OnApp Cloud 5.7
Get Started Guide

Table of Contents

The guides in this section apply to installing the OnApp Cloud 5.7 version. For the release notes list, please refer to the [Release Notes](#) space.

> Make sure you meet the [technical requirements](#) before preparing OnApp Cloud.

1 Technical Details

- [Suggested Specifications](#)
- [Server Config Reminder](#)
- [Software Requirements](#)
- [Recommended Network Configurations](#)
- [Types of Cloud Service with OnApp](#)
- [Supported Functionality](#)

5

2 Installation

- OnApp Installation Walk-through
- Installation Guide
- Installation Guide for High Availability Clusters
- Additional Considerations for ISOs
- Additional Considerations for OVAs
- Getting Support

3 Preparation

- Configure Networks
- Configure Storage
- Configure Servers

4 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](#)

5   What's New in OnApp Cloud 5.7

The OnApp Cloud 5.7 release contains the following changes and new features:

5.1   Buckets

OnApp 5.7 expands the buckets functionality to include smart and baremetal resources, limits and pricing for DRaaS and instance packages, and much more. Among the biggest changes to buckets are:

- Added the Baremetal server type to the bucket's Access Control and Rate Card sections.

- Added the Smart server type to the bucket's Access Control and Rate Card sections.

- Added the Instance Packages limits to the bucket Access Control and Rate Card for the Virtual server type.

- Adapted Federation billing plans to the buckets functionality to enable managing resource allocation and prices of a federated VS through the Access Control and Rate Card.

5.2   Notification Center

OnApp 5.7 makes notifications more flexible, configurable and user-friendly by, for example, by creating custom event types or adding multiple gateways and recipients lists to a subscription. Among the additions to the notifications functionality are:

- Added the ability to add multiple recipients lists, gateways and events to subscriptions.

- Added system notification templates for the reset password, account lock, and transaction approval events. These templates can be edited but cannot be deleted.

- Added a list of available placeholders for notification templates which can be associated with events.

- Implemented ability to add custom event types, add them to subscriptions and trigger such event types.

5.3   OVA Improvements

The 5.7 release introduces the possibility to convert OVA templates more than once into KVM and vCenter virtualization formats. OnApp 5.7 also offers a simplified procedure for configuring CloudBoot backup servers to support the OVA functionality.

5.4   Extended CPU Configuration

OnApp 5.7 introduces the new extended CPU configuration for a compute zone. CPU flags are now assigned by default, based on the CPU characteristics of all compute resources added to the zone. You can also assign additional flags that are common for each compute resource in the compute zone.

5.5   Hardware Info

As a part of the current release, the Hardware Info page has been added at **Control Panel** > **Settings** for you to overview hardware that is used by compute resources and backup servers

available in your cloud. The Hardware Info page provides data on CPU, RAM, hard disk drives, networks and other hardware components.

5.6 CDN

OnApp 5.7 introduces WAF protection and Wildcard Invalidation for CDN resources:

- [WAF protection](#) secures your CDN resources and the CDN Accelerator from malicious threats and attacks. Web Application Firewall (WAF) monitors, filters or blocks the traffic to and from a Web application. It can prevent such attacks as Cross-site scripting (XSS), SQL injection, session hijacking and buffer overflows through customizable web security rules.

- [Wildcard invalidation rules](#) allow you to remove certain folders or files from the cache. You can launch the invalidation process multiple times for a rule you specify. Wildcard invalidation is available for HTTP Pull and HTTP Push resources and you can set up to five wildcard invalidation rules for a resource.

6 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.

6.1 Suggested Specifications

There are many factors that determine how many virtual servers you can run. Below you can find specifications for a Medium Production 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.

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.

On this page:

See also:

6.1.1 Suggested Specifications

OnApp License		Cloud
Number of Control Panel (CP) Servers		1
Separate Database Server/Cluster		No
Dedicated Backup Servers		1
Number of Compute Resources (XEN/KVM)		8
Compute Resource Type (Static / Cloudboot)		Cloudboot
CP Server	Processor	2 x 8 Core CPUs eg. Xeon e5-2640 v3
	Memory	32GB RAM
	Disks	4 x 100GB SSD

	RAID Configuration	RAID 10
	Network Adapters	Dual port 1Gps + Dual Port 10Gbps eg. Intel I350 + X520
Backup Server	**Processor**	2 x 8 Core CPUs eg. Intel Xeon e5-2620 v3
	Memory	32GB RAM
	HDDs	12x2TB SAS
	RAID	RAID10
	Network Interfaces	Dual port 1Gbp Intel NIC + Dual port 10Gbps Intel NIC
Compute Resource	**Processor**	2 x 8 Core CPUs eg. Xeon e5-2640 v3
	Memory	256GB
	HDDs	8 x 400GB SSD
	RAID Controller	PCIe gen3 eg. PERC H730, 1GB cache
	RAID Configuration	JBOD
	Network Interfaces	4 x 10Gbps eg.
iSCSI SAN	**Type**	Optional Dual-Controller Hardware SAN
	HDDs	12+ x SSD
	RAID Configuration	RAID10
Network Hardware		2 x High performance switch with: 48 x 10GbE ports, 4 x 40 GbE ports

6.1.2 Storage Hardware Requirements

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

Integrated Storage Platform	Local Storage Only	Enterprise SAN
• 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)	• minimum 1 dedicated partition in each compute resource • separate disk from the primary OS drive *recommended*	• 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

Integrated Storage Platform	Local Storage Only	Enterprise SAN
• IGMP snooping must be disabled on storage switch for storage network		• multiple NICs bonded or 10GBit/s ethernet *recommended*

6.1.3 Hardware Requirements for HA

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

6.2 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 on which virtualization method you choose, Xen or KVM.

- CloudBoot is not compatible with CentOS 7 Xen compute resources.
- CentOS 5 is only supported for OnApp versions up to 5.3.

Supported server configuration

- **XEN Compute resources** CentOS 6.x x64, CentOS 7.x x86/64

- **KVM Compute resources** CentOS 6.x x64, CentOS 7.x x86/64

- **OnApp Control Panel Server** CentOS 6.x x86/64, CentOS 7.x x86/64

- **OnApp Backup Server** 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

See also:
Supported Functionality
Software Requirements
Recommended Network Configurations
Suggested Specifications
Types of Cloud Service with OnApp

Libvirt Versions

The table below indicates the libvirt version compatible with your system depending on the virtualization type and version:

CentOS 6.x Xen	CentOS 6.x KVM	CentOS 7.x Xen	CentOS 7.x KVM
libvirt 2.2.0 (if CentOS version < 6.9) libvirt 3.2.1 (if CentOS version >=6.9)	libvirt 0.10.2	libvirt 2.4.0 (if CentOS version <7.3) libvirt 3.2.1 (if CentOS version >=7.4)	libvirt 2.0.0 (if CentOS version<7.3) libvirt 3.2.1 (if CentOS version >=7.4)

6.3 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.

> **See also:**
>
> Server Config Reminder
> Supported Functionality
> Recommended Network Configurations
> Suggested Specifications
> Types of Cloud Service with OnApp

6.4 Recommended Network Configurations

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

6.4.1 For Xen/KVM Cloud
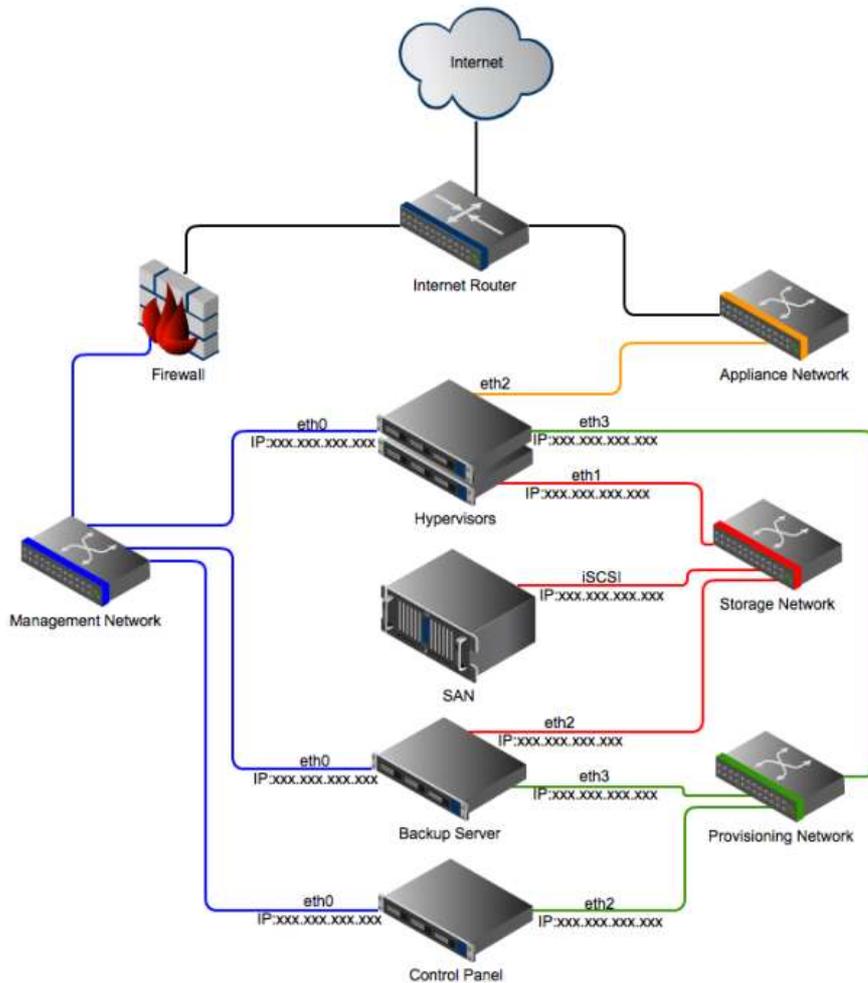
On this page:

See also:

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

Provisioning network is not required for clouds using Integrated Storage with dedicated backup servers.
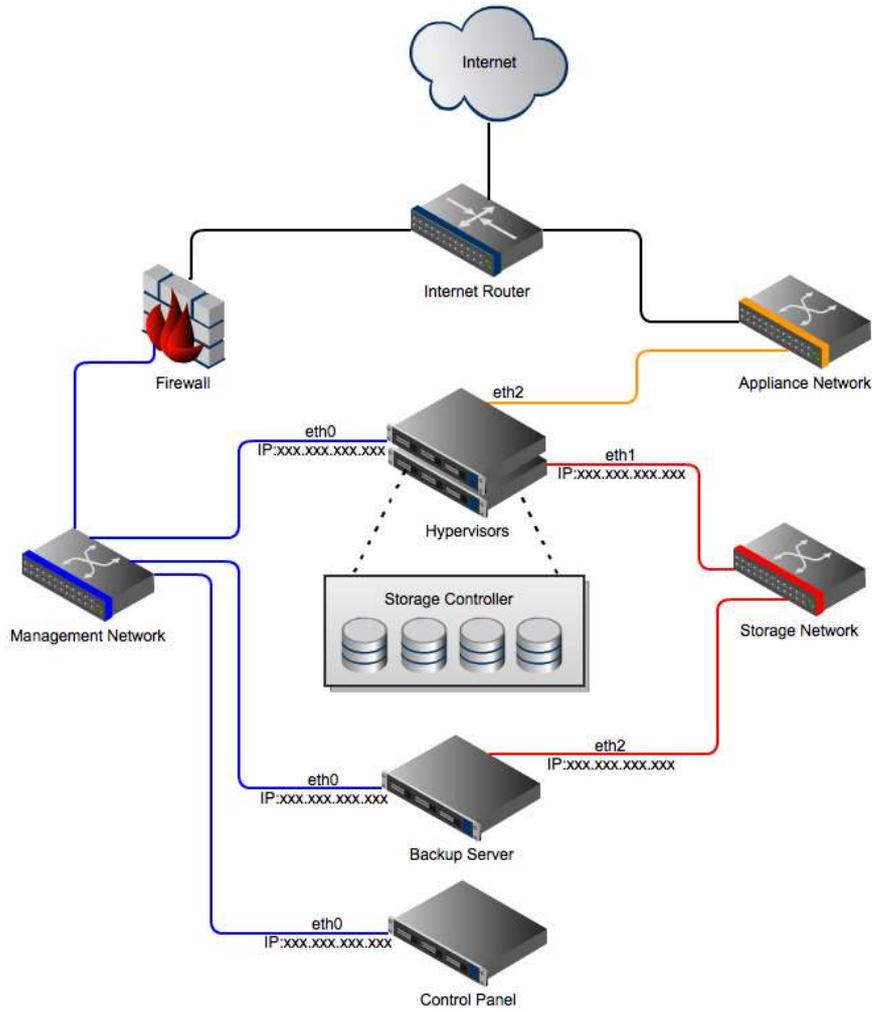
> If you are experiencing MAC address flapping across ports because the switch does not support the balance-rr mode, set up separated VLANs per each bond pair for that switch.

6.5 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.

6.5.1 Public Cloud, By-The-Hour
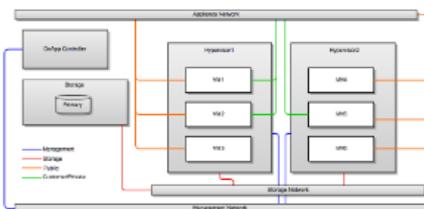
You can use OnApp to set up a complete pay-as-you-go public cloud system and compete with companies like AWS

- 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

On this page:

Public Cloud
Virtual Private Cloud
Cloud VPS
Hybrid Cloud Hosting
Traditional VPS Model
The OnApp Federation

See also:

Server Config Reminder
Supported Functionality
Software Requirements
Recommended Network Configurations
Suggested Specifications

6.5.2 Virtual Private Cloud

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

- Group compute resource, network and storage resources into a single private cloud resource for a customer

- Your customer gets all the benefits of a private cloud, backed by the resources of the whole cloud

- This brings the cost of private clouds down for customers, too
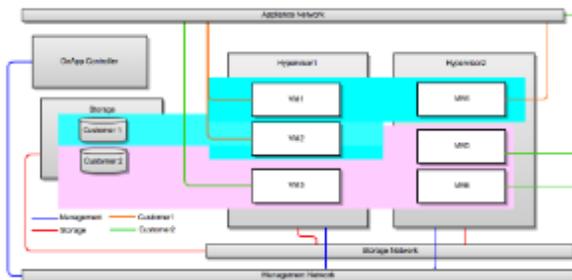
6.5.3 Cloud VPS

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
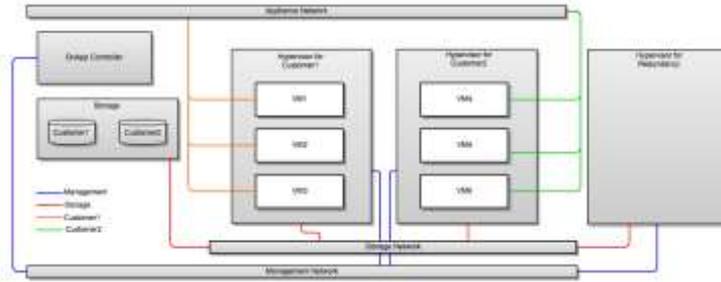
6.5.4 Hybrid Cloud Hosting

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)
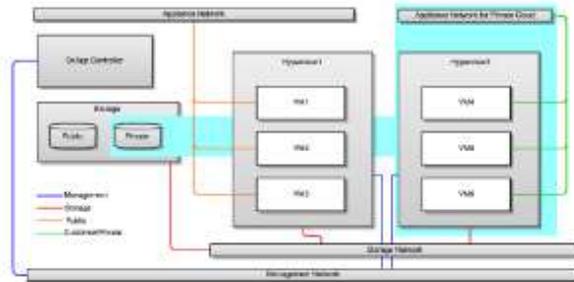
6.5.5 Traditional VPS Model

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
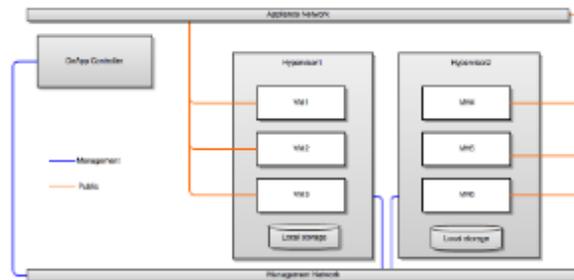
6.5.6 The OnApp Federation

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

6.6 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

- Javascript must be enabled in the browser

See also:

Server Config Reminder
Suggested Specifications
Types of Cloud Service with OnApp

	Small Production Cloud	Medium Production Cloud	Enterprise Cloud
Compute Resource Redundancy (supports failover)	Yes	Yes	Yes
Supports Hot Migration	Yes	Yes (Fast!)	Yes (Fast!)
Storage Network Redundancy	No	Yes	Yes
Production Network Redundancy	No	Yes	Yes
Control Panel Server Redundancy	No	No	Yes
Backup and Template Storage Space (approx)	12TB	12TB	24TB
Integrated Datastore Space (approximately)	4TB	11TB	24TB
Supports Incremental Backups of Linux VS	Yes	Yes	Yes

7 Preparation Guide

This document describes how to prepare the OnApp Cloud 5.7 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.

- Make sure you meet the Technical Details before preparing OnApp Cloud.
- Please do not change the default language settings during the installation process (en_US.UTF-8)!

See also:

Configure networks
Configure storage
Configure servers
Installation Guide
Technical Details

7.1 Configure Networks

This section is the part of the OnApp preparation guide.

Configure Networks > Configure Storage **>** Configure Servers

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.

7.1.1 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:

On this page: Appliance Network/VS Networking
Management Network
Provisioning Network
Storage Network

See also:

Technical Details
Configure Storage
Configure Servers
Installation Guide

```
/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.

7.1.2 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 firewalled 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 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.

7.1.3 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.

7.1.4 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](#).

This section is the part of the OnApp preparation guide.

Configure Networks > [Configure Storage](#) > [Configure Servers](#)

7.2 Configure Storage

This section is the part of the OnApp preparation guide.

[Configure Networks](#) **> Configure Storage >** [Configure Servers](#)

Configuring storage is highly important when preparing the cloud for the installation. Depending on the storage setup type, the installation requirements vary.

7.2.1 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 a InfiniBand HCA controller, since all of these present the block device directly. OnApp does not support services such as NFS for primary storage, because these present a filesystem and not the block device.

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

Fabric Components - the Network Fabric Between Compute Resources and SANs

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

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

7.2.2 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.

7.2.3 Integrated Storage (OnApp Storage)

OnApp Storage is a distributed block storage system that allows you to build a highly scalable and resilient SAN using local disks in compute resources. With OnApp Storage you create a

virtual data store that spans multiple physical drives in compute resources, with RAID-like replication and striping across drives. The SAN is fully integrated into the compute resource platform, and the platform is completely decentralized. There is no single point of failure: for example, if a compute resource fails, the SAN reorganizes itself and automatically recovers the data.

The following requirements are recommended for integrated storage implementation:

- 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.

- Note that advanced disk sector format is not supported for Integrated Storage disks. Ensure that your disk drives support the 512-byte sector alignment before installing and using them with Integrated Storage.

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

7.2.4 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 vis 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](#).

This section is the part of the OnApp preparation guide.

Configure Networks **> Configure Storage >** Configure Servers

---

7.3 Configure Servers

This section is the part of the OnApp preparation guide.

Configure Networks **>** Configure Storage **> Configure Servers**

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

7.3.1 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.

- 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.

On this page: Server Installation Requirements
Control Panel Server
Backup Server
Compute Resource Servers
CloudBoot Compute Resource Servers

See also:

Configure Networks
Configure Storage
Installation Guide
Technical Details

We strongly recommend that you avoid creating mixed compute zones:

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

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

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

Supported server configuration

- **XEN Compute resources** CentOS 6.x x64, CentOS 7.x x86/64

- **KVM Compute resources** CentOS 6.x x64 or CentOS 7.x x86/64

- **OnApp Control Panel Server** CentOS 6.x x86/64 or CentOS 7.x x86/64

- **OnApp Backup Server** CentOS 6.x x64 or CentOS 7.x x86/64

- **Integrated Storage** 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 x86/64

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

7.3.2 Control Panel Server

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

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

The control panel server will become very MySQL heavy as you add more compute resources, so a fast disk array and lots of memory is recommended. A good example would be a 4xSAS RAID10 array with 24GB RAM and quad core Xeon CPU. SSD storage can also be considered. If you have a Control Panel server spec in mind, you're very welcome to send it to your OnApp integrations specialist for review.

7.3.3 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.

7.3.4 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 stability and performance.

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

7.3.5 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.

This section is the part of the OnApp preparation guide.

This section is the part of the OnApp preparation guide.

Configure Networks **>** Configure Storage **> Configure servers**

8   Additional Considerations for ISOs

Perform the following steps to enable building and booting VSs from the ISO for your cloud:

8.1   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 `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.

8.2   Enable Permissions in Control Panel

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

- *Any action on ISOs* - the user can take any action on ISOs

- *Create a new ISO* - the user can create a new ISO

- *Destroy any ISO* - the user can delete any ISO (own, user, and public)

- *Destroy own ISO* - the user can only delete own ISO

- *Destroy user ISO* - the user can delete ISOs created by any user, but not public ISOs

- *Make any ISO public* - the user can make public any ISO available to all users

- *Make own ISO public* - the user can make public own ISOs only

- *Make user ISO public* - the user can make public ISOs created by any user

- *Create and manage own ISOs* - the user can create and edit/delete/view own ISOs

- *Manage all ISOs* - the user can manage own/user/public ISOs

- *Create and manage user ISOs* - the user can view/create/edit/delete ISOs created by any user

- *See all ISOs* - the user can view all ISOs in the cloud

- *See own ISOs* - the user can only view the ISOs created by themselves

- *See all public ISOs* - the user can view all public ISOs

- *See user ISOs* - the user can view the ISOs created by any user in the cloud

- *Update any ISO* - the user can edit any ISO in the cloud

- *Update own ISO* - the user can only edit own ISO

- *Update user ISO* - the user can edit the ISOs created by any user in the cloud

See also:

Manage ISOs
List of All OnApp Permissions

9   Additional Considerations for OVAs

To enable building VSs from OVA for your cloud, perform the following steps.

9.1   Mount OVA Locations

To enable building a VS from OVA, it is required to mount a source location to which OVA is uploaded on CP with a destination location where OVA is stored on a backup server. The location is preconfigured in the *on_app.yml* config file:

- **Source Path** (`ova_path`) - specifies the location where OVAs are downloaded/uploaded 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 mounted to the specified destination location.

- **Destination Path** (`ova_path`) - specifies the location where OVAs are stored on backup 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 shared with the specified source location.

CloudBoot compute resources mount the `/data` location automatically at boot to the `/onapp/tools/recovery` on a backup server. For more information on using OVAs on CloudBoot backup servers, refer to the [Administration Guide](#).

9.2   Enable Permissions in Control Panel

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

- *Any action on OVAs* - the user can take any action on OVAs

- *Create a new OVA* - the user can create a new OVA file

- *Destroy any OVA* - the user can delete any OVA (own, user, and public)

- *Destroy own OVA* - the user can delete only own OVA

- *Destroy user OVA* - the user can delete OVAs created by any user but not public OVAs

- *Make any OVA public* - the user can make public any OVA available to all users

- *Make own OVA public* - the user can make public only own OVAs

- *Create and manage OVAs* - the user can create and edit/delete/view OVAs

- *Manage public OVAs* - the user can manage public OVAs

- *Create and manage user OVAs* - the user can view/create/edit/delete OVAs created by any user

- *See all OVAs* - the user can view all OVAs in the cloud

- *See own OVAs* - the user can only view OVAs created by themselves

- *Read all public OVAs* - the user can view all public OVAs

- *See user OVAs* - the user can view OVAs created by any user in the cloud

- *Unlock any OVA* - the user can unlock any OVA that is currently being converted

- *Update any OVA* - the user can edit any OVA in the cloud

- *Update own OVA* - the user can edit only own OVA

- *Update user OVA* - the user can edit OVAs created by any user in the cloud

See also:

Manage OVAs
Install Backup Server
List of all OnApp Permissions

10 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.