Installation Guide

Document version	0.5
Document release date	13th December 2011
	document revisions

ⓘ PLEASE NOTE:

- *You must have a valid license before beginning your install! If you don't have a valid license, contact the OnApp Sales team or your integration specialist.*

- *The installation processes described in this document require servers to have a base installation of CentOS 5.X x64 with the standard repositories enabled. If you have additional repositories enabled, please disable them before continuing.*

Contents

1. Control Panel Installation

ⓘ If mysql server is already installed, it must not have a password configured: this will be configured by our installer. Any password that is already configured will cause an installer error.

ⓘ Installer output is redirected to ./onapp-cp-install.log

ⓘ All installer critical errors are in /var/log/messages

ⓘ Once the installation of the control panel is complete, your default OnApp login will be **admin / changeme.** *The password can be changed via the Control Panel's Users and Groups menu.*

ⓘ If you're replacing an existing Control Panel with a new install, please dump your current mysql database. Once you've installed your new control panel, overwrite its database with the previous one. You can find details about the database by running cat /onapp/interface/config/database.yml *and looking at the connection details located under 'production'.*

1. **Update your server using YUM:**

```
OnApp-CP#> yum -y update
```

ⓘ If anything was updated, reboot the server.

2. **Download OnApp YUM repository file (for CentOS 5.x x86_64):**

```
OnApp-CP#> wget http://rpm.repo.onapp.com/repo/centos/5/onapp-
repo.noarch.rpm
OnApp-CP#> rpm -ivh onapp-repo.noarch.rpm
OnApp-CP#> yum clean all
```

3. **Install OnApp Control Panel installer package:**

```
OnApp CP#> yum install onapp-cp-install
```

4. **Run Control Panel installer:**

```
OnApp CP#> /onapp/onapp-cp-install/onapp-cp-install.sh
```

5. **Install OnApp License to activate the Control Panel:**

Enter a valid license key via the Web UI (you'll be prompted to do so).

ⓘ PLEASE NOTE: once you have entered a license it can take up to 15 minutes to activate. If you experience license problems after entering a valid license key, please contact support.

2. Hypervisor Installation

ⓘ Once the control panel server has been installed successfully, you can follow the process below to install each hypervisor and add it to the Control Panel server.

1. **Add the hypervisor to your cloud using the OnApp Control Panel:**

   Settings --> Hypervisors --> Add New Hypervisor

   Make sure the hypervisor is visible in the Control Panel, and at this point showing as inactive.

2. **Make sure your OS is up to date:**

```
bash#> yum -y update
```

3. **Enable IPv6:**

ⓘ This step is required regardless of whether you'll be using IPv6 or not.

Edit /etc/modprobe.conf and comment out the following strings:

```
alias ipv6 off
options ipv6 disable=1
```

Next, edit /etc/sysconfig/network and replace

```
NETWORKING_IPV6=no
```

with

```
NETWORKING_IPV6=yes
```

ⓘ These settings won't take effect until you reboot, but do not reboot now. We'll do that later.

4. **Download the OnApp repository:**

```
bash#> wget  http://rpm.repo.onapp.com/repo/centos/5/onapp-repo.noarch.rpm
bash#> rpm  -ivh  onapp-repo.noarch.rpm
bash#> yum clean all
```

5. **Install OnApp from the above repository:**

```
bash#> yum install onapp-hv-install
```

For Xen hypervisors:

```
bash#> /onapp/onapp-hv-install/onapp-hv-xen-install.sh
```

For KVM hypervisors:

```
bash#> /onapp/onapp-hv-install/onapp-hv-kvm-install.sh
```

6. **Configure the hypervisor for your cloud:**

ⓘ Ignore any errors stating stats and vmon services aren't running. This is expected at this stage.

```
bash#> /onapp/onapp-hv-install/onapp-hv-config.sh -h <CP_HOST_IP> -f
<FILE_TRANSFER_SERVER_IP>
```

<CP_HOST_IP> is the IP addresses of the Control Panel server.
<FILE_TRANSFER_SERVER_IP> is the IP address of the server that will hold your backups and templates.

7. **Reboot the hypervisor to complete the installation:**

```
bash#> shutdown -r now
```

3. Data store installation

ⓘ PLEASE NOTE:

- *This process assumes you have already configured a hypervisor to see the ISCSI/ATAoE block device it is connecting to, and that the SAN disk will be shown when running a fdisk -l.*
- *All hypervisors need access to the same datastore. Ensure that you have the block device visible on all hypervisors.*
- *VERY IMPORTANT: only perform this procedure once per data store!*
- *ALSO IMPORTANT: take care when choosing the disk/partition you wish to use for storing VM data!*

1. **Add the new data store to OnApp via the WebUI:**

   Go to *http://xxx.xxx.xxx.xxx/settings/data_stores/new*

   Add a unique label and the disk size of the data store.

2. **Find the data store's unique identifier (this is needed to create your volume group in step# 4):**

   Go back to the data stores page and read the IDENTIFIER.

   http://xxx.xxx.xxx.xxx/settings/data_stores

3. **SSH into a hypervisor that is able to connect to this datastore. Create the physical volume:**

   ```
   bash#> pvcreate --metadatasize 50M /dev/xxx
   ```

   ⓘ Replace xxx with the real device.

4. **Create the volume group:**

   ```
   bash#> vgcreate onapp-IDENTIFIER /dev/xxx
   ```

   ⓘ Replace xxx with the real device and IDENTIFIER with the info from the datastore page in the UI.

5. **Test hypervisor/volume group visibility:**

   Now you have the new datastore formatted you should be able to see the volume group from all hypervisors. To test this, run *pvscan* and *vgscan* on all hypervisors. Make sure you can see all identifiers on all hypervisors.

4. Configure backup volume

ⓘ While a separate backup server is preferred, you can also use the Control Panel server to store backups and templates (make sure you have sufficient disk space). The process below works for both approaches.

1. **Configure and mount the backup volume via NFS**

The backup volume block device should be visible on the backup server. This can be mounted over iSCSI or it could be a local disk array in the backup server. We will use this block device to create a filesystem and export over NFS to the hypervisors and Control Panel server.

In this example our backup volume will be /dev/sdb and our backup network will be 192.168.4.0/24. The backup server will hold 192.168.4.1

If you don't have a backup server then this will need to be done on the control panel server and mounted on the hypervisors.

2. **Format the backup volume with an ext3 filesystem**

```
[root@backup ~]# mke2fs -j /dev/sdb1
```

3. **Make the mount directly and mount the volume**

```
[root@backup ~]# mkdir /data
[root@backup ~]# mount /dev/sdb1 /data
```

4. **Add the entry to fstab to mount it automatically at boot**

```
[root@backup ~]# echo -e "/dev/sdb1\t/data\text3\tdefaults\t1 1" >> /etc/fstab
```

5. **Configure NFS on the backup server**

```
[root@backup ~]# chkconfig nfs on
[root@backup ~]# service nfs start
[root@backup ~]# mkdir /onapp
[root@backup ~]# ln -s /data /onapp/backups
[root@backup ~]# ln -s /data /onapp/templates
[root@backup ~]# echo -e "/onapp/backups\t192.168.4.*(rw,no_root_squash)"
>> /etc/exports
[root@backup ~]# echo -e
"/onapp/templates\t192.168.4.*(rw,no_root_squash)" >> /etc/exports
[root@backup ~]# exportfs -ra
```

6. Configure the Control Panel and Hypervisors

Add an entry to the fstab on all hypervisors and the control panel server, and mount the backup volume. In the example here, the backup server holds 192.168.4.1.

ⓘ Remember to do this on all hypervisors and on the control panel server – not on the backup server!

```
[root@backup ~]# mkdir /onapp/backups
[root@backup ~]# mkdir /onapp/templates
[root@backup ~]# echo "192.168.4.1:/onapp/backups /onapp/backups nfs
soft,noatime,intr,tcp,rsize=32768,wsize=32768 0 0" >> /etc/fstab
[root@backup ~]# echo "192.168.4.1:/onapp/templates /onapp/templates nfs
soft,noatime,intr,tcp,rsize=32768,wsize=32768 0 0" >> /etc/fstab
[root@backup ~]# mount -a
```

7. Download the recovery templates onto the backup server

```
[root@backup ~]# wget http://downloads.repo.onapp.com/get_rtemplate.sh
[root@backup ~]# sh get_rtemplate.sh
```

8. Download the OnApp VM templates to the backup server

ⓘ You must make sure you have already configured the NFS mounts above before running this script.

ⓘ This script MUST be run on the Control Panel server as root, not on the backup server.

```
[root@cp ~]# wget http://downloads.repo.onapp.com/get_template.sh
[root@cp ~]# sh get_template.sh
```

5. Generate SSH keys

ⓘ OnApp requires SSH keys to access various elements of the cloud. The script provided will generate and transfer keys as necessary.

- *The script needs to run on your Control Panel server.*
- *The script will overwrite any keys that already exist, so if you have custom keys already installed you will need to add them again after running the script.*
- *The script will ask you for login details to various servers during the execution. Please follow the onscreen instructions.*

1. **SSH into your Control Panel server**

2. **Download and run the script:**

```
bash#> wget http://downloads.repo.onapp.com/install-all-keys.sh
bash#> /bin/sh install-all-keys.sh
```

ⓘ Do not specify passphrases - just leave them blank!

6. Getting support

OnApp customers with a full (paid) license can contact support at any time:

support@onapp.com

+1 (888) 876 8666

http://onapp.com/support

Response times

OnApp offers a 15 minute SLA for critical issues. A critical issue is one that prevents your cloud service from working.

Known issues

A list of known issues and workarounds for the latest version of OnApp Cloud software is maintained at http://onapp.com/cloud/kis. Please check the list before contacting your support team!

Appendix: document revisions

v0.5, 13th December 2011

- Added note to Control Panel installation section about replacing an existing CP

v0.4, 25th November 2011

- Replaced backup configuration section with more streamlined instructions.

v0.3, 10th November 2011

- Added note: license required before install
- Updated CP install process with license details
- Updated HV install process with IPv6 details
- Added support details and Known Issues link

v0.2, 20th October 2011

- Clarified default CP login details

v0.1, 19th August 2011

- First release