

# **OnApp Cloud 5.10 Upgrade Guide**

## Table of Contents

<b>1</b>	<b>Upgrade.....</b>	<b>4</b>
<b>2</b>	<b>Upgrade Guide for Control Panel Server.....</b>	<b>5</b>
2.1	Important Notes.....	5
2.2	Upgrade Control Panel Server.....	6
<b>3</b>	<b>Upgrade Guide for Cloud with CloudBoot Servers.....</b>	<b>14</b>
3.1	Important Notes.....	14
3.2	Upgrade Control Panel Server.....	15
3.3	Upgrade CloudBoot Packages.....	23
3.4	Upgrade CloudBoot Backup Servers.....	24
3.5	Upgrade CloudBoot Compute Resources.....	24
3.5.1	Simple Reboot.....	25
3.5.2	Migrate and Reboot.....	25
3.6	Local Read Policy.....	26
<b>4</b>	<b>Upgrade Guide for Cloud with Mixed CloudBoot and Static Servers.....</b>	<b>28</b>
4.1	Important Notes.....	28
4.2	Upgrade Control Panel Server.....	29
4.3	Upgrade Static Compute Resources.....	37
4.4	Upgrade Static Backup Servers.....	38
4.5	Upgrade CloudBoot Packages.....	38
4.6	Upgrade CloudBoot Backup Servers.....	39
4.7	Upgrade CloudBoot Compute Resources.....	40
4.7.1	Simple Reboot.....	40
4.7.2	Migrate and Reboot.....	41
4.8	Local Read Policy.....	42
<b>5</b>	<b>Upgrade Guide for Cloud with Static Servers.....</b>	<b>43</b>
5.1	Important Notes.....	43
5.2	Upgrade Control Panel Server.....	44
5.3	Upgrade Static Compute Resources.....	51
5.4	Upgrade Static Backup Servers.....	53
<b>6</b>	<b>Upgrade to Custom Control Panel Version.....</b>	<b>54</b>
<b>7</b>	<b>OS Components Upgrade.....</b>	<b>55</b>
<b>8</b>	<b>OnApp IS Upgrade Paths.....</b>	<b>57</b>
8.1	General information and recommendations about CloudBoot OS and Integrated Storage upgrades.....	57
8.1.1	Each upgrade procedure explanation:.....	58
<b>9</b>	<b>Getting Support for Upgrade.....</b>	<b>59</b>

- OnApp 5.10 is an edge release which is not designed to be installed on production environments.
- You can update to OnApp 5.10 only from OnApp 5.9.

The guides in this section apply to upgrading to the OnApp Cloud 5.10 version. For the release notes list, please refer to the [Release Notes](#) space. For information on how to install OnApp 5.10, refer to the [Installation](#) guide.

# 1 Upgrade

- [Upgrade Guide for Control Panel Server](#)
- [Upgrade Guide for Cloud with CloudBoot Servers](#)
- [Upgrade Guide for Cloud with Static Servers](#)
- [Upgrade Guide for Cloud with Mixed CloudBoot and Static Servers](#)
- [Upgrade to Custom Control Panel Version](#)
- [OS Components Upgrade](#)
- [OnApp IS Upgrade Paths](#)

## 2 Upgrade Guide for Control Panel Server

- OnApp 5.10 is an edge release which is not designed to be installed on production environments.
- You can update to OnApp 5.10 only from OnApp 5.9.

This guide presents the complete walk-through how to upgrade your Control Panel server from OnApp Cloud 5.9 to 5.10. Please follow the complete procedure of the upgrade process. All packages must belong to the same major version to ensure the best performance of your cloud.

### 2.1 Important Notes

1. You must be running the latest OnApp 5.9 version to upgrade to the 5.10 version. If you are using an earlier version, please upgrade to [5.9](#) 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. If you use an isolated license, you need to manually sync with the dashboard by downloading a validation request and then uploading a validation response after the Control Panel upgrade. For more information on how to do this, refer to the [License](#) guide.
6. We strongly recommend that you test all your custom scripts before upgrading your production environment.
7. If you use custom languages on your CP, after the update please check the [i18n Customization](#) menu to submit translations for new UI labels, texts, and messages that will be available in the *Missing translations* tab.

If you are using WHMCS modules for OnApp, it is not recommended to update your cloud to the edge release. To ensure that all WHMCS modules are working correctly you need to be running a Stable or LTS OnApp version.

#### On this page:

[Important Notes](#)  
[Upgrade Control Panel Server](#)

#### See also:

[Installation Guide](#)  
[Upgrade Guide for Cloud with CloudBooted Servers](#)  
[Upgrade Guide for Cloud with Static Servers](#)  
[Upgrade Guide for Cloud with Mixed CloudBooted and Static Servers](#)

### 2.2 Upgrade Control Panel Server

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

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-5.10.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.

Before updating the OnApp Control Panel installer package, apply the following changes to the `/onapp/onapp-cp.conf` file to avoid the RC4 Cipher Suite ([CVE-2015-2808](#)) vulnerability.

```
SSLCIPHERSUITE="EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:EECDH:EDH+aRSA:RC4:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!3DES"
SSLPROTOCOL="all -SSLv2 -SSLv3 -TLSv1"
```

Template server URL

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

# IPs (separated with coma) list for the SNMP to trap. This is the list of Control Panel IP addresses on which the traps sent from the compute resources are processed.

```
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'
```

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

```
MYSQL_WAIT_TIMEOUT=604800
MYSQL_MAX_CONNECTIONS=500
MYSQL_LIMITNOFILE=8192
```

# [Use MariaDB instead of MySQL as OnApp database server](#) (Deprecated parameter. If you set any values for this parameter, they will not take effect)

```
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. Only change this value if you understand what it does.
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
and number of dumps to keep
DB_DUMP_SERVER=""
DB_DUMP_USER="root"
DB_DUMP_SERVER_ROOT="/onapp/backups"
DB_DUMP_SERVER_SSH_OPT="-o StrictHostKeyChecking=no -o
UserKnownHostsFile=/dev/null -o PasswordAuthentication=no"
KEEP_DUMPS=100
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. (Deprecated parameter. If you set any values
for this 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 0.
MAX_UPLOAD_SIZE=0

# Timeout before ping Redis Server to check if it is started. Default is 10 sec.
REDIS_PING_TIMEOUT=10

# 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)
# SSLCertificateFile, 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=""
```

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

5. Run Control Panel installer:

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

For correct display of events you need to update Control Panel with the with the option

--rake=messaging:fix\_events\_data. To do this, run the following command:

```
/onapp/onapp-cp-install/onapp-cp-install.sh --
rake=messaging:fix_events_data
```

If you did not run the rake task during the Control Panel update, you can do it manually after the Control Panel update is done. To do this, run the following command:

```
# cd /onapp/interface/
# su onapp
# rake messaging:fix_events_data
```

The full list of Control Panel installer options.

**Usage:**

```
/onapp/onapp-cp-install/onapp-cp-install.sh [-c CONFIG_FILE] [--
mariadb | --community | --percona | --percona-cluster] [-m
MYSQL_HOST] [--mysql-port=MYSQL_PORT] [--mysql-sock=MYSQL SOCK] [-p
MYSQL_PASSWD] [-d MYSQL_DB] [-u MYSQL_USER] [-U ADMIN_LOGIN] [-P
ADMIN_PASSWD] [-F ADMIN_FIRSTNAME] [-L ADMIN_LASTNAME] [-E
ADMIN_EMAIL] [-v ONAPP_VERSION] [-i SNMP_TRAP_IPS] [--redis-
host=REDIS_HOST] [--redis-bind=REDIS_BIND] [--redis-
passwd=REDIS_PASSWD] [--redis-port=REDIS_PORT] [--redis-
sock=REDIS SOCK] [--rbrhost RBT_HOST] [--vcdlogin VCD_LOGIN] [--
vcdpasswd VCD_PASSWD] [--vcdvhost VCD_VHOST] [--rbtlogin RBT_LOGIN]
[--rbtpasswd RBT_PASSWD] [-a] [-y] [-D] [-t] [--noservices] [--ha-
install] [--rake=RAKE_TASKS] [-h]
```

Where:	
Database server options:	Default database SQL server is MySQL Server. Please use one of the following option to install LOCALLY.
--mariadb	MariaDB Server

--community	MySQL Community Server
--percona	Percona Server
--percona-cluster	Percona Cluster
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 value is 3306 for the local installation
--mysql-sock[=MYSQL SOCK]	Unix socket on which MySQL Server serves connections. Default value 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.
-d MYSQL_DB	OnApp MySQL database name. Default is 'onapp'
-u MYSQL_USER	MySQL user. Default is 'root'
REDIS_*	Options are useful if Redis Server is already installed and configured.
--redis-host=REDIS_HOST	IP address/FQDN where Redis Server runs. It is used by Control Panel to connect to Redis Server. 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. Default value is 127.0.0.1. If local Redis, it will serve as well on the unix socket 'PORT' (if --redis-sock without argument isn't specified).
--redis-bind[=REDIS_BIND]	The IP address for Redis Server to serve connections (to listen). The option isn't mandatory.
--redis-port=REDIS_PORT	Redis Server listen port. Defaults are: 0 - if local server 6379 - if remote server
--redis-passwd[=REDIS_PASSWD]	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.
--redis-sock[=REDIS SOCK]:	Path to the Redis Server's socket. Used if local server only. Default is

	/var/run/redis/redis.sock. The socket is unset if the option's argument isn't specified.
ADMIN_*	Options are used to configure OnApp Control Panel administrator data. Please note, that these options are for NEW INSTALL only and not for upgrade
-P ADMIN_PASSWD	CP administrator password
-F ADMIN_FIRSTNAME	CP administrator first name
-L ADMIN_LASTNAME	CP administrator last name
-E ADMIN_EMAIL	CP administrator e-mail
--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 value is 127.0.0.1.
VCD_*	Options are usefull if vCloud/RabbitMQ are already installed and configured.
--vcdlogin VCD_LOGIN	RabbitMQ/vCloud user. Default value is 'rbtvcd'.
--vcdpasswd VCD_PASSWD	RabbitMQ/vCloud user password. The random password is generated if isn't specified.
--vcdvhost VCD_VHOST	RabbitMQ/vCloud vhost. Default value is '/'
RBT_*	Options are used to configure RabbitMQ manager account. If local RabbitMQ server.
--rbtlogin RBT_LOGIN	RabbitMQ manager login. The default value is 'rbtmgr'.
--rbtpasswd RBT_PASSWD	RabbitMQ manager password. The random password is generated if isn't specified.
--rake RAKE_TASKS	List of OnApp Control Panel rake tasks (separated with space) to run at the very end of install or upgrade.
-v ONAPP_VERSION	Install custom OnApp CP version
-i SNMP_TRAP_IPS	IP addresses separated with coma for snmp to trap
-y	Update OS packages (except of OnApp provided) on the box with 'yum update'.
-a	Is not 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.
--quick --quick-update[=SERVICE]	Proceed with quick update procedure. This will skip update and configuration for services, such as system packages, MySQL database, Redis Server, RabbitMQ Server, and Monit service. Set the SERVICE parameter (space separated list of statements) to define services, which need to be updated. Possible reserved statements are: <i>rpms</i> - for 'system packages' upgrade; <i>mysql</i> - for MySQL database upgrade and configuring; <i>redis</i> - for ERedis Server upgrade and configuring; <i>rabbitmq</i> - for RabbitMQ Server upgrade and configuring; <i>monit</i> - for Monit upgrade and configuring.
--accept-eula	Automatically accept OnApp's End User License Agreement.
-c CONFIG_FILE	Custom installer configuration file. Otherwise, preinstalled one is used.
-h	Print this info

You may want 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.

## 3 Upgrade Guide for Cloud with CloudBoot Servers

- OnApp 5.10 is an edge release which is not designed to be installed on production environments.
- You can update to OnApp 5.10 from only from OnApp 5.9.

This guide presents the complete walk-through on how to upgrade OnApp Cloud 5.9 to 5.10 for the cloud configuration where all servers are CloudBoot except for the Control Panel server. Please follow the complete procedure of the upgrade process. All the packages (Control Panel, CloudBoot, Compute resources) must belong to the same major version to ensure the best performance of your cloud.

### 3.1 Important Notes

1. You must be running the latest OnApp 5.9 version to upgrade to the 5.10 version. If you are using an earlier version, please upgrade to [5.9](#) first.
2. When upgrading CloudBoot CentOS 7 KVM compute resources, you may face dangling device mappers. This is a known issue that doesn't affect the upgrade and that will be fixed in the future OnApp releases.
3. 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.
4. Make sure no Control Panel files are open for editing under the root user account.
5. If you plan to deploy [Accelerator](#), refer to the [RabbitMQ Configuration for Accelerator](#) document for more details.
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.
10. If you use custom languages on your CP, after the update please check the [i18n Customization](#) menu to submit translations for new UI labels, texts, and messages that will be available in the *Missing translations* tab.

- Drives assigned for use by Integrated Storage are identified using a disk signature that is generated using SCSI page query mechanism to the device. Please note that disk signatures may change across different kernel versions following an upgrade and reboot. If this occurs, go to the compute resource edit page to re-identify and select the correct drives. Please contact support if you have any concerns regarding this operation.
- If you are using WHMCS modules for OnApp, it is not recommended to update your cloud to the edge release. To ensure that all WHMCS modules are working correctly you need to be running a Stable or LTS OnApp version.

**On this page:**

[Important Notes](#)  
[Upgrade Control Panel Server](#)  
[Upgrade CloudBoot Packages](#)  
[Local Read Policy](#)

**See also:**

[Installation Guide](#)  
[Upgrade Guide for Control Panel Server](#)  
[Upgrade Guide for Cloud with Static Servers](#)  
[Upgrade Guide for Cloud with Mixed CloudBoot and Static Servers](#)

## 3.2 Upgrade Control Panel Server

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

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-5.10.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.

Before updating the OnApp Control Panel installer package, apply the following changes to the `/onapp/onapp-cp.conf` file to avoid the RC4 Cipher Suite ([CVE-2015-2808](#)) vulnerability.

```
SSLCIPHERSUITE="EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:EECDH:EDH+aRSA:RC4:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!3DES"
SSLPROTOCOL="all -SSLv2 -SSLv3 -TLSv1"
```

### Template server URL

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

# IPs (separated with coma) list for the SNMP to trap. This is the list of Control Panel IP addresses on which the traps sent from the compute resources are processed.

```
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'
```

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

```
MYSQL_WAIT_TIMEOUT=604800
MYSQL_MAX_CONNECTIONS=500
MYSQL_LIMITNOFILE=8192
```

# [Use MariaDB instead of MySQL as OnApp database server](#) (Deprecated parameter. If you set any values for this parameter, they will not take effect)

```
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. Only change this value if you understand what it does.

```
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 and number of dumps to keep

```
DB_DUMP_SERVER=""
DB_DUMP_USER="root"
DB_DUMP_SERVER_ROOT="/onapp/backups"
DB_DUMP_SERVER_SSH_OPT="-o StrictHostKeyChecking=no -o
UserKnownHostsFile=/dev/null -o PasswordAuthentication=no"
KEEP_DUMPS=168
DB_DUMP_CRON='40 * * * *'
```

# [Enable monit - tool for managing and monitoring Unix systems](#)

```
ENABLE_MONIT=1
```

# If enabled (the 1 value is set) - install (if local box) and configures RabbitMQ Server (messaging system) for the vCloud support. (Deprecated parameter. If you set any values for this 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 0.

```
MAX_UPLOAD_SIZE=0
```

```
# Timeout before ping Redis Server to check if it is started. Default is 10 sec.
```

```
REDIS_PING_TIMEOUT=10
```

```
# OnApp Control Panel SSL certificates (please do not change if you aren't familiar with SSL certificates)
```

```
# * The data below to generate self-signed PEM-encoded X.509 certificate
```

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

```
# SSLCertificateFile, SSLCertificateKeyFile Apache directives' values
```

```
# ssl_certificate, ssl_certificate_key Nginx directives' values
```

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

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

```
# SSLCACertificateFile, SSLCertificateChainFile Apache directives' values
```

```
# ssl_client_certificate Nginx directives' values
```

```
SSLCACERTIFICATEFILE=""
SSLCERTIFICATECHAINFILE=""
```

```
# SSLCipherSuite, SSLProtocol Apache directives' values
```

```
# ssl_ciphers, ssl_protocols Nginx directives' values
```

```
SSLCIPHERSUITE=""
SSLPROTOCOL=""
```

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

## 5. Run Control Panel installer:

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

For correct display of events you need to update Control Panel with the with the option

--rake=messaging:fix\_events\_data. To do this, run the following command:

```
/onapp/onapp-cp-install/onapp-cp-install.sh --
rake=messaging:fix_events_data
```

If you did not run the rake task during the Control Panel update, you can do it manually after the Control Panel update is done. To do this, run the following command:

```
# cd /onapp/interface/
# su onapp
# rake messaging:fix_events_data
```

The full list of Control Panel installer options:

**Usage:**

```
/onapp/onapp-cp-install/onapp-cp-install.sh [-c CONFIG_FILE] [--
mariadb | --community | --percona | --percona-cluster] [-m
MYSQL_HOST] [--mysql-port=MYSQL_PORT] [--mysql-sock[=MYSQL SOCK] [-p
MYSQL_PASSWD] [-d MYSQL_DB] [-u MYSQL_USER] [-U ADMIN_LOGIN] [-P
ADMIN_PASSWD] [-F ADMIN_FIRSTNAME] [-L ADMIN_LASTNAME] [-E
ADMIN_EMAIL] [-v ONAPP_VERSION] [-i SNMP_TRAP_IPS] [--redis-
host=REDIS_HOST] [--redis-bind[=REDIS_BIND] [--redis-
passwd[=REDIS_PASSWD] [--redis-port=REDIS_PORT] [--redis-
sock[=REDIS SOCK] [--rbthost RBT_HOST] [--vcdlogin VCD_LOGIN] [--
vcdpasswd VCD_PASSWD] [--vcdyhost VCD_VHOST] [--rbtlogin RBT_LOGIN]
[--rbtpasswd RBT_PASSWD] [-a] [-y] [-D] [-t] [--noservices] [--ha-
install] [--rake=RAKE_TASKS] [-h]
```

<b>Where:</b>	
Database server options:	Default database SQL server is MySQL Server. Please use one of the following option to install LOCALLY.
--mariadb	MariaDB Server
--community	MySQL Community Server
--percona	Percona Server
--percona-cluster	Percona Cluster
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.
-d MYSQL_DB	OnApp MySQL database name. Default is 'onapp'
-u MYSQL_USER	MySQL user. Default is 'root'
REDIS_*	Options are useful if Redis Server is already installed and configured.
--redis-host=REDIS_HOST	IP address/FQDN where Redis Server runs. It is used by Control Panel to connect to Redis Server. 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. Default value is 127.0.0.1. If local Redis, it will serve as well on the unix socket 'PORT' (if --redis-sock without argument isn't specified).
--redis-bind[=REDIS_BIND]	The IP address for Redis Server to serve

	connections (to listen). The option isn't mandatory.
--redis-port=REDIS_PORT	Redis Server listen port. Defaults are: 0 - if local server 6379 - if remote server
--redis-passwd[=REDIS_PASSWD]	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.
--redis-sock[=REDIS SOCK]:	Path to the Redis Server's socket. Used if local server only. Default is /var/run/redis/redis.sock. The socket is unset if the option's argument isn't specified.
ADMIN_*	Options are used to configure OnApp Control Panel administrator data. Please note, that these options are for NEW INSTALL only and not for upgrade
-P ADMIN_PASSWD	CP administrator password
-F ADMIN_FIRSTNAME	CP administrator first name
-L ADMIN_LASTNAME	CP administrator last name
-E ADMIN_EMAIL	CP administrator e-mail
--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 value is 127.0.0.1.
VCD_*	Options are usefull if vCloud/RabbitMQ are already installed and configured.
--vcdlogin VCD_LOGIN	RabbitMQ/vCloud user. Default value is 'rbtvcd'.
--vcdpasswd VCD_PASSWD	RabbitMQ/vCloud user password. The random password is generated if isn't specified.
--vcdvhost VCD_VHOST	RabbitMQ/vCloud vhost. Default value is '/'
RBT_*	Options are used to configure RabbitMQ manager account. If local RabbitMQ server.
--rbtlogin RBT_LOGIN	RabbitMQ manager login. The default value is 'rbtmgr'.
--rbtpasswd RBT_PASSWD	RabbitMQ manager password. The random password is generated if isn't specified.
--rake RAKE_TASKS	List of OnApp Control Panel rake tasks

	(separated with space) to run at the very end of install or upgrade.
-v ONAPP_VERSION	Install custom OnApp CP version
-i SNMP_TRAP_IPS	IP addresses separated with coma for snmp to trap
-y	Update OS packages (except of OnApp provided) on the box with 'yum update'.
-a	Is not 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.
--quick --quick-update[=SERVICE]	Proceed with quick update procedure. This will skip update and configuration for services, such as system packages, MySQL database, Redis Server, RabbitMQ Server, and Monit service. Set the SERVICE parameter (space separated list of statements) to define services, which need to be updated. Possible reserved statements are: <i>rpms</i> - for 'system packages' upgrade; <i>mysql</i> - for MySQL databse upgrade ond configuring; <i>redis</i> - for ERedis Server upgrade and configuring; <i>rabbitmq</i> - for RabbitMQ Server upgrade and configuring; <i>monit</i> - for Monit upgrade and configuring.
--accept-eula	Automatically accept OnApp's End User License Agreement.
-c CONFIG_FILE	Custom installer configuration file. Otherwise, preinstalled one is used.
-h	Print this info

You may want 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.

### 3.3 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:

```
CP_host#> rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.10.noarch.rpm
```

2. Upgrade the packages:

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

DISTRO - 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#> # 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-centos6-xen
bash#> # yum update onapp-ramdisk-centos7-kvm
```

After packages update go to the Control Panel's **Settings** menu > **Configuration** and click the **Save Configuration** button.

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.

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

## 3.5 Upgrade CloudBoot Compute Resources

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

<b>Simple Reboot</b>	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).
<b>Migrate and reboot</b>	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.

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](#).

If you are using the [auto-healing](#) functionality for Integrated Storage, make sure to disable it before an upgrade.

### 3.5.1 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 click 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.

### 3.5.2 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. 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
```

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

2. 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.
3. After that, go to your Control Panel **Settings** menu.
4. Click the **Compute Resources** icon.
5. Click the label of the CloudBoot compute resource you have migrated all VSs from.
6. 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.

7. A new screen will open asking for confirmation (via two checkboxes) before reboot:
  - o **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 the 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.
  - o **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 disks 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 lose access to the vdisk. It can be manifested as IO errors during writes or reads to/from the vdisk inside the virtual server.

8. When you're certain you want to proceed with the reboot, click the **Reboot** button.

9. Repeat these steps for all CloudBoot compute resources in your cloud.

## 3.6 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.

## 4 Upgrade Guide for Cloud with Mixed CloudBoot and Static Servers

- OnApp 5.10 is an edge release which is not designed to be installed on production environments.
- You can update to OnApp 5.10 only from OnApp 5.9.

This guide explains how to upgrade OnApp Cloud 5.9 to 5.10 for the cloud with the mixed CloudBoot 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 the packages (Control Panel, CloudBoot, Compute resources) must belong to the same major version to ensure the best performance of your cloud.

### 4.1 Important Notes

1. You must be running the latest OnApp 5.9 version to upgrade to the 5.10 version. If you are using an earlier version, please upgrade to [5.9](#) first.
2. When upgrading CloudBoot CentOS 7 KVM compute resources, you may face dangling device mappers. This is a known issue that doesn't affect the upgrade and that will be fixed in the future OnApp releases.
3. 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.
4. Make sure no Control Panel files are open for editing under the root user account.
5. If you plan to deploy [Accelerator](#), refer to the [RabbitMQ Configuration for Accelerator](#) document for more details.
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.
10. If you use custom languages on your CP, after the update please check the [i18n Customization](#) menu to submit translations for new UI labels, texts, and messages that will be available in the *Missing translations* tab.

- Drives assigned for use by Integrated Storage are identified using a disk signature that is generated using SCSI page query mechanism to the device. Please note that disk signatures may change across different kernel versions following an upgrade and reboot. If this occurs, go to the compute resource edit page to re-identify and select the correct drives. Please contact support if you have any concerns regarding this operation.
- If you are using WHMCS modules for OnApp, it is not recommended to update your cloud to the edge release. To ensure that all WHMCS modules are working correctly you need to be running a Stable or LTS OnApp version.

**On this page:**

[Important Notes](#)  
[Upgrade Control Panel Server](#)  
[Upgrade Static Compute Resources](#)  
[Upgrade CloudBoot Compute Resources](#)  
[Local Read Policy](#)

**See also:**

[Installation Guide](#)  
[Upgrade Guide for Control Panel Server](#)  
[Upgrade Guide for Cloud with CloudBooted Servers](#)  
[Upgrade Guide for Cloud with Static Servers](#)

## 4.2 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.
- Installer output is redirected to `./onapp-cp-install.log`
- All installer critical errors are in `/var/log/messages`

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-5.10.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.

Before updating the OnApp Control Panel installer package, apply the following changes to the `/onapp/onapp-cp.conf` file to avoid the RC4 Cipher Suite ([CVE-2015-2808](#)) vulnerability.

```
SSLCIPHERSUITE="EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:EECDH:EDH+aRSA:RC4:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!3DES"
SSLPROTOCOL="all -SSLv2 -SSLv3 -TLSv1"
```

Template server URL

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

# IPs (separated with coma) list for the SNMP to trap. This is the list of Control Panel IP addresses on which the traps sent from the compute resources are processed.

```
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'

# MySQL/MariaDB server configuration data (in case of local server)
MYSQL_WAIT_TIMEOUT=604800
MYSQL_MAX_CONNECTIONS=500
MYSQL_LIMITNOFILE=8192

# Use MariaDB instead of MySQL as OnApp database server (Deprecated parameter. If
you set any values for this parameter, they will not take effect)
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. Only change this value if you understand what it does.
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
and number of dumps to keep
DB_DUMP_SERVER=""
DB_DUMP_USER="root"
DB_DUMP_SERVER_ROOT="/onapp/backups"
DB_DUMP_SERVER_SSH_OPT="-o StrictHostKeyChecking=no -o
UserKnownHostsFile=/dev/null -o PasswordAuthentication=no"
KEEP_DUMPS=168
DB_DUMP_CRON='40 * * * *'

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

# If enabled (the 1 value is set) - install (if local box) and configures RabbitMQ Server
(messaging system) for the vCloud support. (Deprecated parameter. If you set any values
for this 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 0.
```

```
MAX_UPLOAD_SIZE=0
```

```
# Timeout before ping Redis Server to check if it is started. Default is 10 sec.
```

```
REDIS_PING_TIMEOUT=10
```

```
# OnApp Control Panel SSL certificates (please do not change if you aren't familiar with SSL
certificates)
```

```
# * The data below to generate self-signed PEM-encoded X.509 certificate
```

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

```
# SSLCertificateFile, SSLCertificateKeyFile Apache directives' values
```

```
# ssl_certificate, ssl_certificate_key Nginx directives' values
```

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

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

```
# SSLCACertificateFile, SSLCertificateChainFile Apache directives' values
```

```
# ssl_client_certificate Nginx directives' values
```

```
SSLCACERTIFICATEFILE=""
SSLCERTIFICATECHAINFILE=""
```

```
# SSLCipherSuite, SSLProtocol Apache directives' values
```

```
# ssl_ciphers, ssl_protocols Nginx directives' values
```

```
SSLCIPHERSUITE=""
SSLPROTOCOL=""
```

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

## 5. Run Control Panel installer:

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

For correct display of events you need to update Control Panel with the with the option

--rake=messaging:fix\_events\_data. To do this, run the following command:

```
/onapp/onapp-cp-install/onapp-cp-install.sh --
rake=messaging:fix_events_data
```

If you did not run the rake task during the Control Panel update, you can do it manually after the Control Panel update is done. To do this, run the following command:

```
# cd /onapp/interface/
```

```
# su onapp
# rake messaging:fix_events_data
```

The full list of Control Panel installer options:

**Usage:**

```
/onapp/onapp-cp-install/onapp-cp-install.sh [-c CONFIG FILE] [--mariadb | --community | --percona | --percona-cluster] [-m MYSQL_HOST] [--mysql-port=MYSQL_PORT] [--mysql-sock=MYSQL SOCK] [-p MYSQL_PASSWD] [-d MYSQL_DB] [-u MYSQL_USER] [-U ADMIN_LOGIN] [-P ADMIN_PASSWD] [-F ADMIN_FIRSTNAME] [-L ADMIN_LASTNAME] [-E ADMIN_EMAIL] [-v ONAPP_VERSION] [-i SNMP_TRAP_IPS] [--redis-host=REDIS_HOST] [--redis-bind=REDIS_BIND] [--redis-passwd=REDIS_PASSWD] [--redis-port=REDIS_PORT] [--redis-sock=REDIS SOCK] [--rbthost RBT_HOST] [--vcdlogin VCD_LOGIN] [--vcdpasswd VCD_PASSWD] [--vcdvhost VCD_VHOST] [--rbtlogin RBT_LOGIN] [--rbtpasswd RBT_PASSWD] [-a] [-y] [-D] [-t] [--noservices] [--ha-install] [--rake=RAKE_TASKS] [-h]
```

<b>Where:</b>	
Database server options:	Default database SQL server is MySQL Server. Please use one of the following option to install LOCALLY.
--mariadb	MariaDB Server
--community	MySQL Community Server
--percona	Percona Server
--percona-cluster	Percona Cluster
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.
-d MYSQL_DB	OnApp MySQL database name. Default is 'onapp'
-u MYSQL_USER	MySQL user. Default is 'root'
REDIS_*	Options are useful if Redis Server is already installed and configured.
--redis-host=REDIS_HOST	IP address/FQDN where Redis Server runs. It is used by Control Panel to connect to Redis Server. 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. Default value is 127.0.0.1. If local

	Redis, it will serve as well on the unix socket 'PORT' (if --redis-sock without argument isn't specified).
--redis-bind[=REDIS_BIND]	The IP address for Redis Server to serve connections (to listen). The option isn't mandatory.
--redis-port=REDIS_PORT	Redis Server listen port. Defaults are: 0 - if local server 6379 - if remote server
--redis-passwd[=REDIS_PASSWD]	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.
--redis-sock[=REDIS SOCK]:	Path to the Redis Server's socket. Used if local server only. Default is /var/run/redis/redis.sock. The socket is unset if the option's argument isn't specified.
ADMIN_*	Options are used to configure OnApp Control Panel administrator data. Please note, that these options are for NEW INSTALL only and not for upgrade
-P ADMIN_PASSWD	CP administrator password
-F ADMIN_FIRSTNAME	CP administrator first name
-L ADMIN_LASTNAME	CP administrator last name
-E ADMIN_EMAIL	CP administrator e-mail
--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 value is 127.0.0.1.
VCD_*	Options are usefull if vCloud/RabbitMQ are already installed and configured.
--vcdlogin VCD_LOGIN	RabbitMQ/vCloud user. Default value is 'rbtvcd'.
--vcdpasswd VCD_PASSWD	RabbitMQ/vCloud user password. The random password is generated if isn't specified.
--vcdvhost VCD_VHOST	RabbitMQ/vCloud vhost. Default value is '/'
RBT_*	Options are used to configure RabbitMQ manager account. If local RabbitMQ server.
--rbtlogin RBT_LOGIN	RabbitMQ manager login. The default value is 'rbtmgr'.
--rbtpasswd RBT_PASSWD	RabbitMQ manager password. The random

	password is generated if isn't specified.
--ha-install	Proceed with Control Panel and High Availability components installation.
--rake RAKE_TASKS	List of OnApp Control Panel rake tasks (separated with space) to run at the very end of install or upgrade.
-v ONAPP_VERSION	Install custom OnApp CP version
-i SNMP_TRAP_IPS	IP addresses separated with coma for snmp to trap
-y	Update OS packages (except of OnApp provided) on the box with 'yum update'.
-a	Is not 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.
--quick --quick-update[=SERVICE]	Proceed with quick update procedure. This will skip update and configuration for services, such as system packages, MySQL database, Redis Server, RabbitMQ Server, and Monit service. Set the SERVICE parameter (space separated list of statements) to define services, which need to be updated. Possible reserved statements are: <i>rpms</i> - for 'system packages' upgrade; <i>mysql</i> - for MySQL database upgrade and configuring; <i>redis</i> - for ERedis Server upgrade and configuring; <i>rabbitmq</i> - for RabbitMQ Server upgrade and configuring; <i>monit</i> - for Monit upgrade and configuring.
--accept-eula	Automatically accept OnApp's End User License Agreement.
-c CONFIG_FILE	Custom installer configuration file.

	Otherwise, preinstalled one is used.
-h	Print this info

You may want 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.

### 4.3 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:

```
bash#> rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.10.noarch.rpm
```

3. Upgrade OnApp compute resource installer package:

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

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

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

5. Run compute resource installer:

For CentOS Xen compute resources:

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

For CentOS KVM compute resources:

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

6. Gracefully reboot static compute resources from UI. To do so, log in to Control Panel and go to **Settings > Compute Resources**. Click the specific compute resource. When the page loads, click **Tools > Reboot Compute resource**. For KVM compute resources only: the kernel package update is a part of the "Upgrade Static Compute Resources" default procedure. If the kernel package was upgraded, reboot KVM compute resources to use the new kernel package.

If you do not have the `/home/mq/onapp/messaging/credentials.yml` file on your compute resources and you 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']
```

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

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

## 4.4 Upgrade Static Backup Servers

To upgrade your static backups servers, install the pciutils RPM package:

```
# yum install pciutils
```

## 4.5 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:

```
CP_host#> rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.10.noarch.rpm
```

2. Upgrade the packages:

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

DISTRO - 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#> # 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-centos6-xen
bash#> # yum update onapp-ramdisk-centos7-kvm
```

After packages update go to the Control Panel's **Settings** menu > **Configuration** and click the **Save Configuration** button.

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.

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

## 4.7 Upgrade CloudBoot Compute Resources

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

<b>Simple Reboot</b>	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).
<b>Migrate and reboot</b>	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.

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](#).

If you are using the [auto-healing](#) functionality for Integrated Storage, make sure to disable it before an upgrade.

### 4.7.1 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 click 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.

### 4.7.2 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. 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
```

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

2. 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.
3. After that, go to your Control Panel **Settings** menu.
4. Click the **Compute Resources** icon.
5. Click the label of the CloudBoot compute resource you have migrated all VSs from.
6. 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.

7. A new screen will open asking for confirmation (via two checkboxes) before reboot:
  - o **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 the 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.

- o **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 disks 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 lose access to the vdisk. It can be manifested as IO errors during writes or reads to/from the vdisk inside the virtual server.

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

## 4.8 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.

## 5 Upgrade Guide for Cloud with Static Servers

- OnApp 5.10 is an edge release which is not designed to be installed on production environments.
- You can update to OnApp 5.10 only from OnApp 5.9.

This guide explains how to upgrade OnApp Cloud 5.9 to 5.10 for the cloud where all servers are static. Follow the procedure listed below in the correct order to upgrade your cloud. All the packages (Control Panel and Compute resources) must belong to the same major version to ensure the best performance of your cloud.

### 5.1 Important Notes

1. You must be running the latest OnApp 5.9 version to upgrade to 5.10 version. If you are using an earlier version, please upgrade to [5.9](#) 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. We strongly recommend that you test all your custom scripts before upgrading your production environment.
6. Be aware that OnApp does not support UEFI on static compute resources. You should disable UEFI on your compute resources before installing OnApp.
7. If you use custom languages on your CP, after the update please check the [i18n Customization](#) menu to submit translations for new UI labels, texts, and messages that will be available in the *Missing translations* tab.

If you are using WHMCS modules for OnApp, it is not recommended to update your cloud to the edge release. To ensure that all WHMCS modules are working correctly you need to be running a Stable or LTS OnApp version.

#### On this page:

[Important Notes](#)  
[Upgrade Control Panel Server](#)  
[Upgrade Static Compute Resources](#)

#### See also:

[Installation Guide](#)  
[Upgrade Guide for Control Panel Server](#)  
[Upgrade Guide for Cloud with CloudBooted Servers](#)  
[Upgrade Guide for Cloud with Mixed CloudBooted and Static Servers](#)

### 5.2 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-5.10.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.

Before updating the OnApp Control Panel installer package, apply the following changes to the `/onapp/onapp-cp.conf` file to avoid the RC4 Cipher Suite (CVE-2015-2808) vulnerability.

```
SSLCIPHERSUITE="EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:EECDH:EDH+aRSA:RC4:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS:!RC4:!3DES"
SSLPROTOCOL="all -SSLv2 -SSLv3 -TLSv1"
```

#### Template server URL

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

# IPs (separated with coma) list for the SNMP to trap. This is the list of Control Panel IP addresses on which the traps sent from the compute resources are processed.

```
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'
```

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

```
MYSQL_WAIT_TIMEOUT=604800
MYSQL_MAX_CONNECTIONS=500
MYSQL_LIMITNOFILE=8192
```

# [Use MariaDB instead of MySQL as OnApp database server](#) (Deprecated parameter. If you set any values for this parameter, they will not take effect)

```
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. Only change this value if you understand what it does.

```
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 and number of dumps to keep

```
DB_DUMP_SERVER=""
DB_DUMP_USER="root"
DB_DUMP_SERVER_ROOT="/onapp/backups"
DB_DUMP_SERVER_SSH_OPT="-o StrictHostKeyChecking=no -o
UserKnownHostsFile=/dev/null -o PasswordAuthentication=no"
KEEP_DUMPS=100
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. (Deprecated parameter. If you set any values for this 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 0.

```
MAX_UPLOAD_SIZE=0
```

# Timeout before ping Redis Server to check if it is started. Default is 10 sec.

```
REDIS_PING_TIMEOUT=10
```

# OnApp Control Panel SSL certificates (please do not change if you aren't familiar with SSL certificates)

# \* The data below to generate self-signed PEM-encoded X.509 certificate

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

# SSLCertificateFile, SSLCertificateKeyFile Apache directives' values

# ssl\_certificate, ssl\_certificate\_key Nginx directives' values

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

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

# SSLCACertificateFile, SSLCertificateChainFile Apache directives' values

# ssl\_client\_certificate Nginx directives' values

```
SSLCACERTIFICATEFILE=""
```

```

SSLCERTIFICATECHAINFILE=""

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

SSLCIPHERSUITE=""
SSLPROTOCOL=""

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

5. Run Control Panel installer:

For CentOS Xen compute resources:

```

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

For CentOS KVM compute resources:

```

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

For correct display of events you need to update Control Panel with the
with the option

--rake=messaging:fix_events_data. To do this, run the following
command:

/onapp/onapp-cp-install/onapp-cp-install.sh --
rake=messaging:fix_events_data

If you did not run the rake task during the Control Panel update, you can
do it manually after the Control Panel update is done. To do this, run the
following command:

# cd /onapp/interface/
# su onapp
# rake messaging:fix_events_data
    
```

The full list of Control Panel installer options:

**Usage:**

```

/onapp/onapp-cp-install/onapp-cp-install.sh [-c CONFIG_FILE] [--
mariadb | --community | --percona | --percona-cluster] [-m
MYSQL_HOST] [--mysql-port=MYSQL_PORT] [--mysql-sock[=MYSQL SOCK] [-p
MYSQL_PASSWD] [-d MYSQL_DB] [-u MYSQL_USER] [-U ADMIN_LOGIN] [-P
ADMIN_PASSWD] [-F ADMIN_FIRSTNAME] [-L ADMIN_LASTNAME] [-E
ADMIN_EMAIL] [-v ONAPP_VERSION] [-i SNMP_TRAP_IPS] [--redis-
host=REDIS_HOST] [--redis-bind[=REDIS BIND] [--redis-
passwd[=REDIS_PASSWD] [--redis-port=REDIS_PORT] [--redis-
sock[=REDIS SOCK] [--rbthost RBT_HOST] [--vcdlogin VCD_LOGIN] [--
vcdpasswd VCD_PASSWD] [--vcdvhost VCD_VHOST] [--rbtlogin RBT_LOGIN]
[--rbtpasswd RBT_PASSWD] [-a] [-y] [-D] [-t] [--noservices] [--ha-
install] [--rake=RAKE_TASKS] [-h]
    
```

<b>Where:</b>	
Database server options:	Default database SQL server is MySQL Server. Please use one of the following option to install LOCALLY.
--mariadb	MariaDB Server
--community	MySQL Community Server
--percona	Percona Server

--percona-cluster	Percona Cluster
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.
-d MYSQL_DB	OnApp MySQL database name. Default is 'onapp'
-u MYSQL_USER	MySQL user. Default is 'root'
REDIS_*	Options are useful if Redis Server is already installed and configured.
--redis-host=REDIS_HOST	IP address/FQDN where Redis Server runs. It is used by Control Panel to connect to Redis Server. 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. Default value is 127.0.0.1. If local Redis, it will serve as well on the unix socket 'PORT' (if --redis-sock without argument isn't specified).
--redis-bind[=REDIS_BIND]	The IP address for Redis Server to serve connections (to listen). The option isn't mandatory.
--redis-port=REDIS_PORT	Redis Server listen port. Defaults are: 0 - if local server 6379 - if remote server
--redis-passwd[=REDIS_PASSWD]	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.
--redis-sock[=REDIS_SOCK]:	Path to the Redis Server's socket. Used if local server only. Default is /var/run/redis/redis.sock. The socket is unset if the option's argument isn't specified.
ADMIN_*	Options are used to configure OnApp

	Control Panel administrator data. Please note, that these options are for NEW INSTALL only and not for upgrade
-P ADMIN_PASSWD	CP administrator password
-F ADMIN_FIRSTNAME	CP administrator first name
-L ADMIN_LASTNAME	CP administrator last name
-E ADMIN_EMAIL	CP administrator e-mail
--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 value is 127.0.0.1.
VCD_*	Options are usefull if vCloud/RabbitMQ are already installed and configured.
--vcdlogin VCD_LOGIN	RabbitMQ/vCloud user. Default value is 'rbtvcd'.
--vcdpasswd VCD_PASSWD	RabbitMQ/vCloud user password. The random password is generated if isn't specified.
--vcdvhost VCD_VHOST	RabbitMQ/vCloud vhost. Default value is '/'
RBT_*	Options are used to configure RabbitMQ manager account. If local RabbitMQ server.
--rbtlogin RBT_LOGIN	RabbitMQ manager login. The default value is 'rbtmgr'.
--rbtpasswd RBT_PASSWD	RabbitMQ manager password. The random password is generated if isn't specified.
--rake RAKE_TASKS	List of OnApp Control Panel rake tasks (separated with space) to run at the very end of install or upgrade.
-v ONAPP_VERSION	Install custom OnApp CP version
-i SNMP_TRAP_IPS	IP addresses separated with coma for snmp to trap
-y	Update OS packages (except of OnApp provided) on the box with 'yum update'.
-a	Is not 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.
<code>--noservices</code>	Do not start OnApp services: <code>monit</code> , <code>onapp</code> and <code>httpd</code> Please note, <code>crond</code> and all OnApp's cron tasks remain running. They could be disabled by stopping <code>crond</code> service manually for your own risk.
<code>-D</code>	Do not make database dump, and make sure it is disabled in the cron and not running at the moment.
<code>--quick --quick-update[=SERVICE]</code>	Proceed with quick update procedure. This will skip update and configuration for services, such as system packages, MySQL database, Redis Server, RabbitMQ Server, and Monit service. Set the SERVICE parameter (space separated list of statements) to define services, which need to be updated. Possible reserved statements are: <i>rpms</i> - for 'system packages' upgrade; <i>mysql</i> - for MySQL database upgrade and configuring; <i>redis</i> - for Redis Server upgrade and configuring; <i>rabbitmq</i> - for RabbitMQ Server upgrade and configuring; <i>monit</i> - for Monit upgrade and configuring.
<code>--accept-eula</code>	Automatically accept OnApp's End User License Agreement.
<code>-c CONFIG_FILE</code>	Custom installer configuration file. Otherwise, preinstalled one is used.
<code>-h</code>	Print this info

You may want 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.

### 5.3 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:

```
bash#> rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.10.noarch.rpm
```

3. Upgrade OnApp compute resource installer package:

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

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

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

5. Run compute resource installer:  
For CentOS 6 XEN compute resources:

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

For CentOS 6/7 KVM and CentOS 7 Xen compute resources to download new recovery images, run:

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

6. Reboot static compute resources.

For KVM compute resources only: the kernel package update is a part of the "Upgrade Static Compute Resources" default procedure. If the kernel package was upgraded, reboot KVM compute resources to use the new kernel package.

If you do not have the `/home/mq/onapp/messaging/credentials.yml` file on your compute resources and you 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']
```

For information on manual configuration for Accelerator, refer to [RabbitMQ Configuration for Accelerator](#). To perform the configuration for a number of compute resources, separate their IPs with a space.

## 5.4 Upgrade Static Backup Servers

1. To upgrade your static backups servers, download and install the latest OnApp YUM repository file:

```
# rpm -Uvh http://rpm.repo.onapp.com/repo/onapp-repo-5.10.noarch.rpm
```

2. Update the onapp-storageAPI RPM package:

```
# yum update onapp-storageAPI
```

## 6 Upgrade to Custom Control Panel Version

- OnApp 5.10 is an edge release which is not designed to be installed on production environments.
- You can update to OnApp 5.10 only from OnApp 5.9.
- You should use the standard upgrade procedure whenever possible to ensure you have the latest features and fixes. Use the custom upgrade only when you have a specific reason for installing an older version.

### See also:

[Upgrade Guide for Control Panel Server](#)

[Upgrade Guide for Cloud with CloudBooted Servers](#)

[Upgrade Guide for Cloud with Static Servers](#)

[Upgrade Guide for Cloud with Mixed CloudBoot and Static Servers](#)

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

## 7 OS Components Upgrade

- OnApp 5.10 is an edge release which is not designed to be installed on production environments.
- You can update to OnApp 5.10 only from OnApp 5.9.

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:

- o **For Control Panel**

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

- o **For Compute resource**

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

- o **For Backup Server**

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

2. Run the following script to update the OS components

- o **For Control Panel**

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

- o **For XEN Compute resource**

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

- o **For KVM Compute resource**

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

- o **For Backup Server**

```
/onapp/onapp-bk-install/onapp-bk-install.sh -y
```

### See also:

[Upgrade Guide for Control Panel Server](#)

[Upgrade Guide for Cloud with CloudBooted Servers](#)

[Upgrade Guide for Cloud with Static Servers](#)

[Upgrade Guide for Cloud with Mixed CloudBoot and Static Servers](#)

## 8 OnApp IS Upgrade Paths

<ul style="list-style-type: none"> <li>OnApp 5.10 is an edge release which is not designed to be installed on production environments.</li> <li>You can update to OnApp 5.10 only from OnApp 5.9.</li> </ul>											
IS Version upgrading to	5.0.0-21	5.1.0-5	5.2.0-5	5.3	5.4	5.5	5.6	5.7	5.8	5.9	5.10
Upgrade by "Simple Reboot"	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Upgrade by "Migrate and Reboot"	Yes	Yes	Yes	Yes	Yes*	Yes	Yes	Yes	Yes	Yes	Yes
Upgrade by "LiveUpgrade"	N/A	N/A	Yes	N/A	Yes*	Yes	No	No	No	No	No

\* Applicable only for CentOS 6 KVM/XEN

Yes - recommended by OnApp

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

No - not available in the corresponding release

- 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 the 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.

### 8.1 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 version 4.1 requires to be rebooted after Integrated Storage update. OnApp will notify in future release notes if the Simple Reboot method is the recommended way to upgrade.

#### 8.1.1 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**

This upgrade method requires to reboot the CloudBoot compute resources to apply security patches, kernel upgrades and updated drivers to the CloudBoot OS and Integrated Storage platform. Your VSs will remain online, you only need 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 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.

- The Live Upgrade method is not available for upgrade from OnApp 5.9 to 5.10.
- Starting from OnApp 5.3, 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.

## 9 Getting Support for Upgrade

You can use the information in this space to perform your own upgrade to the 5.10 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 a usual way. Please be aware, however, that there may be a queue!