front-end

- Password-less ssh access to an OpenNebula LVM-enabled host.

OpenNebula LVM Hosts

LVM must be available in the Hosts. The oneadmin user should be able to execute several LVM related commands with sudo passwordlessly.

- Password-less sudo permission for: lvremove, lvcreate, lvs, vgdisplay and dd.
- LVM2
- oneadmin needs to belong to the disk group (for KVM).

2.7.3 Configuration

Configuring the System Datastore

To use LVM drivers, the system datastore will work both with shared or as ssh. This sytem datastore will hold only the symbolic links to the block devices, so it will not take much space. See more details on the System Datastore Guide.

It will also be used to hold context images and Disks created on the fly, they will be created as regular files.

Configuring Block LVM Datastores

The first step to create a LVM datastore is to set up a template file for it.

The specific attributes for this datastore driver are listed in the following table, you will also need to complete with the common datastore attributes.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS_MAD</td>
<td>Must be lvm</td>
</tr>
<tr>
<td>TM_MAD</td>
<td>Must be lvm</td>
</tr>
<tr>
<td>DISK_TYPE</td>
<td>Must be block</td>
</tr>
<tr>
<td>VG_NAME</td>
<td>The LVM volume group name. Defaults to vg-one</td>
</tr>
<tr>
<td>BRIDGE_LIST</td>
<td>Mandatory space separated list of LVM frontends.</td>
</tr>
</tbody>
</table>

For example, the following examples illustrates the creation of an LVM datastore using a configuration file. In this case we will use the host host01 as one of our OpenNebula LVM-enabled hosts.

```bash
> cat ds.conf
NAME = production
DS_MAD = lvm
TM_MAD = lvm
VG_NAME = vg-one
BRIDGE_LIST = "host01 host02"

> onedatastore create ds.conf
ID: 100

> onedatastore list
ID  NAME    CLUSTER IMAGES TYPE  TM
  0  system  none  0      fs   shared
  1  default none  3      fs   shared
 100 production none  0      lvm  shared
```

The DS and TM MAD can be changed later using the `onedatastore update` command. You can check more details of the datastore by issuing the `onedatastore show` command.

**Warning:** Note that datastores are not associated to any cluster by default, and they are supposed to be accessible by every single host. If you need to configure datastores for just a subset of the hosts take a look to the Cluster guide.

After creating a new datastore the LN_TARGET and CLONE_TARGET parameters will be added to the template. These values should not be changed since they define the datastore behaviour. The default values for these parameters are defined in `oned.conf` for each driver.

**Host Configuration**

The hosts must have LVM2 and have the Volume-Group used in the VG_NAME attributed of the datastore template. CLVM must also be installed and active across all the hosts that use this datastore.

It’s also required to have password-less sudo permission for: `lvremove, lvcreate, lvs` and `dd`.

**2.7.4 Tuning & Extending**

System administrators and integrators are encouraged to modify these drivers in order to integrate them with their datacenter:

Under `/var/lib/one/remotes/`:

- `datastore/lvm/lvm.conf`: Default values for LVM parameters
  - VG_NAME: Default volume group
  - DEFAULT_SIZE: Default size of the snapshots

# 2.7. The Block LVM Datastore
• **datastore/lvm/cp**: Registers a new image. Creates a new logical volume in LVM.
• **datastore/lvm/mkfs**: Makes a new empty image. Creates a new logical volume in LVM.
• **datastore/lvm/rm**: Removes the LVM logical volume.
• **tm/lvm/in**: Links to the LVM logical volume.
• **tm/lvm/clone**: Clones the image by creating a snapshot.
• **tm/lvm/mvds**: Saves the image in a new LV for SAVE_AS.

### 2.8 The Ceph Datastore

The Ceph datastore driver provides OpenNebula users with the possibility of using Ceph block devices as their Virtual Images.

**Warning:** This driver only works with libvirt/KVM drivers. Xen is not (yet) supported.

**Warning:** This driver requires that the OpenNebula nodes using the Ceph driver must be Ceph clients of a running Ceph cluster. More information in Ceph documentation.

### 2.8.1 Requirements

#### Ceph Cluster Configuration

The hosts where Ceph datastores based images will be deployed must be part of a running Ceph cluster. To do so refer to the Ceph documentation.

Also the mon daemon must be defined in the ceph.conf for all the nodes, so hostname and port doesn’t need to be specified explicitly in any Ceph command.

Additionally each OpenNebula datastore is backed by a ceph pool, these pools must be created and configured in the Ceph cluster. The name of the pool by default is one but can be changed on a per-datastore basis (see below).

The ceph cluster admin must include a valid user to be used by one ceph datastore (see below). This user should be configured in the CEPH_USER variable in the datastore template (see below). OpenNebula will issue commands from the oneadmin account in the nodes and in the frontend, using --id $CEPH_USER as a parameter, for example rbd --id $CEPH_USER. If a non-default configuration file needs to be used, it can be passed along with the CEPH_CONF tag: when set, rbd and “rados” commands will called with: rbd --conf=$CEPH_CONF. Ceph authentication must be configured in a way that issuing commands these commands does work.

This driver can work with either RBD Format 1 or RBD Format 2 (default). To set the default you can specify this option in ceph.conf:

```
[global]
  rbd_default_format = 2
```

#### OpenNebula Ceph Frontend

This driver requires the system administrator to specify one or several Ceph frontends (which need to be nodes in the Ceph cluster) where many of the datastores storage actions will take place. For instance, when creating an image, OpenNebula will choose one of the listed Ceph frontends (using a round-robin algorithm) and transfer the image to that node and run qemu-img convert -O rbd. These nodes need to be specified in the BRIDGE_LIST section.
Note that this Ceph frontend can be any node in the OpenNebula setup: the OpenNebula frontend, any worker node, or a specific node (recommended).

**Ceph Nodes**

All the nodes listed in the `BRIDGE_LIST` variable must have `qemu-img` installed.

**OpenNebula Hosts**

There are no specific requirements for the host, besides being libvirt/kvm nodes, since xen is not (yet) supported for the Ceph drivers.

### 2.8.2 Configuration

#### Configuring the System Datastore

To use ceph drivers, the system datastore will work both with `shared` or as `ssh`. This system datastore will hold only the symbolic links to the block devices, so it will not take much space. See more details on the [System Datastore Guide](#).

It will also be used to hold context images and Disks created on the fly, they will be created as regular files.

#### Configuring Ceph Datastores

The first step to create a Ceph datastore is to set up a template file for it.

The specific attributes for this datastore driver are listed in the following table, you will also need to complete with the common datastore attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS_MAD</td>
<td>The DS type, use <code>ceph</code> for the Ceph datastore</td>
</tr>
<tr>
<td>TM_MAD</td>
<td>Transfer drivers for the datastore, use <code>ceph</code>, see below</td>
</tr>
<tr>
<td>DISK_TYPE</td>
<td>The type must be RBD</td>
</tr>
<tr>
<td>BRIDGE_LIST</td>
<td>Mandatory space separated list of Ceph servers that are going to be used as frontends.</td>
</tr>
<tr>
<td>POOL_NAME</td>
<td>The OpenNebula Ceph pool name. Defaults to <code>one</code>. <em>This pool must exist before using the drivers.</em></td>
</tr>
<tr>
<td>STAGING_DIR</td>
<td>Default path for image operations in the OpenNebula Ceph frontend.</td>
</tr>
<tr>
<td>CEPH_HOST</td>
<td>Space-separated list of Ceph monitors. Example: host1 host2:port2 host3 host4:port4 (if no port is specified, the default one is chosen). <em>Required for LibVirt 1.x when cephx is enabled.</em></td>
</tr>
<tr>
<td>CEPH_USER</td>
<td>The OpenNebula Ceph user name. If set it is used by RBD commands. <em>This ceph user must exist before using the drivers. Required for LibVirt 1.x when cephx is enabled.</em></td>
</tr>
<tr>
<td>CEPH_CONF</td>
<td>The non default ceph configuration file. If set it is used by RBD commands: rbd and rados.</td>
</tr>
<tr>
<td>CEPH_SECRET</td>
<td>A generated UUID for a LibVirt secret (to hold the CephX authentication key in LibVirt on each hypervisor). This should be generated when creating the Ceph datastore in OpenNebula. <em>Required for LibVirt 1.x when cephx is enabled.</em></td>
</tr>
<tr>
<td>RBD_FORMAT</td>
<td>By default RBD Format 2 will be used. If <code>RBD_FORMAT=1</code> is specified then when instantiating non-persistent images the Ceph driver will perform <code>rbd copy</code> instead of <code>rbd snap</code>.</td>
</tr>
</tbody>
</table>

For example, the following examples illustrates the creation of an Ceph datastore using a configuration file. In this case we will use the host `cephfrontend` as one the OpenNebula Ceph frontend The one pool must already exist, if it doesn’t create it with:
An example of datastore:

```bash
> cat ds.conf
NAME = "cephds"
DS_MAD = ceph
TM_MAD = ceph
CEPH_HOST = host1 host2:port2

# the following lines *must* be preset
DISK_TYPE = RBD
POOL_NAME = one

# CEPH_USER and CEPH_SECRET are mandatory for cephx
CEPH_USER = libvirt
CEPH_SECRET="6f88b54b-5dae-41fe-a43e-b2763f601cfc"

BRIDGE_LIST = cephfrontend
```

```bash
> onedatastore create ds.conf
ID: 101
```

```bash
> onedatastore list
<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>IMAGES</th>
<th>TYPE</th>
<th>TM</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>system</td>
<td>none</td>
<td>0</td>
<td>fs</td>
<td>shared</td>
</tr>
<tr>
<td>1</td>
<td>default</td>
<td>none</td>
<td>3</td>
<td>fs</td>
<td>shared</td>
</tr>
<tr>
<td>100</td>
<td>cephds</td>
<td>none</td>
<td>0</td>
<td>ceph</td>
<td>ceph</td>
</tr>
</tbody>
</table>
```

The DS and TM MAD can be changed later using the `onedatastore update` command. You can check more details of the datastore by issuing the `onedatastore show` command.

**Warning:** Note that datastores are not associated to any cluster by default, and they are supposed to be accessible by every single host. If you need to configure datastores for just a subset of the hosts take a look to the Cluster guide.

After creating a new datastore the LN_TARGET and CLONE_TARGET parameters will be added to the template. These values should not be changed since they define the datastore behaviour. The default values for these parameters are defined in `oned.conf` for each driver.

### 2.8.3 Using Datablocks with Ceph

It is worth noting that when creating datablock, creating a RAW image is very fast whereas creating a formatted block device takes a longer time. If you want to use a RAW image remember to use the following attribute/option when creating the Image datablock: `FS_TYPE = RAW`.

### 2.8.4 Ceph Authentication (Cephx)

If Cephx is enabled, there are some special considerations the OpenNebula administrator must take into account.

Create a Ceph user for the OpenNebula hosts. We will use the name `client.libvirt`, but any other name is fine. Create the user in Ceph and grant it rwx permissions on the `one` pool:
Distribute the `client.libvirt.key` and `ceph.client.libvirt.keyring` file to all the KVM hosts: 
- `ceph.client.libvirt.keyring` must be placed under `/etc/ceph` (in all the hypervisors and frontend) 
- `client.libvirt.key` must delivered somewhere where oneadmin can read it in order to create the libvirt secret documents.

Generate a UUID, for example running `uuidgen` (the generated uuid will referenced as `$UUID` from now onwards).

Create a file named `secret.xml` (using the generated `$UUID` and distribute it to all the KVM hosts:

```
cat > secret.xml <<EOF
<secret ephemeral='no' private='no'>
  <uuid>$UUID</uuid>
  <usage type='ceph'>
    <name>client.libvirt secret</name>
  </usage>
</secret>
EOF
```

The following commands must be executed in all the KVM hosts as oneadmin (assuming the `secret.xml` and `client.libvirt.key` files have been distributed to the hosts):

```
virsh -c qemu:///system secret-define secret.xml
# Replace $UUID with the value generated in the previous step
virsh -c qemu:///system secret-set-value --secret $UUID --base64 $(cat client.libvirt.key)
```

Finally, the Ceph datastore must be updated to add the following values:

```
CEPH_USER="libvirt"
CEPH_SECRET="$UUID"
CEPH_HOST="<list of ceph mon hosts, see table above>"
```

You can read more information about this in the Ceph guide [Using libvirt with Ceph](#).

### 2.8.5 Using the Ceph Transfer Driver

The workflow for Ceph images is similar to the other datastores, which means that a user will create an image inside the Ceph datastores by providing a path to the image file locally available in the OpenNebula frontend, or to an http url, and the driver will convert it to a Ceph block device.

All the usual operations are available: oneimage create, oneimage delete, oneimage clone, oneimage persistent, oneimage nonpersistent, onevm disk-snapshot, etc...

### 2.8.6 Tuning & Extending

**File Location**

System administrators and integrators are encouraged to modify these drivers in order to integrate them with their datacenter:

Under `/var/lib/one/remotes/`:

- **datastore/ceph/ceph.conf**: Default values for ceph parameters
  
  - HOST: Default OpenNebula Ceph frontend
– **POOL_NAME**: Default volume group
– **STAGING_DIR**: Default path for image operations in the OpenNebula Ceph frontend.

- **datastore/ceph/cp**: Registers a new image. Creates a new logical volume in ceph.
- **datastore/ceph/rm**: Removes the ceph logical volume.
- **tm/ceph/ln**: Does nothing since it’s handled by libvirt.
- **tm/ceph/clone**: Copies the image to a new image.
- **tm/ceph/mvds**: Saves the image in a Ceph block device for SAVE_AS.
- **tm/ceph/delete**: Removes non-persistent image volumes and files.
- **tm/ceph/snap_create**: Creates a disk snapshot.
- **tm/ceph/snap_delete**: Deletes a disk snapshot.
- **tm/ceph/snap_revert**: Reverts to an existing disk snapshot.

### Using SSH System Datastore

Another option would be to manually patch the post and pre-migrate scripts for the `ssh` system datastore to `scp` the files residing in the system datastore before the live-migration. Read more.

### 2.9 The GlusterFS Datastore

GlusterFS driver allows KVM machines access VM images using native GlusterFS API. This datastore uses the **Shared Transfer Manager** and the **Filesystem Datastore** to access a Gluster fuse filesystem to manage images.

**Warning**: This driver **only** works with libvirt/KVM drivers. Xen is not (yet) supported.

**Warning**: All virtualization nodes and the head need to mount the GlusterFS volume used to store images.

**Warning**: The hypervisor nodes need to be part of a working GlusterFS cluster and the Libvirt and QEMU packages need to be recent enough to have support for GlusterFS.

### 2.9.1 Requirements

**GlusterFS Volume Configuration**

OpenNebula does not run as root user. To be able to access native GlusterFS API user access must be allowed. This can be achieved by adding this line to `/etc/glusterfs/glusterd.vol`:

```
option rpc-auth-allow-insecure on
```

and executing this command (replace `<volume>` with your volume name):

```
# gluster volume set <volume> server.allow-insecure on
```
As stated in the Libvirt documentation it will be useful to set the owner-uid and owner-gid to the ones used by oneadmin user and group:

```
# gluster volume set <volume> storage.owner-uid <oneadmin uid>
# gluster volume set <volume> storage.owner-gid <oneadmin gid>
```

To make Qemu work with Gluster over libgfapi we need to create a file `/var/lib/glusterd/groups/virt` with following content

```
quick-read=off
read-ahead=off
io-cache=off
stat-prefetch=on
eager-lock=enable
remote-dio=enable
quorum-type=auto
server.allow-insecure=on
server-quorum-type=server
```

Enable the settings on the group

```
gluster volume set <volume> group virt
```

### Datastore Mount

The GlusterFS volume must be mounted in all the virtualization nodes and the head node using fuse mount. This mount will be used to manage images and VM related files (images and checkpoints). The oneadmin account must have write permissions on the mounted filesystem and it must be accessible by both the system and image datastore. The recommended way of setting the mount points is to mount the gluster volume in a specific path and to symlink the datastore directories:

```
# mkdir -p /var/lib/one/datastores/0
# mount -t glusterfs server:/volume /var/lib/one/datastores/0
# chown oneadmin:oneadmin /var/lib/one/datastores/0
# ln -s /var/lib/one/datastores/0 /var/lib/one/datastores/1
```

#### 2.9.2 Configuration

**Configuring the System Datastore**

The system datastore must be of type shared. See more details on the System Datastore Guide

It will also be used to hold context images and volatile disks.

**Configuring GlusterFS Datastore**

The specific attributes for this datastore driver are listed in the following table, you will also need to complete with the common datastore attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS_MAD</td>
<td>The DS type, use fs for the Gluster datastore</td>
</tr>
<tr>
<td>TM_MAD</td>
<td>Transfer drivers for the datastore, use shared, see below</td>
</tr>
<tr>
<td>DISK_TYPE</td>
<td>The type must be GLUSTER</td>
</tr>
<tr>
<td>GLUSTER_HOST</td>
<td>Host and port of one (only one) Gluster server host:port</td>
</tr>
<tr>
<td>GLUSTER_VOLUME</td>
<td>Gluster volume to use for the datastore</td>
</tr>
</tbody>
</table>
An example of datastore:

```bash
> cat ds.conf
NAME = "glusterds"
DS_MAD = fs
TM_MAD = shared

# the following line *must* be preset
DISK_TYPE = GLUSTER

GLUSTER_HOST = gluster_server:24007
GLUSTER_VOLUME = one_vol

CLONE_TARGET="SYSTEM"
LN_TARGET="NONE"

> onedatastore create ds.conf
ID: 101

> onedatastore list

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>SIZE</th>
<th>AVAIL</th>
<th>CLUSTER</th>
<th>IMAGES</th>
<th>TYPE</th>
<th>DS</th>
<th>TM</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>system</td>
<td>9.9G</td>
<td>98%</td>
<td>-</td>
<td>0</td>
<td>sys</td>
<td>shared</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>default</td>
<td>9.9G</td>
<td>98%</td>
<td>-</td>
<td>2</td>
<td>img</td>
<td>fs</td>
<td>shared</td>
</tr>
<tr>
<td>2</td>
<td>files</td>
<td>12.3G</td>
<td>66%</td>
<td>-</td>
<td>0</td>
<td>fil</td>
<td>fs</td>
<td>ssh</td>
</tr>
<tr>
<td>101</td>
<td>default</td>
<td>9.9G</td>
<td>98%</td>
<td>-</td>
<td>0</td>
<td>img</td>
<td>fs</td>
<td>shared</td>
</tr>
</tbody>
</table>
```

**Warning:** It is recommended to group the Gluster datastore and the Gluster enabled hypervisors in an OpenNebula cluster. ref:cluster<cluster_guide>

### 2.10 The Devices Datastore

This datastore is used to register already existent block devices in the nodes to be used with virtual machines. It does not do any kind of device discovering or setup. The devices should be already setup and available and, VMs using these devices must be fixed to run in the nodes ready for them.

**Warning:** This driver only works with KVM and Xen drivers. VMware is not supported.

#### 2.10.1 Requirements

The devices you want to attach to a VM should be accessible by the hypervisor:

- Xen runs as root so this user should be able to access it.
- KVM usually runs as oneadmin. Make sure this user is in a group with access to the disk (like disk) and has read write permissions for the group.

Images created in this datastore should be persistent. Making the images non persistent allows more than one VM use this device and will probably cause problems and data corruption.

**Warning:** The datastore should only be usable by the administrators. Letting users create images in this datastore will cause security problems. For example, register an image `/dev/sda` and reading the host filesystem.
2.10.2 Configuration

Configuring the System Datastore

The system datastore can be of type shared or ssh. See more details on the System Datastore Guide

Configuring DEV Datastore

The datastore needs to have: DS_MAD and TM_MAD set to dev and DISK_TYPE to BLOCK.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>The name of the datastore</td>
</tr>
<tr>
<td>DS_MAD</td>
<td>The DS type, use dev</td>
</tr>
<tr>
<td>TM_MAD</td>
<td>Transfer drivers for the datastore, use dev</td>
</tr>
<tr>
<td>DISK_TYPE</td>
<td>The type must be BLOCK</td>
</tr>
</tbody>
</table>

Note that for this datastore some of the common datastore attributes do not apply, in particular: - BASE_PATH: does NOT apply - RESTRICTED_DIRS: does NOT apply - SAFE_DIRS: does NOT apply - NO_DECOMPRESS: does NOT apply - LIMIT_TRANSFER_BW: does NOT apply - DATASTORE_CAPACITY_CHECK: does NOT apply

An example of datastore:

```bash
> cat dev.conf
NAME=dev
DISK_TYPE="BLOCK"
DS_MAD="dev"
TM_MAD="dev"
TYPE="IMAGE_DS"

> onedatastore create dev.conf
ID: 101

> onedatastore list
<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>SIZE</th>
<th>AVAIL</th>
<th>CLUSTER</th>
<th>IMAGES</th>
<th>TYPE</th>
<th>DS</th>
<th>TM</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>system</td>
<td>9.9G</td>
<td>98%</td>
<td>-</td>
<td>0 sys</td>
<td>-</td>
<td>shared</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>default</td>
<td>9.9G</td>
<td>98%</td>
<td>-</td>
<td>2 img</td>
<td>shared</td>
<td>shared</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>files</td>
<td>12.3G</td>
<td>66%</td>
<td>-</td>
<td>0 fil</td>
<td>fs</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>dev</td>
<td>1M</td>
<td>100%</td>
<td>-</td>
<td>0 img</td>
<td>dev</td>
<td>dev</td>
<td></td>
</tr>
</tbody>
</table>
```

2.10.3 Use

New images can be added as any other image specifying the path. If you are using the CLI do not use the shorthand parameters as the CLI check if the file exists and the device most provably won’t exist in the frontend. As an example here is an image template to add a node disk /dev/sdb:

```bash
NAME=scsi_device
PATH=/dev/sdb
PERSISTENT=YES
```

**Warning:** As this datastore does is just a container for existing devices images does not take any size from it. All devices registered will render size of 0 and the overall devices datastore will show up with 1MB of available space.
2.11 The Kernels & Files Datastore

The Files Datastore lets you store plain files to be used as VM kernels, ramdisks or context files. The Files Datastore does not expose any special storage mechanism but a simple and secure way to use files within VM templates. There is a Files Datastore (datastore ID: 2) ready to be used in OpenNebula.

2.11.1 Requirements

There are no special requirements or software dependencies to use the Files Datastore. The recommended drivers make use of standard filesystem utils (cp, ln, mv, tar, mkfs...) that should be installed in your system.

2.11.2 Configuration

Most of the configuration considerations used for disk images datastores do apply to the Files Datastore (e.g. driver setup, cluster assignment, datastore management...).

The specific attributes for this datastore driver are listed in the following table, you will also need to complete with the common datastore attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE</td>
<td>Use FILE_DS to setup a Files datastore</td>
</tr>
<tr>
<td>DS_MAD</td>
<td>The DS type, use fs to use the file-based drivers</td>
</tr>
<tr>
<td>TM_MAD</td>
<td>Transfer drivers for the datastore, use ssh to transfer the files</td>
</tr>
</tbody>
</table>

For example, the following illustrates the creation of File Datastore.

```
> cat kernels_ds.conf
NAME = kernels
DS_MAD = fs
TM_MAD = ssh
TYPE = FILE_DS
SAFE_DIRS = /var/tmp/files

> onedatastore create kernels_ds.conf
ID: 100
```

```
> onedatastore list
<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>IMAGES</th>
<th>TYPE</th>
<th>DS</th>
<th>TM</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>system</td>
<td>-</td>
<td>0 sys</td>
<td>-</td>
<td>dummy</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>default</td>
<td>-</td>
<td>0 img</td>
<td>dummy</td>
<td>dummy</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>files</td>
<td>-</td>
<td>0 fil</td>
<td>fs</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>kernels</td>
<td>-</td>
<td>0 fil</td>
<td>fs</td>
<td>ssh</td>
<td></td>
</tr>
</tbody>
</table>
```

The DS and TM MAD can be changed later using the onedatastore update command. You can check more details of the datastore by issuing the onedatastore show command.

2.11.3 Host Configuration

The recommended ssh driver for the File Datastore does not need any special configuration for the hosts. Just make sure that there is enough space under $DATASTORE_LOCATION to hold the VM files in the front-end and hosts.

For more details refer to the Filesystem Datapath guide, as the same configuration guidelines applies.
3.1 Virtualization Overview

The Virtualization Subsystem is the component in charge of talking with the hypervisor installed in the hosts and taking the actions needed for each step in the VM lifecycle.

Configuration options and specific information for each hypervisor can be found in these guides:

- Xen Driver
- KVM Driver
- VMware Driver

3.1.1 Common Configuration Options

Drivers accept a series of parameters that control their execution. The parameters allowed are:

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r &lt;num&gt;</td>
<td>number of retries when executing an action</td>
</tr>
<tr>
<td>-t &lt;num&gt;</td>
<td>number of threads, i.e. number of actions done at the same time</td>
</tr>
<tr>
<td>-l &lt;actions&gt;</td>
<td>actions executed locally</td>
</tr>
</tbody>
</table>

See the Virtual Machine drivers reference for more information about these parameters, and how to customize and extend the drivers.

3.1.2 Hypervisor Configuration

A feature supported by both KVM and Xen Hypervisor drivers is selecting the timeout for VM Shutdown. This feature is useful when a VM gets stuck in Shutdown (or simply does not notice the shutdown command). By default, after the timeout time the VM will return to Running state but is can also be configured so the VM is destroyed after the grace time. This is configured in both /var/lib/one/remotes/vmm/xen/xenrc and /var/lib/one/remotes/vmm/kvm/kvmmc:

```
# Seconds to wait after shutdown until timeout
export SHUTDOWN_TIMEOUT=300

# Uncomment this line to force VM cancellation after shutdown timeout
#export FORCE_DESTROY=yes
```
3.2 Xen Driver

The XEN hypervisor offers a powerful, efficient and secure feature set for virtualization of x86, IA64, PowerPC and other CPU architectures. It delivers both paravirtualization and full virtualization. This guide describes the use of Xen with OpenNebula, please refer to the Xen specific documentation for further information on the setup of the Xen hypervisor itself.

3.2.1 Requirements

The Hosts must have a working installation of Xen that includes a Xen aware kernel running in Dom0 and the Xen utilities.

3.2.2 Considerations & Limitations

• Xen HVM currently only supports 4 IDE devices, for more disk devices you should better use SCSI. You have to take this into account when adding disks. See the Virtual Machine Template documentation for an explanation on how OpenNebula assigns disk targets.

• OpenNebula manages kernel and initrd files. You are encouraged to register them in the files datastore.

• To modify the default disk driver to one that works with your Xen version you can change the files `/etc/one/vmm_exec/vmm_exec_xen*.conf` and `/var/lib/one/remotes/vmm/xen*/xenrc`. Make sure that you have blktap2 modules loaded to use tap2:tapdisk:aio:

```bash
export IMAGE_PREFIX="tap2:tapdisk:aio"

DISK = [ driver = "tap2:tapdisk:aio:" ]
```

• If target device is not supported by the linux kernel you will be able to attach disks but not detach them. It is recommended to attach xvd devices for xen paravirtualized hosts.

3.2.3 Configuration

Xen Configuration

In each Host you must perform the following steps to get the driver running:

• The remote hosts must have the xend daemon running (`/etc/init.d/xend`) and a XEN aware kernel running in Dom0

• The `<oneadmin>` user may need to execute Xen commands using root privileges. This can be done by adding this two lines to the `sudoers` file of the hosts so `<oneadmin>` user can execute Xen commands as root (change paths to suit your installation):

```bash
%xe ALL=(ALL) NOPASSWD: /usr/sbin/xm *
%xe ALL=(ALL) NOPASSWD: /usr/sbin/xentop *
```

• You may also want to configure network for the virtual machines. OpenNebula assumes that the VMs have network access through standard bridging, please refer to the Xen documentation to configure the network for your site.

• Some distributions have `requiretty` option enabled in the `sudoers` file. It must be disabled to so ONE can execute commands using sudo. The line to remove or comment out (by placing a # at the beginning of the line) is this one:
OpenNebula Configuration

OpenNebula needs to know if it is going to use the XEN Driver. There are two sets of Xen VMM drivers, one for Xen version 3.x and other for 4.x, you will have to uncomment the version you will need. To achieve this for Xen version 4.x, uncomment these drivers in `/etc/one/oned.conf`:

```python
IM_MAD = [
    name = "xen",
    executable = "one_im_ssh",
    arguments = "xen"
]

VM_MAD = [
    name = "xen",
    executable = "one_vmm_exec",
    arguments = "xen4",
    default = "vmm_exec/vmm_exec_xen4.conf",
    type = "xen"
]
```

xen4 drivers are meant to be used with Xen >=4.2 with xl/xenlight interface. You will need to stop xend daemon for this. For Xen 3.x and Xen 4.x with xm (with xend daemon) you will need to use xen3 drivers.

Warning: When using "xen3" drivers for Xen 4.x you should change the configuration file `/var/lib/oneremotes/vmm/xen3/xenrc` and uncomment the XM_CREDITS line.

3.2.4 Usage

The following are template attributes specific to Xen, please refer to the template reference documentation for a complete list of the attributes supported to define a VM.

**XEN Specific Attributes**

**DISK**

- **driver**, This attribute defines the Xen backend for disk images, possible values are file:, tap:, aio:... Note the trailing :.

**NIC**

- **model**, This attribute defines the type of the vif. This corresponds to the type attribute of a vif, possible values are ioemu, netfront...
- **ip**, This attribute defines the ip of the vif and can be used to set antispoofing rules. For example if you want to use antispoofing with network-bridge, you will have to add this line to `/etc/xen/xend-config.sxp`:

  ```
  (network-script 'network-bridge antispoofing=yes')
  ```
OS

- **bootloader.** You can use this attribute to point to your pygrub loader. This way you wont need to specify the kernel/initrd and it will use the internal one. Make sure the kernel inside is domU compatible if using paravirtualization.

- When no kernel/initrd or bootloader attributes are set then a HVM machine is created.

CONTEXT

- **driver,** for the CONTEXT device, e.g. ‘file:’, ‘phy:’...

Additional Attributes

The *raw* attribute offers the end user the possibility of passing by attributes not known by OpenNebula to Xen. Basically, everything placed here will be written ad literally into the Xen deployment file.

```
RAW = [ type="xen", data="on_crash=destroy" ]
```

3.2.5 Tuning & Extending

The driver consists of the following files:

- `/usr/lib/one/mads/one_vmm_exec`: generic VMM driver.
- `/var/lib/one/remotes/vmm/xen`: commands executed to perform actions.

And the following driver configuration files:

- `/etc/one/vmm_exec/vmm_exec_xen3/4.conf`: This file is home for default values for domain definitions (in other words, OpenNebula templates). Let’s go for a more concrete and VM related example. If the user wants to set a default value for KERNEL for all of their XEN domain definitions, simply edit the `vmm_exec_xen.conf` file and set a

```
OS = [ kernel="/vmlinuz" ]
```

into it. Now, when defining a ONE template to be sent to a XEN resource, the user has the choice of “forgetting” to set the KERNEL parameter, in which case it will default to /vmlinuz.

It is generally a good idea to place defaults for the XEN-specific attributes, that is, attributes mandatory for the XEN hypervisor that are not mandatory for other hypervisors. Non mandatory attributes for XEN but specific to them are also recommended to have a default.

- `/var/lib/one/remotes/vmm/xen/xenrc`: This file contains environment variables for the driver. You may need to tune the values for XM_PATH, if `/usr/sbin/xm` do not live in their default locations in the remote hosts. This file can also hold instructions to be executed before the actual driver load to perform specific tasks or to pass environmental variables to the driver. The syntax used for the former is plain shell script that will be evaluated before the driver execution. For the latter, the syntax is the familiar:

```
ENVIRONMENT_VARIABLE=VALUE
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMAGE_PREFIX</td>
<td>This will be used as the default handler for disk hot plug</td>
</tr>
<tr>
<td>SHUTDOWN_TIMEOUT</td>
<td>Seconds to wait after shutdown until timeout</td>
</tr>
<tr>
<td>FORCE_DESTROY</td>
<td>Force VM cancellation after shutdown timeout</td>
</tr>
</tbody>
</table>

See the Virtual Machine drivers reference for more information.
3.2.6 Credit Scheduler

Xen comes with a credit scheduler. The credit scheduler is a proportional fair share CPU scheduler built from the ground up to be work conserving on SMP hosts. This attribute sets a 16 bit value that will represent the amount of sharing this VM will have respect to the others living in the same host. This value is set into the driver configuration file, is not intended to be defined per domain.

Xen drivers come preconfigured to use this credit scheduler and uses the scale “1 OpenNebula CPU” = “256 xen scheduler credits”. A VM created with CPU=2.0 will have 512 xen scheduler credits. If you need to change this scaling parameter it can be configured in /etc/one/vmm_exec/vmm_exec_xen[3/4].conf. The variable name is called CREDIT.

3.2.7 Importing VMs

VMs running on XEN hypervisors that were not launched through OpenNebula can be imported in OpenNebula. It is important to highlight that, besides the limitations explained in the host guide, the “Poweroff” operation is not available for these imported VMs in XEN.

3.3 KVM Driver

KVM (Kernel-based Virtual Machine) is a complete virtualization technique for Linux. It offers full virtualization, where each Virtual Machine interacts with its own virtualized hardware. This guide describes the use of the KVM virtualizer with OpenNebula, please refer to KVM specific documentation for further information on the setup of the KVM hypervisor itself.

3.3.1 Requirements

The hosts must have a working installation of KVM, that usually requires:

- CPU with VT extensions
- libvirt >= 0.4.0
- the qemu user-land tools

3.3.2 Considerations & Limitations

- KVM currently only supports 4 IDE devices, for more disk devices you should better use SCSI or virtio. You have to take this into account when adding disks. See the Virtual Machine Template documentation for an explanation on how OpenNebula assigns disk targets.
- By default live migrations are started from the host the VM is currently running. If this is a problem in your setup you can activate local live migration adding -l migrate=migrate_local to vmm_mad arguments.
- If you get error messages similar to error: cannot close file: Bad file descriptor upgrade libvirt version. Version 0.8.7 has a bug related to file closing operations.
- In case you are using disks with a cache setting different to none you may have problems with live migration depending on the libvirt version. You can enable the migration adding the --unsafe parameter to the virsh command. The file to change is /var/lib/one/remotes/vmm/kvm/kvmsync. Uncomment the following line, and execute onehost sync --force afterwards:
MIGRATE_OPTIONS=--unsafe

- Modern qemu versions (>= 1.10) have support some extensions of the qcow2 format that are not compatible with older versions. By default the images are generated in this format. To make them work in previous versions they need to be converted:

```
qemu-img convert -f qcow2 -O qcow2 -o compat=0.10 <source image> <destination image>
```

### 3.3.3 Configuration

#### KVM Configuration

OpenNebula uses the libvirt interface to interact with KVM, so the following steps are required in the hosts to get the KVM driver running:

- Qemu should be configured to not change file ownership. Modify `/etc/libvirt/qemu.conf` to include `dynamic_ownership = 0`. To be able to use the images copied by OpenNebula, change also the user and group under which the libvirtd is run to “oneadmin”:

  ```bash
  $ grep -vE '^($|#)' /etc/libvirt/qemu.conf
  user = "oneadmin"
group = "oneadmin"
dynamic_ownership = 0
  
  Warning: Note that oneadmin’s group may be other than oneadmin. Some distributions adds oneadmin to the cloud group. Use group = “cloud” above in that case.
  
- VMs can not be migrated from hosts with SElinux active to machines with it inactive. To make it work in an infrastructure with mixed SElinux configuration you can disable VM labeling. This is done adding the following lines to `/etc/libvirt/qemu.conf`:

  ```bash
  security_driver = "none"
  security_default_confined = 0
  
  Warning: VMs can not be migrated from hosts with SElinux active to machines with it inactive. To make it work in an infrastructure with mixed SElinux configuration you can disable VM labeling. This is done adding the following lines to `/etc/libvirt/qemu.conf`:
  ```
  
  security_driver = "none"
  security_default_confined = 0
  
- The remote hosts must have the libvirt daemon running.

- The user with access to these remote hosts on behalf of OpenNebula (typically `<oneadmin>`) has to pertain to the `<libvirtd>` and `<kvm>` groups in order to use the deaemon and be able to launch VMs.

  ```bash
  owner /var/lib/one/** rw,
  
  Warning: If apparmor is active (by default in Ubuntu it is), you should add `/var/lib/one` to the end of `/etc/apparmor.d/abstractions/libvirt-qemu`.
  
  owner /var/lib/one/** rw,
  
  Warning: If apparmor is active (by default in Ubuntu it is), you should add `/var/lib/one` to the end of `/etc/apparmor.d/abstractions/libvirt-qemu`.
  
  owner /var/lib/one/** rw,
  
  Warning: If your distro is using PolicyKit you can use this recipe by Jan Horacek to add the require privileges to oneadmin user:

  ```bash
  
  # content of file: /etc/polkit-1/localauthority/50-local.d/50-org.libvirt.unix.manage-opennebula.pkla
  [Allow oneadmin user to manage virtual machines]
  Identity=unix-user:oneadmin
  Action=org.libvirt.unix.manage
  #Action=org.libvirt.unix.monitor
  ResultAny=yes
  ResultInactive=yes
  ResultActive=yes
  ```
OpenNebula uses libvirt’s migration capabilities. More precisely, it uses the qemu+ssh protocol offered by libvirt. In order to configure the physical hosts, the following files have to be modified:

- /etc/libvirt/libvirtd.conf: Uncomment “listen_tcp = 1”. Security configuration is left to the admin’s choice, file is full of useful comments to achieve a correct configuration. As a tip, if you don’t want to use TLS for connections set listen_tls = 0.
- Add the listen option to libvirt init script:
  - /etc/default/libvirt-bin: add -l option to libvirtd_opts
  - For RHEL based distributions, edit this file instead: /etc/sysconfig/libvirtd: uncomment LIBVIRTD_ARGS="--listen"

### OpenNebula Configuration

OpenNebula needs to know if it is going to use the KVM Driver. To achieve this, uncomment these drivers in /etc/one/oned.conf:

```
IM_MAD = [
    name = "kvm",
    executable = "one_im_ssh",
    arguments = "-r 0 -t 15 kvm"
]

VM_MAD = [
    name = "kvm",
    executable = "one_vmm_exec",
    arguments = "-t 15 -r 0 kvm",
    default = "vmm_exec/vmm_exec_kvm.conf",
    type = "kvm"
]
```

### Working with cgroups (Optional)

**Warning:** This section outlines the configuration and use of cgroups with OpenNebula and libvirt/KVM. Please refer to the cgroups documentation of your Linux distribution for specific details.

Cgroups is a kernel feature that allows you to control the amount of resources allocated to a given process (among other things). This feature can be used to enforce the amount of CPU assigned to a VM, as defined in its template. So, thanks to cgroups a VM with CPU=0.5 will get half of the physical CPU cycles than a VM with CPU=1.0.

Cgroups can be also used to limit the overall amount of physical RAM that the VMs can use, so you can leave always a fraction to the host OS.

The following outlines the steps need to configure cgroups, this should be **performed in the hosts, not in the front-end**: 

- Define where to mount the cgroup controller virtual file systems, at least memory and cpu are needed.
- (Optional) You may want to limit the total memory devoted to VMs. Create a group for the libvirt processes (VMs) and the total memory you want to assign to them. Be sure to assign libvirt processes to this group, e.g. with CGROUP_DAEMON or in cgrules.conf. Example:

```bash
#/etc/cgconfig.conf

group virt {
    memory {
        memory.limit_in_bytes = 5120M;
    }
}
```
After configuring the hosts start/restart the cgroups service.

(Optional) If you have limited the amount of memory for VMs, you may want to set `RESERVED_MEM` parameter in host or cluster templates. That’s it. OpenNebula automatically generates a number of CPU shares proportional to the CPU attribute in the VM template. For example, consider a host running 2 VMs (73 and 74, with CPU=0.5 and CPU=1) respectively. If everything is properly configured you should see:

```
/mnt/cgroups/cpu/sysdefault/libvirt/qemu/
|-- cgroup.event_control
  ...
  |-- cpu.shares
  |-- cpu.stat
  |-- notify_on_release
  |-- one-73
  |   |-- cgroup.clone_children
  |   |-- cgroup.event_control
  |   |-- cgroup.procs
  |   |-- cpu.shares
  |   ...
  |   `-- vcpu0
  |       |-- cgroup.clone_children
  |       ...
  |   `-- one-74
  |       |-- cgroup.clone_children
  |       |-- cgroup.event_control
  |       |-- cgroup.procs
  |       |-- cpu.shares
  |       ...
  |       `-- vcpu0
  |           |-- cgroup.clone_children
  |           ...
  `-- tasks
```

and the cpu shares for each VM:

```
> cat /mnt/cgroups/cpu/sysdefault/libvirt/qemu/one-73/cpu.shares
512
> cat /mnt/cgroups/cpu/sysdefault/libvirt/qemu/one-74/cpu.shares
1024
```

VCPUs are not pinned so most probably the virtual process will be changing the core it is using. In an ideal case where the VM is alone in the physical host the total amount of CPU consumed will be equal to VCPU plus any overhead of virtualization (for example networking). In case there are more VMs in that physical node and is heavily used then the VMs will compete for physical CPU time. In this case cgroups will do a fair share of CPU time between VMs (a VM with CPU=2 will get double the time as a VM with CPU=1).
In case you are not overcommitting (CPU=VCPUs) all the virtual CPUs will have one physical CPU (even if it’s not pinned) so they could consume the number of VCPUs assigned minus the virtualization overhead and any process running in the host OS.

**Udev Rules**

When creating VMs as a regular user, `/dev/kvm` needs to be chowned to the `oneadmin` user. For that to be persistent you have to apply the following UDEV rule:

```bash
# cat /etc/udev/rules.d/60-qemu-kvm.rules
KERNEL=="kvm", GROUP="oneadmin", MODE="0660"
```

### 3.3.4 Usage

The following are template attributes specific to KVM, please refer to the template reference documentation for a complete list of the attributes supported to define a VM.

**Default Attributes**

There are some attributes required for KVM to boot a VM. You can set a suitable defaults for them so, all the VMs get needed values. These attributes are set in `/etc/one/vmm_exec/vmm_exec_kvm.conf`. The following can be set for KVM:

- **emulator**, path to the kvm executable. You may need to adjust it to your distro
- **os**, the attributes: kernel, initrd, boot, root, kernel_cmd, and arch
- **vcpu**
- **features**, attributes: acpi, pae
- **disk**, attributes driver and cache. All disks will use that driver and caching algorithm
- **nic**, attribute filter.
- **raw**, to add libvirt attributes to the domain XML file.

For example:

```plaintext
OS = [
    KERNEL = /vmlinuz,
    BOOT = hd,
    ARCH = "x86_64"]

DISK = [ driver = "raw", cache = "none"]

NIC = [ filter = "clean-traffic", model = "virtio"]

RAW = "<devices><serial type="pty"><source path="/dev/pts/5"/><target port="0"/></serial><console type="pty" tty="/dev/pts/5"><source path="/dev/pts/5"/><target port="0"/></console></devices>
```

**KVM Specific Attributes**

**DISK**

- **type**, This attribute defines the type of the media to be exposed to the VM, possible values are: disk (default), cdrom or floppy. This attribute corresponds to the media option of the -driver argument of the kvm
command.

- **driver**, specifies the format of the disk image; possible values are `raw`, `qcow2`... This attribute corresponds to the format option of the `-driver` argument of the `kvm` command.

- **cache**, specifies the optional cache mechanism, possible values are “default”, “none”, “writethrough” and “writeback”.

- **io**, set IO policy possible values are “threads” and “native”

**NIC**

- **target**, name for the tun device created for the VM. It corresponds to the `ifname` option of the ‘-net’ argument of the `kvm` command.

- **script**, name of a shell script to be executed after creating the tun device for the VM. It corresponds to the `script` option of the ‘-net’ argument of the `kvm` command.

- **model**, ethernet hardware to emulate. You can get the list of available models with this command:

  ```
  $ kvm -net nic,model=? -nographic /dev/null
  ```

- **filter** to define a network filtering rule for the interface. Libvirt includes some predefined rules (e.g. clean-traffic) that can be used. Check the Libvirt documentation for more information, you can also list the rules in your system with:

  ```
  $ virsh -c qemu:///system nwfilter-list
  ```

**Graphics**

If properly configured, libvirt and KVM can work with SPICE (check this for more information). To select it, just add to the GRAPHICS attribute:

- **type = spice**

Enabling spice will also make the driver inject specific configuration for these machines. The configuration can be changed in the driver configuration file, variable `SPICE_OPTIONS`.

**Virtio**

Virtio is the framework for IO virtualization in KVM. You will need a linux kernel with the virtio drivers for the guest, check the KVM documentation for more info.

If you want to use the virtio drivers add the following attributes to your devices:

- **DISK**, add the attribute `DEV_PREFIX=vd`

- **NIC**, add the attribute `model=virtio`

**Additional Attributes**

The `raw` attribute offers the end user the possibility of passing by attributes not known by OpenNebula to KVM. Basically, everything placed here will be written literally into the KVM deployment file (use libvirt xml format and semantics).
KVM supports hotplugging to the virtio and the SCSI buses. For disks, the bus the disk will be attached to is inferred from the DEV_PREFIX attribute of the disk template.

- sd: SCSI (default).
- vd: virtio.

If TARGET is passed instead of DEV_PREFIX the same rules apply (what happens behind the scenes is that OpenNebula generates a TARGET based on the DEV_PREFIX if no TARGET is provided).

The configuration for the default cache type on newly attached disks is configured in /var/lib/one/remotes/vmm/kvm/kvmrc:

```bash
# This parameter will set the default cache type for new attached disks. It
# will be used in case the attached disk does not have an specific cache
# method set (can be set using templates when attaching a disk).
DEFAULT_ATTACH_CACHE=none
```

For Disks and NICs, if the guest OS is a Linux flavour, the guest needs to be explicitly tell to rescan the PCI bus. This can be done issuing the following command as root:

```bash
# echo 1 > /sys/bus/pci/rescan
```

### 3.3.5 Tuning & Extending

The driver consists of the following files:

- `/usr/lib/one/mads/one_vmm_exec`: generic VMM driver.
- `/var/lib/one/remotes/vmm/kvm`: commands executed to perform actions.

And the following driver configuration files:

- `/etc/one/vmm_exec/vmm_exec_kvm.conf`: This file is home for default values for domain definitions (in other words, OpenNebula templates).

It is generally a good idea to place defaults for the KVM-specific attributes, that is, attributes mandatory in the KVM driver that are not mandatory for other hypervisors. Non mandatory attributes for KVM but specific to them are also recommended to have a default.

- `/var/lib/one/remotes/vmm/kvm/kvmrc`: This file holds instructions to be executed before the actual driver load to perform specific tasks or to pass environmental variables to the driver. The syntax used for the former is plain shell script that will be evaluated before the driver execution. For the latter, the syntax is the familiar:

```bash
ENVIRONMENT_VARIABLE=VALUE
```

The parameters that can be changed here are as follows:
### Parameter | Description
--- | ---
LIBVIRT_URI | Connection string to libvirtd
QEMU_PROTOCOL | Protocol used for live migrations
SHUTDOWN_TIMEOUT | Seconds to wait after shutdown until timeout
FORCE_DESTROY | Force VM cancellation after shutdown timeout
CANCEL_NO ACPI | Force VM’s without ACPI enabled to be destroyed on shutdown
DEFAUL_T_ATTACH_CACHE | This parameter will set the default cache type for new attached disks. It will be used in case the attached disk does not have an specific cache method set (can be set using templates when attaching a disk).
MIGRATE_OPTIONS | Set options for the virsh migrate command

See the Virtual Machine drivers reference for more information.

### 3.3.6 PCI Passthrough

It is possible to discover PCI devices in the hypervisors and assign them to Virtual Machines for the KVM hypervisor. The setup and environment information is taken from [http://www.firewing1.com/howtos/fedora-20/create-gaming-virtual-machine-using-vfio-pci-passthrough-kvm](http://www.firewing1.com/howtos/fedora-20/create-gaming-virtual-machine-using-vfio-pci-passthrough-kvm). You can safely ignore all the VGA related sections, for PCI devices that are not graphic cards, or if you don’t want to output video signal from them.

**Warning:** The overall setup state was extracted from a preconfigured Fedora 22 machine. Configuration for your distro may be different.

### Requirements

- The host that is going to be used for virtualization needs to support I/O MMU. For Intel processors this is called VT-d and for AMD processors is called AMD-Vi. The instructions are made for Intel branded processors but the process should be very similar for AMD.
  - kernel &ge; 3.12
  - libvirt &ge; 1.1.3
  - kvm hypervisor

### Machine Configuration (Hypervisor)

#### Kernel Configuration

The kernel must be configured to support I/O MMU and to blacklist any driver that could be accessing the PCI’s that we want to use in our VMs. The parameter to enable I/O MMU is:

```
intel_iommu=on
```

We also need to tell the kernel to load the `vfio-pci` driver and blacklist the drivers for the selected cards. For example, for nvidia GPUs we can use these parameters:

```
rd.driver.pre=vfio-pci rd.driver.blacklist=nouveau
```
Loading vfio Driver in initrd

The modules for vfio must be added to initrd. The list of modules are `vfio vfio_iommu_type1 vfio_pci vfio_virqfd`. For example, if your system uses dracut add the file `/etc/dracut.conf.d/local.conf` with this line:

```bash
classic+="vfio vfio_iommu_type1 vfio_pci vfio_virqfd"
```

and regenerate initrd:

```
# dracut --force
```

Driver Blacklisting

The same blacklisting done in the kernel parameters must be done in the system configuration.

```bash
/etc/modprobe.d/blacklist.conf
```

- `blacklist nouveau`
- `blacklist lbm-nouveau`
- `options nouveau modeset=0`
- `alias nouveau off`
- `alias lbm-nouveau off`

Alongside this configuration vfio driver should be loaded passing the id of the PCI cards we want to attach to VMs. For example, for nvidia Grid K2 GPU we pass the id `10de:11bf`. File `/etc/modprobe.d/local.conf`:

```bash
options vfio-pci ids=10de:11bf
```

vfio Device Binding

I/O MMU separates PCI cards into groups to isolate memory operation between devices and VMs. To add the cards to vfio and assign a group to them we can use the scripts shared in the aforementioned web page.

This script binds a card to vfio. It goes into `/usr/local/bin/vfio-bind`:

```bash
#!/bin/sh
modprobe vfio-pci
do
vendor=$(cat /sys/bus/pci/devices/$dev/vendor)
device=$(cat /sys/bus/pci/devices/$dev/device)
if [ -e /sys/bus/pci/devices/$dev/driver ]; then
  echo $dev > /sys/bus/pci/devices/$dev/driver/unbind
fi
echo $vendor $device > /sys/bus/pci/drivers/vfio-pci/new_id
done
```

The configuration goes into `/etc/sysconfig/vfio-bind`. The cards are specified with PCI addresses. Addresses can be retrieved with `lspci` command. Make sure to prepend the domain that is usually `0000`. For example:

```bash
DEVICES="0000:04:00.0 0000:05:00.0 0000:84:00.0 0000:85:00.0"
```

Here is a systemd script that executes the script. It can be written to `/etc/systemd/system/vfio-bind.service` and enabled:

```bash
[Unit]
Description=binds devices to vfio-pci
After=syslog.target
```

3.3. KVM Driver
[Service]
EnvironmentFile=/etc/sysconfig/vfio-bind
Type=oneshot
RemainAfterExit=yes
ExecStart=/usr/local/bin/vfio-bind $DEVICES

[Install]
WantedBy=multi-user.target

qemu Configuration

Now we need to give qemu access to the vfio devices for the groups assigned to the PCI cards. We can get a list of PCI cards and its I/O MMU group using this command:

```
# find /sys/kernel/iommu_groups/ -type l
```

In our example our cards have the groups 45, 46, 58 and 59 so we add this configuration to /etc/libvirt/qemu.conf:

```bash
cgroup_device_acl = [
    "/dev/null", "/dev/full", "/dev/zero",
    "/dev/random", "/dev/urandom",
    "/dev/ptmx", "/dev/kvm", "/dev/kqemu",
    "/dev/rtc", "/dev/hpet", "/dev/vfio/vfio",
    "/dev/vfio/45", "/dev/vfio/46", "/dev/vfio/58",
    "/dev/vfio/59"
]
```

Driver Configuration

The only configuration that is needed is the filter for the monitoring probe that gets the list of PCI cards. By default the probe lists all the cards available in a host. To narrow the list a filter configuration can be changed in /var/lib/one/remotes/im/kvm-probes.d/pci.rb and set a list with the same format as lspci:

```bash
# This variable contains the filters for PCI card monitoring. The format
# is the same as lspci and several filters can be added separated by commas.
# A nil filter will retrieve all PCI cards.
#
# From lspci help:
# -d [<vendor>]:[<device>]:[<class>]
#
# For example
#
# FILTER = ':0300' # all VGA cards
# FILTER = '10de:0300' # all NVIDIA VGA cards
# FILTER = '10de:11bf:0300' # only GK104GL [GRID K2]
# FILTER = '8086:0300,::0106' # all Intel VGA cards and any SATA controller
```

Usage

The basic workflow is to inspect the host information, either in the CLI or in Sunstone, to find out the available PCI devices, and to add the desired device to the template. PCI devices can be added by specifying VENDOR, DEVICE and CLASS, or simply CLASS. Note that OpenNebula will only deploy the VM in a host with the available PCI device. If no hosts match, an error message will appear in the Scheduler log.
CLI

A new table in `onehost show` command gives us the list of PCI devices per host. For example:

PCI DEVICES

<table>
<thead>
<tr>
<th>VM ADDR</th>
<th>VENDOR</th>
<th>TYPE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00.0 8086:0a04:0600</td>
<td>8086</td>
<td>DRAM Controller</td>
<td>Haswell-ULT DRAM Controller</td>
</tr>
<tr>
<td>00:02.0 8086:0a16:0300</td>
<td>8086</td>
<td>Integrated Graphics Controller</td>
<td>Haswell-ULT Integrated Graphics Controller</td>
</tr>
<tr>
<td>123 00:03.0 8086:0a0c:0403</td>
<td>8086</td>
<td>HD Audio Controller</td>
<td>Haswell-ULT HD Audio Controller</td>
</tr>
<tr>
<td>00:14.0 8086:9c31:0c03</td>
<td>8086</td>
<td>USB xHCI HC</td>
<td>8 Series USB xHCI HC</td>
</tr>
<tr>
<td>00:16.0 8086:9c3a:0780</td>
<td>8086</td>
<td>HECI #0</td>
<td>8 Series HECI #0</td>
</tr>
<tr>
<td>00:1b.0 8086:9c20:0403</td>
<td>8086</td>
<td>Audio Controller</td>
<td>8 Series HD Audio Controller</td>
</tr>
<tr>
<td>00:1c.0 8086:9c10:0604</td>
<td>8086</td>
<td>PCI Express Root Port 1</td>
<td>8 Series PCI Express Root Port 1</td>
</tr>
<tr>
<td>00:1c.2 8086:9c14:0604</td>
<td>8086</td>
<td>PCI Express Root Port 3</td>
<td>8 Series PCI Express Root Port 3</td>
</tr>
<tr>
<td>00:1d.0 8086:9c26:0c03</td>
<td>8086</td>
<td>USB EHCI #1</td>
<td>8 Series USB EHCI #1</td>
</tr>
<tr>
<td>00:1f.0 8086:9c43:0601</td>
<td>8086</td>
<td>LPC Controller</td>
<td>8 Series LPC Controller</td>
</tr>
<tr>
<td>00:1f.2 8086:9c03:0106</td>
<td>8086</td>
<td>SATA Controller 1 [AHCI mode]</td>
<td>8 Series SATA Controller 1 [AHCI mode]</td>
</tr>
<tr>
<td>00:1f.3 8086:9c22:0c05</td>
<td>8086</td>
<td>SMBus Controller</td>
<td>8 Series SMBus Controller</td>
</tr>
<tr>
<td>02:00.0 8086:08b1:0280</td>
<td>8086</td>
<td>Wireless 7260</td>
<td>Wireless 7260</td>
</tr>
</tbody>
</table>

- **VM**: The VM ID using that specific device. Empty if no VMs are using that device.
- **ADDR**: PCI Address.
- **TYPE**: Values describing the device. These are VENDOR:DEVICE:CLASS. These values are used when selecting a PCI device do to passthrough.
- **NAME**: Name of the PCI device.

To make use of one of the PCI devices in a VM a new option can be added selecting which device to use. For example this will ask for a *Haswell-ULT HD Audio Controller*:

```json
PCI = [  
    VENDOR = "8086",  
    DEVICE = "0a0c",  
    CLASS = "0403"  
]
```

The device can be also specified without all the type values. For example, to get any PCI Express Root Ports this can be added to a VM template:

```json
PCI = [  
    CLASS = "0604"  
]
```

More than one **PCI** options can be added to attach more than one PCI device to the VM.

Sunstone

In Sunstone the information is displayed in the **PCI** tab:
To add a PCI device to a template, select the Other tab:

3.3.7 Enabling QEMU Guest Agent

QEMU Guest Agent allows the communication of some actions with the guest OS. This agent uses a virtio serial connection to send and receive commands. One of the interesting actions is that it allows to freeze the filesystem before doing an snapshot. This way the snapshot won’t contain half written data. Filesystem freeze will only be used with CEPH and qcow2 storage drivers.

The agent package needed in the Guest OS is available in most distributions. Is called `qemu-guest-agent` in most of them. If you need more information you can follow these links:

To enable the communication channel with the guest agent this line must be present in `/etc/one/vmm_exec/vmm_exec_kvm.conf`:

```
RAW = "<devices><channel type='unix'><source mode='bind'/><target type='virtio' name='org.qemu.guest_agent.0'/></channel></devices>
```

### 3.3.8 Importing VMs

VMs running on KVM hypervisors that were not launched through OpenNebula can be imported in OpenNebula. It is important to highlight that, besides the limitations explained in the host guide, the “Poweroff” operation is not available for these imported VMs in KVM.

### 3.3.9 Multiple Actions per Host

**Warning:** This feature is experimental. Some modifications to the code must be done before this is a recommended setup.

By default the drivers use a unix socket to communicate with the libvirt daemon. This method can only be safely used by one process at a time. To make sure this happens the drivers are configured to send only one action per host at a time. For example, there will be only one deployment done per host at a given time.

This limitation can be solved configuring libvirt to accept TCP connections and OpenNebula to use this communication method.

#### Libvirt configuration

Here is described how to configure libvirtd to accept unencrypted and unauthenticated TCP connections in a CentOS 7 machine. For other setup check your distribution and libvirt documentation.

Change the file `/etc/libvirt/libvirtd-conf` in each of the hypervisors and make sure that these parameters are set and have the following values:

```
listen_tls = 0
listen_tcp = 1
tcp_port = "16509"
auth_tcp = "none"
```

You will also need to modify `/etc/sysconfig/libvirtd` and uncomment this line:

```
LIBVIRT_D_ARGS="--listen"
```

After modifying these files the libvirt daemon must be restarted:

```
$ sudo systemctl restart libvirtd
```

#### OpenNebula configuration

The VMM driver must be configured so it allows more than one action to be executed per host. This can be done adding the parameter `-p` to the driver executable. This is done in `/etc/one/oned.conf` in the VM_MAD configuration section:

3.3. KVM Driver
VM_MAD = {
    name = "kvm",
    executable = "one_vmm_exec",
    arguments = "-t 15 -r 0 kvm -p",
    default = "vmm_exec/vmm_exec_kvm.conf",
    type = "kvm"
}

Change the file `/var/lib/one/remotes/vmm/kvm/kvmrc` so set a TCP endpoint for libvirt communication:
```
export LIBVIRT_URI=qemu+tcp://localhost/system
```

The scheduler configuration should also be changed to let it deploy more than one VM per host. The file is located at `/etc/one/sched.conf` and the value to change is MAX_HOST. For example, to let the scheduler submit 10 VMs per host use this line:
```
MAX_HOST = 10
```

After this update the remote files in the nodes and restart opennebula:
```
$ onehost sync --force
$ sudo systemctl restart opennebula
```

### 3.3.10 Troubleshooting

**image magic is incorrect**

When trying to restore the VM from a suspended state this error is returned:
```
libvirtd1021: operation failed: image magic is incorrect
```

It can be fixed by applying:
```
options kvm_intel nested=0
options kvm_intel emulate_invalid_guest_state=0
options kvm ignore_msrs=1
```

### 3.4 VMware Drivers

The **VMware Drivers** enable the management of an OpenNebula cloud based on VMware ESX 5.5 hypervisors. They use libvirt and direct API calls using RbVmomI to invoke the Virtual Infrastructure SOAP API exposed by the VMware hypervisors, and feature a simple configuration process that will leverage the stability, performance and feature set of any existing VMware based OpenNebula cloud.

#### 3.4.1 Requirements

In order to use the **VMware Drivers**, some software dependencies have to be met:

- **libvirt**: At the OpenNebula front-end, libvirt is used to access the VMware hypervisors, so it needs to be installed with ESX support. We recommend version 0.8.3 or higher, which enables interaction with the vCenter VMware product, required to use vMotion. This will be installed by the OpenNebula package.
- **rbvmomi**: Also at the OpenNebula front-end, the rbvmomi gem needs to be installed. This will be installed by the OpenNebula package or the install_gems script.
• **ESX ESX 5.5**: At least one VMware hypervisor needs to be installed. Further configuration for the `DATASTORE` is needed, and it is explained in the TM part of the Configuration section.

**Optional Requirements.** To enable some OpenNebula features you may need:

• **vMotion**: VMware’s vMotion capabilities allows to perform live migration of a Virtual Machine between two ESX hosts, allowing for load balancing between cloud worker nodes without downtime in the migrated virtual machine. In order to use this capability, the following requisites have to be meet:
  – **Shared storage** between the source and target host, mounted in both hosts as the same `DATASTORE` (we are going to assume it is called “images” in the rest of this document)
  – A **datacenter** created in the vCenter server that includes all ESX hosts between which Virtual Machines want to be live migrated (we are going to assume it is called “onecenter” in the rest of this document).
  – A **user** created in vCenter with the same username and password than the ones in the ESX hosts, with administrator permissions.

• **For VNC to work properly**:
  – Please install **VMware Tools (for Windows)** or **Open Virtual Machine Tools** (for *nix) in the guest OS.
  – To enable VNC functionality, repeat the following procedure for each ESX:
    * In the vSphere client proceed to Home -> Inventory -> Hosts and Clusters
    * Select the ESX host, Configuration tab and select Security Profile in the Software category
    * In the Firewall section, select Edit. Enable GDB Server, then click OK
    * Make sure that the ESX hosts are reachable from the OpenNebula front-end

**Warning:** When the vCenter is configured all the actions on VMs go through the vCenter. It does not add any feature but vMotion (live migration) compared to direct ESX communication. The storage commands still use ssh connection to the ESX hosts.

**Warning:** Please note that the libvirt version shipped with some linux distribution does not include ESX support. In these cases it may be needed to recompile the libvirt package with the –with-esx option.

### 3.4.2 Considerations & Limitations

• Only one vCenter can be used for livemigration.

• Datablock images and volatile disk images will be always created without format, and thus have to be formatted by the guest.

• In order to use the **attach/detach** functionality, the original VM must have at least one SCSI disk, and the disk to be attached/detached must be placed on a SCSI bus (ie, “sd” as `DEV_PREFIX`).

• The ESX hosts need to be properly licensed, with write access to the exported API (as the Evaluation license does).
3.4.3 VMware Configuration

Users & Groups

The creation of a user in the VMware hypervisor is recommended. Go to the Users & Group tab in the VI Client, and create a new user (for instance, “oneadmin”) with the same UID and username as the oneadmin user executing OpenNebula in the front-end. Please remember to give full permissions to this user (Permissions tab).

Warning: After registering a datastore, make sure that the “oneadmin” user can write in said datastore (this is not needed if the “root” user is used to access the ESX). In case “oneadmin” cannot write in “/vmfs/volumes/<ds_id>”, then permissions need to be adjusted. This can be done in various ways, the recommended one being:

- Add “oneadmin” to the “root” group using the Users & Group tab in the VI Client
- $ chmod g+w /vmfs/volumes/<ds_id> in the ESX host

SSH Access

SSH access from the front-end to the ESX hosts is required (or, at least, they need it to unlock all the functionality of OpenNebula). To ensure so, please remember to click the “Grant shell access to this user” checkbox when creating the oneadmin user.

The access via SSH needs to be passwordless. Please follow the next steps to configure the ESX node:

- login to the esx host (ssh <esx-host>)
More information on passwordless ssh connections here.

**Tools Setup**

- In order to enable all the functionality of the drivers, several short steps remain:

  ```
  $ su
  $ chmod +s /sbin/vmkfstools
  ```

  - In order to use the **attach/detach functionality** for VM disks, some extra configuration steps are needed in the ESX hosts.

    ```
    $ su
    $ chmod +s /bin/vim-cmd
    ```

  - In order to use the **dynamic network mode** for VM disks, some extra configuration steps are needed in the ESX hosts.

    ```
    $ su
    $ chmod +s /sbin/esxcfg-vswitch
    ```

**Persistency**

Persistency of the ESX filesystem has to be handled with care. Most of ESX 5 files reside in an in-memory filesystem, meaning faster access and also non persistency across reboots, which can be inconvenient at the time of managing a ESX farm for a OpenNebula cloud.

Here is a recipe to make the configuration needed for OpenNebula persistent across reboots. The changes need to be done as root.

```bash
# vi /etc/rc.local
## Add this at the bottom of the file
mkdir /etc/ssh/keys-oneadmin
cat > /etc/ssh/keys-oneadmin/authorized_keys << _SSH_KEYS_
ssh-rsa <really long string with oneadmin's ssh public key>
_SSH_KEYS_
chmod 600 /etc/ssh/keys-oneadmin/authorized_keys
chmod +s /sbin/vmkfstools /bin/vim-cmd
chmod 755 /etc/ssh/keys-oneadmin
chown oneadmin /etc/ssh/keys-oneadmin/authorized_keys
# /sbin/auto-backup.sh
```

This information was based on this blog post.
Storage

There are additional configuration steps regarding storage. Please refer to the VMware Storage Model guide for more details.

Networking

Networking can be used in two different modes: **pre-defined** (to use pre-defined port groups) or **dynamic** (to dynamically create port groups and VLAN tagging). Please refer to the VMware Networking guide for more details.

3.4.4 OpenNebula Configuration

OpenNebula Daemon

- In order to configure OpenNebula to work with the VMware drivers, the following sections need to be uncommented or added in the /etc/one/oned.conf file.

```bash
# VMware Virtualization Driver Manager Configuration
VM_MAD = [
    name = "vmware",
    executable = "one_vmm_sh",
    arguments = "-t 15 -r 0 vmware -s sh",
    default = "vmm_exec/vmm_exec_vmware.conf",
    type = "vmware"
]

# VMware Information Driver Manager Configuration
IM_MAD = [
    name = "vmware",
    executable = "one_im_sh",
    arguments = "-c -t 15 -r 0 vmware"
]

SCRIPTS_REMOTE_DIR=/tmp/one
```

VMware Drivers

The configuration attributes for the VMware drivers are set in the /etc/one/vmwarerc file. In particular the following values can be set:

<table>
<thead>
<tr>
<th>SCHEDULED OPTIONS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>:libvirt_uri</td>
<td>used to connect to VMware through libvirt. When using VMware Server, the connection string set under LIBVIRT_URI needs to have its prefix changed from esx to gss</td>
</tr>
<tr>
<td>:username</td>
<td>username to access the VMware hypervisor</td>
</tr>
<tr>
<td>:password</td>
<td>password to access the VMware hypervisor</td>
</tr>
<tr>
<td>:datacenter</td>
<td>(only for vMotion) name of the datacenter where the hosts have been registered.</td>
</tr>
<tr>
<td>:vcenter</td>
<td>(only for vMotion) name or IP of the vCenter that manage the ESX hosts</td>
</tr>
<tr>
<td>:reserve_memory_in_disk</td>
<td>Y to instruct ESX to create vswp files with disk reservation for memory, N for the vice versa</td>
</tr>
</tbody>
</table>
Example of the configuration file:

```yaml
:libvirt_uri: "esx://@HOST@/?no_verify=1&auto_answer=1"
:username: "oneadmin"
:password: "mypass"
:datacenter: "ha-datacenter"
:vcenter: "London-DC"
```

**Warning:** Please be aware that the above rc file, in stark contrast with other rc files in OpenNebula, uses yaml syntax, therefore please input the values between quotes.

### VMware Physical Hosts

The physical hosts containing the VMware hypervisors need to be added with the appropriate **VMware Drivers**. If the box running the VMware hypervisor is called, for instance, `esx-host`, the host would need to be registered with the following command (dynamic netwotk mode):

```bash
$ onehost create esx-host -i vmware -v vmware -n vmware
```

or for pre-defined networking

```bash
$ onehost create esx-host -i vmware -v vmware -n dummy
```

### 3.4.5 Usage

#### Images

To register an existing VMware disk in an OpenNebula image catalog you need to:

- Place all the `.vmdk` files that conform a disk (they can be easily spotted, there is a main `<name-of-the-image>.vmdk` file, and various `<name-of-the-image-sXXX.vmdk` flat files) in the same directory, with no more files than these.

- Afterwards, an image template needs to be written, using the the absolut path to the directory as the `PATH` value. For example:

```yaml
NAME = MyVMwareDisk
PATH =/absolute/path/to/disk/folder
TYPE = OS
```

**Warning:** To register a `.iso` file with type CDROM there is no need to create a folder, just point with `PATH` to the absolute path of the `.iso` file.

**Warning:** In order to register a VMware disk through Sunstone, create a zip compressed tarball (.tar.gz) and upload that (it will be automatically decompressed in the datastore). Please note that the tarball is only of the folder with the `.vmdk` files inside, no extra directories can be contained in that folder.

Once registered the image can be used as any other image in the OpenNebula system as described in the Virtual Machine Images guide.
Datablocks & Volatile Disks

Datablock images and volatile disks will appear as a raw devices on the guest, which will then need to be formatted. The FORMAT attribute is compulsory, possible values (more info on this here) are:

- vmdk_thin
- vmdk_zeroedthick
- vmdk_eagerzeroedthick

Virtual Machines

The following attributes can be used for VMware Virtual Machines:

- GuestOS: This parameter can be used in the OS section of the VM template. The os-identifier can be one of this list.

  `OS=[GUESTOS=<os-identifier>]`

- PCIBridge: This parameter can be used in the FEATURES section of the VM template. The `<bridge-number>` is the number of PCI Bridges that will be available in the VM (that is, 0 means no PCI Bridges, 1 means PCI Bridge with ID = 0 present, 2 means PCI Bridges with ID = 0,1 present, and so on).

  `FEATURES=[PCIBRIDGE=<bridge-number>]`

3.4.6 Custom VMX Attributes

You can add metadata straight to the .vmx file using RAW/DATA_VMX. This comes in handy to specify for example a specific guestOS type, more info here.

Following the two last sections, if we want a VM of guestOS type “Windows 7 server 64bit”, with disks plugged into a LSI SAS SCSI bus, we can use a template like:

```
NAME = myVMwareVM
CPU = 1
MEMORY = 256

DISK = [IMAGE_ID="7"]
NIC = [NETWORK="public"]
RAW=[
   DATA="<devices><controller type='scsi' index='0' model='lsisas1068'/></devices>",
   DATA_VMX="pciBridge0.present = "TRUE"
   pciBridge4.present = "TRUE"
   pciBridge4.virtualDev = "TRUE"
   pciBridge7.functions = "8"
   guestOS = "windows7srv-64"
   TYPE="vmware"
]
```

3.4.7 Tuning & Extending

The VMware Drivers consists of three drivers, with their corresponding files:

- VMM Driver
  - `/var/lib/one/remotes/vmm/vmware`: commands executed to perform actions.

- IM Driver
• **TM Driver**
  - `/usr/lib/one/tm_commands`: commands executed to perform transfer actions.

And the following driver configuration files:

• **VMM Driver**
  - `/etc/one/vmm_exec/vmm_exec_vmware.conf`: This file is home for default values for domain definitions (in other words, OpenNebula templates). For example, if the user wants to set a default value for CPU requirements for all of their VMware domain definitions, simply edit the `/etc/one/vmm_exec/vmm_exec_vmware.conf` file and set a CPU=0.6 into it. Now, when defining a template to be sent to a VMware resource, the user has the choice of “forgetting” to set the CPU requirement, in which case it will default to 0.6.

It is generally a good idea to place defaults for the VMware-specific attributes, that is, attributes mandatory for the VMware hypervisor that are not mandatory for other hypervisors. Non mandatory attributes for VMware but specific to them are also recommended to have a default.

• **TM Driver**
  - `/etc/one/tm_vmware/tm_vmware.conf`: This files contains the scripts tied to the different actions that the TM driver can deliver. You can here deactivate functionality like the DELETE action (this can be accomplished using the dummy tm driver, dummy/tm_dummy.sh) or change the default behavior.

More generic information about drivers:

• Virtual Machine Manager drivers reference
• Transfer Manager driver reference

### 3.5 VMware vCenter Drivers

OpenNebula seamlessly integrates vCenter virtualized infrastructures so leveraging the advanced features such as vMotion, HA or DRS scheduling provided by the VMware vSphere product family. On top of it, OpenNebula exposes a multi-tenant, cloud-like provisioning layer, including features like virtual data centers, datacenter federation or hybrid cloud computing to connect in-house vCenter infrastructures with public clouds. You also take a step toward liberating your stack from vendor lock-in.

These drivers are for companies that want to keep VMware management tools, procedures and workflows. For these companies, throwing away VMware and retooling the entire stack is not the answer. However, as they consider moving beyond virtualization toward a private cloud, they can choose to either invest more in VMware, or proceed on a tactically challenging but strategically rewarding path of open.

The OpenNebula - vCenter combination allows you to deploy advanced provisioning infrastructures of virtualized resources. In this guide you’ll learn how to configure OpenNebula to access one or more vCenters and set-up VMware-based virtual machines.

#### 3.5.1 Overview and Architecture

The VMware vCenter drivers enable OpenNebula to access one or more vCenter servers that manages one or more ESX Clusters. Each ESX Cluster is presented in OpenNebula as an aggregated hypervisor, i.e. as an OpenNebula host. Note that OpenNebula scheduling decisions are therefore made at ESX Cluster level, vCenter then uses the DRS component to select the actual ESX host and Datastore to deploy the Virtual Machine.
As the figure shows, OpenNebula components see two hosts where each represents a cluster in a vCenter. You can further group these hosts into OpenNebula clusters to build complex virtual data centers for your user groups in OpenNebula.

**Note:** Together with the ESX Cluster hosts you can add other hypervisor types or even hybrid cloud instances like Microsoft Azure or Amazon EC2.

Virtual Machines are deployed from VMware VM Templates that must exist previously in vCenter. There is a one-to-one relationship between each VMware VM Template and the equivalent OpenNebula Template. Users will then instantiate the OpenNebula Templates where you can easily build from any provisioning strategy (e.g. access control, quota...).

Networking is handled by creating Virtual Network representations of the vCenter networks. OpenNebula additionally can handle on top of these networks three types of Address Ranges: Ethernet, IPv4 and IPv6. This networking
information can be passed to the VMs through the contextualization process.

Therefore there is no need to convert your current Virtual Machines or import/export them through any process; once ready just save them as VM Templates in vCenter, following this procedure.

Note: After a VM Template is cloned and booted into a vCenter Cluster it can access VMware advanced features and it can be managed through the OpenNebula provisioning portal -to control the lifecycle, add/remove NICs, make snapshots- or through vCenter (e.g. to move the VM to another datastore or migrate it to another ESX). OpenNebula will poll vCenter to detect these changes and update its internal representation accordingly.

### 3.5.2 Requirements

The following must be met for a functional vCenter environment:

- vCenter 5.5 and/or 6.0, with at least one cluster aggregating at least one ESX 5.5 and/or 5.5 host.

- VMware tools are needed in the guestOS to enable several features (contextualization and networking feedback). Please install VMware Tools (for Windows) or Open Virtual Machine Tools (for *nix) in the guestOS.

- Define a vCenter user for OpenNebula. This vCenter user (let’s call her oneadmin) needs to have access to the ESX clusters that OpenNebula will manage. In order to avoid problems, the hassle free approach is to declare this oneadmin user as Administrator. In production environments though, it may be needed to perform a more fine grained permission assignment (please note that the following permissions related to operations are related to the use that OpenNebula does with this operations):
<table>
<thead>
<tr>
<th>vCenter Operation</th>
<th>Privileges</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloneVM_Task</td>
<td>None</td>
<td>Creates a clone of a particular VM</td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Interact.SetCDMedia</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Interact.SetFloppyMedia</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.Rename</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.Annotation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.AddExistingDisk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.RemoveDisk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.CPUCount</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.Memory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.RawDevice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.AddRemoveDevice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.EmbedDevice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.HostUSBDevice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.DiskExtend</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.ChangeTracking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DVPortgroup.CanUse VIRTUALMACHINE.CONFIG.RawDevice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.AddExistingDisk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VirtualMachine.Config.AddNewDisk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Datastore.AllocateSpace</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network.Assign</td>
<td></td>
</tr>
<tr>
<td>Destroy_Task</td>
<td>VirtualMachine.Inventory.Delete</td>
<td>Deletes a VM (including disks)</td>
</tr>
<tr>
<td>SuspendVM_Task</td>
<td>VirtualMachine.Interact.Suspend</td>
<td>Suspends a VM</td>
</tr>
<tr>
<td>RebootGuest</td>
<td>VirtualMachine.Interact.Reset</td>
<td>Reboots VM's guest Operating System</td>
</tr>
<tr>
<td>RebootGuest</td>
<td>VirtualMachine.Interact.Reset</td>
<td>Reboots VM's guest Operating System</td>
</tr>
<tr>
<td>RevertToSnapshot_Task</td>
<td>VirtualMachine.State.RevertToSnapshot</td>
<td>Revers a virtual machine to a particular snapshot</td>
</tr>
</tbody>
</table>

**Note:** For security reasons, you may define different users to access different ESX Clusters. A different user can defined in OpenNebula per ESX cluster, which is encapsulated in OpenNebula as an OpenNebula host.

- All ESX hosts belonging to the same ESX cluster to be exposed to OpenNebula **must** share one datastore among them.
• The ESX cluster should have DRS enabled. DRS is not required but it is recommended. OpenNebula does not schedule to the granularity of ESX hosts, DRS is needed to select the actual ESX host within the cluster, otherwise the VM will be launched in the ESX where the VM template has been created.

• Save as VMs Templates those VMs that will be instantiated through the OpenNebula provisioning portal
• To enable VNC functionality, repeat the following procedure for each ESX:
  – In the vSphere client proceed to Home -> Inventory -> Hosts and Clusters
  – Select the ESX host, Configuration tab and select Security Profile in the Software category
  – In the Firewall section, select Edit. Enable GDB Server, then click OK
  – Make sure that the ESX hosts are reachable from the OpenNebula front-end

Important: OpenNebula will NOT modify any vCenter configuration.

3.5.3 Considerations & Limitations

• Unsupported Operations: The following operations are NOT supported on vCenter VMs managed by OpenNebula, although they can be performed through vCenter:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>attach_disk</td>
<td>Action of attaching a new disk to a running VM</td>
</tr>
<tr>
<td>detach_disk</td>
<td>Action of detaching a new disk to a running VM</td>
</tr>
<tr>
<td>migrate</td>
<td>VMs cannot be migrated between ESX clusters</td>
</tr>
</tbody>
</table>

• No Security Groups: Firewall rules as defined in Security Groups cannot be enforced in vCenter VMs.

• There is a known issue regarding VNC ports, preventing VMs with ID 89 to work correctly through VNC. This is being addressed [here](#).

• OpenNebula treats snapshots a tad different from VMware. OpenNebula assumes that they are independent, whereas VMware builds them incrementally. This means that OpenNebula will still present snapshots that are no longer valid if one of their parent snapshots are deleted, and thus revert operations applied upon them will fail.

• No files in context: Passing entire files to VMs is not supported, but all the other CONTEXT sections will be honored

• Cluster name cannot contain spaces

• vCenter credential password cannot have more than 22 characters

3.5.4 Configuration

OpenNebula Configuration

There are a few simple steps needed to configure OpenNebula so it can interact with vCenter:

Step 1: Check connectivity

The OpenNebula front-end needs network connectivity to all the vCenters that it is supposed to manage.

Additionaly, to enable VNC access to the spawned Virtual Machines, the front-end also needs network connectivity to all the ESX hosts

Step 2: Enable the drivers in oned.conf

3.5. VMware vCenter Drivers
In order to configure OpenNebula to work with the vCenter drivers, the following sections need to be uncommented or added in the /etc/one/oned.conf file:

```
# vCenter Information Driver Manager Configuration
# -r number of retries when monitoring a host
# -t number of threads, i.e. number of hosts monitored at the same time

IM_MAD = [
    name = "vcenter",
    executable = "one_im_sh",
    arguments = "-c -t 15 -r 0 vcenter"
]
```

```
# vCenter Virtualization Driver Manager Configuration
# -r number of retries when monitoring a host
# -t number of threads, i.e. number of hosts monitored at the same time

VM_MAD = [
    name = "vcenter",
    executable = "one_vmm_sh",
    arguments = "-t 15 -r 0 vcenter -s sh",
    type = "xml"
]
```

Step 3: Importing vCenter Clusters

OpenNebula ships with a powerful CLI tool to import vCenter clusters, VM Templates, Networks and running VMs. The tools is self-explanatory, just set the credentials and IP to access the vCenter host and follow on screen instructions.

A sample section follows:

```
$ onehost list
ID  NAME    CLUSTER   RVM  ALLOCATED_CPU  ALLOCATED_MEM  STAT
0   clusterA  -       -       -           -              -init
1   clusterB  -       -       -           -              -init

$ onevcenter hosts --vcenter <vcenter-host> --vuser <vcenter-username> --vpass <vcenter-password>
Connecting to vCenter: <vcenter-host>...done!
Exploring vCenter resources...done!
Do you want to process datacenter Development [y/n]? y
  * Import cluster clusterA [y/n]? y
    OpenNebula host clusterA with id 0 successfully created.

  * Import cluster clusterB [y/n]? y
    OpenNebula host clusterB with id 1 successfully created.

$ onehost list
ID  NAME    CLUSTER   RVM  ALLOCATED_CPU  ALLOCATED_MEM  STAT
0   clusterA  -       -       -           -              -init
1   clusterB  -       -       -           -              -init

$ onehost list
ID  NAME    CLUSTER   RVM  ALLOCATED_CPU  ALLOCATED_MEM  STAT
0   clusterA  -       -       0 / 800 (0%)  0K / 16G (0%)  on
1   clusterB  -       -       -           -              -init

$ onehost list
ID  NAME    CLUSTER   RVM  ALLOCATED_CPU  ALLOCATED_MEM  STAT
0   clusterA  -       -       0 / 800 (0%)  0K / 16G (0%)  on
1   clusterB  -       -       0 / 1600 (0%)  0K / 16G (0%)  on
```

The following variables are added to the OpenNebula hosts representing ESX clusters:

### Operation

<table>
<thead>
<tr>
<th>Operation</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCENTER_HOST</td>
<td>hostname or IP of the vCenter host</td>
</tr>
<tr>
<td>VCENTER_USER</td>
<td>Name of the vCenter user</td>
</tr>
<tr>
<td>VCENTER_PASSWORD</td>
<td>Password of the vCenter user</td>
</tr>
</tbody>
</table>

**Note:** OpenNebula will create a special key at boot time and save it in /var/lib/one/.one/one_key. This key will be used as a private key to encrypt and decrypt all the passwords for all the vCenters that OpenNebula can access. Thus, the password shown in the OpenNebula host representing the vCenter is the original password encrypted with this special key.

The vCenter credentials that OpenNebula use can be confined into a Resource Pool, to allow only a fraction of the vCenter infrastructure to be used by OpenNebula users. The steps to confine OpenNebula users into a Resource Pool are:

- Create a new vCenter user
- Create a Resource Pool in vCenter and assign the subset of Datacenter hardware resources wanted to be exposed through OpenNebula
- Give vCenter user Resource Pool Administration rights over the Resource Pool
- Give vCenter user Resource Pool Administration (or equivalent) over the Datastores the VMs are going to be running on

Afterwards, these credentials can be used to add to OpenNebula the host representing the vCenter cluster. Add a new tag called VCENTER_RESOURCE_POOL to the host template representing the vCenter cluster (for instance, in the info tab of the host, or in the CLI), with the name of the resource pool.

---

**Step 4:**

### Importing vCenter VM Templates, Networks and running VMs

The same `onevcenter` tool can be used to import existing VM templates from the ESX clusters:

```
$ ./onevcenter templates --vcenter <vcenter-host> --vuser <vcenter-username> --vpass <vcenter-password>
```

Connecting to vCenter: `<vcenter-host>`...done!

Looking for VM Templates...done!

---

3.5. VMware vCenter Drivers 79
Do you want to process datacenter Development [y/n]? y

* VM Template found:
  - Name : ttyTemplate - clusterA
  - UUID : 421649f3-92d4-49b0-8b3e-358abd18b7dc
  - Cluster: clusterA
Import this VM template [y/n]? y
OpenNebula template 4 created!

* VM Template found:
  - Name : Template test - clusterB
  - UUID : 4216d5af-7c51-914c-33af-1747667c1019
  - Cluster: clusterB
Import this VM template [y/n]? y
OpenNebula template 5 created!

$ onetemplate list

<table>
<thead>
<tr>
<th>ID</th>
<th>USER</th>
<th>GROUP</th>
<th>NAME</th>
<th>REGTIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>ttyTemplate</td>
<td>09/22 11:54:33</td>
</tr>
<tr>
<td>5</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>Template test</td>
<td>09/22 11:54:35</td>
</tr>
</tbody>
</table>

$ onetemplate show 5

**TEMPLATE 5 INFORMATION**

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>USER</th>
<th>GROUP</th>
<th>REGISTRATION TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Template test - clusterB</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>09/22 11:54:35</td>
</tr>
</tbody>
</table>

**PERMISSIONS**

<table>
<thead>
<tr>
<th>OWNER</th>
<th>GROUP</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>um-</td>
<td>----</td>
<td>----</td>
</tr>
</tbody>
</table>

**TEMPLATE CONTENTS**

- CPU="1"
- MEMORY="512"
- PUBLIC_CLOUD=[
  - TYPE="vcenter",
  - VM_TEMPLATE="4216d5af-7c51-914c-33af-1747667c1019"
]  
- SCHED_REQUIREMENTS="NAME="devel"
- VCPU="1"

**Note:** VM Templates imported from vCenter will have their names appended with the name of the cluster where these resources belong in vCenter, to ease their identification within OpenNebula.

Moreover the same `onevcenter` tool can be used to import existing Networks and distributed vSwitches from the ESX clusters:

```
$ .onevcenter networks --vcenter <vcenter-host> --vuser <vcenter-username> --vpass <vcenter-password>

Connecting to vCenter: <vcenter-host>...done!
Looking for vCenter networks...done!
```

Do you want to process datacenter vOneDatacenter [y/n]? y
* Network found:
  - Name : MyvCenterNetwork - clusterA
  - Type : Port Group
  - Cluster : clusterA
Import this Network [y/n]? y
How many VMs are you planning to fit into this network [255]? 45
What type of Virtual Network do you want to create (IPv[4],IPv[6],[E]thernet) ? E
Please input the first MAC in the range [Enter for default]:
OpenNebula virtual network 29 created with size 45!

$ onevnet list
<table>
<thead>
<tr>
<th>ID</th>
<th>USER</th>
<th>GROUP</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>BRIDGE</th>
<th>LEASES</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>MyvCenterNetwork -</td>
<td>-</td>
<td>MyFakeNe</td>
<td>0</td>
</tr>
</tbody>
</table>

$ onevnet show 29
VIRTUAL NETWORK 29 INFORMATION
ID : 29
NAME : MyvCenterNetwork
USER : oneadmin
GROUP : oneadmin
CLUSTER : -
BRIDGE : MyvCenterNetwork
VLAN : No
USED LEASES : 0

PERMISSIONS
OWNER : um-
GROUP : ---
OTHER : ---

VIRTUAL NETWORK TEMPLATE
BRIDGE="MyvCenterNetwork"
PHYDEV=""
VCENTER_TYPE="Port Group"
VLAN="NO"
VLAN_ID=""

ADDRESS RANGE POOL
<table>
<thead>
<tr>
<th>AR</th>
<th>TYPE</th>
<th>SIZE</th>
<th>LEASES</th>
<th>MAC</th>
<th>IP</th>
<th>GLOBAL_PREFIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ETHER</td>
<td>45</td>
<td>0</td>
<td>02:00:97:7f:0f:87</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

LEASES
<table>
<thead>
<tr>
<th>AR</th>
<th>OWNER</th>
<th>MAC</th>
<th>IP</th>
<th>IP6_GLOBAL</th>
</tr>
</thead>
</table>

Note: Networks and Distributed vSwitches imported from vCenter will have their names appended with the name of the cluster where this resources belong in vCenter, to ease their identification within OpenNebula.

To import existing VMs, the ‘onehost importvm’ command can be used. VMs in running state can be imported, and also VMs defined in vCenter that are not in power.on state (this will import the VMs in OpenNebula as in the poweroff state).

$ onehost show 0
HOST 0 INFORMATION
ID : 0
NAME : MyvCenterHost
CLUSTER : -
[.....]

3.5. VMware vCenter Drivers
WILD VIRTUAL MACHINES

<table>
<thead>
<tr>
<th>NAME</th>
<th>IMPORT_ID</th>
<th>CPU</th>
<th>MEMORY</th>
</tr>
</thead>
<tbody>
<tr>
<td>RunningVM</td>
<td>4223cbb1-34a3-6a58-5ec7-a55db235ac64</td>
<td>1</td>
<td>1024</td>
</tr>
</tbody>
</table>

$ onehost importvm 0 RunningVM
$ onevm list

<table>
<thead>
<tr>
<th>ID</th>
<th>USER</th>
<th>GROUP</th>
<th>NAME</th>
<th>STAT</th>
<th>UCPU</th>
<th>UMEM</th>
<th>HOST</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>RunningVM</td>
<td>runn</td>
<td>0</td>
<td>590M</td>
<td>MyvCenterHost</td>
<td>0d 01h02</td>
</tr>
</tbody>
</table>

After a Virtual Machine is imported, their lifecycle (including creation of snapshots) can be controlled through OpenNebula. The following operations cannot be performed on an imported VM:

- Delete –recreate
- Undeploy (and Undeploy –hard)
- Migrate (and Migrate –live)
- Stop

Also, network management operations are present like the ability to attach/detach network interfaces, as well as capacity (CPU and MEMORY) resizing operations and VNC connections if the ports are opened before hand. The same import mechanism is available graphically through Sunstone for hosts, networks, templates and running VMs. vCenter hosts can be imported using the vCenter host create dialog, and Networks and VM Templates through the Import button in the Virtual Networks and Templates tab respectively. Running and Powered Off VMs can be imported through the WILDS tab in the Host info tab.
3.5. VMware vCenter Drivers

Note: running VMS can only be imported after the vCenter host has been successfully acquired.

Note: If you are running Sunstone using nginx/apache you will have to forward the following headers to be able to interact with vCenter, HTTP_X_VCENTER_USER, HTTP_X_VCENTER_PASSWORD and HTTP_X_VCENTER_HOST. For example in nginx you have to add the following attrs to the server section of your nginx file (underscores_in_headers on; proxy_pass_request_headers on;)

![Create Host](image-url)
3.5.5 Usage

VM Template definition

In order to manually create a VM Template definition in OpenNebula that represents a vCenter VM Template (or several, note the HOST attribute in PUBLIC_CLOUD vector attribute, which can be repeated on a single VM Template), the following attributes are needed:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Physical CPUs to be used by the VM. This does not have to relate to the CPUs used by the vCenter VM Template, OpenNebula will change the value accordingly</td>
</tr>
<tr>
<td>MEMORY</td>
<td>Physical Memory in MB to be used by the VM. This does not have to relate to the CPUs used by the vCenter VM Template, OpenNebula will change the value accordingly</td>
</tr>
<tr>
<td>NIC</td>
<td>Check VM template reference. Valid MODELs are: virtuale1000, virtuale1000e, virtualpcnet32, virtualsrovethernetcard, virtualvmxnetm, virtualvmxnet2, virtualvmxnet3.</td>
</tr>
<tr>
<td>GRAPHICS</td>
<td>Multi-value - Only VNC supported, check the VM template reference.</td>
</tr>
<tr>
<td>PUB-LIC_CLOUD</td>
<td>Multi-value. TYPE must be set to vcenter, VM_TEMPLATE must point to the uuid of the vCenter VM that is being represented and HOST must refer to the name of the vCenter Cluster (represented by a vOneCloud host) where the template is available</td>
</tr>
<tr>
<td>SCHED_REQUIREMENTS</td>
<td>name of the vCenter cluster where this VM Template can instantiated into a VM’. See VM Scheduling section for more details.</td>
</tr>
<tr>
<td>CONTEXT</td>
<td>All sections will be honored except FILES</td>
</tr>
<tr>
<td>KEEP_DISKS_ON_DONE</td>
<td>(Optional) Prevent OpenNebula from erasing the VM disks upon reaching the done state (either via shutdown or cancel)</td>
</tr>
</tbody>
</table>

You can find more information about contextualization in the vcenter Contextualization section.

After a VM Template is instantiated, the lifecycle of the resulting virtual machine (including creation of snapshots) can be controlled through OpenNebula. Also, all the operations available in the vCenter Admin view can be performed, including:

- network management operations like the ability to attach/detach network interfaces
- capacity (CPU and MEMORY) resizing
- VNC connectivity

The monitoring attributes retrieved from a vCenter VM are:

- ESX_HOST
- GUEST_IP
- GUEST_STATE
- VMWARETOOLS_RUNNING_STATUS
- VMWARETOOLS_VERSION
- VMWARETOOLS_VERSION_STATUS

Note: VMs will be named in vCenter as ‘one-<vid>-<VM Name>’, where <vid> is the id of the VM and VM Name is the name given to the VM in OpenNebula.

Virtual Network definition

Virtual Networks from vCenter can be represented using OpenNebula standard networks, taking into account that the BRIDGE of the Virtual Network needs to match the name of the Network defined in vCenter. OpenNebula supports both “Port Groups” and “Distributed Port Groups”.

84 Chapter 3. Virtualization
Virtual Networks in vCenter can be created using the vCenter web client, with any specific configuration like for instance VLANs. OpenNebula will use these networks with the defined characteristics, but it cannot create new Virtual Networks in vCenter, but rather only OpenNebula vnet representations of such Virtual Networks. OpenNebula additionally can handle on top of these networks three types of Address Ranges: Ethernet, IPv4 and IPv6.

vCenter VM Templates can define their own NICs, which OpenNebula cannot manage. However, any NIC added in the OpenNebula VM Template, or through the attach_nic operation, will be handled by OpenNebula, and as such it is subject to be detached and its information (IP, MAC, etc) is known by OpenNebula.

**VM Scheduling**

OpenNebula scheduler should only choose a particular OpenNebula host for a OpenNebula VM Template representing a vCenter VM Template, since it most likely only would be available in a particular vCenter cluster.

Since a vCenter cluster is an aggregation of ESX hosts, the ultimate placement of the VM on a particular ESX host would be managed by vCenter, in particular by the Distribute Resource Scheduler (DRS).

In order to enforce this compulsory match between a vCenter cluster and a OpenNebula/vCenter VM Template, add the following to the OpenNebula VM Template:

```
SCHED_REQUIREMENTS = "NAME="name of the vCenter cluster where this VM Template can instantiated into"
```

In Sunstone, a host abstracting a vCenter cluster will have an extra tab showing the ESX hosts that conform the cluster.

---

3.5.6 VM Template Cloning Procedure

OpenNebula uses VMware cloning VM Template procedure to instantiate new Virtual Machines through vCenter. From the VMware documentation:

- Deploying a virtual machine from a template creates a virtual machine that is a copy of the template. The new virtual machine has the virtual hardware, installed software, and other properties that are configured for the template.

A VM Template is tied to the host where the VM was running, and also the datastore(s) where the VM disks where placed. Due to shared datastores, vCenter can instantiate a VM Template in any of the hosts belonging to the same cluster as the original one.

OpenNebula uses several assumptions to instantiate a VM Template in an automatic way:

- **diskMoveType**: OpenNebula instructs vCenter to “move only the child-most disk backing. Any parent disk backings should be left in their current locations.”. More information [here](#)
- **Target resource pool**: OpenNebula uses the default cluster resource pool to place the VM instantiated from the VM template, unless VCENTER RESOURCE POOL variable defined in the OpenNebula host template
4.1 Networking Overview

Before diving into Network configuration in OpenNebula make sure that you’ve followed the steps described in the Networking section of the Installation guide.

When a new Virtual Machine is launched, OpenNebula will connect its network interfaces (defined in the NIC section of the template) to the bridge or physical device specified in the Virtual Network definition. This will allow the VM to have access to different networks, public or private.

The OpenNebula administrator must take into account that although this is a powerful setup, it should be complemented with mechanisms to restrict network access only to the expected Virtual Machines, to avoid situations in which an OpenNebula user interacts with another user’s VM. This functionality is provided through Virtual Network Manager drivers. The OpenNebula administrator may associate one of the following drivers to each Host, when the hosts are created with the `onehost command`:

- **dummy**: Default driver that doesn’t perform any network operation. Security Group rules are also ignored.
- **Security Groups**: Security Group rules are applied to filter specific traffic. Drivers based on Linux bridges (802.1Q, vxlan and etables) are prepared to work with the Security Groups driver.
- **802.1Q**: restrict network access through VLAN tagging, which also requires support from the hardware switches.
- **VXLAN**: implements VLANs using the VXLAN protocol that relies on a UDP encapsulation and IP multicast.
- **etables**: restrict network access through Etables rules. No special hardware configuration is required.
- **ovswitch**: restrict network access with Open vSwitch Virtual Switch.
- **VMware**: uses the VMware networking infrastructure to provide an isolated and 802.1Q compatible network for VMs launched with the VMware hypervisor.

Note that some of these drivers also create the bridging device in the hosts if needed.

The administrator must take into account the following matrix that shows the compatibility of the hypervisors with each networking driver:

<table>
<thead>
<tr>
<th>Hypervisor</th>
<th>Security Groups</th>
<th>Open vSwitch</th>
<th>802.1Q</th>
<th>VXLAN</th>
<th>etables</th>
<th>VMware</th>
</tr>
</thead>
<tbody>
<tr>
<td>KVM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Xen</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>VMware</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

The Virtual Network isolation is enabled with any of the 801.1Q, vxlan, etables, vmware or ovswitch drivers. Additionally the drivers based on Linux bridges (vxlan, 802.1Q and etables) can be combined with security groups driver to allow a regular OpenNebula user to filter TCP, UDP or ICMP traffic.
4.1.1 Tuning & Extending

Configuration

Some drivers have the ability to customize their behaviour by editing a configuration file. This file is located in 
/var/lib/one/remotes/vnm/OpenNebulaNetwork.conf.

Currently it supports the following options:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Driver</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start_vlan</td>
<td>802.1Q, vxlan, ovswitch, vmware</td>
<td>Configure the initial VLAN ID tag (corresponds to vnet ID = 0)</td>
</tr>
<tr>
<td>arp_cache_poisoning</td>
<td>ovswitch</td>
<td>Enable ARP Cache Poisoning Prevention Rules.</td>
</tr>
<tr>
<td>vxlan_mc</td>
<td>vxlan</td>
<td>Base multicast address for each VLAN. The multicast address is vxlan_mc + vlan_id</td>
</tr>
</tbody>
</table>

**Warning:** If this file is changed, please run onehost sync to deploy the file to all the nodes.

Customization of the Drivers

The network is dynamically configured in three different steps:

- **Pre**: Right before the hypervisor launches the VM.
- **Post**: Right after the hypervisor launches the VM.
- **Clean**: Right after the hypervisor shuts down the VM.

Each driver execute different actions (or even none at all) in these phases depending on the underlying switching fabric. Note that, if either Pre or Post fail, the VM will be shut down and will be placed in a FAIL state.

You can easily customize the behavior of the driver for your infrastructure by modifying the files in located in 
/var/lib/one/remotes/vnm. Each driver has its own folder that contains at least three programs pre, post and clean. These programs are executed to perform the steps described above.

Fixing Default Paths

The default paths for the binaries/executables used during the network configuration may change depending on the distro. OpenNebula ships with the most common paths, however these may be wrong for your particular distro. In that case, please fix the proper paths in the COMMANDS hash of /var/lib/one/remotes/vnm/command.rb:

```ruby
# Command configuration for common network commands. This CAN be adjusted
# to local installations. Any modification requires to sync the hosts with
# onehost sync command.
COMMANDS = {
  :ebtables => "sudo ebtables",
  :iptables => "sudo iptables",
  :brctl => "sudo brctl",
  :ip => "sudo ip",
  :virsh => "virsh -c qemu:///system",
  :xm => Configuration::get_xen_command,
  :ovs_vsctl=> "sudo ovs-vsctl",
  :ovs_ofctl=> "sudo ovs-ofctl",
  :lsmod => "lsmod",
  :ipset => "sudo ipset"
}
```
4.2 802.1Q VLAN

This guide describes how to enable Network isolation provided through host-managed VLANs. This driver will create a bridge for each OpenNebula Virtual Network and attach an VLAN tagged network interface to the bridge. This mechanism is compliant with IEEE 802.1Q.

The VLAN id will be the same for every interface in a given network, calculated by adding a constant to the network id. It may also be forced by specifying an VLAN_ID parameter in the Virtual Network template.

4.2.1 Requirements

A network switch capable of forwarding VLAN tagged traffic. The physical switch ports should be VLAN trunks.

4.2.2 Considerations & Limitations

This driver requires some previous work on the network components, namely the switches, to enable VLAN trunking in the network interfaces connected to the OpenNebula hosts. If this is not activated the VLAN tags will not get trough and the network will behave erratically.

4.2.3 Configuration

Hosts Configuration

- The `sudoers` file must be configured so `oneadmin` can execute `brctl` and `ip` in the hosts.
- Hosts must have the module `8021q` loaded.

To enable VLAN (802.1Q) support in the kernel, one must load the 8021q module:

```bash
$ modprobe 8021q
```

If the module is not available, please refer to your distribution’s documentation on how to install it.

OpenNebula Configuration

To enable this driver, use `802.1Q` as the Virtual Network Manager driver parameter when the hosts are created with the `onehost` command:

```bash
$ onehost create host01 -i kvm -v kvm -n 802.1Q
```

802.1Q Options

It is possible specify the start VLAN ID by editing `/var/lib/one/remotes/vnm/OpenNebulaNetwork.conf`. This driver accepts an `MTU` attribute that will be used when creating the tagged interface and bridge.
Driver Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre</td>
<td>Creates a V AN interface through PHYDEV, creates a bridge (if needed) and attaches the vxlan device.</td>
</tr>
<tr>
<td>Post</td>
<td>When the VM is associated to a security group, the corresponding iptables rules are applied.</td>
</tr>
<tr>
<td>Clean</td>
<td>It doesn’t do anything. The VLAN tagged interface and bridge are kept in the Host to speed up future VMs</td>
</tr>
</tbody>
</table>

4.2.4 Usage

The driver will be automatically applied to every Virtual Machine deployed in the Host. However, this driver requires a special configuration in the Virtual Network template: only the virtual networks with the attribute VLAN set to YES will be isolated. The attribute PHYDEV must be also defined, with the name of the physical network device that will be attached to the bridge. The BRIDGE attribute is not mandatory, if it isn’t defined, OpenNebula will generate one automatically.

```plaintext
NAME = "hmnet"

PHYDEV = "eth0"
VLAN = "YES"
VLAN_ID = 50 # optional
BRIDGE = "brhm" # optional
```

In this scenario, the driver will check for the existence of the brhm bridge. If it doesn’t exist it will be created. eth0 will be tagged (eth0.<vlan_id>) and attached to brhm (unless it’s already attached).

**Warning:** Any user with Network creation/modification permissions may force a custom vlan id with the VLAN_ID parameter in the network template. You **MUST** restrict permissions on Network creation to admin groups with ACL rules. Regular uses will then be able to safely make address reservations on the Networks.

4.2.5 Tuning & Extending

**Warning:** Remember that any change in the /var/lib/one/remotes directory won’t be effective in the Hosts until you execute, as oneadmin:

The code can be enhanced and modified, by chaning the following files in the frontend:

- /var/lib/one/remotes/vnm/802.1Q/post
- /var/lib/one/remotes/vnm/802.1Q/vlan_tag_driver.rb
- /var/lib/one/remotes/vnm/802.1Q/clean
- /var/lib/one/remotes/vnm/802.1Q/pre

Remember to sync any changes to the notes and to backup the changes in order to re-apply them after upgrading to a new release of OpenNebula:
4.3 VXLAN

This guide describes how to enable Network isolation provided through the VXLAN encapsulation protocol. This driver will create a bridge for each OpenNebula Virtual Network and attach a VXLAN tagged network interface to the bridge.

The VLAN id will be the same for every interface in a given network, calculated by adding a constant to the network id. It may also be forced by specifying an VLAN_ID parameter in the Virtual Network template.

Additionally each VLAN has associated a multicast address to encapsulate L2 broadcast and multicast traffic. This address is assigned by default to the 239.0.0.0/8 range as defined by RFC 2365 (Administratively Scoped IP Multicast). In particular the multicast address is obtained by adding the VLAN_ID to the 239.0.0.0/8 base address.

4.3.1 Requirements

The hypervisors must run a Linux kernel (>3.7.0) that natively supports the VXLAN protocol and the associated iproute2 package.

When all the hypervisors are connected to the same broadcasting domain just be sure that the multicast traffic is not filtered by any iptable rule in the hypervisors. However if the multicast traffic needs to traverse routers a multicast protocol like IGMP needs to be configured in your network.

4.3.2 Considerations & Limitations

This driver works with the default UDP server port 8472.

VXLAN traffic is forwarded to a physical device, this device can be configured to be a VLAN tagged interface. The current version of the driver does not automatically create the 802.1Q interface, so you need to configured it in the hypervisors in case you need them.

4.3.3 Configuration

Hosts Configuration

- The sudoers file must be configured so oneadmin can execute brctl and ip in the hosts.

OpenNebula Configuration

To enable this driver, use vxlan as the Virtual Network Manager driver parameter when the hosts are created with the onehost command:

```
$ onehost create host01 -i kvm -v kvm -n vxlan
```

VXLAN Options

It is possible specify the start VLAN ID and the base multicast address by editing /var/lib/one/remotes/vnm/OpenNebulaNetwork.conf.

This driver accepts an MTU attribute that will be used when creating the tagged interface and bridge. Also TTL can be adjusted for routed multicast networks (IGMP).
## Driver Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre</td>
<td>Creates a VXLAN interface through PHYDEV, creates a bridge (if needed) and attaches the vxlan device.</td>
</tr>
<tr>
<td>Post</td>
<td>When the VM is associated to a security group, the corresponding iptables rules are applied.</td>
</tr>
<tr>
<td>Clean</td>
<td>It doesn’t do anything. The VXLAN interface and bridge are kept in the Host to speed up future VMs</td>
</tr>
</tbody>
</table>

### 4.3.4 Usage

The driver will be automatically applied to every Virtual Machine deployed in the Host. However, this driver requires a special configuration in the Virtual Network template: only the virtual networks with the attribute VLAN set to YES will be isolated. The attribute PHYDEV must be also defined, with the name of the physical network device that will be attached to the bridge. The BRIDGE attribute is not mandatory, if it isn’t defined, OpenNebula will generate one automatically.

```ruby
NAME = "vxlan_net"
PHYDEV = "eth0"
VLAN = "YES"
VLAN_ID = 50    # optional
BRIDGE = "vxlan50" # optional
...
```

In this scenario, the driver will check for the existence of the vxlan50 bridge. If it doesn’t exist it will be created. eth0 will be tagged (eth0.<vlan_id>) and attached to vxlan (unless it’s already attached). Note that eth0 can be a 802.1Q tagged interface if you want to isolate the OpenNebula VXLAN traffic.

**Warning:** Any user with Network creation/modification permissions may force a custom vlan id with the VLAN_ID parameter in the network template. You MUST restrict permissions on Network creation to admin groups with ACL rules. Regular users will then be able to safely make address reservations on the Networks.

### 4.3.5 Tuning & Extending

**Warning:** Remember that any change in the /var/lib/one/remotes directory won’t be effective in the Hosts until you execute, as oneadmin:

The code can be enhanced and modified, by changing the following files in the frontend:

- /var/lib/one/remotes/vnm/vxlan/vxlan_driver.rb
- /var/lib/one/remotes/vnm/vxlan/post
- /var/lib/one/remotes/vnm/vxlan/clean
- /var/lib/one/remotes/vnm/vxlan/pre

Remember to sync any changes to the notes and to backup the changes in order to re-apply them after upgrading to a new release of OpenNebula:

```bash
oneadmin@frontend $ onehost sync
```
4.4 Security Groups

Using Security Groups, administrators can define the firewall rules and apply them to the Virtual Machines.

By default, the default security group is applied to new VMs, which allows all OUTBOUND traffic but blocks any INBOUND traffic. Modify the default security group to allow all INBOUND connections or to define any rules you might want.

Warning: These drivers deprecate the old firewall drivers. However, it will respect backwards compatibility and if old rules such WHITE_PORTS_TCP, etc are defined, the old drivers will be used and it will completely ignore the new security drivers mechanism.

4.4.1 Definition

A Security Group is composed of several Rules. Each Rule is defined with the following attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Type</th>
<th>Meaning</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTOCOL</td>
<td>Mandatory</td>
<td>Defines the protocol of the rule</td>
<td>ALL, TCP, UDP, ICMP, IPSEC</td>
</tr>
<tr>
<td>RULE_TYPE</td>
<td>Mandatory</td>
<td>Defines the direction of the rule</td>
<td>INBOUND, OUTBOUND</td>
</tr>
<tr>
<td>IP</td>
<td>Optional</td>
<td>If the rule only applies to a specific net.</td>
<td>A valid IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is the first IP of the consecutive set</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>of IPs. Must be used with SIZE.</td>
<td></td>
</tr>
<tr>
<td>SIZE</td>
<td>Optional</td>
<td>If the rule only applies to a net. The number</td>
<td>An integer &gt;= 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>of total consecutive IPs of the network. Use always</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>with IP.</td>
<td></td>
</tr>
<tr>
<td>RANGE</td>
<td>Optional</td>
<td>A Port Range to filter specific ports. Only works</td>
<td>(iptables syntax) multiple ports or port ranges</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with TCP and UDP.</td>
<td>are separated using a comma, and a port range is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>specified using a colon. Example:</td>
</tr>
<tr>
<td>ICMP_TYPE</td>
<td>Optional</td>
<td>A specific ICMP type of the rule. If a type has</td>
<td>0,3,4,5,8,9,10,11,12,13,14,17,18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>multiple codes, it includes all the codes within.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This can only be used with ICMP. If omitted</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the rule will affect the whole ICMP protocol.</td>
<td></td>
</tr>
</tbody>
</table>

To create a Security Group, use the Sunstone web interface, or create a template file following this example:

```bash
$ cat ./sg.txt
NAME = test
RULE = [
  PROTOCOL = TCP,
  RULE_TYPE = inbound,
  RANGE = 1000:2000
]
RULE = [
  PROTOCOL= TCP,
  RULE_TYPE = outbound,
  RANGE = 1000:2000
]```
RULE = [
  PROTOCOL = ICMP,
  RULE_TYPE = inbound,
  NETWORK_ID = 0
]

$ onesecgroup create ./sg.txt
ID: 102

4.4.2 Usage

To apply a Security Group to your Virtual Machines, you can assign them to the Virtual Networks. Either use the Sunstone wizard, or set the SECURITY_GROUPS attribute:

$ onevnet update 0
SECURITY_GROUPS = "100, 102, 110"
When a Virtual Machine is instantiated, the rules are copied to the VM resource and can be seen in the CLI and Sunstone.
Advanced Usage

To accommodate more complex scenarios, you can also set Security Groups to each Address Range of a Virtual Network.

```
$ onevnet updatear 0 1
SECURITY_GROUPS = "100, 102, 110"
```

Moreover, each Virtual Machine Template NIC can define a list of Security Groups:

```
NIC = {
    NETWORK = "private-net",
    NETWORK_UNAME = "oneadmin",
    SECURITY_GROUPS = "103, 125"
}
```

If the Address Range or the Template NIC define SECURITY_GROUPS, the IDs do not overwrite the ones defined in the Virtual Network. All the Security Group IDs are combined, and applied to the Virtual Machine instance.

### 4.4.3 Default Security Group

There is a default Security Group with ID 0. At bootstrap, it contains only a rule to allow all outbound traffic. You can update it to add any default rules that may suit your infrastructure.

This special Security Group is added to all the Virtual Networks when they are created, but you can remove it later updating the network’s properties.
4.4.4 Considerations and Limitations

The Security Groups can be updated to edit or add new rules. Bear in mind that the new rules will not be applied to any existing Virtual Machine. You can see the actual rules applied to each VM in the output of the `onevm show <id>` command, or in the individual VM panel in Sunstone.

4.4.5 Configuration

Security groups is only supported and automatically enabled when using the following drivers:

- 802.1Q
- ebtables
- fw
- vxlan

Note: Openvswitch and vmware do not support Security Groups.

Due to backwards compatibility reasons, if the old firewall rules exist in the template, security groups will be ignored and the deprecated way will be honored:

- `WHITE_PORTS_TCP = <iptables_range>`: Permits access to the VM only through the specified ports in the TCP protocol. Supersedes `BLACK_PORTS_TCP` if defined.
- `BLACK_PORTS_TCP = <iptables_range>`: Doesn’t permit access to the VM through the specified ports in the TCP protocol. Superseded by `WHITE_PORTS_TCP` if defined.
- `WHITE_PORTS_UDP = <iptables_range>`: Permits access to the VM only through the specified ports in the UDP protocol. Supersedes `BLACK_PORTS_UDP` if defined.
- `BLACK_PORTS_UDP = <iptables_range>`: Doesn’t permit access to the VM through the specified ports in the UDP protocol. Superseded by `WHITE_PORTS_UDP` if defined.
- `ICMP = drop`: Blocks ICMP connections to the VM. By default it’s set to accept.

4.5 Open vSwitch

This guide describes how to use the Open vSwitch network drives. They provide two indepent functionalities that can be used together: network isolation using VLANs, and network filtering using OpenFlow. Each Virtual Network interface will receive a VLAN tag enabling network isolation. Other traffic attributes that may be configured through Open vSwitch are not modified.

The VLAN id will be the same for every interface in a given network, calculated by adding a constant to the network id. It may also be forced by specifying an VLAN_ID parameter in the Virtual Network template.

The network filtering functionality is very similar to the Firewall drivers, with a few limitations discussed below.

4.5.1 Requirements

This driver requires Open vSwitch to be installed on each OpenNebula Host. Follow the resources specified in `hosts_configuration` to install it.
4.5.2 Considerations & Limitations

Integrating OpenNebula with Open vSwitch brings a long list of benefits to OpenNebula, read Open vSwitch Features to get a hold on these features.

This guide will address the usage of VLAN tagging and OpenFlow filtering of OpenNebula Virtual Machines. On top of that any other Open vSwitch feature may be used, but that’s outside of the scope of this guide.

ovswitch and ovswitch_brcompat

OpenNebula ships with two sets of drivers that provide the same functionality: ovswitch and ovsvswitch_brcompat. The following list details the differences between both drivers:

- **ovswitch**: Recommended for kvm hosts. Only works with kvm. Doesn’t require the Open vSwitch compatibility layer for Linux bridging.
- **ovswitch_brcompat**: Works with kvm and xen. This is the only set that currently works with xen. Not recommended for kvm. Requires Open vSwitch compatibility layer for Linux bridging.

4.5.3 Configuration

Hosts Configuration

- You need to install Open vSwitch on each OpenNebula Host. Please refer to the Open vSwitch documentation to do so.
- If using ovswitch_brcompat it is also necessary to install the Open vSwitch compatibility layer for Linux bridging.
- The sudoers file must be configured so oneadmin can execute ovs-vsctl in the hosts.

OpenNebula Configuration

To enable this driver, use ovswitch or ovswitch_brcompat as the Virtual Network Manager driver parameter when the hosts are created with the onehost command:

```
# for kvm hosts
$ onehost create host01 -i kvm -v kvm -n ovswitch

# for xen hosts
$ onehost create host02 -i xen -v xen -n ovswitch_brcompat
```

Open vSwitch Options

It is possible to disable the ARP Cache Poisoning prevention rules by changing this snippet in /var/lib/one/remotes/vnm/OpenNebulaNetwork.conf:

```
# Enable ARP Cache Poisoning Prevention Rules
:arp_cache_poisoning: true
```

The start VLAN id can also be set in that file.
Driver Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre</td>
<td>N/A</td>
</tr>
<tr>
<td>Post</td>
<td>Performs the appropriate Open vSwitch commands to tag the virtual tap interface.</td>
</tr>
<tr>
<td>Clean</td>
<td>It doesn’t do anything. The virtual tap interfaces will be automatically discarded when the VM is shut down.</td>
</tr>
</tbody>
</table>

Multiple VLANs (VLAN trunking)

VLAN trunking is also supported by adding the following tag to the NIC element in the VM template or to the virtual network template:

- VLAN_TAGGED_ID: Specify a range of VLANs to tag, for example: 1,10,30,32.

Different Bridge for OpenvSwitch

If a template is intended to be instantiated in hosts with ovswitch vnm driver and also in hosts with a different driver, it’s possible to specify what bridge in both sets of hosts by setting the BRIDGE_OVS parameter in addition to the regular BRIDGE parameter. BRIDGE will be used for non ovswitch hosts and BRIDGE_OVS for ovswitch hosts.

For example, consider the following network template:

```
BRIDGE="br0"
BRIDGE_OVS="ovsbr0"
```

- If instantiated in a host with vnm=dummy the virtual network interface will be connected to the br0 bridge.
- Whereas if instantiated in a host with vnm=ovswitch, it will be connected to the ovsbr0 ovs switch.

4.5.4 Usage

Network Isolation

The driver will be automatically applied to every Virtual Machine deployed in the Host. Only the virtual networks with the attribute VLAN set to YES will be isolated. There are no other special attributes required.

```
NAME    = "ovswitch_net"
BRIDGE  = vbr1

VLAN    = "YES"
VLAN_ID = 50                     # optional
...
```

**Warning:** Any user with Network creation/modification permissions may force a custom vlan id with the VLAN_ID parameter in the network template. In that scenario, any user may be able to connect to another network with the same network id. Techniques to avoid this are explained under the Tuning & Extending section.
Network Filtering

The first rule that is always applied when using the Open vSwitch drivers is the MAC-spoofing rule, that prevents any traffic coming out of the VM if the user changes the MAC address.

The firewall directives must be placed in the network section of the Virtual Machine template. These are the possible attributes:

- **BLACK_PORTS_TCP** = `iptables_range`: Doesn’t permit access to the VM through the specified ports in the TCP protocol. Superseded by WHITE_PORTS_TCP if defined.

- **BLACK_PORTS_UDP** = `iptables_range`: Doesn’t permit access to the VM through the specified ports in the UDP protocol. Superseded by WHITE_PORTS_UDP if defined.

- **ICMP** = `drop`: Blocks ICMP connections to the VM. By default it’s set to accept.

`iptables_range`: a list of ports separated by commas, e.g.: `80, 8080`. Currently no ranges are supporteg, e.g.: `5900:6000` is not supported.

Example:

```bash
NIC = [ NETWORK_ID = 3, BLACK_PORTS_TCP = "80, 22", ICMP = drop ]
```

Note that WHITE_PORTS_TCP and BLACK_PORTS_TCP are mutually exclusive. In the event where they’re both defined the more restrictive will prevail i.e. WHITE_PORTS_TCP. The same happens with WHITE_PORTS_UDP and BLACK_PORTS_UDP.

4.5.5 Tuning & Extending

**Warning:** Remember that any change in the `/var/lib/one/remotes` directory won’t be effective in the Hosts until you execute, as oneadmin:

```bash
oneadmin@frontend $ onehost sync
```

This way in the next monitoring cycle the updated files will be copied again to the Hosts.

Restricting Manually the VLAN ID

You can either restrict permissions on Network creation with **ACL rules**, or you can entirely disable the possibility to redefine the VLAN_ID by modifying the source code of `/var/lib/one/remotes/vnm/ovswitch/OpenvSwitch.rb`. Change these lines:

```ruby
if nic[:vlan_id]
    vlan = nic[:vlan_id]
else
    vlan = CONF[:start_vlan] + nic[:network_id].to_i
end
```

with this one:

```ruby
vlan = CONF[:start_vlan] + nic[:network_id].to_i
```

OpenFlow Rules

To modify these rules you have to edit: `/var/lib/one/remotes/vnm/ovswitch/OpenvSwitch.rb`. 
Mac-spoofing
These rules prevent any traffic to come out of the port the MAC address has changed.

\[
\begin{align*}
\text{in}_\text{port}=\langle\text{PORT}\rangle, \text{dl}_\text{src}=\langle\text{MAC}\rangle, \text{priority}=40000, \text{actions}=&\text{normal} \\
\text{in}_\text{port}=\langle\text{PORT}\rangle, \text{priority}=39000, \text{actions}=&\text{normal}
\end{align*}
\]

IP hijacking
These rules prevent any traffic to come out of the port for IPv4 IP’s not configured for a VM

\[
\begin{align*}
\text{in}_\text{port}=\langle\text{PORT}\rangle, \text{arp}, \text{dl}_\text{src}=\langle\text{MAC}\rangle, \text{priority}=45000, \text{actions}=&\text{drop} \\
\text{in}_\text{port}=\langle\text{PORT}\rangle, \text{arp}, \text{dl}_\text{src}=\langle\text{MAC}\rangle, \text{nw}_\text{src}=\langle\text{IP}\rangle, \text{priority}=46000, \text{actions}=&\text{normal}
\end{align*}
\]

Black ports (one rule per port)
\[
tcp, \text{dl}_\text{dst}=\langle\text{MAC}\rangle, \text{tp}_\text{dst}=\langle\text{PORT}\rangle, \text{actions}=&\text{drop}
\]

ICMP Drop
\[
\text{icmp}, \text{dl}_\text{dst}=\langle\text{MAC}\rangle, \text{actions}=&\text{drop}
\]

4.6 Ebtables
This guide describes how to enable Network isolation provided through ebtables rules applied on the bridges. This method will only permit isolation with a mask of 255.255.255.0.

4.6.1 Requirements
This hook requires ebtables to be available in all the OpenNebula Hosts.

4.6.2 Considerations & Limitations
Although this is the most easily usable driver, since it doesn’t require any special hardware or any software configuration, it lacks the ability of sharing IPs amongst different VNETs, that is, if an VNET is using leases of 192.168.0.0/24, another VNET can’t be using IPs in the same network.

4.6.3 Configuration

Hosts Configuration
- The package ebtables must be installed in the hosts.
- The sudoers file must be configured so oneadmin can execute ebtables in the hosts.

OpenNebula Configuration
To enable this driver, use ebtables as the Virtual Network Manager driver parameter when the hosts are created with the onehost command:

\[
\$ \text{onehost create host01 -i kvm -v kvm -n ebtables}
\]
### Driver Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre</td>
<td>N/A</td>
</tr>
<tr>
<td>Post</td>
<td>Creates EBTABLES rules in the Host where the VM has been placed.</td>
</tr>
<tr>
<td>Clean</td>
<td>Removes the EBTABLES rules created during the Post action.</td>
</tr>
</tbody>
</table>

### 4.6.4 Usage

The driver will be automatically applied to every Virtual Machine deployed in the Host. Only the virtual networks with the attribute VLAN set to YES will be isolated. There are no other special attributes required.

```plaintext
NAME = "ebtables_net"
BRIDGE = vbr1
VLAN = "YES"
```

### 4.6.5 Tuning & Extending

**EBTABLES Rules**

This section lists the EBTABLES rules that are created:

```plaintext
# Drop packets that don't match the network's MAC Address
-s ! <mac_address>/ff:ff:ff:ff:ff:0 -o <tap_device> -j DROP

# Prevent MAC spoofing
-s ! <mac_address> -i <tap_device> -j DROP
```

### 4.7 VMware Networking

This guide describes how to use the VMware network driver in OpenNebula. This driver optionally provides network isolation through VLAN tagging. The VLAN id will be the same for every interface in a given network, calculated by adding a constant to the network id. It may also be forced by specifying an VLAN_ID parameter in the Virtual Network template.

#### 4.7.1 Requirements

In order to use the dynamic network mode for VM disks, some extra configuration steps are needed in the ESX hosts.

```plaintext
$ su
$ chmod +s /sbin/esxcfg-vswitch
```

#### 4.7.2 Considerations & Limitations

It should be noted that the drivers will not create/delete/manage VMware virtual switches, these should be created before-hand by VMware administrators.

Since the dynamic driver will however create VMware port groups, it should be noted that there’s a default limit of 56 port groups per switch. Administrators should be aware of these limitations.
4.7.3 Configuration

The vSphere hosts can work in two different networking modes, namely:

- **pre-defined**: The VMWare administrator has set up the network for each vSphere host, defining the vSwitch’es and port groups for the VMs. This mode is associated with the dummy network driver. To configure this mode use *dummy* as the Virtual Network Manager driver parameter when the hosts are created:

  ```
  $ onehost create host01 -i vmware -v vmware -n dummy
  ```

- **dynamic**: In this mode OpenNebula will create on-the-fly port groups (with an optional VLAN_ID) for your VMs. The VMWare administrator has to set up only the vSwitch to be used by OpenNebula. To enable this driver, use *vmware* as the VNM driver for the hosts:

  ```
  $ onehost create host02 -i vmware -v vmware -n vmware
  ```

**Warning**: Dynamic and pre-defined networking modes can be mixed in a datacenter. Just use the desired mode for each host.

VMware Options

It is possible specify the start VLAN ID by editing `/var/lib/one/remotes/vnm/OpenNebulaNetwork.conf`.

4.7.4 Usage

**Using the Pre-defined Network Mode**

In this mode there the VMware admin has created one or more port groups in the ESX hosts to bridge the VMs. The port group has to be specified for each Virtual Network in its template through the BRIDGE attribute (check the Virtual Network usage guide for more info).

The NICs of the VM in this Virtual Network will be attached to the specified port group in the vSphere host. For example:

```
NAME = "pre-defined_vmware_net"
BRIDGE = "VM Network"  # This is the port group
...
```

**Using the Dynamic Network Mode**

In this mode the driver will dynamically create a port-group with name `one-pg-<network_id>` in the specified vSwitch of the target host. In this scenario the vSwitch is specified by the BRIDGE attribute of the Virtual Network template.

Additionally the port groups can be tagged with a vlan_id. You can set VLAN=“YES” in the Virtual Network template to automatically tag the port groups in each ESX host. Optionally the tag can be specified through the VLAN_ID attribute. For example:

```
NAME = "dynamic_vmware_net"
BRIDGE = "vSwitch0"  # In this mode this is the vSwitch name
VLAN = "YES"
VLAN_ID = 50  # optional
...
```
4.7.5 Tuning & Extending

The predefined mode (dummy driver) does not execute any operation in the pre, post and clean steps (see for more details on these phases).

The strategy of the dynamic driver is to dynamically create a VMware port group attached to a pre-existing VMware virtual switch (standard or distributed) for each Virtual Network.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre</td>
<td>Creates the VMware port group with name one-pg-&lt;network_id&gt;.</td>
</tr>
<tr>
<td>Post</td>
<td>No operation</td>
</tr>
<tr>
<td>Clean</td>
<td>No operation</td>
</tr>
</tbody>
</table>
5.1 Monitoring Overview

This guide provides an overview of the OpenNebula monitoring subsystem. The monitoring subsystem gathers information relative to the hosts and the virtual machines, such as the host status, basic performance indicators, as well as VM status and capacity consumption. This information is collected by executing a set of static probes provided by OpenNebula. The output of these probes is sent to OpenNebula in two different ways: using a push or a pull paradigm. Below you can find a brief description of the two models and when to use one or the other.

5.1.1 The UDP-push Model

| Warning: Default. This is the default IM for KVM and Xen in OpenNebula >= 4.4. |

In this model, each host periodically sends monitoring data via UDP to the frontend which collects it and processes it in a dedicated module. This distributed monitoring system resembles the architecture of dedicated monitoring systems, using a lightweight communication protocol, and a push model.

This model is highly scalable and its limit (in terms of number of VMs monitored per second) is bounded to the performance of the server running oned and the database server.

Please read the UDP-push guide for more information.

When to Use the UDP-push Model

This mode can be used only with Xen and KVM (VMware only supports the SSH-pull mode).

This monitoring model is adequate when:

- You are using KVM or Xen (VMware is not supported in this mode)
- Your infrastructure has a medium-to-high number of hosts (e.g. more than 50)
- You need a high responsive system
- You need a high frequently updated monitor information
- All your hosts communicate through a secure network (UDP packages are not encrypted and their origin is not verified)
5.1.2 The Pull Model

When using this mode OpenNebula periodically actively queries each host and executes the probes via ssh. In KVM and Xen this means establishing an ssh connection to each host and executing several scripts to retrieve this information. Note that VMware uses the VI API for this, instead of a ssh connection.

This mode is limited by the number of active connections that can be made concurrently, as hosts are queried sequentially.

Please read the KVM and Xen SSH-pull guide or the ESX-pull guide for more information.

When to Use the SSH-pull Model

This mode can be used with VMware, Xen and KVM.

This monitoring model is adequate when:

- Your infrastructure has a low number of hosts (e.g. 50 or less)
- You are communicating with the hosts through an insecure network
- You do not need to update the monitoring with a high frequency (e.g. for 50 hosts the monitoring period would be typically of about 5 minutes)

5.1.3 Other Monitorization Systems

OpenNebula can be easily integrated with other monitorization system. Please read the Information Manager Driver integration guide for more information.

5.1.4 The Monitor Metrics

The information manage by the monitoring system includes the typical performance and configuration parameters for the host and VMs, e.g. CPU or network consumption, Hostname or CPU model.

These metrics are gathered by specialized programs, called probes, that can be easily added to the system. Just write your own program, or shell script that returns the metric that you are interested in. Please read the Information Manager Driver integration guide for more information.

5.2 KVM and Xen SSH-pull Monitoring

KVM and Xen can be monitored with this ssh based monitoring system. The OpenNebula frontend starts a driver which triggers ssh connections to the hosts which return the monitoring information of the host and of all the virtual machines running within.

5.2.1 Requirements

- ssh access from the frontends to the hosts as oneadmin without password has to be possible.
- ruby is required in the hosts.
- KVM hosts: libvirt must be enabled.
- Xen hosts: sudo access to run xl or xm and xentop as oneadmin.
5.2.2 OpenNebula Configuration

Enabling the Drivers

To enable this monitoring system `/etc/one/oned.conf` must be configured with the following snippets:

**KVM:**

```plaintext
IM_MAD = [
    name = "kvm",
    executable = "one_im_ssh",
    arguments = ":-r 0 -t 15 kvm-probes"
]
```

**Xen 3.x:**

```plaintext
IM_MAD = [
    name = "xen",
    executable = "one_im_ssh",
    arguments = ":-r 0 -t 15 xen3-probes"
]
```

**Xen 4.x:**

```plaintext
IM_MAD = [
    name = "xen",
    executable = "one_im_ssh",
    arguments = ":-r 0 -t 15 xen4-probes"
]
```

The arguments passed to this driver are:

- `-r`: number of retries when monitoring a host
- `-t`: number of threads, i.e. number of hosts monitored at the same time

Monitoring Configuration Parameters

OpenNebula allows to customize the general behaviour of the whole monitoring subsystem:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MONITORING_INTERVAL</td>
<td>Time in seconds between host and VM moniarization. It must have a value greater than the manager timer</td>
</tr>
<tr>
<td>HOST_PER_INTERVAL</td>
<td>Number of hosts monitored in each interval.</td>
</tr>
<tr>
<td>VM_PER_INTERVAL</td>
<td>Number of VMs monitored in each interval.</td>
</tr>
</tbody>
</table>

**Warning:** VM_PER_INTERVAL is only relevant in case of host failure when OpenNebula pro-actively monitors each VM. You need to set VM_INDIVIDUAL_MONITORING to "yes" in oned.conf.

The information gathered by the probes is also stored in a monitoring table. This table is used by Sunstone to draw monitoring graphics and can be queried using the OpenNebula API. The size of this table can be controlled with:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOST_MONITORING_EXPIRATION</td>
<td>Number in seconds, to expire monitoring information. Use 0 to disable HOST monitoring recording.</td>
</tr>
<tr>
<td>VM_MONITORING_EXPIRATION</td>
<td>Number in seconds, to expire monitoring information. Use 0 to disable VM monitoring recording.</td>
</tr>
</tbody>
</table>
5.2.3 Troubleshooting

In order to test the driver, add a host to OpenNebula using `onehost`, specifying the defined IM driver:

```
$ onehost create ursa06 --im xen --vm xen --net dummy
```

Now give it time to monitor the host (this time is determined by the value of MONITORING_INTERVAL in `/etc/one/oned.conf`). After one interval, check the output of `onehost list`, it should look like the following:

```
$ onehost list

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>RVM</th>
<th>ALLOCATED_CPU</th>
<th>ALLOCATED_MEM</th>
<th>STAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ursa06</td>
<td>-</td>
<td>0</td>
<td>0 / 400 (0%)</td>
<td>0K / 7.7G (0%)</td>
<td>on</td>
</tr>
</tbody>
</table>
```

Host management information is logged to `/var/log/one/oned.log`. Correct monitoring log lines look like this:

```
Fri Nov 22 12:02:26 2013 [InM][D]: Monitoring host ursa06 (0)
Fri Nov 22 12:02:30 2013 [InM][D]: Host ursa06 (0) successfully monitored.
```

Both lines have the ID of the host being monitored.

If there are problems monitoring the host you will get an `err` state:

```
$ onehost list

<table>
<thead>
<tr>
<th>ID</th>
<th>NAME</th>
<th>CLUSTER</th>
<th>RVM</th>
<th>ALLOCATED_CPU</th>
<th>ALLOCATED_MEM</th>
<th>STAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ursa06</td>
<td>-</td>
<td>0</td>
<td>0 / 400 (0%)</td>
<td>0K / 7.7G (0%)</td>
<td>err</td>
</tr>
</tbody>
</table>
```

The way to get the error message for the host is using `onehost show` command, specifying the host id or name:

```
$ onehost show 0

[...]
MONITORING INFORMATION
ERROR=
  MESSAGE="Error monitoring host 0: MONITOR FAILURE 0 Could not update remotes",
  TIMESTAMP="Nov 22 12:02:30 2013"
```

The log file is also useful as it will give you even more information on the error:

```
Mon Oct 3 15:26:57 2011 [InM][I]: Monitoring host ursa06 (0)
Mon Oct 3 15:26:57 2011 [InM][I]: Command execution fail: scp -r /var/lib/one/remotes/. ursa06:/var/tmp/one
Mon Oct 3 15:26:57 2011 [InM][I]: ssh: Could not resolve hostname ursa06: nodename nor servname provided, or not known
Mon Oct 3 15:26:57 2011 [InM][I]: lost connection
Mon Oct 3 15:26:57 2011 [InM][I]: ExitCode: 1
Mon Oct 3 15:26:57 2011 [InM][E]: Error monitoring host 0: MONITOR FAILURE 0 Could not update remotes
```

In this case the node `ursa06` could not be found in the DNS or `/etc/hosts`.

5.2.4 Tuning & Extending

The probes are specialized programs that obtain the monitor metrics. Probes are defined for each hypervisor, and are located at `/var/lib/one/remotes/im/<hypervisor>-probes.d` for Xen and KVM.

You can easily write your own probes or modify existing ones, please see the Information Manager Drivers guide. Remember to synchronize the monitor probes in the hosts using `onehost sync` as described in the *Managing Hosts* guide.
5.3 KVM and Xen UDP-push Monitoring

KVM and Xen can be monitored with this UDP based monitoring system. Monitorization data is sent from each host to the frontend periodically via UDP by an agent. This agent is started by the initial bootstrap system of the monitoring system which is performed via ssh like with the SSH-pull system.

5.3.1 Requirements

- **ssh** access from the frontends to the hosts as oneadmin without password has to be possible.
- **ruby** is required in the hosts.
- KVM hosts: **libvirt** must be enabled.
- Xen hosts: sudo access to run xl or xm and xentop as oneadmin.
- The firewall of the frontend (if enabled) must allow UDP packages incoming from the hosts on port 4124.

5.3.2 Overview

OpenNebula starts a **collectd** daemon running in the frontend host that listens for UDP connections on port 4124. In the first monitoring cycle the OpenNebula connects to the host using ssh and starts a daemon that will execute the probe scripts as in the SSH-pull model and sends the collected data to the collectd daemon in the fronted every specific amount of seconds (configurable with the -i option of the **collectd IM_MAD**). This way the monitoring subsystem doesn’t need to make new ssh connections to the hosts when it needs data.

If the agent stops in a specific host, OpenNebula will detect that no monitorization data is received from that hosts and will automatically fallback to the SSH-pull model, thus starting the agent again in the host.
5.3.3 OpenNebula Configuration

Enabling the Drivers

To enable this monitoring system /etc/one/oned.conf must be configured with the following snippets:

```
collectd
```
must be enabled both for KVM and Xen:

```
IM_MAD = [  
    name = "collectd",
    executable = "collectd",
    arguments = "-p 4124 -f 5 -t 50 -i 20" 
]
```

Valid arguments for this driver are:

- **-a**: Address to bind the collectd socket (default 0.0.0.0)
- **-p**: Port number
- **-f**: Interval in seconds to flush collected information to OpenNebula (default 5)
- **-t**: Number of threads for the collectd server (default 50)
- **-i**: Time in seconds of the monitoring push cycle. This parameter must be smaller than MONITORING_INTERVAL (see below), otherwise push monitoring will not be effective.

**KVM**:

```
IM_MAD = [  
    name = "kvm",
    executable = "one_im_ssh",
    arguments = "-r 3 -t 15 kvm" 
]
```

**Xen 3**:

```
IM_MAD = [  
    name = "xen",
    executable = "one_im_ssh",
    arguments = "-r 3 -t 15 xen3" 
]
```

**Xen 4**:

```
IM_MAD = [  
    name = "xen",
    executable = "one_im_ssh",
    arguments = "-r 3 -t 15 xen4" 
]
```

The arguments passed to this driver are:

- **-r**: Number of retries when monitoring a host
- **-t**: Number of threads, i.e. number of hosts monitored at the same time

**Monitoring Configuration Parameters**

OpenNebula allows to customize the general behaviour of the whole monitoring subsystem:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MONITORING_INTERVAL</td>
<td>Time in seconds between host and VM monitoring. It must have a value greater than the manager timer</td>
</tr>
<tr>
<td>HOST_PER_INTERVAL</td>
<td>Number of hosts monitored in each interval.</td>
</tr>
</tbody>
</table>
Warning: Note that in this case HOST.PER_INTERVAL is only relevant when bootstrapping the monitor agents. Once the agents are up and running, OpenNebula does not polls the hosts.

5.3.4 Troubleshooting

Healthy Monitoring System

If the UDP-push model is running successfully, it means that it has not fallen back to the SSH-pull model. We can verify this based on the information logged in oned.log.

Every (approximately) monitoring_push_cycle of seconds OpenNebula is receiving the monitoring data of every Virtual Machine and of a host like such:

<table>
<thead>
<tr>
<th>Time</th>
<th>Log Level</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Nov 18 22:25:00 2013</td>
<td>[InM][D]</td>
<td>Host thost001 (1) successfully monitored.</td>
</tr>
<tr>
<td>Mon Nov 18 22:25:01 2013</td>
<td>[VMM][D]</td>
<td>VM 0 successfully monitored: ...</td>
</tr>
<tr>
<td>Mon Nov 18 22:25:21 2013</td>
<td>[InM][D]</td>
<td>Host thost001 (1) successfully monitored.</td>
</tr>
<tr>
<td>Mon Nov 18 22:25:21 2013</td>
<td>[VMM][D]</td>
<td>VM 0 successfully monitored: ...</td>
</tr>
<tr>
<td>Mon Nov 18 22:25:40 2013</td>
<td>[InM][D]</td>
<td>Host thost001 (1) successfully monitored.</td>
</tr>
<tr>
<td>Mon Nov 18 22:25:41 2013</td>
<td>[VMM][D]</td>
<td>VM 0 successfully monitored: ...</td>
</tr>
</tbody>
</table>

However, if in oned.log a host is being monitored actively periodically (every MONITORING_INTERVAL seconds) then the UDP-push monitorization is not working correctly:

<table>
<thead>
<tr>
<th>Time</th>
<th>Log Level</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Nov 18 22:22:30 2013</td>
<td>[InM][D]</td>
<td>Monitoring host thost087 (87)</td>
</tr>
<tr>
<td>Mon Nov 18 22:23:30 2013</td>
<td>[InM][D]</td>
<td>Monitoring host thost087 (87)</td>
</tr>
<tr>
<td>Mon Nov 18 22:24:30 2013</td>
<td>[InM][D]</td>
<td>Monitoring host thost087 (87)</td>
</tr>
</tbody>
</table>

If this is the case it’s probably because OpenNebula is receiving probes faster than it can process. See the Tuning section to fix this.

Monitoring Probes

For the troubleshooting of errors produced during the execution of the monitoring probes, please refer to the troubleshooting section of the SSH-pull guide.

5.3.5 Tuning & Extending

Adjust Monitoring Interval Times

In order to tune your OpenNebula installation with appropriate values of the monitoring parameters you need to adjust the -i option of the collectd IM_MAD (the monitoring push cycle).

If the system is not working healthily it will be due to the database throughput since OpenNebula will write the monitoring information to a database, an amount of ~4KB per VM. If the number of virtual machines is too large and the monitoring push cycle too low, OpenNebula will not be able to write that amount of data to the database.

Driver Files

The probes are specialized programs that obtain the monitor metrics. Probes are defined for each hypervisor, and are located at /var/lib/one/remotes/im/<hypervisor>-probes.d for Xen and KVM.
You can easily write your own probes or modify existing ones, please see the Information Manager Drivers guide. Remember to synchronize the monitor probes in the hosts using `onehost sync` as described in the Managing Hosts guide.

## 5.4 VMware VI API-pull Monitor

### 5.4.1 Requirements

- VI API access to the ESX hosts.
- ESX hosts configured to work with OpenNebula

### 5.4.2 OpenNebula Configuration

In order to configure VMware you need to:

- Enable the VMware monitoring driver in `/etc/one/oned.conf` by uncommenting the following lines:

```
IM_MAD = [
  name = "vmware",
  executable = "one_im_sh",
  arguments = "-c -t 15 -r 0 vmware"
]
```

- Make sure that the configuration attributes for VMware drivers are set in `/etc/one/vmwarerc`, see the VMware guide

### Monitoring Configuration Parameters

OpenNebula allows to customize the general behaviour of the whole monitoring subsystem:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MONITORING_INTERVAL</td>
<td>Time in seconds between host and VM monitorization. It must have a value greater than the manager timer</td>
</tr>
<tr>
<td>HOST_PER_INTERVAL</td>
<td>Number of hosts monitored in each interval.</td>
</tr>
<tr>
<td>VM_PER_INTERVAL</td>
<td>Number of VMs monitored in each interval.</td>
</tr>
</tbody>
</table>

**Warning:** VM_PER_INTERVAL is only relevant in case of host failure when OpenNebula pro-actively monitors each VM. You need to set VM_INDIVIDUAL_MONITORING to “yes” in oned.conf.

The information gathered by the probes is also stored in a monitoring table. This table is used by Sunstone to draw monitoring graphics and can be queried using the OpenNebula API. The size of this table can be controlled with:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOST_MONITORING_EXPIRATION</td>
<td>Time, in seconds, to expire monitoring information. Use 0 to disable HOST monitoring recording.</td>
</tr>
<tr>
<td>VM_MONITORING_EXPIRATION</td>
<td>Time, in seconds, to expire monitoring information. Use 0 to disable VM monitoring recording.</td>
</tr>
</tbody>
</table>

### 5.4.3 Troubleshooting

In order to test the driver, add a host to OpenNebula using `onehost`, specifying the defined IM driver:
$ onehost create esx_node1 --im vmware --vm vmware --net dummy

Now give it time to monitor the host (this time is determined by the value of MONITORING_INTERVAL in /etc/one/oned.conf). After one interval, check the output of `onehost list`, it should look like the following:

```
$ onehost list

+-----------------+-----------------+-------+--------+-----------------------+-----------------+--------------+
| ID              | NAME            | CLUSTER| RVM    | ALLOCATED_CPU         | ALLOCATED_MEM   | STAT         |
|-----------------+-----------------+-------+-------+-----------------------+-----------------+--------------+
| 0               | esx_node1       | -     | 0      | 0 / 400 (0%)          | 0K / 7.7G (0%)  | on           |
```

Host management information is logged to `/var/log/one/oned.log`. Correct monitoring log lines look like this:

```
Fri Nov 22 12:02:26 2013 [InM][D]: Monitoring host esx_node1 (0)
Fri Nov 22 12:02:30 2013 [InM][D]: Host esx1_node (0) successfully monitored.
```

Both lines have the ID of the host being monitored.

If there are problems monitoring the host you will get an `err` state:

```
$ onehost list

+-----------------+-----------------+-------+--------+-----------------------+-----------------+--------------+
| ID              | NAME            | CLUSTER| RVM    | ALLOCATED_CPU         | ALLOCATED_MEM   | STAT         |
|-----------------+-----------------+-------+-------+-----------------------+-----------------+--------------+
| 0               | esx_node1       | -     | 0      | 0 / 400 (0%)          | 0K / 7.7G (0%)  | err          |
```

The way to get the error message for the host is using `onehost show` command, specifying the host id or name:

```
$ onehost show 0

[...] MONITORING INFORMATION
ERROR={
    MESSAGE="Error monitoring host 0 : MONITOR FAILURE 0 Could not update remotes",
    TIMESTAMP="Nov 22 12:02:30 2013"
}
```

The log file is also useful as it will give you even more information on the error.

## 5.4.4 Tuning & Extending

The probes are specialized programs that obtain the monitor metrics. VMware probes are obtained by querying the ESX server through the VI API. The probe is located at `/var/lib/one/remotes/im/vmware.d`.

You can easily write your own probes or modify existing ones, please see the Information Manager Drivers guide.
6.1 Users & Groups Overview

OpenNebula includes a complete user & group management system. Users in an OpenNebula installation are classified in four types:

- **Administrators**, an admin user belongs to an admin group (oneadmin or otherwise) and can perform manage operations.
- **Regular users**, that may access most OpenNebula functionality.
- **Public users**, only basic functionality (and public interfaces) are open to public users.
- **Service users**, a service user account is used by the OpenNebula services (i.e. cloud APIs like EC2 or GUI’s like Sunstone) to proxy auth requests.

The resources a user may access in OpenNebula are controlled by a permissions system that resembles the typical UNIX one. By default, only the owner of a resource (e.g. a VM or an image) can use and manage it. Users can easily share the resources by granting use or manage permissions to other users in her group or to any other user in the system.

Upon group creation, an associated admin user can be created. By default this user will be able to create users in the new group, and manage non owned resources for the regular group, through the CLI and/or a special Sunstone view. This group can also be assigned to VDC, what is basically a pool of OpenNebula physical resources (hosts, datastores and virtual networks).

Along with the users & groups the Auth Subsystem is responsible for the authentication and authorization of user’s requests.

Any interface to OpenNebula (CLI, Sunstone, Ruby or Java OCA) communicates with the core using xml-rpc calls, that contain the user’s session string, which is authenticated by the OpenNebula core comparing the username and password with the registered users.

Each operation generates an authorization request that is checked against the registered ACL rules. The core then can grant permission, or reject the request.

OpenNebula comes with a default set of ACL rules that enables a standard usage. You don’t need to manage the ACL rules unless you need the level of permission customization if offers.

Please proceed to the following guides to learn more:

- Managing Users
- Managing Groups
- Managing VDCs
- Managing Permissions
By default, the authentication and authorization is handled by the OpenNebula Core as described above. Optionally, you can delegate it to an external module, see the Authentication Guide for more information.

6.2 Managing Users

OpenNebula supports user accounts and groups. This guide shows how to manage users, groups are explained in their own guide. To manage user rights, visit the Managing ACL Rules guide.

A user in OpenNebula is defined by a username and password. You don’t need to create a new Unix account in the front-end for each OpenNebula user, they are completely different concepts. OpenNebula users are authenticated using a session string included in every operation, which is checked by the OpenNebula core.

Each user has a unique ID, and belongs to a group.

After the installation, you will have two administrative accounts, oneadmin and serveradmin; and two default groups. You can check it using the oneuser list and onegroup list commands.

There are different user types in the OpenNebula system:

- **Cloud Administrators**, the oneadmin account is created the first time OpenNebula is started using the ONE_AUTH data. oneadmin has enough privileges to perform any operation on any object. Any other user in the oneadmin group has the same privileges as oneadmin
- **Infrastructure User** accounts may access most of the functionality offered by OpenNebula to manage resources.
- **Group Administrators** accounts manage a limited set of resources and users.
- **Users** access a simplified Sunstone view with limited actions to create new VMs, and perform basic life cycle operations.
- **Public users** can only access OpenNebula through a public API (EC2), hence they can only use a limited set of functionality and can not access the xml-rpc API directly (nor any application using it like the CLI or SunStone)

- User serveradmin is also created the first time OpenNebula is started. Its password is created randomly, and this account is used by the Sunstone and EC2 servers to interact with OpenNebula.

**Note:** The complete OpenNebula approach to user accounts, groups and VDC is explained in more detail in the Understanding OpenNebula guide.

6.2.1 Shell Environment

OpenNebula users should have the following environment variables set, you may want to place them in the .bashrc of the user’s Unix account for convenience:

**ONE_XMLRPC**

URL where the OpenNebula daemon is listening. If it is not set, CLI tools will use the default: http://localhost:2633/RPC2. See the PORT attribute in the Daemon configuration file for more information.
ONE_AUTH

Needs to point to a file containing a valid authentication key, it can be:

- A password file with just a single line stating "username:password".
- A token file with just a single line with "username:token", where token is a valid token created with the oneuser login command or API call.

If ONE_AUTH is not defined, $HOME/.one/one_auth will be used instead. If no auth file is present, OpenNebula cannot work properly, as this is needed by the core, the CLI, and the cloud components as well.

ONE_POOL_PAGE_SIZE

By default the OpenNebula Cloud API (CLI and Sunstone make use of it) paginates some pool responses. By default this size is 2000 but it can be changed with this variable. A numeric value greater that 2 is the pool size. To disable it you can use a non numeric value.

```
$ export ONE_POOL_PAGE_SIZE=5000  # Sets the page size to 5000
$ export ONE_POOL_PAGE_SIZE=disabled  # Disables pool pagination
```

ONE_CERT_DIR and ONE_DISABLE_SSL_VERIFY

If OpenNebula XMLRPC endpoint is behind an SSL proxy you can specify an extra trusted certificates directory using ONE_CERT_DIR. Make sure that the certificate is named <hash>.0. You can get the hash of a certificate with this command:

```
$ openssl x509 -in <certificate.pem> -hash
```

Alternatively you can set the environment variable ONE_DISABLE_SSL_VERIFY to any value to disable certificate validation. You should only use this parameter for testing as it makes the connection insecure.

For instance, a user named regularuser may have the following environment:

```
$ tail ~/.bashrc
ONE_XMLRPC=http://localhost:2633/RPC2
export ONE_XMLRPC

$ cat ~/.one/one_auth
regularuser:password
```

Note: Please note that the example above is intended for a user interacting with OpenNebula from the front-end, but you can use it from any other computer. Just set the appropriate hostname and port in the ONE_XMLRPC variable.

Note: If you do not want passwords to be stored in plain files, protected with basic filesystem permissions, please refer to the token-based authentication mechanism described below.

An alternative method to specify credentials and OpenNebula endpoint is using command line parameters. Most of the commands can understand the following parameters:

```
--user name
User name used to connect to OpenNebula
--password password
Password to authenticate with OpenNebula
--endpoint endpoint
```

6.2. Managing Users
URL of OpenNebula xmlrpc frontend

If `user` is specified but not `password` the user will be prompted for the password. `endpoint` has the same meaning and get the same value as `ONE_XMLRPC`. For example:

```
$ onevm list --user my_user --endpoint http://one.frontend.com:2633/RPC2
Password: 
[...]
```

**Warning:** You should better not use `--password` parameter in a shared machine. Process parameters can be seen by any user with the command `ps` so it is highly insecure.

**Shell Environment for Self-Contained Installations**

If OpenNebula was installed from sources in **self-contained mode** (this is not the default, and not recommended), these two variables must be also set. These are not needed if you installed from packages, or performed a system-wide installation from sources.

**ONE_LOCATION**

It must point to the installation `<destination_folder>`.

**PATH**

The OpenNebula bin files must be added to the path

```
$ export PATH=$ONE_LOCATION/bin:$PATH
```

### 6.2.2 Adding and Deleting Users

User accounts within the OpenNebula system are managed by `oneadmin` with the `oneuser create` and `oneuser delete` commands. This section will show you how to create the different account types supported in OpenNebula

**Administrators**

Administrators can be easily added to the system like this:

```
$ oneuser create otheradmin password
ID: 2

$ oneuser chgrp otheradmin oneadmin

$ oneuser list

<table>
<thead>
<tr>
<th>ID</th>
<th>GROUP</th>
<th>NAME</th>
<th>AUTH</th>
<th>PASSWORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>oneadmin</td>
<td>oneadmin</td>
<td>core</td>
<td>5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8</td>
</tr>
<tr>
<td>1</td>
<td>oneadmin</td>
<td>serveradmin</td>
<td>server_c</td>
<td>1224ff12545a2e5dfeda4eddacdc682d719c26d5</td>
</tr>
<tr>
<td>2</td>
<td>oneadmin</td>
<td>otheradmin</td>
<td>core</td>
<td>5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8</td>
</tr>
</tbody>
</table>

$ oneuser show otheradmin

<table>
<thead>
<tr>
<th>USER 2 INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID                  : 2</td>
</tr>
<tr>
<td>NAME                : otheradmin</td>
</tr>
<tr>
<td>GROUP               : 0</td>
</tr>
<tr>
<td>PASSWORD            : 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8</td>
</tr>
<tr>
<td>AUTH_DRIVER         : core</td>
</tr>
</tbody>
</table>
```
Regular Users

Simply create the users with the create command:

```
$ oneuser create regularuser password
ID: 3
```

The enabled flag can be ignored as it doesn’t provide any functionality. It may be used in future releases to temporarily disable users instead of deleting them.

Public Users

Public users need to define a special authentication method that internally relies on the core auth method. First create the public user as it was a regular one:

```
$ oneuser create publicuser password
ID: 4
```

and then change its auth method (see below for more info) to the public authentication method.

```
$ oneuser chauth publicuser public
```

Server Users

Server user accounts are used mainly as proxy authentication accounts for OpenNebula services. Any account that uses the server_cipher or server_x509 auth methods are a server user. You will never use this account directly. To create a user account just create a regular account

```
$ oneuser create serveruser password
ID: 5
```

and then change its auth method to `server_cipher` (for other auth methods please refer to the Authentication guide):

```
$ oneuser chauth serveruser server_cipher
```

6.2.3 Managing Users

User Authentication

In order to authenticate with OpenNebula you need a valid password or authentication token. Its meaning depends on the authentication driver, `AUTH_DRIVER`, set for the user. Note that you will be using this password or token to authenticate within the Sunstone portal or at the CLI/API level.

The default driver, `core`, is a simple user-password match mechanism. To configure a user account simply add to `$HOME/.one/one_auth` a single line with the format `<username>:<password>`. For example, for user `oneadmin` and password `opennebula` the file would be:

```
$ cat $HOME/.one/one_auth
oneadmin:opennebula
```

6.2. Managing Users
Once configured you will be able to access the OpenNebula API and use the CLI tools:

```
$ oneuser show
USER 0 INFORMATION
ID : 0
NAME : oneadmin
GROUP : oneadmin
PASSWORD : c24783ba96a35464632a624d9f829136edc0175e
```

**Note:** OpenNebula does not store the plain password but a hashed version in the database, as show by the `oneuser` example above.

Note that `$HOME/.one/one_auth` is just protected with the standard filesystem permissions. To improve the system security you can use authentication tokens. In this way there is no need to store plain passwords, OpenNebula can generate or use an authentication token with a given expiration time. By default, the tokens are also stored in `$HOME/.one/one_auth`.

The following example shows the token generation and usage for the previous `oneadmin` user:

```
$ ls $ONE_AUTH
ls: cannot access /home/oneadmin/.one/one_auth: No such file or directory

$ oneuser login oneadmin
Password:

$cat $HOME/.one/one_auth
oneadmin:800481374d8888805dd51dabd36ca50d77e2132e

$ oneuser show
USER 0 INFORMATION
ID : 0
NAME : oneadmin
GROUP : oneadmin
PASSWORD : c24783ba96a35464632a624d9f829136edc0175e
AUTH_DRIVER : core
LOGIN_TOKEN : 800481374d8888805dd51dabd36ca50d77e2132e
TOKEN VALIDITY : not after 2014-09-15 14:27:19 +0200
```

By default tokens are generated with a valid period of ten hours. This can be adjusted when issuing the token with the `oneuser login` command. You can also use this token to authenticate through Sunstone.

Finally, you can configure multiple authentication drivers, read the **External Auth guide** for more information about, enabling **LDAP/AD**, **SSH** or **x509** authentication.

**Note:** The purpose of the `$HOME/.one/one_auth` file and the token generation/usage are valid for any authentication mechanism.

**User Templates**

The **USER TEMPLATE** section can hold any arbitrary data. You can use the `oneuser update` command to open an editor and add, for instance, the following **DEPARTMENT** and **EMAIL** attributes:

```
$ oneuser show 2
USER 2 INFORMATION
ID : 2
NAME : regularuser
GROUP : 1
```
These attributes can be later used in the Virtual Machine Contextualization. For example, using contextualization the user’s public ssh key can be automatically installed in the VM:

```
ssh_key = "$USER[SSH_KEY]"
```

### 6.2.4 Manage your Own User

Regular users can see their account information, and change their password.

For instance, as regularuser you could do the following:

```
$ oneuser list

$ oneuser show
USER 2 INFORMATION
ID : 2
NAME : regularuser
GROUP : 1
PASSWORD : 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
AUTH_DRIVER : core
ENABLED : Yes

USER TEMPLATE
DEPARTMENT=IT
EMAIL=user@company.com

$ oneuser passwd 1 abcdpass
```

As you can see, any user can find out his ID using the `oneuser show` command without any arguments.

Regular users can retrieve their quota and user information in the settings section in the top right corner of the main
6.2.5 Managing Users in Sunstone

All the described functionality is available graphically using Sunstone:

6.3 Managing Groups

A group in OpenNebula makes it possible to isolate users and resources. A user can see and use the shared resources from other users.
The group is an authorization boundary for the users, but you can also partition your cloud infrastructure and define what resources are available to each group using Virtual Data Centers (VDC). You can read more about OpenNebula’s approach to VDCs and the cloud from the perspective of different user roles in the Understanding OpenNebula guide.

### 6.3.1 Adding and Deleting Groups

There are two special groups created by default. The onedmin group allows any user in it to perform any operation, allowing different users to act with the same privileges as the oneadmin user. The users group is the default group where new users are created.

You can use the onegroup command line tool to manage groups in OpenNebula. There are two groups created by default, oneadmin and users.

To create new groups:

```bash
$ onegroup list
   ID   NAME
   0   oneadmin
   1   users

$ onegroup create "new group"
   ID: 100
```

The new group has ID 100 to differentiate the special groups from the user-defined ones.

**Note:** When a new group is created, an ACL rule is also created to provide the default behaviour, allowing users to create basic resources. You can learn more about ACL rules in this guide; but you don’t need any further configuration to start using the new group.

### 6.3.2 Adding Users to Groups

Use the oneuser chgrp command to assign users to groups.

```bash
$ oneuser chgrp -v regularuser "new group"
   USER 1: Group changed

$ onegroup show 100
   GROUP 100 INFORMATION
   ID   : 100
   NAME : new group

   USERS
   ID   NAME
   1    regularuser
```

To delete a user from a group, just move it again to the default users group.

### 6.3.3 Admin Users and Allowed Resources

Upon group creation, a special admin user account can be defined. This admin user will have administrative privileges only for the new group, not for all the resources in the OpenNebula cloud as the ‘oneadmin’ group users have.

Another aspect that can be controlled on creation time is the type of resources that group users will be allowed to create.
This can be managed visually in Sunstone, and can also be managed through the CLI. In the latter, details of the group are passed to the `onegroup create` command as arguments. This table lists the description of said arguments.

<table>
<thead>
<tr>
<th>Argument</th>
<th>M / O</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-n, --name name</td>
<td>Manda-</td>
<td>Any string</td>
<td>Name for the new group</td>
</tr>
<tr>
<td>-u, --admin_user</td>
<td>Opti-</td>
<td>Any string</td>
<td>Creates an admin user for the group with the given name</td>
</tr>
<tr>
<td>-p, --admin_password</td>
<td>Opti-</td>
<td>Any string</td>
<td>Password for the admin user of the group</td>
</tr>
<tr>
<td>-d, --admin_driver</td>
<td>Opti-</td>
<td>Any string</td>
<td>Auth driver for the admin user of the group</td>
</tr>
<tr>
<td>-r, --resources</td>
<td>Opti-</td>
<td>“+” separated list</td>
<td>Which resources can be created by group users (VM+IMAGE+TEMPLATE by default)</td>
</tr>
</tbody>
</table>

An example:

```bash
$ onegroup create --name groupA \
    --admin_user admin_userA --admin_password somestr \
    --resources TEMPLATE+VM
```

### 6.3.4 Add Admin Users to an Existing Group

Any user can be configured to be Admin of a group with the commands `onegroup addadmin` and `deladmin`. 
6.3.5 Managing Groups and Virtual Resources

You can make the following virtual resources available to group users:

- Virtual Machine Templates
- Service Templates
- Images
- Files & Kernels

To make a virtual resource owned by oneadmin available to users of the new group, you have two options:

- Change the resource’s group, and give it GROUP USE permissions. This will make the resource only available to users in that group. The recommended practice to assign golden resources to groups is to first clone the resource and then assign it to the desired group for their users’ consumption.

- Leave the resource in the oneadmin group, and give it OTHER USE permissions. This will make the resource available to every user in OpenNebula.
The Virtual Machine and Service Templates are visible to the group users when they want to create a new VM or Service. The Images (including File Images) used by those Templates are not visible to the users, but must be also made available, otherwise the VM creation will fail with an error message similar to this one:

```
```

You can read more about OpenNebula permissions in the *Managing Permissions* and *Managing ACL Rules* guides.

### 6.3.6 Primary and Secondary Groups

With the commands `oneuser addgroup` and `delgroup` the administrator can add or delete secondary groups. Users assigned to more than one group will see the resources from all their groups. e.g. a user in the groups testing and production will see VMs from both groups.

The group set with `chgrp` is the primary group, and resources (Images, VMs, etc) created by a user will belong to this primary group. Users can change their primary group to any of their secondary group without the intervention of an administrator, using `chgrp` again.

### 6.3.7 Managing Groups in Sunstone

All the described functionality is available graphically using *Sunstone*: 

---

<table>
<thead>
<tr>
<th>Permissions:</th>
<th>Use</th>
<th>Manage</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Ownership**

- **Owner**: `oneadmin`
- **Group**:
  - `0: oneadmin`
  - `1: users`
  - `101: devs`
6.4 Managing VDCs

A VDC (Virtual Data Center) defines an assignment of one or several groups to a pool of physical resources. This pool of Physical Resources consists of resources from one or several Clusters that could belong to different Zones or public external clouds for hybrid cloud computing. You can read more about OpenNebula’s approach to VDCs and the cloud from the perspective of different user roles in the Understanding OpenNebula guide.

6.4.1 The Default VDC

There is a special default VDC created during the installation that allows the use of ALL the physical resources. The users group belongs to this VDC, and any new group is automatically added to the default VDC. You can modify the VDC physical resources, even remove all of them, but it can’t be deleted.

Note: Before adding a new group to a specific VDC, you may want to remove it from the default one, since it allows the use of ALL the physical resources.

6.4.2 Adding and Deleting VDCs

Your can use the onevdc command line tool to manage VDCs in OpenNebula.

To create new VDCs:

```
$ onevdc list
ID  NAME
  0  default

$ onevdc create "high-performance"
ID: 100
```

The new VDC has ID 100 to differentiate the default VDC from the user-defined ones.
6.4.3 Adding Groups to VDCs

By default a group doesn’t belong to any VDC, so users won’t be entitled to use any resource until explicitly added to one.

To add groups to a VDC:

```
$ onevdc addgroup <vdc_id> <group_id>
```

6.4.4 Adding Physical Resources to VDCs

Physical resources (hosts, virtual networks, and datastores) can be added to the VDC. Internally, the VDC will create ACL Rules that will allow the VDC groups to use this pool of resources.

Typically, you will want to add Clusters to the VDC. For instance, Cluster 7 from Zone 0:

```
$ onevdc addcluster <vdc_id> 0 7
```

But you can also add individual hosts, virtual networks, and datastores:

```
$ onevdc addhost <vdc_id> 0 3
$ onevdc addvnet <vdc_id> 0 9
$ onevdc adddatastore <vdc_id> 0 102
```

The special id ALL can be used to add all clusters/hosts/vnets/datastores from the given zone:

```
$ onevdc addcluster <group_id> 0 ALL
```

To remove physical resources from the VDC, use the symmetric operations delcluster, delhost, delvnet, deldatastore.

When you assign physical resources to a VDC, users in that VDC’s groups will be able to use the Datastores and Virtual Networks. The scheduler will also deploy VMs from that group to any of the VDC Hosts.

If you are familiar with ACL rules, you can take a look at the rules that are created with oneacl list. These rules are automatically added, and should not be manually edited. They will be removed by the onevdc del* commands.

6.4.5 Examples

The VDC management offers plenty of flexibility to suit many different scenarios. This section lists a few of them to help to visualize the possibilities of your OpenNebula infrastructure.

For example, let’s say Web Development, Human Resources, and Big Data Analysis as business units represented by Groups in a private OpenNebula cloud, with resources allocated from your zones and public clouds in order to create three different VDCs.

- **VDC BLUE**: VDC that allocates resources from DC_West_Coast + Cloudbursting to Web Development
- **VDC RED**: VDC that allocates resources from DC_West_Coast + DC_Europe + Cloudbursting to Human Resources
- **VDC GREEN**: VDC that allocates resources from DC_West_Coast + DC_Europe to Big Data Analysis
Flexible Groups

If you plan to have a small infrastructure, the VDC management may seem like an unnecessary extra step to assign physical resources to each Group. But having an independent VDC object allows it to have more than one Group, and at the same time a Group can be part of more than one VDC.

In practical terms, this means that once you organize your Users into Groups, and then your physical resources into VDCs, you can easily assign more or less resources to those Groups.

Using the previous scenario as an example, the Cloud Admin can add the Group Web Development to the VDCs RED and GREEN if their workload increases, and then remove it again a few days later.

Create Super-Clusters

A VDC can have more than one physical resource of each type (Cluster, Hosts, VNets, Datastores), and a physical resource can be in more than one VDC. In contrast, a Host, VNet or Datastore can be part of only one Cluster. This means that you can decide to create a VDC that encompasses resources that may not be part of the same physical Cluster.

For example, a VDC called ‘high-performance’ may contain Hosts from two incompatible Clusters, let’s say ‘kvm-ceph’ and ‘xen-gluster’. These Hosts may be part of the same VDC, but from the deployment point of view, the important factor is their Cluster. The scheduler will decide the deployment target based on each Host’s Cluster, and this guarantees that the VMs are always deployed in a compatible Host.

Partition a Cluster

Since a VDC can contain individual Hosts, VNets and Datastores, you can use VDCs to partition a Cluster into “sub-clusters” that contain a few Hosts.
Following the previous example, you may have a big “kvm-ceph” Cluster. A VDC with one or two Hosts can be created to isolate a small portion of the Cluster. In this case, remember to add the necessary Datastores and VNets to the VDC, otherwise the Users won’t be able to instantiate the VM Templates.

**Share Physical Resources**

You may have two Groups with a similar workload, but want to keep their users and virtual resources isolated. In this case, both can be added to the same VDC. In a similar way, a physical resource (such as a host) can be part of two different VDCs.

The Groups will share the physical resources, but without being aware of it. If the physical resources are not exclusively assigned to a Group, you may want to set *usage quotas*.

### 6.4.6 Managing VDCs in Sunstone

All the described functionality is available graphically using *Sunstone*:

![Sunstone Interface](image.png)

**6.5 Managing Permissions**

Most OpenNebula resources have associated permissions for the *owner*, the users in her *group*, and *others*. For each one of these groups, there are three rights that can be set: *USE*, *MANAGE* and *ADMIN*. These permissions are very similar to those of UNIX file system.
The resources with associated permissions are Templates, VMs, Images and Virtual Networks. The exceptions are Users, Groups and Hosts.

### 6.5.1 Managing Permission through the CLI

This is how the permissions look in the terminal:

```bash
$ onetemplate show 0
TEMPLATE 0 INFORMATION
ID : 0
NAME : vm-example
USER : oneuser1
GROUP : users
REGISTER TIME : 01/13 05:40:28

PERMISSIONS
OWNER : um-
GROUP : u--
OTHER : ---

[...]
```

The previous output shows that for the Template 0, the owner user `oneuser1` has USE and MANAGE rights. Users in the group `users` have USE rights, and users that are not the owner or in the `users` group don’t have any rights over this Template.

You can check what operations are allowed with each of the USE, MANAGE and ADMIN rights in the xml-rpc reference documentation. In general these rights are associated with the following operations:

- **USE**: Operations that do not modify the resource like listing it or using it (e.g. using an image or a virtual network). Typically you will grant USE rights to share your resources with other users of your group or with the rest of the users.

- **MANAGE**: Operations that modify the resource like stopping a virtual machine, changing the persistent attribute of an image or removing a lease from a network. Typically you will grant MANAGE rights to users that will manage your own resources.

- **ADMIN**: Special operations that are typically limited to administrators, like updating the data of a host or deleting an user group. Typically you will grant ADMIN permissions to those users with an administrator role.

**Warning**: By default every user can update any permission group (owner, group or other) with the exception of the admin bit. There are some scenarios where it would be advisable to limit the other set (e.g. OpenNebula Zones so users can not break the group limits). In these situations the ENABLE_OTHER_PERMISSIONS attribute can be set to NO in `/etc/one/oned.conf` file.

### Changing Permissions with chmod

The previous permissions can be updated with the chmod command. This command takes an octet as a parameter, following the octal notation of the Unix chmod command. The octet must be a three-digit base-8 number. Each digit, with a value between 0 and 7, represents the rights for the owner, group and other, respectively. The rights are represented by these values:

- **USE** bit adds 4 to its total (in binary 100)
- **MANAGE** bit adds 2 to its total (in binary 010)
- **ADMIN** bit adds 1 to its total (in binary 001)
Let’s see some examples:

```
$ onetemplate show 0
... 
PERMISSIONS
OWNER : um-
GROUP : u--
OTHER : ---

$ onetemplate chmod 0 664 -v
VMTEMPLATE 0: Permissions changed

$ onetemplate show 0
...
PERMISSIONS
OWNER : um-
GROUP : um-
OTHER : u--

$ onetemplate chmod 0 644 -v
VMTEMPLATE 0: Permissions changed

$ onetemplate show 0
...
PERMISSIONS
OWNER : um-
GROUP : u--
OTHER : u--

$ onetemplate chmod 0 607 -v
VMTEMPLATE 0: Permissions changed

$ onetemplate show 0
...
PERMISSIONS
OWNER : um-
GROUP : ---
OTHER : um-
```

Setting Default Permissions with umask

The default permissions given to newly created resources can be set:

- Globally, with the `DEFAULT_UMASK` attribute in `oned.conf`
- Individually for each User, using the `oneuser umask` command.

These mask attributes work in a similar way to the Unix `umask` command. The expected value is a three-digit base-8 number. Each digit is a mask that disables permissions for the `owner`, `group` and `other`, respectively.

This table shows some examples:

<table>
<thead>
<tr>
<th>umask</th>
<th>permissions (octal)</th>
<th>permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>177</td>
<td>600</td>
<td>um- --- ---</td>
</tr>
<tr>
<td>137</td>
<td>640</td>
<td>um- u-- ---</td>
</tr>
<tr>
<td>113</td>
<td>664</td>
<td>um- um- u--</td>
</tr>
</tbody>
</table>
### 6.5.2 Managing Permissions in Sunstone

Sunstone offers a convenient way to manage resources permissions. This can be done by selecting resources from a view (for example the templates view) and clicking on the **update properties** button. The update dialog lets the user conveniently set the resource’s permissions.

![Image of Sunstone interface](image)

### 6.6 Accounting Client

The accounting toolset visualizes and reports resource usage data. This accounting tool addresses the accounting of the virtual resources. It includes resource consumption of the virtual machines as reported from the hypervisor.

#### 6.6.1 Usage

**oneacct** - prints accounting information for virtual machines

```
Usage: oneacct [options]

-s, --start TIME  Start date and time to take into account
-e, --end TIME    End date and time
-u, --user user   User id to filter the results
-g, --group group Group id to filter the results
-H, --host hostname Host id to filter the results
- xpath expression Xpath expression to filter the results. For example: oneacct --xpath 'HISTORY[ETIME>0]'  
-j, --json         Output in json format
-x, --xml          Output in xml format
--csv              Write table in csv format
- --split          Split the output in a table for each VM
-h, --help         Show this message
```

The time can be written as **month/day/year hour:minute:second**, or any other similar format, e.g **month/day hour:minute**.

To integrate this tool with other systems you can use **-j**, **-x** or **--csv** flags to get all the information in an easy computer readable format.
6.6.2 Accounting Output

The oneacct command shows individual Virtual Machine history records. This means that for a single VM you may get several accounting entries, one for each migration or stop/suspend action. A resize or disk/nic attachment will also create a new entry.

Each entry contains the complete information of the Virtual Machine, including the Virtual Machine monitoring information. By default, only network consumption is reported, see the Tuning & Extending section for more information.

When the results are filtered with the -s and/or -e options, all the history records that were active during that time interval are shown, but they may start or end outside that interval.

For example, if you have a VM that was running from 01/01/2012 to 05/15/2012, and you request the accounting information with this command:

```
$ oneacct -s '02/01/2012' -e '01/03/2012'
Showing active history records from Wed Feb 01 00:00:00 +0100 2012 to Tue Jan 03 00:00:00 +0100 2012
```

<table>
<thead>
<tr>
<th>VID</th>
<th>HOSTNAME</th>
<th>REAS</th>
<th>START_TIME</th>
<th>END_TIME</th>
<th>MEMORY</th>
<th>CPU</th>
<th>NET_RX</th>
<th>NET_TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>host01</td>
<td>none</td>
<td>01/01 14:03:27</td>
<td>05/15 16:38:05</td>
<td>1024K</td>
<td>2</td>
<td>1.5G</td>
<td>23G</td>
</tr>
</tbody>
</table>

The record shows the complete history record, and total network consumption. It will not reflect the consumption made only during the month of February.

Other important thing to pay attention to is that active history records, those with END_TIME '-', refresh their monitoring information each time the VM is monitored. Once the VM is shut down, migrated or stopped, the END_TIME is set and the monitoring information stored is frozen. The final values reflect the total for accumulative attributes, like NET_RX/TX.

Sample Output

Obtaining all the available accounting information:

```
$ oneacct
# User 0 oneadmin
```

<table>
<thead>
<tr>
<th>VID</th>
<th>HOSTNAME</th>
<th>REAS</th>
<th>START_TIME</th>
<th>END_TIME</th>
<th>MEMORY</th>
<th>CPU</th>
<th>NET_RX</th>
<th>NET_TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>host02</td>
<td>user</td>
<td>06/04 14:55:49</td>
<td>06/04 15:05:02</td>
<td>1024M</td>
<td>1</td>
<td>0K</td>
<td>0K</td>
</tr>
</tbody>
</table>

```
# User 2 oneuser1
```

<table>
<thead>
<tr>
<th>VID</th>
<th>HOSTNAME</th>
<th>REAS</th>
<th>START_TIME</th>
<th>END_TIME</th>
<th>MEMORY</th>
<th>CPU</th>
<th>NET_RX</th>
<th>NET_TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>host01</td>
<td>stop</td>
<td>06/04 14:55:49</td>
<td>06/04 14:56:28</td>
<td>1024M</td>
<td>1</td>
<td>0K</td>
<td>0K</td>
</tr>
<tr>
<td>1</td>
<td>host01</td>
<td>user</td>
<td>06/04 14:56:49</td>
<td>06/04 14:58:49</td>
<td>1024M</td>
<td>1</td>
<td>0K</td>
<td>0.6K</td>
</tr>
<tr>
<td>1</td>
<td>host02</td>
<td>none</td>
<td>06/04 14:58:49</td>
<td>-</td>
<td>1024M</td>
<td>1</td>
<td>0K</td>
<td>0.1K</td>
</tr>
<tr>
<td>2</td>
<td>host02</td>
<td>erro</td>
<td>06/04 14:57:19</td>
<td>06/04 15:03:27</td>
<td>4G</td>
<td>2</td>
<td>OK</td>
<td>0K</td>
</tr>
<tr>
<td>3</td>
<td>host01</td>
<td>none</td>
<td>06/04 15:04:47</td>
<td>-</td>
<td>4G</td>
<td>2</td>
<td>OK</td>
<td>0.1K</td>
</tr>
</tbody>
</table>

The columns are:
Obtaining the accounting information for a given user

$ oneacct -u 2 --split

# User 2 oneuser1

<table>
<thead>
<tr>
<th>VID</th>
<th>HOSTNAME</th>
<th>REAS</th>
<th>START_TIME</th>
<th>END_TIME</th>
<th>MEMORY</th>
<th>CPU</th>
<th>NET_RX</th>
<th>NET_TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>host01</td>
<td>stop</td>
<td>06/04 14:55:49</td>
<td>06/04 14:56:28</td>
<td>1024M</td>
<td>1</td>
<td>0K</td>
<td>0K</td>
</tr>
<tr>
<td>1</td>
<td>host01</td>
<td>user</td>
<td>06/04 14:56:49</td>
<td>06/04 14:58:49</td>
<td>1024M</td>
<td>1</td>
<td>0K</td>
<td>0.6K</td>
</tr>
<tr>
<td>1</td>
<td>host02</td>
<td>none</td>
<td>06/04 14:58:49</td>
<td>-</td>
<td>1024M</td>
<td>1</td>
<td>0K</td>
<td>0.1K</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VID</th>
<th>HOSTNAME</th>
<th>REAS</th>
<th>START_TIME</th>
<th>END_TIME</th>
<th>MEMORY</th>
<th>CPU</th>
<th>NET_RX</th>
<th>NET_TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>host02</td>
<td>erro</td>
<td>06/04 14:57:19</td>
<td>06/04 15:03:27</td>
<td>4G</td>
<td>2</td>
<td>0K</td>
<td>0K</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VID</th>
<th>HOSTNAME</th>
<th>REAS</th>
<th>START_TIME</th>
<th>END_TIME</th>
<th>MEMORY</th>
<th>CPU</th>
<th>NET_RX</th>
<th>NET_TX</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>host01</td>
<td>none</td>
<td>06/04 15:04:47</td>
<td>-</td>
<td>4G</td>
<td>2</td>
<td>0K</td>
<td>0.1K</td>
</tr>
</tbody>
</table>

In case you use CSV output (--csv) you will get a header with the name of each column and then the data. For example:

$ oneacct --csv

| UID,VID,HOSTNAME,ACTION,REASON,START_TIME,END_TIME,MEMORY,CPU,NET_RX,NET_TX |
|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| 3,68,esx2,none,none,02/17 11:16:06,-- ,512M,1,OK,OK |
| 0,0,piscis,none,erro,09/18 15:57:55,09/18 15:57:57,1024M,1,OK,OK |
| 0,0,piscis,shutdown-hard,user,09/18 16:01:55,09/18 16:19:57,1024M,1,OK,OK |
| 0,1,piscis,none,09/18 16:20:25,-- ,1024M,1,2G,388M |
| 0,2,esx1,shutdown-hard,user,09/18 19:27:14,09/19 12:23:45,512M,1,OK,OK |

Output Reference

If you execute oneacct with the -x option, you will get an XML output defined by the following xsd:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"

  <xs:element name="HISTORY_RECORDS">
    <xs:complexType>
      <xs:sequence maxOccurs="1" minOccurs="1">
        ...
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```
<xs:element name="HISTORY">  
  <xs:complexType>  
    <xs:sequence>  
      <xs:element name="OID" type="xs:integer"/>  
      <xs:element name="SEQ" type="xs:integer"/>  
      <xs:element name="HOSTNAME" type="xs:string"/>  
      <xs:element name="HID" type="xs:integer"/>  
      <xs:element name="STIME" type="xs:integer"/>  
      <xs:element name="ETIME" type="xs:integer"/>  
      <xs:element name="VMMMAD" type="xs:string"/>  
      <xs:element name="VNMMAD" type="xs:string"/>  
      <xs:element name="TMMAD" type="xs:string"/>  
      <xs:element name="DS_ID" type="xs:integer"/>  
      <xs:element name="PSTIME" type="xs:integer"/>  
      <xs:element name="PETIME" type="xs:integer"/>  
      <xs:element name="RSTIME" type="xs:integer"/>  
      <xs:element name="RETIME" type="xs:integer"/>  
      <xs:element name="ESTIME" type="xs:integer"/>  
      <xs:element name="EETIME" type="xs:integer"/>  
      <!-- REASON values:  
      NONE   = 0 Normal termination  
      ERROR  = 1 The VM ended in error  
      STOP_RESUME = 2 Stop/resume request  
      USER   = 3 Migration request  
      CANCEL = 4 Cancel request  
      -->  
      <xs:element name="REASON" type="xs:integer"/>  
    </xs:sequence>  
  </xs:complexType>  
</xs:element>  

<xs:element name="VM">  
  <xs:complexType>  
    <xs:sequence>  
      <xs:element name="ID" type="xs:integer"/>  
      <xs:element name="UID" type="xs:integer"/>  
      <xs:element name="GID" type="xs:integer"/>  
      <xs:element name="UNAME" type="xs:string"/>  
      <xs:element name="GNAME" type="xs:string"/>  
      <xs:element name="NAME" type="xs:string"/>  
      <xs:element name="PERMISSIONS" minOccurs="0" maxOccurs="1">  
        <xs:complexType>  
          <xs:sequence>  
            <xs:element name="OWNER_U" type="xs:integer"/>  
            <xs:element name="OWNER_M" type="xs:integer"/>  
            <xs:element name="OWNER_A" type="xs:integer"/>  
            <xs:element name="GROUP_U" type="xs:integer"/>  
            <xs:element name="GROUP_M" type="xs:integer"/>  
            <xs:element name="GROUP_A" type="xs:integer"/>  
            <xs:element name="OTHER_U" type="xs:integer"/>  
            <xs:element name="OTHER_M" type="xs:integer"/>  
            <xs:element name="OTHER_A" type="xs:integer"/>  
          </xs:sequence>  
        </xs:complexType>  
      </xs:element>  
    </xs:sequence>  
  </xs:complexType>  
</xs:element>
<xs:element name="LAST_POLL" type="xs:integer"/>

<!-- STATE values,
see http://opennebula.org/documentation:documentation:api#actions_for_virtual_machine_management

INIT = 0
PENDING = 1
HOLD = 2
ACTIVE = 3 In this state, the Life Cycle Manager state is relevant
STOPPED = 4
SUSPENDED = 5
DONE = 6
POWEROFF = 8
-->
<xs:element name="STATE" type="xs:integer"/>

<!-- LCM_STATE values, this sub-state is relevant only when STATE is
ACTIVE (4)

LCM_INIT = 0
PROLOG = 1
BOOT = 2
RUNNING = 3
MIGRATE = 4
SAVE_STOP = 5
SAVE_SUSPEND = 6
SAVE_MIGRATE = 7
PROLOG_MIGRATE = 8
PROLOG_RESUME = 9
EPILOG_STOP = 10
EPILOG = 11
SHUTDOWN = 12
CANCEL = 13
FAILURE = 14
CLEANUP = 15
UNKNOWN = 16
HOTPLUG = 17
SHUTDOWN_POWEROFF = 18
BOOT_UNKNOWN = 19
BOOT_POWEROFF = 20
BOOT_SUSPENDED = 21
BOOT_STOPPED = 22
-->
<xs:element name="LCM_STATE" type="xs:integer"/>
<xs:element name="RESCHED" type="xs:integer"/>
<xs:element name="STIME" type="xs:integer"/>
<xs:element name="ETIME" type="xs:integer"/>
<xs:element name="DEPLOY_ID" type="xs:string"/>

<!-- MEMORY consumption in kilobytes -->
<xs:element name="MEMORY" type="xs:integer"/>

<!-- Percentage of 1 CPU consumed (two fully consumed cpu is 200) -->
<xs:element name="CPU" type="xs:integer"/>

<!-- NET_TX: Sent bytes to the network -->
<xs:element name="NET_TX" type="xs:integer"/>
6.6.3 Sunstone

Sunstone also displays information about accounting. Information is accessible via the User dialogs for the user and admin views. The cloud view can access the metering information in the dashboard, whereas the group admin user can access them under the users section.

6.6.4 Tuning & Extending

There are two kinds of monitoring values:

- Instantaneous values: For example, VM/CPU or VM/MEMORY show the memory consumption last reported by the monitoring probes.
- Accumulative values: For example, VM/NET_TX and VM/NET_TX show the total network consumption since the history record started.

Developers interacting with OpenNebula using the Ruby bindings can use the `VirtualMachinePool.accounting` method to retrieve accounting information filtering and ordering by multiple parameters.
6.7 Showback

The showback toolset reports resource usage cost, and allows the integration with chargeback and billing platforms. The toolset generates showback reports using the information retrieved from OpenNebula.

6.7.1 Set the VM Cost

Each VM Template can optionally define a cost (see the syntax here). The cost is defined as cost per cpu per hour, and cost per memory MB per hour. The cost units are abstract and their equivalent to monetary or other cost metrics have to be defined in each deployment.

Using this cost schema allows the users to resize the Virtual Machine instances.
There is a default cost that will be applied to VM Templates without a cost defined. It can be set in the `oned.conf` file.
Warning: If your users can access the Sunstone ‘user’ view, it’s important to set a default cost. These users can manage their own Templates, which won’t have a specific cost assigned.

6.7.2 Calculate Monthly Reports

Before the cost reports can be seen by the users, the administrator has to generate them. To create the monthly cost reports, use the oneshowback command:

$ oneshowback calculate -h
Usage: oneshowback [options]
  -s, --start TIME  First month of the data
  -e, --end TIME    Last month of the data

When this command is executed, the OpenNebula core reads all the accounting records, and calculates the total cost for each month. The records include the total cost of the month, and basic information about the VM and its owner. This information is then stored in the database, to be consumed with the oneshowback list command.

The monthly cost of each VM is calculated as the sum of:

- CPU_COST * CPU * HOURS
- MEMORY_COST * MEMORY * HOURS
- DISK_COST * DISK_SIZE * HOURS

The number of hours is calculated as the total number of hours that a VM has been running. The time a VM is in other states, such as pending, poweroff, or stopped does not count towards the cost.

If the time range includes the current month, OpenNebula will calculate the cost up to today’s date. It is up to the administrators to leave the current month out of the showback records, to update it daily, or hourly. In any case, it is important to re-calculate it when the month ends. This operation can be easily automated by a cron job.

The oneshowback command can only be executed by the oneadmin user.

Some examples:

To calculate all records, starting from March up to today:

$ oneshowback calculate --start "03/2014"

To calculate only September:

$ oneshowback calculate --start "09/2014" --end "09/2014"

Note: This is a resource intensive operation. For big deployments, it is recommended to use the --start option to process only the last missing months.

Note: Existing records can be re-calculated. This can be useful to update old records when a VM is renamed, or the owner is changed. In this case, the cost of previous months will be also assigned to the new user.

6.7.3 Retrieve Monthly Reports

Any user or administrator can see their monthly showback reports from the CLI or Sunstone:
oneshowback list -h

## USAGE

list

    Returns the showback records

## OPTIONS

- **-s, --start TIME**    First month of the data
- **-e, --end TIME**      Last month of the data
- **-u, --userfilter user** User name or id to filter the results
- **-g, --group group**   Group name or id to filter the results
- **-x, --xml**           Show the resource in xml format
- **-j, --json**          Show the resource in json format
- **--describe**          Describe list columns
- **-l, --list x,y,z**    Selects columns to display with list command
- **--csv**               Write table in csv format
6.7.4 Disable Showback in Sunstone

Showback reports can be disabled in any of the Sunstone views modifying the yaml file of those views. These files can be found in /etc/one/sunstone-views

...  
features:  
    showback: false  

6.7.5 Tuning & Extending

To integrate the showback reports with external tools, you can get the CLI output as xml, json, or csv data.

$ oneshowback list -u cloud_user --list YEAR,MONTH,VM_ID,COST --csv  
YEAR,MONTH,VM_ID,COST  
2012,10,4258,1824279.62  
2012,10,4265,433749.03  
2012,11,4258,34248600

Developers interacting with OpenNebula using the Ruby bindings can use the VirtualMachinePool.showback method to retrieve showback information filtering and ordering by multiple parameters.

6.8 Managing ACL Rules

The ACL authorization system enables fine-tuning of the allowed operations for any user, or group of users. Each operation generates an authorization request that is checked against the registered set of ACL rules. The core then can grant permission, or reject the request.

This allows administrators to tailor the user roles according to their infrastructure needs. For instance, using ACL rules you could create a group of users that can see and use existing virtual resources, but not create any new ones. Or grant permissions to a specific user to manage Virtual Networks for some of the existing groups, but not to perform any other operation in your cloud. Some examples are provided at the end of this guide.

Please note: the ACL rules is an advanced mechanism. For most use cases, you should be able to rely on the built-in resource permissions and the ACL Rules created automatically when a group is created, and when physical resources are added to a VDC.

6.8.1 Understanding ACL Rules

Let's start with an example:

#5 IMAGE+TEMPLATE/@103 USE+MANAGE #0

This rule grants the user with ID 5 the right to perform USE and MANAGE operations over all Images and Templates in the group with id 103.

The rule is split in four components, separated by a space:

• **User** component is composed only by an ID definition.
• **Resources** is composed by a list of ‘+’ separated resource types, ‘/’ and an ID definition.
• **Rights** is a list of Operations separated by the ‘+’ character.
• **Zone** is an ID definition of the zones where the rule applies. This last part is optional, and can be ignored unless OpenNebula is configured in a federation.
The **ID definition** for User in a rule is written as:
- `#<id>` : for individual IDs
- `@<id>` : for a group ID
- `*` : for All

The **ID definition** for a Resource has the same syntax as the ones for Users, but adding:
- `%<id>` : for cluster IDs

Some more examples:

This rule allows all users in group 105 to create new virtual resources:

```
@105 VM+NET+IMAGE+TEMPLATE/* CREATE
```

The next one allows all users in the group 106 to use the Virtual Network 47. That means that they can instantiate VM templates that use this network.

```
@106 NET/#47 USE
```

**Note:** Note the difference between `* NET/#47 USE` vs `* NET/@47 USE`

All Users can use NETWORK with ID 47 vs All Users can use NETWORKS belonging to the Group whose ID is 47

The following one allows users in group 106 to deploy VMs in Hosts assigned to the cluster 100

```
@106 HOST/%100 MANAGE
```

### 6.8.2 Managing ACL Rules via Console

The ACL rules are managed using the `oneacl` command. The ‘oneacl list’ output looks like this:

```
$ oneacl list

<table>
<thead>
<tr>
<th>ID</th>
<th>USER</th>
<th>RES_VHNIUTGDCOZS</th>
<th>RID</th>
<th>OPE_UMAC</th>
<th>ZONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>@1</td>
<td>V-NI-T----O----</td>
<td>*</td>
<td>---c</td>
<td>#0</td>
</tr>
<tr>
<td>1</td>
<td>*</td>
<td>-----------Z---</td>
<td>*</td>
<td>u---</td>
<td>*</td>
</tr>
<tr>
<td>2</td>
<td>@1</td>
<td>H-------------</td>
<td>*</td>
<td>-m--</td>
<td>#0</td>
</tr>
<tr>
<td>3</td>
<td>@1</td>
<td>N----D------</td>
<td>*</td>
<td>u---</td>
<td>#0</td>
</tr>
<tr>
<td>4</td>
<td>#5</td>
<td>---N---------</td>
<td>@104</td>
<td>u---</td>
<td>#0</td>
</tr>
<tr>
<td>5</td>
<td>@106</td>
<td>---I--------</td>
<td>#31</td>
<td>u---</td>
<td>#0</td>
</tr>
</tbody>
</table>
```

The rules shown correspond to the following ones:

- `@1 VM+NET+IMAGE+TEMPLATE+DOCUMENT/* CREATE #0`
- `* ZONE/* USE *`
- `@1 HOST/* MANAGE #0`
- `@1 NET+DATASO#/* USE #0`
- `#5 NET+IMAGE+TEMPLATE/@104 USE #0`
- `@106 IMAGE/#31 USE #0`

The first four were created on bootstrap by OpenNebula, and the last two were created using oneacl:

```
$ oneacl create "#5 NET+IMAGE+TEMPLATE/@104 USE"
ID: 4

$ oneacl create "@106 IMAGE/#31 USE"
ID: 5
```
The ID column identifies each rule’s ID. This ID is needed to delete rules, using `oneacl delete <id>`.

Next column is USER, which can be an individual user (#) or group (@) id; or all (*) users.

The Resources column lists the existing Resource types initials. Each rule fills the initials of the resource types it applies to.

- V : VM
- H : HOST
- N : NET
- I : IMAGE
- U : USER
- T : TEMPLATE
- G : GROUP
- D : DATASTORE
- C : CLUSTER
- O : DOCUMENT
- Z : ZONE
- S : SECURITY GROUP

RID stands for Resource ID, it can be an individual object (#), group (@) or cluster (%) id; or all (*) objects.

The next Operations column lists the allowed operations initials.

- U : USE
- M : MANAGE
- A : ADMIN
- C : CREATE

And the last column, Zone, shows the zone(s) where the rule applies. It can be an individual zone id (#), or all (*) zone.

### 6.8.3 Managing ACLs via Sunstone

Sunstone offers a very intuitive and easy way of managing ACLs.

Select ACLs in the left-side menu to access a view of the current ACLs defined in OpenNebula:
This view is designed to easily understand what the purpose of each ACL is. You can create new ACLs by clicking on the New button at the top. A dialog will pop up:
In the creation dialog you can easily define the resources affected by the rule and the permissions that are granted upon them.

### 6.8.4 How Permission is Granted or Denied

**Note:** Visit the XML-RPC API reference documentation for a complete list of the permissions needed by each OpenNebula command.

For the internal Authorization in OpenNebula, there is an implicit rule:

- The oneadmin user, or users in the oneadmin group are authorized to perform any operation.

If the resource is one of type VM, NET, IMAGE, TEMPLATE, or DOCUMENT the object’s permissions are checked. For instance, this is an example of the oneimage show output:

```
$ oneimage show 2
IMAGE 2 INFORMATION
ID : 2
[...]
PERMISSIONS
OWNER : um-
```
The output above shows that the owner of the image has **USE** and **MANAGE** rights.

If none of the above conditions are true, then the set of ACL rules is iterated until one of the rules allows the operation.

An important concept about the ACL set is that each rule adds new permissions, and they can’t restrict existing ones: if any rule grants permission, the operation is allowed.

This is important because you have to be aware of the rules that apply to a user and his group. Consider the following example: if a user **#7** is in the group **@108**, with the following existing rule:

```
@108 IMAGE/#45 USE+MANAGE
```

Then the following rule won’t have any effect:

```
#7 IMAGE/#45 USE
```

### Special Authorization for Virtual Network Reservations

There is a special sub-type of Virtual Network: reservations. For these virtual networks the ACL system makes the following exceptions:

- ACL rules that apply to ALL (*) are ignored
- ACL rules that apply to a cluster (%) are ignored

The other ACL rules are enforced: individual (#) and group (@). The Virtual Network object’s permissions are also enforced as usual.

### 6.9 Managing Quotas

This guide will show you how to set the usage quotas for users and groups.

#### 6.9.1 Overview

The quota system tracks user and group usage of system resources, and allows the system administrator to set limits on the usage of these resources. Quota limits can be set for:

- **users**, to individually limit the usage made by a given user.
- **groups**, to limit the overall usage made by all the users in a given group. This can be of special interest for the OpenNebula Zones and Virtual Data Center (VDC) components.

#### 6.9.2 Which Resource can be limited?

The quota system allows you to track and limit usage on:

- **Datastores**, to control the amount of storage capacity allocated to each user/group for each datastore.
- **Compute**, to limit the overall memory, cpu or VM instances.
- **Network**, to limit the number of IPs a user/group can get from a given network. This is specially interesting for networks with public IPs, which usually are a limited resource.
• **Images**, you can limit the how many VM instances from a given user/group are using a given image. You can take advantage of this quota when the image contains consumable resources (e.g. software licenses).

### 6.9.3 Defining User/Group Quotas

Usage quotas are set in a traditional template syntax (either plain text or XML). The following table explains the attributes needed to set each quota:

**Datastore Quotas. Attribute name: DATASTORE**

<table>
<thead>
<tr>
<th>DATASTORE Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the Datastore to set the quota for</td>
</tr>
<tr>
<td>SIZE</td>
<td>Maximum size in MB that can be used in the datastore</td>
</tr>
<tr>
<td>IMAGE</td>
<td>Maximum number of images that can be created in the datastore</td>
</tr>
</tbody>
</table>

**Compute Quotas. Attribute name: VM**

<table>
<thead>
<tr>
<th>VM Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMS</td>
<td>Maximum number of VMs that can be created</td>
</tr>
<tr>
<td>MEMORY</td>
<td>Maximum memory in MB that can be requested by user/group VMs</td>
</tr>
<tr>
<td>CPU</td>
<td>Maximum CPU capacity that can be requested by user/group VMs</td>
</tr>
<tr>
<td>SYSTEM_DISK_SIZE</td>
<td>Maximum size (in MB) of system disks that can be requested by user/group VMs</td>
</tr>
</tbody>
</table>

**Network Quotas. Attribute name: NETWORK**

<table>
<thead>
<tr>
<th>NETWORK Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the Network to set the quota for</td>
</tr>
<tr>
<td>LEASES</td>
<td>Maximum IPs that can be leased from the Network</td>
</tr>
</tbody>
</table>

**Image Quotas. Attribute name: IMAGE**

<table>
<thead>
<tr>
<th>IMAGE Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the Image to set the quota for</td>
</tr>
<tr>
<td>RVMS</td>
<td>Maximum VMs that can used this image at the same time</td>
</tr>
</tbody>
</table>

For each quota, there are two special limits:

- **-1** means that the **default quota** will be used
- **-2** means **unlimited**

**Warning:** Each quota has an usage counter associated named `<QUOTA_NAME>_USED`. For example, `MEMORY_USED` means the total memory used by user/group VMs, and its associated quota is `MEMORY`.

The following template shows a quota example for a user in plain text. It limits the overall usage in Datastore 0 to 20Gb (for an unlimited number of images); the number of VMs that can be created to 4 with a maximum memory to 2G and 5 CPUs; the number of leases from network 1 to 4; and image 1 can only be used by 3 VMs at the same time:
Warning: Note that whenever a network, image, datastore or VM is used the corresponding quota counters are created for the user with an unlimited value. This allows to track the usage of each user/group even when quotas are not used.

### 6.9.4 Setting User/Group Quotas

User/group quotas can be easily set up either through the command line interface or sunstone. Note that you need MANAGE permissions to set a quota of a user, and ADMIN permissions to set the quota of a group. In this way, by default, only one admin can set quotas for a group, but if you define a group manager she can set specific usage quotas for the users on her group (so distributing resources as required). You can always change this behaviour setting the appropriate ACL rules.

To set the quota for a user, e.g. userA, just type:

```
$ oneuser quota userA
```

This will open an editor session to edit a quota template (with some tips about the syntax).

Warning: Usage metrics are included for information purposes (e.g. CPU_USED, MEMORY_USED, LEASES_USED...) you cannot modify them

Warning: You can add as many resource quotas as needed even if they have not been automatically initialized.

Similarly, you can set the quotas for group A with:
There is a `batchquota` command that allows you to set the same quotas for several users or groups:

```
$ oneuser batchquota userA, userB, 35
$ onegroup batchquota 100..104
```

You can also set the user/group quotas in Sunstone through the user/group tab.
6.9.5 Setting Default Quotas

There are two default quota limit templates, one for users and another for groups. This template applies to all users/groups, unless they have an individual limit set.

Use the `oneuser/onegroup defaultquota` command.

```
$ oneuser defaultquota
```

6.9.6 Checking User/Group Quotas

Quota limits and usage for each user/group is included as part of its standard information, so it can be easily check with the usual commands. Check the following examples:

```
$ oneuser show uA
USER 2 INFORMATION
ID : 2
NAME : uA
GROUP : gA
PASSWORD : a9993e364706816aba3e25717850c26c9cd0d89d
AUTH_DRIVER : core
ENABLED : Yes

USER TEMPLATE

RESOURCE USAGE & QUOTAS

<table>
<thead>
<tr>
<th>DATASTORE ID</th>
<th>IMAGES (used)</th>
<th>IMAGES (limit)</th>
<th>SIZE (used)</th>
<th>SIZE (limit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1024</td>
<td>0</td>
</tr>
</tbody>
</table>

VMS

<table>
<thead>
<tr>
<th>MEMORY (used)</th>
<th>MEMORY (limit)</th>
<th>CPU (used)</th>
<th>CPU (limit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1024</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

NETWORK ID

<table>
<thead>
<tr>
<th>LEASES (used)</th>
<th>LEASES (limit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

IMAGE ID

<table>
<thead>
<tr>
<th>RVMS (used)</th>
<th>RVMS (limit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

And for the group:

```
$ onegroup show gA
GROUP 100 INFORMATION
ID : 100
NAME : gA

USERS
ID
2
3

RESOURCE USAGE & QUOTAS

<table>
<thead>
<tr>
<th>DATASTORE ID</th>
<th>IMAGES (used)</th>
<th>IMAGES (limit)</th>
<th>SIZE (used)</th>
<th>SIZE (limit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2048</td>
<td>0</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>VMS</th>
<th>MEMORY (used)</th>
<th>MEMORY (limit)</th>
<th>CPU (used)</th>
<th>CPU (limit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2048</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NETWORK ID</th>
<th>LEASES (used)</th>
<th>LEASES (limit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IMAGE ID</th>
<th>RVMS (used)</th>
<th>RVMS (limit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

This information is also available through Sunstone as part of the user/group information.
7.1 Authentication Overview

OpenNebula comes by default with an internal user/password authentication system, see the *Users & Groups Subsystem guide* for more information. You can enable an external Authentication driver.

7.1.1 Authentication

In the figure to the right of this text you can see three authentication configurations you can customize in OpenNebula.

a) CLI/API Authentication

You can choose from the following authentication drivers to access OpenNebula from the command line:

- *Built-in User/Password and token authentication*
- *SSH Authentication*
- *X509 Authentication*
- *LDAP Authentication*

b) Sunstone Authentication

By default any authentication driver configured to work with OpenNebula can be used out-of-the-box with Sunstone. Additionally you can add SSL security to Sunstone as described in the *Sunstone documentation*
c) Servers Authentication

This method is designed to delegate the authentication process to high level tools interacting with OpenNebula. You’ll be interested in this method if you are developing your own servers.

By default, OpenNebula ships with two servers: Sunstone and EC2. When a user interacts with one of them, the server authenticates the request and then forwards the requested operation to the OpenNebula daemon.

The forwarded requests are encrypted by default using a Symmetric Key mechanism. The following guide shows how to strengthen the security of these requests using x509 certificates. This is specially relevant if you are running your server in a machine other than the frontend.

- Cloud Servers Authentication

7.2 SSH Auth

This guide will show you how to enable and use the SSH authentication for the OpenNebula CLI. Using this authentication method, users login to OpenNebula with a token encrypted with their private ssh keys.

7.2.1 Requirements

You don’t need to install any additional software.

7.2.2 Considerations & Limitations

With the current release, this authentication method is only valid to interact with OpenNebula using the CLI.

7.2.3 Configuration

OpenNebula Configuration

The Auth MAD and ssh authentication is enabled by default. In case it does not work make sure that the authentication method is in the list of enabled methods.

```python
AUTH_MAD = [
    executable = "one_auth_mad",
    authn = "ssh,x509,ldap,server_cipher,server_x509"
]
```

There is an external plain user/password authentication driver, and existing accounts will keep working as usual.

7.2.4 Usage

Create New Users

This authentication method uses standard ssh rsa keypairs for authentication. Users can create these files if they don’t exist using this command:

```
newuser@frontend $ ssh-keygen -t rsa
```
OpenNebula commands look for the files generated at the standard location ($HOME/.ssh/id_rsa) so it is a good idea not to change the default path. It is also a good idea to protect the private key with a password.

The users requesting a new account have to generate a public key and send it to the administrator. The way to extract it is the following:

newuser@frontend $ oneuser key
Enter PEM pass phrase: MIIBCAKCAQEApUO+JISjSf02rFVtDrlyar/34EoUoVETx0n+RqwWNav+5wi+gHiPp3e03AfEkXzjDYi8F
voS4a445sf10U0qQddfyPECn590eX82u4DH3gp1VUuDeeE8WJWyAzdK5hg6F+RdyPlpT26mnyunZB8Xd
bl18seo1AQiO6t1VfA8FrtwLQmdEETfttS9ukyGxw5vdTpsle/fcam+r9AXBR06zjc77x+DbRFbXcglI
1XiIpYrjCFL0fdN53L0aU7kTE9VNExRlxK8sPv1Nfx+FQWpX/HtH81C5WREs2GmXPA0/IkrSpMVg5t4aS
jie9JAfOMesjFIwggT8Jh6cNXuYsQ/5wIwIBIw==

The string written to the console must be sent to the administrator, so the can create the new user in a similar way as the default user/password authentication users.

The following command will create a new user with username ‘newuser’, assuming that the previous public key is saved in the text file /tmp/pub_key:

oneadmin@frontend $ oneuser create newuser --ssh --read-file /tmp/pub_key

Instead of using the -read-file option, the public key could be specified as the second parameter.

If the administrator has access to the user’s private ssh key, he can create new users with the following command:

oneadmin@frontend $ oneuser create newuser --ssh --key /home/newuser/.ssh/id_rsa

Update Existing Users to SSH

You can change the authentication method of an existing user to SSH with the following commands:

oneadmin@frontend $ oneuser chauth <id|name> ssh
oneadmin@frontend $ oneuser passwd <id|name> --ssh --read-file /tmp/pub_key

As with the create command, you can specify the public key as the second parameter, or use the user’s private key with the -key option.

User Login

Users must execute the ‘oneuser login’ command to generate a login token. The token will be stored in the $ONE_AUTH environment variable. The command requires the OpenNebula username, and the authentication method (ssh in this case).

newuser@frontend $ oneuser login newuser --ssh

The default ssh key is assumed to be in ~/.ssh/id_rsa, otherwise the path can be specified with the -key option.

The generated token has a default expiration time of 10 hour. You can change that with the -time option.

7.3 x509 Authentication

This guide will show you how to enable and use the x509 certificates authentication with OpenNebula. The x509 certificates can be used in two different ways in OpenNebula.
The first option that is explained in this guide enables us to use certificates with the CLI. In this case the user will generate a login token with his private key, OpenNebula will validate the certificate and decrypt the token to authenticate the user.

The second option enables us to use certificates with Sunstone and the Public Cloud servers included in OpenNebula. In this case the authentication is leveraged to Apache or any other SSL capable http proxy that has to be configured by the administrator. If this certificate is validated the server will encrypt those credentials using a server certificate and will send the token to OpenNebula.

7.3.1 Requirements

If you want to use the x509 certificates with Sunstone or one of the Public Clouds, you must deploy a SSL capable http proxy on top of them in order to handle the certificate validation.

7.3.2 Considerations & Limitations

The X509 driver uses the certificate DN as user passwords. The x509 driver will remove any space in the certificate DN. This may cause problems in the unlikely situation that you are using a CA signing certificate subjects that only differ in spaces.

7.3.3 Configuration

The following table summarizes the available options for the x509 driver (/etc/one/auth/x509_auth.conf):

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>:ca_dir</td>
<td>Path to the trusted CA directory. It should contain the trusted CA's for the server, each CA certificate should be name CA_hash.0</td>
</tr>
<tr>
<td>:check_crl</td>
<td>By default, if you place CRL files in the CA directory in the form CA_hash.r0, OpenNebula will check them. You can enforce CRL checking by defining :check_crl, i.e. authentication will fail if no CRL file is found. You can always disable this feature by moving or renaming .r0 files</td>
</tr>
</tbody>
</table>

Follow these steps to change oneadmin’s authentication method to x509:

Warning: You should have another account in the oneadmin group, so you can revert these steps if the process fails.

- Change the oneadmin password to the oneadmin certificate DN.

oneadmin@frontend $ oneuser chauth 0 x509 --x509 --cert /tmp/newcert.pem

- Add trusted CA certificates to the certificates directory

$ openssl x509 -noout -hash -in cacert.pem

78d0bbd8

$ sudo cp cacert.pem /etc/one/auth/certificates/78d0bbd8.0

- Create a login for oneadmin using the –x509 option. This token has a default expiration time set to 1 hour, you can change this value using the option –time.

oneadmin@frontend $ oneuser login oneadmin --x509 --cert newcert.pem --key newkey.pem

Enter PEM pass phrase:

export ONE_AUTH=/home/oneadmin/.one/one_x509

Chapter 7. Authentication
• Set ONE_AUTH to the x509 login file

oneadmin@frontend $ export ONE_AUTH=/home/oneadmin/.one/one_x509

7.3.4 Usage

Add and Remove Trusted CA Certificates

You need to copy all trusted CA certificates to the certificates directory, renaming each of them as "<CA_hash>.0". The hash can be obtained with the openssl command:

```
$ openssl x509 -noout -hash -in cacert.pem
78d0bbd8
```

```
$ sudo cp cacert.pem /etc/one/auth/certificates/78d0bbd8.0
```

To stop trusting a CA, simply remove its certificate from the certificates directory.

This process can be done without restarting OpenNebula, the driver will look for the certificates each time an authentication request is made.

Create New Users

The users requesting a new account have to send their certificate, signed by a trusted CA, to the administrator. The following command will create a new user with username ‘newuser’, assuming that the user’s certificate is saved in the file /tmp/newcert.pem:

```
oneadmin@frontend $ oneuser create newuser --x509 --cert /tmp/newcert.pem
```

This command will create a new user whose password contains the subject DN of his certificate. Therefore if the subject DN is known by the administrator the user can be created as follows:

```
oneadmin@frontend $ oneuser create newuser --x509 "user_subject_DN"
```

Update Existing Users to x509 & Multiple DN

You can change the authentication method of an existing user to x509 with the following command:

• Using the user certificate:

```
oneadmin@frontend $ oneuser chauth <id|name> x509 --x509 --cert /tmp/newcert.pem
```

• Using the user certificate subject DN:

```
oneadmin@frontend $ oneuser chauth <id|name> x509 --x509 "user_subject_DN"
```

You can also map multiple certificates to the same OpenNebula account. Just add each certificate DN separated with ‘|’ to the password field.

```
oneadmin@frontend $ oneuser passwd <id|name> --x509 "/DC=es/O=one/CN=user|/DC=us/O=two/CN=user"
```
User Login

Users must execute the ‘oneuser login’ command to generate a login token. The token will be stored in the $ONE_AUTH environment variable. The command requires the OpenNebula username, and the authentication method (–x509 in this case).

```
newuser@frontend $ oneuser login newuser --x509 --cert newcert.pem --key newkey.pem
Enter PEM pass phrase:
```

The generated token has a default expiration time of 10 hours. You can change that with the –time option.

7.3.5 Tuning & Extending

The x509 authentication method is just one of the drivers enabled in AUTH_MAD. All drivers are located in /var/lib/one/remotes/auth.

OpenNebula is configured to use x509 authentication by default. You can customize the enabled drivers in the AUTH_MAD attribute of oned.conf. More than one authentication method can be defined:

```
AUTH_MAD = [
    executable = "one_auth_mad",
    authn = "ssh,x509,ldap,server_cipher,server_x509"
]
```

7.3.6 Enabling x509 auth in Sunstone

Update the /etc/one/sunstone-server.conf :auth parameter to use the x509 auth:

```
:auth: x509
```

7.4 LDAP Authentication

The LDAP Authentication addon permits users to have the same credentials as in LDAP, so effectively centralizing authentication. Enabling it will let any correctly authenticated LDAP user to use OpenNebula.

7.4.1 Prerequisites

**Warning:** This Addon requires the ‘net/ldap’ ruby library provided by the ‘net-ldap’ gem.

This Addon will not install any Ldap server or configure it in any way. It will not create, delete or modify any entry in the Ldap server it connects to. The only requirement is the ability to connect to an already running Ldap server and being able to perform a successful `ldapbind` operation and have a user able to perform searches of users, therefore no special attributes or values are required in the LDIF entry of the user authenticating.

7.4.2 Configuration

Configuration file for auth module is located at /etc/one/auth/ldap_auth.conf. This is the default configuration:

server 1:

# Ldap user able to query, if not set connects as anonymous. For
# Active Directory append the domain name. Example:
# Administrator@my.domain.com
#:user: 'admin'
#:password: 'password'

#:auth_method: :simple

#:host: localhost
#:port: 389

#:encryption: :simple_tls

#:base: 'dc=domain'

#:group: 'cn=cloud,ou=groups,dc=domain'

#:user_field: 'cn'

#:group_field: 'member'

#:user_group_field: 'dn'

:mapping_generate: true

:mapping_timeout: 300

:mapping_filename: server1.yaml

:mapping_key: GROUP_DN

:mapping_default: 1

# this example server wont be called as it is not in the :order list
server 2:

#:auth_method: :simple
#:host: localhost
#:port: 389
#:base: 'dc=domain'
#:group: 'cn=cloud,ou=groups,dc=domain'

7.4. LDAP Authentication 161
The structure is a hash where any key different to :order will contain the configuration of one ldap server we want to query. The special key :order holds an array with the order we want to query the configured servers. Any server not listed in :order won't be queried.

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>:user</td>
<td>Name of the user that can query ldap. Do not set it if you can perform queries anonymously</td>
</tr>
<tr>
<td>:password</td>
<td>Password for the user defined in :user. Do not set if anonymous access is enabled</td>
</tr>
<tr>
<td>:auth_method</td>
<td>Can be set to :simple_tls if ssl connection is needed</td>
</tr>
<tr>
<td>:encryption</td>
<td>Can be set to :simple_tls if ssl connection is needed</td>
</tr>
<tr>
<td>:host</td>
<td>Host name of the ldap server</td>
</tr>
<tr>
<td>:port</td>
<td>Port of the ldap server</td>
</tr>
<tr>
<td>:base</td>
<td>Base leaf where to perform user searches</td>
</tr>
<tr>
<td>:group</td>
<td>If set the users need to belong to this group</td>
</tr>
<tr>
<td>:user_field</td>
<td>Field in ldap that holds the user name</td>
</tr>
<tr>
<td>:mapping_generate</td>
<td>Generate automatically a mapping file. It can be disabled in case it needs to be done manually</td>
</tr>
<tr>
<td>:mapping_timeout</td>
<td>Number of seconds between automatic mapping file generation</td>
</tr>
<tr>
<td>:mapping_filename</td>
<td>Name of the mapping file. Should be different for each server</td>
</tr>
<tr>
<td>:mapping_key</td>
<td>Key in the group template used to generate the mapping file. It should hold the DN of the mapped group</td>
</tr>
<tr>
<td>:mapping_default</td>
<td>Default group used when no mapped group is found. Set to false in case you don’t want the user to be authorized if it does not belong to a mapped group</td>
</tr>
</tbody>
</table>

To enable ldap authentication the described parameters should be configured. OpenNebula must be also configured to enable external authentication. Add this line in /etc/one/oned.conf

DEFAULT_AUTH = "ldap"

### 7.4.3 User Management

Using LDAP authentication module the administrator doesn’t need to create users with oneuser command as this will be automatically done.

Users can store their credentials into $ONE_AUTH file (usually $HOME/.one/one_auth) in this fashion:

```
<user_dn>:ldap_password
```

where

- `<user_dn>` the DN of the user in the LDAP service
- `ldap_password` is the password of the user in the LDAP service

Alternatively a user can generate an authentication token using the oneuser login command, so there is no need to keep the ldap password in a plain file. Simply input the ldap_password when requested. More information on the management of login tokens and $ONE_AUTH file can be found in Managing Users Guide.
DN's With Special Characters

When the user dn or password contains blank spaces the LDAP driver will escape them so they can be used to create OpenNebula users. Therefore, users needs to set up their $ONE_AUTH file accordingly.

Users can easily create escaped $ONE_AUTH tokens with the command `oneuser encode <user> [<password>]`, as an example:

```bash
$ oneuser encode 'cn=First Name,dc=institution,dc=country' 'password'
```

cn=First%20Name,dc=institution,dc=country:pass%20word

The output of this command should be put in the $ONE_AUTH file.

7.4.4 Active Directory

LDAP Auth drivers are able to connect to Active Directory. You will need:

- Active Directory server with support for simple user/password authentication.
- User with read permissions in the Active Directory user’s tree.

You will need to change the following values in the configuration file (`/etc/one/auth/ldap_auth.conf`):

- `:user`: the Active Directory user with read permissions in the user’s tree plus the domain. For example for user **Administrator** at domain **win.opennebula.org** you specify it as **Administrator@win.opennebula.org**
- `:password`: password of this user
- `:host`: hostname or IP of the Domain Controller
- `:base`: base DN to search for users. You need to decompose the full domain name and use each part as DN component. Example, for **win.opennebula.org** you will get te base DN: DN=win,DN=opennebula,DN=org
- `:user_field`: set it to sAMAccountName

:group parameter is still not supported for Active Directory, leave it commented.

7.4.5 Group Mapping

You can make new users belong to an specific group upon creation. To do this a mapping is generated from the LDAP group to an existing OpenNebula group. This system uses a mapping file specified by `:mapping_file` parameter and resides in OpenNebula `var` directory. The mapping file can be generated automatically using data in the group template that tells which LDAP group maps to that specific group. For example we can add in the group template this line:

```plaintext
GROUP_DN="CN=technicians,CN=Groups,DC=example,DC=com"
```

And in the ldap configuration file we set the `:mapping_key` to GROUP_DN. This tells the driver to look for the group DN in that template parameter. This mapping expires the number of seconds specified by `:mapping_timeout`. This is done so the authentication is not continually querying OpenNebula.

You can also disable the automatic generation of this file and do the mapping manually. The mapping file is in YAML format and contains a hash where the key is the LDAP’s group DN and the value is the ID of the OpenNebula group. For example:

```yaml
CN=technicians,CN=Groups,DC=example,DC=com: '100'
CN=Domain Admins,CN=Users,DC=example,DC=com: '101'
```
When several servers are configured you should have different :mapping_key and :mapping_file values for each one so they don’t collide. For example:

```
internal:
  :mapping_file: internal.yaml
  :mapping_key: INTERNAL_GROUP_DN

external:
  :mapping_file: external.yaml
  :mapping_key: EXTERNAL_GROUP_DN
```

And in the OpenNebula group template you can define two mappings, one for each server:

```
INTERNAL_GROUP_DN="CN=technicians,CN=Groups,DC=internal,DC=com"
EXTERNAL_GROUP_DN="CN=staff,DC=other-company,DC=com"
```

### 7.4.6 Enabling LDAP auth in Sunstone

Update the `/etc/one/sunstone-server.conf` :auth parameter to use the opennebula:

```
:auth: opennebula
```

Using this method the credentials provided in the login screen will be sent to the OpenNebula core and the authentication will be delegated to the OpenNebula auth system, using the specified driver for that user. Therefore any OpenNebula auth driver can be used through this method to authenticate the user (i.e: LDAP).

To automatically encode credentials as explained in *DN’s with special characters* section also add this parameter to sunstone configuration:

```
:encode_user_password: true
```
8.1 OpenNebula Sunstone: The Cloud Operations Center

OpenNebula Sunstone is the OpenNebula Cloud Operations Center, a Graphical User Interface (GUI) intended for regular users and administrators that simplifies the typical management operations in private and hybrid cloud infrastructures. OpenNebula Sunstone allows to easily manage all OpenNebula resources and perform typical operations on them.

OpenNebula Sunstone can be adapted to different user roles. For example, it will only show the resources the users have access to. Its behaviour can be customized and extended via views.

8.1.1 Requirements

You must have an OpenNebula site properly configured and running to use OpenNebula Sunstone, be sure to check the OpenNebula Installation and Configuration Guides to set up your private cloud first. This guide also assumes that you are familiar with the configuration and use of OpenNebula.
OpenNebula Sunstone was installed during the OpenNebula installation. If you followed the installation guide then you already have all ruby gem requirements. Otherwise, run the `install_gem` script as root:

```bash
# /usr/share/one/install_gems sunstone
```

The Sunstone Operation Center offers the possibility of starting a VNC/SPICE session to a Virtual Machine. This is done by using a VNC/SPICE websocket-based client (noVNC) on the client side and a VNC proxy translating and redirecting the connections on the server-side.

**Warning:** The SPICE Web client is a prototype and is limited in function. More information of this component can be found in the following link.

Requirements:

- Websockets-enabled browser (optional): Firefox and Chrome support websockets. In some versions of Firefox manual activation is required. If websockets are not enabled, flash emulation will be used.
- Start the novnc-server included with OpenNebula, both VNC and SPICE use this server as they have no built in support for the WebSocket protocol.
- Installing the `python-numpy` package is recommended for a better vnc performance.

### 8.1.2 Considerations & Limitations

OpenNebula Sunstone supports Internet Explorer (>= 9), Firefox (> 3.5) and Chrome browsers. Other browsers are not supported and may not work well.

The upload option for files and images is limited to Firefox 4+ and Chrome 11+.

### 8.1.3 Configuration

**Cannot connect to OneFlow server**

The last two tabs, OneFlow Services and Templates, will show the following message:

```plaintext
Cannot connect to OneFlow server
```

You need to start the OneFlow component following this guide, or disable these two menu entries in the `admin.yaml` and `user.yaml sunstone views`.

**sunstone-server.conf**

Sunstone configuration file can be found at `/etc/one/sunstone-server.conf`. It uses YAML syntax to define some options:

Available options are:
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>:tmpdir</td>
<td>Uploaded images will be temporally stored in this folder before being copied to OpenNebula.</td>
</tr>
<tr>
<td>:one_xmlrpc</td>
<td>OpenNebula daemon host and port.</td>
</tr>
<tr>
<td>:host</td>
<td>IP address on which the server will listen. 0.0.0.0 for everyone. 127.0.0.1 by default.</td>
</tr>
<tr>
<td>:port</td>
<td>Port on which the server will listen. 9869 by default.</td>
</tr>
<tr>
<td>:sessions</td>
<td>Method of keeping user sessions. It can be memory or memcache. For server that spawn more than one process (like Passenger or Unicorn) memcache should be used</td>
</tr>
<tr>
<td>:mem_cache_host</td>
<td>Host where memcached server resides</td>
</tr>
<tr>
<td>:mem_cache_port</td>
<td>Port of memcached server</td>
</tr>
<tr>
<td>:mem_cache_namespace</td>
<td>memcache namespace where to store sessions. Useful when memcached server is used by more services</td>
</tr>
<tr>
<td>:debug_level</td>
<td>Log debug level: 0 = ERROR, 1 = WARNING, 2 = INFO, 3 = DEBUG</td>
</tr>
<tr>
<td>:env</td>
<td>Execution environment for Sunstone. dev, Instead of pulling the minified js all the files will be pulled (app/main.js). Check the Building from Source guide in the docs, for details on how to run Sunstone in development. prod, the minified js will be used (dist/main.js)</td>
</tr>
<tr>
<td>:auth</td>
<td>Authentication driver for incoming requests. Possible values are sunstone, opennebula, remote and x509. Check authentication methods for more info</td>
</tr>
<tr>
<td>:core_auth</td>
<td>Authentication driver to communicate with OpenNebula core. Possible values are x509 or cipher. Check cloud_auth for more information</td>
</tr>
<tr>
<td>:lang</td>
<td>Default language for the Sunstone interface. This is the default language that will be used if user has not defined a variable LANG with a different valid value its user template</td>
</tr>
<tr>
<td>:vnc_proxy_port</td>
<td>Base port for the VNC proxy. The proxy will run on this port as long as Sunstone server does. 29876 by default.</td>
</tr>
<tr>
<td>:vnc_proxy_support_wss</td>
<td>yes, no, only. If enabled, the proxy will be set up with a certificate and a key to use secure websockets. If set to only the proxy will only accept encrypted connections, otherwise it will accept both encrypted or unencrypted ones.</td>
</tr>
<tr>
<td>:vnc_proxy_cert</td>
<td>Full path to certificate file for wss connections.</td>
</tr>
<tr>
<td>:vnc_proxy_key</td>
<td>Full path to key file. Not necessary if key is included in certificate.</td>
</tr>
<tr>
<td>:vnc_proxy_ipv6</td>
<td>Enable ipv6 for novnc. (true or false)</td>
</tr>
<tr>
<td>:vnc_request_password</td>
<td>Request VNC password for external windows, by default it will not be requested (true or false)</td>
</tr>
<tr>
<td>:table_order</td>
<td>Default table order, resources get ordered by ID in asc or desc order.</td>
</tr>
<tr>
<td>:marketplace_username</td>
<td>Username credential to connect to the Marketplace.</td>
</tr>
<tr>
<td>:marketplace_password</td>
<td>Password to connect to the Marketplace.</td>
</tr>
<tr>
<td>:marketplace_url</td>
<td>Endpoint to connect to the Marketplace. If commented, a 503 service unavailable error will be returned to clients.</td>
</tr>
<tr>
<td>:one_flow_server</td>
<td>Endpoint to connect to the OneFlow server.</td>
</tr>
<tr>
<td>:routes</td>
<td>List of files containing custom routes to be loaded. Check server plugins for more info.</td>
</tr>
<tr>
<td>:instance_types</td>
<td>Default instance types for Cloud View Instance Types for Cloud View</td>
</tr>
</tbody>
</table>

**Warning:** In order to access Sunstone from other place than localhost you need to set the server’s public IP in the :host option. Otherwise it will not be reachable from the outside.

### Starting Sunstone

To start Sunstone just issue the following command as oneadmin

8.1. OpenNebula Sunstone: The Cloud Operations Center 167
You can find the Sunstone server log file in `/var/log/one/sunstone.log`. Errors are logged in `/var/log/one/sunstone.error`.

To stop the Sunstone service:

```bash
$ sunstone-server stop
```

## VNC Troubleshooting

There can be multiple reasons that may prevent noVNC from correctly connecting to the machines. Here’s a checklist of common problems:

- noVNC requires Python >= 2.5 for the websockets proxy to work. You may also need additional modules as python2<version>-numpy.
- You can retrieve useful information from `/var/log/one/novnc.log`.
- You must have a GRAPHICS section in the VM template enabling VNC, as stated in the documentation. Make sure the attribute IP is set correctly (0.0.0.0 to allow connections from everywhere), otherwise, no connections will be allowed from the outside.
- Your browser must support websockets, and have them enabled. This is the default in latest Chrome and Firefox, but former versions of Firefox (i.e. 3.5) required manual activation. Otherwise Flash emulation will be used.
- Make sure there are not firewalls blocking the connections. The proxy will redirect the websocket data from the VNC proxy port to the VNC port stated in the template of the VM. The value of the proxy port is defined in `sunstone-server.conf`.
- Make sure that you can connect directly from Sunstone frontend to the VM using a normal VNC client tools such as `vncviewer`.
- When using secure websockets, make sure that your certificate and key (if not included in certificate), are correctly set in Sunstone configuration files. Note that your certificate must be valid and trusted for the wss connection to work. If you are working with a certificate that it is not accepted by the browser, you can manually add it to the browser trust-list visiting `https://sunstone.server.address:vnc_proxy_port`. The browser will warn that the certificate is not secure and prompt you to manually trust it.
- If your connection is very, very, very slow, there might be a token expiration issue. Please try the manual proxy launch as described below to check it.
- Doesn’t work yet? Try launching Sunstone, killing the websocketify proxy and relaunching the proxy manually in a console window with the command that is logged at the beginning of `/var/log/one/novnc.log`. You must generate a lock file containing the PID of the python process in `/var/lock/one/.novnc.lock`. Leave it running and click on the VNC icon on Sunstone for the same VM again. You should see some output from the proxy in the console and hopefully the cause of why the connection does not work.
- Please contact the user list only when you have gone through the suggestion above and provide full sunstone logs, shown errors and any relevant information of your infrastructure (if there are Firewalls etc)
- The message “SecurityError: The operation is insecure.” is usually related to a Same-Origin-Policy problem. If you have Sunstone TLS secured and try to connect to an insecure websocket for VNC, Firefox blocks that. For Firefox, you need to have both connections secured to not get this error. And don’t use a self-signed certificate for the server, this would raise the error again (you can setup your own little CA, that works, but don’t use a self-signed server certificate). The other option would be to go into the Firefox config (about:config) and set “network.websocket.allowInsecureFromHTTPS” to “true”.

---

168 Chapter 8. Sunstone GUI
Instance Types for Cloud View

These are the default instance types for the Cloud View, these types are presented in the cloud view to customize VM Templates and they can be customized to meet your requirements. Each type is defined by:

- name: the name of the type
- cpu: capacity allocated to the VM for scheduling purposes
- vcpu: number of cores
- memory: in MB for the VM
- description: to help the user pick one, it may include purpose or price.

```yaml
:instance_types:
  - :name: small-x1
    :cpu: 1
    :vcpu: 1
    :memory: 128
    :description: Very small instance for testing purposes
  - :name: small-x2
    :cpu: 2
    :vcpu: 2
    :memory: 512
    :description: Small instance for testing multi-core applications
  - :name: medium-x2
    :cpu: 2
    :vcpu: 2
    :memory: 1024
    :description: General purpose instance for low-load servers
  - :name: medium-x4
    :cpu: 4
    :vcpu: 4
    :memory: 2048
    :description: General purpose instance for medium-load servers
  - :name: large-x4
    :cpu: 4
    :vcpu: 4
    :memory: 4096
    :description: General purpose instance for servers
  - :name: large-x8
    :cpu: 8
    :vcpu: 8
    :memory: 8192
    :description: General purpose instance for high-load servers
```

8.1.4 Commercial Support Integration

We are aware that in production environments, access to professional, efficient support is a must, and this is why we have introduced an integrated tab in Sunstone to access OpenNebula Systems (the company behind OpenNebula, formerly C12G) professional support. In this way, support ticket management can be performed through Sunstone, avoiding disruption of work and enhancing productivity.
This tab and can be disabled in the admin, admin_vcenter and user yaml files inside the sunstone views configuration directory:

```yaml
enabled_tabs:
  - dashboard-tab
  - system-tab
  - users-tab
  - groups-tab
  - acls-tab
  - vresources-tab
  - vms-tab
  - templates-tab
  - images-tab
  - files-tab
  - infra-tab
  #- clusters-tab
  - hosts-tab
  - datastores-tab
  - vnets-tab
  - marketplace-tab
  - oneflow-dashboard
  - oneflow-services
  - oneflow-templates
  - zones-tab
  #- support-tab
```

### 8.1.5 Tuning & Extending

For more information on how to customize and extend you Sunstone deployment use the following links:

- *Sunstone Views*, different roles different views.
- *Security & Authentication Methods*, improve security with x509 authentication and SSL
• Advanced Deployments, improving scalability and isolating the server

8.2 Sunstone Views

Using the OpenNebula Sunstone Views you will be able to provide a simplified UI aimed at end-users of an OpenNebula cloud. The OpenNebula Sunstone Views are fully customizable, so you can easily enable or disable specific information tabs or action buttons. You can define multiple views for different user groups. Each view defines a set of UI components so each user just access and view the relevant parts of the cloud for her role.

The OpenNebula Sunstone Views can be grouped in two different layouts. On one hand, the classic Sunstone layout exposes a complete view of the cloud, allowing administrators and advanced users to have full control of any physical or virtual resource of the cloud. On the other hand, the newer cloud layout exposes a simplified version of the cloud where group administrators and cloud end-users will be able to manage any virtual resource of the cloud, without taking care of the physical resources management.

8.2.1 Default Views

OpenNebula provides three default advanced views, admin, admin_vcenter and user and three simplified cloud view groupadmin, cloud_vcenter and cloud that implements six common views. By default, the admin view is only available to the oneadmin group. New users will be included in the users group and will use the default cloud view.

<table>
<thead>
<tr>
<th>Advanced view layout</th>
<th>System</th>
<th>Infrastructure</th>
<th>Virtual Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Users</td>
<td>Groups</td>
<td>ACLs</td>
</tr>
<tr>
<td>Admin</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Admin vCenter</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>User</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloud view layout</th>
<th>System</th>
<th>Virtual Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Users</td>
<td>VMs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Saved Templates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Services</td>
</tr>
<tr>
<td>Group Admin</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Cloud vCenter</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Cloud</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

**Admin View**

This view provides full control of the cloud.
Admin vCenter View

View designed to present the valid operations against a vCenter infrastructure to a cloud administrator.

User View

In this view users will not be able to manage nor retrieve the hosts and clusters of the cloud. They will be able to see Datastores and Virtual Networks in order to use them when creating a new Image or Virtual Ma-
chine, but they will not be able to create new ones. For more information about this view, please check the `/etc/one/sunstone-views/user.yaml` file.

**Group Admin View**

This view provides control of all the resources belonging to a group, but with no access to resources outside that group, that is, restricted to the physical and virtual resources of the group. This view features the ability to create new users within the group as well as set and keep track of user quotas. For more information on how to configure this scenario see [this guide](#)
Cloud View

This is a simplified view mainly intended for user that just require a portal where they can provision new virtual machines easily from pre-defined Templates. For more information about this view, please check the /etc/one/sunstone-views/cloud.yaml file.

In this scenario the cloud administrator must prepare a set of templates and images and make them available to the cloud users. These Templates must be ready to be instantiated, i.e. they define all the mandatory attributes. Before using them, users can optionally customize the VM capacity, add new network interfaces and provide values required
by the template. Thereby, the user doesn’t have to know any details of the infrastructure such as networking, storage. For more information on how to configure this scenario see this guide.

8.2.2 Requirements

OpenNebula Sunstone Views does not require any additional service to run. You may want to review the Sunstone configuration to deploy advanced setups, to scale the access to the web interface or to use SSL security.

8.2.3 Configuring Access to the Views

By default, the admin view is only available to the oneadmin group. New users will be included in the users group and will use the default cloud view. The views assigned to a given group can be defined in the group creation form or updating an existing group to implement different OpenNebula models, for more information on the different OpenNebula models please check the Understanding OpenNebula guide.
Sunstone will calculate the views available to users using:

- From all the groups the user belongs to, the SUNSTONE_VIEWS (comma separated list of views) attributes is
  pulled. Those views combined would be presented to the user

- If no views available from users, the defaults would be fetched from sunstone-views.yaml. Here, views
  can be defined for:
  
  - Each user (users: section), list each user and the set of views available for her.
  
  - Each group (groups: section), list the set of views for the group.
  
  - The default view, if a user is not listed in the users: section, nor its group in the groups: section, the
    default views will be used.

- By default users in the oneadmin group have access to all views

- By default users in the users group can use coud_view

Regarding sunstone-views.yaml, the following example enables the user (user.yaml) and the cloud
(cloud.yaml) views for helen and the cloud (cloud.yaml) view for group cloud-users. If more than one view for a
given user the first one is the default.

```
...
users:
  helen:
    - cloud
    - user

groups:
  cloud-users:
    - cloud
default:
    - user
```
8.2.4 Usage

Sunstone users can configure several options from the configuration tab:

- **Language**: select the language that they want to use for the UI.
- **Use secure websockets for VNC**: Try to connect using secure websockets when starting VNC sessions.
- **Views**: change between the different available views for the given user/group
- **Display Name**: If the user wishes to customize the username that is shown in Sunstone it is possible to so by adding a special parameter named `SUNSTONE_DISPLAY_NAME` with the desired value. It is worth noting that Cloud Administrators may want to automate this with a hook on user create in order to fetch the user name from outside OpenNebula.

These options are saved in the user template, as well as other hidden settings like for instance the attribute that lets Sunstone remember the number of items displayed in the datatables per user. If not defined, defaults from `sunstone-server.conf` are taken.

### Changing your View

If more than one view are available for this user, she can easily change between them in the settings window, along with other settings (e.g. language). See the *Configuring Access to the Views* section to learn how views are calculated per user.

### Internationalization and Languages

Sunstone support multiple languages. If you want to contribute a new language, make corrections or complete a translation, you can visit our:

- Transifex project page

Translating through Transifex is easy and quick. All translations should be submitted via Transifex.
Users can update or contribute translations anytime. Prior to every release, normally after the beta release, a call for translations will be made in the user list. Then the source strings will be updated in Transifex so all the translations can be updated to the latest OpenNebula version. Translation with an acceptable level of completeness will be added to the final OpenNebula release.

### 8.2.5 Advanced Configuration

There are three basic areas that can be tuned to adapt the default behavior to your provisioning needs:

- Define views, the set of UI components that will be enabled.
- Define the users and groups that may access to each view.
- Brand your OpenNebula Sunstone portal.

#### Defining a New OpenNebula Sunstone View or Customizing an Existing one

View definitions are placed in the `/etc/one/sunstone-views` directory. Each view is defined by a configuration file, in the form:

```
<view_name>.yaml
```

The name of the view is the the filename without the yaml extension. The default views are defined by the user.yaml and admin.yaml files, as shown below:

```
/etc/
  ...
  |-- sunstone-views/
  |   |-- admin.yaml  <--- the admin view
  |   `-- user.yaml
  `-- sunstone-views.yaml
  ...
```

The content of a view file specifies the tabs available in the view (note: tab is on of the main sections of the UI, those in the left-side menu). Each tab can be enabled or disabled by updating the `enabled_tabs` attribute. For example to disable the Clusters tab, comment the `clusters-tab` entry:

```
enabled_tabs:
  - dashboard-tab
  - system-tab
  - users-tab
  - groups-tab
  - acls-tab
  - vresources-tab
  - vms-tab
  - templates-tab
  - images-tab
  - files-tab
  - infra-tab
  # - clusters-tab
  - hosts-tab
  - datastores-tab
  - vnets-tab
  - marketplace-tab
  - oneflow-dashboard
  - oneflow-services
  - oneflow-templates
```

Each tab, can be tuned by selecting:

- The bottom tabs available (panel_tabs: attribute) in the tab, these are the tabs activated when an object is selected (e.g. the information, or capacity tabs in the Virtual Machines tab).
- The columns shown in the main information table (table_columns: attribute).
- The action buttons available to the view (actions: attribute).

The attributes in each of the above sections should be self-explanatory. As an example, the following section, defines a simplified datastore tab, without the info panel_tab and no action buttons:

```yaml
datastores-tab:
  panel_tabs:
    datastore_info_tab: false
    datastore_image_tab: true
  table_columns:
    - 0  # Checkbox
    - 1  # ID
    - 2  # Owner
    - 3  # Group
    - 4  # Name
    - 5  # Cluster
    #- 6 # Basepath
    #- 7 # TM
    #- 8 # DS
    #- 9 # Type
  actions:
    Datastore.refresh: true
    Datastore.create_dialog: false
    Datastore.addtocluster: false
    Datastore.chown: false
    Datastore.chgrp: false
    Datastore.chmod: false
    Datastore.delete: false
```

The table columns defined in the view.yaml file will apply not only to the main tab, but also to other places where the resources are used. For example, if the admin.yaml file defines only the Name and Running VMs columns for the host table:

```yaml
hosts-tab:
  table_columns:
    #- 0  # Checkbox
    #- 1  # ID
    - 2  # Name
    #- 3 # Cluster
    - 4  # RVMs
    #- 5 # Real CPU
    #- 6 # Allocated CPU
    #- 7 # Real MEM
    #- 8 # Allocated MEM
    #- 9 # Status
    #- 10 # IM MAD
    #- 11 # VM MAD
    #- 12 # Last monitored on
```

These will be the only visible columns in the main host list:
And also in the dialogs where a host needs to be selected, like the VM deploy action:

The cloud layout can also be customized by changing the following section of the yaml files:

```yaml
provision-tab:
  panel_tabs:
    users: false
    flows: true
    templates: true
  actions:
```

---

180 Chapter 8. Sunstone GUI
In this section you can customize the options available when instantiating a new template, the dashboard setup or the resources available for cloud users.

Note: The easiest way to create a custom view is to copy the admin.yaml file to the new view then harden it as needed.

### A Different Endpoint for Each View

OpenNebula Sunstone views can be adapted to deploy a different endpoint for each kind of user. For example if you want an endpoint for the admins and a different one for the cloud users. You will just have to deploy a new sunstone server and set a default view for each sunstone instance:

```bash
# Admin sunstone
cat /etc/one/sunstone-server.conf
...  :host: admin.sunstone.com
...
cat /etc/one/sunstone-views.yaml
...  users:
     groups:
     default:
        - admin

# Users sunstone
cat /etc/one/sunstone-server.conf
...  :host: user.sunstone.com
...
cat /etc/one/sunstone-views.yaml
...  users:
     groups:
     default:
        - user
```

### Branding the Sunstone Portal

You can easily add you logos to the login and main screens by updating the logo: attribute as follows:

- The login screen is defined in the /etc/one/sunstone-views.yaml.
• The logo of the main UI screen is defined for each view in the view file.

8.3 Self-service Cloud View

This is a simplified view intended for cloud consumers that just require a portal where they can provision new virtual machines easily. To create new VMs and Services, they just have to select one of the available templates prepared by the administrators.

8.3.1 Using the Cloud

Create VM

In this scenario the cloud administrator must prepare a set of templates and images and make them available to the cloud users. These Templates must be ready to be instantiated, i.e. they define all the mandatory attributes. Before using them, users can optionally customize the VM capacity, add new network interfaces and provide values required by the template. Check How to Prepare the Virtual Machine Templates for more information.
Create Virtual Machine

Virtual Machine Name

Select a Template

<table>
<thead>
<tr>
<th>System</th>
<th>VOC</th>
<th>Saved</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 6.6</td>
<td>Ubuntu 14.04</td>
<td>Fedora 20</td>
</tr>
<tr>
<td>CentOS</td>
<td>Ubuntu</td>
<td>Fedora Desktop Edition</td>
</tr>
<tr>
<td>CentOS Server 6.6</td>
<td>Ubuntu 14.04.1 Trusty Tahr</td>
<td>Fedora 20 Desktop Edition</td>
</tr>
</tbody>
</table>

Create

Any user of the Cloud View can save the changes made to a VM back to a new Template, and use this Template to instantiate new VMs later. For example a regular user can instantiate a clean VM prepared by the cloud administrator, install software needed by his application and save it in a new Template to instantiate new VMs. A Saved Template created by a regular user is only available for that user and is listed under the “Saved” tab.

The Group admin can also share his own Saved Templates with the rest of the group. These shared templates will be listed under the “Group” tab when trying to create a new VM.

Access to the VM, SSH Keys

Any user can provide his own ssh public key to be included in the VMs created through this view. Note that the template has to be configured to include it.
Add a public SSH key to your account!
You will be able to access your Virtual Machines without password

Manage VMs

The status of the VMs can be monitored from the VMs tab.
Information of the capacity, OS, IPs, creation time and monitoring graphs for a specific VM are available in the detailed view of the VM.
A user can perform the following actions from this view:

- Access the VNC console, note that the Template has to be configured for this
- Reboot the VM, the user can send the reboot signal (reboot) or reboot the machine (reboot hard)
- Power off the VM, the user can send the power off signal (poweroff) or power off the machine (poweroff hard)
- Delete the VM, all the information will be lost
- Save the VM into a new Template
- Power on the VM
Save a VM

Any user of the Cloud View can save the changes made to a VM back to a new Template, and use this Template to instantiate new VMs later.

The user has to power off the VM first and then the save operation will create a new Image and a Template referencing this Image.

A Saved Template created by a regular user is only available for that user and is listed under the “Saved” tab.
Saved Templates can be managed from the Templates tab. When deleting a saved template both the Image and the Template will be removed from OpenNebula.

For more details about the limitations of saved VM, continue to the Managing Virtual Machines guide.

Create Service

In this scenario the cloud administrator must prepare a set of Service templates and make them available to the cloud users. These Service templates must be ready to be instantiated, i.e. they define all the mandatory attributes and the templates that are referenced are available for the user. Before using them, users can optionally customize the Service cardinality, define the network interfaces and provide values required by the template. Check How to Prepare the Service Templates for more information.
Create Service

Select a Template

Manage Services

The status of the Services can be monitored from the Services tab
Information of the creation time, cardinality and status for each Role are available in the detailed view of the Service.

A user can perform the following actions from this view:

- Change the cardinality of each Role
- Retrieve the VMs of each Role
- Delete the Service
- Recover the Service from a fail status

**Usage, Accounting and Showback**

The user can check his current usage and quotas.
Also, the user can generate accounting reports for a given range of time.
User Settings

From the user settings tab, the user can change his password, language, ssh key and view
8.3.2 How to Prepare the Virtual Machine Templates

The dialog to launch new VMs from the Cloud View is a bit different from the standard “Template instantiate” action. To make a Template available for end users, take into account the following items:

**Capacity is Customizable**

You must set a default CPU and Memory for the Template, but users can change these values. The available capacity presets can be *customized*.
You can disable this option for the whole cloud modifying the `cloud.yaml` or `groupadmin.yaml` view files or per template in the template creation wizard:

```yaml
provision-tab:
  ...  
  create_vm:
    capacity_select: true
    network_select: true
```

### Set a Cost

Each VM Template can have a cost. This cost is set by CPU and MB, to allow users to change the capacity and see the cost updated accordingly. VMs with a cost will appear in the `showback reports`.
Enable Cloud View Features

There are a few features of the Cloud View that will work if you configure the Template to make use of them:

- Users will see the Template logo and description, something that is not so visible in the normal admin view.
- The Cloud View gives access to the VM’s VNC, but only if it is configured in the Template.
- End users can upload their public ssh key. This requires the VM guest to be contextualized, and the Template must have the ssh contextualization enabled.

Further Contextualize the Instance with User Inputs

A Template can define USER INPUTS. These inputs will be presented to the Cloud View user when the Template is instantiated. The VM guest needs to be contextualized to make use of the values provided by the user.
Make the Images Non-Persistent

The Images used by the Cloud View Templates should not be persistent. A persistent Image can only be used by one VM simultaneously, and the next user will find the changes made by the previous user.

If the users need persistent storage, they can use the *Save a VM* functionality

Prepare the Network Interfaces

Users can select the VM network interfaces when launching new VMs. You can create templates without any NIC, or set the default ones. If the template contains any NIC, users will still be able to remove them and select new ones.
Because users will add network interfaces, you need to define a default NIC model in case the VM guest needs a specific one (e.g. virtio for KVM). This can be done with the NIC_DEFAULT attribute, or through the Template wizard. Alternatively, you could change the default value for all VMs in the driver configuration file (see the KVM one for example).
You can disable this option for the whole cloud modifying the `cloud.yaml` or `groupadmin.yaml` view files or per template in the template creation wizard.

```
provision-tab:
  ...
  create_vm:
    capacity_select: true
    network_select: true
```

**Change Permissions to Make It Available**

To make a Template available to other users, you have two options:

- Change the Template’s group, and give it GROUP USE permissions. This will make the Template only available to users in that group.

- Leave the Template in the oneadmin group, and give it OTHER USE permissions. This will make the Template available to every user in OpenNebula.
Please note that you will need to do the same for any Image and Virtual Network referenced by the Template, otherwise the VM creation will fail with an error message similar to this one:

```
```

You can read more about OpenNebula permissions in the *Managing Permissions* and *Managing ACL Rules* guides.

### 8.3.3 How to Prepare the Service Templates

When you prepare a OneFlow Service Template to be used by the Cloud View users, take into account the following:

- You can define dynamic networks in the Service Template, to allow users to choose the virtual networks for the new Service instance.
- If any of the Virtual Machine Templates used by the Roles has User Inputs defined (see the section above), the user will be also asked to fill them when the Service Template is instantiated.
- Users will also have the option to change the Role cardinality before the Service is created.
Network

Private network for the service traffic

INTERFACE devs-private

Network with access to public IPs

Select a Network for this interface

Search

devs-private

Private network for the devs group

public

Network with connectivity to the internet
To make a Service Template available to other users, you have two options:

- Change the Template’s group, and give it GROUP USE permissions. This will make the Service Template only available to users in that group.

- Leave the Template in the oneadmin group, and give it OTHER USE permissions. This will make the Service Template available to every user in OpenNebula.

Please note that you will need to do the same for any VM Template used by the Roles, and any Image and Virtual Network referenced by those VM Templates, otherwise the Service deployment will fail.

### 8.3.4 Resource Sharing

When a new group is created the cloud administrator can define if the users of this view will be allowed to view the VMs and Services of other users in the same group. If this option is checked a new ACL rule will be created to give users in this group acces to the VMS and Services in the same group. Users will not able to manage these resources but they will be included in the list views of each resource.
8.3.5 How to Enable

The cloud view is enabled by default for all users and you can enable/disable it for a specific group in the group creation form.

Note: Any user can change the current view in the Sunstone settings. Administrators can use this view without any problem if they find it easier to manage their VMs.

8.3.6 Customizing the View

The actions available for a given VM can be customized and extended by modifying the `cloud.yaml` file. You can even insert VM panels from the admin view into this view, for example to use the disk snapshots or scheduled actions.

- Hiding the delete button

```
tabs:
  provision-tab:
    ...
    actions: &provisionactions
    ...
    VM.shutdown_hard: false
    VM.delete: false
```

- Using undeploy instead of power off

```
tabs:
  provision-tab:
    ...
    actions: &provisionactions
    ...
```
• Adding panels from the admin view, for example the disk snapshots tab

```yaml
tabs:
  provision-tab:
    panel_tabs:
      ...
      vm_snapshot_tab: true
      ...
      actions: &provisionactions
      ...
      VM.disk_snapshot_create: true
      VM.disk_snapshot_revert: true
      VM.disk_snapshot_delete: true
```

8.4 Group Admin View

The role of a Group Admin is to manage all the virtual resources of the Group, including the creation of new users. When one of these Group Admin users access Sunstone, they get a limited view of the cloud, but more complete than the one end users get with the Cloud View.

You can read more about OpenNebula’s approach to Groups and VDC’s from the perspective of different user roles in the Understanding OpenNebula guide.
8.4.1 Manage Users

The Group Admin can create new user accounts, that will belong to the same Group.
They can also see the current resource usage of all the Group users, and set quota limits for each one of them.
8.4.2 Manage Resources

The Group admin can manage the Services, VMs and Templates of other users in the Group. The resources of a specific user can be filtered in each of the list views for each resource type or can be listed in the detailed view of the user.
Filtering Resources by User

The Group admin view is an extension of the Cloud view, and includes all the functionality provided through the Cloud view. The Group admin can create new resources in the same way as a regular user does.
8.4.4 Prepare Resources for Other Users

Any user of the Cloud View can save the changes made to a VM back to a new Template, and use this Template to instantiate new VMs later. The Group admin can also share his own Saved Templates with the rest of the group. For example the Group admin can instantiate a clean VM prepared by the cloud administrator, install software needed by other users in his Group, save it in a new Template and make it available for the rest of the group.

The Group admin has to power off the VM first and then the save operation will create a new Image and a Template referencing this Image. Note that only the first disk will be saved, if the VM has more than one disk, they will not be saved.

The Group admin can share/unshare saved templates from the list of templates.

These shared templates will be listed under the “Group” tab when trying to create a new VM. A Saved Template created by a regular user is only available for that user and is listed under the “Saved” tab.
When deleting a saved template both the Image and the Template will be removed from OpenNebula.

### 8.4.5 Accounting & Showback

**Group Accounting & Showback**

The Group info tab provides information of the usage of the Group and also accounting and showback reports can be generated. These reports can be configured to report the usage per VM or per user for a specific range of time.
VDC Accounting

Start time: 2014/7/1
End time: Today
Group by: User

Get Accounting

VDC Quotas

<table>
<thead>
<tr>
<th>VMs</th>
<th></th>
<th>7 / 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td></td>
<td>8 / 400</td>
</tr>
<tr>
<td>Memory</td>
<td></td>
<td>6.5GB / 78.1GB</td>
</tr>
<tr>
<td>Volatile disks</td>
<td></td>
<td>0KB / -</td>
</tr>
<tr>
<td>Image</td>
<td>ID</td>
<td>Running VMs</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>7 / -</td>
</tr>
<tr>
<td>Network</td>
<td>ID</td>
<td>Leases</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>6 / -</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1 / -</td>
</tr>
<tr>
<td>Datastore</td>
<td>ID</td>
<td>Images</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

OpenNebula 4.8.0 by C1G Labs.
User Accounting & Showback

The detailed view of the user provides information of the usage of the user, from this view accounting reports can be also generated for this specific user.
8.4.6 How to Enable

By default the Group Admin account is not created for a new group. It can be enabled in the Admin tab of the Group creation form, this view will be automatically assigned to him.
8.5 User Security and Authentication

By default Sunstone works with the core authentication method (user and password) although you can configure any authentication mechanism supported by OpenNebula. In this guide you will learn how to enable other authentication methods and how to secure the Sunstone connections through SSL.

8.5.1 Authentication Methods

Authentication is two-folded:

- **Web client and Sunstone server.** Authentication is based on the credentials store in the OpenNebula database for the user. Depending on the type of these credentials the authentication method can be: basic, x509 and opennebula (supporting LDAP or other custom methods).

- **Sunstone server and OpenNebula core.** The requests of a user are forwarded to the core daemon, including the original user name. Each request is signed with the credentials of an special server user. This authentication mechanism is based either in symmetric key cryptography (default) or x509 certificates. Details on how to configure these methods can be found in the Cloud Authentication guide.

The following sections details the client-to-Sunstone server authentication methods.

### Basic Auth

In the basic mode, username and password are matched to those in OpenNebula’s database in order to authorize the user at the time of login. Rack cookie-based sessions are then used to authenticate and authorize the requests.

To enable this login method, set the `:auth:` option of `/etc/one/sunstone-server.conf` to `sunstone`.

```bash
:auth: sunstone
```

### OpenNebula Auth

Using this method the credentials included in the header will be sent to the OpenNebula core and the authentication will be delegated to the OpenNebula auth system, using the specified driver for that user. Therefore any OpenNebula auth driver can be used through this method to authenticate the user (i.e: LDAP). The sunstone configuration is:

```bash
:auth: opennebula
```

### x509 Auth

This method performs the login to OpenNebula based on a x509 certificate DN (Distinguished Name). The DN is extracted from the certificate and matched to the password value in the user database.

The user password has to be changed running one of the following commands:

```bash
oneuser chauth new_user x509 "\"/C=ES/O=ONE/OU=DEV/CN=clouduser\"
```

or the same command using a certificate file:

```bash
oneuser chauth new_user --x509 --cert /tmp/my_cert.pem
```

New users with this authentication method should be created as follows:
oneuser create new_user "/C=ES/O=ONE/OU=DEV/CN=clouduser" --driver x509

or using a certificate file:

oneuser create new_user --x509 --cert /tmp/my_cert.pem

To enable this login method, set the :auth: option of /etc/one/sunstone-server.conf to x509:

:auth: x509

The login screen will not display the username and password fields anymore, as all information is fetched from the user certificate:

![Login screen without username and password fields](image)

Note that OpenNebula will not verify that the user is holding a valid certificate at the time of login: this is expected to be done by the external container of the Sunstone server (normally Apache), whose job is to tell the user’s browser that the site requires a user certificate and to check that the certificate is consistently signed by the chosen Certificate Authority (CA).

**Warning:** Sunstone x509 auth method only handles the authentication of the user at the time of login. Authentication of the user certificate is a complementary setup, which can rely on Apache.

**remote Auth**

This method is similar to x509 auth. It performs the login to OpenNebula based on a Kerberos REMOTE_USER. The USER@DOMAIN is extracted from REMOTE_USER variable and matched to the password value in the user database. To use Kerberos authentication users needs to be configured with the public driver. Note that this will prevent users to authenticate through the XML-RPC interface, only Sunstone access will be granted to these users.
To update existing users to use the Kerberos authentication change the driver to public and update the password as follows:

```bash
oneuser chauth new_user public "new_user@DOMAIN"
```

New users with this authentication method should be created as follows:

```bash
oneuser create new_user "new_user@DOMAIN" --driver public
```

To enable this login method, set the `:auth:` option of `/etc/one/sunstone-server.conf` to `remote`:

```bash
:auth: remote
```

The login screen will not display the username and password fields anymore, as all information is fetched from Kerberos server or a remote authentication service.

Note that OpenNebula will not verify that the user is holding a valid Kerberos ticket at the time of login: this is expected to be done by the external container of the Sunstone server (normally Apache), whose job is to tell the user’s browser that the site requires a valid ticket to login.

**Warning:** Sunstone remote auth method only handles the authentication of the user at the time of login. Authentication of the remote ticket is a complementary setup, which can rely on Apache.

### 8.5.2 Configuring a SSL Proxy

OpenNebula Sunstone runs natively just on normal HTTP connections. If the extra security provided by SSL is needed, a proxy can be set up to handle the SSL connection that forwards the petition to the Sunstone server and takes back the answer to the client.

This set up needs:

- A server certificate for the SSL connections
- An HTTP proxy that understands SSL
- OpenNebula Sunstone configuration to accept petitions from the proxy

If you want to try out the SSL setup easily, you can find in the following lines an example to set a self-signed certificate to be used by a web server configured to act as an HTTP proxy to a correctly configured OpenNebula Sunstone.

Let’s assume the server where the proxy is going to be started is called `cloudserver.org`. Therefore, the steps are:

**Step 1: Server Certificate (Snakeoil)**

We are going to generate a snakeoil certificate. If using an Ubuntu system follow the next steps (otherwise your mileage may vary, but not a lot):

- Install the `ssl-cert` package

  ```bash
  $ sudo apt-get install ssl-cert
  ```

- Generate the certificate

  ```bash
  $ sudo /usr/sbin/make-ssl-cert generate-default-snakeoil
  ```

- As we are using lighttpd, we need to append the private key with the certificate to obtain a server certificate valid to lighttpd

---

8.5. User Security and Authentication 217
Step 2: SSL HTTP Proxy

lighttpd

You will need to edit the `/etc/lighttpd/lighttpd.conf` configuration file and

- Add the following modules (if not present already)
  - mod_access
  - mod_alias
  - mod_proxy
  - mod_accesslog
  - mod_compress

- Change the server port to 443 if you are going to run lighttpd as root, or any number above 1024 otherwise:

```
server.port = 8443
```

- Add the proxy module section:

```
#### proxy module
## read proxy.txt for more info
proxy.server = ( "" =>
  ("" =>
    {
      "host" => "127.0.0.1",
      "port" => 9869
    }
  )
)
#### SSL engine
ssl.engine = "enable"
ssl.pemfile = "/etc/lighttpd/server.pem"
```

The host must be the server hostname of the computer running the Sunstone server, and the port the one that the Sunstone Server is running on.

nginx

You will need to configure a new virtual host in nginx. Depending on the operating system and the method of installation, nginx loads virtual host configurations from either `/etc/nginx/conf.d` or `/etc/nginx/sites-enabled`.

- A sample `cloudserver.org` virtual host is presented next:

```
#### OpenNebula Sunstone upstream
upstream sunstone {
  server 127.0.0.1:9869;
}
```
### cloudserver.org HTTP virtual host

server {
    listen 80;
    server_name cloudserver.org;

    ### Permanent redirect to HTTPS (optional)
    return 301 https://$server_name:8443;
}

### cloudserver.org HTTPS virtual host

server {
    listen 8443;
    server_name cloudserver.org;

    ### SSL Parameters
    ssl on;
    ssl_certificate /etc/ssl/certs/ssl-cert-snakeoil.pem;
    ssl_certificate_key /etc/ssl/private/ssl-cert-snakeoil.key;

    ### Proxy requests to upstream
    location / {
        proxy_pass http://sunstone;
    }
}

The IP address and port number used in `upstream` must be the ones of the server Sunstone is running on. On typical installations the nginx master process is run as user root so you don’t need to modify the HTTPS port.

**Step 3: Sunstone Configuration**

Start the Sunstone server using the default values, this way the server will be listening at localhost:9869.

Once the proxy server is started, OpenNebula Sunstone requests using HTTPS URIs can be directed to `https://cloudserver.org:8443`, that will then be unencrypted, passed to localhost, port 9869, satisfied (hopefully), encrypted again and then passed back to the client.

### 8.6 Cloud Servers Authentication

OpenNebula ships with two servers: **Sunstone** and EC2. When a user interacts with one of them, the server authenticates the request and then forwards the requested operation to the OpenNebula daemon.

The forwarded requests between the servers and the core daemon include the original user name, and are signed with the credentials of an special `server` user.

In this guide this request forwarding mechanism is explained, and how it is secured with a symmetric-key algorithm or x509 certificates.

#### 8.6.1 Server Users

The **Sunstone** and EC2 services communicate with the core using a `server` user. OpenNebula creates the `serveradmin` account at bootstrap, with the authentication driver `server_cipher` (symmetric key).

This `server` user uses a special authentication mechanism that allows the servers to perform an operation on behalf of other user.
You can strengthen the security of the requests from the servers to the core daemon changing the serveruser’s driver to server_x509. This is specially relevant if you are running your server in a machine other than the frontend.

Please note that you can have as many users with a server_* driver as you need. For example, you may want to have Sunstone configured with a user with server_x509 driver, and EC2 with server_cipher.

### 8.6.2 Symmetric Key

#### Enable

This mechanism is enabled by default, you will have a user named serveradmin with driver server_cipher.

To use it, you need a user with the driver server_cipher. Enable it in the relevant configuration file in /etc/one:

- **Sunstone**: /etc/one/sunstone-server.conf
- **EC2**: /etc/one/econe.conf

```
:core_auth: cipher
```

#### Configure

You must update the configuration files in /var/lib/one/.one if you change the serveradmin’s password, or create a different user with the server_cipher driver.

```
$ ls -1 /var/lib/one/.one
ec2_auth
sunstone_auth

$ cat /var/lib/one/.one/sunstone_auth
serveradmin:1612b78a4843647a4b541346f678f9e1b43bbcf9
```

**Warning:** serveradmin password is hashed in the database. You can use the -sha1 flag when issuing oneuser passwd command for this user.

**Warning:** When Sunstone is running in a different machine than oned you should use an SSL connection. This can be archived with an SSL proxy like stunnel or apache/nginx acting as proxy. After securing OpenNebula XMLRPC connection configure Sunstone to use https with the proxy port:

```
:one_xmlrpc: https://frontend:2634/RPC2
```

### 8.6.3 x509 Encryption

#### Enable

To enable it, change the authentication driver of the serveradmin user, or create a new user with the driver server_x509:

```
$ oneuser chauth serveradmin server_x509
$ oneuser passwd serveradmin --x509 --cert usercert.pem
```

The serveradmin account should look like:
You need to edit /etc/one/auth/server_x509_auth.conf and uncomment all the fields. The defaults should work:

```
# User to be used for x509 server authentication
:srv_user: serveradmin

# Path to the certificate used by the OpenNebula Services
# Certificates must be in PEM format
:one_cert: "'/etc/one/auth/cert.pem"
:one_key: "'/etc/one/auth/pk.pem"
```

Copy the certificate and the private key to the paths set in :one_cert: and :one_key:, or simply update the paths.

Then edit the relevant configuration file in /etc/one:

- **Sunstone**: /etc/one/sunstone-server.conf
- **EC2**: /etc/one/econe.conf

Configure

To trust the serveradmin certificate, /etc/one/auth/cert.pem if you used the default path, the CA’s certificate must be added to the ca_dir defined in /etc/one/auth/x509_auth.conf. See the x509 Authentication guide for more information.

```
$ openssl x509 -noout -hash -in cacert.pem
78d0bbd8

$ sudo cp cacert.pem /etc/one/auth/certificates/78d0bbd8.0
```

8.6.4 Tuning & Extending

Files

You can find the drivers in these paths: /var/lib/one/remotes/auth/server_cipher/authenticate /var/lib/one/remotes/auth/server_server/authenticate

Authentication Session String

OpenNebula users with the driver server_cipher or server_x509 use a special authentication session string (the first parameter of the XML-RPC calls). A regular authentication token is in the form:

```
username:secret
```

Whereas a user with a server_* driver must use this token format:
username:target_username:secret

The core daemon understands a request with this authentication session token as perform this operation on behalf of target\_user. The secret part of the token is signed with one of the two mechanisms explained below.
9.1 MySQL Backend

The MySQL backend is an alternative to the default Sqlite backend. Either of them can be used seamlessly to the upper layers and ecosystem tools. These high level components do not need to be modified or configured.

The two backends cannot coexist, and you will have to decide which one is going to be used while planning your OpenNebula installation.

**Note:** If you are planning to install OpenNebula with MySQL backend, please follow this guide *prior* to start OpenNebula the first time to avoid problems with oneadmin and serveradmin credentials.

9.1.1 Installation

First of all, you need a working MySQL server.

Of course, you can use any instance you have already deployed. OpenNebula will connect to other machines different from localhost.

You can also configure two different OpenNebula installations to use the same MySQL server. In this case, you have to make sure that they use different database names.

**Configuring MySQL**

In order to let OpenNebula use your existing MySQL database server, you need to add a new user and grant it privileges on one new database. This new database doesn’t need to exist, OpenNebula will create it the first time you run it.

Assuming you are going to use the default values, log in to your MySQL server and issue the following commands:

```
$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor. [...]

mysql> GRANT ALL PRIVILEGES ON opennebula.* TO 'oneadmin' IDENTIFIED BY 'oneadmin';
Query OK, 0 rows affected (0.00 sec)
```

**Note:** Remember to choose different values, at least for the password.

**GRANT ALL PRIVILEGES ON <db_name>.* TO <user> IDENTIFIED BY <passwd>**

Visit the MySQL documentation to learn how to manage accounts.
Now configure the transaction isolation level:

```sql
mysql> SET GLOBAL TRANSACTION ISOLATION LEVEL READ COMMITTED;
```

### Configuring OpenNebula

Before you run OpenNebula, you need to set in `oned.conf` the connection details, and the database you have granted privileges on.

```python
# Sample configuration for MySQL
DB = [ backend = "mysql",
      server = "localhost",
      port = 0,
      user = "oneadmin",
      passwd = "oneadmin",
      db_name = "opennebula" ]
```

Fields:

- **server**: url of the machine running the MySQL server
- **port**: port for the connection to the server. If set to 0, the default port is used.
- **user**: MySQL user-name
- **passwd**: MySQL password
- **db_name**: Name of the MySQL database OpenNebula will use

### 9.1.2 Using OpenNebula with MySQL

After this installation and configuration process you can use OpenNebula as usual.
10.1 ONED Configuration

The OpenNebula daemon oned manages the cluster nodes, virtual networks, virtual machines, users, groups and storage datastores. The configuration file for the daemon is called oned.conf and it is placed inside the /etc/one directory. In this reference document we describe all the format and options that can be specified in oned.conf.

10.1.1 Daemon Configuration Attributes

- **MANAGER_TIMER**: Time in seconds the core uses to evaluate periodical functions. MONITORING_INTERVAL cannot have a smaller value than MANAGER_TIMER.
- **MONITORING_INTERVAL**: Time in seconds between each monitorization.
- **MONITORING_THREADS**: Max. number of threads used to process monitor messages
- **HOST_PER_INTERVAL**: Number of hosts monitored in each interval.
- **HOST_MONITORING_EXPIRATION_TIME**: Time, in seconds, to expire monitoring information. Use 0 to disable HOST monitoring recording.
- **VM_INDIVIDUAL_MONITORING**: VM monitoring information is obtained along with the host information. For some custom monitor drivers you may need activate the individual VM monitoring process.
- **VM_PER_INTERVAL**: Number of VMs monitored in each interval.
- **VM_MONITORING_EXPIRATION_TIME**: Time, in seconds, to expire monitoring information. Use 0 to disable VM monitoring recording.
- **SCRIPTS_REMOTE_DIR**: Remote path to store the monitoring and VM management script.
- **PORT**: Port where oned will listen for xml-rpc calls.
- **LISTEN_ADDRESS**: Host IP to listen on for xmlrpc calls (default: all IPs).
- **DB**: Vector of configuration attributes for the database backend.
  - backend: Set to sqlite or mysql. Please visit the MySQL configuration guide for more information.
  - server (MySQL only): Host name or an IP address for the MySQL server.
  - user (MySQL only): MySQL user’s login ID.
  - passwd (MySQL only): MySQL user’s password.
  - db_name (MySQL only): MySQL database name.
- **VNC_BASE_PORT**: VNC ports for VMs can be automatically set to VNC_BASE_PORT + VMID. Refer to the VM template reference for further information.
- **VM_SUBMIT_ON_HOLD**: Forces VMs to be created on hold state instead of pending. Values: YES or NO.
- **LOG**: Configure the logging system
  - **SYSTEM**: Can be either file (default) or syslog.
  - **DEBUG_LEVEL**: Sets the level of verbosity of the log messages. Possible values are:

<table>
<thead>
<tr>
<th>DEBUG_LEVEL</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ERROR</td>
</tr>
<tr>
<td>1</td>
<td>WARNING</td>
</tr>
<tr>
<td>2</td>
<td>INFO</td>
</tr>
<tr>
<td>3</td>
<td>DEBUG</td>
</tr>
</tbody>
</table>

Example of this section:

```cpp
#*******************************************************************************
# Daemon configuration attributes
#*******************************************************************************

LOG = [  
    system = "file",
    debug_level = 3
]

#MANAGER_TIMER = 30

MONITORING_INTERVAL = 60
MONITORING_THREADS = 50

#HOST_PER_INTERVAL    = 15
#HOST_MONITORING_EXPIRATION_TIME = 43200

#VM_INDIVIDUAL_MONITORING    = "no"
#VM_PER_INTERVAL      = 5
#VM_MONITORING_EXPIRATION_TIME = 14400

SCRIPTS_REMOTE_DIR=/var/tmp/one

PORT = 2633
LISTEN_ADDRESS = "0.0.0.0"

DB = [ backend = "sqlite" ]

# Sample configuration for MySQL
# DB = [ backend = "mysql",
#        server = "localhost",
#        port = 0,
#        user = "oneadmin",
#        passwd = "oneadmin",
#        db_name = "opennebula" ]

VNC_BASE_PORT = 5900

#VM_SUBMIT_ON_HOLD = "NO"

10.1.2 Federation Configuration Attributes

Control the federation capabilities of oned. Operation in a federated setup requires a special DB configuration.
• **FEDERATION**: Federation attributes.
  - **MODE**: Operation mode of this oned.
    * **STANDALONE**: not federated. This is the default operational mode
    * **MASTER**: this oned is the master zone of the federation
    * **SLAVE**: this oned is a slave zone
  - **ZONE_ID**: The zone ID as returned by onezone command.
  - **MASTER_ONED**: The xml-rpc endpoint of the master oned, e.g. http://master.one.org:2633/RPC2

```
#******************************************************************************
# Federation configuration attributes
#******************************************************************************

FEDERATION = [
    MODE = "STANDALONE",
    ZONE_ID = 0,
    MASTER_ONED = ""
]
```

### 10.1.3 Default Showback Cost

The following attributes define the default cost for Virtual Machines that don’t have a CPU, MEMORY or DISK cost. This is used by the `oneshowback calculate method`.

```
#******************************************************************************
# Default showback cost
#******************************************************************************

DEFAULT_COST = [
    CPU_COST = 0,
    MEMORY_COST = 0,
    DISK_COST = 0
]
```

### 10.1.4 XML-RPC Server Configuration

- **MAX_CONN**: Maximum number of simultaneous TCP connections the server will maintain
- **MAX_CONN_BACKLOG**: Maximum number of TCP connections the operating system will accept on the server’s behalf without the server accepting them from the operating system
- **KEEPALIVE_TIMEOUT**: Maximum time in seconds that the server allows a connection to be open between RPCs
- **KEEPALIVE_MAX_CONN**: Maximum number of RPCs that the server will execute on a single connection
- **TIMEOUT**: Maximum time in seconds the server will wait for the client to do anything while processing an RPC
- **RPC_LOG**: Create a separated log file for xml-rpc requests, in `/var/log/one/one_xmlrpc.log`
- **MESSAGE_SIZE**: Buffer size in bytes for XML-RPC responses.
- **LOG_CALL_FORMAT**: Format string to log XML-RPC calls. Interpreted strings:
  - `%i` - request id
- %m – method name
- %u – user id
- %U – user name
- %l – param list
- %p – user password
- %g – group id
- %G – group name
- %a – auth token
- %% – %

#*******************************************************************************
# XML-RPC server configuration
#*******************************************************************************

#MAX_CONN = 15
#MAX_CONN_BACKLOG = 15
#KEEPALIVE_TIMEOUT = 15
#KEEPALIVE_MAX_CONN = 30
#TIMEOUT = 15
#RPC_LOG = NO
#MESSAGE_SIZE = 1073741824
#LOG_CALL_FORMAT = "Req:%i UID:%u %m invoked %l"

Warning: This functionality is only available when compiled with xmlrpc-c libraries >= 1.32. Currently only the packages distributed by OpenNebula are linked with this library.

10.1.5 Virtual Networks

- NETWORK_SIZE: Default size for virtual networks
- MAC_PREFIX: Default MAC prefix to generate virtual network MAC addresses

Sample configuration:

#*******************************************************************************
# Physical Networks configuration
#*******************************************************************************

NETWORK_SIZE = 254
MAC_PREFIX = "02:00"

10.1.6 Datastores

The Storage Subsystem allows users to set up images, which can be operative systems or data, to be used in Virtual Machines easily. These images can be used by several Virtual Machines simultaneously, and also shared with other users.

Here you can configure the default values for the Datastores and Image templates. You have more information about the templates syntax here.
• **DATASTORE_LOCATION**: Path for Datastores in the hosts. It is the same for all the hosts in the cluster. **DATASTORE_LOCATION** is only for the hosts and not the front-end. It defaults to /var/lib/one/datastores (or $ONE_LOCATION/var/datastores in self-contained mode)

• **DATASTORE_BASE_PATH**: This is the base path for the SOURCE attribute of the images registered in a Datastore. This is a default value, that can be changed when the datastore is created.

• **DATASTORE_CAPACITY_CHECK**: Checks that there is enough capacity before creating a new imag. Defaults to Yes.

• **DEFAULT_IMAGE_TYPE**: Default value for TYPE field when it is omitted in a template. Values accepted are OS, CDROM, DATABLOCK.

• **DEFAULT_DEVICE_PREFIX**: Default value for DEV_PREFIX field when it is omitted in a template. The missing DEV_PREFIX attribute is filled when Images are created, so changing this prefix won’t affect existing Images. It can be set to:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Device type</th>
</tr>
</thead>
<tbody>
<tr>
<td>hd</td>
<td>IDE</td>
</tr>
<tr>
<td>sd</td>
<td>SCSI</td>
</tr>
<tr>
<td>xvd</td>
<td>XEN Virtual Disk</td>
</tr>
<tr>
<td>vd</td>
<td>KVM virtual disk</td>
</tr>
</tbody>
</table>

• **DEFAULT_CDROM_DEVICE_PREFIX**: Same as above but for CDROM devices.

More information on the image repository can be found in the Managing Virtual Machine Images guide.

Sample configuration:

```bash
#*******************************************************************************
# Image Repository Configuration
#*******************************************************************************

#DATASTORE_LOCATION = /var/lib/one/datastores

#DATASTORE_BASE_PATH = /var/lib/one/datastores

DATASTORE_CAPACITY_CHECK = "yes"

DEFAULT_IMAGE_TYPE = "OS"
DEFAULT_DEVICE_PREFIX = "hd"

DEFAULT_CDROM_DEVICE_PREFIX = "hd"
```

## 10.1.7 Information Collector

This driver CANNOT BE ASSIGNED TO A HOST, and needs to be used with KVM or Xen drivers Options that can be set:

- `-a`: Address to bind the collectd socket (default 0.0.0.0)
- `-p`: UDP port to listen for monitor information (default 4124)
- `-f`: Interval in seconds to flush collected information (default 5)
- `-t`: Number of threads for the server (default 50)
- `-i`: Time in seconds of the monitorization push cycle. This parameter must be smaller than MONITOR-ING_INTERVAL, otherwise push monitorization will not be effective.

Sample configuration:
10.1.8 Information Drivers

The information drivers are used to gather information from the cluster nodes, and they depend on the virtualizer you are using. You can define more than one information manager but make sure it has different names. To define it, the following needs to be set:

- **name**: name for this information driver.
- **executable**: path of the information driver executable, can be an absolute path or relative to /usr/lib/one/mads/
- **arguments**: for the driver executable, usually a probe configuration file, can be an absolute path or relative to /etc/one/.

For more information on configuring the information and monitoring system and hints to extend it please check the information driver configuration guide.

Sample configuration:

```ini
#--------------------------------------------------------------
# KVM Information Driver Manager Configuration
# -r number of retries when monitoring a host
# -t number of threads, i.e. number of hosts monitored at the same time
#--------------------------------------------------------------
IM_MAD = [
    name = "kvm",
    executable = "one_im_ssh",
    arguments = "-r 0 -t 15 kvm"
]
#--------------------------------------------------------------
```

10.1.9 Virtualization Drivers

The virtualization drivers are used to create, control and monitor VMs on the hosts. You can define more than one virtualization driver (e.g. you have different virtualizers in several hosts) but make sure they have different names. To define it, the following needs to be set:

- **name**: name of the virtualization driver.
- **executable**: path of the virtualization driver executable, can be an absolute path or relative to /usr/lib/one/mads/
- **arguments**: for the driver executable
- **type**: driver type, supported drivers: xen, kvm or xml
- **default**: default values and configuration parameters for the driver, can be an absolute path or relative to /etc/one/

For more information on configuring and setting up the virtualizer please check the guide that suits you:

- Xen Adaptor
- KVM Adaptor
- VMware Adaptor
Sample configuration:

```plaintext
# Virtualization Driver Configuration

VM_MAD = [
    name = "kvm",
    executable = "one_vmm_ssh",
    arguments = "-t 15 -r 0 kvm",
    default = "vmm_ssh/vmm_ssh_kvm.conf",
    type = "kvm"
]
```

### 10.1.10 Transfer Driver

The transfer drivers are used to transfer, clone, remove and create VM images. The default TM_MAD driver includes plugins for all supported storage modes. You may need to modify the TM_MAD to add custom plugins.

- **executable**: path of the transfer driver executable, can be an absolute path or relative to `/usr/lib/one/mads/`
- **arguments**: for the driver executable:
  - `-t`: number of threads, i.e. number of transfers made at the same time
  - `-d`: list of transfer drivers separated by commas, if not defined all the drivers available will be enabled

For more information on configuring different storage alternatives please check the storage configuration guide.

Sample configuration:

```plaintext
# Transfer Manager Driver Configuration

TM_MAD = [
    executable = "one_tm",
    arguments = "-t 15 -d dummy,lvm,shared,fs_lvm,qcow2,ssh,vmfs,ceph"
]
```

The configuration for each driver is defined in the TM_MAD_CONF section. These values are used when creating a new datastore and should not be modified since they define the datastore behaviour.

- **name**: name of the transfer driver, listed in the `-d` option of the TM_MAD section
- **ln_target**: determines how the persistent images will be cloned when a new VM is instantiated.
  - NONE: The image will be linked and no more storage capacity will be used
  - SELF: The image will be cloned in the Images datastore
  - SYSTEM: The image will be cloned in the System datastore
- **clone_target**: determines how the non persistent images will be cloned when a new VM is instantiated.
  - NONE: The image will be linked and no more storage capacity will be used
  - SELF: The image will be cloned in the Images datastore
  - SYSTEM: The image will be cloned in the System datastore
- **shared**: determines if the storage holding the system datastore is shared among the different hosts or not. Valid values: yes or no.
Sample configuration:

```python
TM_MAD_CONF = [
    name = "lvm",
    ln_target = "NONE",
    clone_target = "SELF",
    shared = "yes"
]

TM_MAD_CONF = [
    name = "shared",
    ln_target = "NONE",
    clone_target = "SYSTEM",
    shared = "yes"
]
```

### 10.1.11 Datastore Driver

The Datastore Driver defines a set of scripts to manage the storage backend.

- **executable**: path of the transfer driver executable, can be an absolute path or relative to `/usr/lib/one/mads/`
- **arguments**: for the driver executable
  - `-t` number of threads, i.e. number of repo operations at the same time
  - `-d` datastore mads separated by commas

Sample configuration:

```python
DATASTORE_MAD = [
    executable = "one_datastore",
    arguments = "-t 15 -d dummy,fs,vmfs,lvm,ceph"
]
```

For more information on this Driver and how to customize it, please visit its reference guide.

### 10.1.12 Hook System

Hooks in OpenNebula are programs (usually scripts) which execution is triggered by a change in state in Virtual Machines or Hosts. The hooks can be executed either locally or remotely in the node where the VM or Host is running. To configure the Hook System the following needs to be set in the OpenNebula configuration file:

- **executable**: path of the hook driver executable, can be an absolute path or relative to `/usr/lib/one/mads/`
- **arguments**: for the driver executable, can be an absolute path or relative to `/etc/one/`

Sample configuration:

```python
HM_MAD = [
    executable = "one_hm" ]
```

Virtual Machine Hooks (VM_HOOK) defined by:

- **name**: for the hook, useful to track the hook (OPTIONAL).
- **on**: when the hook should be executed,
- **CREATE**, when the VM is created (onevm create)
- **PROLOG**, when the VM is in the prolog state
- **RUNNING**, after the VM is successfully booted
- **UNKNOWN**, when the VM is in the unknown state
- **SHUTDOWN**, after the VM is shutdown
- **STOP**, after the VM is stopped (including VM image transfers)
- **DONE**, after the VM is deleted or shutdown
- **CUSTOM**, user defined specific STATE and LCM_STATE combination of states to trigger the hook

  - **command**: path can be absolute or relative to /usr/share/one/hooks
  - **arguments**: for the hook. You can access to VM information with $
    - **$ID**, the ID of the virtual machine
    - **$TEMPLATE**, the VM template in xml and base64 encoded multiple
    - **PREV_STATE**, the previous STATE of the Virtual Machine
    - **PREV_LCM_STATE**, the previous LCM STATE of the Virtual Machine
  - **remote**: values,
    - **YES**, The hook is executed in the host where the VM was allocated
    - **NO**, The hook is executed in the OpenNebula server (default)

**Host Hooks (HOST_HOOK) defined by:**

  - **name**: for the hook, useful to track the hook (OPTIONAL)
  - **on**: when the hook should be executed,
    - **CREATE**, when the Host is created (onehost create)
    - **ERROR**, when the Host enters the error state
    - **DISABLE**, when the Host is disabled
  - **command**: path can be absolute or relative to /usr/share/one/hooks
  - **arguments**: for the hook. You can use the following Host information:
    - **$ID**, the ID of the host
    - **$TEMPLATE**, the Host template in xml and base64 encoded
  - **remote**: values,
    - **YES**, The hook is executed in the host
    - **NO**, The hook is executed in the OpenNebula server (default)

Sample configuration:

```python
VM_HOOK = [
    name = "advanced_hook",
    on = "CUSTOM",
    state = "ACTIVE",
    lcm_state = "BOOT_UNKNOWN",
]
```
10.1.13 Auth Manager Configuration

- **AUTH_MAD**: The *driver* that will be used to authenticate and authorize OpenNebula requests. If not defined, OpenNebula will use the built-in auth policies.
  - **executable**: path of the auth driver executable, can be an absolute path or relative to /usr/lib/one/mads/.
  - **authn**: list of authentication modules separated by commas, if not defined all the modules available will be enabled.
  - **authz**: list of authentication modules separated by commas.

- **SESSION_EXPIRATION_TIME**: Time in seconds to keep an authenticated token as valid. During this time, the driver is not used. Use 0 to disable session caching.

- **ENABLE_OTHER_PERMISSIONS**: Whether or not to enable the permissions for ‘other’. Users in the oneadmin group will still be able to change these permissions. Values: YES or NO.

- **DEFAULT_UMASK**: Similar to Unix umask, sets the default resources permissions. Its format must be 3 octal digits. For example a umask of 137 will set the new object’s permissions to 640 um- u- --

Sample configuration:

```
AUTH_MAD = [
    executable = "one_auth_mad",
    authn = "ssh,x509,ldap,server_cipher,server_x509"
]

SESSION_EXPIRATION_TIME = 900

#ENABLE_OTHER_PERMISSIONS = "YES"

DEFAULT_UMASK = 177
```

The **DEFAULT_AUTH** can be used to point to the desired default authentication driver, for example `ldap`:

```
DEFAULT_AUTH = "ldap"
```

10.1.14 Restricted Attributes Configuration

Users outside the oneadmin group won’t be able to instantiate templates created by users outside the ‘oneadmin’ group that include the attributes restricted by:

- **VM_RESTRICTED_ATTR**: Virtual Machine attribute to be restricted for users outside the ‘oneadmin’ group.
- **IMAGE_RESTRICTED_ATTR**: Image attribute to be restricted for users outside the ‘oneadmin’ group.
- **VNET_RESTRICTED_ATTR**: Virtual Network attribute to be restricted for users outside the ‘oneadmin’ group when updating a reservation. These attributes are not considered for regular VNET creation.

If the VM template has been created by admins in the ‘oneadmin’ group, then users outside the ‘oneadmin’ group can instantiate these templates.

Sample configuration:
VM_RESTRICTED_ATTR = "CONTEXT/FILES"
VM_RESTRICTED_ATTR = "NIC/MAC"
VM_RESTRICTED_ATTR = "NIC/VLAN_ID"
VM_RESTRICTED_ATTR = "NIC/BRIDGE"
VM_RESTRICTED_ATTR = "NIC_DEFAULT/MAC"
VM_RESTRICTED_ATTR = "NIC_DEFAULT/VLAN_ID"
VM_RESTRICTED_ATTR = "DISK/TOTAL_BYTES_SEC"
VM_RESTRICTED_ATTR = "DISK/READ_BYTES_SEC"
VM_RESTRICTED_ATTR = "DISK/WRITE_BYTES_SEC"
VM_RESTRICTED_ATTR = "DISK/TOTAL_IOPS_SEC"
VM_RESTRICTED_ATTR = "DISK/READ_IOPS_SEC"
VM_RESTRICTED_ATTR = "DISK/WRITE_IOPS_SEC"
VM_RESTRICTED_ATTR = "DISK/SIZE"
VM_RESTRICTED_ATTR = "DISK/ORIGINAL_SIZE"
VM_RESTRICTED_ATTR = "CPU_COST"
VM_RESTRICTED_ATTR = "MEMORY_COST"
VM_RESTRICTED_ATTR = "DISK_COST"

VNET_RESTRICTED_ATTR = "PHYDEV"
VNET_RESTRICTED_ATTR = "VLAN_ID"
VNET_RESTRICTED_ATTR = "VLAN"
VNET_RESTRICTED_ATTR = "BRIDGE"
VNET_RESTRICTED_ATTR = "AR/PHYDEV"
VNET_RESTRICTED_ATTR = "AR/VLAN_ID"
VNET_RESTRICTED_ATTR = "AR/VLAN"
VNET_RESTRICTED_ATTR = "AR/BRIDGE"

OpenNebula evaluates these attributes:
- on VM template instantiate (onetemplate instantiate)
- on VM create (onevm create)
- on VM attach nic (onevm nic-attach) (for example to forbid users to use NIC/MAC)

### 10.1.15 Inherited Attributes Configuration

The following attributes will be copied from the resource template to the instantiated VMs. More than one attribute can be defined.

- **INHERIT_IMAGE_ATTR**: Attribute to be copied from the Image template to each VM/DISK.
- **INHERIT_DATASTORE_ATTR**: Attribute to be copied from the Datastore template to each VM/DISK.
- **INHERIT_VNET_ATTR**: Attribute to be copied from the Network template to each VM/NIC.

Sample configuration:

```bash
#INHERIT_IMAGE_ATTR = "EXAMPLE"
#INHERIT_IMAGE_ATTR = "SECOND_EXAMPLE"
#INHERIT_DATASTORE_ATTR = "COLOR"
```
10.1.16 OneGate Configuration

- **ONEGATE_ENDPOINT**: Endpoint where OneGate will be listening. Optional.

Sample configuration:

```
ONEGATE_ENDPOINT = "http://192.168.0.5:5030"
```

10.2 Scheduler

The Scheduler module is in charge of the assignment between pending Virtual Machines and known Hosts. OpenNebula’s architecture defines this module as a separate process that can be started independently of oned. The OpenNebula scheduling framework is designed in a generic way, so it is highly modifiable and can be easily replaced by third-party developments.

10.2.1 The Match-making Scheduler

OpenNebula comes with a **match making scheduler** (*mm_sched*) that implements the *Rank Scheduling Policy*. The goal of this policy is to prioritize those resources more suitable for the VM.

The match-making algorithm works as follows:

- Each disk of a running VM consumes storage from an Image Datastore. The VMs that require more storage than there is currently available are filtered out, and will remain in the ‘pending’ state.
- Those hosts that do not meet the VM requirements (see the SCHED_REQUIREMENTS attribute) or do not have enough resources (available CPU and memory) to run the VM are filtered out (see below for more information).
- The same happens for System Datastores: the ones that do not meet the DS requirements (see the SCHED_DS_REQUIREMENTS attribute) or do not have enough free storage are filtered out.
- The SCHED_RANK and SCHED_DS_RANK expressions are evaluated upon the Host and Datastore list using the information gathered by the monitor drivers. Any variable reported by the monitor driver (or manually set in the Host or Datastore template) can be included in the rank expressions.
- Those resources with a higher rank are used first to allocate VMs.

This scheduler algorithm easily allows the implementation of several placement heuristics (see below) depending on the RANK expressions used.
Configuring the Scheduling Policies

The policy used to place a VM can be configured in two places:

- For each VM, as defined by the SCHED_RANK and SCHED_DS_RANK attributes in the VM template.
- Globally for all the VMs in the sched.conf file

Re-Scheduling Virtual Machines

When a VM is in the running state it can be rescheduled. By issuing the `onevm resched` command the VM’s rescheduling flag is set. In a subsequent scheduling interval, the VM will be considered for rescheduling, if:

- There is a suitable host for the VM
- The VM is not already running in it

This feature can be used by other components to trigger rescheduling action when certain conditions are met.

Scheduling VM Actions

Users can schedule one or more VM actions to be executed at a certain date and time. The `onevm` command ‘schedule’ option will add a new SCHED_ACTION attribute to the Virtual Machine editable template. Visit the VM guide for more information.

10.2.2 Configuration

The behavior of the scheduler can be tuned to adapt it to your infrastructure with the following configuration parameters defined in `/etc/one/sched.conf`:

- `MESSAGE_SIZE`: Buffer size in bytes for XML-RPC responses.
- `ONED_PORT`: Port to connect to the OpenNebula daemon oned (Default: 2633)
- `SCHED_INTERVAL`: Seconds between two scheduling actions (Default: 30)
- `MAX_VM`: Maximum number of Virtual Machines scheduled in each scheduling action (Default: 5000). Use 0 to schedule all pending VMs each time.
- `MAX_DISPATCH`: Maximum number of Virtual Machines actually dispatched to a host in each scheduling action (Default: 30)
- `MAX_HOST`: Maximum number of Virtual Machines dispatched to a given host in each scheduling action (Default: 1)
- `LIVE_RESCHEDS`: Perform live (1) or cold migrations (0) when rescheduling a VM
- `DEFAULT_SCHED`: Definition of the default scheduling algorithm.
  - `RANK`: Arithmetic expression to rank suitable hosts based on their attributes.
  - `POLICY`: A predefined policy, it can be set to:
### POLICY | DESCRIPTION
--- | ---
0 | **Packing**: Minimize the number of hosts in use by packing the VMs in the hosts to reduce VM fragmentation
1 | **Striping**: Maximize resources available for the VMs by spreading the VMs in the hosts
2 | **Load-aware**: Maximize resources available for the VMs by using those nodes with less load
3 | **Custom**: Use a custom RANK
4 | **Fixed**: Hosts will be ranked according to the PRIORITY attribute found in the Host or Cluster template

- **DEFAULT_DS_SCHED**: Definition of the default storage scheduling algorithm.
  - **RANK**: Arithmetic expression to rank suitable *datastores* based on their attributes.
  - **POLICY**: A predefined policy, it can be set to:

| POLICY | DESCRIPTION |
--- | --- |
0 | **Packing**: Tries to optimize storage usage by selecting the DS with less free space
1 | **Striping**: Tries to optimize I/O by distributing the VMs across datastores
2 | **Custom**: Use a custom RANK
3 | **Fixed**: Datastores will be ranked according to the PRIORITY attribute found in the Datastore template

The optimal values of the scheduler parameters depend on the hypervisor, storage subsystem and number of physical hosts. The values can be derived by finding out the max number of VMs that can be started in your set up with out getting hypervisor related errors.

**Sample Configuration:**

```plaintext
MESSAGE_SIZE = 1073741824
ONED_PORT = 2633
SCHED_INTERVAL = 30
MAX_VM = 5000
MAX_DISPATCH = 30
MAX_HOST = 1
LIVE_RESCHEDS = 0
DEFAULT_SCHED = [
    policy = 3,
    rank = "-(RUNNING_VMS * 50 + FREE_CPU)"
]
DEFAULT_DS_SCHED = [
    policy = 1
]
```

### Pre-defined Placement Policies

The following list describes the predefined policies (**DEFAULT_SCHED**) that can be configured through the sched.conf file.

**Packing Policy**

- **Target**: Minimize the number of cluster nodes in use
• **Heuristic**: Pack the VMs in the cluster nodes to reduce VM fragmentation
• **Implementation**: Use those nodes with more VMs running first

\[ RANK = \text{RUNNING\_VMS} \]

**Striping Policy**

• **Target**: Maximize the resources available to VMs in a node
• **Heuristic**: Spread the VMs in the cluster nodes
• **Implementation**: Use those nodes with less VMs running first

\[ RANK = \text{"- RUNNING\_VMS"} \]

**Load-aware Policy**

• **Target**: Maximize the resources available to VMs in a node
• **Heuristic**: Use those nodes with less load
• **Implementation**: Use those nodes with more FREE\_CPU first

\[ RANK = \text{FREE\_CPU} \]

**Fixed Policy**

• **Target**: Sort the hosts manually
• **Heuristic**: Use the PRIORITY attribute
• **Implementation**: Use those nodes with more PRIORITY first

\[ RANK = \text{PRIORITY} \]

**Pre-defined Storage Policies**

The following list describes the predefined storage policies (**DEFAULT\_DS\_SCHED**) that can be configured through the `sched.conf` file.

**Packing Policy**

Tries to optimize storage usage by selecting the DS with less free space

• **Target**: Minimize the number of system datastores in use
• **Heuristic**: Pack the VMs in the system datastores to reduce VM fragmentation
• **Implementation**: Use those datastores with less free space first

\[ RANK = \text{"- FREE\_MB"} \]
Striping Policy

- **Target:** Maximize the I/O available to VMs
- **Heuristic:** Spread the VMs in the system datastores
- **Implementation:** Use those datastores with more free space first

\[ RANK = "FREE_MB" \]

Fixed Policy

- **Target:** Sort the datastores manually
- **Heuristic:** Use the PRIORITY attribute
- **Implementation:** Use those datastores with more PRIORITY first

\[ RANK = \text{PRIORITY} \]

### 10.2.3 Limiting the Resources Exposed by a Host

Prior to assigning a VM to a Host, the available capacity is checked to ensure that the VM fits in the host. The capacity is obtained by the monitor probes. You may alter this behaviour by reserving an amount of capacity (memory and cpu). You can reserve this capacity:

- Cluster-wise, by updating the cluster template (e.g. `onecluster update`). All the host of the cluster will reserve the same amount of capacity.
- Host-wise, by updating the host template (e.g. `onehost update`). This value will override those defined at cluster level.

In particular the following capacity attributes can be reserved:

- `RESERVED_CPU` in percentage. It will be subtracted from the TOTAL CPU
- `RESERVED_MEM` in KB. It will be subtracted from the TOTAL MEM

**Note:** These values can be negative, in that case you’ll be actually increasing the overall capacity so overcommitting host capacity.

### 10.3 Logging & Debugging

OpenNebula provides logs for many resources. It supports two logging systems: file based logging systems and syslog logging.

In the case of file based logging, OpenNebula keeps separate log files for each active component, all of them stored in `/var/log/one`. To help users and administrators find and solve problems, they can also access some of the error messages from the CLI or the Sunstone GUI.

With syslog the logging strategy is almost identical, except that the logging message change slightly their format following syslog logging conventions.
10.3.1 Configure the Logging System

The Logging system can be changed in `/etc/one/oned.conf`, specifically under the LOG section. Two parameters can be changed: SYSTEM, which is either ‘syslog’ or ‘file’ (default), and the DEBUG_LEVEL is the logging verbosity.

For the scheduler the logging system can be changed in the exact same way. In this case the configuration is in `/etc/one/sched.conf`.

10.3.2 Log Resources

There are different log resources corresponding to different OpenNebula components:

- **ONE Daemon**: The core component of OpenNebula dumps all its logging information onto `/var/log/one/oned.log`. Its verbosity is regulated by DEBUG_LEVEL in `/etc/one/oned.conf`. By default the one start up scripts will backup the last oned.log file using the current time, e.g. oned.log.20121011151807. Alternatively, this resource can be logged to the syslog.

- **Scheduler**: All the scheduler information is collected into the /var/log/one/sched.log file. This resource can also be logged to the syslog.

- **Virtual Machines**: The information specific of the VM will be dumped in the log file `/var/log/one/<vmid>.log`. All VMs controlled by OpenNebula have their folder, `/var/lib/one/vms/<VID>`, or to the syslog if enabled. You can find the following information in it:
  
  - **Deployment description files**: Stored in deployment.<EXECUTION>, where <EXECUTION> is the sequence number in the execution history of the VM (deployment.0 for the first host, deployment.1 for the second and so on).
  
  - **Transfer description files**: Stored in transfer.<EXECUTION>.<OPERATION>, where <EXECUTION> is the sequence number in the execution history of the VM, <OPERATION> is the stage where the script was used, e.g. transfer.0.prolog, transfer.0.epilog, or transfer.1.cleanup.

- **Drivers**: Each driver can have activated its ONE_MAD_DEBUG variable in their RC files. If so, error information will be dumped to `/var/log/one/name-of-the-driver-executable.log`; log information of the drivers is in oned.log.

10.3.3 Logging Format

The anatomy of an OpenNebula message for a file based logging system is the following:

```
date [Z<zone_id>][module][log_level]: message body
```

In the case of syslog it follows the standard:

```
date hostname process[pid]: [Z<zone_id>][module][log_level]: message body
```

Where the zone_id is the ID of the zone in the federation, 0 for single zone set ups, module is any of the internal OpenNebula components: VMM, ReM, TM, etc. And the log_level is a single character indicating the log level: I for info, D for debug, etc.

For the syslog, OpenNebula will also log the Virtual Machine events like this:

```
date hostname process[pid]: [VM id][module][log_level]: message body
```
10.3.4 Virtual Machine Errors

Virtual Machine errors can be checked by the owner or an administrator using the `onevm show` output:

```
$ onevm show 0
VIRTUAL MACHINE 0 INFORMATION
ID : 0
NAME : one-0
USER : oneadmin
GROUP : oneadmin
STATE : ACTIVE
LCM_STATE : PROLOG_FAILED
START TIME : 07/19 17:44:20
END TIME : 07/19 17:44:31
DEPLOY ID : -

VIRTUAL MACHINE MONITORING
NET_TX : 0
NET_RX : 0
USED MEMORY : 0
USED CPU : 0

VIRTUAL MACHINE TEMPLATE
CONTEXT=[
    FILES=/tmp/some_file,
    TARGET=hdb ]
CPU=0.1
ERROR=[
    MESSAGE="Error executing image transfer script: Error copying /tmp/some_file to /var/lib/one/0/images/isofiles",
    TIMESTAMP="Tue Jul 19 17:44:31 2011" ]
MEMORY=64
NAME=one-0
VMID=0

VIRTUAL MACHINE HISTORY
SEQ HOSTNAME ACTION START TIME PTIME
0 host01 none 07/19 17:44:31 00 00:00:00 00 00:00:00
```

Here the error tells that it could not copy a file, most probably it does not exist.

Alternatively you can also check the log files for the VM at `/var/log/one/<vmid>.log`.

**Warning:** Check the Virtual Machines High Availability Guide, to learn how to recover a VM in fail state.

10.3.5 Host Errors

Host errors can be checked executing the `onehost show` command:

```
$ onehost show 1
HOST 1 INFORMATION
ID : 1
NAME : host01
STATE : ERROR
IM_MAD : im_kvm
VM_MAD : vmm_kvm
TM_MAD : tm_shared
```
The error message appears in the ERROR value of the monitoring. To get more information you can check /var/log/one/oned.log. For example for this error we get in the log file:

From the execution output we notice that the host name is not know, probably a mistake naming the host.

### 10.4 Onedb Tool

This guide describes the onedb CLI tool. It can be used to get information from an OpenNebula database, upgrade it, or fix inconsistency problems.

#### 10.4.1 Connection Parameters

The command onedb can connect to any SQLite or MySQL database. Visit the onedb man page for a complete reference. These are two examples for the default databases:

```
$ onedb <command> -v --sqlite /var/lib/one/one.db

$ onedb <command> -v -S localhost -u oneadmin -p oneadmin -d opennebula
```

#### 10.4.2 onedb fsck

Checks the consistency of the DB, and fixes the problems found. For example, if the machine where OpenNebula is running crashes, or looses connectivity with the database, you may have a wrong number of VMs running in a Host, or incorrect usage quotas for some users.

```
$ onedb fsck --sqlite /var/lib/one/one.db
Sqlite database backup stored in /var/lib/one/one.db.bck
Use 'onedb restore' or copy the file back to restore the DB.

Host 0 RUNNING_VMS has 12 is 11
Host 0 CPU_USAGE has 1200 is 1100
Host 0 MEM_USAGE has 1572864 is 1441792
```
If onedb fsck shows the following error message:

[UNREPAIRED] History record for VM <<vid>> seq # <<seq>> is not closed (etime = 0)

This is due to bug #4000. It means that when using accounting or showback, the etime (end-time) of that history record is not set, and the VM is considered as still running when it should not. To fix this problem, locate the time when the VM was shut down in the logs and then execute this patch to edit the times manually:

$ onedb patch -v --sqlite /var/lib/one/one.db /usr/lib/one/ruby/onedb/patches/history_times.rb

Version read:
Shared tables 4.11.80 : OpenNebula 4.14.1 daemon bootstrap
Local tables  4.13.85 : OpenNebula 4.14.1 daemon bootstrap

Sqlite database backup stored in /var/lib/one/one.db_2015-10-13_12:40:2.bck
Use 'onedb restore' or copy the file back to restore the DB.

> Running patch /usr/lib/one/ruby/onedb/patches/history_times.rb
This tool will allow you to edit the timestamps of VM history records, used to calculate accounting and showback. VM ID: 1
History sequence number: 0

STIME Start time : 2015-10-08 15:24:06 UTC
PSTIME Prolog start time : 2015-10-08 15:24:06 UTC
PETIME Prolog end time : 2015-10-08 15:24:29 UTC
RSTIME Running start time : 2015-10-08 15:24:29 UTC
RETIME Running end time : 2015-10-08 15:42:35 UTC
ESTIME Epilog start time : 2015-10-08 15:42:35 UTC
EETIME Epilog end time : 2015-10-08 15:42:36 UTC
ETIME End time : 2015-10-08 15:42:36 UTC

To set new values:
empty to use current value; <YYYY-MM-DD HH:MM:SS> in UTC; or 0 to leave unset (open history record)

STIME Start time : 2015-10-08 15:24:06 UTC
New value :

ETIME End time : 2015-10-08 15:42:36 UTC
New value :

The history record # 0 for VM 1 will be updated with these new values:
STIME Start time : 2015-10-08 15:24:06 UTC
PSTIME Prolog start time : 2015-10-08 15:24:06 UTC
PETIME Prolog end time : 2015-10-08 15:24:29 UTC
RSTIME Running start time : 2015-10-08 15:24:29 UTC
RETIME Running end time : 2015-10-08 15:42:35 UTC
ESTIME Epilog start time : 2015-10-08 15:42:35 UTC
EETIME Epilog end time : 2015-10-08 15:42:36 UTC
10.4.3 onedb version

Prints the current DB version.

```
$ onedb version --sqlite /var/lib/one/one.db
3.8.0
```

Use the --v flag to see the complete version and comment.

```
$ onedb version -v --sqlite /var/lib/one/one.db
Version: 3.8.0
Timestamp: 10/19 16:04:17
Comment: Database migrated from 3.7.80 to 3.8.0 (OpenNebula 3.8.0) by onedb command.
```

If the MySQL database password contains special characters, such as @ or #, the onedb command will fail to connect to it.

The workaround is to temporarily change the oneadmin’s password to an ASCII string. The set password statement can be used for this:

```
$ mysql -u oneadmin -p
mysql> SET PASSWORD = PASSWORD('newpass');
```

10.4.4 onedb history

Each time the DB is upgraded, the process is logged. You can use the history command to retrieve the upgrade history.

```
$ onedb history -S localhost -u oneadmin -p oneadmin -d opennebula
Version: 3.0.0
Timestamp: 10/07 12:40:49
Comment: OpenNebula 3.0.0 daemon bootstrap

... Version: 3.7.80
Timestamp: 10/08 17:36:15
Comment: Database migrated from 3.6.0 to 3.7.80 (OpenNebula 3.7.80) by onedb command.

Version: 3.8.0
Timestamp: 10/19 16:04:17
Comment: Database migrated from 3.7.80 to 3.8.0 (OpenNebula 3.8.0) by onedb command.
```

10.4.5 onedb upgrade

The upgrade process is fully documented in the Upgrading from Previous Versions guide.
10.4.6 onedb backup

Dumps the OpenNebula DB to a file.

```bash
$ onedb backup --sqlite /var/lib/one/one.db /tmp/my_backup.db
Sqlite database backup stored in /tmp/my_backup.db
Use 'onedb restore' or copy the file back to restore the DB.
```

10.4.7 onedb restore

Restores the DB from a backup file. Please note that this tool will only restore backups generated from the same backend, i.e. you cannot backup a SQLite database and then try to populate a MySQL one.