4.1 Get Started

The guides in this section apply to installing the OnApp Cloud 4.1 version. For the release notes list, please refer to the Release Notes space.

Make sure you meet the Technical Details before preparing OnApp Cloud.

What's New in OnApp Cloud 4.1

The OnApp Cloud 4.1 release contains the following changes and new features:

**Changes to terminology and the user interface**

The following terminology changes have been made in the 4.1 version of the OnApp Cloud: hypervisors have been renamed as compute resources and hypervisor zones - as compute zones. Compute resources is a collective name for hypervisors, vCloud hypervisors and other hypervisor types.

**New and Improved Cloud Components**

**Application Servers**

Now you can install different applications (like Drupal, Joomla, WordPress etc.) on a server using web interface. This is implemented by means of application server. Application Server is a regular VS based on default CentOS template with pre-installed additional software. For more info, refer to Application Servers section of this guide.

**Instance Types**

Added possibility to use instance types during VS creation process. Instance types are preconfigured CPU/RAM/Disk/Bandwidth packages. You can add multiple instance types specifying different values for the parameters to suit your customer’s needs.

**Raw logs**

The raw logs functionality allows you to send logs associated with your CDN resources to your distant server in real time. The raw log allows customers to understand, analyze, and debug files delivered via OnApp CDN, or can be served as audit trailed.

**User Profile**

User profile UI was updated. Now at the Overview tab you can see user’s details at the left side of the page and billing details, prices and backups at the right side of the page.

**Java 8 Console Support**

Added support for Java 8 integrated console for appliances.

**Federation and vCloud Integration Improvements**

For the list of improvements, refer to Federation and OnApp and vCloud Director Configuration guides.

**Technical Details**

This chapter will list all the technical requirements as well as architecture diagrams that you should consider before creating a cloud in OnApp.
Hardware Requirements

An OnApp installation requires at least two physical machines – one for the Control Panel server, and the other for the compute resource server. You can have as many compute resource servers as you need. You will also need storage for your virtual servers (a data store), and we recommend that you set up a separate server for storing backups and templates. These are the minimum requirements for a small cloud. For a larger deployment, OnApp's technical team will advise you on the best possible setup.

On this page:

- Server Requirements
  - Compute resource servers
  - Control Panel server
  - Backup server
  - SAN
- Storage Requirements

Server Requirements

Compute resource servers

- x64 platform with AMD-V/VT-x hardware virtualization support enabled (CentOS 5 or 6)
- Quad Core 2Ghz+ CPU
- 8GB+ RAM
- 3x Gig network interface cards (4 recommended)
- 30 GB of free disk space (SSD Recommended)

Control Panel server

- Dual or Quad Core 2Ghz+ CPU
- 8GB RAM (16GB+ recommended)
- 100GB Raid 1
- 2x Gig network interface cards

Backup server

- 4GB RAM (8GB+ recommended)
- Dual or Quad Core 2Ghz+
- 2TB Storage mounted locally
- 2x Gig NIC
- CentOS 5 or 6 (x64)

SAN

- 1TB block storage minimum
- iSCSI, AoE or Fiber
- Can even be on a shared SAN

Storage Requirements
If you are going to use OnApp Integrated Storage, make sure to meet the following requirements:

<table>
<thead>
<tr>
<th>Integrated Storage Platform</th>
<th>Local Storage Only</th>
<th>Enterprise SAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>• any number of integrated storage drives can be grouped together across any compute resource</td>
<td>• minimum 1 dedicated partition in each compute resource</td>
<td>• centralised Block Storage SAN (iSCSI, ATA over Ethernet or Fibre Channel) accessible to every compute resource</td>
</tr>
<tr>
<td>• SSD drives recommended for best performance</td>
<td>• separate disk from the primary OS drive recommended</td>
<td>• at least 1 dedicated 1GBit/s NIC assigned per compute resource for the SAN</td>
</tr>
<tr>
<td>• at least 1 dedicated NIC assigned per compute resource for the SAN</td>
<td></td>
<td>• multiple NICs bonded or 10GBit/s ethernet recommended</td>
</tr>
<tr>
<td>• multiple NICs bonded or 10GBit/s ethernet recommended</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Hardware Requirements for High Availability CP

The basic implementation of High Availability requires that you deploy two Control Panel servers and one Database & Transactions server. We recommend the following configurations for those servers.

Please contact your account manager to enable High Availability Control Panel for your cloud.

Main Control Panel:

• Dual or Quad Core 2Ghz+ CPU
• 8GB RAM (16GB+ recommended)
• 100GB Raid 1
• 2x Gig network interface cards

Redundant Control Panel server

• Dual or Quad Core 2Ghz+ CPU
• 8GB RAM (16GB+ recommended)
• 100GB Raid 1
• 2x Gig network interface cards

Database & Transactions Server

• Dual or Quad Core 2Ghz+ CPU
• 8GB RAM (16GB+ recommended)
• 100GB Raid 1
• 2x Gig network interface cards

The recommendations for other servers are the same as for standard OnApp installation.

Software Requirements

This section contains software requirements for the OnApp installation.

The requirements for OnApp Control Panel, Static Compute resources and Static Backup Servers based on RHEL or CentOS are:

• Install CentOS from the minimal CentOS ISO for Control Panel servers, static backup servers and static compute resources.
• The minimum running services list on the box:

```
  network 0:off 1:off 2:on 3:on 4:on 5:on 6:off
  sshd 0:off 1:off 2:on 3:on 4:on 5:off 6:off
```
• The network on the box, should be configured with an ability to access rpm.repo.onapp.com and templates.repo.onapp.com

• The open ssh server should be configured with an ability for user(s) to access and log into the box.

• The root user should be available on the box and configured as root account: root user: superuser with an access to all files, commands/tools and services on system. Installers should be run from under the root.

• The curl, rpm, yum and grub packages must be installed on the system. The grub is a mandatory boot loader for Static Compute resources only.

• Avoid using additional (not native) repositories for RHEL/CentOS like “Extra Packages for Enterprise Linux” (epel) and others.

Recommended Network Configurations
This section lists the recommended network configurations for an OnApp Cloud installation.

- For Xen/KVM Cloud
- For Xen/KVM Cloud Using OnApp Storage (Integrated Distributed SAN)
- For Baremetal Server Cloud
- For Smart Server Cloud
- For Mixed Smart/Baremetal Server Cloud

For Xen/KVM Cloud
Provisioning network is not required for clouds using Integrated Storage with dedicated backup servers.

If you are experiencing MAC address flapping across ports because the switch does not support the balance-rr mode, set up
Baremetal Server Cloud
Mixed Smart/Baremetal Server Cloud
Recommended Network Configurations for High Availability CP

When planning your network configuration for high availability cluster, make sure to consider the following aspects:

- add the control panel servers which will serve as the nodes to the cluster
- add the data server that includes the database, Redis or stock RabbitMQ (this can be one or separate servers)
- join the Control Panel servers to management and provisioning networks

This section lists the recommended network configurations for High Availability CP.
Redundant CP/Non redundant Database&Transactions server
Redundant CP/Redundant Database & Transactions server
Suggested Specifications for OnApp

There are many factors that determine how many virtual servers you can run. Below you can find specifications for a small starter cloud and a more advanced cloud for three different deployment scenarios - using a centralized SAN, using OnApp's integrated SAN, and using simple local storage in compute resources.

On this page:

- Centralized SAN
- Centralized SAN with High Availability Control Panel
- Integrated SAN (OnApp Storage)
- Local storage

Need more help?

With the full version of OnApp Cloud you get free support from our integrations team to spec the exact hardware you'll need for your cloud deployment.

See also:

- Server Config Reminder - supported versions of the servers
- Hardware Requirements for High Availability CP
- Hardware Requirements
- Software Requirements
- Recommended Network Configurations
- Recommended Network Configurations for High Availability CP
- Types of Cloud Service with OnApp

Centralized SAN

<table>
<thead>
<tr>
<th></th>
<th>'Starter' cloud</th>
<th>'Advanced' cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Control Panel</strong></td>
<td>2 x Intel Xeon CPUs</td>
<td>2 x Intel Xeon CPUs</td>
</tr>
<tr>
<td></td>
<td>8GB DDR3 1333/1066/800MHz ECC Registered DIMM</td>
<td>24GB DDR3 1333/1066/800MHz ECC Registered DIMM</td>
</tr>
<tr>
<td></td>
<td>2 x Intel Dual-Port Gigabit Ethernet Controllers</td>
<td>2 x Intel Dual-Port Gigabit Ethernet Controllers</td>
</tr>
<tr>
<td></td>
<td>6Gbps hardware SAS Controller</td>
<td>6Gbps hardware SAS Controller</td>
</tr>
<tr>
<td></td>
<td>4 x 80GB SAS (RAID10)</td>
<td>4 x 80GB SAS (RAID10)</td>
</tr>
</tbody>
</table>
### Compute resources

**Minimum of 3, plus 1 spare for failover:**
- 2 x Intel Xeon Quad Core E5620 CPUs
- 64GB DDR3 1333/1066/800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controller
- 2 x 60GB SATA RAID1

**Minimum of 5, plus 1 spare for failover:**
- 2 x Intel Xeon Quad Core E5620 CPUs
- 64GB DDR3 1333/1066/800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- 1 x Intel Dual-Port 10 Gigabit Ethernet Controller
- 2 x 60GB SATA RAID1

### Backup server 1
- 2 x Intel Xeon CPUs
- 12GB DDR3 1333/1066/800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- 6Gb hardware SAS Controller
- 12 x 2TB SAS RAID5

### Backup server 2
- 2 x Intel Xeon CPUs
- 12GB DDR3 1333/1066/800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- 1 x Intel Dual-Port 10 Gigabit Ethernet Controller
- 6Gb Hardware SAS Controller
- 12 x 2TB SAS RAID5

### Primary storage array
- iSCSI hardware storage array
- 12 x 500GB SAS RAID10

### VS rating
- 'Starter' cloud: 192
- 'Advanced' cloud: 320

### Centralized SAN with High Availability Control Panel

<table>
<thead>
<tr>
<th>'Starter' cloud</th>
<th>'Advanced' cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Control Panel</strong></td>
<td><strong>Redundant Control Panel</strong></td>
</tr>
<tr>
<td>2 x Intel Xeon CPUs</td>
<td>2 x Intel Xeon CPUs</td>
</tr>
<tr>
<td>8GB DDR3 1333/1066/800MHz ECC Registered DIMM</td>
<td>24GB DDR3 1333/1066/800MHz ECC Registered DIMM</td>
</tr>
<tr>
<td>2 x Intel Dual-Port Gigabit Ethernet Controllers</td>
<td>2 x Intel Dual-Port Gigabit Ethernet Controllers</td>
</tr>
<tr>
<td>6Gbps hardware SAS Controller</td>
<td>6Gbps hardware SAS Controller</td>
</tr>
<tr>
<td>4 x 80GB SAS (RAID10)</td>
<td>4 x 80GB SAS (RAID10)</td>
</tr>
</tbody>
</table>
### Database & Transactions Server

- **2 x Intel Xeon CPUs**
- **8GB DDR3 1333/1066/800MHz ECC Registered DIMM**
- **2 x Intel Dual-Port Gigabit Ethernet Controllers**
- **6Gbps hardware SAS Controller**
- **4 x 80GB SAS (RAID10)**

### Compute Resources

- **Minimum of 3, plus 1 spare for failover:**
  - **2 x Intel Xeon Quad Core E5620 CPUs**
  - **64GB DDR3 1333/1066/800MHz ECC Registered DIMM**
  - **2 x Intel Dual-Port Gigabit Ethernet Controllers**
  - **6Gb hardware SAS Controller**
  - **12 x 2TB SAS RAID5**

- **Minimum of 5, plus 1 spare for failover:**
  - **2 x Intel Xeon Quad Core E5620 CPUs**
  - **64GB DDR3 1333/1066/800MHz ECC Registered DIMM**
  - **2 x Intel Dual-Port Gigabit Ethernet Controllers**
  - **1 x Intel Dual-Port 10 Gigabit Ethernet Controller**
  - **2 x 60GB SATA RAID1**

### Backup Server 1

- **2 x Intel Xeon CPUs**
- **12GB DDR3 1333/1066/800MHz ECC Registered DIMM**
- **2 x Intel Dual-Port Gigabit Ethernet Controllers**
- **6Gb hardware SAS Controller**
- **12 x 2TB SAS RAID5**

### Backup Server 2

- **2 x Intel Xeon CPUs**
- **12GB DDR3 1333/1066/800MHz ECC Registered DIMM**
- **2 x Intel Dual-Port Gigabit Ethernet Controllers**
- **1 x Intel Dual-Port 10 Gigabit Ethernet Controller**
- **6Gb Hardware SAS Controller**
- **12 x 2TB SAS RAID5**

### Primary Storage Array

- **iSCSI hardware storage array**
- **12 x 500GB SAS RAID10**

### VS Rating

<table>
<thead>
<tr>
<th></th>
<th>'Starter' cloud</th>
<th>'Advanced' cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192</td>
<td>320</td>
</tr>
</tbody>
</table>

### Integrated SAN (OnApp Storage)
### Control Panel
- 2 x Intel Xeon Processor
- 8GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- 6Gbps hardware SAS Controller
- 4 x 80GB SAS (RAID10)

### Compute resources
Minimum of 3, plus 1 spare for failover:
- 2 x Intel Xeon Quad Core E5620
- 64GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- 2 x 60GB SATA RAID1 (OnApp installation)
- 8 x 250GB SAS RAID10 (local primary storage)

Minimum of 5, plus 1 spare for failover:
- 2 x Intel Xeon Quad Core E5620
- 64GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- 1 x Intel Dual-Port 10 Gigabit Ethernet Controller
- 2 x 60GB SATA RAID1 (OnApp installation)
- 8 x 250GB SAS RAID10 (local primary storage volume)

### Backup server 1
- 2 x Intel Xeon CPUs
- 12GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- Hardware 6Gb SAS Controller
- 12 x 2TB SAS RAID5

### Backup server 2
- 2 x Intel Xeon CPUs
- 12GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- 1 x Intel Dual-Port 10 Gigabit Ethernet Controller
- 6Gb hardware SAS Controller
- 12 x 2TB SAS RAID5

### VS rating
192

### Local storage

<table>
<thead>
<tr>
<th>'Starter' cloud</th>
<th>'Advanced' cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Panel</td>
<td></td>
</tr>
</tbody>
</table>
| 2 x Intel Xeon Processor
- 8GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- 6Gbps hardware SAS Controller
- 4 x 80GB SAS (RAID10) |
|                 | 2 x Intel Xeon Processor
- 24GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- 6Gbps hardware SAS Controller
- 4 x 80GB SAS (RAID10) |
## Compute resources

Minimum of 3, plus 1 spare for failover:
- 2 x Intel Xeon Quad Core E5620
- 64GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controller
- 2 x 60GB SATA RAID1 (OnApp installation)
- 8 x 250GB SAS RAID10 (local primary storage)

Minimum of 5, plus 1 spare for failover:
- 2 x Intel Xeon Quad Core E5620
- 64GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- or 1 x Intel Dual-Port 10 Gigabit Ethernet Controller
- 2 x 60GB SATA RAID1 (OnApp installation)
- 8 x 250GB SAS RAID10 (local primary storage volume)

## Backup server

1
- 2 x Intel Xeon CPUs
- 12GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- Hardware 6Gb SAS Controller
- 12 x 2TB SAS RAID5

2
- 2 x Intel Xeon CPUs
- 12GB DDR3 1333/ 1066/ 800MHz ECC Registered DIMM
- 2 x Intel Dual-Port Gigabit Ethernet Controllers
- or 1 x Intel Dual-Port 10 Gigabit Ethernet Controller
- 6Gb hardware SAS Controller
- 12 x 2TB SAS RAID5

## VS rating

192 320

- **NICs**: the starter specification assumes 1Gbit connectivity for storage/provisioning data. The advanced spec assumes 10Gbit. Infiniband and FiberChannel are suitable alternatives for 10Gbit, too, though connectivity on servers with access to the storage network would need to be amended with hardware HBAs.

- **Compute resources**: recommended minimum redundancy is 1 spare compute resource per 3-5 primary compute resources. N+1 redundancy would require 1 redundant compute resource server for each primary compute resource server.

- **VS rating**: estimated VS capacity is a guideline only, since VS load and requirements will vary enormously. We’ve assumed an average VS requirement of 1GB RAM, 10GB disk and 1/8 contention on the CPU cores.

---

### Server Config Reminder

OnApp Cloud runs on CentOS or (for the OnApp Control Panel server) Red Hat Enterprise Linux Server. Please note that the required RHEL/CentOS versions can vary, depending which virtualization method you choose, Xen or KVM.

CloudBoot is not compatible with CentOS 6 Xen compute resources and CentOS 5 KVM compute resources.

### Supported server configuration

- **XEN Compute resources** CentOS 5.x x64 or CentOS 6.x x64
- **KVM Compute resources** CentOS 5.x x64 or CentOS 6.x x64
- **OnApp Control Panel Server** CentOS 5.x x86/X64 or CentOS 6.x x86/64
- **OnApp Backup Server** CentOS 5.x x64 or CentOS 6.x x64
- **Integrated Storage** CentOS 5.x x64 or CentOS 6.x x64

**Recommended server configuration**

We highly recommend using the following server configuration:

- **XEN 4.0 Compute resources** CentOS 6.x x64,
- **KVM Compute resources** CentOS 6.x x64
- **OnApp Control Panel Server** CentOS 6.x x86/64
- **OnApp Backup Server** CentOS 6.x x64

---

**Types of Cloud Service with OnApp**

You can build many different kinds of cloud service with OnApp. Below you can find more details about such cloud types as public, private, hybrid or VPS cloud.

---

**Public cloud, by-the-hour**

You can use OnApp to set up a complete pay-as-you-go public cloud system and compete with companies like AWS

- Sell virtual servers to customers who pay for hourly for cloud resources
- Set different prices for RAM, CPU and storage
- Set up different availability zones with different pricing

---

**Virtual private clouds**

Use OnApp to offer virtual private cloud services and compete with companies like AWS. You can run private clouds alongside a public cloud service, too.

- Group compute resource, network and storage resources into a single private cloud
resource for a customer
• Your customer gets all the benefits of a private cloud, backed by the resources of the whole cloud
• This brings the cost of private clouds down for customers, too

Cloud VPS

Use OnApp to compete with services like VPS.NET, by creating a cloud hosting service with resources packaged as a pre-configured VPS

• Group cloud resources into packages that you can sell on a monthly/plan billing basis
• Your customers use packages as the building blocks for their VSs
• This approach makes it easy to transition traditional VPS customers to the cloud

Hybrid cloud hosting

This is where dedicated hosting meets the cloud. You can use OnApp to offer hybrid servers to customers, and compete with every dedicated server provider out there:

• Allocate compute resources on a 1:1 basis: each customer gets a dedicated compute resource for their hosted service
• Failover is provided by the rest of the cloud (for example, one compute resource might act as failover for 5 "live" compute resources)

Traditional VPS model

You can use OnApp to provide traditional VPS services too, based on local storage:

• OnApp doesn't demand that you have a SAN back-end
• This means, if you want to provide customers with traditional VPSs using local storage, OnApp can handle that too

The OnApp Federation

The OnApp Federation is a global network of clouds you can use to add scale and reach to your own cloud service. It gives you instant access to global compute cloud and content delivery infrastructure.

• Expand your cloud to 170+ locations, on demand
• Add global scale for compute and content delivery
• Host customers close to their users, to improve performance
• Host customers in specific locations (or outside specific locations) for compliance
• You can sell cloud infrastructure to the OnApp Federation, too. You set the wholesale price and get paid when other members of the Federation use your resources

OnApp 4.1 Preparation Guide

This document describes how to prepare the OnApp Cloud 4.1 version for the deployment. Please review the configuration details in each chapter carefully, as they are vital to the smooth operation of OnApp Cloud.

To prepare OnApp Cloud, you need to:
Configure Networks

The correct network configuration is important to ensure your cloud has optimal performance and stability. There are four core networks in a standard OnApp Cloud installation: storage, management, provisioning and appliance.

It is very important to separate these four core networks, either physically, using different switches, or with VLANs if your network supports it. The role of each network is explained below.

Please also refer to Recommended Network Configurations section for details on configs.

On this page:

- Appliance Network/VS Networking
- Management Network
- Provisioning Network
- Storage Network

Appliance Network/VS Networking

The appliance Network in OnApp is used for VS networking only: it provides network connectivity for virtual servers.

OnApp will bridge the public NIC and assign virtual interfaces to it, when VSs are provisioned, and/or when additional network interfaces are added to VSs from the Web UI, or via the OnApp API. As the public interface is managed fully by OnApp, the public NIC requires a blank config - for example:

```
/etc/sysconfig/network-scripts/ifcfg-ethX
ONBOOT=no
BOOTPROTO=none
```
You should configure your network interface file accordingly. You will not need to add any configuration to this NIC, so no subnet, gateway or IP address details should be added. The NIC could either be a standard physical interface (e.g. eth1) or a bonded interface (e.g. bond1). It cannot be a sub-interface (e.g. eth1:1) or a vlan sub-interface (e.g. eth1.101) so you should allow for this when you are designing your compute resource, as you must make sure you have a physical NIC available. This network should be a minimum of 1Gbit. You should also consider bonding on the appliance network to introduce redundancy at the network level.

Configuring a switch trunk port is the preferred method, because it gives you additional flexibility and security. Alternatively, you can configure a switch access port. If this is the case, you will not need to specify a VLAN when adding the range to OnApp.

You'll need to connect your appliance Network to a switch trunk port, if you want to use VLANs. VLANs allow a network administrator to segregate traffic for bandwidth or security purposes.

If you choose to VLAN your VS networking, you'll need to associate your VLAN with the subnet when you add the VS networking range to OnApp.

Some hosting companies have limitations and the transfer of IP addresses between servers can sometimes require manual interventions - a change on their user portal, for example - so if you are leasing hosting server solutions, it is worth double-checking with your host that this will be possible.

Management Network

**OnApp standard deployment (XEN/KVM) requirements**

This network is responsible for a couple of different tasks. It provides incoming and outgoing connectivity to the servers, which means the management network should always be the default gateway.

If you are going to use Cloud Boot, this should be a local network behind a gateway device, that is capable of bridging traffic to the Internet to allow the servers to perform tasks such as dns resolution, ntp updates and operating system updates. Also, you have to open the 5555 port for outgoing connections to the licensing server.

The control panel will need to have incoming traffic allowed to ports 80/443 & 30000->40000. This should again be configured at the gateway with incoming NAT. If your gateway device is not capable of supporting this, this network can also be an external network, but should always be firewallled at the gateway to block all incoming traffic, with the exception of the ports listed above.

The management network also serves as a route for communication between the control panel server and the compute resources for critical OnApp internal traffic. That means, the stability of this network is critical: you should always consider bonding to introduce network level redundancy, and the network should run at least 1Gbit.

If your management network is behind a firewall, please make sure that ports 22/80/5555/30000-40000 are open to the world for the Control Panel server, and port 22 for all other servers. The 22/80/5555/30000-40000 ports are not required if you are going to use HTML5 console, as it proxies over port 80 or 443.

**OnApp and vCloud Director integration requirements**

OnApp and vCloud connection is supported with RabbitMQ. OnApp CP connects to vCloud Director using REST API and requires outgoing connection to vCloud API interface via ports 80,443.

If RabbitMQ server, installed by OnApp by default, is used, incoming connection to port 5672 is required in management network. Also port 15672 is optional for RabbitMQ server management.

If external AMQP server is used, outgoing connection to RabbitMQ default port 5672 is required.

Provisioning Network

The provisioning network is used to transfer backup and template data between the provisioning server and the primary storage volumes.

The network will be used to transfer large amount of data, so we recommend that it runs at least 1Gbit. Ideally, you should consider 10Gbit, FibreChannel, InfiniBand or aggregated 1Gbit links for maximum throughput.

Provisioning network is not required for clouds using Integrated Storage with dedicated backup servers.

Storage Network

The storage network provides the connection between storage devices (e.g. SANs) and the compute resources. The type of network will depend on what kind of connectivity your primary storage requires. For example, if you are using iSCSI or ATAoE, you will need to set up an ethernet network. If your SAN has fibre connectivity, then the storage network will be a fiber network.
The stability of the storage network is absolutely critical. You should always make redundancy your primary concern when designing this network. The Centralized Storage (SAN) section of this document discusses this in more detail.

- The storage network must be a local network.
- We recommend this network runs at 10 Gbit, at least; FibreChannel or InfiniBand to achieve maximum performance.
- We strongly recommend that you avoid NICs using Broadcom chipsets on the Storage Network due to known issues surrounding iSCSI and TCP offload in the Linux kernel modules.
- To achieve better performance and redundancy over 1Gbit you should consider NIC teaming/bonding and LACP or MPIO over multiple subnets.
- If your primary storage network is running over Ethernet, then it is important that the switch connecting the compute resources to the SAN supports jumbo frames: the storage network on the compute resources and the SAN(s) must have MTU set to 9000 to optimize performance.

Emulex hardware currently does not have support for 3.x Linux kernels, so is only compatible with CentOS 5.x

Now proceed to configuring storage.

Centralized Storage (SAN)

Primary storage is critical to your cloud, and your SAN will have a huge impact on the performance of the whole platform.

OnApp gives you a lot of flexibility in your primary storage technology. It supports anything that is capable of presenting a block device to compute resources. This could be, for example, FiberChannel, SCSI or SAS HBA, iSCSI or ATAloE, or a InfiniBand HCA controller, since all of these present the block device directly. OnApp does not support services such as NFS for primary storage, because these present a filesystem and not the block device.

Beyond the type of block device, there are three main things to consider in your SAN design: the host, fabric and storage components. You need to think about each very carefully and pay particular attention to performance, stability and throughput when planning your SAN.

Fabric Components - the Network Fabric Between Compute Resources and SANs

You will need to think about redundancy, and whether you need to design a fault tolerant switching mesh to coincide with your multipath configurations at the host and SAN ends.

You should also think about future growth: as you add more compute resources and SANs to the cloud you will need to be able to grow the physical connectivity without downtime on the Storage Network.
Host Components - Compute Resource Connectivity to the Storage Network

You will need to make sure that your ethernet or HBA drivers are stable in this release. We recommend that you test this thoroughly before handing over to OnApp to deploy your cloud on your infrastructure.

You will also need to think about the throughput, and whether the connectivity on compute resources will be suitable for the virtual servers they'll be running. A bottleneck here will cause major performance issues.

Consider adding multiple HBAs or NICs if you plan to run a redundant switching mesh (see the fabric section below) as bonding or multipath will be required, unless the redundancy is built into the physical switch chassis (failover backplanes for example).

Storage Components - SAN Chassis, Controllers and Disk Trays

You need to take into consideration the size of storage required and the physical capacity you have to achieve this. This will give you a good idea on the size of disks you will be adding into the array and the RAID level you will choose.

As a general rule, more spindles in the array will give you better performance; you should avoid using a small number of large disks, or you will start to see I/O bottlenecks as you make increasing use of the storage in future.

You should also think about the physical storage hardware, and whether you'll be using SATA, SAS or SSD. Again, this will have a great impact on the I/O capabilities of the array.

It's also a good idea to consider RAID levels carefully and look into the advantages and disadvantages of each. We recommend RAID10.

Although you will lose 50% of your capacity you will see good performance for both read and write, which is important for primary storage. RAID10 will also give you much better redundancy on the array.

Controller caching is another issue to consider. You should always aim to have both read and write caching. If you are looking at write caching you should also look at battery backups for the write cache. Some controllers also support SSD caching which can be a great advantage.

As with the host components, you should also take your HBA and Ethernet connectivity into consideration, to ensure you have both the redundancy and throughput required for your cloud infrastructure.

Integrated Storage (OnApp Storage)

OnApp Storage is a distributed block storage system that allows you to build a highly scalable and resilient SAN using local disks in compute resources. With OnApp Storage you create a virtual data store that spans multiple physical drives in compute resources, with RAID-like replication and striping across drives. The SAN is fully integrated into the compute resource platform, and the platform is completely decentralized. There is no single point of failure: for example, if a compute resource fails, the SAN reorganizes itself and automatically recovers the data.

The following requirements are recommended for integrated storage implementation:

- Any number of integrated storage drives can be grouped together across any compute resource
- SSD drives are recommended for best performance
- At least 1 dedicated NIC assigned per compute resource for the SAN
- Multiple NICs bonded or 10Gbit/s Ethernet (recommended)

To start using integrated storage, you must enable it in the system configuration first (Settings > Configuration > System Configuration > OnApp Storage).

The Bonded NICs for the management/boot interface are not yet available (they will be introduced in future releases)

SolidFire Integration

Starting with the 3.0 version, OnApp is integrated with the SolidFire storage management system. With the Solid Fire integration it is possible to utilize the SF SAN directly within the OnApp cloud and manage the SolidFire cluster via the SolidFire API. To be able to utilize SolidFire in the cloud, you need to install the SolidFire storage system first.

You can perform the following options with SolidFire:

- Utilize SolidFire SAN in the OnApp cloud.
- Allocate dedicated LUNs from the SF cluster per virtual server disk, when creating a VS. (LUN is created per each VS disk, with a separate lun per swap disk.)
- Manage SolidFire LUNs automatically via API.
• Create virtual servers without the swap disk.
• Implement backups / snapshots using SF CloneVolume method

There is a disk dependency between OnApp and SolidFire - when a new disk is created on the OnApp side, a new LUN is created automatically on the SF side, using the CreateVolume API call. The LUNs on the SolidFire are managed automatically via SolidFire API.

Inasmuch SolidFire data store has two interfaces: OnApp and SolidFire, you have to specify two IP addresses when creating a SolidFire Data Store.

To be able to use the SF volume, you have to enable export to this device (compute resource or a data store). To do that, you need to send an account username and initiator password to the iscsi_ip address. You will be able to use this device after the authorization.

The following options are not available under SolidFire:
• It is not possible to migrate SolidFire disks, as SF virtualizes the storage layer.
• SolidFire does not support live disk resize. To resize disk, you need to shut down the virtual server first and use the CloneVolume functionality to increase the disk size. After the disk resize operation is complete, the original volume will be replaced with the new one and deleted, after that the VS will be booted.

Now proceed to configuring servers.

---

**Configure Servers**

---

Once you have configured networks and storage, proceed to setting up the Control Panel, Backup, and Compute resource servers.

---

**Server Installation Requirements**

This section lists the server installation requirements needed for an OnApp Cloud installation. For minimum hardware specs, see Technical Details. OnApp primarily runs on CentOS or Red Hat, but the version depends on what virtualization method you are running.

• We recommend installing CentOS from the minimal CentOS ISO for Control Panel servers, static backup servers and static compute resources.
• CloudBoot is not compatible with CentOS 6 Xen compute resources and CentOS 5 KVM compute resources.
• Full root access: please do not create the user ‘onapp’ since this is created as part of the RPM installation.
• Currently Emulex hardware does not support 3.x Linux kernels, so it is only compatible with CentOS 5.x.

We strongly recommend that you avoid creating mixed compute zones:
• do not add CloudBoot and static boot compute resources to one compute zone

---

See also:
• Configure Networks
• Configure Storage
• OnApp Cloud v.4.1 Installation Guide
• OnApp v.4.0 to v.4.1 Upgrade Guide
• Technical Details
Supported server configuration

- **XEN Compute resources** CentOS 5.x x64 or CentOS 6.x x64
- **KVM Compute resources** CentOS 5.x x64 or CentOS 6.x x64
- **OnApp Control Panel Server** CentOS 5.x x86/64 or CentOS 6.x x64
- **OnApp Backup Server** CentOS 5.x x64 or CentOS 6.x x64
- **Integrated Storage** CentOS 5.x x64 or CentOS 6.x x64

Recommended server configuration

We highly recommend using the following server configuration:

- **XEN 4.0 Compute resources** CentOS 6.x x64,
- **KVM Compute resources** CentOS 6.x x64
- **OnApp Control Panel Server** CentOS 6.x x86/64
- **OnApp Backup Server** CentOS 6.x x64

Control Panel Server

The Control Panel server is absolutely critical to the stability and performance of the cloud.

There are a few things to consider when choosing hardware for this server. It is very simple to grow your cloud, as you start to sell more resources, and as you add more compute resources and SANs this puts more load on the control panel. Choosing the right hardware at the beginning is important and avoids having to take the server down for upgrades later down the line, causing interruption to customers.

The control panel server will become very MySQL heavy as you add more compute resources, so a fast disk array and lots of memory is recommended. A good example would be a 4xSAS RAID10 array with 24GB RAM and quad core Xeon CPU. SSD storage can also be considered.

If you have a Control Panel server spec in mind, you're very welcome to send it to your OnApp integrations specialist for review.

Backup Server

The backup server stores virtual server backups and templates. It is also responsible for processing any disk transactions running in your cloud, such as provisioning virtual servers, taking backups or resizing disks.

The backup server must hold a backup storage volume. This can be a local disk array or can be mounted via NFS or iSCSI from a back end storage node. Note, that the backup volume should not be presented from the same physical hardware that presents the primary storage volume to the compute resources.

Unlike primary storage, performance is not so essential here – there is less need for RAID10 or a high volume of spindles. You can consider a RAID level that provides more space as opposed to redundancy and performance: RAID5 or 6 is usually ideal for the backup volume. Take care when configuring the SAN, however: a larger block size is recommended owing to the nature of the data being stored on this array.

Backup storage will be used to hold very large files, so we recommend that it's at least 1.5 - 2x larger than the primary storage volume(s) available in the cloud. Additional backup servers can be added to your cloud as needed.

In the traditional/centralized SAN configuration, you have to bind all your data stores to the backup server. Volume groups of each data store based on SAN must be shared with the backup server.

In the OnApp cloud with CloudBoot enabled, you have to use CloudBoot backup servers instead of dedicated backup servers. To do so, you have to create a CloudBoot compute resource to be used as a backup server.

You can set up CloudBoot backup servers and virtual dedicated backup servers to be used with the Integrated Storage functionality. The backup scheme remains unchanged.

Compute Resource Servers

- do not add both XEN and KVM compute resources to one zone

The reason is that XEN VSs cannot migrate/failover to a KVM compute resource and KVM VSs cannot migrate/failover to a XEN compute resource.
Compute resources are where virtual servers live in your cloud. A small amount of compute resource CPU, memory and disk resource is reserved for the OnApp engine: the remainder is available as virtual resources to allocate to virtual servers.

If you are using a centralized SAN, then the virtual servers’ disks will live on that SAN, and, the compute resource’s own disk will simply be used to boot the compute resource and run the OnApp engine. Performance here is not critical, but we recommend introducing some redundancy: RAID1 SATA/SAS would be perfect.

If you are using OnApp Storage (our integrated SAN), you should obviously factor more disks into your compute resource spec to enable the creation of a distributed SAN using those disks.

If you choose not to run a centralized SAN or OnApp Storage, it is possible to have storage running locally on compute resources, though you lose the ability to failover from compute resource to compute resource: this is not recommended for an optimal cloud set-up.

When you are building your hardware it's important to take into consideration the specifications of the primary components that will be virtualized - the RAM and CPU.

Remember, that while you can oversell CPU cores in OnApp, RAM is a dedicated resource, so the physical limitation to how many virtual servers you can fit on a single compute resource is limited by the amount of RAM installed in that compute resource.

Another limitation to consider is that the compute resource’s CPU is a shared resource: the physical cores are shared among the VVs running on a compute resource. Do not overload the compute resource with too many virtual servers, as this will stretch the available CPU time and degrade the performance of all servers on that compute resource.

It's also important to note, that too many virtual servers could potentially saturate the SAN NICs on the compute resource, which will also introduce instability and performance loss to virtual servers (see the Host Components - Compute Resource Connectivity to the Storage Network section for more details).

In the Recommended Network Configurations chapter, you can see that OnApp requires at least 4 NICs on the compute resources. Note, that this does not take into consideration any bonding or multipath configurations, which we recommend for any production setup on most if not all of our networks. You should at least consider bonding on the management network and multipath on the storage network(s) to improve stability and performance.

You must have Intel-VT or AMD-V enabled in the BIOS of all compute resources to enable you to provision Windows-based virtual servers on your OnApp cloud!

CloudBoot Compute Resource Servers

CloudBoot is a feature that enables fast provisioning of Xen and KVM compute resources without any pre-installation requirements. Using network/PXE boot methods, a new server can be plugged in and powered on, being automatically discovered by the OnApp Control Panel Server, and installed over the network so it boots as a fully configured compute resource, ready to host virtual servers.

The Control Panel Server manages IP address to hardware MAC assignment, and the booting of a Xen or KVM image on demand. Compute resource images come pre-installed, with all the SSH keys and any other settings specific to the node, to enable compute resources to come online instantly. Images are booted as a standalone RAM disk, so once bootstrapped, they operate independently from other servers, but without any persistent installation dependency.

This enables booting of diskless blades, as well as booting compute resources with the new integrated storage platform enabled (OnApp Storage) where all local storage drives are presented to the integrated SAN.

Dependencies:

- Network/PXE boot must be supported and enabled on the primary management NIC for the compute resource servers
- A secondary NIC is recommended for the Control Panel Server to provide a fully isolated network for the compute resource management subnet, including PXE boot and DHCP support for the compute resources.

For resilience, a secondary static tftp server target can be configured to handle Control Panel server failure and ensure hardware boot consistency in the event of such a failure.

OnApp Installation Walk-through

Generally, the OnApp installation includes the following steps:

1. Prepare Servers Configuration

Before installing OnApp, it is required to make sure your network, storage, and servers...
configuration meets the requirements.

See also:
OnApp Cloud v.4.1 Installation Guide
OnApp 4.1 Preparation Guide

2. Install Control Panel Server

The Control Panel server hosts the OnApp user interface and manages all the processes controlled by OnApp. The Control Panel server is installed from the ready-made installer package provided by OnApp.

3. Install Compute Resources

Compute resources provide system resources such as CPU, memory, and network, and control secure virtualization. After the Control Panel server installation, proceed to the compute resource installation. Depending on the desired cloud configuration, you can opt for Static compute resources or CloudBoot servers.

4. Install Data Stores

Make sure to install the appropriate storage for templates, backups, ISOs, and virtual server disks. You can set up a separate server with NFS or SSH connection, use any block-based storage, or set up an OnApp Integrated storage.

5. Install Backup Server

Backup servers are servers responsible for storing backups and templates of virtual servers running in the cloud, in order to prevent data loss in the event of failure. You can install static or CloudBoot backup server.

6. Download and Configure Templates on Control Panel Server

If you are not using a dedicated backup server for storing templates, it is required to download the templates to the backup&templates server.

7. Configure Cloud

After you have set up the servers, log in to OnApp CP and configure the relations between the entities.

OnApp Cloud v.4.1 Installation Guide

This document describes how to install the 4.1 version of the OnApp Cloud. Please read each section carefully, as it is vital to the smooth operation of OnApp Cloud.

Preparation

1. Read the Technical Details
2. Read the Preparation Guide

Installation

1. Install Control Panel server
2. Install compute resources
3. Install data stores
4. Install backup server
5. Download and configure templates on template server.

Post install configuration
Configure Cloud

Please do not change the default language settings during the installation process (en_US.UTF-8)!

Install Control Panel Server

This section is the part of the OnApp installation procedure.

Install Control Panel Server  >  Install Compute Resources  >  Install Data Stores  >  Install Backup Server  >  Download and Configure Templates on Control Panel Server  >  Configure Cloud

- Review the Preparation Guide to ensure that you have a suitable environment before starting the installation.
- Use corresponding option of the Control Panel installer in case MySQL is already installed and configured.
- Installer output is redirected to /onapp-cp-install.log
- All installer critical errors are in /var/log/messages
- If you consider deploying High Availability Clusters, refer to OnApp Cloud Installation Guide for High Availability Clusters.
- If you're replacing an existing Control Panel with a new install, refer to Control Panel Migration Guide for instructions.

To install Control Panel server, perform the following procedure:

1. Update your server:

   bash# yum update

2. Download OnApp YUM repository file:

   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo.noarch.rpm

3. Install OnApp Control Panel installer package:

   bash#> yum install onapp-cp-install

4. Set the custom Control Panel configuration. It is important to set the custom values before the installer script runs.

   Edit the /onapp/onapp-cp.conf file to set Control Panel custom values

   # Template server URL

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

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

See also:

Technical Details
OnApp 4.1 Preparation Guide
OnApp Cloud Installation Guide for High Availability Clusters
vCloud Setup and Upgrade - OnApp and vCloud Director Configuration Guide
SNMP_TRAP_IPS=

# OnApp Control Panel custom version

ONAPP_VERSION=

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

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

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

MYSQL_WAIT_TIMEOUT=604800
MYSQL_MAX_CONNECTIONS=500
MYSQL_PORT=3306

# Use MariaDB instead of MySQL as OnApp database server

WITH_MARIADB=0

# Configure the database server relative amount of available RAM

TUNE_DB_SERVER=0

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

RUBY_GC_MALLOC_LIMIT=16000000

# sysctl.conf net.core.somaxconn value

NET_CORE_SOMAXCONN=2048

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

# Remote server's (to store database dumps) IP, user, path, openssh connection options ans number of dumps to keep
DB_DUMP_SERVER=
DB_DUMP_USER=root
DB_DUMP_SERVER_ROOT=/onapp/backups
DB_DUMP_SERVER_SSH_OPT="-o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null
PasswordAuthentication=no"
KEEP_DUMPS=168
DB_DUMP_CRON='40 * * * *'

# Enable monit - tool for managing and monitoring Unix systems
ENABLE_MONIT=1

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

# Rotate transactions' log files created more then TRANS_LOGS_ROTATE_TIME day(s) ago
TRANS_LOGS_ROTATE_TIME=30

# Maximum allowed for uploading file size in bytes, from 0 (meaning unlimited) to 2147483647 (2GB). Default is 1GB
MAX_UPLOAD_SIZE=1073741824

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

# OnApp Control Panel SSL certificates (please do not change if you aren't familiar with SSL certificates)
# * The data below to generate self-signed PEM-encoded X.509 certificate
SSL_CERT_COUNTRY_NAME=UK
SSL_CERT_ORGANIZATION_NAME='OnApp Limited'
SSL_CERT_ORGANIZATION_ALUNITNAME='OnApp Cloud'
SSL_CERT_COMMON_NAME=`hostname --fqdn 2>/dev/null`

# SSLCertificateFile, SSLCertificateKeyFile Apache directives' values
# ssl_certificate, ssl_certificate_key Nginx directives' values
SSLCERTIFICATEFILE=/etc/pki/tls/certs/ca.crt
SSLCERTIFICATECSRFILE=/etc/pki/tls/private/ca.csr
SSLCERTIFICATEKEYFILE=/etc/pki/tls/private/ca.key

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

# SSLCipherSuite, SSLProtocol Apache directives' values
# ssl_ciphers, ssl_protocols Nginx directives' values
SSLCIPHERSUITE=
SSLPROTOCOL=

bash# vi /onapp/onapp-cp.conf

5. Run the Control Panel installer:

bash#> /onapp/onapp-cp-install/onapp-cp-install.sh -i SNMP_TRAP_IPS

* The full list of Control Panel installer options:
Usage:

```
```

Where:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MYSQL_*</td>
<td>Options are useful if MySQL is already installed and configured.</td>
</tr>
<tr>
<td>-m MYSQL_HOST</td>
<td>MySQL host</td>
</tr>
<tr>
<td>-p MYSQL_PASSWD</td>
<td>MySQL password</td>
</tr>
<tr>
<td>-d MYSQL_DB</td>
<td>OnApp MySQL database name</td>
</tr>
<tr>
<td>-u MYSQL_USER</td>
<td>MySQL user</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REDIS_*</td>
<td>Options are useful if Redis Server is already installed and configured.</td>
</tr>
<tr>
<td>--redis-host=</td>
<td>IP address/FQDN where Redis Server runs. The Redis Server will be installed</td>
</tr>
<tr>
<td>REDIS_HOST</td>
<td>and configured on the current box if localhost/127.0.0.1 or box's public IP</td>
</tr>
<tr>
<td></td>
<td>address (listed in SNMP_TRAP_IPS) is specified. If local Redis, it will</td>
</tr>
<tr>
<td></td>
<td>serve as well on the unix socket '/tmp/redis.sock'. Default value is 127.0.0.1.</td>
</tr>
<tr>
<td>--redis-port=</td>
<td>Redis Server listen port. Defaults are:</td>
</tr>
<tr>
<td>REDIS_PORT</td>
<td>0 - if local server</td>
</tr>
<tr>
<td></td>
<td>6379 - if remote server</td>
</tr>
<tr>
<td>--redis-passwd</td>
<td>Redis Server password to authentificate. Random password is generated if</td>
</tr>
<tr>
<td>[=REDIS_PASSWD]</td>
<td>the option's argument isn't specified. By default no password is used for</td>
</tr>
<tr>
<td></td>
<td>local Redis.</td>
</tr>
<tr>
<td>--redis-sock=</td>
<td>Path to the Redis Server's socket. Used if local server only. Default is</td>
</tr>
<tr>
<td>REDIS_PATH</td>
<td>/tmp/redis.sock</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN_*</td>
<td>Options are used to configure OnApp Control Panel administrator data.</td>
</tr>
<tr>
<td></td>
<td>Please note, that these options are for NEW INSTALL only and not for upgrade</td>
</tr>
<tr>
<td>-P ADMIN_PASSWD</td>
<td>CP administrator password</td>
</tr>
<tr>
<td>-F ADMIN_FIRSTNAME</td>
<td>CP administrator first name</td>
</tr>
<tr>
<td>-L ADMIN_LASTNAME</td>
<td>CP administrator last name</td>
</tr>
<tr>
<td>-E ADMIN_EMAIL</td>
<td>CP administrator e-mail</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--rbthost</td>
<td>IP address/FQDN where RabbitMQ Server runs. The RabbitMQ will be installed</td>
</tr>
<tr>
<td>RBT_HOST</td>
<td>and configured on the current box if localhost/127.0.0.1 or box's public IP</td>
</tr>
<tr>
<td></td>
<td>address (enlisted in SNMP_TRAP_IPS) Default values are 127.0.0.1.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VCD_*</td>
<td>Options are usefull if vCloud/RabbitMQ are already installed and configured.</td>
</tr>
<tr>
<td>--vcdlogin</td>
<td>RabbitMQ/vCloud user. Default value is ‘rbtvc’d.</td>
</tr>
<tr>
<td>--vcdpasswd</td>
<td>RabbitMQ/vCloud user password. The random password is generated if isn’t</td>
</tr>
<tr>
<td></td>
<td>specified.</td>
</tr>
<tr>
<td>--vcdvhost</td>
<td>RabbitMQ/vCloud vhost. Default value is ‘/’</td>
</tr>
<tr>
<td>RBT_*</td>
<td>Options are used to configure RabbitMQ manager account. If local RabbitMQ</td>
</tr>
<tr>
<td></td>
<td>server.</td>
</tr>
<tr>
<td>--rbtlogin</td>
<td>RabbitMQ manager login. The default value is ‘rbtmgr’.</td>
</tr>
<tr>
<td>--rbtpasswd</td>
<td>RabbitMQ manager password. The random password is generated if isn’t</td>
</tr>
<tr>
<td></td>
<td>specified.</td>
</tr>
<tr>
<td>-v ONAPP_VERSION</td>
<td>Install custom OnApp CP version</td>
</tr>
<tr>
<td>-i SNMP_TRAP_IPS</td>
<td>IP addresses separated with coma for snmp to trap</td>
</tr>
<tr>
<td>-c CONFIG_FILE</td>
<td>Custom installer configuration file. Otherwise, preinstalled one is used.</td>
</tr>
<tr>
<td>-y</td>
<td>update OS packages (except of OnApp provided) on the box with ‘yum update’.</td>
</tr>
<tr>
<td>-a</td>
<td>do not be interactive. Process with automatic installation.</td>
</tr>
<tr>
<td>-D</td>
<td>do not make database dump, and make sure it is disabled in the cron and not</td>
</tr>
<tr>
<td></td>
<td>running at the moment</td>
</tr>
<tr>
<td>-h</td>
<td>print this info</td>
</tr>
</tbody>
</table>

6. Install Cloudboot dependencies:

```bash
bash$> yum install onapp-store-install
bash$> /onapp/onapp-store-install/onapp-store-install.sh
```

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

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

8. Restart the OnApp service:

```bash
bash$> service onapp restart
```

9. After you have installed the Control Panel server, configure your Cloud Settings. See Configure Cloud for details.

This section is the part of the OnApp installation procedure.
Install Compute Resources

This section is the part of the OnApp installation procedure.

Install Control Panel Server > Install Compute Resources > Install Data Stores > Install Backup Server > Download and Configure Templates on Control Panel Server > Configure Cloud

Once the Control Panel server has been installed successfully, you can follow one of two processes to set up Xen or KVM compute resources:

- Install CloudBoot Compute Resources - the CloudBoot method where compute resources are installed over your network
- Install Static Compute Resources - standard static installation process to each compute resource's local disk

To deploy OnApp and vCloud integration, refer to vCloud Setup and Upgrade section of OnApp and vCloud Director Configuration Guide.

We strongly recommend that you avoid creating mixed compute zones:

- do not add CloudBoot and static boot compute resources to one compute zone
- do not add both XEN and KVM compute resources to one zone

The reason is that XEN VSs cannot migrate/failover to a KVM compute resource and KVM VSs cannot migrate/failover to a XEN compute resource.

Install CloudBoot Compute Resources

Follow this method to enable CloudBoot for your compute resources. CloudBoot compute resource installation enables dynamic boot of compute resource servers without any persistent installation requirements. The servers must support and have PXE boot enabled on the Network Interface Card (setup in the BIOS if not already enabled by default). See Configure CloudBoot Settings in BIOS for details. We strongly recommend you to deploy one or more backup servers for backups and VS provisioning when using CloudBoot functionality.

1. Enable CloudBoot in the Control Panel:
   a. Go to Settings > Configuration > System > CloudBoot
   b. Scroll down to the CloudBoot section and check the Enable box.

2. Enable Storage in the Control Panel:
   a. Go to Settings > Configuration > System > OnApp Storage
   b. Scroll down to the OnApp Storage section and check the Enable OnApp Storage box.
   c. Tick the Use Local Read Path check box to minimise the network throughput dependency for read heavy workloads.

3. Enter IP addresses for static content target and Control Panel server CloudBoot interface:

Static content, such as CloudBoot images, kernels, virtual server templates, can be hosted on a standalone NFS server if you wish. The default configuration is to install everything on the Control Panel server.
Enter the relevant IPs in Settings > Configuration > System > CloudBoot

4. Add IP address range for compute resources:
   Settings > Compute resources > CloudBootIPs > New IP Address

5. Power on servers and allow them to boot the default image.
   Add servers to the Control Panel by selecting MAC addresses and assigning IP address
   Settings > Compute resources > Add a new CloudBoot Compute resource
   If you want to expose drives in compute resources to OnApp Storage, our integrated storage platform, then you must select them at this point.
   For more information on setting up and configuring CloudBoot, see the CloudBoot Compute resources section of the Admin guide.
   To increase dom0 memory for all new Xen compute resources, edit the dom0 value in the /tftpboot/pxelinux.cfg/template-xen file on the CP server.
   To increase dom0 memory for a single Xen compute resource, edit the /tftpboot/pxelinux.cfg/xx-xx-xx-xx-xx-xx file, where you have to replace the x's with your compute resource's management NIC MAC address.

6. CloudBoot compute resources mount the following locations automatically at boot:
   • /tftpboot/export/centos5/xen to /.ro
     The path may vary depending on the compute resource template used.
   • /data to /onapp/tools/recovery
   • /tftpboot/images/centos5/ramdisk-xen to /cloudboot/centos5/ramdisk-xen
     The path may vary depending on the compute resource template.
   The NFS server from which these are mounted is defined by the Static Config target parameter (see Edit System Configuration section for details). You can set the default Control Panel server IP to any other server. This change will affect all CloudBoot compute resources.
   The following paths must be available in the static config target to make it possible to use CloudBoot:
   • /tftpboot/export
   • /data
   • /tftpboot/images
   Compute resources will use local templates (mounted from Static Config target) during the server provisioning if the Use SSH file transfer configuration setting is disabled or the template has null backup_server_id.

7. If you do not have a Dedicated Backup Server in place, please use Custom Config to mount /onapp/templates and /onapp/backups from your Control Panel server or another NFS export.

8. After you have installed CloudBoot compute resource proceed to the Configure CloudBoot Settings in BIOS section.

If you do not have a dedicated backup server you must mount your Template and Backup repository to the Compute resource for VS provisioning and backups to work, for example from your Control Panel server:

Add to /etc/exports on the Control Panel server:
/onapp/templates 192.168.10.0/24(rw,no_root_squash)
/onapp/backups 192.168.10.0/24(rw,no_root_squash)

Add to Custom Config on the Compute resource and run them manually on the command line (In this example we are mounting from 192.168.10.101):
```
mkdir -p /onapp/backups & & mount -t nfs 192.168.10.101:/onapp/backups /onapp/backups
mkdir -p /onapp/templates & & mount -t nfs 192.168.10.101:/onapp/templates /onapp/templates
```
To use PXE boot, you have to make sure it is enabled in BIOS. To do so:

1. Select the required ethernet card supporting PXE as a boot device:

2. After that, go to the **Advanced** settings > **PCI/PnP configuration**.

3. In the **Advanced** settings, select the first/primary Onboard LAN/NIC Option ROM and press **Enter**. Use up and down arrow keys to set Option ROM settings to enabled and press **Enter**. Press **Escape** key to return to the **Advanced** menu.

4. Set local disk as a second boot device.

Configure InfiniBand

Your BIOS settings may vary from the example provided in this section.

Your hardware must meet the following requirements for Ethernet mode utilization:
To set up a compute resource to operate in IB/Ethernet mode on the SAN network:

1. Add new compute resource based on boot MAC from UI, but do not configure storage yet.
2. Log in to the compute resource via SSH and run the following commands:

   ```bash
   HV# /sbin/connectx_port_config -n
   ``

   Choose Ethernet mode, and run:

   ```bash
   HV# mkdir -p /.rw/overlay/etc/infiniband
   HV# cp -a /etc/infiniband/connectx.conf /.rw/overlay/etc/infiniband
   HV# init 6
   ``

3. After the compute resource reboots, perform the CloudBoot compute resource setup, as described in Create CloudBoot Compute resource.
4. Run the following script on the Control Panel server:

   ```bash
   CP# cd /tftpboot/images/centos5/diskless/snapshot
   CP# cp -Rp default/overlay <MAC_OF_HV_MGT_NIC>/
   ``

5. Reboot the compute resource via UI.
6. After that, you will be able to select the InfiniBand interface as a storage NIC.
7. Then you can safely remove the `/tftpboot/images/centos5/diskless/snapshot/default/overlay` directory.

Current limitations:
- IB in Ethernet mode is only supported for Centos6/KVM nodes. It will not work with CentOS5 / Xen.
- InfiniBand is only supported for the SAN network, not PXE boot.

Install Static Compute Resources

**Before you proceed**

1. Install base CentOS packages on the local drive before compute resource installation, depending which virtualization method you choose:
   - Xen 3 compute resources: CentOS 5.x x64
   - Xen 4 compute resources: CentOS 6.x x64
   - KVM compute resources: CentOS 5.x x64 or CentOS 6.x x64

2. We recommend installing CentOS from the minimal CentOS ISO for static compute resources.
3. Disable CPU power-saving features in BIOS before you proceed to the compute resource installation.
4. If you are not using a dedicated backup server in your cloud setup, configure NFS server with the following options to preserve files owner and group settings during template unpacking on NFS storage:
   - no_root_squash
   - no_all_squash
5. Pay attention that smart and baremetal servers cannot be installed using the static compute resource installation method.

To install a compute resource:

1. Add the compute resource to your cloud using the OnApp Control Panel: Settings > Compute resources > Add New Compute
Make sure the compute resource is visible in the Control Panel, and at this point showing as inactive.

2. Update your server:

   bash# yum update

3. Download the OnApp repository:

   bash#> rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo.noarch.rpm

4. Install the OnApp compute resource installer package:

   bash#> yum install onapp-hv-install

5. Update OS components using the following command:

   For XEN

   bash# /onapp/onapp-hv-install/onapp-hv-xen-install.sh -y

   or

   For KVM

   bash# /onapp/onapp-hv-install/onapp-hv-kvm-install.sh -y

6. Edit custom compute resource configuration. Custom values must be set before the installer script runs.

   #vi /onapp/onapp-hv.conf

   The full list of OnApp compute resource custom values
   • OnApp HV tools custom version
     HV_VERSION=""
   • OnApp StorageAPI custom version
     API_VERSION=""
   • Default server to sync time on the HV
     NTP_TIME_SERVER='pool.ntp.org'

   If deploying XEN onto a server running CentOS 6, it is important to specify a number for XEN_DOM0_MAX_VCPUS. We recommend that this is set to 2 if the compute resource has 12 cores or less. Or 4 if the compute resource has more than 12 cores.
• Xen HV (Domain-0) related configuration

```
XEN_DOM0_MEM_MIN=409600
XEN_DOM0_MEM_DIVISOR=48
XEN_DOM0_MAX_VCPUS=
XEN_DOM0_VCPUS_PIN_ENABLE=0
XEN_DOM0_SCHEDULER_WEIGHT=65535
XEN_DOM0_SCHEDULER_CAP=200

4.2.x and higher versions only:
XEN_DOM0_SCHEDULER_RATELIMIT_US=100
XEN_DOM0_SCHEDULER_TIMESLICE_MS=5
```

• The number of loopback devices created

```
LOOPBACKS=128
```

• The maximum size of the connection tracking table.

```
The value can't be greater than 65536 if the total memory of Xen Domain-0 or KVM is less than 1Gb. The value could be doubled (or even more, depends on memory amount).

NET_IPV4_NETFILTER_IP_CONTRACK_MAX=
```

• The divisor to calculate the hash table. The recommended value is 8.

```
hashsize = nf_contrack_max / 8
CONTRACK_TO_HASHSIZE=8
```

• Outdated Xen HVs’ (Domain-0) configuration parameters

```
XEN_DOM0_MEM_OVERHEAD_MIN=262144
P_TO_VCPUS=4
```

7. Run the OnApp compute resource installer script:

- The full list of installer options

  **Usage:**

  ```
  ```

  **Where:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c CONFIG_FILE</td>
<td>custom installer configuration file. Otherwise, preinstalled one is used.</td>
</tr>
<tr>
<td>-a</td>
<td>do NOT be interactive. Process with automatic installation.</td>
</tr>
</tbody>
</table>
7. **HV VERSION**
   custom Compute resource Tools version

8. **API VERSION**
   custom StorageAPI version

- **y**
  update OS packages (except for OnApp provided) on the box with 'yum update'.

- **t**
  initiate Recovery templates and ISO(s), which are used to provision FreeBSD guests, download
  The download is initiated if `-a` option is used

- **s**
  skip packages management: install, remove, upgrade

- **h**
  print this info

**Run the OnApp compute resource installer script for Xen compute resources:**

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

**Run the OnApp compute resource installer script for KVM compute resources:**

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

8. **Configure the compute resource for your cloud. This step is also required for the SNMP statistics receiver configuration:**

```
```

**The full list of configuration options**

**Usage:**

```
```

**Where:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h CP_HOST_IP</td>
<td>FQDN or IP Address of the management server which should receive all status reports and is authoritative for this compute resource</td>
</tr>
<tr>
<td>-p HV_HOST_IP</td>
<td>FQDN or IP Address of Server (the Compute resource) which will serve all stats related and other requests send by the CP_HOST_IP. Used by snmpd, snmptrapd and StorageAPI.</td>
</tr>
<tr>
<td>-b HV_BSNET_IP</td>
<td>Compute resource's IP Address from Backup Servers' network Used to bind the SCSI target daemon.</td>
</tr>
<tr>
<td>-f FTS_IP</td>
<td>File Transfer Server FQDN or IP address, used for daily cron update recovery ISO by recovery.sh</td>
</tr>
<tr>
<td>-a</td>
<td>Install AoE</td>
</tr>
<tr>
<td>-s</td>
<td>Install sshfs</td>
</tr>
</tbody>
</table>
9. Reboot the compute resource to complete the installation:

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

10. 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. It 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.

11. If you are installing a new cloud, SSH into your Control Panel server then download and run the script:

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

12. If you are adding additional compute resources to an existing cloud, update the authorized_keys file by running the following script on the Control Panel server:

```bash
bash#> ssh-copy-id -i /home/onapp/.ssh/id_rsa.pub root@HV_HOST_IP
```

13. Mount the locations for templates and backups:

If you do not have a dedicated backup server you must mount your Template and Backup repository to the compute resource for VS provisioning and backups to work, for example from your Control Panel server:

Add to `/etc/exports` on the Control Panel server then reboot:

```
/onapp/templates 192.168.10.0/24(rw,no_root_squash)
/onapp/backups 192.168.10.0/24(rw,no_root_squash)
```

Add to `/etc/rc.local` on the Compute resource and run them manually on the command line (In this example we are mounting from 192.168.10.101):

```
mkdir -p /onapp/backups && mount -t nfs 192.168.10.101:/onapp/backups /onapp/backups
mkdir -p /onapp/templates && mount -t nfs 192.168.10.101:/onapp/templates /onapp/templates
```

14. Mount ISO locations:

To rebuild a VS from ISO, it is required to mount and share the location where the ISOs are stored at CP with all the compute resources. When the virtual servers are booted from the ISOs, the ISO is taken from the compute resource server. The location is preconfigured at onapp.yml config file:

- **iso_path_on_cp** - specifies the location where ISOs are stored on the Control Panel server. By default the location is /data. You can change it to any other suitable location. Make sure that this location is shared with the specified iso_path_on_hv location.
- **iso_path_on_hv** - specifies the location where ISOs are located on the compute resource servers. By default the location is /data. You can change it to any other suitable location with the onappowner and read/write access. Make sure that this location is mounted to the specified iso_path_on_cp location.

CloudBoot compute resources mount the /data location automatically at boot to the /onapp/tools/recovery on compute resource.

ISOs can be hosted on a dedicated server at any desired location with an arbitrary name if you wish. In this case it is necessary to mount the ISOs' location on this server to the Control Panel iso_path_on_cp directory and all the compute resource's iso_path_on_hv locations. This can be a backup server to avoid the excess usage of the Control Panel's space.
Install Data Stores

This section is the part of the OnApp installation procedure.

Once the Control Panel server has been installed successfully, you can use one of the following processes to set up data stores:

- Install LVM Data Store
- Install Integrated Storage Data Store
- Install SolidFire Data Store

See also:
- Install Control Panel Server
- Install Backup Server
- Technical Details
- OnApp 4.1 Preparation Guide
- OnApp v.4.0 to v.4.1 Upgrade Guide

On this page:
- Install LVM Data Store
- Install Integrated Storage Data Store
- Install SolidFire Data Store

Search for other docs:

Install LVM Data Store

PLEASE NOTE:

- To configure an Integrated Storage data store, please consult the Admin guide.
- This process assumes you have already configured a compute resource 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 compute resources need access to the same data store. Ensure that you have the block device visible on all compute resources.
- 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 Control Panel user interface:
   a. Go to your Control Panel Settings menu.
   b. Click the Data Stores icon.
   c. Click the Create Data Store link at the bottom of the screen.
   d. Follow the steps in the creation wizard:

   Step 1 of 2
**Enter a label and IP address for your data store.**
**Select the data store type: lvm.**
**Move the slider to the right to enable a data store. When disabled, OnApp will not allow new disks to be created automatically on that data store. This is useful to prevent an established data store from becoming too full. It also lets you prevent the automatic creation of root disks on 'special' data stores (high speed, etc).**
**Click Next.**

**Step 2**

- Set disk capacity in GB.
- If required, you can also bind the data store with a local compute resource. This is helpful if you wish that the data store and a compute resource were located on the same physical server thus decreasing the time needed for a compute resource-data store connection.
- If required, you can also assign the data store to a data store zone. The drop-down menu lists all data store zones set up in the cloud (to add or edit data store zones, see the section on Data store zones in the Settings section of this guide)

e. When you've finished configuring the store, click the **Create Data Store** button.

To use the data store, you have to assign it either to a compute resource or a compute zone.

2. Find the data store's unique identifier (this is needed to create your volume group in step# 4):
   (Read the IDENTIFIER from the data stores screen: http://xxx.xxx.xxx.xxx/settings/data_stores)

3. SSH into a compute resource that is able to connect to this data store. Create the physical volume:

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

Replace xxx with the real device.

4. Create the volume group:

```bash
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 compute resource/volume group visibility:

   Now you have the new data store formatted you should be able to see the volume group from all compute resources. To test this, run `pvscan` and `vgscan` on all compute resources. Make sure you can see all identifiers on all compute resources.

### Install Integrated Storage Data Store

Before creating an integrated storage data store:

1. Create one or more Xen or KVM compute resources with integrated storage enabled to group their drives together into a virtual data store.
2. Create a compute zone.
3. Add your compute resources to the compute zone.

After that, you can proceed to the integrated storage data store creation.

To create a new integrated storage data store:

1. Go to your Control Panel's **Integrated Storage > Data Stores** menu.
2. On the screen that appears, you'll see the list of all integrated storage data stores in the cloud.
3. To create a new data store, click the **Create New Integrated Storage Data Store** button, and complete the wizard that follows:

   - **Name** - give your data store a name
Show advanced options - select this check box to reveal the list of advanced settings:

- **Replicas** - specify the number of data copies to increase the resilience to individual drive failure. You can specify 1, 2 or 4 replicas.
- **Stripes** - specify the number of data splittings to increase the number of physical disks included to the virtual disk. You can specify 0, 2 or 4 stripes.
- **Overcommit** - specify the over-provisioning percentage. You can set the following overcommit values: none (0%), 20%, 50% or unlimited (100%).

In order for your hard drives (nodes) to be detected and active, multicast traffic should be enabled on your switch, for the Onapp Integrated Storage Network/VLAN.

**Storage Nodes**

- **Filter by compute resource** - use this to filter the nodes (disks) available for inclusion in this data store, by specific compute resources.
- **Filter by performance** - use this to filter the nodes available for inclusion in this data store by performance.

4. Click the **Save** button to create the data store. The data store must be assigned to a compute zone and data store zone before you can provision storage to a VS.

---

**Install SolidFire Data Store**

You can create one SolidFire data store per cloud that will represent the space available at the SolidFire side.

To create a SolidFire data store:

1. Go to your Control Panel **Settings** menu.
2. Click the **Data Stores** icon.
3. Click the **Create Data Store** link at the bottom of the screen.
4. Follow the steps in the creation wizard:

**Step 1 of 3**

- Enter a data store label.
- Specify an IP address to be used for managing the data store via CP (Inasmuch SolidFire data stores have two interfaces, you'll have to specify the IP address for the cluster admin later.)
- Select a **solidfire** data store type.
- Move the slider to the right to enable a data store. When disabled, OnApp will not allow new disks to be created automatically on that data store. This is useful to prevent an established data store from becoming too full. It also lets you prevent the automatic creation of root disks on ‘special’ data stores (high speed, etc).
- Click **Next**.

**Step 2 of 3**

- Set disk capacity in GB.
- If required, you can also bind the data store with a local compute resource. This is helpful if you wish that the data store and a compute resource were located on the same physical server thus decreasing the time needed for a compute resource-data store connection.
- If required, you can also assign the data store to a data store zone. The drop-down menu lists all data store zones set up in the cloud (to add or edit data store zones, see the section on Data store zones in the Settings section of this guide).

**Step 3**

- Specify the cluster Admin settings:
  - **iSCSI IP** - iSCSI IP address
  - **Username** - specify username for cluster authorization
  - **Password** - specify password for cluster authorization.

Specify the SolidFire Account settings:

- **Username** - specify SolidFire account username
- **Initiator secret** - specify iSCSI initiator secret (optional)
- **Target secret** - specify iSCSI initiator secret (optional)

**Initiator secret** and **target secret** are optional parameters. They are created automatically for a newly created account. For the
new account they will be taken from the SolidFire database.
If you specify target and initiator secrets for an existing user, they will be overwritten.

5. When you've finished configuring the store, click the Create Data Store button.

---

**Install Backup Server**

Follow one of two processes to set up a backup server in your cloud:

- Install Static Backup Server
- Install CloudBoot Backup Server

Choose the one that suits you best.

---

**Install Static Backup Server**

To install static backup server, run the following procedure. Skip this section if you are using a CloudBoot method. We recommend installing CentOS from the minimal CentOS ISO for static backup servers.

1. Add a backup server via the Control Panel user interface:
   a. Go to your Control Panel's Settings menu, then press Backup servers icon.
   b. Click the Create Backup Server button.
   c. Fill in the form that appears:
      - Label - give your backup server a label
      - IP address - enter the backup server IP address (IPv4)
- Backup IP address - add a provisioning network IP address
- Capacity - set the backup server capacity (in GB)
- Backup server zone - select the backup server zone to which this backup server will be assigned.

d. Move the Enabled slider to the right to enable the backup server.
e. Click the Add Backup Server button.

2. Update your server:

```
bash# yum update
```

3. Download the OnApp repository:

```
bash# rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo.noarch.rpm
```

4. Install the OnApp Backup Server installer package:

```
bash# yum install onapp-bk-install
```

5. Check and set Backup Server default settings:

- Edit Backup Server default settings by editing the /onapp/onapp-bk.conf file:
  - OnApp BK tools custom version
  ```bash
  BK_VERSION=""
  ```
  - OnApp StorageAPI custom version
  ```bash
  API_VERSION=""
  ```
  - Default server to synch time on the HV
  ```bash
  NTP_TIME_SERVER='pool.ntp.org'
  ```
  - The number of retries for WGET to download the file
  ```bash
  WGET_TRIES=5
  ```
  - OnApp templates directory.
  ```bash
  TEMPLATES_DIR='/onapp/templates'
  ```
  - OnApp backups directory.
  ```bash
  Please refer to the corresponding settings at OnApp Control Panel web interface
  TEMPLATES_DIR='/onapp/templates'
  ```
Run the installer. It is recommended to download Base, Load Balancer and CDN templates while running the installer. You may rerun the installer later with the `-t` option.

```
bash# sh /onapp/onapp-bk-install/onapp-bk-install.sh
```

**The full list of installer options:**

**Usage:**

```
```

**Where:**

- `-c CONFIG_FILE` Custom installer configuration file. Otherwise, preinstalled one is used.
- `-a` Do NOT be interactive. Proceed with automatic installation.
- `-y` Update OS packages (except of OnApp provided) on the box with `yum update`.
- `-t` Initiate Base, Load Balancer and CDN templates download. The download is initiated if `-a` option is used.
- `-h` Print this info

7. Configure the backup server for your cloud. This step is also required for the SNMP statistics receiver configuration:

```
```

**The full list of configuration options:**

**Usage:**

```
/onapp/onapp-bk-install/onapp-bk-config.sh [-h CP_HOST_IP] [ -p BK_HOST_IP] [-f FTS_IP] [ -a|-i [USER:PASSWD]] [-s] -?
```

**Where:**

- `-h CP_HOST_IP` FQDN or IP Address of the management server which should receive all status reports and is authoritative for this backup server.
**Install CloudBoot Backup Server**

CloudBoot backup servers are CloudBooted KVM compute resources that can be be used as backup servers. Follow the step-by-step instructions provided in this chapter to configure CloudBoot backup servers in your cloud.

- You should configure some local or remote attached storage for persistent backups on the provisioning/backup server.
- We strongly recommend you to deploy one or more backup servers on your cloud, Incremental backups are only supported with a dedicated backup server.

To create a CloudBoot backup server:

1. Update CloudBoot and CP server RPMs:

   ```
   yum update onapp-store-install yum update onapp-cp-install
   ```

2. Configure CloudBoot settings:

   ```
   /onapp/onapp-store-install/onapp-store-install.sh
   ```

3. Create new CloudBoot compute resource with an IP address from the dynamic range. Refer to the Create CloudBoot Compute resource section of the Admin guide for details.
4. Ensure to choose the ‘Backup’ option and don’t format disks.
5. Go to your Control Panel’s Settings menu, then press Backup Servers icon.
6. Click the Create Backup Server button.
7. Fill in the form that appears:
   - Tick the Enabled box to enable the backup server.
   - Label - give your backup server a label
   - IP address - enter the IP address of a compute resource you have created at step 1
   - Backup IP address - add a provisioning network IP address
   - Capacity - set the backup server capacity (in GB)
8. After that, assign your backup server to the backup server zone.

   If you intend to attach LVM-based storage and create backups, you should also add the IP address of the KVM compute resource added in step 1 in the ‘Backup IP address’ field of each of your compute resources.

**Further steps:**

1. Format and mount the local storage:
a. SSH to the backup server
b. Format the storage with your preferred filesystem type, e.g.:

```bash
bash#> mkfs.ext4 /dev/sda
```

c. Make folder for backups if it does not exist

```bash
bash#> mkdir /backupstorage
```

d. Mount the storage to /onapp/backups:

```bash
bash#> mount /dev/sda /backupstorage
```

e. Make folder for storing templates:

```bash
bash#> mkdir /backupstorage/templates
```

f. Make folder for storing backups:

```bash
bash#> mkdir /backupstorage/backups
```

g. Create symbolic links in /onapp

```bash
bash#> ln -s /backupstorage/backups /onapp/backups
```

h. Add the following to custom config file:

```bash
mkdir /backupstorage
mount /dev/sda /backupstorage
ln -s /backupstorage/backups /onapp/backups
ln -s /backupstorage/templates /onapp/templates
```

2. Update the database so that the location of the templates is known:

a. Find the database password:

```bash
cat /onapp/interface/config/database.yml | grep password
```

b. Open the onapp database in MySQL:

```bash
bash#> mysql -p bash#> use onapp;
```

c. Find the ID of the backup server:
bash#> select * from backup_servers;

d. For all of the templates, set the required backup_server_id:

bash#> update templates set backup_server_id='[your_id]';

3. To download the base templates during the installation to your Control Panel, download and run the following script:

bash#> wget http://downloads.repo.onapp.com/get_template.sh
bash#> /bin/sh get_template.sh

To ensure your backups don’t disappear after rebooting the CloudBoot backup server, add a mount command to the CloudBoot backup servers custom config so it is automatically mounted after future reboots.

To fix your custom config settings, you can use one of the following options provided in the examples below (you will have to specify your own device names):

a. If you have a separate partition for backups and templates (/dev/sda1 and /dev/sda2)

   mkdir -p /onapp/backups
   mkdir -p /onapp/template
   mount /dev/sda1 /onapp/backups
   mount /dev/sda2 /onapp/templates

b. If you current array is detected as /dev/sda1 and currently everything is located in /onapp within templates and backup directories within:

   mkdir -p /onapp
   mount /dev/sda1 /onapp

This section is the part of the OnApp installation procedure.

| Install Control Panel Server | Install Compute Resources | Install Data Stores | Install Backup Server | Download and Configure Templates on Control Panel Server | Configure Cloud |

Enable Recovery Mode for Baremetal Servers

To enable recovery mode for baremetal servers, perform the following steps:

1. Download the following files:
   http://templates.repo.onapp.com/Linux/recovery-baremetal.kernel
2. Place the files into the /tftpboot/images/ramdisk-recovery/ directory.
3. Create template file /tftpboot/pxelinux.cfg/template-baremetal-recovery with following contents:

```bash
default baremetal-recovery
label baremetal-recovery
kernel images/ramdisk-recovery/recovery-baremetal.kernel
append initrd=images/ramdisk-recovery/recovery-baremetal.initrd
root=live:/recovery-centos-3.2.iso rootfstype=auto ro liveimg
rd.luks=0 rd.md=0 rd.dm=0
```

4. Restart the OnApp services:

```bash
service onapp restart
service httpd restart
```

After that, recovery mode option will appear in the baremetal server's Tools menu:

![Baremetal Server details](image)

Download and Configure Templates on Control Panel Server

This section is the part of the OnApp installation procedure.
To download and configure templates on Control Panel server, log in to the CP server as root, and run:

```
bash#> wget http://downloads.repo.onapp.com/get_template.sh
bash#> /bin/sh get_template.sh
```

See also:
- Install Control Panel Server
- Install Backup Server
- Technical Details
- OnApp 4.1 Preparation Guide

Search for other docs:

Configure Cloud

This section is the part of the OnApp installation procedure.

Once you've set up your hardware, the final step is to configure your cloud in your Control Panel. This section explains how to configure a basic cloud. If you complete these steps you should be in a position to create VSs.

To avoid VNC console issues, make sure that ServerName Apache setting matches the SSL certificate.

1. Configure Control Panel Settings

   Once you have installed OnApp, you need to make the necessary Control Panel configurations. Set the system, backups/templates, interface and defaults CP options.

2. Configure Compute Resources

   To deploy virtual servers, you need to add compute zones and compute resources to your cloud. After that, attach the newly created compute resource to the compute zone you've added. Make sure to enable Integrated storage in the Settings > Configuration to group compute resource drives together into a virtual data store. Also, to use Integrated Storage, select the compute zone as a storage API endpoint.

3. Configure Data Stores

   To provide your virtual servers with storage space, you need to configure data store zones and data stores. Data stores can be Traditional/ Centralized SAN and OnApp Storage/Integrated SAN. You should also attach the new data store to the data store zone you've added.

   In case of Traditional storage you need to configure data store(s) on your compute resource. The commands below use /dev/sda5 as an example. You can find the volume group identifier we’re using in the second command, from the Data Stores screen in the Control Panel. Follow these steps for each local storage block on the compute resource:
4. Configure Networks

To provide IP address(es) to your future virtual servers, you need to perform the necessary network configurations. To do this, create network zones and networks. When adding the network, select the network zone you've created. The network will be automatically attached to the network zone you chose during creation. You should also add a range of IP addresses to the new network.

5. Configure Relations Between Entities

Once you've added all the necessary resources to your cloud, you need to associate them with the compute resource you've created in Step 2. For this, assign the data store (Step 3) and network (Step 4) to the compute resource (Step 2).

6. Configure ISOs

To be able to later build and boot VSs from ISOs, additional steps are required. For more information refer to the ISOs section.

OnApp Cloud v.4.1 Installation Guide for High Availability Clusters.

Please contact your account manager to enable High Availability Control Panel for your cloud.

Setting up a High Availability cluster requires additional configuration besides the standard installation procedure. The general workflow is the following:

**Preparation**

1. Read the Technical Details
2. Read the Preparation Guide

**Installation**

1. Configure Database & Transactions Server
2. Install Control Panel server
3. Configure Control Panels for High Availability Cluster
4. Install compute resources
5. Install data stores
6. Install backup server
7. Download and configure templates on template server.
8. Configure Cloud

The detailed instructions are provided below.

See also:
- Install Data Stores
- Install Backup Server
- Technical Details
- OnApp 4.1 Preparation Guide
- OnApp v.4.0 to v.4.1 Upgrade Guide

On this page:
- Configure Database & Transactions Server
- Install Control Panels for High Availability Cluster
- Configure High Availability
- Further Steps

Configure Database & Transactions Server
For the clusters with High Availability Control Panel enabled it is recommended to deploy a separate database&transactions server where the database, Redis and RabbitMQ will run. We assume that you have already installed the database&transactions server. Follow the listed instructions to configure the server:

1. Log in to Database&Transactions server.
2. Enter the MySQL database and set the password.
3. For each Control Panel IP address, run the following command:

   ```
   > GRANT ALL PRIVILEGES ON onapp.* TO root"cp_ip_address" IDENTIFIED BY 'PASSWORD' WITH GRANT OPTION;
   ```

   where:
   - `cp_ip_address` - the address of the Control Panel node.
   - `password` - the password to the database

4. Configure Redis. Download OnApp yum repository file:

   ```
   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo.noarch.rpm
   ```

5. Install OnApp Redis package:

   ```
   bash#> yum install redis
   ```

6. Open the Redis configuration file `/etc/redis.conf` and set:
   - `bind` - the IP address of the Database&Transactions server where Redis is installed
   - `port` - the port to which Redis is listening. By default the 6379 port is set.
   - `requirepass` - the password to connect to Redis instance

7. Restart Redis. Run:

   ```
   service redis restart
   ```

8. Update relevant attributes in CP server's configuration:

   ```
   /onapp/interface/config/redis.yml
   ```

---

Install Control Panels for High Availability Cluster

Currently, you can set up two Control Panel servers for clusters with High Availability. Follow the procedure below to set up two Control Panels.

Install the CPs according to Install Control Panel Server documentation. Pay attention to the following:

- Make sure to set the MySQL and Redis configs using the appropriate parameters.
- Disable monitis before installing the CP server:

   ```
   vim /onapp/onapp-cp.conf
   ENABLE_MONIT=0
   ```

- Ensure that you set license key for both Control Panels.
- After the installation, it is recommended to increase the soft and hard limits for the opened files:
  1. Open the `/etc/security/limits.conf` file:
vim /etc/security/limits.conf

2. Change the following parameters to at least the following:

   root soft nofile 2048
   root hard nofile 4096

   For heavy loaded cloud deployments, the limits should be increased.

**Configure High Availability**

After the CP servers are installed, it is required to configure them. To do so:

1. Install the High Availability package:

   yum install onapp-cp-ha

2. Run the script:

   /onapp/onapp-ha/onapp-cp-ha.sh

3. Log in to your Control Panel **Settings > HA Clusters** menu. On the page that loads, fill in the high availability cluster configuration settings.

4. Configure the clusters:

   **UI Cluster**
   - `virtual_ip` - set the virtual IP address of the control panels

   Specify the following parameters for the first node:
   - `name` - specify the hostname of the first node
   - `IP address` - specify the physical IP address of the first node
   - `interface` - specify the network interface for the node
   - `priority` - set the priority for the first node. The node with the highest priority will take over the virtual IP address when the component of the cluster fails.

   Specify the following parameters for the second node:
   - `name` - specify the hostname of the second node
   - `IP address` - specify the physical IP address of the second node
   - `interface` - specify the network interface for the node
   - `priority` - set the priority for the second node. The node with the highest priority will take over the virtual IP address when the component of the cluster fails.

   Click **Save Cluster Configuration** to apply the settings.

   **Daemon Cluster**
   - `virtual_ip` - set the virtual IP address of the control panels

   Specify the following parameters for the first node:
   - `name` - specify the hostname of the first node
   - `IP address` - specify the physical IP address of the first node
   - `interface` - specify the network interface for the node
   - `priority` - set the priority for the first node. The node with the highest priority will take over the virtual IP address when the
component of the cluster fails.

Specify the following parameters for the second node:

- **name** - specify the hostname of the second node
- **IP address** - specify the physical IP address of the second node
- **interface** - specify the network interface for the node
- **priority** - set the priority for the second node. The node with the highest priority will take over the virtual IP address when the component of the cluster fails.

Click **Save Cluster Configuration** to apply the settings.

**Cloud_boot Cluster**

- **virtual_ip** - set the virtual IP address of the cloudboot clusters

Please note, that **virtual_ip** must be equal to Static Config target and CP server Cloudboot target IP addresses that you set at Settings > Configuration screen

Specify the following parameters for the first node:

- **name** - specify the hostname of the first node
- **IP address** - specify the physical IP address of the first node
- **interface** - specify the network interface for the node
- **priority** - set the priority for the first node. The node with the highest priority will take over the virtual IP address when the component of the cluster fails.

Specify the following parameters for the second node:

- **name** - specify the hostname of the second node
- **IP address** - specify the physical IP address of the second node
- **interface** - specify the network interface for the node
- **priority** - set the priority for the second node. The node with the highest priority will take over the virtual IP address when the component of the cluster fails.

Click **Save Cluster Configuration** to apply the settings.

3. Go to `/onapp/interface` and issue:

   'RAILS_ENV=production rake ha:init'

4. **(Optional)** To check the status of services, run the following:

   `crm_mon -r`

5. Check that the redundant node has the appropriate virtual IP of the cluster. Run:

   `ip a`

6. Add public key of root user of the main Control Panel to the authorized keys at a secondary Control Panel. And vice versa.

7. Configure high availability on a secondary Control Panel server:

   'RAILS_ENV=production rake ha:join'

**Further Steps**
To finish the cloud configuration, follow the standard installation process:

1. Install Compute Resources
2. Install Data Stores
3. Install Backup Server
4. Download and Configure Templates on Control Panel Server
5. Configure Cloud

OnApp v.4.0 to v.4.1 Upgrade Guide

This guide explains how to upgrade OnApp Cloud v4.0 to the v4.1. OnApp 4.1 updates only Control Panel server. Follow the procedure listed below in the correct order to upgrade your cloud.

You must be running OnApp 4.0 to upgrade to 4.1. If you are using an earlier version, please upgrade to 4.0. first.

On this page:

- Introduction and Important Notes
- Upgrade Control Panel Server

Introduction and Important Notes

Before you begin

1. Check the Activity Log in your OnApp CP dashboard if there are no transactions running in your cloud. If so, wait until all transactions are complete.
2. Make sure no Control Panel files are open for editing under the root user account.
3. If you are using a third-party billing platform, please ensure that this is compatible with OnApp 4.1 before proceeding with the upgrade! The latest WHMCS modules can be found here.
4. If you are using WHMCS modules, make sure to update the PHP Wrapper after you update OnApp Cloud. Download the latest wrapper.
5. We strongly recommend that you test all your custom scripts before upgrading your production environment.
6. Installer output is redirected to ./onapp-cp-install.log
7. All installer critical errors are in /var/log/messages

Getting support for your upgrade

You can use the information in this document to perform your own upgrade to the 4.1 version of the OnApp Cloud. However, if you have a full (paid) OnApp Cloud license, you are entitled to free upgrade support from the OnApp Support team.

If you would prefer to have the Support team perform the upgrade for you, just raise a ticket in the normal way. Please be aware, however, that there may be a queue!

For help with your upgrade, visit the OnApp community forum: http://forum.onapp.com.

Upgrade Control Panel Server

To upgrade your Control Panel server:

1. Run the following command from the CP server to stop the OnApp service:

   ```
   service onapp stop
   ```
2. Download and install the latest OnApp YUM repository file:

```
bash#> rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo.noarch.rpm
```

3. Upgrade OnApp Control Panel installer package:

```
bash#> yum update onapp-cp-install
```

4. Update your server OS components (if required):

```
bash# /onapp/onapp-cp-install/onapp-cp-install.sh -y
```

5. *(Optional)* If you need some custom Control Panel configuration, set the values before the installer script runs.

   - Edit the `/onapp/onapp-cp.conf` file to set Control Panel custom values

```
# Template server URL

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

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

SNMP_TRAP_IPS=

# OnApp Control Panel custom version

ONAPP_VERSION=

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

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

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

MYSQL_WAIT_TIMEOUT=604800
MYSQL_MAX_CONNECTIONS=500
MYSQL_PORT=3306

# Use MariaDB instead of MySQL as OnApp database server
```
WITH_MARIADB=0

# Configure the database server relative amount of available RAM
TUNE_DB_SERVER=0

# The number of C data structures that can be allocated before triggering the garbage collector. It defaults to 8 million
RUBY_GC_MALLOC_LIMIT=16000000

# sysctl.conf net.core.somaxconn value
NET_CORE_SOMAXCONN=2048

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

# Remote server's (to store database dumps) IP, user, path, openssh connection options ans number of dumps to keep
DB_DUMP_SERVER=
DB_DUMP_USER=root
DB_DUMP_SERVER_ROOT=/onapp/backups
DB_DUMP_SERVER_SSH_OPT="-o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -o PasswordAuthentication=no"
KEEP_DUMPS=168
DB_DUMP_CRON='40 * * * *'

# Enable monit - tool for managing and monitoring Unix systems
ENABLE_MONIT=1

# If enabled (the 1 value is set) - install (if local box) and configures RabbitMQ Server (messaging system) for the vCloud
ENABLE_RABBITMQ=1
# Rotate transactions' log files created more then TRANS_LOGS_ROTATE_TIME day(s) ago

TRANS_LOGS_ROTATE_TIME=30

# Maximum allowed for uploading file size in bytes, from 0 (meaning unlimited) to 2147483647 (2GB). Default is 1GB

MAX_UPLOAD_SIZE=1073741824

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

REDIS_PING_TIMEOUT=5

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

SSL_CERT_COUNTRY_NAME=UK
SSL_CERT_ORGANIZATION_NAME='OnApp Limited'
SSL_CERT_ORGANIZATION_ALUNITNAME='OnApp Cloud'
SSL_CERT_COMMON_NAME=`hostname --fqdn 2>/dev/null`

# SSLCertificateFile, SSLCertificateKeyFile Apache directives' values
# ssl_certificate, ssl_certificate_key Nginx directives' values

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

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

SSLCACERTIFICATEFILE=
SSLCERTIFICATECHAINFILE=

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

SSLCIPHERSUITE=
SSLPROTOCOL=
6. Run Control Panel installer:

```
bash# /onapp/onapp-cp-install/onapp-cp-install.sh
```

See the installer options below for details.

The full list of Control Panel installer options:

```
Usage:

```

<table>
<thead>
<tr>
<th>Where</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MYSQL_*</td>
<td>Options are useful if MySQL is already installed and configured.</td>
</tr>
<tr>
<td>-m MYSQL_HOST</td>
<td>MySQL host</td>
</tr>
<tr>
<td>-p MYSQL_PASSWD</td>
<td>MySQL password</td>
</tr>
<tr>
<td>-d MYSQL_DB</td>
<td>OnApp MySQL database name</td>
</tr>
<tr>
<td>-u MYSQL_USER</td>
<td>MySQL user</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REDIS_*</th>
<th>Options are useful if Redis Server is already installed and configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>--redis-host=</td>
<td>IP address/FQDN where Redis Server runs.</td>
</tr>
<tr>
<td>REDIS_HOST</td>
<td>The Redis Server will be installed and configured on the current box if</td>
</tr>
<tr>
<td></td>
<td>localhost/127.0.0.1 or box's public IP address (listed in SNMP_TRAP_IPS)</td>
</tr>
<tr>
<td></td>
<td>is specified. If local Redis, it will serve as well on the unix socket</td>
</tr>
<tr>
<td></td>
<td>'/tmp/redis.sock'. Default value is 127.0.0.1.</td>
</tr>
<tr>
<td>--redis-port=</td>
<td>Redis Server listen port.</td>
</tr>
<tr>
<td>REDIS_PORT</td>
<td>Defaults are: 0 - if local server</td>
</tr>
<tr>
<td></td>
<td>6379 - if remote server</td>
</tr>
<tr>
<td>--redis-passwd=</td>
<td>Redis Server password to authentificate.</td>
</tr>
<tr>
<td>REDIS_PASSWD</td>
<td>Random password is generated if the option's argument isn't specified.</td>
</tr>
<tr>
<td></td>
<td>By default no password is used for local Redis.</td>
</tr>
<tr>
<td>--redis-sock=</td>
<td>Path to the Redis Server's socket. Used if local server only.</td>
</tr>
<tr>
<td>REDIS_PATH</td>
<td>Default is /tmp/redis.sock</td>
</tr>
</tbody>
</table>

```
With OnApp you can upgrade to a custom CP version, i.e. not the latest one available in production. Make sure to update within the same major version. For example, you can upgrade from 3.2.2-9 to 3.2.2-<x>, but not from 3.0.x-<x> to 3.2.x-<x>.

To upgrade to the specific OnApp Control Panel version, perform the following steps:

1. Run the following command to eliminate all of the files which yum uses to determine the remote availability of packages:

   ```bash
   bash# yum clean metadata
   ``

2. Remove OnApp:

   ```bash
   bash# yum remove onapp-cp
   ``

3. Install OnApp Control Panel installer package for the required Control Panel version:

   ```bash
   bash# yum install onapp-cp-<ONAPP_VERSION>
   ``

   Where:
   
   ONAPP_VERSION - the required OnApp version with its build, e.g. 3.2.2-15

---

### Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--P ADMIN_PASSWD</td>
<td>CP administrator password</td>
</tr>
<tr>
<td>-F ADMIN_FIRSTNAME</td>
<td>CP administrator first name</td>
</tr>
<tr>
<td>-L ADMIN_LASTNAME</td>
<td>CP administrator last name</td>
</tr>
<tr>
<td>-E ADMIN_EMAIL</td>
<td>CP administrator e-mail</td>
</tr>
<tr>
<td>-v ONAPP_VERSION</td>
<td>Install custom OnApp CP version</td>
</tr>
<tr>
<td>-i SNMP_TRAP_IPS</td>
<td>IP addresses separated with coma for snmp to trap</td>
</tr>
<tr>
<td>-c CONFIG_FILE</td>
<td>Custom installer configuration file. Otherwise, preinstalled one is used.</td>
</tr>
<tr>
<td>-y</td>
<td>update OS packages (except of OnApp provided) on the box with 'yum update'.</td>
</tr>
<tr>
<td>-a</td>
<td>do not be interactive. Process with automatic installation.</td>
</tr>
<tr>
<td>-D</td>
<td>do not make database dump, and make sure it is disabled in the cron and not running at the moment</td>
</tr>
<tr>
<td>-h</td>
<td>print this info</td>
</tr>
</tbody>
</table>

---

You may wish to reboot your Control Panel server to take advantage of a new kernel if it is installed. It is not required immediately as a part of the upgrade process though.

7. In the OnApp UI navigate to **Settings > Configuration** and click **Save** to complete the process.

### Upgrade to Custom Control Panel Version

You should use the standard upgrade procedure whenever possible to ensure you have the latest features and fixes. Only use the custom upgrade when you have a specific reason for installing an older version.

---

**See also:**

- Install Control Panel Server
- Install Data Stores
- Install Backup Server
- Technical Details
- OnApp 4.1 Preparation Guide
- OnApp v.4.0 to v.4.1 Upgrade Guide
Update OS Components

From now on, there is a possibility to update the OS components for static Compute resource, Control Panel Server, and static Backup Server outside of the distributive packages provided by OnApp.

To do so:

1. Upgrade the installer:
   - **For Control Panel**
     
     bash#> yum update onapp-cp-install
   
   - **For Compute resource**
     
     bash#> yum update onapp-hv-install
   
   - **For Backup Server**
     
     bash#> yum update onapp-bk-install

2. Run the following script to update the OS components
   - **For Control Panel**
     
     bash#
     /onapp/onapp-cp-install/onapp-cp-install.sh -y
   
   - **For XEN Compute resource**
     
     bash#
     /onapp/onapp-hv-install/onapp-hv-xen-install.sh -y
   
   - **For KVM Compute resource**
     
     bash#
     /onapp/onapp-hv-install/onapp-hv-kvm-install.sh -y
   
   - **For Backup Server**
     
     /onapp/onapp-bk-install/onapp-bk-install.sh -y

See also:

- Install Control Panel Server
- Install Data Stores
- Install Backup Server
- Technical Details
- OnApp 4.1 Preparation Guide
- OnApp v.4.0 to v.4.1 Upgrade Guide

ISOs

OnApp 4.0 and up introduces possibility to boot a VS from the ISO. Perform the following steps to enable this functionality for your cloud:
Mount ISO locations

To rebuild a VS from ISO, it is required to mount and share the location where the ISOs are stored at CP with all the hypervisors. When the virtual servers are booted from the ISOs, the ISO is taken from the hypervisor server. The location is preconfigured at onapp.yml config file:

iso_path_on_cp - specifies the location where ISOs are stored on the Control Panel server. By default the location is /data. You can change it to any other suitable location. Make sure that this location is shared with the specified iso_path_on_hv location.

iso_path_on_hv - specifies the location where ISOs are located on the hypervisor servers. By default the location is /data. You can change it to any other suitable location with the onapppowner and read/write access. Make sure that this location is mounted to the specified iso_path_on_cp location.

CloudBoot hypervisors mount the /data location automatically at boot to the /onapp/tools/recovery on HV.

ISOs can be hosted on a dedicated server at any desired location with an arbitrary name if you wish. In this case it is necessary to mount the ISOs' location on this server to the Control Panel iso_path_on_cp directory and all the hypervisors' iso_path_on_hv locations. This can be a backup server to avoid the excess usage of the Control Panel's space.

Enable Permissions in Control Panel

Make sure to enable the following permissions for your Admin and other roles as appropriate:

- Any action on ISOs - the user can take any action on ISOs
- Create a new ISO - the user can create a new ISO
- Destroy any ISO - the user can delete any ISO (own, user, and public)
- Destroy own ISO - the user can only delete own ISO
- Destroy user ISO - the user can delete ISOs created by any user, but not public ISOs
- Make any ISO public - the user can make public any ISO available to all users
- Make own ISO public - the user can make public own ISOs only
- Make user ISO public - the user can make public ISOs created by any user
- Create and manage own ISOs - the user can create and edit/delete/view own ISOs
- Manage all ISOs - the user can manage own/user/public ISOs
- Create and manage user ISOs - the user can view/create/edit/delete ISOs created by any user
- See all ISOs - the user can view all ISOs in the cloud
- See own ISOs - the user can only view the ISOs created by themselves
- See all public ISOs - the user can view all public ISOs
- See user ISOs - the user can view the ISOs created by any user in the cloud
- Update any ISO - the user can edit any ISO in the cloud
- Update own ISO - the user can only edit own ISO
- Update user ISO - the user can edit the ISOs created by any user in the cloud

Getting Support

24x7 support
OnApp customers with a full (paid) license can contact OnApp Support at any time:

- support@onapp.com
- http://onapp.com/support
- (+1) 888 876 8666
Forums
Visit http://forum.onapp.com to get support from the OnApp community. Members of OnApp's support and engineering teams also monitor the forums and contribute to discussions. To access the forums, log in with your OnApp Dashboard account details.

Documentation
For the latest OnApp documentation, see https://docs.onapp.com.

What does OnApp Support in my Cloud?

OnApp provides support for anything directly related to our core products - OnApp Cloud, OnApp CDN and OnApp Storage - as well as the add-ons for these. As such, we maintain responsibility for the software, bug fixes, patches and general maintenance of our products.

Unfortunately, we do not offer support for the following:

- Switch, router and firewall configuration
- SAN configuration/optimization
- Attaching/removing/resizing LUNs
- Compute resource and Control Panel server hardware support
- Operating System installation/support
- Maintenance of your passwords or whitelists
- Configuration/troubleshooting inside virtual machines
- VMware vSphere installation/configuration
- Known bugs/limitations within virtualization platforms
- 3rd party integrations
- Alpha/Beta releases
- Coding for recipes

Some of these areas can be touched during investigation and resolution of support tickets. We will attempt to offer possible suggestions, or put you in touch with our professional services team to quote the work. However, they are not covered under standard OnApp support.