OnApp Cloud 5.4
Get Started Guide
OnApp Cloud 5.4 Get Started Guide

5.4 Get Started ........................................................................................................................................... 18
1.1 What's New in OnApp Cloud 5.4 ........................................................................................................... 18
1.2 Technical Details ................................................................................................................................... 19
1.2.1 Suggested Specifications .................................................................................................................. 19
1.2.2 Server Config Reminder ................................................................................................................... 21
1.2.3 Software Requirements .................................................................................................................... 21
1.2.4 Recommended Network Configurations ............................................................................................. 22
1.2.5 Types of Cloud Service with OnApp .................................................................................................. 27
1.2.6 Supported Functionality ................................................................................................................... 28
1.3 Preparation Guide ................................................................................................................................... 29
1.3.1 Configure Networks .......................................................................................................................... 29
1.3.2 Configure Storage ............................................................................................................................. 31
1.3.3 Configure Servers ............................................................................................................................. 33
1.4 OnApp Installation Walk-through ......................................................................................................... 36
1.5 Installation Guide ................................................................................................................................... 37
1.5.1 Install Control Panel Server ............................................................................................................. 37
1.5.2 Install Compute Resources ............................................................................................................... 44
1.5.3 Install Data Stores ............................................................................................................................. 54
1.5.4 Install Backup Server ......................................................................................................................... 57
1.5.5 Enable Recovery Mode for Baremetal Servers .................................................................................. 62
1.5.6 Configure vCloud Director Integration .............................................................................................. 63
1.5.7 Configure Cloud ................................................................................................................................. 65
1.5.8 Quick vCloud Director Integration ..................................................................................................... 67
1.6 Upgrade Guide for Cloud with CloudBooted Servers ............................................................................ 71
1.7 Upgrade Guide for Cloud with Static Servers ......................................................................................... 83
1.8 Upgrade Guide for Cloud with Mixed CloudBooted and Static Servers ..................................................... 92
1.9 Upgrade to Custom Control Panel Version ............................................................................................ 106
1.10 OS Components Upgrade ................................................................................................................... 107
1.11 Additional Considerations for ISOs ..................................................................................................... 108
1.12 OnApp IS Upgrade Paths ..................................................................................................................... 109
1.13 Getting Support ..................................................................................................................................... 110
5.4 Get Started

The guides in this section apply to installing the OnApp Cloud 5.4 version. For the release notes list, please refer to the Release Notes space.

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

Technical Details

- Suggested Specifications
- Server Config Reminder
- Software Requirements
- Recommended Network
- Configurations Types of Cloud Service
- with OnApp Supported Functionality

Installation

- OnApp Installation Walk-through
- Installation Guide
- Installation Guide for High Availability Clusters
- Additional Considerations for ISOs
- Quick vCloud Director Integration
- Getting Support

Preparation

- Configure Networks
- Configure Storage
- Configure Servers

Upgrade

- Upgrade Guide for Cloud with CloudBooted Servers
- Upgrade Guide for Cloud with Static Servers
- Upgrade Guide for Cloud with Mixed CloudBooted and Static Servers
- Upgrade to Custom Control Panel Version
- OS Components Upgrade
- OnApp IS Upgrade Paths

What's New in OnApp Cloud 5.4

The OnApp Cloud 5.4 release contains the following changes and new features:

SDN

Added software defined network (SDN) capability to OnApp, which allows you to offer a broad range of networking services and create more flexibility. OnApp 5.4 introduces network IP nets. A network can include several IP nets which are IP ranges with a default gateway.

Cold migration for VSs and disks

Added ability to migrate disks and virtual servers cold between compute resources with local storage or across zones.

Backups for obscure VSs

Added possibility to back up the disks of the virtual servers created from ISO, VSs imported from OVA, and Container servers.

Disk reassignment between VSs

Now you can re-assign a disk from one VS to another VS that is owned by the same owner.

Maintenance mode for CloudBoot compute resources

Implemented the maintenance mode feature for CloudBoot compute resources. The maintenance mode is used to temporarily take the compute resource out of service, fix or upgrade it.
IOPS limiting

Implemented an IOPS limiting feature which allows you to prioritize the load on a SAN for VSs. You can set IOPS limiting for data stores and disks.

CDN reporting

CDN reporting functionality allows you to study and review the in-depth analysis on your own CDN resources by viewing different reports. Added CDN Visitors and Admin Reports.

VS creation wizard improvements

The Templates step of the virtual server creation wizard has been redesigned. Also domain field has been added to the Virtual Server Properties step of the wizard.

Federation improvements

The following improvements of Federation are implemented:

- improved Cloud Motion functionality
- added ability to configure recipes and custom recipe variables for VSs created in Federation
- added resources ratios for VSs built on public federated zones
- added ability to install SSH Keys for federated virtual servers

vCloud Director improvements

The following improvements of vCloud Director functionality are implemented:

- added possibility to create vCloud Director application servers and CDN edge servers
- added ability to manage advanced edge gateway services
- added ability to edit static IP pools for org networks

vCenter improvements

Improved OnApp and vCenter integration networking functionality:

- added import of vCenter infrastructure (networks and data stores)
- added ability to import VS from vCenter

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.

Suggested Specifications

Here are many factors that determine how many virtual servers you can run. Below you can find specifications for a Small Production Cloud, Medium Production Cloud and Enterprise Cloud as well the requirements for Integrated Storage.

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.

On this page:

- Suggested Specifications
- Storage Hardware Requirements
- Hardware Requirements for HA

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
- Supported Functionality
- Software Requirements
- Recommended Network Configurations
- Types of Cloud Service with OnApp
## Suggested Specifications

<table>
<thead>
<tr>
<th></th>
<th>Small Production Cloud</th>
<th>Medium Production Cloud</th>
<th>Enterprise Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OnApp License</strong></td>
<td>Host Package + Integrated Storage (add on)</td>
<td>MSP package</td>
<td>Enterprise Package</td>
</tr>
<tr>
<td><strong>Number of Control Panel (CP) Servers</strong></td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td><strong>Separate Database Server/Cluster</strong></td>
<td>No</td>
<td>No</td>
<td>Optional</td>
</tr>
<tr>
<td><strong>Dedicated Backup Servers</strong></td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td><strong>Number of Compute Resources (XEN/KVM)</strong></td>
<td>3</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td><strong>Compute Resource Type (Static / Cloudboot)</strong></td>
<td>Cloudboot</td>
<td>Cloudboot</td>
<td>Cloudboot</td>
</tr>
<tr>
<td><strong>CP Server</strong></td>
<td><strong>Processor</strong> 2 x 8 Core CPUs eg. Xeon e5-2640 v3</td>
<td><strong>Processor</strong> 2 x 8 Core CPUs eg. Xeon e5-2640 v3</td>
<td><strong>Processor</strong> 2 x 8 Core CPUs eg. Xeon e5-2640 v3</td>
</tr>
<tr>
<td></td>
<td><strong>Memory</strong> 16GB RAM</td>
<td><strong>Memory</strong> 32GB RAM</td>
<td><strong>Memory</strong> 64GB RAM</td>
</tr>
<tr>
<td></td>
<td><strong>Disks</strong> 2 x 400GB SSD</td>
<td><strong>Disks</strong> 4 x 100GB SSD</td>
<td><strong>Disks</strong> 4 x 100GB SSD</td>
</tr>
<tr>
<td></td>
<td><strong>RAID Configuration</strong>        RAID 1</td>
<td><strong>RAID Configuration</strong>        RAID 10</td>
<td><strong>RAID Configuration</strong>        RAID 10</td>
</tr>
<tr>
<td></td>
<td><strong>Network Adapters</strong> Quad port 1Gbp NIC</td>
<td><strong>Network Adapters</strong> Dual port 1Gbps + Dual Port 10Gbps eg. Intel I350 + X520</td>
<td><strong>Network Adapters</strong> Dual port 1Gbps + 2 x Dual Port 10Gbps eg. Intel I350 + 2 x Intel X520</td>
</tr>
<tr>
<td><strong>Backup Server</strong></td>
<td><strong>Processor</strong> 2 x 8 Core CPUs eg. Intel Xeon e5-2620 v3</td>
<td><strong>Processor</strong> 2 x 8 Core CPUs eg. Intel Xeon e5-2620 v3</td>
<td><strong>Processor</strong> 2 x 8 Core CPUs eg. Intel Xeon e5-2620 v3</td>
</tr>
<tr>
<td></td>
<td><strong>Memory</strong> 32GB RAM</td>
<td><strong>Memory</strong> 32GB RAM</td>
<td><strong>Memory</strong> 32GB RAM</td>
</tr>
<tr>
<td></td>
<td><strong>HDDs</strong> 12x2TB SAS</td>
<td><strong>HDDs</strong> 12x2TB SAS</td>
<td><strong>HDDs</strong> 12x2TB SAS</td>
</tr>
<tr>
<td></td>
<td><strong>RAID</strong> RAID10</td>
<td><strong>RAID</strong> RAID10</td>
<td><strong>RAID</strong> RAID10</td>
</tr>
<tr>
<td></td>
<td><strong>Network Interfaces</strong> Dual port 1Gbp Intel NIC + Dual port 10Gbps Intel NIC</td>
<td><strong>Network Interfaces</strong> Dual port 1Gbps Intel NIC + Dual port 10Gbps Intel NIC</td>
<td><strong>Network Interfaces</strong> Dual port 1Gbps Intel NIC + Dual port 10Gbps Intel NIC</td>
</tr>
<tr>
<td><strong>Compute Resource</strong></td>
<td><strong>Processor</strong> 2 x 8 Core CPUs eg. Xeon e5-2640 v3</td>
<td><strong>Processor</strong> 2 x 8 Core CPUs eg. Xeon e5-2640 v3</td>
<td><strong>Processor</strong> 2 x 8 Core CPUs eg. Xeon e5-2640 v3</td>
</tr>
<tr>
<td></td>
<td><strong>Memory</strong> 128GB</td>
<td><strong>Memory</strong> 256GB</td>
<td><strong>Memory</strong> 256GB</td>
</tr>
<tr>
<td></td>
<td><strong>HDDs</strong> 8 x 400GB SSD</td>
<td><strong>HDDs</strong> 8 x 400GB SSD</td>
<td><strong>HDDs</strong> 8 x 400GB SSD</td>
</tr>
<tr>
<td></td>
<td><strong>RAID Controller</strong>        PCIe gen3 eg. PERC H730, 1GB cache</td>
<td><strong>RAID Controller</strong>        PCIe gen3 eg. PERC H730, 1GB cache</td>
<td><strong>RAID Controller</strong>        PCIe gen3 eg. PERC H730, 1GB cache</td>
</tr>
<tr>
<td></td>
<td><strong>RAID Configuration</strong>        JBOD</td>
<td><strong>RAID Configuration</strong>        JBOD</td>
<td><strong>RAID Configuration</strong>        JBOD</td>
</tr>
<tr>
<td></td>
<td><strong>Network Interfaces</strong> Dual port 1Gbps + Dual Port 10Gbps eg. Intel I350 + X520</td>
<td>4 x 10Gbps</td>
<td>4 x 10Gbps</td>
</tr>
<tr>
<td><strong>iSCSI SAN</strong></td>
<td><strong>Type</strong> Optional Dual-Controller Hardware SAN</td>
<td><strong>Type</strong> Optional Dual-Controller Hardware SAN</td>
<td><strong>Type</strong> Optional Dual-Controller Hardware SAN</td>
</tr>
<tr>
<td></td>
<td><strong>HDDs</strong> 12+ x SSD</td>
<td><strong>HDDs</strong> 12+ x SSD</td>
<td><strong>HDDs</strong> 12+ x SSD</td>
</tr>
<tr>
<td></td>
<td><strong>RAID Configuration</strong>        RAID10</td>
<td><strong>RAID Configuration</strong>        RAID10</td>
<td><strong>RAID Configuration</strong>        RAID10</td>
</tr>
</tbody>
</table>
Network Hardware

Switch
with:
- 48 x 1GbE ports,
- 4 x 10GbE ports.

High performance switch
with:
- 48 x 10GbE ports,
- 4 x 40 GbE ports.

Network Hardware

Switch with:
- 4 x High performance switch
- 48 x 10GbE ports,
- 4 x 40 GbE ports.

Storage Hardware Requirements

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

### Integrated Storage Platform
- Integrated Storage can group together any number of drives across any compute resource. We strongly recommend a minimum of 2 drives per compute resource to enable redundant data store configurations.
- at least 1 dedicated NIC assigned per compute resource for the storage network (SAN)
- IGMP snooping must be disabled on storage switch for storage network

### Local Storage Only
- minimum 1 dedicated partition in each compute resource
- separate disk from the primary OS drive recommended

### Enterprise SAN
- centralised Block Storage SAN (iSCSI, ATA over Ethernet or Fibre Channel) accessible to every compute resource
- at least 1 dedicated 1Gbit/s NIC assigned per compute resource for the SAN
- multiple NICs bonded or 10GBit/s ethernet recommended

Hardware Requirements for HA

For information about hardware requirements for HA refer to the Suggested Specifications section of Get Started for Clouds with High Availability guide.

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 7 Xen compute resources and CentOS 5 KVM compute resources.
- CentOS 5 is only supported for OnApp versions up to 5.3.

Supported server configuration

- XEN Compute resources CentOS 5.x x64 or CentOS 6.x x64
- KVM Compute resources CentOS 5.x x64, CentOS 6.x x64, CentOS 7.x x86/64
- OnApp Control Panel Server CentOS 5.x x86/X64, CentOS 6.x x86/64, CentOS 7.x x86/64
- OnApp Backup Server CentOS 5.x x64, CentOS 6.x x64, CentOS 7.x x86/64
- Integrated Storage 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

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:on 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 CDN Configuration

**See also:**

Server Config Reminder - supported versions of the servers
Supported Functionality
Recommended Network Configurations
Suggested Specifications
Types of Cloud Service with OnApp

---

For Xen/KVM Cloud
Xen/KVM Cloud Using OnApp Storage (Integrated Distributed SAN)

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 separated VLANs per each bond pair for that switch.
Baremetal Server Cloud
Smart Server Cloud

Mixed Smart/Baremetal Server Cloud
CDN Configuration
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
OnApp Cloud 5.4 Get Started Guide

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

Supported Functionality

This page lists the supported features depending on the type of the cloud.

For the list of requirements for the different components of the cloud, refer to Suggested Specifications.

Please, be aware that OnApp supports the following:

- Two latest versions of most popular browsers are supported (Google Chrome and Firefox)
- Opera is not supported
Preparation Guide

This document describes how to prepare the OnApp Cloud 5.4 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:

1. Configure networks
2. Configure storage
3. Configure servers

Each step is explained in the following sections. If you have questions after reading this guide, see Getting Support section.

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.
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**.

Configure Storage

Configuring storage is highly important when preparing the cloud for the installation. Depending on the storage setup type, the installation requirements vary.
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 ATAoE, or an 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 Cloud 5.4 Get Started Guide

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:

- Integrated Storage can group together any number of drives across any compute resource. We strongly recommend a minimum of 2 drives per compute resource to enable redundant datastore configurations.
- SSD drives are recommended for best performance.
- At least 1 dedicated NIC assigned per compute resource for the storage network (SAN).
- Multiple NICs bonded or 10Gbit/s Ethernet (recommended).
- MTU on storage NIC: 9000 (recommended).
- IGMP snooping must be disabled on storage switch for storage network.

Enabling jumbo frames MTU > 1500, up to a maximum of 9000, requires NIC and switch support. Ensure that your network infrastructure has jumbo frame support and that jumbo frames are enabled in any switches. Otherwise leave MTU as default 1500 for storage NICs. Additionally, MTU must be equal for all storage NICs for compute resources, including for Backup servers.

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

Integrated storage uses a certain RAM amount on each compute resource, but the exact RAM amount depends on the number of drives and controllers which will be configured.

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 the 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.

On this page:
- Server Installation Requirements
- Control Panel Server
- Backup Server
- Compute Resource Servers
- CloudBoot 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 7 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.
- When installing CentOS, do not use a partition scheme that will allocate the majority of disk space to a dedicated /home partition leaving the root partition a small amount of space. Instead, the majority of disk space should be allocated to the root partition or a dedicated /onapp partition.

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 VSSs cannot migrate/failover to a KVM compute resource and KVM VSSs cannot migrate/failover to a XEN compute resource.

Supported server configuration

- **XEN Compute resources** CentOS 5.x x64 or CentOS 6.x x64
- **KVM Compute resources** CentOS 5.x x64, CentOS 6.x x64 or CentOS 7.x x86/64
- **OnApp Control Panel Server** CentOS 5.x x64, CentOS 6.x x64 or CentOS 7.x x86/64
- **OnApp Backup Server** CentOS 5.x x64, CentOS 6.x x64 or CentOS 7.x x86/64
- **Integrated Storage** CentOS 5.x x64 (only if running on Xen 3.x), CentOS 6.x x64, CentOS 7.x x64 (only if running on KVM)

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 x64/64
- **OnApp Backup Server** CentOS 6.x x64
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

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 VSs 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
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.

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. Configure Cloud

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

Installation Guide

This document describes how to install the 5.4 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. Configure vCloud director integration

Post install configuration

1. 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.

- 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
To install Control Panel server, perform the following procedure:

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

2. Download OnApp YUM repository file:
   
   ```bash
   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.4.noarch.rpm
   ```

3. Install OnApp Control Panel installer package:
   
   ```bash
   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='http://templates-manager.onapp.com';
   
   SNMP_TRAP_IPS=
   
   ONAPP_VERSION="" 
   
   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)
# Use MariaDB instead of MySQL as OnApp database server (Deprecated parameter. If you set any values for this parameter, they will not take effect)

```bash
WITH_MARIADB=0
```

# Configure the database server relative amount of available RAM (Deprecated parameter. If you set any values for this parameter, they will not take effect)

```bash
TUNE_DB_SERVER=0
```

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

```bash
RUBY_GC_MALLOC_LIMIT=16000000
```

# `sysctl.conf net.core.somaxconn` value

```bash
NET_CORE_SOMAXCONN=2048
```

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

```bash
ONAPP_DB_DUMP_ROOT=""
```

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

```bash
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

```bash
ENABLE_MONIT=1
```

# If enabled (the 1 value is set) - install (if local box) and configures RabbitMQ Server (messaging system) for the vCloud support. (Deprecated parameter. If you set any values for this parameter, they will not take effect)

```bash
MYSQL_WAIT_TIMEOUT=604800
MYSQL_MAX_CONNECTIONS=500
MYSQL_PORT=3306
WITH_MARIADB=0
```
ENABLE_RABBITMQ=1

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

# Maximum allowed for uploading file size in bytes, from 0 (meaning unlimited) to 2147483647 (2GB). Default is 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
OnApp Cloud 5.4 Get Started Guide

# ssl_ciphers, ssl_protocols Nginx directives' values

SSL_CIPHERSUITES=
SSL_PROTOCOL=

5. Run the Control Panel installer:

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

Set the OPENSSL_ENABLE_MD5_VERIFY=1 environment variable if installing on RHEL/CentOS 6.x with self-signed certificates. So the installer command should look like:

```bash
# export OPENSSL_ENABLE_MD5_VERIFY=1 &&
/onapp/onapp-cp-install/onapp-cp-install.sh -i SNMP_TRAP_IPS
```

The full list of Control Panel installer options:

**Usage:**

```
/onapp/onapp-cp-install/onapp-cp-install.sh -hUsage:
/onapp/onapp-cp-install/onapp-cp-install.sh [-c CONFIG_FILE]
[--redis-host=REDIS_HOST] [--redis-password=REDIS_PASSWORD]
```

**Where:**

<table>
<thead>
<tr>
<th>Database server options</th>
<th>Default database SQL server is MySQL Server. Please use one of the following option to install locally.</th>
</tr>
</thead>
<tbody>
<tr>
<td>--mariadb</td>
<td>MariaDB Server</td>
</tr>
<tr>
<td>--percona</td>
<td>Percona Server</td>
</tr>
<tr>
<td>--percona-cluster</td>
<td>Percona Cluster</td>
</tr>
<tr>
<td>MYSQL_*</td>
<td>Options are useful if MySQL is already installed and configured.</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>-m MYSQL_HOST</td>
<td>MySQL host. Default is 'localhost'</td>
</tr>
<tr>
<td>-p MYSQL_PASSWD</td>
<td>MySQL password. Random is generated if is not set or specified.</td>
</tr>
<tr>
<td>-d MYSQL_DB</td>
<td>OnApp MySQL database name. Default is 'onapp'</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=REDIS_HOST</td>
<td>IP address/FQDN where Redis Server runs. The Redis Server will be installed and configured on the current box if localhost/127.0.0.1 or box's public IP address (listed in SNMP_TRAP_IPS) is specified. If local Redis, it will serve as well on the unix socket '/tmp/redis.sock'. Default value is 127.0.0.1.</td>
</tr>
<tr>
<td>--redis-port=REDIS_PORT</td>
<td>Redis Server listen port. Defaults are: 0 - if local server 6379 - if remote server</td>
</tr>
<tr>
<td>--redis-passwd=REDIS_PASSWD</td>
<td>Redis Server password to authenticate. Random password is generated if the option's argument isn't specified. By default no password is used for local Redis.</td>
</tr>
<tr>
<td>--redis-sock=REDIS_PATH</td>
<td>Path to the Redis Server's socket. Used if local server only. Default is /tmp/redis.sock</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ADMIN_*</th>
<th>Options are used to configure OnApp Control Panel administrator data. Please note, that these options are for NEW INSTALL only and not for upgrade</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>
</tbody>
</table>

| --rbthost RBT_HOST | IP address/FQDN where RabbitMQ Server runs. The RabbitMQ will be installed and configured on the current box if localhost/127.0.0.1 or box's public IP address (enlisted in SNMP_TRAP_IPS) Default values are 127.0.0.1. |

<table>
<thead>
<tr>
<th>VCD_*</th>
<th>Options are useful if vCloud/RabbitMQ are already installed and configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>--vcdlogin VCD_LOGIN</td>
<td>RabbitMQ/vCloud user. Default value is 'rbtvcd'.</td>
</tr>
<tr>
<td>--vcdpasswd VCD_PASSWD</td>
<td>RabbitMQ/vCloud user password. The random password is generated if isn't specified.</td>
</tr>
<tr>
<td>--vcdvhost VCD_VHOST</td>
<td>RabbitMQ/vCloud vhost. Default value is '/'</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RBT_*</th>
<th>Options are used to configure RabbitMQ manager account. If local RabbitMQ server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>--rbtlogin RBT_LOGIN</td>
<td>RabbitMQ manager login. The default value is 'rbtmgr'.</td>
</tr>
<tr>
<td>--rbtpasswd RBT_PASSWD</td>
<td>RabbitMQ manager password. The random password is generated if isn't specified.</td>
</tr>
</tbody>
</table>

| -v ONAPP_VERSION | Install custom OnApp CP version |
6. Install Cloudboot dependencies:

Depending on the needed compute resource type, you should install onapp-ramdisk-DISTRO-FLAVOR package(s), where:

DISTRO - CentOS5, CentOS6 or CentOS7
FLAVOR - XEN, KVM

It is required to install `yum install onapp-ramdisk-centos7-default` together with onappstore packages.

It is recommended to install all packages. Below you can find an example:

```
bash#> # yum install onapp-ramdisk-centos7-default
bash#> # yum install onapp-ramdisk-centos6-kvm
bash#> # yum install onapp-ramdisk-centos5-xen
bash#> # yum install onapp-ramdisk-centos6-xen
bash#> # yum install onapp-ramdisk-centos7-kvm
bash#> /onapp/onapp-store-install/onapp-store-install.sh
```

After `onapp-ramdisk-centos7-default` installation the following packages will be installed automatically:

`onapp-store-
install onapp-
ramdisk-tools`

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 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#> service onapp restart
```

9. After you have installed the Control Panel server, configure your Cloud Settings. See Configure Cloud for details.
10. If you plan to configure an Accelerator, run the following command:
   - For all compute resources:
     
     ```
     rake hypervisor:messaging:configure
     ```
   - For certain compute resources only:
     
     ```
     rake hypervisor:messaging:configure['11.0.50.111 11.0.50.112']
     ```

   To perform the configuration for a number of compute resources, separate their IPs with a space.

   The command above runs on compute resources that are online. If some compute resources are offline, you should run the command again when they are online.

   The `rabbitmq_host` parameter in the `on_app.yml` file should contain the real IP address of the server with RabbitMQ installed. The `rabbitmq_host` parameter should not be set to 'localhost' or '127.0.0.1'.

   The server with RabbitMQ installed should be available from the compute resources.

   For information on manual configuration for Accelerator, refer to [RabbitMQ Configuration for Accelerator](#).

---

**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 > Configure vCloud Director Integration > 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

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
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.
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/backup` 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.

   **Perform the following steps if you plan to deploy Accelerator. Otherwise skip.**

9. Run the following command on the CP server:
   - For all compute resources:
     ```bash
     rake hypervisor:messaging:configure
     ```
   - For certain compute resources only:
     ```bash
     rake hypervisor:messaging:configure['11.0.50.111 11.0.50.112']
     ```

   To perform the configuration for a number of compute resources, separate their IPs with a space.

10. The command above should be run after every reboot. However, you can avoid the necessity to run the command repeatedly after every reboot by copying the following information (using your parameters) from `/home/mq/onapp/messaging/credentials.yml` to the custom config.
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.

For information on manual configuration for Accelerator, refer to RabbitMQ Configuration for Accelerator.
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 hardware must meet the following requirements for Ethernet mode
  - utilization: VPI enabled switches (including a proper license key).
  - VPI adapter cards (HCAs).
- Be aware that InfiniBand is not supported for CloudBoot CentOS7 image due to lack of integrated OFED stack.

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.
**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, CentOS 6.x x64 or CentOS 7.x x86/64
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 resource
   Make sure the compute resource is visible in the Control Panel, and at this point showing as inactive.
2. Update your server:
   ```bash
   bash# yum update
   ```
3. Download the OnApp repository:
   ```bash
   bash#> rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.4.noarch.rpm
   ```
4. Install the OnApp compute resource installer package:
   ```bash
   bash#> yum install onapp-hv-install
   ```
5. Update OS components using the following command:
   **For XEN**
   ```bash
   bash# /onapp/onapp-hv-install/onapp-hv-xen-install.sh -y
   ```
   or
   **For KVM**
6. Edit custom compute resource configuration. Custom values must be set before the installer script runs.

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.

# 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 compute resource
  
  NTP_TIME_SERVER='pool.ntp.org'

- Xen HV (Domain-0) related configuration
  
  XEN_DOM0_MEM_MIN=409600
  XEN_DOM0_MEM_DEVISOR=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 compute resource’s (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:

   -c CONFIG_FILE   custom installer configuration file. Otherwise, preinstalled one is used.
   -a               do NOT be interactive. Process with automatic installation.
   -v HV_VERSION    custom Compute resource Tools version
   -p 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:
8. Configure the compute resource for your cloud. This step is also required for the SNMP statistics receiver configuration:

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

```
```

- 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>
</tbody>
</table>

If unsure, set the Control Panel server’s management IP as **CP_HOST_IP** and **FILE_TRANSFER_SERVER_IP**.

- Install AoE
- Install sshfs
- Print this help info

9. Run the following commands:

```
# yum install gdisk lsblk-wrapper
```

10. Reboot the compute resource to complete the installation:

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

11. 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.

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

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

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

14. 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

15. 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 resources' iso_path_on_hv locations. This can be a backup server to avoid the excess usage of the Control Panel's space.

16. Reboot static compute resources.

If you do not have the /home/mq/onapp/messaging/credentials.yml file on your compute resources and plan to deploy an Accelerator, run the following command on the CP server:

- For all compute resources:

  rake hypervisor:messaging:configure

- For certain compute resources only:

  rake hypervisor:messaging:configure['11.0.50.111
  11.0.50.112']
Install Data Stores

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

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

   Replace xxx with the real device.

4. Create the volume group:

   bash#> vgcreate onapp-IDENTIFIER /dev/xxx

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

5. Test 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%).
   - **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.

   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.

   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-5.4.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**
   ```
   BK_VERSION=""
   ```

   **OnApp StorageAPI custom version**
   ```
   API_VERSION=""
   ```

   **Default server to synch time on the HV**
   ```
   NTP_TIME_SERVER='pool.ntp.org'
   ```

   **The number of retries for WGET to download the file**
   ```
   WGET_TRIES=5
   ```

   **OnApp templates directory.**

   Please refer to the corresponding settings at OnApp Control Panel web interface
6. 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
   bash# sh /onapp/onapp-bk-install/onapp-bk-install.sh
   ```

   **The full list of installer options:**
   
   **Usage:**
   
   ```
   ```

   **Where:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-c</code> CONFIG_FILE</td>
<td>Custom installer configuration file. Otherwise, preinstalled one is used.</td>
</tr>
<tr>
<td><code>-a</code></td>
<td>Do NOT be interactive. Process with automatic installation.</td>
</tr>
<tr>
<td><code>-y</code></td>
<td>Update OS packages (except of OnApp provided) on the box with 'yum update'.</td>
</tr>
<tr>
<td><code>-t</code></td>
<td>Initiate Base, Load Balancer and CDN templates download.</td>
</tr>
<tr>
<td><code>-h</code></td>
<td>Print this info</td>
</tr>
</tbody>
</table>

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

   ```bash
   bash#> /onapp/onapp-bk-install/onapp-bk-config.sh -h <CP_HOST_IP> -p [BK_HOST_IP]
   ```

   **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 backup server.</td>
</tr>
<tr>
<td>-p BK_HOST_IP</td>
<td>FQDN or IP Address of Backup Server which will serve all stats related and other requests send by the CP_HOST_IP. Used by snmpd and StorageAPI.</td>
</tr>
<tr>
<td>-a</td>
<td>Install AoE</td>
</tr>
<tr>
<td>-i [USER:PASSWD]</td>
<td>Install iSCSI utils and configure with USER and PASSWD (if specified)</td>
</tr>
<tr>
<td>-s</td>
<td>Install sshfs</td>
</tr>
<tr>
<td>-?</td>
<td>Print this help info</td>
</tr>
</tbody>
</table>

8. Run the following commands:

```
# yum install gdisk fuse fuse-libs fuse-devel qemu-img libvmdk libvmdk-tools
```

Install CloudBoot Backup Server

CloudBoot backup servers are CloudBooted KVM compute resources that can 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: at the first step of the creation wizard choose the type - Backup (CloudBoot Provisioning and Backup Resource). Refer to the Create CloudBoot Compute resource section of the Admin guide for details.

4. Go to your Control Panel’s Settings menu, then press Backup Servers icon.

5. Click the Create Backup Server button.
6. 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)

7. 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
   bash#> unlink /onapp/templates
   bash#> ln -s /backupstorage/templates /onapp/templates
   ```
   h. Add the following to custom config file:

   ```bash
   mkdir /backupstorage
   mount /dev/sda /backupstorage
   ln -s /backupstorage/backups /onapp/backups
   unlink /onapp/templates
   ln -s /backupstorage/templates /onapp/templates
   ```
2. Update the database so that the location of the templates is known:

   a. Find the database password:

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

   b. Open the onapp database in MySQL:

   ```
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
   ```

---

**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](http://templates.repo.onapp.com/Linux/recovery-baremetal.kernel)
   - [http://templates.repo.onapp.com/Linux/recovery-baremetal.initrd](http://templates.repo.onapp.com/Linux/recovery-baremetal.initrd)
2. Place the files into the `/tftpboot/images/ramdisk-recovery/` directory.
3. Create template file `/tftpboot/pxelinux.cfg/template-baremetal-recovery` with following contents:
4. Restart the OnApp services:

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

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

![Baremetal Server details](image)

**Configure vCloud Director Integration**

This section is the part of the OnApp installation procedure.
OnApp Cloud 5.4 Get Started Guide

The vCloud Director integration is included by default into the OnApp installer. Perform the following steps to install vCloud Director:

- RabbitMQ And OnApp Control Panel Connection
- Import of vCloud Director resources into OnApp

**RabbitMQ And OnApp Control Panel Connection**

OnApp vCD integration requires the use of RabbitMQ to keep vCD and OnApp synchronised. If you plan using the RabbitMQ server installed by OnApp by default, there is no need for additional configuration in OnApp Control Panel. Though, it is required that you edit the AMQP settings in vCD.

**To specify RabbitMQ settings in vCD:**

1. Go to your OnApp Control Panel server.
2. Open the `/onapp/interface/config/on_app.yml` file.
3. Find the RabbitMQ parameters:
   - `rabbitmq_login`
   - `rabbitmq_password`
   - `rabbitmq_vhost`
   - `rabbitmq_host` - make sure it is reachable by vCloud Director
4. Edit your AMQP settings in vCD with the RabbitMQ details found at step 3:
   a. Navigate to the Administration tab of your System Organization, expand System Settings and select Extensibility.
   b. Click Enable Notifications.
   c. Add the details from OnApp.
   d. Set Exchange vcloud.

Remember that `rabbitmq_host` must be reachable by vCloud Director.

If you are running your own RabbitMQ server, it is required that you add the RabbitMQ details through the OnApp Control Panel.

**To specify RabbitMQ settings in OnApp Control Panel:**

If you want to use a separate RabbitMQ instance for vCloud Director, specify the following vCloud Director RabbitMQ parameters in the `/onapp/configuration/rabbit_mq/vcloud/credentials.yml` file:

- `:host` - RabbitMQ server IP address
- `:port` - RabbitMQ port
- `:vhost` - the name of the "virtual host" (or vhost) that specifies the namespace for entities (exchanges and queues) referred to by the protocol. Note that this is not virtual hosting in the HTTP sense.
- `:user` - RabbitMQ login
- `:password` - RabbitMQ password

If you want to use the same RabbitMQ instance both for vCloud Director and OnApp engine:

1. Go to your Control Panel's Settings menu, and click the Configuration icon.
2. Click the System tab to change the following application settings:
   - **RabbitMQ**
     - `Host` - RabbitMQ server IP address
     - `Virtual Host` - the name of the "virtual host" (or vhost) that specifies the namespace for entities (exchanges and queues) referred to by the protocol. Note that this is not virtual hosting in the HTTP sense.
     - `Login` - RabbitMQ login
     - `Password` - RabbitMQ password

You have to restart OnApp daemon after changing RabbitMQ credentials.

**Import of vCloud Director resources into OnApp**

As initial import of vCloud Director into OnApp might take a considerable amount of time, you may consider increasing the *Idle session timeout* parameter in the vCloud Director at Administration > General, to avoid the possible import failure.

See also:
- Quick vCloud Director Integration
Before you start

- Your vCD should be v8.0 or later
- vCD public addresses should be configured properly
- Make sure your OnApp cloud admin has See vApp permissions before the import
- Ensure you have a user with vApp author role created on the vCloud Director with your valid email. (Go to vCD Console > OnApp tab > Administration and right click your user)
- All vCD users should have a valid email, or else they won’t be imported
- Currently fast-provisioned virtual datacenters are not supported for vApp provisioning
- vApps and vApp Templates that have "system" owner won’t be imported
- VSs currently cannot be connected to network during provisioning
- VS passwords are not imported into OnApp
- vCloud Director system admins are not imported into OnApp and all management tasks are performed via the vCloud Director web interface.
- vCloud Director compute resource passwords are encrypted by default.

Import

To import your vCloud Director resources into OnApp:

1. Log in to OnApp CP as an administrator.
2. Set Rabbit MQ credentials for the OnApp CP and your vCloud Director.
3. Create a compute zone in which the vCloud Director compute resource will reside.

To create a compute zone:

- Go to your Control Panel’s Settings menu and click the Compute Zones icon.
- Press "+" or click the Add New Compute Zone button.
- On the screen that follows:
  - Label - give your compute zone a name
  - Server type - select a type for your zone. For vCloud Director compute zones select the Virtual Private Cloud type.
  - Location group - select the location group to which this Compute zone will be assigned
  - Failover timeout - set the time period for which the iterations will run during the failover if the compute resource does not respond
- Click the Save button.

4. Create a compute resource of a vcloud type and specify vCloud Director global system admin credentials and API URL of your vCloud Director.

To create a compute resource:

- Go to your Control Panel Settings menu.
- Click the Compute Resources icon.
- Press "+" button or click the Add New Compute Resource button underneath the list of compute resources on the screen.
- On the screen that appears:
  - Label - enter a compute resource name.
  - Compute resource type - choose a compute resource type. Select vcloud.
  - Compute zone - select the compute zone you added on Step 3.
  - Login - specify the vCloud Director system admin login
  - Password - specify the vCloud Director system admin password
  - API URL - set the vCloud Director API URL - e.g. https://example.com
  - AMQP Exchange Name - specify your vCloud Director AMQP exchange name (this can be taken in your vCloud Director instance Extensibility > Settings > Exchange)
- Click the Save button. The compute resource will be added to the system and the import will start automatically.

5. The import will start automatically. After the transaction is successfully completed, all your vCloud Director resources will be shown in OnApp. You can view log output of transaction Import vCloud to Control Panel for more import details.

This section is the part of the OnApp installation procedure.

Install Control Panel Server > Install Compute Resources > Install Data Stores > Install Backup Server > Configure vCloud Director Integration > Configure Cloud

Configure Cloud
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.

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:

- Xen compute resources can be assigned to compute zones of the Virtual and Baremetal types
- KVM compute resources can be assigned to compute resources of the Virtual and Smart types
- vCloud Director compute resources can be assigned to compute zones of the VPC type
- VMware vCenter compute resources can be assigned to compute zones of the Virtual type

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:

bash#> pvcreate --metadatasize=50M /dev/sda5
bash#> vgcreate onapp-ar0akk2wyer3tf /dev/sda5

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 Backup Servers

If you plan to use backup servers to store such items as, for example, templates, ISOs or backups, you need to add backup servers and backup server zones to your cloud. After that, attach the newly created backup server to backup server zone you've added.

6. 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 or compute zone (Step 2). You also need to assign
7. Configure Templates

To built Linux virtual servers you need to download templates using the UI downloader. For this, install XEN and KVM templates and create a template store. You should also add the installed templates to that template store.

8. Configure ISOs

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

Quick vCloud Director Integration

If you wish to deploy only the vCD integration model, you only need to install the Control Panel server, configure Rabbit MQ, and import vCloud Director.

See also:

Full Cloud Installation

On this page:

- Install/Update Control Panel Server
- Configure RabbitMQ And OnApp Control Panel Connection
- Import of vCloud Director resources into OnApp

- As initial import of vCloud Director into OnApp might take a considerable amount of time, you may consider increasing the idle session timeout parameter in the vCloud Director at Administration > General, to avoid the possible import failure.
- It is recommended to have vCloud Director and OnApp Control Panel in one network.

Install/Update Control Panel Server

To install/update control panel server:

1. Update your server:

   ```bash
   # yum update
   ```

2. Download OnApp YUM repository file:

   ```bash
   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.2.noarch.rpm
   ```
3. Install OnApp Control Panel installer package:

   bash#> yum install onapp-cp-install

4. Edit the /onapp/onapp-cp.conf file to set Control Panel custom values. Custom values must be set before the installer script runs.

   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

Ensure that the SNMP_TRAP_IP should be the management IP of your CP server.

If you are upgrading from 4.1 OnApp version, run Control Panel installer with specified rake task:

   # /onapp/onapp-cp-install/onapp-cp-install.sh
   --rake='vcloud:resync'

**vCD and Rabbit MQ options**
The installer will automatically install/upgrade RabbitMQ server on the CP's box and configure it if no options are specified. Consider the options below for Rabbit MQ configuration if it is already installed on server separate from CP.

<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 and configured on the current box if localhost/127.0.0.1 or box's public IP address (enlisted in SNMP_TRAP_IPS). Default values is 127.0.0.1.</td>
</tr>
<tr>
<td>RBT_HOST</td>
<td></td>
</tr>
<tr>
<td>VCD_*</td>
<td>These options are useful if vCloud Director/RabbitMQ is already installed and configured.</td>
</tr>
<tr>
<td>--vcdlogin</td>
<td>RabbitMQ/vCloud Director user. Default value is 'rbtvcd'.</td>
</tr>
<tr>
<td>VCD_LOGIN</td>
<td></td>
</tr>
<tr>
<td>--vcdpasswd</td>
<td>RabbitMQ/vCloud Director user password. The random password is generated if isn't specified.</td>
</tr>
<tr>
<td>VCD_PASSWD</td>
<td></td>
</tr>
<tr>
<td>--vcdvhost</td>
<td>RabbitMQ/vCloud Director vhost. Default value is '/'</td>
</tr>
<tr>
<td>VCD_VHOST</td>
<td></td>
</tr>
<tr>
<td>RBT_*</td>
<td>These options are used to configure RabbitMQ manager account. If local RabbitMQ server.</td>
</tr>
<tr>
<td>--rbtlogin</td>
<td>RabbitMQ manager login. The default value is 'rbtmgm'.</td>
</tr>
<tr>
<td>RBT_LOGIN</td>
<td></td>
</tr>
<tr>
<td>--rbtpasswd</td>
<td>RabbitMQ manager password. The random password is generated if isn't specified.</td>
</tr>
<tr>
<td>RBT_PASSWD</td>
<td></td>
</tr>
</tbody>
</table>

6. Install OnApp license to activate the Control Panel:

   Enter a valid license key via the Web UI (you'll be prompted to do so). Once you have entered a license it can take up to 15 minutes to activate.

7. Restart the OnApp service:
8. Once the installation of the Control Panel is complete, your default OnApp login will be admin/changeme. The password can be changed via the Control Panel’s Users menu.

- Installer output is redirected to ./onapp-cp-install.log
- All installer critical errors are in /var/log/messages

Configure RabbitMQ And OnApp Control Panel Connection

OnApp vCD integration requires the use of RabbitMQ to keep vCD and OnApp synchronised. If you plan using the RabbitMQ server installed by OnApp by default, there is no need for additional configuration in OnApp Control Panel. Though, it is required that you edit the AMQP settings in vCD.

To specify RabbitMQ settings in vCD:

1. Go to your OnApp Control Panel server.
2. Open the /onapp/interface/config/on_app.yml file.
3. Find the RabbitMQ parameters:
   - rabbitmq_login
   - rabbitmq_password
   - rabbitmq_vhost
   - rabbitmq_host - make sure it is reachable by vCloud Director
4. Edit your AMQP settings in vCD with the RabbitMQ details found at step 3:
   a. Navigate to the Administration tab of your System Organization, expand System Settings and select Extensibility.
   b. Click Enable Notifications.
   c. Add the details from OnApp.
   d. Set Exchange vcloud.

Remember that rabbitmq_host must be reachable by vCloud Director.

If you are running your own RabbitMQ server, it is required that you add the RabbitMQ details through the OnApp Control Panel.

To specify RabbitMQ settings in OnApp Control Panel:

If you want to use a separate RabbitMQ instance for vCloud Director, specify the following vCloud Director RabbitMQ parameters in the /onapp/configuration/rabbit_mq/vcloud/credentials.yml file:

- :host: - RabbitMQ server IP address
- :port: - RabbitMQ port
- :vhost: - the name of the "virtual host" (or vhost) that specifies the namespace for entities (exchanges and queues) referred to by the protocol. Note that this is not virtual hosting in the HTTP sense.
- :user: - RabbitMQ login
- :password: - RabbitMQ password

If you want to use the same RabbitMQ instance both for vCloud Director and OnApp engine:

1. Go to your Control Panel’s Settings menu, and click the Configuration icon.
2. Click the System tab to change the following application settings:
   RabbitMQ
   - Host - RabbitMQ server IP address
   - Virtual Host - the name of the "virtual host" (or vhost) that specifies the namespace for entities (exchanges and queues) referred to by the protocol. Note that this is not virtual hosting in the HTTP sense.
   - Login - RabbitMQ login
   - Password - RabbitMQ password

You have to restart OnApp daemon after changing RabbitMQ credentials.
Import of vCloud Director resources into OnApp

Before you start

- Your vCD should be v8.0 or later
- vCD public addresses should be configured properly
- Make sure your OnApp cloud admin has See vApp permissions before the import
- Ensure you have a user with vApp author role created on the vCloud Director with your valid email. (Go to vCD Console > OnApp tab > Administration and right click your user)
- All vCD users should have a valid email, or else they won’t be imported
- Currently fast-provisioned virtual datacenters are not supported for vApp provisioning
- vApps and vApp Templates that have “system” owner won’t be imported
- VSs currently cannot be connected to network during provisioning
- VS passwords are not imported into OnApp
- vCloud Director system admins are not imported into OnApp and all management tasks are performed via the vCloud Director web interface.
- vCloud Director compute resource passwords are encrypted by default.

Import

To import your vCloud Director resources into OnApp:

1. Log in to OnApp CP as an administrator.
2. Set Rabbit MQ credentials for the OnApp CP and your vCloud Director.
3. Create a compute zone in which the vCloud Director compute resource will reside.

To create a compute zone:
   a. Go to your Control Panel's Settings menu and click the Compute Zones icon.
   b. Press "+" or click the Add New Compute Zone button.
   c. On the screen that follows:
      i. **Label** - give your compute zone a name
      ii. **Server type** - select a type for your zone. For vCloud Director compute zones select the Virtual Private Cloud type.
      iii. **Location group** - select the location group to which this Compute zone will be assigned
      iv. **Failover timeout** - set the time period for which the iterations will run during the failover if the compute resource does not respond
   d. Click the Save button.

4. Create a compute resource of a vcloud type and specify vCloud Director global system admin credentials and API URL of your vCloud Director.

To create a compute resource:
   a. Go to your Control Panel Settings menu.
   b. Click the Compute Resources icon.
   c. Press "+" button or click the Add New Compute Resource button underneath the list of compute resources on the screen.
   d. On the screen that appears:
      • **Label** - enter a compute resource name.
      • **Compute resource type** - choose a compute resource type. Select vcloud.
      • **Compute zone** - select the compute zone you added on Step 3.
      • **Login** - specify the vCloud Director system admin login
      • **Password** - specify the vCloud Director system admin password
      • **API URL** - set the vCloud Director API URL - e.g. https://example.com
      • **AMQP Exchange Name** - specify your vCloud Director AMQP exchange name (this can be taken in your vCloud Director instance Extensibility > Settings > Exchange)
   e. Click the Save button. The compute resource will be added to the system and the import will start automatically.

5. The import will start automatically. After the transaction is successfully completed, all your vCloud Director resources will be shown in OnApp. You can view log output of transaction Import vCloud to Control Panel for more import details.

Remember that `rabbitmq_host` must be reachable by vCloud Director.
Upgrade Guide for Cloud with CloudBooted Servers

This guide presents the complete walk-through how to upgrade OnApp Cloud v5.3 to the v5.4 for the cloud configuration where all servers are CloudBooted except Control Panel server. Please follow the complete procedure of the upgrade process. All packages (Control Panel, CloudBoot, Compute resources) must belong to the same major version to ensure the best performance of your cloud.

Important Notes

1. You must be running the latest patch of OnApp 5.3 version to upgrade to 5.4 version. If you are using an earlier version, please upgrade to 5.3 first.
2. 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.
3. Make sure no Control Panel files are open for editing under the root user account.
4. If you plan to deploy Accelerator, refer to the RabbitMQ Configuration for Accelerator document for more details.
5. Be aware that from now on, OnApp Licensing has a standalone client. Use only 443 port to connect from Control Panel to licensing server.
6. We strongly recommend that you test all your custom scripts before upgrading your production environment.
7. Be aware that OnApp does not support UEFI on static compute resources. You should disable UEFI on your compute resources before installing OnApp.
8. If you are using the auto healing functionality for Integrated Storage, make sure to disable it before an upgrade.
9. If you are using Integrated Storage, refer to the OnApp IS Upgrade Paths for more information about the upgrade details.

Check Your Cloud Configuration

Please note

- At the moment, vCloud system admins are not imported into OnApp and all management tasks are performed via the vCloud Director web interface.
- V5 passwords are not imported into OnApp.
- vCloud compute resource passwords are encrypted by default.
Starting with OnApp 5.4, networks are made up of sub-networks called IP nets which contain ranges of IP addresses. To make your system compatible with the new networking scheme, a rake task will run with the installer. The rake task will modify your networks to contain IP ranges and IP nets. If a network contains two or more consecutive IP addresses of the same range of addresses, they will be united into one IP range. Individual IPs will each constitute an IP range. For each of the IP ranges an IP net will be added to the network. If at least one conflict is found in the configuration, the cloud will not be updated. If your cloud configuration is correct, the CP installer will be run and your networks will be modified to include IP nets and IP ranges.

Prior to the update procedure, it is required to check your cloud configuration. The cloud should comply with the following requirements for a successful upgrade:

- all VLANs indicated for the networks in the cloud should have a relevant value. The value for VLAN should not exceed 4095.
- all networks which have one or several IP addresses assigned to user(s) should be within a network zone
- all IP addresses added to the cloud should be represented with feasible values
- all network masks should have relevant lengths
- there should be no overlapping IP addresses in a single network

If one or several of the IP address you've added to the cloud do not correspond with their prefix, the system will offer to switch on the force option. When the force option is enabled, the system will automatically change the IP address to correspond with their prefix. For example, if you've had a 198.168.0.1/255.255.0.0 IP address with 8 as its prefix, the system will change the address to 198.168.0.1/255.0.0.0.

If any inconsistencies are detected in your system, the update procedure will stop and the networks will undergo no changes. In such a case, you need to address the issues that have been found and run the CP installer again. If it is not possible to fix the cloud configuration, please, contact our support team.

If the configuration of the cloud meets the requirements listed above, the update to OnApp 5.4 will go smoothly, and all networks will be modified to include IP nets and IP ranges.

When you run the Control Panel installer the system will check your configuration. You can view the log at log/ip_consistency_check.log. If any inconsistencies are found, the log might contain any of the following warning messages:

- an incorrect VLAN for a network has been detected. The ID and label of the network will be provided.
- a network that has an IP address assigned to a user and which is not in a network zone has been detected. The ID of the network, the ID of the assigned IP address and the ID of the user to whom the IP is assigned will be provided.
- an IP address which is represented incorrectly has been detected. The ID of the IP address will be provided.
- an IP address which does not correspond with its prefix has been detected. The ID of the network, the ID of the IP address and the existing and expected prefixes will be provided.
- overlapping IP addresses have been detected in one network. The IP addresses and the network ID will be provided.

Upgrade Control Panel Server

- CP installer for Installation and Upgrade contains a new -D option enabling to avoid OnApp database dumping during the install/upgrade.
- To increase the cloud performance we recommend setting RUBY_GC_MALLOC_LIMIT parameter in custom configurations to 16 millions. For more information on RUBY_GC_MALLOC_LIMIT parameter, refer to Ruby's GC Configuration and Garbage Collection articles.
- Installer output is redirected to ./onapp-cp-install.log
- All installer critical errors are in /var/log/messages
- Custom values must be set before the installer script runs.
- 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.

To upgrade your Control Panel server:

1. Download and install the latest OnApp YUM repository file:
2. Upgrade OnApp Control Panel installer package:

   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.4.noarch.rpm

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

   # yum update onapp-cp-install

4. (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 (Deprecated parameter. If you set any values for this parameter, the

   WITH_MARIADB=0
OnApp Cloud 5.4 Get Started Guide

# Configure the database server relative amount of available RAM

TUNE_DB_SERVER=1

# 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 UserKnownHostsFi
PasswordAuthentication=no"
KEEP_DUMPS=168
DB_DUMP_CRON='40 * * * *'

# Enable monit - tool for managing and monitoring Unix systems

ENABLE_MONIT=1

# If enabled (the 1 value is set) - install (if local box) and configures RabbitMQ Server (messaging system) for the vCloud support. parameter, they will not take effect)

ENABLE_RABBITMQ=1

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

TRANS_LOGS_ROTATE_TIME=30

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

```
SSLCIPHERSUIT=
SSLPROTOCOL=
```
5. Run Control Panel installer:

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

The full list of Control Panel installer options:

**Usage:**

```
/onapp/onapp-cp-install/onapp-cp-install.sh -h
```

**Where:**

<table>
<thead>
<tr>
<th>Database server options:</th>
<th>Default database SQL server is MySQL Server. Please use one of the following option to install LOCALLY.</th>
</tr>
</thead>
<tbody>
<tr>
<td>--mariadb</td>
<td>MariaDB Server</td>
</tr>
<tr>
<td>--percona</td>
<td>Percona Server</td>
</tr>
<tr>
<td>--percona-cluster</td>
<td>Percona Cluster</td>
</tr>
</tbody>
</table>

**MySQL_***

Options are useful if MySQL is already installed and configured.

-`-m MYSQL_HOST`  MySQL host. Default is 'localhost'

-`--mysql-port=MYSQL_PORT`  TCP port where MySQL Server serves connections. Default values is 3306 for the local installation

-`--mysql-sock[=MYSQL.SOCK]`  Unix socket on which MySQL Server serves connections. Default values is /var/lib/mysql/mysql.sock. Used if local server only. The socket is unset if the option's argument isn't specified.

-`-p MYSQL_PASSWD`  MySQL password. Random is generated if is not set or specified.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d MYSQL_DB</td>
<td>OnApp MySQL database name. Default is ‘onapp’</td>
</tr>
<tr>
<td>-u MYSQL_USER</td>
<td>MySQL user. Default is ‘root’</td>
</tr>
<tr>
<td>REDIS_*</td>
<td>Options are useful if Redis Server is already installed and configured.</td>
</tr>
<tr>
<td>--redis-host=REDIS_HOST</td>
<td>IP address/FQDN where Redis Server runs. The Redis Server will be installed and configured on the current box if localhost/127.0.0.1 or box’s public IP address (listed in SNMP_TRAP_IPS) is specified. If local Redis, it will serve as well on the unix socket ‘/tmp/redis.sock’. Default value is 127.0.0.1.</td>
</tr>
<tr>
<td>--redis-bind[=REDIS_BIND]</td>
<td>The IP address for Redis Server to serve connections (to listen). The option is not mandatory.</td>
</tr>
<tr>
<td>--redis-port=REDIS_PORT</td>
<td>Redis Server listen port. Defaults are: 0 - if local server 6379 - if remote server</td>
</tr>
<tr>
<td>--redis-passwd[=REDIS_PASSWD]</td>
<td>Redis Server password to authenticate. Random password is generated if the option’s argument isn’t specified. By default no password is used for local Redis.</td>
</tr>
<tr>
<td>--redis-sock[=REDIS_SOCK]</td>
<td>Path to the Redis Server’s socket. Used if local server only. Default is /tmp/redis.sock. The socket is unset if the option’s argument is not specified.</td>
</tr>
<tr>
<td>ADMIN_*</td>
<td>Options are used to configure OnApp Control Panel administrator data. 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>
<tr>
<td>--rbthost RBT_HOST</td>
<td>IP address/FQDN where RabbitMQ Server runs. The RabbitMQ will be installed and configured on the current box if localhost/127.0.0.1 or box’s public IP address (listed in SNMP_TRAP_IPS) are specified. Default values are 127.0.0.1.</td>
</tr>
<tr>
<td>VCD_*</td>
<td>Options are useful if vCloud/RabbitMQ are already installed and configured.</td>
</tr>
<tr>
<td>--vcdlogin VCD_LOGIN</td>
<td>RabbitMQ/vCloud user. Default value is ‘rbtvcd’.</td>
</tr>
<tr>
<td>--vcdpasswd VCD_PASSWD</td>
<td>RabbitMQ/vCloud user password. The random password is generated if isn’t specified.</td>
</tr>
<tr>
<td>--vcdvhost VCD_VHOST</td>
<td>RabbitMQ/vCloud vhost. Default value is ‘/’</td>
</tr>
<tr>
<td>RBT_*</td>
<td>Options are used to configure RabbitMQ manager account. If local RabbitMQ server.</td>
</tr>
<tr>
<td>--rbllogin RBT_LOGIN</td>
<td>RabbitMQ manager login. The default value is ‘rbtmgr’.</td>
</tr>
<tr>
<td>--rbtpasswd RBT_PASSWD</td>
<td>RabbitMQ manager password. The random password is generated if isn’t specified.</td>
</tr>
<tr>
<td>--ha-install</td>
<td>Proceed with Control Panel and High Availability components installation</td>
</tr>
<tr>
<td>--rake RAKE_TASKS</td>
<td>List of OnApp Control Panel rake tasks (separated with space) to run at the very end of install or upgrade.</td>
</tr>
<tr>
<td>-v ONAPP_VERSION</td>
<td>Install custom OnApp CP version</td>
</tr>
</tbody>
</table>
**SNMP_TRAP_IPS**

IP addresses separated with coma for snmp to trap

- The `-i` option has higher priority than 'on_app.yml'/'onapp-cp.conf' files.
- In case of the Control Panel upgrade with the `-i` option the snmp address will be overwritten in the `on_app.yml`/`onapp-cp.conf` files.
- During the Control Panel upgrade without the `-i` option the `on_app.yml` file has higher priority than the `onapp-cp.conf` file.
- In this case the snmp address will be taken from the `on_app.yml` file and the `onapp-cp.conf` file will be overwitten.

**CONFIG_FILE**

Custom installer configuration file. Otherwise, preinstalled one is used.

**-y**

update OS packages (except of OnApp provided) on the box with `yum update`.

**-a**

Do not be interactive. Process with automatic installation. Please note, this will continue OnApp Control Panel install/upgrade even if there is transaction currently running.

**-t**

Add to the database and download Base Templates. For new installs only. If this option is not used, then only the following mandatory System Templates will be added by default during fresh install: OnApp CDN Appliance; Load Balancer Virtual Appliance; Application Server Appliance.

**--noservices**

Do not start OnApp services: monit, onapp and httpd.

Please note, crond and all OnApp's cron tasks remain running. They could be disabled by stopping crond service manually for your own risk.

**-D**

do not make database dump, and make sure it is disabled in the cron and not running at the moment

**-h**

print this info

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.

---

**Upgrade CloudBoot Packages**

Create a backup of the `/tftpboot` directory in case storage packages rollback will be needed.

To upgrade the OnApp Storage packages:

1. Upgrade the repo:

```bash
CP_host#> rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.4.noarch.rpm
```

2. Upgrade the packages:

   Depending on the needed compute resource type, you should install `onapp-ramdisk-DISTRO-FLAVOR` package(s), where:

   - **DISTRO** - CentOS5, CentOS6 or CentOS7
   - **FLAVOR** - XEN, KVM

   Also it is required to install `yum install onapp-ramdisk-centos7-default` together with onappstore packages.

   It is recommended to update all packages. Below you can find an example:
Run the script:

When run in the interactive mode, enter the required information.

Upgrade CloudBoot Backup Servers

Make sure to update CloudBoot packages on your Control Panel server before proceeding to the upgrade of CloudBoot backup servers.

CloudBoot backup servers are CloudBooted KVM compute resources that can be used as backup servers. The CloudBoot backup server upgrade procedure is almost the same as the CloudBoot compute resource upgrade. Follow the instructions provided in this section to upgrade CloudBoot backup servers in your cloud.

Once you have upgraded the CloudBoot dependencies, you have to reboot your Cloud Boot compute resource to update the Cloud Boot RPM. You do not need to perform any backup server upgrade operations using console.

To do so:

1. Go to your Control Panel Settings menu.
2. Click the Compute resources icon.
3. Click the label of the CloudBoot compute resource the backup server is based on.
4. On the compute resource details screen, click the Actions button, then click Reboot Compute resource.
5. A new screen will open asking for confirmation before reboot:
   * Are you sure you want to reboot this compute resource? Confirm that you want the compute resource to reboot.
6. When you're certain you want to proceed with the reboot, click the Reboot button.
7. Repeat these steps for all CloudBoot backup servers in your cloud.
8. Once all are rebooted, proceed to CloudBoot compute resources upgrade.

Upgrade CloudBoot Compute Resources

Depending on the infrastructure, scale and needs of your cloud we suggest the following methods of upgrading CloudBoot compute resources:
Simple Reboot

Follow the below procedure to upgrade the CloudBoot compute resources with reboot:

1. **Upgrade CloudBoot Packages.**
2. When the CloudBoot packages upgrade is complete, stop all virtual servers which reside on the CloudBoot compute resources.
3. **Reboot all CloudBoot compute resources.**

Once the compute resources are rebooted, the upgrade is complete. Before starting all Virtual Servers please ensure that the diagnostics page does not report any issue. In case of any issue, please press repair button to resolve it, then continue with starting Virtual Servers.

Note that virtual servers cannot be stopped simultaneously, but must be stopped in sequence. This can result in considerable downtime if there are a large number of virtual servers.

Migrate and reboot

Use this procedure if you prefer migrating all virtual servers to another compute resource and conducting overall upgrade of your CloudBoot and Integrated Storage. Virtual servers that do not support hot migrate will have to be stopped.

Once you have upgraded the CloudBoot packages, you have to reboot your CloudBoot compute resources to update them.

To do so:

1. Migrate all the virtual servers from the CloudBoot compute resource to another compute resource. Follow the instructions described in the Migrate Virtual Server section of the Admin guide to migrate virtual servers.
2. After that, go to your Control Panel Settings menu.
3. Click the Compute Resources icon.
4. Click the label of the CloudBoot compute resource you have migrated all VSs from.
5. On the compute resource details screen, click the Actions button, then click Reboot Compute resource.

Rebooting a compute resource assigned to a data store with a single replica (single-replica compute resource) or degraded virtual disks may result in data loss.

6. A new screen will open asking for confirmation (via two check boxes) before reboot:

   - **Stop all virtual servers that cannot be migrated to another compute resource?** Check this box if you want VSs that cannot be migrated to be powered off. When a compute resource is scheduled for a reboot, OnApp will first attempt to hot migrate all VSs it hosts. If hot migration is not possible for a VS, OnApp will attempt to cold migrate that VS. With this box...
checked, if cold migration fails, the VS will be stopped so the reboot may proceed. If you don’t check this box, OnApp will attempt to hot and then cold migrate all VSs hosted by the compute resource being rebooted – but will stop the migration process if any VS cannot be migrated.

- **Are you sure you want to reboot this compute resource?** A simple confirmation to confirm that you want the compute resource to reboot.

Before the reboot, please ensure that all vdisks are fully synced and redundant. If some of them are not fully synced, the virtual server, that is owner of a degraded (or non-redundant) vdisk, can loose access to the vdisk. It can be manifested as IO errors during writes or reads to/from the vdisk inside the virtual server.

7. When you’re certain you want to proceed with the reboot, click the **Reboot** button.
8. Repeat these steps for all CloudBoot compute resources in your cloud.

### Live Upgrade

Live Upgrade is only applicable if your cloud is running latest 5.3 CloudBoot RPM.

- Live Upgrade with passthrough is currently unsupported. Passthrough to storage means that network interface will be added to the Storage Controller Server without the bond and the Storage Controller Server will have the complete control over this interface.
- Power off all Windows virtual machines and virtual backup servers before starting the live upgrade.
- If your current Storage package is 4.0, Windows virtual servers can remain running.
- During the CloudBoot compute resource live upgrade, only the control stack for managing integrated storage is upgraded. Other changes come into effect after the compute resource is next rebooted. Due to this, hot migration may fail between compute resource which is already rebooted and the one that hasn't.
- Do not make any changes to the cloud during the upgrade process!
- Any offline Cloudboot compute resources should be removed from the CP server before running live upgrade as the scripts expect to be able to speak to all compute resources during these steps.
- Please, consult OnApp IS Upgrade Paths to learn the minimum Integrated Storage version required for the current update to be performed in Live Upgrade mode.

Use this procedure to upgrade without rebooting your servers:

1. Make sure no disks are out of sync. To do so, check the Diagnostics page in CP at **Dashboard > Integrated Storage > Compute zone label > Diagnostics**. Alternatively, log into a compute resource and run the command below:

   ```
   HV_host#> getdegradedvdisk
   ```

2. Repair all the degraded disks before proceeding to the upgrade process. To do so, log in to your CP and go to **Integrated Storage > Compute zone label > diagnostics** page. Alternatively, run one of the following commands:

   - To repair a specific vdisk, use the following command:

     ```
     HV_host#> onappstore repair uuid=
     ```

   - To repair all vdisks one by one, use the following command:

     ```
     HV_host#> repairvdisk
     ```

   - To repair all vdisks in 10 threads simultaneously, use the following command:

     ```
     HV_host#> parallelrepairvdisk
     ```
OnApp Cloud 5.4 Get Started Guide

Please note, that `parallelrepairvdisks` command performs the repairs much faster but makes an impact on the Integrated Storage SAN network. Vdisk performance may be slower during the repair.

In case you have a Cloudboot Backup Server, you can perform these commands on the Backup Server. The repairs will be triggered across all Cloudboot compute zones.

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

```
CP_host#> service onapp stop
```

4. Stop the Apache server:

```
CP_host#> service httpd stop
```

5. Make sure to update CloudBoot packages before proceeding to the following steps.

6. Run the following command from the Control Panel server terminal to display the list of compute resources with their IP addresses. Make a note of the list of IPs:

```
CP_host#> liveUpdate listHVs
```

This command will also show whether compute resources are eligible for live upgrade.

If the command `liveUpdate` is not available then it may be located in the `sbin` directory instead (cd /usr/local/sbin).

7. Run the following command for every compute resource:

```
CP_host#> liveUpdate updateToolstack <HV IP Addr>
```

Once all the toolstacks are updated run the following command for every compute resource:

```
CP_host#> liveUpdate refreshControllers <HV IP Addr>
```

Wait several minutes for all degraded disks to come to synchronized state. The synchronization will take approximately three minutes for each compute resource.

After each controller restart, check for any issues on the backup server (or on one Compute resource from each zone):

1. Log on via SSH to the backup server (or Compute resource).
2. Run `getdegradednodes` from the SSH console.
3. Run `getdegradedvdisks` from the SSH console.

8. Restarts the storage controllers. This command can be performed later at a more suitable time.

Run the following command for each compute resource in turn:

```
CP_host#> liveUpdate restartControllers <HV IP Addr>
```

Please make sure you restart all controllers and don’t leave your cloud in a partially updated state for too long. Note that when operating in LiveUpdated mode (e.g. with the tool stacks updated but before you have performed the controller restart) you cannot use disk hot plug.
9. Make sure that the package versions are upgraded by running the following command on each compute resource:

```
HV_host#> cat /onappstore/package-version.txt | grep Source
```

10. Start the Apache server:

```
CP_host#> service httpd start
```

11. Start the OnApp service:

```
CP_host#> service onapp start
```

**Local Read Policy**

Enabling Local Read on a compute zone ensures that the locally stored copy of the data will always be used for reads. This significantly reduces read latency and improves overall storage performance by reducing load on the SAN network. However, in order to use this policy every compute resource must have sufficient physical drives to be able to store the number of stripes specified in the data store. E.g. in a 2R4S data store there must be at least 4 physical disks on the compute resource to use local read.

**Changes to Local Read Policy Enforcement**

Originally, when this policy was introduced OnApp did not enforce the requirement for the minimum number of drives. Consequently, some users who set the policy having insufficient drives may see the following error message:

```
Fatal: OnApp::Actions::Fatal Storage API Call failed:
{"result":"FAILURE", "error":"Local reads have been enabled on the zone - members required per host: 4, required hosts: 2, available hosts: 0"}
```

The solution is to either add additional drives to that compute resource and then add them to the data store or to disable read local.

**Getting support for your upgrade**

You can use the information in this document to perform your own upgrade to the 5.4 version of the OnApp Cloud. However, if you have a full 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](http://forum.onapp.com).

**Upgrade Guide for Cloud with Static Servers**

This guide explains how to upgrade OnApp Cloud v5.3 to the v5.4 for the cloud where all servers are static. Follow the procedure listed below in the correct order to upgrade your cloud. All
packages (Control Panel and Compute resources) must belong to the same major version to ensure the best performance of your cloud.

Make sure that your cloud configuration meets all the requirements before upgrading to OnApp 5.4. See the Check Your Cloud Configuration section of this document for details.

**Important Notes**

1. You must be running the latest patch of OnApp 5.3 version to upgrade to 5.4 version. If you are using an earlier version, please upgrade to 5.3.
2. 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.
3. Make sure no Control Panel files are open for editing under the root user account.
4. If you plan to deploy Accelerator, refer to the RabbitMQ Configuration for Accelerator document for more details.
5. Be aware that from now on, OnApp Licensing has a standalone client. Use only 443 port to connect from Control Panel to licensing server.
6. We strongly recommend that you test all your custom scripts before upgrading your production environment.
7. Be aware that OnApp does not support UEFI on static compute resources. You should disable UEFI on your compute resources before installing OnApp.
8. If you are using the auto healing functionality for Integrated Storage, make sure to disable it before an upgrade.
9. If you are using Integrated Storage, refer to the OnApp IS Upgrade Paths for more information about the upgrade details.

**Check Your Cloud Configuration**

Starting with OnApp 5.4, networks are made up of sub-networks called IP nets which contain ranges of IP addresses. To make your system compatible with the new networking scheme, a rake task will run with the installer. The rake task will modify your networks to contain IP ranges and IP nets. If a network contains two or more consecutive IP addresses of the same range of addresses, they will be united into one IP range. Individual IPs will each constitute an IP range. For each of the IP ranges an IP net will be added to the network. If at least one conflict is found in the configuration, the cloud will not be updated. If your cloud configuration is correct, the CP installer will be run and your networks will be modified to include IP nets and IP ranges.

Prior to the update procedure, it is required to check your cloud configuration. The cloud should comply with the following requirements for a successful upgrade:

- all VLANs indicated for the networks in the cloud should have a relevant value. The value for VLAN should not exceed 4095.
- all networks which have one or several IP addresses assigned to user(s) should be within a network zone.
- all IP addresses added to the cloud should be represented with feasible values.
- all network masks should have relevant lengths.
- there should be no overlapping IP addresses in a single network.

If one or several of the IP address you’ve added to the cloud do not correspond with their prefix, the system will offer to switch on the force option. When the force option is enabled, the system will automatically change the IP address to correspond with their prefix. For example, if you’ve had a 198.168.0.1/255.255.0.0 IP address with 8 as its prefix, the system will change the address to 198.168.0.1/255.0.0.0.

If any inconsistencies are detected in your system, the update procedure will stop and the networks will undergo no changes. In
such a case, you need to address the issues that have been found and run the CP installer again. If it is not possible to fix the cloud configuration, please, contact our support team.

If the configuration of the cloud meets the requirements listed above, the update to OnApp 5.4 will go smoothly, and all networks will be modified to include IP nets and IP ranges.

When you run the Control Panel installer the system will check your configuration. You can view the log at log/ip_consistency_check.log. If any inconsistencies are found, the log might contain any of the following warning messages:

- an incorrect VLAN for a network has been detected. The ID and label of the network will be provided.
- a network that has an IP address assigned to a user and which is not in a network zone has been detected. The ID of the network, the ID of the assigned IP address and the ID of the user to whom the IP is assigned will be provided.
- an IP address which is represented incorrectly has been detected. The ID of the IP address will be provided.
- an IP address which does not correspond with its prefix has been detected. The ID of the network, the ID of the IP address and the existing and expected prefixes will be provided.
- overlapping IP addresses have been detected in one network. The IP addresses and the network ID will be provided.

**Upgrade Static Compute Resources**

At first upgrade your static compute resources.

1. Make sure your compute resource is visible and online in the Control Panel.
2. Download and install the latest OnApp YUM repository file:

   ```
   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.4.noarch.rpm
   ```

3. Upgrade OnApp compute resource installer package:

   ```
   # yum update onapp-hv-install
   ```

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

   For XEN compute resource:

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

   For KVM compute resource:

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

5. Run compute resource installer:

   For XEN compute resource:

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

   For KVM compute resource:

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

Reboot XEN compute resource, which is running on CentOS 6.x, after upgrade to newer XEN version.
6. Reboot static compute resources.
   For KVM compute resources only: the kernel package update is a part of "Upgrade Static Compute Resources" default procedure. So reboot is required, if kernel package was upgraded and customer is willing Compute Resource(s) running it (for security reason).

## Upgrade Control Panel Server

To upgrade your Control Panel server:

1. Download and install the latest OnApp YUM repository file:

   ```
   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.4.noarch.rpm
   ```

2. Upgrade OnApp Control Panel installer package:

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

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

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

4. *(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 (Deprecated parameter. If you set any values for this parameter, the
WITH_MARIADB=0

# Configure the database server relative amount of available RAM

TUNE_DB_SERVER=1

# 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=PasswordAuthentication=no"
KEEP_DUMPS=168
DB_DUMP_CRON='40 * * * *'

# Enable monit - tool for managing and monitoring Unix systems
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENABLE_MONIT=1</td>
<td>If enabled (the 1 value is set) - install (if local box) and configures RabbitMQ Server (messaging system) for the vCloud support. If the value is not set, they will not take effect.</td>
</tr>
<tr>
<td>ENABLE_RABBITMQ=1</td>
<td>Rotate transactions' log files created more than TRAN/logs ROTATE TIME day(s) ago.</td>
</tr>
<tr>
<td>TRANS_LOGS_ROTATE_TIME=30</td>
<td>Maximum allowed for uploading file size in bytes, from 0 (meaning unlimited) to 2147483647 (2GB). Default is 1GB</td>
</tr>
</tbody>
</table>
OnApp Cloud 5.4 Get Started Guide

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_UNIT_NAME='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=
5. Run Control Panel installer:

```
# vi /onapp/onapp-cp.conf
```

If the `onapp-cp.conf` file is not configured correctly, it will replace the SSL files with a self-signed even if a legitimate certificate is already installed.

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

The full list of Control Panel installer options:

Usage:

```
/onapp/onapp-cp-install/onapp-cp-install.sh -h
/onapp/onapp-cp-install/onapp-cp-install.sh [-c CONFIG_FILE]
[--mariadb | --percona | --percona-cluster] [-m MYSQL_HOST]
[--redis-host=REDIS_HOST] [--redis-bind=REDIS_BIND]
[--redis-passwd=REDIS_PASSWORD] [--redis-port=REDIS_PORT]
[-t] [--noservices] [--ha-install] [--rake=RAKE_TASKS] [-h]
```

**Where:**

<table>
<thead>
<tr>
<th>Database server options:</th>
<th>Default database SQL server is MySQL Server. Please use one of the following option to install LOCALLY.</th>
</tr>
</thead>
<tbody>
<tr>
<td>--mariadb</td>
<td>MariaDB Server</td>
</tr>
<tr>
<td>--percona</td>
<td>Percona Server</td>
</tr>
<tr>
<td>--percona-cluster</td>
<td>Percona Cluster</td>
</tr>
</tbody>
</table>

**MySQL_***

Options are useful if MySQL is already installed and configured.

- **-m MYSQL_HOST**
  MySQL host. Default is ‘localhost’

- **--mysql-port=MYSQL_PORT**
  TCP port where MySQL Server serves connections. Default values is 3306 for the local installation

- **--mysql-sock=MYSQL_SOCKET**
  Unix socket on which MySQL Server serves connections. Default values is /var/lib/mysql/mysql.sock. Used if local server only. The socket is unset if the option’s argument isn’t specified.

- **-p MYSQL_PASSWORD**
  MySQL password. Random is generated if is not set or specified.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d MySQL_DB</td>
<td>OnApp MySQL database name. Default is 'onapp'</td>
</tr>
<tr>
<td>-u MySQL_USER</td>
<td>MySQL user. Default is 'root'</td>
</tr>
<tr>
<td>REDIS_*</td>
<td>Options are useful if Redis Server is already installed and configured.</td>
</tr>
<tr>
<td>--redis-host=REDIS_HOST</td>
<td>IP address/FQDN where Redis Server runs. The Redis Server will be installed and configured on the current box if localhost/127.0.0.1 or box's public IP address (listed in SNMP_TRAP_IPS) is specified. If local Redis, it will serve as well on the unix socket '/tmp/redis.sock'. Default value is 127.0.0.1.</td>
</tr>
<tr>
<td>--redis-bind[=REDIS_BIND]</td>
<td>The IP address for Redis Server to serve connections (to listen). The option is not mandatory.</td>
</tr>
<tr>
<td>--redis-port=REDIS_PORT</td>
<td>Redis Server listen port. Defaults are: 0 - if local server 6379 - if remote server</td>
</tr>
<tr>
<td>--redis-passwd[=REDIS_PASSWD]</td>
<td>Redis Server password to authenticate. Random password is generated if the option's argument isn't specified. By default no password is used for local Redis.</td>
</tr>
<tr>
<td>--redis-sock[=REDIS_SOCK]</td>
<td>Path to the Redis Server's socket. Used if local server only. Default is /tmp/redis.sock. The socket is unset if the option's argument is not specified.</td>
</tr>
<tr>
<td>ADMIN_*</td>
<td>Options are used to configure OnApp Control Panel administrator data. 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>
<tr>
<td>--rhost RBT_HOST</td>
<td>IP address/FQDN where RabbitMQ Server runs. The RabbitMQ will be installed and configured on the current box if localhost/127.0.0.1 or box's public IP address (listed in SNMP_TRAP_IPS) Default values are 127.0.0.1.</td>
</tr>
<tr>
<td>VCD_*</td>
<td>Options are useful if vCloud/RabbitMQ are already installed and configured.</td>
</tr>
<tr>
<td>--vcdlogin VCD_LOGIN</td>
<td>RabbitMQ/vCloud user. Default value is 'rbtvcd'.</td>
</tr>
<tr>
<td>--vcdpasswd VCD_PASSWD</td>
<td>RabbitMQ/vCloud user password. The random password is generated if isn't specified.</td>
</tr>
<tr>
<td>--vcdvhost VCD_VHOST</td>
<td>RabbitMQ/vCloud vhost. Default value is '/'</td>
</tr>
<tr>
<td>RBT_*</td>
<td>Options are used to configure RabbitMQ manager account. If local RabbitMQ server.</td>
</tr>
<tr>
<td>--rbllogin RBT_LOGIN</td>
<td>RabbitMQ manager login. The default value is 'rbtmgr'.</td>
</tr>
<tr>
<td>--rblpasswd RBT_PASSWD</td>
<td>RabbitMQ manager password. The random password is generated if isn't specified.</td>
</tr>
<tr>
<td>--ha-install</td>
<td>Proceed with Control Panel and High Availability components installation</td>
</tr>
<tr>
<td>--rake RAKE_TASKS</td>
<td>List of OnApp Control Panel rake tasks (separated with space) to run at the very end of install or upgrade.</td>
</tr>
<tr>
<td>-v ONAPP_VERSION</td>
<td>Install custom OnApp CP version</td>
</tr>
</tbody>
</table>
### `-i SNMP_TRAP_IPS`
IP addresses separated with coma for snmp to trap

The `-i` option has higher priority than `on_app.yml`/`onapp-cp.conf` files.
In case of the Control Panel upgrade with the `-i` option the snmp address will be overwritten in the `on_app.yml`/`onapp-cp.conf` files.

During the Control Panel upgrade without the `-i` option the `on_app.yml` file has higher priority than the `onapp-cp.conf` file.
In this case the snmp address will be taken from the `on_app.yml` file and the `onapp-cp.conf` file will be overwritten.

### `-c CONFIG_FILE`
Custom installer configuration file. Otherwise, preinstalled one is used.

### `-y`
update OS packages (except of OnApp provided) on the box with `yum update`.

### `-a`
Do not be interactive. Process with automatic installation. Please note, this will continue OnApp Control Panel install/upgrade even if there is transaction currently running.

### `-t`
Add to the database and download Base Templates. For new installs only. If this option is not used, then only the following mandatory System Templates will be added by default during fresh install: OnApp CDN Appliance; Load Balancer Virtual Appliance; Application Server Appliance.

### `--noservices`
Do not start OnApp services: monit, onapp and httpd
Please note, crond and all OnApp’s cron tasks remain running. They could be disabled by stopping crond service manually for your own risk.

### `-D`
do not make database dump, and make sure it is disabled in the cron and not running at the moment

### `-h`
print this info

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.

---

If you face the problem with viewing the maps on VS/Smart/Application server creation wizard (Locations step), refer to the [Add Google Map API Key document](#).

---

### Getting support for your upgrade
You can use the information in this document to perform your own upgrade to the 5.4 version of the OnApp Cloud. However, if you have a full 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](http://forum.onapp.com).

### Upgrade Guide for Cloud with Mixed CloudBooted and Static Servers
This guide explains how to upgrade OnApp Cloud v5.3 to the v5.4 for the cloud with the mixed CloudBooted servers and Static servers configuration. Follow the procedure listed below in the correct order to upgrade your cloud. Please follow the complete procedure of the upgrade process. All packages (Control Panel, CloudBoot, Compute resources) must belong to the same major version to ensure the best performance of your cloud.

Make sure that your cloud configuration meets all the requirements before upgrading to OnApp 5.4. See the [Check Your Cloud Configuration](#) section of this document for details.
Important Notes

1. You must be running the latest patch of OnApp 5.3 version to upgrade to 5.4 version. If you are using an earlier version, please upgrade to 5.3.
2. 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.
3. Make sure no Control Panel files are open for editing under the root user account.
4. If you plan to deploy Accelerator, refer to the RabbitMQ Configuration for Accelerator document for more details.
5. Be aware that from now on, OnApp Licensing has a standalone client. Use only 443 port to connect from Control Panel to licensing server.
6. We strongly recommend that you test all your custom scripts before upgrading your production environment.
7. If you are using Integrated Storage, refer to the OnApp IS Upgrade Paths for more information about the upgrade details.

Check Your Cloud Configuration

Starting with OnApp 5.4, networks are made up of sub-networks called IP nets which contain ranges of IP addresses. To make your system compatible with the new networking scheme, a rake task will run with the installer. The rake task will modify your networks to contain IP ranges and IP nets. If a network contains two or more consecutive IP addresses of the same range of addresses, they will be united into one IP range. Individual IPs will each constitute an IP range. For each of the IP ranges an IP net will be added to the network. If at least one conflict is found in the configuration, the cloud will not be updated. If your cloud configuration is correct, the CP installer will be run and your networks will be modified to include IP nets and IP ranges.

Prior to the update procedure, it is required to check your cloud configuration. The cloud should comply with the following requirements for a successful upgrade:

- all VLANs indicated for the networks in the cloud should have a relevant value. The value for VLAN should not exceed 4095.
- all networks which have one or several IP addresses assigned to user(s) should be within a network zone
- all IP addresses added to the cloud should be represented with feasible values
- all network masks should have relevant lengths
- there should be no overlapping IP addresses in a single network

If one or several of the IP address you've added to the cloud do not correspond with their prefix, the system will offer to switch on the force option. When the force option is enabled, the system will automatically change the IP address to correspond with their prefix. For example, if you've had a 198.168.0.1/255.255.0.0 IP address with 8 as its prefix, the system will change the address to 198.168.0.1/255.0.0.0.
When you run the Control Panel installer the system will check your configuration. You can view the log at log/ip_consistency_check.log. If any inconsistencies are found, the log might contain any of the following warning messages:

- an incorrect VLAN for a network has been detected. The ID and label of the network will be provided.
- a network that has an IP address assigned to a user and which is not in a network zone has been detected. The ID of the network, the ID of the assigned IP address and the ID of the user to whom the IP is assigned will be provided.
- an IP address which is represented incorrectly has been detected. The ID of the IP address will be provided.
- an IP address which does not correspond with its prefix has been detected. The ID of the network, the ID of the IP address and the existing and expected prefixes will be provided.
- overlapping IP addresses have been detected in one network. The IP addresses and the network ID will be provided.

Upgrade Control Panel Server

- CP installer for Installation and Upgrade contains a new -D option enabling to avoid OnApp database dumping during the install/upgrade.
- To increase the cloud performance we recommend setting RUBY_GC_MALLOC_LIMIT parameter in custom configurations to 16 millions. For more information on RUBY_GC_MALLOC_LIMIT parameter, refer to Ruby's GC Configuration and Garbage Collection articles.
- Installer output is redirected to ./onapp-cp-install.log
- All installer critical errors are in /var/log/messages
- 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.
- Custom values must be set before the installer script runs.

To upgrade your Control Panel server:

1. Download and install the latest OnApp YUM repository file:

   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.4.noarch.rpm

2. Upgrade OnApp Control Panel installer package:

   # yum update onapp-cp-install

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

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

4. (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 (Deprecated parameter. If you set any values for this parameter, the
WITH_MARIADB=0

# Configure the database server relative amount of available RAM
TUNE_DB_SERVER=1

# 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=PasswordAuthentication=no"
KEEP_DUMPS=168
DB_DUMP_CRON='40 * * * *'

# Enable monit - tool for managing and monitoring Unix systems

ENABLE_MONIT=1

# If enabled (the 1 value is set) - install (if local box) and configures RabbitMQ Server (messaging system) for the vCloud support. parameter, they will not take effect

ENABLE_RABBITMQ=1

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

TRANS_LOGS_ROTATE_TIME=30

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

```
MAX_UPLOAD_SIZE=1073741824
```

### REDIS_PING_TIMEOUT

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

### OnApp Control Panel 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`
```

* PEM-encoded CA Certificate (if custom one exists)

```
SSLCA_CERTIFICATEFILE=/etc/pki/tls/certs/ca.crt
SSLCA_CERTIFICATECSRFILE=/etc/pki/tls/private/ca.csr
SSLCA_CERTIFICATECHAINFILE=/etc/pki/tls/private/ca.key
```

### SSLCertificateFile, SSLCertificateKeyFile

* Nginx directives' values

```
SSL_CERTIFICATEFILE=/etc/pki/tls/certs/ca.crt
SSL_CERTIFICATECSRFILE=/etc/pki/tls/private/ca.csr
SSL_CERTIFICATEKEYFILE=/etc/pki/tls/private/ca.key
```

### SSLCipherSuite, SSLProtocol

* Nginx directives' values

```
SSL_CIPHERS=
SSL_PROTOCOL=
```
5. Run Control Panel installer:

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

The full list of Control Panel installer options:

**Usage:**

```
/onapp/onapp-cp-install/onapp-cp-install.sh -h
```

```
```

**Where:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database server options:</td>
<td>Default database SQL server is MySQL Server. Please use one of the following option to install LOCALLY.</td>
</tr>
<tr>
<td>--mariadb</td>
<td>MariaDB Server</td>
</tr>
<tr>
<td>--percona</td>
<td>Percona Server</td>
</tr>
<tr>
<td>--percona-cluster</td>
<td>Percona Cluster</td>
</tr>
<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. Default is 'localhost'</td>
</tr>
<tr>
<td>--mysql-port=MYSQL_PORT</td>
<td>TCP port where MySQL Server serves connections. Default values is 3306 for the local installation</td>
</tr>
<tr>
<td>--mysql-sock=MYSQL_SOCK</td>
<td>Unix socket on which MySQL Server serves connections. Default values is /var/lib/mysql/mysql.sock. Used if local server only. The socket is unset if the option's argument isn't specified.</td>
</tr>
<tr>
<td>-p MYSQL_PASSWD</td>
<td>MySQL password. Random is generated if is not set or specified.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>MySQL_DB</td>
<td>OnApp MySQL database name. Default is ‘onapp’</td>
</tr>
<tr>
<td>MySQL_USER</td>
<td>MySQL user. Default is ‘root’</td>
</tr>
<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 and configured on the current box if localhost/127.0.0.1 or box’s public IP address (listed in SNMP_TRAP_IPS) is specified. If local Redis, it will serve as well on the unix socket ‘/tmp/redis.sock’. Default value is 127.0.0.1.</td>
</tr>
<tr>
<td>redis-bind</td>
<td>The IP address for Redis Server to serve connections (to listen). The option is not mandatory.</td>
</tr>
<tr>
<td>redis-port</td>
<td>Redis Server listen port. Defaults are: 0 - if local server 6379 - if remote server</td>
</tr>
<tr>
<td>redis-passwd</td>
<td>Redis Server password to authenticate. Random password is generated if the option’s argument isn’t specified. By default no password is used for local Redis.</td>
</tr>
<tr>
<td>redis-sock</td>
<td>Path to the Redis Server’s socket. Used if local server only. Default is /tmp/redis.sock. The socket is unset if the option’s argument is not specified.</td>
</tr>
<tr>
<td>ADMIN_*</td>
<td>Options are used to configure OnApp Control Panel administrator data. Please note, that these options are for NEW INSTALL only and not for upgrade</td>
</tr>
<tr>
<td>ADMIN_PASSWD</td>
<td>CP administrator password</td>
</tr>
<tr>
<td>ADMIN_FIRSTNAME</td>
<td>CP administrator first name</td>
</tr>
<tr>
<td>ADMIN_LASTNAME</td>
<td>CP administrator last name</td>
</tr>
<tr>
<td>ADMIN_EMAIL</td>
<td>CP administrator e-mail</td>
</tr>
<tr>
<td>rbthost</td>
<td>IP address/FQDN where RabbitMQ Server runs. The RabbitMQ will be installed and configured on the current box if localhost/127.0.0.1 or box’s public IP address (enlisted in SNMP_TRAP_IPS) Default values are 127.0.0.1.</td>
</tr>
<tr>
<td>VCD_*</td>
<td>Options are useful if vCloud/RabbitMQ are already installed and configured.</td>
</tr>
<tr>
<td>vcdlogin</td>
<td>RabbitMQ/vCloud user. Default value is ‘rbtvcd’.</td>
</tr>
<tr>
<td>vcdpasswd</td>
<td>RabbitMQ/vCloud user password. The random password is generated if isn’t 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 server.</td>
</tr>
<tr>
<td>rbtlogin</td>
<td>RabbitMQ manager login. The default value is ‘rbtmgr’.</td>
</tr>
<tr>
<td>rbtpassword</td>
<td>RabbitMQ manager password. The random password is generated if isn’t specified.</td>
</tr>
<tr>
<td>ha-install</td>
<td>Proceed with Control Panel and High Availability components installation</td>
</tr>
<tr>
<td>rake</td>
<td>List of OnApp Control Panel rake tasks (separated with space) to run at the very end of install or upgrade.</td>
</tr>
<tr>
<td>ONAPP_VERSION</td>
<td>Install custom OnApp CP version</td>
</tr>
</tbody>
</table>
OnApp Cloud 5.4 Get Started Guide

### -I SNMP_TRAP_IPS
IP addresses separated with coma for snmp to trap

The `-i` option has higher priority than 'on_app.yml'/`onapp-cp.conf' files.
In case of the Control Panel upgrade with the `-i` option the snmp address will be overwritten in the 'on_app.yml'/`onapp-cp.conf' files.

During the Control Panel upgrade without the `-i` option the 'on_app.yml' file has higher priority than the 'onapp-cp.conf' file.
In this case the snmp address will be taken from the 'on_app.yml' file and the 'onapp-cp.conf' file will be overwritten.

### -c CONFIG_FILE
Custom installer configuration file. Otherwise, preinstalled one is used.

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

### -a
Do not be interactive. Process with automatic installation. Please note, this will continue OnApp Control Panel install/upgrade even if there is transaction currently running.

### -t
Add to the database and download Base Templates. For new installs only. If this option is not used, then only the following mandatory System Templates will be added by default during fresh install: OnApp CDN Appliance; Load Balancer Virtual Appliance; Application Server Appliance.

### --noservices
Do not start OnApp services: monit, onapp and httpd
Please note, crond and all OnApp's cron tasks remain running. They could be disabled by stopping crond service manually for your own risk.

### -D
do not make database dump, and make sure it is disabled in the cron and not running at the moment

### -h
print this info

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.

---

## Upgrade Static Compute Resources

At first upgrade your static compute resources.

1. Make sure your compute resource is visible and online in the Control Panel.
2. Download and install the latest OnApp YUM repository file:

   ```
   # rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.4.noarch.rpm
   ```

3. Upgrade OnApp compute resource installer package:

   ```
   # yum update onapp-hv-install
   ```

4. Update your server OS components (if required):
   For XEN compute resource:

   ```
   # /onapp/onapp-hv-install/onapp-hv-xen-install.sh -y
   ```
5. Run compute resource installer:
   For XEN compute resource:
   ```bash
   # /onapp/onapp-hv-install/onapp-hv-xen-install.sh
   ```

   For KVM compute resource:
   ```bash
   # /onapp/onapp-hv-install/onapp-hv-kvm-install.sh
   ```

   Reboot XEN compute resource, which is running on CentOS 6.x, after upgrade to newer XEN version.

6. Reboot static compute resources.  
   For KVM compute resources only: the kernel package update is a part of "Upgrade Static Compute Resources" default procedure. So reboot is required, if kernel package was upgraded and customer is willing Compute Resource(s) running it (for security reason).

Upgrade CloudBoot Packages

Create a backup of the /tftpboot directory in case storage packages rollback will be needed.

To upgrade the OnApp Storage packages:

1. Upgrade the repo:
   ```bash
   CP_host#> rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.4.noarch.rpm
   ```

2. Upgrade the packages:
   Depending on the needed compute resource type, you should install onapp-ramdisk-DISTRO-FLAVOR package(s), where:

   DISTRO - CentOS5, CentOS6 or CentOS7  
   FLAVOR - XEN, KVM

   Also it is required to install `yum install onapp-ramdisk-centos7-default` together with onappstore packages.

   It is recommended to update all packages. Below you can find an example:
   ```bash
   bash#> # yum install onapp-ramdisk-centos7-default  
   bash#> # yum update onapp-store-install  
   bash#> # yum update onapp-ramdisk-tools  
   bash#> # yum update onapp-ramdisk-centos6-kvm  
   bash#> # yum update onapp-ramdisk-centos5-xen  
   bash#> # yum update onapp-ramdisk-centos6-xen  
   bash#> # yum update onapp-ramdisk-centos7-kvm
   ```
3. Run the script:

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

Be aware that the disk-less nodes password is the root password for the CloudBoot compute resources. By default it is blank.

When run in the interactive mode, enter the required information.

### Upgrade CloudBoot Backup Servers

CloudBoot backup servers are CloudBooted KVM compute resources that can be be used as backup servers. The CloudBoot backup server upgrade procedure is almost the same as the CloudBoot compute resource upgrade. Follow the instructions provided in this section to upgrade CloudBoot backup servers in your cloud.

Once you have upgraded the CloudBoot dependencies, you have to reboot your Cloud Boot compute resource to update the Cloud Boot RPM. You do not need to perform any backup server upgrade operations using console.

To do so:

1. Go to your Control Panel **Settings** menu.
2. Click the **Compute resources** icon.
3. Click the label of the CloudBoot compute resource the backup server is based on.
4. On the compute resource details screen, click the **Actions** button, then click **Reboot Compute resource**.
5. A new screen will open asking for confirmation before reboot:

   - **Are you sure you want to reboot this compute resource?** Confirm that you want the compute resource to reboot.

6. When you're certain you want to proceed with the reboot, click the **Reboot** button.
7. Repeat these steps for all CloudBoot backup servers in your cloud.
8. Once all are rebooted, proceed to CloudBoot compute resources upgrade.

### Upgrade CloudBoot Compute Resources

Depending on the infrastructure, scale and needs of your cloud we suggest the following methods of upgrading CloudBoot compute resources:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple Reboot</td>
<td>This method is the simplest method technically. It also ensures all tools are updated. However, it will result in some limited downtime (its duration depends on how many virtual servers are running on each compute resource).</td>
</tr>
<tr>
<td>Migrate and reboot</td>
<td>This method involves migrating all virtual servers off each CloudBoot compute resource in turn. The compute resource can then be safely rebooted, picking up the upgraded Integrated Storage and CloudBoot packages. Virtual servers that do not support hot migrate will have to be stopped.</td>
</tr>
<tr>
<td>Live Upgrade</td>
<td>This method will upgrade Integrated Storage components but will not upgrade CloudBoot image.</td>
</tr>
</tbody>
</table>

In case you have applied any custom configuration to your CloudBoot servers, it is recommended to recheck that this customization does not break new cloud boot image version. For this, reboot a compute resource and run **Storage Health Check** and **Network Health Check**. Make sure that Vdisks hosted on a compute resource are redundant and healthy before rebooting a CloudBoot compute resource.

For more information about upgrade scenarios, refer to the [OnApp IS Upgrade Paths](#).
Simple Reboot

Follow the below procedure to upgrade the CloudBoot compute resources with reboot:

1. **Upgrade CloudBoot Packages.**
2. When the CloudBoot packages upgrade is complete, stop all virtual servers which reside on the CloudBoot compute resources.
3. **Reboot all CloudBoot compute resources.**

Once the compute resources are booted, the upgrade is complete. Before starting all Virtual Servers please ensure that the diagnostics page does not report any issue. In case of any issue, please press repair button to resolve it, then continue with starting Virtual Servers.

Note that virtual servers cannot be stopped simultaneously, but must be stopped in sequence. This can result in considerable downtime if there are a large number of virtual servers.

Migrate and reboot

Live Upgrade is only applicable if your cloud is running latest 5.3 CloudBoot RPM.

Use this procedure if you prefer migrating all virtual servers to another compute resource and conducting overall upgrade of your CloudBoot and Integrated Storage. Virtual servers that do not support hot migrate will have to be stopped.

Once you have upgraded the CloudBoot packages, you have to reboot your CloudBoot compute resources to update them.

To do so:

1. Migrate all the virtual servers from the CloudBoot compute resource to another compute resource. Follow the instructions described in the Migrate Virtual Server section of the Admin guide to migrate virtual servers.
2. After that, go to your Control Panel Settings menu.
3. Click the Compute Resources icon.
4. Click the label of the CloudBoot compute resource you have migrated all VSs from.
5. On the compute resource details screen, click the Actions button, then click Reboot Compute resource.

Rebooting a compute resource assigned to a data store with a single replica (single-replica compute resource) or degraded virtual disks may result in data loss.

6. A new screen will open asking for confirmation (via two check boxes) before reboot:
   - **Stop all virtual servers that cannot be migrated to another compute resource?** Check this box if you want VSs that cannot be migrated to be powered off. When a compute resource is scheduled for a reboot, OnApp will first attempt to hot migrate all VSs it hosts. If hot migration is not possible for a VS, OnApp will attempt to cold migrate that VS. With this box checked, if cold migration fails, the VS will be stopped so the reboot may proceed. If you don't check this box, OnApp will attempt to hot and then cold migrate all VSs hosted by the compute resource being rebooted – but will stop the migration process if any VS cannot be migrated.
   - **Are you sure you want to reboot this compute resource?** A simple confirmation to confirm that you want the compute resource to reboot.

Before the reboot, please ensure that all vdisks are fully synced and redundant. If some of them are not fully synced, the virtual server, that is owner of a degraded (or non-redundant) vdisk, can loose access to the vdisk. It can be manifested as IO errors during writes or reads to/from the vdisk inside the virtual server.

7. When you're certain you want to proceed with the reboot, click the Reboot button.
8. Repeat these steps for all CloudBoot compute resources in your cloud.
Live Upgrade

Live Upgrade is only applicable if your cloud is running latest 5.3 CloudBoot RPM.

- Live Upgrade with passthrough is currently unsupported. Passthrough to storage means that network interface will be added to the Storage Controller Server without the bond and the Storage Controller Server will have the complete control over this interface.
- Power off all Windows virtual machines and virtual backup servers before starting the live upgrade.
- If your current Storage package is 4.0, Windows virtual servers can remain running.
- During the CloudBoot compute resource live upgrade, only the control stack for managing integrated storage is upgraded. Other changes come into effect after the compute resource is next rebooted. Due to this, hot migration may fail between compute resource which is already rebooted and the one that hasn't.
- Do not make any changes to the cloud during the upgrade process!
- Any offline Cloudboot compute resources should be removed from the CP server before running live upgrade as the scripts expect to be able to speak to all compute resources during these steps.
- Please, consult OnApp IS Upgrade Paths to learn the minimum Integrated Storage version required for the current update to be performed in LiveUpgrade mode.

Use this procedure to upgrade without rebooting your servers:

1. Make sure no disks are out of sync. To do so, check the Diagnostics page in CP at Dashboard > Integrated Storage > Compute zone label > Diagnostics. Alternatively, log into a compute resource and run the command below:

   ```
   HV_host#> getdegradedvdisks
   ```

2. Repair all the degraded disks before proceeding to the upgrade process. To do so, log in to your CP and go to Integrated Storage > Compute zone label > Diagnostics page. Alternatively, run one of the following commands:

   - To repair a specific vdisk, use the following command:

     ```
     HV_host#> onappstore repair uuid=
     ```

   - To repair all vdisks one by one, use the following command:

     ```
     HV_host#> repairvdisks
     ```

   - To repair all vdisks in 10 threads simultaneously, use the following command:

     ```
     HV_host#> parallelrepairvdisks
     ```

   Please note, that `parallelrepairvdisks` command performs the repairs much faster but makes an impact on the Integrated Storage SAN network. Vdisk performance may be slower during the repair.

   In case you have a Cloudboot Backup Server, you can perform these commands on the Backup Server. The repairs will be triggered across all Cloudboot compute zones.

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

   ```
   CP_host#> service onapp stop
   ```

4. Stop the Apache server:
5. Make sure to update CloudBoot packages before proceeding to the following steps.
6. Run the following command from the Control Panel server terminal to display the list of compute resources with their IP addresses. Make a note of the list of IPs:

   ```
   CP_host#> liveUpdate listHVs
   ```

   This command will also show whether compute resources are eligible for live upgrade.

   If the command liveUpdate is not available then it may be located in the sbin directory instead (cd /usr/local/sbin).

7. Run the following command for every compute resource:

   ```
   CP_host#> liveUpdate updateToolstack <HV IP Addr>
   ```

   Once all the toolstacks are updated run the following command for every compute resource:

   ```
   CP_host#> liveUpdate refreshControllers <HV IP Addr>
   ```

   Wait several minutes for all degraded disks to come to synchronized state. The synchronization will take approximately three minutes for each compute resource.

   After each controller restart, check for any issues on the backup server (or on one Compute resource from each zone):

   1. Log on via SSH to the backup server (or Compute resource).
   2. Run getdegradednodes from the SSH console.
   3. Run getdegradedvdisks from the SSH console.

8. Restarts the storage controllers. This command can be performed later at a more suitable time.

   Run the following command for each compute resource in turn:

   ```
   CP_host#> liveUpdate restartControllers <HV IP Addr>
   ```

   Please make sure you restart all controllers and don’t leave your cloud in a partially updated state for too long. Note that when operating in LiveUpdated mode (e.g. with the tool stacks updated but before you have performed the controller restart) you cannot use disk hot plug.

   After each controller restart check for any issues on the backup server or one Hypervisor from each zone:
   1. Log on via SSH to the backup server (or Hypervisor).
   2. Run getdegradednodes from the SSH console.
   3. Run getdegradedvdisks from the SSH console.
   If there are any issues seen please rectify them before continuing with the next controller restart.

9. Make sure that the package versions are upgraded by running the following command on each compute resource:
10. Start the Apache server:

```
HV_host#> cat /onappstore/package-version.txt | grep Source
```

11. Start the OnApp service:

```
CP_host#> service httpd start
CP_host#> service onapp start
```

**Local Read Policy**

Enabling Local Read on a compute zone ensures that the locally stored copy of the data will always be used for reads. This significantly reduces read latency and improves overall storage performance by reducing load on the SAN network. However, in order to use this policy every compute resource must have sufficient physical drives to be able to store the number of stripes specified in the data store. E.g. in a 2R4S data store there must be at least 4 physical disks on the compute resource to use local read.

**Changes to Local Read Policy Enforcement**

Originally, when this policy was introduced OnApp did not enforce the requirement for the minimum number of drives. Consequently, some users who set the policy having insufficient drives may see the following error message:

```
Fatal: OnApp::Actions::Fatal Storage API Call failed:
{"result"=>"FAILURE", "error"=>"Local reads have been enabled on the zone - members required per host: 4, required hosts: 2, available hosts: 0"}
```

The solution is to either add additional drives to that compute resource and then add them to the data store or to disable read local.

**Getting support for your upgrade**

You can use the information in this document to perform your own upgrade to the 5.4 version of the OnApp Cloud. However, if you have a full 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 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.

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:

```
# yum clean metadata
```

2. Remove OnApp:

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

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

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

Where:

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

### OS Components Upgrade

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
     bash#> yum update onapp-cp-install
     ```
   - **For Compute resource**
     ```bash
     bash#> yum update onapp-hv-install
     ```
   - **For Backup Server**
     ```bash
     bash#> yum update onapp-bk-install
     ```

2. Run the following script to update the OS components
   - **For Control Panel**
     ```bash
     bash
     /onapp/onapp-cp-install/onapp-cp-installall.sh -y
     ```
   - **For XEN Compute resource**
Additional Considerations for ISOs

Perform the following steps to enable building and booting VSs from the ISO 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 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 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 is o_path_on_cp directory and all the compute resources' `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

---

**More info:**
- ISOs - general information on ISOs in OnApp
- Boot from ISO - the walk-through how you can boot a VS from ISO
- ISOs (API Guide) - the list of available API requests
OnApp IS Upgrade Paths

<table>
<thead>
<tr>
<th>IS Version upgrading to</th>
<th>5.0.0-21</th>
<th>5.1.0-5</th>
<th>5.2.0-5</th>
<th>5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade by &quot;Simple Reboot&quot;</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Upgrade by &quot;Migrate and Reboot without IS update&quot;</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Upgrade by &quot;Migrate and Reboot&quot;</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Upgrade by &quot;LiveUpgrade&quot;</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Yes - recommended by OnApp
N/A - not recommended by OnApp, will not update properly the CloudBoot OS or Integrated Storage

For versions < 5.0 please use only "Simple Reboot" upgrade method. Use "Migrate and reboot" only if you are running 4.2.1-8.
For information about upgrade of versions previous to 5.0.0-21, refer to the OnApp IS Upgrade Paths (4.0.0-3 - 4.2.1-11 versions) section.

General information and recommendations about CloudBoot OS and Integrated Storage upgrades

Starting with OnApp 5.0 LTS, we have made some changes to updates for CloudBoot OS and Integrated Storage. CloudBoot OS upgrades that include security patches, kernel upgrades and updated drivers will be released on a regular basis. If a security patch was released by CentOS it will be included in the next released RPM.
These releases may not include updates for Integrated Storage, a component of the CloudBoot OS, as this platform is very stable and does not require changes with every release.

For the best experience, stability and security OnApp recommends that the CloudBoot compute resources should be upgraded by reboot at a convenient time if a new CloudBoot RPM is released. This is required to completely apply the security patches, kernel upgrades and updated drivers.

Integrated Storage as a platform does not strictly require the CloudBoot compute resource to be rebooted after upgrade. However in case of critical updates and fixes it can be required to reboot the CloudBoot compute resource for them to take full effect. Currently only versions 4.1 and 5.0 require to be rebooted after Integrated Storage upgrade. OnApp will notify in future release notes if the Simple Reboot method is the recommended way to upgrade.

Each upgrade procedure explanation:

Simple Reboot

This upgrade method requires to reboot the CloudBoot compute resources with all VSs (Virtual Servers) powered off to apply security patches, kernel upgrades and updated drivers to the CloudBoot OS. Simple reboot is the fastest and the safest way to upgrade, but does result in some downtime for the Virtual Servers. Integrated Storage virtual disks do not become degraded. This upgrade method also upgrades the Integrated Storage platform as a component of the CloudBoot OS.
Migrate and Reboot without Integrated Storage update
This upgrade method requires to reboot the CloudBoot compute resources to apply security patches, kernel upgrades and updated drivers to the CloudBoot OS. This method is only applicable if the Integrated Storage platform is not updated. Your VSs will remain online, you only require to migrate them from the CloudBoot compute resources that will be rebooted. Keep in mind that it is required to repair any degraded virtual disks before proceeding with a compute resource reboot.

Migrate and Reboot
This upgrade method requires to reboot the CloudBoot compute resources to update the Integrated Storage Platform and the CloudBoot OS. Your VSs will remain online. Keep in mind that it is required to repair any degraded virtual disks before proceeding with reboot.

LiveUpgrade
This upgrade method upgrades the Integrated Storage platform only. Your VSs will remain online. There is almost no risk of data loss and zero downtime. However this method does not update the CloudBoot OS, you will not get the security patches, kernel upgrades and updated drivers if they are included in the release.

Starting from OnApp 5.3 version, each CloudBoot OS image is divided to a separate package for better experience and support. For example if the CentOS 6 Xen CloudBoot OS image receives a security patch it will be updated and released by OnApp. Only this image will be downloaded during the upgrade procedure, saving internet traffic and time.

Please contact our Support team if you are unsure regarding the right upgrade path for you to ensure you choose the right path for you and your clients.

Getting Support

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

- OnApp support portal
- (+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.