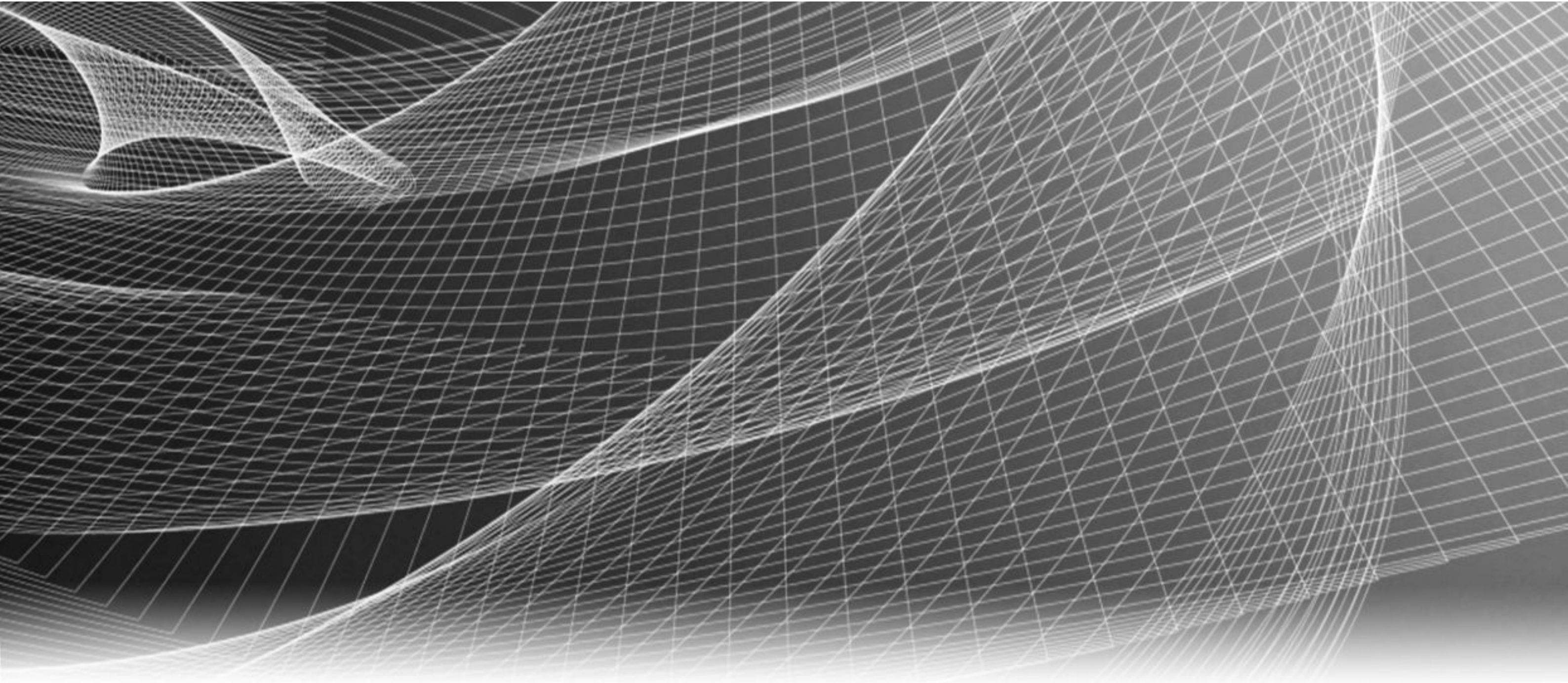


EMC NetWorker 8.x with EMC CloudBoost

Version 2.1

Integration Guide

P/N 302-001-736

REV 02

EMC^{2}

Published December 2016

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com).

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

Figures 5

Tables 7

About this document 9

Chapter 1 Introduction 11

NetWorker with CloudBoost 12

Long term retention to the cloud 12

Supported server and client versions 12

Cloud providers supported by CloudBoost appliances 13

Prepare for installing the CloudBoost appliance 14

Firewall port requirements 15

Chapter 2 EMC NetWorker with CloudBoost Solution Requirements 17

Solution requirements 18

CloudBoost sizing and performance considerations 19

CloudBoost appliance cache sizing 21

Chapter 3 Install the Virtual CloudBoost Appliance on ESX 23

Installing the virtual CloudBoost appliance 24

Chapter 4 Deploy the CloudBoost Appliance 25

Deploying the virtual CloudBoost appliance in Amazon EC2 26

Chapter 5 Configure Network Settings for a CloudBoost Appliance 27

Configuring network settings for a CloudBoost appliance 28

Chapter 6 Register and Configure a New CloudBoost Appliance 31

Create and manage cloud profiles for CloudBoost 32

Validate cloud storage credentials 32

Registering a CloudBoost appliance 34

Enable remote client mounting 35

Disable remote client mounting 35

Configuring a new CloudBoost appliance 36

Chapter 7 Integrate NetWorker 8.x with CloudBoost 39

Connecting NetWorker 8.x to CloudBoost 40

Chapter 8 Monitor, Manage, and Support CloudBoost 43

CloudBoost reporting 44
Upgrading a CloudBoost appliance 45
CloudBoost integration with EMC Secure Remote Services 45
Registering CloudBoost with EMC Secure Remote Services 46
Increasing the CloudBoost appliance site cache 47
Changing log levels for CloudBoost debugging 47
Restarting a CloudBoost appliance 48
Recovering a CloudBoost appliance 48
Deleting a CloudBoost appliance 50

Chapter 9 SSL Certificate Management for CloudBoost 53

Self-signed SSL certificates 54
    Generating a self-signed SSL certificate 54
Converting a PEM file to PKCS #12 55
Verifying your certificate 56
Manage the SSL certificate for a CloudBoost appliance 56

Chapter 10 Common Cloud Portal Tasks 57

Resetting your personal Cloud Portal password at sign-in 58
Editing your personal Cloud Portal account profile 58
Manage Cloud Portal Users 58
    Adding a new user and sending a Cloud Portal account invitation 59
    Editing a Cloud Portal user account 61
    Deleting a Cloud Portal user account 63
Changing the event notification settings in the Cloud Portal 63
Events history in the Cloud Portal 64
Getting Help inside the Cloud Portal 65

Appendix A About this document 67

FIGURES

1 Long term retention to the cloud 12
2 CLI for CloudBoost 28
3 CLI for CloudBoost 33
4 Appliances page 36
5 Appliances page 44
6 Appliance configuration details and storage use history 44
7 New, unconfigured appliance 49
8 Appliance to recover 49
9 Recover tab 50
10 CLI for CloudBoost 51
11 The Cloud Portal Help Page 65

TABLES

1 Document revision history 9
2 Supported private clouds 13
1 Supported public clouds ....
4 Firewall port requirements 15
5 Minimum and recommended configuration 21
6 How events are prioritized in Events History 64
7 Document revision history 67

About this document

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note

This document was accurate at publication time. Go to EMC Online Support at https://support.emc.com to ensure that you are using the latest version of this document.

Purpose

This document describes the integration of NetWorker® with CloudBoost™.

Audience

This guide is part of the CloudBoost documentation set, and is intended for use by system administrators who are responsible for setting up and maintaining backups on a network. Operators who monitor daily backups will also find this guide useful.

Revision history

The following table presents the revision history of this document.

Table 1 Document revision history

Revision	Date	Description
01	October 11, 2016	Initial release of *EMC Networker 8.x with CloudBoost 2.1 Integration Guide*.

Related documentation

The following EMC publications provide information about CloudBoost.

- *EMC CloudBoost Release Notes*
  Contains information about new features and changes, fixed problems, known limitations, environment and system requirements for the latest release.
- *EMC CloudBoost 100 Installation Guide*
  Guide for installing the physical CloudBoost 100 appliance, and initial configuration at command line interface.
- *EMC CloudBoost Disk Array Expansion Shelf Installation Guide*
  Guide for installing the disk array expansion shelf for use with the physical appliance.
- *EMC CloudBoost Hardware Component Replacement Guide*
  Guide for customers replacing hardware components for the CloudBoost physical appliance.

You may find these publications helpful when integrating CloudBoost with different systems.

- *EMC NetWorker with EMC CloudBoost Integration Guide*
  Guide for integrating EMC NetWorker with EMC CloudBoost.

- *EMC NetWorker 8.x with EMC CloudBoost Integration Guide*
  Guide for integrating EMC NetWorker 8.x with EMC CloudBoost.
- *EMC Avamar with EMC CloudBoost Integration Guide*
  Guide for integrating EMC Avamar with EMC CloudBoost.
- *Veritas NetBackup with EMC CloudBoost Integration Guide*
  Guide for integrating Veritas NetBackup with EMC CloudBoost.

You may also find it helpful to refer to these NetWorker publications.

- *EMC NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *EMC NetWorker Installation Guide*
  Provides information about how to install, uninstall, and update the NetWorker software for clients, storage nodes, and serves on all supported operating systems.

Where to get support

Go to EMC Online Support at https://support.emc.com/ and click **Service Center**. You will see several options for contacting EMC Technical Support. To open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

How to provide feedback

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to mailto:techpubcomments@emc.com.

Please include the following information.

- Product name and version
- Document name, part number, and revision (for example, 01)
- Page numbers
- Topic titles
- Other details to help address documentation issues

CHAPTER 1

Introduction

The CloudBoost appliance provides an integration into your existing supported backup environment. This enables you to transfer backups to the cloud. The CloudBoost appliance enables backups to public, hybrid, or private cloud storage.

CloudBoost decouples metadata from data, which removes a bottleneck for cloud reads and writes. Encryption keys, metadata, and file system information are housed separately from the data. All advanced data services, such as chunking, encryption, inline de-duplication, compression, and bulk data transfers are performed separately from storing the metadata.

CloudBoost is available as a physical appliance, a VMware virtual appliance, and a virtual appliance resident in Amazon EC2.

CloudBoost is integrated with EMC Secure Remote Services, which may be enabled to monitor the health of the appliances.

Individual CloudBoost™ deployments can support only one target object store. When a cloud object store is selected and the CloudBoost appliance is configured, the appliance is locked to that target. To change object storage targets, the appliance must be re-deployed.

- NetWorker with CloudBoost........12
- Supported server and client versions........12
- Cloud providers supported by CloudBoost appliances........13
- Prepare for installing the CloudBoost appliance........14
- Firewall port requirements........15

NetWorker with CloudBoost

NetWorker with CloudBoost sends a backup clone to the CloudBoost appliance. CloudBoost translates these clones into generic objects which are sent to an object store, which can be a public, private, or hybrid cloud.

The CloudBoost appliance presents itself as a NetWorker Advanced File Type Device. The enabled workflow is a clone operation to the cloud; it is not a backup to the cloud. With this low cost tape replacement solution, each CloudBoost appliance can support up to 6 PB of addressable back end storage.

Long term retention to the cloud

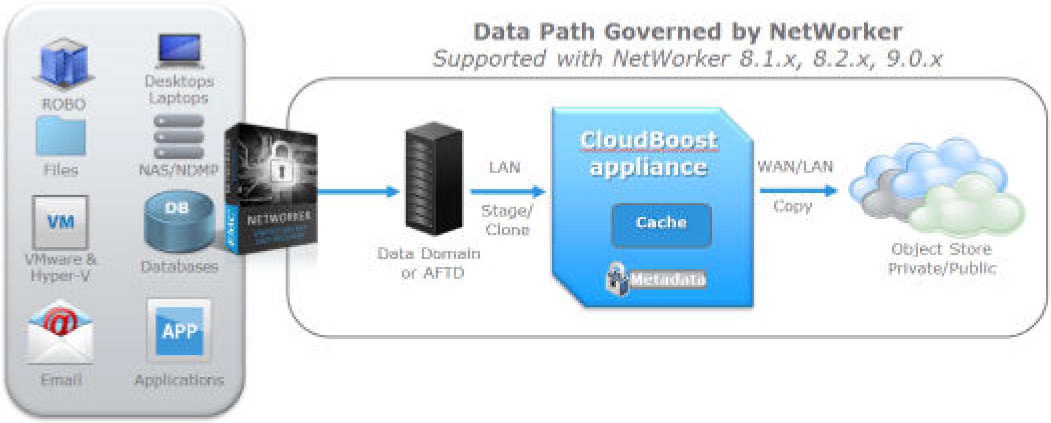
Versions of the CloudBoost appliance earlier than 2.1 only enabled a clone operation to the cloud; it is not a direct backup to the cloud.

This use case is intended for when the customer has existing on-site infrastructure and would like to use object storage for long-term retention and compliance requirements. Backup copies required for short term operational recovery remain on-site for fast restore. An optional disaster recovery site may be established for contingency purposes.

The optional site cache eliminates the impact of long-distance connectivity. Site caches are beneficial for environments such as remote and branch offices where low bandwidth, high latency, or network reliability may be an issue.

NetWorker sends backup clones to the CloudBoost appliance, which translates the clones into generic objects that are sent to an object store. The object store can be a public, private, or hybrid cloud. The CloudBoost appliance presents itself in NetWorker Server 8.1.x and 8.2.x as a NetWorker Advanced File Type Device.

Figure 1 Long term retention to the cloud



Supported server and client versions

These server and client versions are supported in CloudBoost integrations.

For a complete list of supported clients, see the Software Compatibility Guides at http://compatibilityguide.emc.com:8080/CompGuideApp/.

NetWorker 8.2.x client with CloudBoost 2.1 or later requirements and limitations

The following is the suggested solution requirements and limitations for NetWorker 8.2.x with CloudBoost 2.1 or later appliance.

- Support for all clients cloning to the cloud for long term retention.
- Support for all clients back up to the cloud with the following exceptions.
  - Microsoft Windows file system block-based backups
  - Microsoft Exchange backups
  - Microsoft Hyper-V backups
  - VMWare image backups

Note

- The minimum version of NetWorker Module for Microsoft (NMM) that is supported with CloudBoost is 8.2.3.6.
- Granular recovery from cloned image level backups (VMWare, Microsoft Hyper-V, and Microsoft Exchange) is only possible if a backup is cloned back to local storage first.

Cloud providers supported by CloudBoost appliances

CloudBoost appliances support these private and public clouds.

Table 2 Supported private clouds

Cloud provider	Information required by CloudBoost
EMC ATMOS	Access Point URL, Full Token ID (subtenant/uid), Shared Secret
EMC ECS Appliance	ECS Endpoint, ECS Access Key ID, ECS Secret Access Key
Generic OpenStack Swift	Swift Provider Authentication Endpoint, Swift Authentication Type, Region (optional), Swift Credentials (as tenant name and username separate by a colon, then password), Swift Secret Key

Table 3 Supported public clouds

Cloud provider	Information required by CloudBoost
Virtustream Storage Cloud (Standard and Premium)	Pre-configured as a Cloud Profile when ordered. Provisioned by EMC Sales. Virtustream Storage Cloud is available for use only with specific EMC appliances, such as CloudBoost. It is a viable alternative to general-purpose public cloud storage with advantages of ease of use. When provisioned by EMC Sales, standard and premium cloud profiles are automatically available.
Amazon Web Services (S3)	Storage Region, AWS Access Key ID, AWS Secret Access Key
AT&T Synaptic Storage	AT&T Synaptic Subtenant ID, AT&T Synaptic User ID, AT&T Synaptic Secret Key
Google Cloud Storage (Standard, DRA, Nearline)	Access Key, Secret

Table 3 Supported public clouds (continued)

Cloud provider	Information required by CloudBoost
	Note Integration with Google Cloud Storage relies on the XML v1.0 API, which is not enabled by default. To learn how to enable access to v.1.0 by setting a default project and generating S3-compatible credentials, see the Google developer documentation at https://cloud.google.com/storage/docs/migrating?hl=en#migration-simple.
Microsoft Azure Storage (general purpose accounts, replication types LRS, GRS, RA-GRS)	Azure Account Name, Azure API Key **Note** Object storage only accounts are not supported.

Prepare for installing the CloudBoost appliance

Perform these tasks before you install the CloudBoost appliance. You must ensure proper integration with the DHCP, DNS, Active Directory, and ports configuration.

- Obtain the necessary credentials for your cloud storage profile, such as the endpoint URL, the token ID or access key, and the secret key. For more information, see Cloud providers supported by CloudBoost appliances on page 13.
- Determine the fully qualified domain name for your CloudBoost deployment.
- Obtain a static IP or reserved DHCP address for the CloudBoost appliance and determine the subnet mask, the gateway, and create forward and reverse DNS records.
- Register the CloudBoost hostname/IP address in DNS. The hostname/IP address must be statically registered in DNS regardless of any mappings created by DHCP. Failure to do this may result in indeterministic service unavailability and downtime.
- For integration with Active Directory, identify the full domain name, such as corp.example.com, and a domain user with privileges to join a computer to the domain. This is an elevated permission and may require assistance from a domain administrator.

  Note

  Integration with Active Directory for centralized credential management and authentication is not required for CloudBoost, but is highly recommended for production deployments. Operating the CloudBoost appliance without authentication and AD integration is useful for evaluation and test deployments.

- Open the necessary ports. For more information, see Firewall port requirements on page 15.
- By default, CloudBoost uses a self-signed SSL certificate. If you intend to use a publicly signed certificate, you should plan and prepare your SSL Certificate usage for testing and production environments. For more information, see SSL Certificate Management for CloudBoost on page 53.

- Install the EMC NetWorker 8.x server if you have not all ready installed the server. For more information, see the *NetWorker 8.2.x Administration Guide*.

Firewall port requirements

As with all networked software solutions, adhering to best practices for security is encouraged to protect your deployment. If these ports are not configured before you configure the CloudBoost appliance, it will be necessary to reboot the CloudBoost appliance.

Note

It is not recommended to route outbound http traffic from the CloudBoost appliance through a proxy. This can create a performance bottleneck. In environments where outbound http traffic is restricted, it is recommended to create an exception for the appliance in the firewall after consultation with the IT security team.

Table 4 Firewall port requirements

Out	In	TCP Port	Description
Administrator workstation	CloudBoost appliance	22	SSH for maintenance and troubleshooting
CloudBoost appliance	• Cloud storage (public or private) • EMC Cloud Portal • Ubuntu upgrade server • CloudBoost upgrade server	443	• HTTPS to access object store (if supported) • HTTPS to EMC Cloud Portal and Cloud Portal Services/APIs • https://mirrors.kernel.org This is required only for initial configuration. It is not used during normal operations. • https://upgrade-prd.s.objectstorage.io This is required when the CloudBoost appliance upgrades
Administrator workstation	CloudBoost appliance	4444	HTTPS to local appliance administration page that is used by support for troubleshooting
NetWorker server	CloudBoost appliance	7937–7999	When NetWorker is deployed with CloudBoost, this is necessary for various NetWorker services.
CloudBoost appliance	ECS storage	9020–9021	
CloudBoost appliance	ESRS gateway	9443	Communication from CloudBoost appliance to the EMC Secure Remote Services gateway

For information about firewall ports for any system being deployed with CloudBoost, refer to the documentation for that system.

For information about NetWorker, see Configuring TCP Networks and Network Firewalls for EMC NetWorker at http://www.emc.com

CHAPTER 2

EMC NetWorker with CloudBoost Solution Requirements

Before you begin the installation and configuration of your CloudBoost appliance, it is important that you understand all the requirements ahead of time.

- Solution requirements..18
- CloudBoost sizing and performance considerations.. 19
- CloudBoost appliance cache sizing... 21

Solution requirements

Requirements for the CloudBoost appliance.

Minimum deployment virtual machine requirements for ESX

These are the minimum and default requirements for the VMware ESX virtual CloudBoost appliance.

- ESX 5 or greater
- 4 cores *
- 16 GB of RAM *
- 41 GB of OS and storage node hard disk (SSD recommended for storage)
- 40 GB of metadata store hard disk (SSD recommended for storage)
- 10 GB of site cache hard disk (SSD recommended for storage)

* Numbers must be doubled if a site cache is used.

For more information on metadata store and site cache hard disk sizing, see CloudBoost sizing and performance considerations on page 19.

Large deployment virtual machine requirements for ESX

These are the requirements for a large deployment of the VMware ESX virtual CloudBoost appliance.

- 8 cores *
- 32 GB of RAM *
- 41 GB of OS and storage node hard disk (SSD recommended for storage)
- Extendable up to 3 TB of metadata store hard disk (SSD recommended for storage)
- At least 200 GB expandable to 6 TB of site cache hard disk (SSD recommended for storage)

* Numbers must be doubled if a site cache is used.

For more information on metadata store and site cache hard disk sizing, see CloudBoost sizing and performance considerations on page 19.

Minimum deployment virtual machine requirements for EC2

These are the minimum and default requirements for the VMware EC2 virtual CloudBoost appliance.

- 4 vCPUs *
- 16 GB of RAM *
- 100GB IOPS optimized SSD4 storage volume for appliance metadata (example: type AWS EBS io1) per 400TB of logical backup data under management

The AWS EC2 m4.xlarge is suggested.

Note

Smaller environments can alternatively choose an instance with unified compute and storage such as AWS EC2 m3.xlarge that includes 4 vCPUs, 15GB memory and 2x40GB SSD storage.

For more information on metadata store hard disk sizing, see CloudBoost sizing and performance considerations on page 19.

Large deployment virtual machine requirements for EC2

These are the requirements for a large deployment of the VMware EC2 virtual CloudBoost appliance.

- 8 cores
- 32 GB of RAM
- 100GB IOPS optimized SSD4 storage volume for appliance metadata (example: type AWS EBS io1) per 400TB of logical backup data under management
  The primary metadata volume can be expanded to 3TB to manage up to 6PB of logical protected capacity.

The CloudBoost appliance requires Amazon Elastic Block Store (AWS EBS) for the operating system disk and metadata database as AWS EC2 instance default storage volumes are ephemeral and should not be used for the CloudBoost appliance

For more information on metadata store hard disk sizing, see CloudBoost sizing and performance considerations on page 19.

WAN requirements

These are the minimum WAN requirements.

- >= 10MBits bandwidth
- <= 100ms RTT latency

Installation workflow

These are the steps you should take when integrating with Networker.

1. If not already installed, install Networker.
2. Perform all the tasks listed in Prepare for installing the CloudBoost appliance on page 14 before installing the CloudBoost appliance.
3. Open all the required ports listed in the Firewall port requirements on page 15 section.
4. Install the CloudBoost appliance.
5. Register the CloudBoost appliance in the EMC Cloud Portal.
6. Configure the CloudBoost appliance in the EMC Cloud Portal. For more information, see Configuring a new CloudBoost appliance on page 36.
7. Configure Networker to work with the CloudBoost appliance. For more information, see Connecting NetWorker 8.x to CloudBoost on page 40.
8. Install and configure the CloudBoost client when needed. For more information, see the *EMC CloudBoost Client Guide*

CloudBoost sizing and performance considerations

You can find information about CloudBoost sizing, performance and requirements here.

CloudBoost virtual appliance sizing

SSDs are recommended for optimal performance. Sizing for the virtual CloudBoost appliance depends upon whether optional site caching is enabled. If site caching is not enabled, 4 cores with 16 GB of memory is recommended. If site caching is enabled, 16 cores and 64 GB of memory is recommended. Site cache is not available on EC2 deployments.

The CloudBoost virtual appliance requires a minimum of 100 GB of internal capacity for storing CloudBoost metadata; however, the amount of space provisioned for metadata directly affects the logical capacity addressable by the CloudBoost virtual appliance. The ratio of metadata space to logical capacity is 2000:1. For example, 100 GB of metadata allows the appliance to address 200 TB of logical capacity. Therefore, to address the maximum logical capacity of 6 PB, 3 TB of metadata space is needed.

The CloudBoost virtual appliance assumes that the underlying storage is protected. The CloudBoost virtual appliance does not provide protection against a failed virtual data disk.

De-duplication and cloud capacity

Both the physical and virtual CloudBoost appliances support up to 6 PB of logical capacity using 3TB of metadata disk space. This is the total amount of unique data prior to de-duplication. Based on preliminary test data, CloudBoost expects to achieve a 2x–4x range of de-duplication. Backups of file systems, applications, and databases where file sizes are typically small are expected to achieve close to 2x de-duplication on average. Backups of virtual machines where typical virtual disks sizes are larger could see up to 4x de-duplication. Based on this range of de-duplication, each CloudBoost appliance can support up to 6 PB of logical capacity. That said, proof of concept testing, or testing with up-to-date, real data is recommended.

End-to-end bottlenecks

WAN bandwidth is expected to be the most common bottleneck. A properly-resourced CloudBoost appliance can saturate a 1 GB/s link with 30 ms RTT latency without hitting any limits within the VM itself. Object store ingest limits are another potential bottleneck. In some cases we reach the objects/sec limit that can be sustained by a single logical container in the object store.

Minimum WAN requirements

We recommend a minimum bandwidth of at least 10 Mbit/s to the cloud with a maximum latency of less than 100 ms RTT for the CloudBoost solution. Extremely low bandwidth links may result in backup and restore timeouts.

CloudBoost caching

The optional site cache allows backups to complete quickly over the LAN while trickling more slowly over the WAN. This enables faster backup and recovery for the objects most recently written to or read from the cloud. This persistent cache is flushed and reused as needed during these processes.

The ingestion rate for a CloudBoost appliance without site cache enabled has been measured at up to 100 MB/s. The site cache has a 50 MB/s ingestion rate for the 32 TB physical appliance and 25 MB/s ingestion rate for all other appliances, improved by de-duplication and compression, depending on the workload.

The size of the cache cannot be increased by growing the existing data disk size in vCenter, nor can the size of the cache be reduced. The minimum size of the cache is 200 GB, and it can be increased to up to 6 TB on the virtual appliance by adding additional disks that match the size of the existing site cache disks. The cache is firewall-friendly, in that multiple ports do not need to be opened.

Use of the cache is advisable under these circumstances.

- Weak connection to the object store, where bandwidth is low with high latency, anything less than 200 Mbps (25 MB/s) to the cloud store.
- You do not have streaming workload or continuous backup.

Do not use the cache if you get higher ingestion speed when connecting directly to the cloud store. If use a site cache with higher ingestion speeds, your backups will exceed the capacity of the cache.

Metadata disk pool

In addition to the operating system disk pool, there is a pool for metadata, and an optional pool for the cache. Before starting the appliance, you must ensure that the size of the metadata pool is the correct size. A 100 GB of metadata allows the appliance to address 200 TB of logical capacity. To address the maximum logical capacity of 6 PB, 3 TB of metadata space is needed. If at a later date you need to support a larger logical capacity, you may resize the metadata disk. You have to reboot the appliance in order for the appliance to see the added capacity.

Multiple clone sessions

For parallelism, we recommend creating multiple AFTD devices under the `/mnt/magfs/base` mount point within CloudBoost, and using one clone session per device. One session per device is recommended for optimal performance and de-duplication. Multiple clone sessions to the same device can result in lower de-duplication ratios and longer clone times.

CloudBoost appliance cache sizing

If you intend to enable the site cache for a CloudBoost appliance, you should change the data disk size before you initially configure the CloudBoost appliance at the CLI.

Note

If you are deploying using the AWS AMI, the use of site cache is not supported. The AMI does not include a site cache hard disk.

The CloudBoost appliance arrives with this configuration, which is appropriate when site cache is not enabled.

- 4-core virtual CPU
- 16 GB of RAM
- 41 GB of OS and storage node hard disk
- 40 GB of metadata store hard disk
- 10 GB of site cache hard disk

However, you can change these parameters in vCenter virtual machine configurations before you begin initial CloudBoost configuration at the CLI. It is recommended that you change these numbers to the appropriate levels based upon the amount of data you plan to backup.

Table 5 Minimum and recommended configuration

Minimum configuration	Recommended configuration
4-core virtual CPU	16-core virtual CPU
16 GB of RAM	64 GB of RAM
10 GB with no site cache enabled	at least 200 GB site cache data disk, can be increased up to 6 TB

CHAPTER 3

Install the Virtual CloudBoost Appliance on ESX

This chapter applies to installing the virtual CloudBoost appliance on ESX. For information on installing the virtual appliance on Amazon EC2, see Deploy the CloudBoost Appliance on page 25. For information on installing the physical appliance, see the *EMC CloudBoost Installation Guide*.

You must obtain the `.OVA` file from https://support.emc.com to install the virtual appliance.

- Installing the virtual CloudBoost appliance 24

Installing the virtual CloudBoost appliance

Install the virtual CloudBoost appliance in vSphere.

Before you begin

- Determine the location of the `.OVA` file that must be downloaded. This could be a URL, or a location accessible from the computer, such as a local hard drive or a network share.
- For the target data store, identify an available SSD with at least 700 GB of available space.

Procedure

1. In the vSphere client, click **File** › **Deploy OVF Template**, browse to the location of the OVA package, and then click **Next**.
2. Select the **Inventory Location** (the ESX cluster and host to run the virtual machine), type the name of the virtual machine, and then click **Next**.
3. Select the host or cluster for the VMDK files, and then click **Next**.
4. Select the resource pool, and then click **Next**.
5. Select the storage destination, and then click **Next**.
6. Set the virtual disk format, and then click **Next**.

   For best production performance, select **Thick Provisioned Eager Zeroed**. For testing purposes, the default 50 GB thin or thick provisioned storage is sufficient.
7. Set the network mapping, and then click **Next**.
8. On the **Ready to Complete** page of the wizard, review the deployment settings.
9. Select the **Power on after deployment checkbox**, and then click **Finish**.
10. Right-click on the virtual machine and click **Edit Settings**, then on the **Resources** tab, click **Memory**, ensure that **Reservation** is set to **`16384 MB`**, and then click **OK.**

    Note

    Memory must be reserved rather than shared for performance reasons.

Results

The CloudBoost virtual appliance is installed.

After you finish

You must use the CLI for the virtual appliance to set its IP address and networking before you can finish deployment within the EMC Cloud Portal.

CHAPTER 4

Deploy the CloudBoost Appliance

This chapter applies to deploying the virtual CloudBoost appliance.

- Deploying the virtual CloudBoost appliance in Amazon EC2.................................. 26

Deploying the virtual CloudBoost appliance in Amazon EC2

Learn about deploying the virtual CloudBoost appliance in Amazon EC2.

Once you have ordered the CloudBoost appliance, EMC licensing sends an email with a Request for More Information (RFMI) form. Complete this form and return it to CloudBoost.licensing@emc.com. Included in this form is your Amazon EC2 account ID. Your account ID is required for the Amazon EC2 AMI to be shared with you in Amazon.

Note

Site cache is not supported on Amazon EC2 because the network is too fast and disk space is too expensive.

Procedure

1. Log in to the Amazon EC2 **Dashboard**, then open the **AWS Marketplace**.
2. Search for and choose the CloudBoost AMI.
3. Under **Private Images**, find and launch the CloudBoost image.
4. Under **Instance Type**, select 8 CPUs and 32 GB of memory.
5. Under **Configure Instance Details**:
   a. Type the number of instances to create.
   b. Choose the appropriate network and submask.
   c. Enable **Auto-assign Public IP**.
6. Verify that under **Add Storage** for **Root**, **Size (GiB)** is set to 41, and that the EBS volume is present for metadata.

   The default size for the added volume is 40 GB. The size should be increased based on a 1:4000 ratio.
7. Under **Tag Instance**, define up to 10 keys to assist with AMI management.
8. Under **Configure Security Group**, create or select a security group (set of firewall rules) to allow or deny public access, keeping in mind the port requirements for the CloudBoost appliance.
9. Review information about the instance, and if any changes are necessary click **Previous**.
10. Choose or create a key pair to use when connecting to the CloudBoost appliance, and then click **Launch instances**

Results

The CloudBoost appliance is launched and running in Amazon EC2.

CHAPTER 5

Configure Network Settings for a CloudBoost Appliance

After you start the CloudBoost appliance, you should configure its network settings.

By default, the CloudBoost appliance starts with the IP address obtained via DHCP. It is also possible to manually set a static IP address.

Note

Both static IP and reserved IP using DHCP are supported. Dynamic DHCP is not supported. It is best to assign static IP addresses using DHCP (via DHCP reservations) unless you have disabled DHCP in the data center.

You must configure the resolvable fully qualified domain name (FQDN), such as **`cloudboost.example.com`**. The FQDN must be registered in your DNS with both forward and reverse domain name resolutions. The FQDN must be in lowercase.

You are required to change the default administrator password to one of your own choosing, and then you can configure the remaining IP settings and hostname.

- Configuring network settings for a CloudBoost appliance..................................... 28

Configuring network settings for a CloudBoost appliance

You must provide basic network settings information for a CloudBoost appliance at the Command Line Interface (CLI) before you can register it and complete initial configuration in the EMC Cloud Portal.

Note

The CloudBoost AMI automatically uses the default VPC settings for the appliances IP address, DNS, and FQDN. If you need to change these network settings, you can use the commands below.

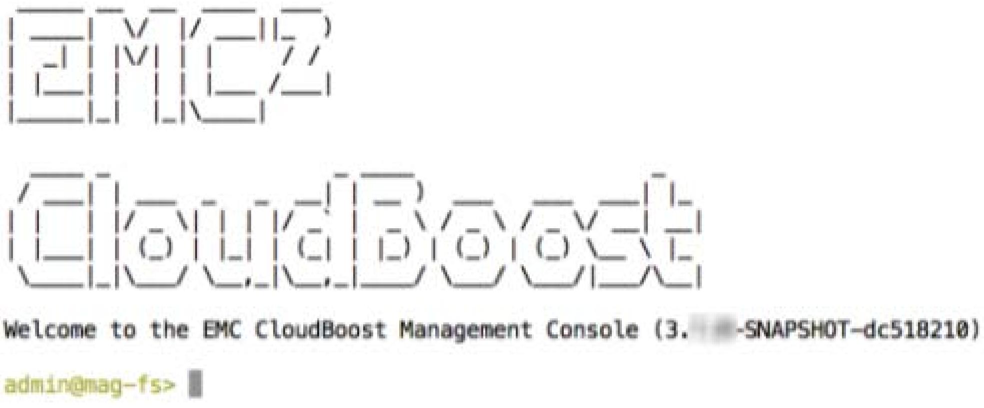
Procedure

1. Open a CLI window on the CloudBoost appliance.

Option	Description
vSphere client	In the vSphere client, right-click **VM** › **Open Console**.
EC2	a. Log in to EC2, select your CloudBoost appliance, and then click **Connect**. b. In the **Connect To Your Instance** wizard, choose whether to connect with an SSH client or from the browser, and then follow the instructions. c. In the SSH terminal, run this command, `ssh - i "private key" admin@AWS FQDN or IP` where *private key* is the private key you used as the key pair when you installed your CloudBoost AMI.

The CloudBoost CLI appears.

Figure 2 CLI for CloudBoost



```
Welcome to the EMC CloudBoost Management Console (3.[redacted]-SNAPSHOT-dc518210)

admin@mag-fs>
```

2. Authenticate with the default password, **`password`**.
3. Set the new administrator password.

4. To see the current network configuration of the appliance, run this command.

   ```
   status
   ```

   The `status` command also shows the ethernet interfaces to use in the `net config` command.

```
admin@mag-fs> status
Host Configuration:
  Hostname:        hostname
  Domain:          domain
  FQDN:            fqdn
Version Information:
  Version:         version identifier
  Revision:        revision identifier
Network Interfaces:
             name             mode         address        netmask
             ----             ----         -------        -------
             eth0             dhcp    10.5.96.123      address

Network Routes:
           prefix          netmask         gateway
           ------          -------         -------
          default          0.0.0.0      10.5.96.1
       10.5.96.0          address                *
DNS Configuration
  DNS Servers:     10.5.96.91
Appliance status:  Not yet registered

Domain name:       domain name
```

5. To statically set the IP address and netmask, run these commands. If you have multiple networks you must run this command for each network listed in the `status` command.

   ```
   net config interface IP address netmask netmask address
   ```

   For example,

   ```
   net config eth0 10.5.96.123 netmask 0.0.0.0
   ```

6. To manually add the gateway, run these commands. If you have multiple networks, you also have to add multiple routes to the appropriate gateways.

   ```
   route add IP address netmask netmask address gw gateway address
   ```

   For example,

   ```
   route add 0.0.0.0 netmask 0.0.0.0 gw 10.5.96.1
   ```

7. To manually set the DNS, run these commands.

   ```
   dns set primary primary IP address
   dns set secondary secondary IP address
   dns set tertiary tertiary IP address
   ```

   For example:

   ```
   dns set primary 10.5.96.91
   dns set secondary 10.5.96.92
   dns set tertiary 10.5.96.93
   ```

8. To set the FQDN, run this command.

   ```
   fqdn servername.yourcompanydomain
   ```

   Note

   The FQDN must be in lowercase.

   For example:

   ```
   fqdn cloudboost.example.com
   ```

9. To verify the networking setup and see the status of the appliance, run this command.

   ```
   status
   ```

   For example,

```
admin@mag-fs> status
Host Configuration:
  Hostname:        hostname
  Domain:          domain
  FQDN:            fqdn
Version Information:
  Version:         version identifier
  Revision:        revision identifier
Network Interfaces:
             name             mode         address        netmask
             ----             ----         -------        -------
             eth0             static    10.5.96.123      address

Network Routes:
           prefix          netmask         gateway
           ------          -------         -------
          default          0.0.0.0      10.5.96.1
       10.5.96.0          address               *
DNS Configuration
  DNS Servers:     10.8.192.91
Appliance status:  Not yet registered

Domain name:       domain name
```

Results

After you have verified the system's basic networking settings, you can register the appliance and then configure CloudBoost using the EMC Cloud Portal.

Note

Other commands are also available from the command line. To get help, type **`help`** or **`?`**.

CHAPTER 6

Register and Configure a New CloudBoost Appliance

After you install a CloudBoost appliance and configure it at the CLI, you can register it and complete configuration in the EMC Cloud Portal. You must create a cloud profile for the storage provider the appliance will use before you can complete its configuration.

- Create and manage cloud profiles for CloudBoost 32
- Validate cloud storage credentials 32
- Registering a CloudBoost appliance 34
- Enable remote client mounting 35
- Disable remote client mounting 35
- Configuring a new CloudBoost appliance 36

Create and manage cloud profiles for CloudBoost

Before you configure a CloudBoost appliance in the EMC Cloud Portal, you should create a cloud profile for the storage it will use.

Before you begin

Obtain the necessary credentials for the cloud provider you intend to use. For more information, see Cloud providers supported by CloudBoost appliances on page 13.

If your account was provisioned with Virtustream Storage Cloud by EMC Sales, your provisioned storage classes appear on the **Cloud Profiles** page. If the account has been activated for use with CloudBoost, it appears automatically as a cloud profile. If Virtustream Storage Cloud has not been activated for use with CloudBoost, contact EMC sales. You cannot edit or delete existing Virtustream Storage Cloud cloud profiles that have been provisioned for you, nor can you add a new Virtustream Storage Cloud profile yourself.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials you created from your invitation.
2. Click **Cloud Portal**, and then click **CloudBoost.**
3. In the left menu, click **Cloud Profiles**.

   The **Cloud Profiles** page opens.
4. To create a new cloud profile, click **New Cloud Profile**.
   a. In the **Display Name** field, type the name for this cloud profile.
   b. In the **Cloud Storage Provider** field, select the appropriate cloud provider.
   c. In the fields that appear for the selected cloud provider, provide the additional information and credentials required to access this particular cloud object store.
   d. Click **Save**.
5. To change information for an existing cloud profile, click **Edit**.
   a. On the **Edit a Cloud Profile** page, change any fields necessary.
   b. Click **Save**.
6. To delete an existing cloud profile, click **Delete**.

Results

The cloud profiles listed can be used by CloudBoost appliances.

Validate cloud storage credentials

You should use the cloud storage credential validator (sometimes referred to as the *blobstore validator (BSV)*) to validate the cloud storage credentials you intend to use with the CloudBoost appliance.

Before you begin

Configure your CloudBoost appliance with a valid cloud storage provider.

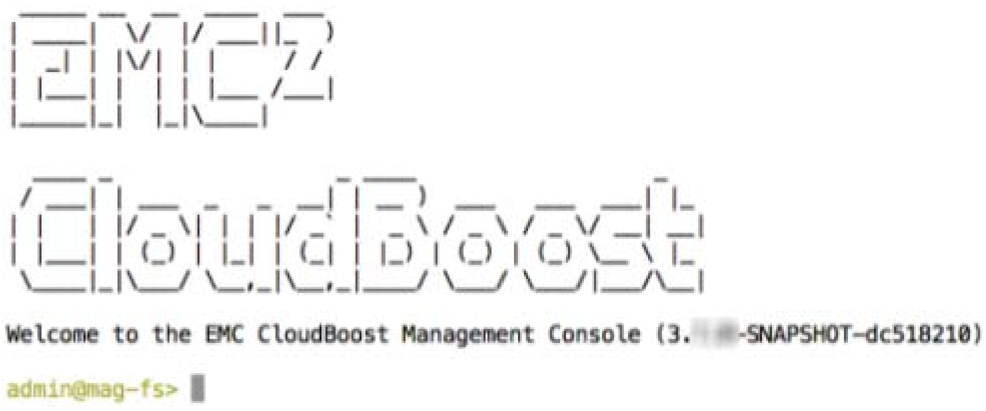
Procedure

1. Open a CLI window on the CloudBoost appliance.

Option	Description
vSphere client	In the vSphere client, right-click **VM** › **Open Console**.
EC2	a. Log in to EC2, select your CloudBoost appliance, and then click **Connect**. b. In the **Connect To Your Instance** wizard, choose whether to connect with an SSH client or from the browser, and then follow the instructions. c. In the SSH terminal, run this command, `ssh - i "private key" admin@AWS FQDN or IP` where *private key* is the private key you used as the key pair when you installed your CloudBoost AMI.

The CloudBoost CLI appears.

Figure 3 CLI for CloudBoost



```
Welcome to the EMC CloudBoost Management Console (3.[redacted]-SNAPSHOT-dc518210)

admin@mag-fs>
```

2. Run this command to see a list of valid cloud profiles.

```
diagnostics bsv-cli "--cloud_profile_id="
```

Note

The quotation marks are required.

The result should be similar to the following, with a list of possible cloud profiles that are available.

```
Can't find cloud profile with ID . Possible values are:
1    VSC Virtustream Storage Cloud standard Storage
% Can't find cloud profile with ID
```

3. To validate the storage credentials for profiles listed as a result of Step 1, run this command.

```
diagnostics bsv-cli "--cloud_profile_id=1"
```

1 represents the cloud profile to validate as listed in the result of Step 1.

The result should indicate that various BSV CLI commands are being validated.

```
Running BSV CLI with java options: -Djclouds.trust-all-certs=true -Djclouds.s3.virtual-
host-buckets=false
Running BSV CLI with arguments: --provider=atmos --
identity=05832cb9d39a40af96aaafd4a406aa6f/A8581914817a4a8c264d
--credential=fXPGEkxSCo9Zt6QHLtg05I/axjc=
--endpoint=https://api.atmosonline.com  validate
...
continues to validate
```

Registering a CloudBoost appliance

You must register a CloudBoost appliance at the CLI and in the EMC Cloud Portal before you can configure it in the Portal.

Before you begin

You must provide basic IP address information at the CLI for the CloudBoost appliance before you can generate a claim code used to register the appliance. For more information, seeConfiguring network settings for a CloudBoost appliance on page 28. You must also have consumed your invitation to create an account in the EMC Cloud Portal.

Procedure

1. Establish an SSH session to the IP address for CloudBoost appliance and log in with the username **`admin`** and the password you set earlier.
2. Run this command.

   ```
   register
   ```

3. Copy or make note of the resulting claim code.
4. Use a web browser to sign in to the EMC Cloud Portal with the credentials you created from your invitation.
5. In the upper right-most corner of any portal page, click ••• **(Cloud Portal Options)**, and then click **Register a CloudBoost Appliance**.
6. In the **Claim code** field, type the claim code from Step 3, and then click **Register**.
7. In the CLI window, this message appears: `Appliance successfully registered.`

Results

The appliance is registered. You can now configure CloudBoost in the EMC Cloud Portal.

Note

If you have registered a physical CloudBoost appliance, you should immediately apply any available system upgrades. For more information, see Upgrading a CloudBoost appliance on page 45.

If you have an EMC Secure Remote Services (ESRS) gateway installation, you can also register your CloudBoost appliance to be monitored by ESRS. For information about installing an ESRS gateway and registering a CloudBoost appliance with ESRS, see Monitor, Manage, and Support CloudBoost on page 43.

Enable remote client mounting

When you enable Windows clients to mount remotely, you create the password to be used. Share the user name and password with anyone who needs to remotely mount with the Windows client.

When you enable Windows clients to mount remotely, you create the password to be used. Share the user name and password with anyone who needs to remotely mount with the Windows client.

Procedure

1. Open a CLI window for the appliance, and then log in with the admin username and password.
2. Run this command, where the value for *password* is a password you create.

```
remote-mount-password enable password
```

3. Share the credentials to be used when mounting with the Windows client with the people who perform that task.

   The user name is **remotebackup**. The password is the one you created in Step 2.

Results

Remote Windows clients can mount with these credentials. For information about the Windows client, see the *EMC CloudBoost Client Guide*.

Disable remote client mounting

When you enable Windows clients to mount remotely, you create the password to be used. Share the user name and password with anyone who needs to remotely mount with the Windows client.

Procedure

1. Open a CLI window for the appliance, and then log in with the admin username and password.
2. Run this command.

```
remote-mount-password disable
```

Results

For information about the Windows client, see the *EMC CloudBoost Client Guide*.

Configuring a new CloudBoost appliance

After you provide basic network information for the appliance at the CLI and then register it, you must use a web browser finish configuration in the EMC Cloud Portal. You can change certain configuration information for an appliance after initial configuration.

Before you begin

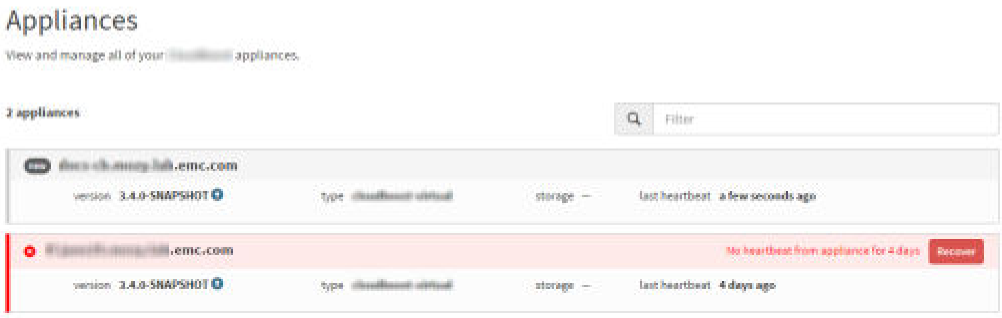
You should understand SSL Certificate management for CloudBoost. For more information, see SSL Certificate Management for CloudBoost on page 53. You must also have defined a cloud profile for use with this appliance.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials you created from your invitation.
2. Click **Cloud Portal**, and then click **CloudBoost.**
3. In the left menu, click **Appliances**.

   The **Appliances** page opens.

   Figure 4 Appliances page



Appliances

View and manage all of your [redacted] appliances.

2 appliances

[redacted].emc.com

version 3.4.0-SNAPSHOT type [redacted] storage – last heartbeat a few seconds ago

[redacted].emc.com No heartbeat from appliance for 4 days

version 3.4.0-SNAPSHOT type [redacted] storage – last heartbeat 4 days ago

4. In the list of appliances, click the appliance that you want to configure.

   The **Overview** page of the appliance opens.

   Note

   If you are preparing an appliance as the target for recovering a failed appliance, upgrade if necessary to ensure the target appliance is running the same version as the appliance to be recovered. Do not configure the target appliance any further. Failed appliances cannot be recovered to configured target appliances.

   For information about upgrading, see Upgrading a CloudBoost appliance on page 45.
5. Review the configuration information on the **Overview** page, and then click **Configure**.
6. To change the display name for this appliance from the default FQDN set in the CLI, enter the display name in the **Name** field.

   The FQDN must be in lowercase.
7. In the **Cloud Profile** field, select one of the cloud profiles that was previously set up.

Note

This cannot be changed after initial configuration.

8. To prevent this appliance from using a site cache, deselect **Enable Site Cache**.

Note

This cannot be changed after initial configuration.

9. To use a CA-signed certificate, select **Provide a CA-signed certificate**, then choose a PKCS12 certificate file to upload and provide the key file password if necessary.

   CA certificate information must be provided in lowercase.

Note

CA-signed certificates are preferred because of the higher level of security available from trusted certificate authorities. To obtain a CA-signed certificate, visit the website of your preferred authority.

10. To minimize clock drift, select **Enable NTP** checkbox, and then enter the URL or IP address for at least one NTP server.
11. To set the frequency of backups, select a schedule for **Backup Frequency**.

Note

The backups referred to here are for the system state of the appliance and for the stored metadata. This is not a reference to any backup software integration.

12. To use asymmetric encryption keys, select **Enable backup encryption with asymmetric keys**.

    a. Refer to the displayed instructions to help you create your private and public encryption keys. This is the only method of asymmetric key creation supported for the CloudBoost appliance.

    b. Copy the entire public key from the resulting output file and paste it into the text box below the instructions on the **Configure** tab.

    c. Copy the entire private key from the resulting output file and paste it somewhere safe. If you created a pass phrase, copy that as well.

    ⚠ CAUTION

    You must safely store your private key and pass phrase. They must be provided to decrypt a recovered backup. Appliances backed up using the public key provided on the Configure tab cannot be recovered without your private key and pass phrase.

13. Review your selections, then click **Update Configuration** to save these settings for the appliance.

Results

The appliance is configured and a backup immediately begins.

CHAPTER 7

Integrate NetWorker 8.x with CloudBoost

Read this chapter if you are integrating CloudBoost™ with NetWorker® Server 8.1x or 8.2x.

- Connecting NetWorker 8.x to CloudBoost 40

Connecting NetWorker 8.x to CloudBoost

Connect NetWorker to CloudBoost to send a NetWorker backup clone to CloudBoost.

Before you begin

For information about installing and configuring NetWorker, storage nodes, and advanced file type devices (AFTDs), see the *EMC NetWorker Installation Guide* and the *EMC NetWorker Administration Guide*.

Read this topic if you are integrating CloudBoost with NetWorker Server 8.1x or 8.2x.

If you are integrating CloudBoost with NetWorker Server 9.0.x, see the *EMC NetWorker Installation Guide* and the *EMC NetWorker Administration Guide*.

Perform the following tasks inside the Networker administration interface.

Procedure

1. Right-click **Storage Node**, and then click **New**.
2. On the **General** tab, type the FQDN in the **Name** text box, and then add a comment if needed. Verify that scsi is selected next to **Type of storage node**, and then click **OK**.
3. Right-click **Devices**, and then click **New Device Wizard**.
4. Select **Advanced File Type Device (AFTD)**, and then click **Next**.
5. Select the CloudBoost storage node you just created. Leave the rest of the fields with their default settings, and then click **Next**.
6. Select the CloudBoost share, and then click **Next**.

   Make sure the path `/mnt/magfs/base` is selected.
7. In the Networker Device Name field, type the FQDN of the CloudBoost appliance, add a comment if you want, and then click **Next**.
8. Select **Label and Mount device after creation**, select **Backup Clone** under **Pool Type**, select **Default Clone** under **Pool**, and then click **Next**.
9. Review the configuration, click **Configure**, and then click **Finish**.
10. Right-click **Clones**, and then click **New**.
11. Type the name of the clone and a comment in the Name and Comment fields, and then in the **Storage node to WRITE save sets** drop-down select the CloudBoost storage node you created.
12. Make any other changes you want to the clone, then click **OK**.
13. Click the **Monitoring** tab.
14. Under **Clones**, click the **Clones** tab, and then right-click the newly created clone and click **Start**.
15. To verify that CloudBoost is receiving clones from NetWorker, log in to the EMC Cloud Portal.

    a. Click **Cloud Portal**, and then click CloudBoost.

    b. Select the appropriate appliance.

    c. Under **Storage Use History** at the bottom of the **Overview** tab, review the storage consumption information for data sent to the share and received by CloudBoost.

    For information about monitoring a CloudBoost appliance, see the Monitor, Manage, and Support CloudBoost on page 43.

Results

You may also test restoring data from the share by using the NetWorker Recovery Wizard.

CHAPTER 8

Monitor, Manage, and Support CloudBoost

You can see status and performance information for CloudBoost appliances, change log levels, upgrade, restart, recover, and remove appliances. You can also register CloudBoost appliances with EMC Secure Remote Services.

If CloudBoost appliances are not registered with EMC Secure Remote Services, you will need to manually monitor their health, collect and review logs, and contact EMC Support should any issues arise.

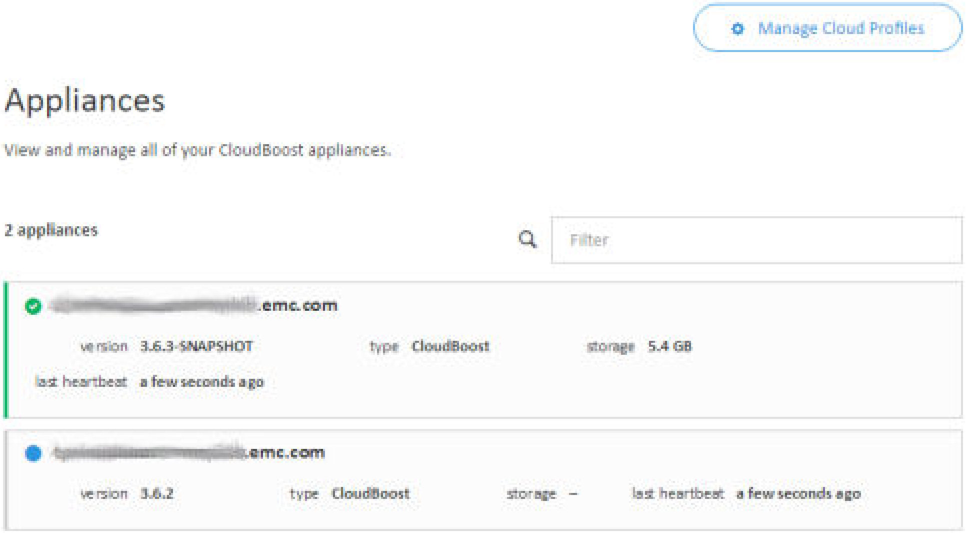
- CloudBoost reporting 44
- Upgrading a CloudBoost appliance 45
- CloudBoost integration with EMC Secure Remote Services 45
- Registering CloudBoost with EMC Secure Remote Services 46
- Increasing the CloudBoost appliance site cache 47
- Changing log levels for CloudBoost debugging 47
- Restarting a CloudBoost appliance 48
- Recovering a CloudBoost appliance 48
- Deleting a CloudBoost appliance 50

CloudBoost reporting

You can monitor the health of CloudBoost appliances and see the amount of data sent over time, and see the corresponding storage consumed over time by de-duplicated data.

When you sign in to the EMC Cloud Portal, click **Cloud Portal**, then **CloudBoost**, and then **Appliances** to see your list of appliances. On the **Appliances** page, you can see the status of each appliance and see whether an upgrade is available. To filter the list of appliances, type a portion of the name of the appliance or appliances you want to see.

Figure 5 Appliances page



Appliances

View and manage all of your CloudBoost appliances.

2 appliances

[redacted].emc.com

version 3.6.3-SNAPSHOT type CloudBoost storage 5.4 GB

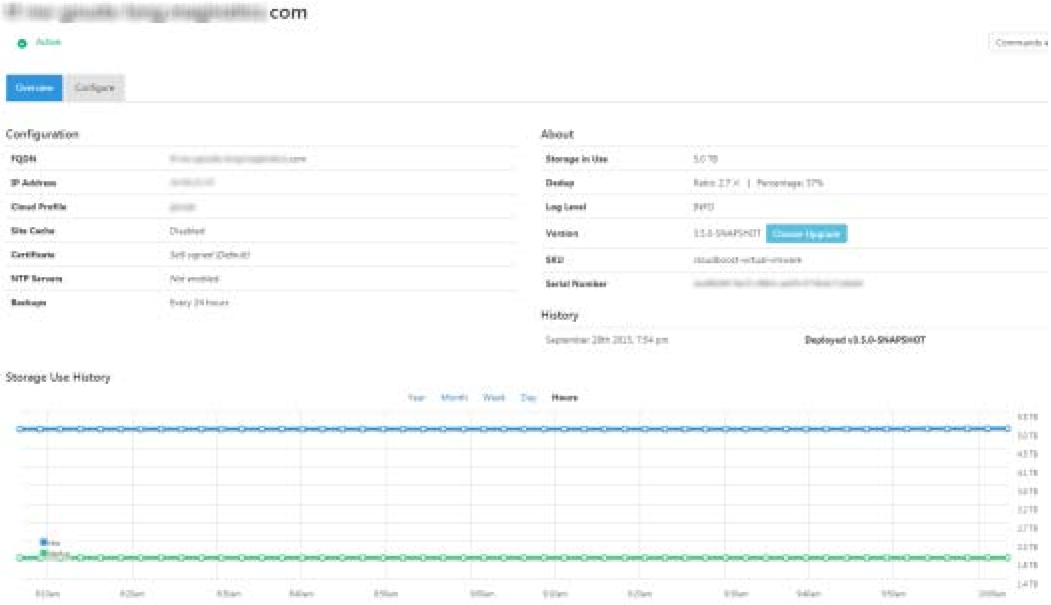
last heartbeat a few seconds ago

[redacted].emc.com

version 3.6.2 type CloudBoost storage – last heartbeat a few seconds ago

Select an appliance to see information about it, including its configuration and storage use history.

Figure 6 Appliance configuration details and storage use history



[redacted] com

Active

Configuration

FQDN [redacted]

IP Address [redacted]

Cloud Profile [redacted]

Site Cache Disabled

Certificate Self signed (Default)

NTP Servers Not enabled

Backups Every 24 hours

About

Storage in Use 5.0 TB

Dedup Ratio 2.7 X | Percentage 37%

Log Level INFO

Version 3.5.0-SNAPSHOT

SKU cloudboost-virtual-vmware

Serial Number [redacted]

History

September 28th 2015, 7:54 pm Deployed v3.5.0-SNAPSHOT

Storage Use History

Under **Configuration**, you can see a brief summary of some of the settings made on the **Configure** tab.

Under **About**, you can see information about the appliance, including how much storage is used. You can see the deduplication ratio, and the affect of deduplication and compression as a percentage of the original size of the data, which is sent to the cloud storage provider.

Under **History**, you can see the deployment and upgrade history for the appliance.

Storage Use History shows how much raw data the appliance has received, and how much deduplicated and compressed data was sent to the cloud storage provider. You can change the view from the default, Hours, to show storage used over the course of days, weeks, months or years.

Upgrading a CloudBoost appliance

You can upgrade CloudBoost appliance software from within the EMC Cloud Portal. During the installation the CloudBoost appliance will be unavailable. The appliance will restart after the upgrade is complete.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials you created from your invitation.
2. Click **Cloud Portal**, and then click **CloudBoost.**
3. Select the appliance to upgrade.
4. On the **Overview** tab, click **Choose Upgrade** under **About**.
5. Select the version to upgrade to, and then click **Start Upgrade**.
6. Review the warning message, and then click **Confirm**.

   After a moment, the **Appliances** page appears.
7. Monitor the progress of the upgrade, which can take some time.

Results

After the upgrade is complete, you can see the upgrade history on the **Overview** tab for the appliance, under **History**.

CloudBoost integration with EMC Secure Remote Services

EMC Secure Remote Services (ESRS) is a virtual appliance that enables two-way remote communication for EMC to monitor system health and to proactively communicate alerts and issues to EMC Customer Support. ESRS is included at no extra charge in the enhanced or premium warranty or maintenance agreement.

When registered with your ESRS gateway, the CloudBoost appliance continuously communicates with ESRS, sending it status information and reports on a schedule. When appropriate, appliance alerts from ESRS appear in the EMC Cloud Portal. When necessary, EMC CloudBoost Technical Support is notified of issues and can open an SSH session with the appliance to obtain additional logs and reports. You can allow or deny this remote activity for any reason. When a tech support agent initiates a connection through ESRS, an email is sent to you requesting access, you can choose to grant/deny the request. You can also audit EMC remote support activity, including the date and time of remote sessions, the ticket number, the EMC technician, and more.

If you choose not to register CloudBoost appliances with ESRS, you must manually monitor your appliances. If any issues arise, you must contact EMC Support yourself.

You can install the EMC Secure Remote Services gateway version 3.6.0 or later in a VM separate from the CloudBoost appliance. After your CloudBoost appliance is registered in the EMC Cloud Portal, you can then also register it with ESRS.

For information about installing the ESRS gateway, refer to the EMC Secure Remote Services Virtual Edition topics at these sites.

- https://support.emc.com/products/37716_EMC-Secure-Remote-Services-Virtual-Edition
- https://support.emc.com/products/37716_EMC-Secure-Remote-Services-Virtual-Edition/Topics/pg58757/

Note

When you install the ESRS gateway, make note of the IP address or URL and the serial number. You will need to provide them at the CloudBoost CLI when you register the appliance with ESRS, along with the SID from the email sent from EMC ESRS Support. For information about registering your CloudBoost appliance with ESRS, see Registering CloudBoost with EMC Secure Remote Services on page 46.

Registering CloudBoost with EMC Secure Remote Services

You can register a CloudBoost appliance with your EMC Secure Remote Services (ESRS) gateway to enable two-way remote communication with EMC. This purpose for ESRS is to monitor system health and to proactively communicate alerts and issues to EMC Customer Support.

Before you begin

Your ESRS gateway must be installed, and your CloudBoost appliance must be registered in the EMC Cloud Portal before you can register it with ESRS. Remote access must be enabled for your appliance. For information about installing your ESRS gateway, see CloudBoost integration with EMC Secure Remote Services on page 45.

Note

If a firewall exists between the CloudBoost appliance and the ESRS server, certain ports (for example, port 9443) must be open. For information about which ports must be opened, see Firewall port requirements on page 15.

Procedure

1. Find your ESRS SID in the email from EMC ESRS Support.
2. Have the IP address or URL and the serial number of your installed ESRS gateway available.
3. Establish an SSH session to the IP address for the CloudBoost appliance and log in with the administrator credentials.
4. Run this command.

```
support esrs register esrs_gateway username password sid gateway_sn
```

   esrs_gateway is either the IP address or the FQDN for your ESRS gateway virtual machine. *username* and *password* are the credentials used to set up your ESRS gateway. *sid* is the ESRS serial number provided by EMC ESRS Support in an email. *gateway_sn* is the serial number for the ESRS gateway.

Note

If you see this message, `Approval Request Pending - Contact EMC Customer Support`, contact EMC Customer Support and ask for the device registration in ESRS to be manually approved. Once the request is approved by EMC support, you can run the command in step 4 again. Once a device is successfully registered, you can also use the `status` command to verify your connection. At the bottom of the window, you will see the ESRS Server details listed.

Results

The CloudBoost appliance is registered with ESRS, and continuous support monitoring begins.

Increasing the CloudBoost appliance site cache

You can increase the cache size after deployment by adding additional virtual data disks in vCenter virtual machine configuration, but you must reboot the CloudBoost appliance after doing so.

Any new data disk should be equal to the initial site cache data disk size during deployment.

- If a new data disk is less than the initial data disk size, CloudBoost generates a warning event and the disk is not added to the system.
- If a new data disk is bigger than the initial data disk size, CloudBoost generates a warning event, the disk is added to the system, but the excess space is not used.
- The supported number of caching disks are either 1, 2, 4, 8, 16, or the maximum of 32. If the number of available caching disks is not equal to the number of supported disks, site cache consumes the maximum supported disk count less than or equal to the available disks, and the remaining disks are not used. For example, if the number of available caching disks is 19, the caching server uses only 16; the rest are not used. If the number of caching disks is 45, the caching server uses 32, and the rest are not used.

Additional data disks must be thick provisioned.

Changing log levels for CloudBoost debugging

Log files are an important tool when investigating issues. At the direction of EMC Support, you can change logging levels to increase the amount of information collected for their use in trouble shooting.

While increasing the logging level may assist in diagnosing a reported problem, it can decrease the performance of an appliance.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials you created from your invitation.
2. Click **Cloud Portal**, and then click **CloudBoost.**
3. Select the appropriate appliance, and then in the upper right-most corner of the page, click **Commands**.
4. Select the appropriate log level.

- **Change Log Level to INFO** This is the default log level.
- **Change Log Level to DEBUG**
- **Change Log Level to TRACE**

Results

When an elevated log level is no longer needed for diagnosing and troubleshooting issues, you can reduce the level and thereby improve performance.

Restarting a CloudBoost appliance

You can restart a CloudBoost appliance like any other computer. You might do this at the direction of EMC Support. Appliances are automatically restarted when you upgrade them.

You may restart an appliance from within the EMC Cloud Portal or at the CLI.

Procedure

1. If the CloudBoost appliance you need to restart can communicate with the EMC Cloud Portal, you can restart it from there.
   a. Use a web browser to log in to the EMC Cloud Portal..
   b. Click **Cloud Portal**, and then click CloudBoost.
   c. Select the appropriate appliance, and then click **Commands**.
   d. Select **Reboot Appliance**.
2. If you cannot restart the appliance from within the EMC Cloud Portal, you can restart it from the CLI.
   a. Establish an SSH session to the IP address for the CloudBoost appliance and log in with the admin username and password.
   b. Run this command.

```
reboot
```

Results

The appliance becomes inactive during the soft restart, like any other computer, then becomes active again. The restart event is logged.

Recovering a CloudBoost appliance

If a CloudBoost appliance fails, you can recover to a CloudBoost appliance that is registered but not configured.

Before you begin

The recovery target appliance must be running the same version of the CloudBoost software as the failed appliance had been running. Upgrade the target appliance if necessary to ensure it is running the same version as the appliance to be recovered. For information about upgrading, see Upgrading a CloudBoost appliance on page 45.

Note

Do not configure the target appliance any further. Failed appliances cannot be recovered to configured target appliances.

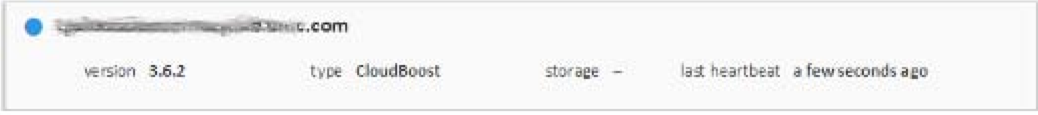
If a CloudBoost appliance fails, you must deploy a second CloudBoost appliance to restore the metadata from backups stored in the cloud. Backups of the CloudBoost metadata are run (according to the scheduled frequency that is specified in the appliance configuration) and are stored in the same object store as the data. The recovery process requires this metadata to be restored to the newly deployed CloudBoost appliance.

For testing purposes, you can force recovery for an active appliance.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials you created from your invitation.
2. Click **Cloud Portal**, and then click **CloudBoost.**
3. On the **Appliances** page, verify that an unconfigured appliance is available that you can recover the failed appliance to.

   Figure 7 New, unconfigured appliance

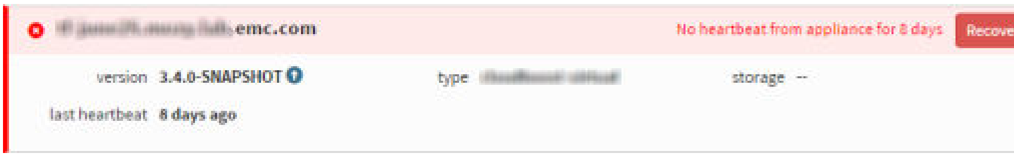
   

   ● [redacted]c.com

   version 3.6.2 type CloudBoost storage – last heartbeat a few seconds ago

4. Verify that the unconfigured appliance is running the same version as the failed appliance. Upgrade if necessary.
5. Recover the failed appliance.
   - Find the inactive appliance on the **Appliances** page, and then click **Recover** for that appliance.

     Figure 8 Appliance to recover

     [redacted]emc.com No heartbeat from appliance for 8 days Recove

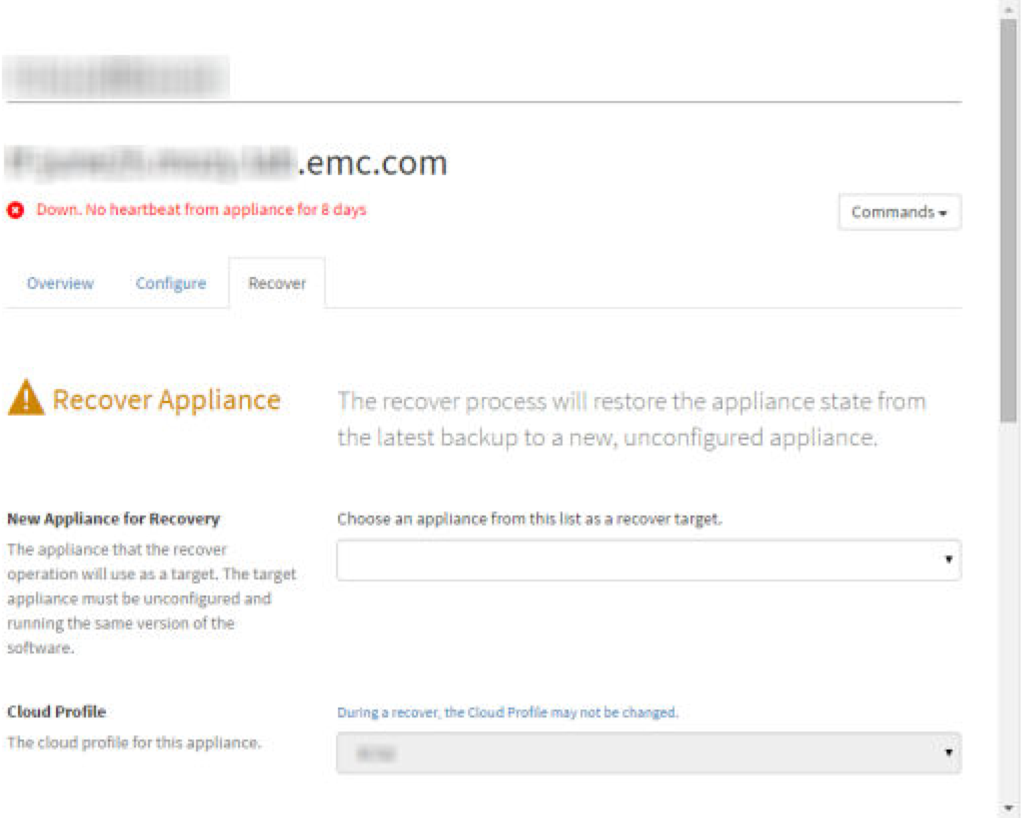
     version 3.4.0-SNAPSHOT type [redacted] storage --

     last heartbeat 8 days ago

   - To test the recovery process with an active appliance, select the appropriate appliance on the **Appliances** page, and then on the appliance details page, click **Commands**, and then **Force recover appliance**.

   The **Recover** tab opens.

Figure 9 Recover tab



[redacted]

[redacted].emc.com

Down. No heartbeat from appliance for 8 days

Recover Appliance

The recover process will restore the appliance state from the latest backup to a new, unconfigured appliance.

New Appliance for Recovery

The appliance that the recover operation will use as a target. The target appliance must be unconfigured and running the same version of the software.

Choose an appliance from this list as a recover target.

Cloud Profile

The cloud profile for this appliance.

During a recover, the Cloud Profile may not be changed.

[redacted]

6. If the appliance being recovered had been configured to use asymmetric encryption, provide the private key required to decrypt the backed up data.
   a. If a pass phrase was created to use with the private key, type that pass phrase.
7. Select the appropriate CloudBoost appliance as the recovery target.

   Note

   The recovery target appliance must be running the same version of the CloudBoost software as the appliance being recovered.

   The recovery target appliance adopts the FQDN and display name of the recovered appliance.
8. Provide the remaining configuration information, and then click **Start Recover Operation**.

After you finish

If the recovered appliance used asymmetric encryption, you can rotate the encryption keys. To do this, open the **Configure** tab for the recovered appliance, enable backup encryption with asymmetric keys, and create the public and private keys. For more information, see Configuring a new CloudBoost appliance on page 36.

Deleting a CloudBoost appliance

You can delete an appliance so that it can be deployed once again, as if it were a new appliance. You might want to do this in a production environment if a problem happened during deployment or configuration, before any backups were made. You might also want to delete an appliance set up for testing purposes, if its backups had value only for testing.

An appliance that is inactive or unusable appears in red on the **Appliances** page. When you select such an appliance, the status at the top of the appliance detail page is **Down**.

An appliance is considered active if sufficient configuration has happened, even if no backups have been made. If an error was made during configuration, such as choosing the wrong cloud profile, you can delete an active appliance so that you can redeploy it.

Note

If a CloudBoost appliance had been actively used to back up production data, you should recover it, rather than remove it. For information about recovering an appliance, see Recovering a CloudBoost appliance on page 48.

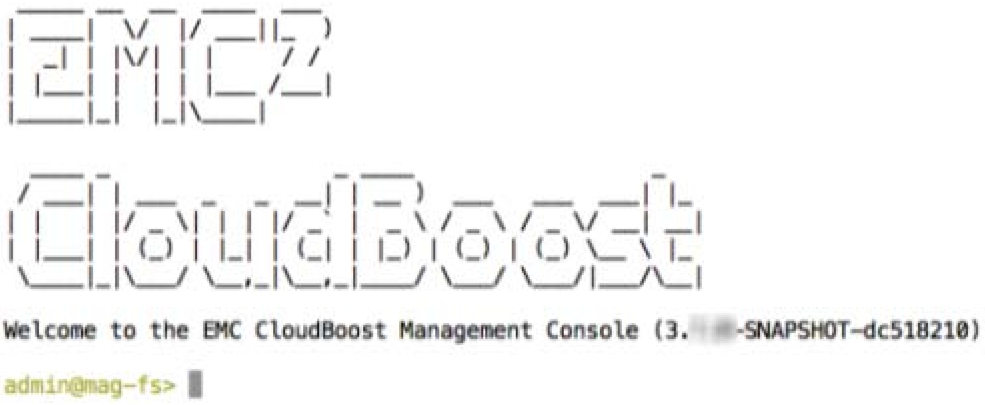
Procedure

1. Carefully identify the appliance that must be deleted.
2. Open a CLI window on the CloudBoost appliance.

Option	Description
vSphere client	In the vSphere client, right-click **VM** › **Open Console**.
EC2	a. Log in to EC2, select your CloudBoost appliance, and then click **Connect**. b. In the **Connect To Your Instance** wizard, choose whether to connect with an SSH client or from the browser, and then follow the instructions. c. In the SSH terminal, run this command, `ssh - i "private key" admin@AWS FQDN or IP` where *private key* is the private key you used as the key pair when you installed your CloudBoost AMI.

The CloudBoost CLI appears.

Figure 10 CLI for CloudBoost



```
Welcome to the EMC CloudBoost Management Console (3.[redacted]-SNAPSHOT-dc518210)

admin@mag-fs>
```

3. Run this command.

   ```
   factory-reset erase-everything
   ```

   The appliance is reset back to its original pre-deployed state. This includes resetting CloudBoost to its original version. Any upgrades that occurred during its deployment are no longer in effect.

4. To delete all the data in the cloud, run this command.

   ```
   destroy-appliance
   ```

5. Use a web browser to sign in to the EMC Cloud Portal with the credentials you created from your invitation.
6. Click **Cloud Portal**, and then click **CloudBoost**.
7. In the left menu, click **Appliances**.
8. Select the appliance to delete.
9. On the appliance details page, click …, and then **Delete Appliance**.
10. In the confirmation message, click **Ok**.

    The **Appliances** page appears, where you can verify that the appliance was deleted.

Results

The EMC Cloud Portal no longer has a record of this appliance. The appliance is reset to its original state. You may redeploy the appliance as if it were new.

CHAPTER 9

SSL Certificate Management for CloudBoost

In production environments, you should use a wildcard SSL certificate signed by a trusted Certificate Authority. Wildcard certificates are public key certificates that can be used with multiple sub-domains. Only a single level of sub-domain matching is supported.

The CA-signed wildcard certificate must be suitable for SSL server usage and must cover all the host names in the CloudBoost deployment. Certificates that do not cover your entire CloudBoost deployment will be rejected. Additional names (beyond the server the certificate is being installed on) such as CNAMEs are not automatically validated; the administrator must manually validate these names.

The signed certificate must not expire in less than one month. If you attempt to upload a certificate that will expire in less than one month, the server will reject it.

If your signed certificate is due to expire within three months, a warning message appears within CloudBoost appliance management in the EMC Cloud Portal until the issue is resolved.

Note

Because self-signed SSL certificates are less secure than those signed by a trusted Certificate Authority, self-signed certificates should be used only for test deployments.

CloudBoost uses the certificate storage solutions within the operating systems for Mac, Windows and iOS.

Note

If you use a self-signed certificate, you must push the root CA certificate to the certificate store of each device.

- Self-signed SSL certificates 54
- Converting a PEM file to PKCS #12 55
- Verifying your certificate 56
- Manage the SSL certificate for a CloudBoost appliance 56

Self-signed SSL certificates

Because self-signed SSL certificates are less secure than those signed by a trusted Certificate Authority, self-signed certificates should be used only for test CloudBoost deployments.

If you deploy an instance for testing and later decide to move it to production, you can update the SSL certificate.

Note

Changing the SSL certificate has no impact on the data or metadata of the share. Before you apply your new certificate, you should plan for a short service outage. You must stop all services for the share before you can update the certificate.

Selecting **Use the default self-signed certificate** in the EMC Cloud Portal does not provide a certificate for you to deploy on other machines. Therefore, if you wish to access any deployed share from a client running on a separate machine, you should generate your own self-signed certificate.

Generating a self-signed SSL certificate

You can generate a self-signed certificate for testing purposes from a Linux terminal which can be deployed elsewhere as required.

The resulting `.pem` file can be converted to a PKCS #12 file for use on the CloudBoost appliance page in the EMC Cloud Portal.

The openssl toolkit is used to generate an RSA Private Key and CSR (Certificate Signing Request). It can also be used to generate self-signed certificates that can be used for testing purposes or internal usage.

Procedure

1. Create an openssl configuration file that enables subject alternative names (config.cnf).

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
[req_distinguished_name]
countryName = US
localityName = Mountain View
organizationalUnitName = <%= brand_name %>
commonName = EMC, inc.
emailAddress = support@emc.com

[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

[alt_names]
DNS.1 = cloudboost1.example.com
DNS.2 = cloudboost2.example.org
```

2. Save the file.
3. To generate a valid private RSA key, run this command.

```
openssl genrsa 2048 > host.key
```

Once the private key is generated, a Certificate Signing Request can be generated.

4. To use the CSR to self-sign the CSR, run this command.

   ```
   openssl req -new -key host.key -out host.csr -config config.cnf
   ```

5. To self-sign the certificate request, setting a life-span of the certificate, run this command.

```
openssl x509 -req -days 365 -in host.csr -signkey host.key -out host.crt -extensions
v3_req -extfile config.cnf
```

6. To combine the files to generate a valid `.pem` file, run this command.

   ```
   cat host.crt host.key > host.pem
   ```

Converting a PEM file to PKCS #12

Convert a PEM file to PKCS #12 to enable SSL certificate provision on the CloudBoost appliance page in the EMC Cloud Portal.

PKCS #12 defines an archive file format for storing multiple cryptographic objects as a single file. In the case of a CA-signed certificate, the PKCS #12 file commonly bundles both the certificate and private keys. The file can be encrypted with a pass phrase (although this is not mandatory). PKCS #12 files commonly have a `.p12` or `.pfx` file extension.

If you have separate certificate and key PEM files (base64 ASCII), but no PKCS #12 file, you can convert them using openssl. The PKCS #12 file contains the certificate, private key and intermediate certificates (up to the CA root).

Note

For use with CloudBoost, PKCS #12 filenames must be lowercase.

Procedure

1. In a Linux terminal, execute this command.

   ```
   openssl pkcs12 -export -chain -CAfile foo.com.chain.pem
   -in magfs.io.pem -inkey foo.com.key
   -passout file:passphrase.txt
   -out foo.com.chain.p12
   ```

   Where:

Option	Description
foo.com.chain.pem	is the concatenation of the intermediate certificate (root is the last)
foo.com.pem	is the **.foo.com* certificate
foo.com.key	is the private key for the above certificate
passphrase.txt	contains the pass phrase to use for the `.p12` file

Verifying your certificate

Verify an SSL certificate before providing it on the CloudBoost appliance page in the EMC Cloud Portal.

OpenSSL provides tools to verify an SSL certificate. It is best practice to verify your certificate before providing on the CloudBoost appliance page in the EMC Cloud Portal.

For more information about SSL certificate verification, refer to the official OpenSSL documentation at http://www.openssl.org/docs/apps/verify.html.

Procedure

1. From a Linux terminal, execute this command, replacing *host.crt* with the appropriate certificate filename.

```
openssl verify -purpose sslserver host.crt
```

Manage the SSL certificate for a CloudBoost appliance

You can change whether a CloudBoost appliance uses the default self-signed certificate or a CA-signed SSL certificate.

Because self-signed SSL certificates are less secure than those signed by a trusted Certificate Authority, self-signed certificates should be used only for test deployments.

In production environments, you should use an SSL certificate signed by a trusted Certificate Authority. The CA-signed certificate must be suitable for SSL server usage and must cover all the host names in the deployment.

If you deploy an instance for testing and later decide to move it to production, you can update the SSL certificate.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials you created from your invitation.
2. Click **Cloud Portal**, and then click **CloudBoost.**
3. Select the appropriate appliance, and then click **Configure**.
4. Next to **Certificate**, select the type of SSL certificate and provide the necessary certificate information.

Option	Description
Use the default self-signed certificate	This is selected by default. This is acceptable in test environments, but should not be used in a production environment.
Provide a CA-signed certificate	Upload a CA-signed wildcard certificate in the form of a `.p12` or `.pfx` file and if necessary, type the key file password. **Note** CA certificate information must be provided in lowercase.

5. Click **Update Configuration**.

CHAPTER 10

Common Cloud Portal Tasks

These administrative tasks are common across the entire EMC Cloud Portal.

- Resetting your personal Cloud Portal password at sign-in 58
- Editing your personal Cloud Portal account profile 58
- Manage Cloud Portal Users 58
- Changing the event notification settings in the Cloud Portal 63
- Events history in the Cloud Portal 64
- Getting Help inside the Cloud Portal 65

Resetting your personal Cloud Portal password at sign-in

If you forget your EMC Cloud Portal user account password while signing in, you can reset it.

Procedure

1. From the **Sign In** page of the portal, select **Forgot Password?**
2. On the **Forgotten Password** page, specify the email address that you used when you set up your account, then select **Reset Password**.

   The page displays a prompt for you to check your email for a link to reset your password.
3. Check the email account that you used for the setting up your Cloud Portal account.

   You should receive a message with a link to reset your password.
4. Open your EMC email and select the link named **Set New Password**.

   The **Forgotten Password** page in the Cloud Portal opens in your browser.
5. On the **Forgotten Password** page, use the listed criteria to create and type a new password, then select **Set as password**.

   If your password does not match during confirmation, you are prompted to try again. If it does match, you are prompted to select a link to return to the Cloud Portal.

Editing your personal Cloud Portal account profile

If you want a new password, email address, or username, you can sign in to the EMC Cloud Portal and then edit your Cloud Portal profile to make the updates that you want.

Procedure

1. In the upper right-most corner of any page in the portal, select ••• (**Services Menu**) **› Edit Profile**.
2. On the **Edit Profile** page, edit the information in any field (or select **Change Password** and then create a new password), and then select **Update Profile**.

Manage Cloud Portal Users

As a tenant administrator, you can use the User Management function in the EMC Cloud Portal to manage the users who are now in the EMC Cloud Portal account and you can also invite other users whom you want to be added to the account. Users who accept the invitation to establish an account will have the same portal privileges that you now have, which means that they too will be able to invite other users, edit user information, or delete them as a Cloud Portal user.

Invite a user

You can invite one or more users to establish a Cloud Portal account. You will need to know the email address of each user you want to invite. For details, see Adding a new user and sending a Cloud Portal account invitation on page 59.

Edit a user

When you edit a user account with the User Management function, you can modify the username and email address. You can also reset the password. For details, see Editing a Cloud Portal user account on page 61.

Delete a User

You can delete one or more user accounts with the User Management function in the portal. Before any account is deleted, however, you are asked to confirm that you want to delete. For details, see Deleting a Cloud Portal user account on page 63.

Adding a new user and sending a Cloud Portal account invitation

As a Cloud Portal tenant administrator, you can add new users and invite them to create an EMC Cloud Portal account. Any user who accepts your invitation will have the same administrative privileges that you have.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials that you created from your own invitation.
2. In the upper right-most corner of any page in the portal, click ••• (**Services Menu**) **› User Management**.

   The **View Users** page opens.
3. Click **Invite Users**.

Option	Description
On the View Users page, select the Users mode, and then click Invite Users.	Opens a slide-out dialog where you can add the email addresses of users you want to invite to establish an account.
On the View Users page, select the Invitations mode, and then click Invite Users.	Opens a slide-out dialog where you can add the email addresses of users you want to invite to establish an account.

   Choosing either of these options opens the same dialog box.
4. In the **Invite Users** dialog box, enter the email address of the user you want to invite to establish an account.

   You can add as many email addresses as you like, but each address must be separated by a semicolon and each address must be valid.

   Valid email addresses are formatted in the form of *<local_part>*@*<domain_part>*, for example, `user@example.com`.
5. When you have entered email addresses for those you want to invite, click **Invite**.
   a. A popup appears to notify you that the email has been sent to the invitee.
   b. The user receives the email invitation, and the email address of the user is added to the list of invitations sent.
   c. (Conditional) If the user accepts the invitation, the email address is added to the list of users.
   d. (Conditional) If the users neglects the invitation, it expires in 90 days.

Note

You can re-invite a user who has already accepted an invitation, but you must use an alternate email address to add the recipient as a new user.
If the user does not accept the invitation, you can resend it. For more information, see Resending a Cloud Portal account invitation on page 60.

If you decide to withdraw the user invitation before it is accepted, you can delete it. For more information, see Deleting a Cloud Portal account invitation on page 61.

Resending a Cloud Portal account invitation

As a Cloud Portal tenant administrator, you can resend an account-creation invitation via email to a user who might have forgotten the original invitation.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials that you created from your own invitation.
2. In the upper right-most corner of any page in the portal, click ••• (**Services Menu**) › **User Management**.

   The **View Users** page opens.
3. Click **Invitations**, and then in the **User email** list, select one or more email addresses of the user account invitations you want to resend.

   The **Resend Invitation** button displays if you selected only one user account. The **Resend Invitations** button displays if you select multiple accounts. Two other buttons are also displayed.

   - **Invite Users**
   - **Delete Invitations**
     For more information about these options, see Adding a new user and sending a Cloud Portal account invitation on page 59 or Deleting a Cloud Portal account invitation on page 61.
4. When you have selected email addresses for the invitations you want to resend, click **Resend Invitation** (or click **Resend Invitations**, if multiple invitations are to be re-sent).

   a. A popup appears to notify you that the email has been re-sent to the invitee(s).

   b. The user receives the email invitation, and the email address of the user is added to the list of invitations sent.

   c. (Conditional) If the user accepts the invitation, the email address is added to the list of users.

   d. (Conditional) If the users neglects the invitation, it expires in 90 days.

Note

You can re-invite a user who has already accepted an invitation, but you must use an alternate email address to add the recipient as a new user.
If you decide to withdraw the user invitation before it is accepted, you can delete it. For more information, see Deleting a Cloud Portal account invitation on page 61.

Deleting a Cloud Portal account invitation

As a Cloud Portal tenant administrator, if an account-creation invitation has been ignored or if you sent it in error, you can delete it. Deletion of the email invitation makes its future acceptance impossible; a new invitation must be sent.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials that you created from your own invitation.
2. In the upper right-most corner of any page in the portal, click ••• (**Services Menu**) › **User Management**.

   The **View Users** page opens.
3. Click **Invitations**, and then in the **User email** list, select one or more email addresses of the user account invitations you want to resend.

   The **Delete Invitation** button is displayed if you selected only one user account. The **Delete Invitations** button is displayed if you select multiple accounts. Two other buttons are also displayed.

   - **Invite Users**
   - **Resend Invitations**
     For more information about these options, see Adding a new user and sending a Cloud Portal account invitation on page 59 or Resending a Cloud Portal account invitation on page 60.
4. When you have selected email addresses for the invitations you want to delete, click **Delete Invitation** (or click **Delete Invitations**, if multiple invitations are to be deleted).

   A popup appears to notify you that the email to the invitee(s) has been deleted.

Editing a Cloud Portal user account

As an EMC Cloud Portal tenant administrator, you can apply the Cloud Portal **User Management** function to edit some user account information. You can also reset a user password or delete a user account while using this function.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials that you created from your own invitation.
2. In the upper right-most corner of any page in the portal, click ••• (**Services Menu**) › **User Management**.

   The **View Users** page opens.
3. Click **Users**, and then in the **User email** list, select the email address of the user account you want to edit.

   The **Edit User** control is displayed (along with other controls).

Note

Selecting more than one email address removes the **Edit User** button from the page. One of the exposed controls is the **Invite Users** button and the other is the **Delete User** button. For more information about these options, see Adding a new user and sending a Cloud Portal account invitation on page 59 or Deleting a Cloud Portal user account on page 63.

4. Click **Edit User**.

   The **View user details** slide-out dialog box is displayed.

5. In the **View user details** dialog box, edit the fields as needed:

   - **First Name**

   Edit the name as you want it to appear in the salutation of emails sent from Cloud Portal.

   - **Email address**

   Edit the email address as needed. Valid email addresses are formatted in the form of `<local_part>@<domain_part>`, for example, `user@example.com`.

6. When you have made the changes you want, click **Update**.

   A popup appears to notify you that the user details have been updated.

Resetting a Cloud Portal user account password

As a Cloud Portal tenant administrator, you can reset the password on any EMC Cloud Portal user account, including your own.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials that you created from your own invitation.

2. In the upper right-most corner of any page in the portal, click ••• (**Services Menu**) › **User Management**.

   The **View Users** page opens.

3. Click **Users**, and then in the **User email** list, select the email address of the user account for which you want to reset the password that you want to edit.

   The **Edit User** control is displayed (along with other controls).

Note

One of the exposed controls is the **Invite Users** button and the other is the **Delete User** button. For more information about these options, see Adding a new user and sending a Cloud Portal account invitation on page 59 or Deleting a Cloud Portal user account on page 63.

4. Click **Edit User**.

   The **View user details** slide-out dialog box is displayed.

5. In the **View user details** dialog box, click the ⋯ button to expose two options.

   - **Reset Password**
   - **Delete**
     For more information about the **Delete** option, see Deleting a Cloud Portal user account on page 63.

6. Click **Reset Password**.

    a. A popup appears to notify you that a reset password instructional email has been sent to the user.

    b. The user receives the reset password instructional email.

Deleting a Cloud Portal user account

As an EMC Cloud Portal tenant administrator, you can apply the Cloud Portal **User Management** function to delete a user account. You can choose either of two methods to delete the account.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials that you created from your own invitation.
2. In the upper right-most corner of any page in the portal, click ••• (**Services Menu**) **›** **User Management**.

    The **View Users** page opens.
3. Click **Users**, and then in the **User email** list, select the email address of the user account you want to delete.

    The **Delete User** control is displayed (along with the **Invite Users** and **Edit User** controls).

    Note

    For more information about the other options, see Adding a new user and sending a Cloud Portal account invitation on page 59 and Editing a Cloud Portal user account on page 61.
4. Delete the user account using either of two methods.

Option	Description
Click **Delete User.**	Use this method to delete the user account directly from the **View Users** page.
Click **Edit User ›** ⬭ **› Delete User.**	Use this method to delete the user account if you decide to do so while in the **Edit User** mode.

Both of these methods effectively delete the selected user account from Cloud Portal.

Changing the event notification settings in the Cloud Portal

You can configure EMC Cloud Portal to push important event notifications in the form of alerts, system errors, system warnings, or other important information you want the portal or the portal plugin to communicate.

You can also choose how end users are to receive such a message.

- An email message to specified recipients
- An instant, onscreen message called a *toast notification*
- An email and a toast notification

To access these settings in the portal, select ••• (**Services Menu**) **› Events › Notification Settings**.

Email notifications

By default, email notifications for events are turned on, with the following event types available for selection:

- **Alerts** (critical events that require prompt action)
- **Errors** (operational errors that have occurred in the portal or in a portal plugin)
- **Warnings** (preemptive messages that draw attention to abnormal operating conditions)

You can clear the selection of any of these settings or add the **Info** event type (that is, status messages regarding the portal or portal plugin operations) to the selection.

The default recipient of these event email messages is the administrator whose email address was provided when the account was set up or edited. You can add other email recipients as needed.

Toast notifications

A toast notification is an onscreen alert message that you see as a text box sliding up from behind the action bar at the bottom of the page. The toast displays for 7 seconds before fading out. Its content is also added to a drop-down list (signified by the 🔔 icon) available in the portal utility bar. While it displays, you can click or tap the toast notification alert for more information, or you can do the same from the drop-down list. If an alert remains unopened, the portal reminds you.

By default, toast notifications for events are turned on, with only **Alerts** selected to display. You can clear the selection **Alerts**, or you select other event types (**Errors**, **Warnings**, **Info**) to display.

Events history in the Cloud Portal

The events history shows you at a glance the most important information about the operations of EMC Cloud Portal.

Any operation that EMC Cloud Portal records it also adds to a comprehensive list, available for viewing from the **Events History** page and accessed from ••• (**Services Menu**). In the list, you can:

- Filter the events further (by product name).
- Select event types (Alerts, Errors, Warnings, or Information).
- Select an event checkbox and then click the event name to view its details (including next steps and related information) or to dismiss it from the history list.

Event severity

Because events vary in importance or severity, and because there might be many events in the list, they are sorted into the following order and categories, by default, to prioritize your attention:

Table 6 How events are prioritized in Events History

1	🔔	Active alerts
2	🔔	Inactive alerts
3	⊗	Errors
4	⚠	Warnings

Table 6 How events are prioritized in Events History (continued)

5	(no icon)	Information

Within each of these categories, the events are sorted by most recent first. Use the controls at the bottom of the page to navigate to all the events, paged in groups of 30.

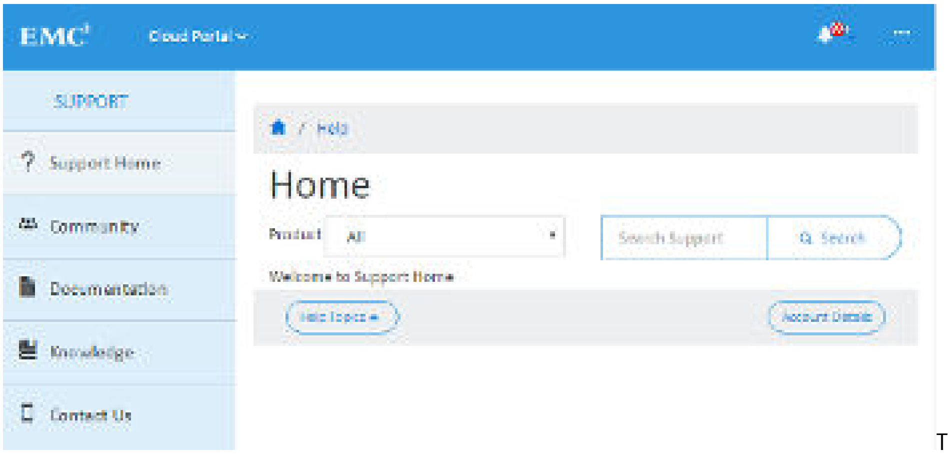
Getting Help inside the Cloud Portal

The EMC Cloud Portal provides a variety of help methods relevant for portal itself and also for EMC products using the portal as a platform.

Whether you want to view product documentation, monitor or consult EMC product community forums, consult the EMC Support Knowledge Base, find contact information for EMC Support, or learn more details about your customer account, help is available inside the Cloud Portal. To access help, select ••• (**Services Menu**) **› Help** In the upper right-most corner of any page in the portal.

The **Help** page displays these options.

Figure 11



The Cloud Portal Help Page

Note

The help mode icons on the **Help** home page are repeated as menu options at the top of every Help subpage. Each subpage also includes a Search (Search) feature that restricts its queries according to the help mode selected.

Product
This drop-down selector lists all the EMC Cloud Portal plugins that you have purchased. Selecting a product name filters the help resources to include items relevant to that product only.

Community
This button links to the EMC product community page that matches the product filter you have selected. The respective community pages, which are located outside the portal, have a built-in **Search** function that queries community-specific topics only.

Knowledge Base

This button links to a **Knowledge Base** home page that lists trending and recently updated Knowledge Base articles. These articles match the product filter that you select. You can search the entire Knowledge Base using your own search term or you can use one of the listed popular search terms.

Documentation

This button links to a **Documentation** home page that lists published guides and release notes. The content titles on the page match the product filter that you select. If no product is selected, a page listing all available documentation options is displayed.

Every documentation page is organized with left-hand navigation and nested topics, to ease browsing.

Other features available on every documentation page include the following:

- **Print Article**: This button launches the browser's print dialog box, from which you can print the currently displayed HTML page.
- **Download Guide**: This button downloads a PDF version of the entire publication.
- **Rate Article**: This button lets you vote on whether the content on the page was helpful to you.
- **Send Feedback**: This button lets you leave feedback for the writer of the content.

Contact Us

This button links to the **Contact Us** page that lists telephone numbers for EMC Global support centers and field offices. The page also provides a link to a list of in-country support phone numbers and another link to the **EMC Support** home page.

Help Topics

This button links to more articles about using the Cloud Portal, troubleshooting information, using EMC Support, and so on.

Account Details

This button links to information about your customer account, your account administrator, and the products and services that your account is entitled to.

APPENDIX A

About this document

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note

This document was accurate at publication time. Go to EMC Online Support at https://support.emc.com to ensure that you are using the latest version of this document.

Purpose

This document describes the integration of NetWorker® with CloudBoost™.

Audience

This guide is part of the CloudBoost documentation set, and is intended for use by system administrators who are responsible for setting up and maintaining backups on a network. Operators who monitor daily backups will also find this guide useful.

Revision history

The following table presents the revision history of this document.

Table 7 Document revision history

Revision	Date	Description
01	October 11, 2016	Initial release of *EMC Networker 8.x with CloudBoost 2.1 Integration Guide*.

Related documentation

The following EMC publications provide information about CloudBoost.

- *EMC CloudBoost Release Notes*
  Contains information about new features and changes, fixed problems, known limitations, environment and system requirements for the latest release.
- *EMC CloudBoost 100 Installation Guide*
  Guide for installing the physical CloudBoost 100 appliance, and initial configuration at command line interface.
- *EMC CloudBoost Disk Array Expansion Shelf Installation Guide*
  Guide for installing the disk array expansion shelf for use with the physical appliance.
- *EMC CloudBoost Hardware Component Replacement Guide*
  Guide for customers replacing hardware components for the CloudBoost physical appliance.

You may find these publications helpful when integrating CloudBoost with different systems.

- *EMC NetWorker with EMC CloudBoost Integration Guide*
  Guide for integrating EMC NetWorker with EMC CloudBoost.
- *EMC NetWorker 8.x with EMC CloudBoost Integration Guide*
  Guide for integrating EMC NetWorker 8.x with EMC CloudBoost.
- *EMC Avamar with EMC CloudBoost Integration Guide*
  Guide for integrating EMC Avamar with EMC CloudBoost.
- *Veritas NetBackup with EMC CloudBoost Integration Guide*
  Guide for integrating Veritas NetBackup with EMC CloudBoost.

You may also find it helpful to refer to these NetWorker publications.

- *EMC NetWorker Administration Guide*
  Describes how to configure and maintain the NetWorker software.
- *EMC NetWorker Installation Guide*
  Provides information about how to install, uninstall, and update the NetWorker software for clients, storage nodes, and serves on all supported operating systems.

Where to get support

Go to EMC Online Support at https://support.emc.com/ and click **Service Center**. You will see several options for contacting EMC Technical Support. To open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

How to provide feedback

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to mailto:techpubcomments@emc.com.

Please include the following information.

- Product name and version
- Document name, part number, and revision (for example, 01)
- Page numbers
- Topic titles
- Other details to help address documentation issues