Chapter 11  Common Cloud Portal Tasks  93
Resetting your personal Cloud Portal password at sign-in............... 94
Editing your personal Cloud Portal account profile......................... 94
Manage Cloud Portal users......................................................... 94
  Adding a new user and sending a Cloud Portal account invitation.... 95
  Editing a Cloud Portal user account....................................... 97
  Deleting a Cloud Portal user account..................................... 98
Changing the event notification settings in the Cloud Portal............. 99
Events history in the Cloud Portal.............................................. 100
Getting help inside the Cloud Portal........................................ 100
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 EMC® NetWorker® with EMC® 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

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>January 12, 2017</td>
<td>Updated content for downloading the CloudBoost VHDs and JSON file from <a href="https://support.emc.com">https://support.emc.com</a></td>
</tr>
<tr>
<td>01</td>
<td>December 22, 2016</td>
<td>Initial release of <em>EMC NetWorker 9.1 with CloudBoost 2.1 Integration Guide</em></td>
</tr>
</tbody>
</table>

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 9.1 with EMC CloudBoost Integration Guide**
  Guide for integrating EMC NetWorker 9.1 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 servers on all supported operating systems.

### Special notice conventions that are used in this document

EMC uses the following conventions for special notices:

- **NOTICE**
  Identifies content that warns of potential business or data loss.

- **Note**
  Contains information that is incidental, but not essential, to the topic.

### Typographical conventions

EMC uses the following type style conventions in this document:

**Table 2 Style conventions**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Used for names of interface elements, such as names of buttons, fields, tab names, and menu paths (what the user specifically selects or clicks)</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Used for full titles of publications that are referenced in text</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Used for:</td>
</tr>
<tr>
<td></td>
<td>• System code</td>
</tr>
<tr>
<td></td>
<td>• System output, such as an error message or script</td>
</tr>
<tr>
<td></td>
<td>• Pathnames, file names, prompts, and syntax</td>
</tr>
<tr>
<td></td>
<td>• Commands and options</td>
</tr>
<tr>
<td><em>Monospace italic</em></td>
<td>Used for variables</td>
</tr>
<tr>
<td><em>Monospace bold</em></td>
<td>Used for user input</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose optional values</td>
</tr>
</tbody>
</table>
Table 2 Style conventions (continued)

| Vertical bar indicates alternate selections - the bar means “or” |
| { } Braces enclose content that the user must specify, such as x or y or z |
| ... Ellipses indicate non-essential information that is omitted from the example |

Where to get help
EMC support, product, and licensing information can be obtained as follows:

Product information
For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support
Go to EMC Online Support and click Service Center. Several options for contacting EMC Technical Support appear on the site. Note that 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.

Online communities
Go to the EMC Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all EMC products.

Your comments
Your suggestions help to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.
Preface
CHAPTER 1

About CloudBoost Integration with NetWorker

This section contains the following topics:

- About CloudBoost ................................................................. 12
- CloudBoost with NetWorker .................................................. 12
- Supported server and client versions ...................................... 16
- Supported private clouds ....................................................... 16
- Supported public clouds ....................................................... 17
- Firewall port requirements ................................................... 18
- Installation roadmap ............................................................. 19
About CloudBoost

The CloudBoost appliance provides an integrated solution with your existing supported backup environment by enabling you to transfer backups to the cloud. The CloudBoost appliance enables backups to public, hybrid, or private cloud storage.

CloudBoost decouples metadata from data. Encryption keys, metadata, and file system information are housed separately from the data, which removes a common bottleneck for cloud reads and writes. 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 supported private and public clouds.

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.

CloudBoost with NetWorker

A NetWorker with CloudBoost environment can extend on-site data protection to the cloud with the following solutions.

- Backup to the cloud
- Backup to cloud directly with the Networker Linux client
- Backup in the cloud using Amazon EC2 and Amazon S3
- Backup in the cloud using Microsoft Azure

CloudBoost requirements and considerations

Before you can use the CloudBoost 2.1 Appliance to protect data in a NetWorker datazone, you must deploy a CloudBoost 2.1 appliance in the environment.

Client Direct

The Client Direct feature is only supported on 64-bit Linux NetWorker clients and requires the following Linux package requirements:

- libc 2.5 or later
- libstdc++ 6.0.8 or later (GLIBCXX_3.4.8)

Block Based Backup or NetWorker Module for Microsoft (NMM) backup data

You cannot recover Block Based Backup (BBB) or NetWorker Module for Microsoft (NMM) backup data from a CloudBoost device.

To recover Block Based Backup (BBB) or NetWorker Module for Microsoft (NMM) backup data:

1. Clone the data from the CloudBoost device to an AFTD or Data Domain device.
2. Recover the data from the clone device.

**Back up to the cloud**

As of CloudBoost version 2.1, when used with NetWorker 9.0.1 or later, backup directly to the cloud is supported without having to first clone data to a staging server. The CloudBoost appliance is a device type in NetWorker 9.0.1 or later.

This use case is intended for when you have onsite infrastructure and would like to use public cloud object storage for all backup workloads. This includes short term backups for operational recovery and long term backups for compliance.

The optional site cache eliminates the impact of long-distance connectivity. It also better meets recovery time objectives because the most frequently used data is locally cached.

**Note**

- If backing up several Windows clients to the cloud, use a NetWorker storage node that is deployed on a separate Linux server, and do not use the NetWorker Storage Node on the CloudBoost appliance. This method moves some of the load from the CloudBoost appliance to the separate NetWorker Storage Node. For information on how to install a NetWorker Storage Node on a Linux server, see the *NetWorker Administration Guide*.

- If you are using a Linux NetWorker client and backing up directly to the cloud, you do not need to deploy a separate Linux NetWorker Storage Node.

**Figure 1** Back up to the cloud

Back up to the cloud is recommended for use with the following use cases:

- On site object store such as the EMC ECS Appliance
- With a high bandwidth pipe to a public object store
- For non-critical applications that can tolerate longer backup service level agreements
Direct back up to the cloud with Linux clients

CloudBoost 2.1 or later and the Linux clients for NetWorker 9.0.1 or later back up directly to the cloud.

This use case is intended for when you have on-site infrastructure and would like to use object storage for all backup workloads, including short term backups for operational recovery and long term backups for compliance.

The optional site cache eliminates the impact of long-distance connectivity. It also meets recovery time objectives quicker, because the most frequently used data is locally cached.

Figure 2 Linux clients back up directly to cloud

Back up in Amazon EC2 to Amazon S3 storage

NetWorker 9.0.1 or later when used with CloudBoost version 2.1 and later can run on Amazon EC2 to back up directly to Amazon S3.

This use case is intended for when you have workloads running in public cloud and would like to use inexpensive S3 cloud object storage for all backups, including short term backups for operational recovery and long term retention backups for compliance.

In support of the hybrid cloud, sometimes known as the lift and shift use case, the NetWorker tools you use to manage on-site data protection processes are the same for your cloud-based data protection processes.
The optional site cache service is not available when the CloudBoost appliance is deployed within EC2.

Cloud best practices

Consider the topics and recommendations in this section before implementing cloud backups.

Backups to a cloud storage device

Backups are sent to a cloud storage device by using media pools, in the same way that client backups are directed to a device or set of devices.

Consider the following recommendations:

- Set up one or more media pools for CloudBoost devices and provide the pool with a unique label template.
- Do not mix CloudBoost backup devices with other types of backup devices in a media pool.

Concurrent backup and recovery operations

You can mount a single CloudBoost appliance as multiple cloud storage devices to support concurrent backup and recovery operations.

For example, to optimize performance you can mount the CloudBoost appliance on three cloud storage devices: one for backup (device CL1), one for recovery (device CL2), and one for clone operations (device CL3). There is no limit to the number of cloud storage devices that can be mounted on a single cloud volume. Consider such an approach to optimize backup and recovery performance.

Network dependencies

Cloud backups are highly dependent on the network connection that is used to access the cloud service. Any disruption in connectivity or a slowdown in network access speed may adversely affect cloud backups or recoveries.

Proper name resolution and internet access is required for the CloudBoost appliance. The CloudBoost appliance documentation provides more information.
Supported server and client versions

These server and client versions are supported in CloudBoost integrations.

- NetWorker Server 9.0.1 or later

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

NetWorker Requirements

The use of a native CloudBoost device requires a NetWorker storage node on the Linux platform. For more information, see the EMC NetWorker Administration Guide.

Note

The NetWorker storage node can be on a separate system, on the NetWorker server itself or embedded in the CloudBoost appliance.

NetWorker provides support for all clients cloning to the cloud for long term retention.

NetWorker Limitations

NetWorker provides support for all clients backing 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

- Backing up directly to the cloud is only supported by the NetWorker Linux client. All other clients are directed through a NetWorker Storage Node.
- 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.

Supported private clouds

Table 3 Supported private clouds

<table>
<thead>
<tr>
<th>Cloud provider</th>
<th>Information required by CloudBoost</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC ATMOS</td>
<td>Access Point URL, Full Token ID (subtenant/uid), Shared Secret</td>
</tr>
<tr>
<td>EMC ECS Appliance</td>
<td>ECS Endpoint, ECS Access Key ID, ECS Secret Access Key</td>
</tr>
</tbody>
</table>

Note

ECS Community version is not supported with CloudBoost.
**Table 3** Supported private clouds (continued)

<table>
<thead>
<tr>
<th>Cloud provider</th>
<th>Information required by CloudBoost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic OpenStack Swift</td>
<td>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</td>
</tr>
</tbody>
</table>

**Supported public clouds**

**Table 4** Supported public clouds

<table>
<thead>
<tr>
<th>Cloud provider</th>
<th>Information required by CloudBoost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtustream Storage Cloud (Standard and Premium)</td>
<td>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, and therefore cannot be selected when creating a new cloud profile.</td>
</tr>
<tr>
<td>Amazon Web Services (S3)</td>
<td>Storage Region, AWS Access Key ID, AWS Secret Access Key</td>
</tr>
<tr>
<td>AT&amp;T Synaptic Storage</td>
<td>AT&amp;T Synaptic Subtenant ID, AT&amp;T Synaptic User ID, AT&amp;T Synaptic Secret Key</td>
</tr>
<tr>
<td>Google Cloud Storage (Standard, DRA, Nearline)</td>
<td>Access Key, Secret</td>
</tr>
</tbody>
</table>

**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](https://cloud.google.com/storage/docs/migrating?hl=en#migration-simple).

<table>
<thead>
<tr>
<th>Microsoft Azure Storage (general purpose accounts, replication types LRS, GRS, RA-GRS)</th>
<th>Azure Account Name, Azure API Key</th>
</tr>
</thead>
</table>

**Note**

Object storage only accounts are not supported.

<table>
<thead>
<tr>
<th>Microsoft Azure ARM</th>
<th>Azure Account Name, Azure API Key, Storage account name, storage access key, storage connection string</th>
</tr>
</thead>
</table>

**Note**

Object storage only accounts are not supported.
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, 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 5 Firewall port requirements

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

For information about firewall ports for any system being deployed with CloudBoost, refer to the documentation for that system.
For information about NetWorker, refer to the *EMC NetWorker Security Configuration Guide*.

## Installation roadmap

Follow these steps when integrating with NetWorker.

### Procedure

1. If not already installed, install NetWorker.
2. Open all the required ports listed in *Firewall port requirements* on page 18.
3. Deploy the CloudBoost appliance.
   - To deploy on ESX, see *Deploying the virtual CloudBoost appliance on ESX* on page 30.
   - To deploy on Amazon EC2, see *Deploying the CloudBoost appliance in Amazon EC2* on page 46.
   - To deploy on Microsoft Azure, see *Deploying CloudBoost in Microsoft Azure ARM* on page 37.
4. Register the CloudBoost appliance in the EMС Cloud Portal.
   For more information, see *Registering a CloudBoost appliance* on page 59.
5. Configure the CloudBoost appliance in the EMС Cloud Portal.
   For more information, see *Configuring a new CloudBoost appliance* on page 60.
6. Configure NetWorker to work with the CloudBoost appliance.
   For more information, see *Configure NetWorker with CloudBoost* on page 63.
7. Install and configure the CloudBoost client when needed.
   For more information, see the *EMC CloudBoost Client Guide*
About CloudBoost Integration with NetWorker
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 ................................................................. 22
- CloudBoost sizing and performance considerations .................. 24
- Installation roadmap ................................................................. 26
Solution requirements

The following topics outline the solution requirements for the CloudBoost appliance.

For more information on metadata store and site cache hard disk sizing, see CloudBoost sizing and performance considerations on page 24.

WAN requirements

These are the WAN requirements.

- Greater than or equal to 10MBits bandwidth
- Less than or equal to 100ms RTT latency

Requirements for the VMware ESX virtual CloudBoost appliance

The following section outlines the requirements for the VMware ESX virtual CloudBoost appliance.

Minimum deployment virtual machine requirements for ESX

The following types of work flows are supported.

- Client Direct: The NetWorker 9.0.1 or later Linux client is connecting directly to the specified cloud provider for backup.
- Backup: The NetWorker client is connecting to a storage node for backup. The storage node can be an external Linux storage node or the storage node embedded within the CloudBoost appliance. It is recommended to use an external storage node particularly for large scale deployments.
- Clone: NetWorker clients are backed up to a local target such as a Data Domain and then cloned to cloud for long-term retention of data.

<table>
<thead>
<tr>
<th>Work Flow Type</th>
<th>Site Cache</th>
<th>CPU</th>
<th>Memory</th>
<th>OS</th>
<th>Metadata</th>
<th>Site Cache Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client direct backup</td>
<td>No</td>
<td>4</td>
<td>16 GB</td>
<td>41 GB</td>
<td>100 GB</td>
<td>NA</td>
</tr>
<tr>
<td>Backup/clone via CloudBoost appliance</td>
<td>No</td>
<td>8</td>
<td>32 GB</td>
<td></td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>16</td>
<td>64 GB</td>
<td></td>
<td></td>
<td>200 GB</td>
</tr>
</tbody>
</table>

Large deployment virtual machine requirements for ESX

The following requirements apply.

- 8 cores (double this number if a site cache is used)
- 32 GB of RAM (double this number if a site cache is used)
- 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)

Requirements for the VMware EC2 virtual CloudBoost appliance

The following section outlines the requirements for the VMware EC2 virtual CloudBoost appliance.

Minimum deployment requirements for AWS EC2

The following requirements are the minimum deployment requirements for CloudBoost deployed on AWS EC2.

The following types of work flows are supported.

- Client Direct: The NetWorker 9.0.1 or later Linux client is connecting directly to the specified cloud provider for backup.
- Backup: The NetWorker client is connecting to a storage node for backup. The storage node can be an external Linux storage node or the storage node embedded within the CloudBoost appliance. It is recommended to use an external storage node particularly for large scale deployments.
- Clone: NetWorker clients are backed up to a local target such as a Data Domain and then cloned to cloud for long-term retention of data.

Note

Site cache is not supported for deployments on EC2.

Table 7 Minimum deployment requirements for AWS EC2

<table>
<thead>
<tr>
<th>Work Flow Type</th>
<th>CPU</th>
<th>Memory</th>
<th>OS</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client direct backup</td>
<td>4</td>
<td>16 GB</td>
<td>41 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td>Backup/Clone via CloudBoost appliance</td>
<td>8</td>
<td>32 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

EMC suggests using the AWS EC2 instance type m4.xlarge for small Client Direct installs.

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.

Large deployment requirements for AWS EC2

These are the requirements for a large deployment on AWS EC2.
Table 8 Large deployment requirements for AWS EC2

<table>
<thead>
<tr>
<th>CPU</th>
<th>Memory</th>
<th>OS</th>
<th>Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>32 GB</td>
<td>41 GB</td>
<td>100 GB metadata required per 200 TB of logical capacity</td>
</tr>
</tbody>
</table>

The primary metadata volume can be expanded to 3TB to manage up to 6PB of logical protected capacity.

EMC suggests using the AWS EC2 instance type m2.xlarge for client direct or for all installs of backup/clone via the EMC appliance.

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.

CloudBoost sizing and performance considerations

The following topics contain information about CloudBoost sizing, performance and requirements.

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 enabled, 16 cores and 64 GB of memory is recommended.
- If site caching is not enabled, 4 cores with 16 GB of memory is recommended.

Note

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 1:2000. 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.

Deduplication and cloud capacity

Both the physical and virtual CloudBoost appliances support up to 6 PB of logical capacity using 3TB of metadata disk space before deduplication.

Based on preliminary test data, CloudBoost is expected to achieve a 4x–8x range of deduplication.

Based on this range of deduplication, each CloudBoost appliance can support up to approximately 6 PB of logical capacity.
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 virtual machine.

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

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

About CloudBoost caching

The optional site cache allows quick backups over the LAN when trickling more slowly over the WAN.

Site caching enables faster backup and recovery for the objects that have been most recently written to or read from the cloud. This persistent cache is wiped and reused as needed during these processes.

If you intend to enable the site cache for a CloudBoost appliance, change the data disk size before initial configuration of the CloudBoost appliance at the CLI.

Use of the cache is advisable under these circumstances.

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

Note

Site cache is only available on ESX deployments or with physical hardware.

CloudBoost appliance cache sizing

If you intend to enable the site cache for a CloudBoost appliance, change the data disk size before initial configuration of the CloudBoost appliance at the CLI.

Change the 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 on the amount of data you plan to backup.

Consider the following:

- The ingestion rate for a CloudBoost appliance without site cache enabled is measured at up to 100 MB/s.
- The site cache has a 50 MB/s ingestion rate for the 32 TB physical appliance.
- The site cache has a 25 MB/s ingestion rate for all other appliances that can be improved by de-duplication and compression, depending on the workload.
- The underlying storage rate must be 25 MB/s for simultaneous reading and writing.
- An average chunk size of 256 KB equals a few hundred IOPS.
- The total number of site cache disks must be a multiple of 2 up to 32 disks. For example 1, 2, 4, 8, 16 or 32 disks.
To optimize performance, configure each site cache VMDK on a different data store. For example, for a 2TB site cache 4x500GB VMDKs can be used.

- The size of the cache cannot be increased or decreased by growing the existing data disk size in vCenter.
- The minimum size of the cache is 200 GB, and can be increased up to 6 TB on the virtual appliance by adding disks that match the size of the existing site cache disks.
- The cache is firewall-friendly, so multiple ports do not need to be opened.

Note

If higher ingestion speeds occur when connecting directly to the cloud store, do not use the cache. The backups might exceed the capacity of the cache.

Table 9 ESX site cache minimum requirements

<table>
<thead>
<tr>
<th>Work Flow Type</th>
<th>Site Cache</th>
<th>CPU</th>
<th>Memory</th>
<th>OS</th>
<th>Metadata</th>
<th>Site Cache Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup/Clone</td>
<td>Yes</td>
<td>16</td>
<td>64 GB</td>
<td>41 GB</td>
<td>100 GB</td>
<td>200 GB</td>
</tr>
</tbody>
</table>

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.

Installation roadmap

Follow these steps when integrating with NetWorker.

Procedure

1. If not already installed, install NetWorker.
2. Open all the required ports listed in Firewall port requirements on page 18.
3. Deploy the CloudBoost appliance.
   - To deploy on ESX, see Deploying the virtual CloudBoost appliance on ESX on page 30.
   - To deploy on Amazon EC2, see Deploying the CloudBoost appliance in Amazon EC2 on page 46.
   - To deploy on Microsoft Azure, see Deploying CloudBoost in Microsoft Azure ARM on page 37.
4. Register the CloudBoost appliance in the EMC Cloud Portal.
   For more information, see Registering a CloudBoost appliance on page 59.
5. Configure the CloudBoost appliance in the EMC Cloud Portal.
   For more information, see Configuring a new CloudBoost appliance on page 60.

6. Configure NetWorker to work with the CloudBoost appliance.
   For more information, see Configure NetWorker with CloudBoost on page 63.

7. Install and configure the CloudBoost client when needed.
   For more information, see the EMC CloudBoost Client Guide
CHAPTER 3

Deploy the Virtual CloudBoost Appliance on ESX

This section includes the following topics:

- About installing ................................................................. 30
- Deploying the virtual CloudBoost appliance on ESX .................. 30
- Configuring network settings for a CloudBoost appliance ............ 31
About installing

This section applies to installing the virtual CloudBoost appliance on ESX. For information on installing the physical appliance, see the *EMC CloudBoost Installation Guide*.

You must obtain the .ova file from [https://support.emc.com](https://support.emc.com) to install the virtual appliance.

The procedures for deploying virtual appliance differ for each cloud provider:

- To deploy the CloudBoost virtual appliance on Amazon EC2, see Deploying the CloudBoost Appliance in Amazon EC2 on page 45.
- To deploy the CloudBoost virtual appliance on Microsoft Azure, see Deploying CloudBoost in Microsoft Azure ARM on page 37.

Deploying the virtual CloudBoost appliance on ESX

Deploy 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 drive, an SSD drive is recommended, with at least 100 GB of available space, plus what is required for the site cache if you choose to use a site cache.

**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 that runs the VM), and then type the name of the VM.

3. Select the data store for the VMDK files, and then click **Next**.

   For optimal performance, select **Thick Provisioned Eager Zeroed** when selecting the target data store. However, for testing purposes, the default 50 GB thin or thick provisioned storage is sufficient.

4. On the **Ready to Complete** page of the wizard, review the deployment settings.

5. Clear the **Power on after deployment** checkbox, and then click **Finish**.

6. Right-click the virtual machine:
   - Click **Edit Settings**.
   - On the **Hardware** tab, click **Memory**.
   - Ensure that **Reservation** is set to **all**.
   - Click **OK**.
Note

For performance, memory must be reserved rather than shared.

7. Adjust the size of hard disk 2 (metadata store) and hard disk 3 (site cache) as needed.
   a. Right-click on the virtual machine.
   b. Click Edit Settings.
   c. On the Resources tab, type the sizes of hard disk 2 and 3 in the appropriate fields.
   d. Click OK.

Any other hard disks that are added are used for the site cache. For more information on how to size these disks appropriately, see CloudBoost sizing and performance considerations on page 24.

The CloudBoost virtual appliance is installed.

Note

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. For more information, see Configure Network Settings for a CloudBoost Appliance on page 49.

Configuring network settings for a CloudBoost appliance

Procedure

1. Open a CLI window on the CloudBoost appliance. The procedures differ depending on where the CloudBoost appliance CLI is to be opened.

   Use the following table for instructions on how to open the CLI on different platforms.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere client</td>
<td>In the vSphere client, right-click VM &gt; Open Console.</td>
</tr>
<tr>
<td>EC2</td>
<td>a. Log in to EC2, select the CloudBoost appliance, and then click Connect.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>c. In the SSH terminal, type the following command:</td>
</tr>
<tr>
<td></td>
<td>ssh -i &quot;private key&quot; admin@AWS FQDN or IP</td>
</tr>
<tr>
<td></td>
<td>where private key is the private key you used as the key pair when you installed your CloudBoost AMI.</td>
</tr>
</tbody>
</table>
Deploy the Virtual CloudBoost Appliance on ESX

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>It is best practice to keep the DHCP configuration options supplied by Amazon.</td>
</tr>
</tbody>
</table>

**Microsoft Azure**

a. Log in to Microsoft Azure, select, and open the CloudBoost appliance.

b. Connect to the CloudBoost appliance using either of the following methods:
   - Use an SSH client
   - Log in through a browser

The CloudBoost CLI appears.

*Figure 4 CLI for CloudBoost*

Welcome to the EMC CloudBoost Management Console (3.0.0-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     ----       -------
```
5. For CloudBoost 2.1, if the network interface card was not configured when the CloudBoost appliance was installed in the ESX server, run the following command to add a new virtual LAN on the appliance:

```
net create interface interface vlan vlan_id
```

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

- For CloudBoost 2.1:

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

For example,

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

- For CloudBoost 2.0:

```
ip-address static <ip_address> netmask <netmask> gateway <gateway>
```

7. For CloudBoost 2.1, manually add the gateway by running these commands. If you have multiple networks, you must also add multiple routes to the 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
```
8. To manually set the DNS, type these commands:

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

For example:

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

9. To set the FQDN, type this command:

```bash
fqdn servername.yourcompanydomain
```

**Note**

The FQDN must be in lowercase.

For example:

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

10. To verify the networking setup and see the status of the appliance, type this command:

```bash
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

Network Routes:
    prefix          netmask         gateway
    ------          -------         -------
    default         0.0.0.0         10.5.96.1
    0.0.0.0         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 by using the EMC Cloud Portal.

Note

Other commands are also available from the command line. To get help, type `help` or `?`. 
Deploy the Virtual CloudBoost Appliance on ESX
CHAPTER 4

Deploying CloudBoost in Microsoft Azure ARM

Use the procedures in this section to deploy the CloudBoost appliance in Microsoft Azure ARM.

- About CloudBoost with Microsoft Azure .......................................................... 38
- Configuring Microsoft Azure for CloudBoost .................................................. 38
- Downloading the VHDs and JSON template .................................................. 39
- Uploading the VHDs ........................................................................................ 39
- Deploying CloudBoost with the JSON template ................................ .......... 41
- Verifying networking setup and status of the appliance ............................... 42
About CloudBoost with Microsoft Azure

CloudBoost integration leverages Microsoft Azure low-cost blob storage to provide deduplication at the source, minimizing bandwidth and storage consumption.

Use the following procedures to deploy and integrate CloudBoost with Microsoft Azure.

Configuring Microsoft Azure for CloudBoost

**Before you begin**

- Ensure that you have a Microsoft Azure Account.
- Ensure that you have Azure CLI tools.

Refer to the Microsoft Azure documentation for installation and configuration details.

**Procedure**

1. **Authenticate Azure with the account.**
   a. Open the Azure CLI and type the following command:
   ```
   azure login
   ```
   A device code appears with a link to the Microsoft Azure Device Login page.
   b. Browse to the provided Microsoft Azure Device Login page.
   c. Type the device code in the field.

2. **Create or use a storage account with the following properties:**
   - Deployment Model - Resource Manager
   - Account Kind - General Purpose
   - Replication - Select any type. Do not select ZRS.

3. **Set the deployment mode to Resource Mode:**
   ```
   azure config mode arm
   ```

4. **Open the Azure Resource Manager and perform the following steps:**
   a. Create a resource group or use an existing resource group to deploy the CloudBoost Virtual Machine (VM).
      This resource group is used in the steps that follow.
   b. Create a container within the storage account.

5. **Retrieve the Azure storage account information:**
   - To list details about the storage account, type the following command:
   ```
   azure storage account list
   ```
This command lists the storage account name, type, location, and resource group.

- To retrieve the Azure storage access key, type the following command:

```bash
azure storage account keys list <storage_account_name> -g <resource_group>
```

6. Add the following Azure credentials to the storage account by typing the following command:

```bash
export AZURE_STORAGE_ACCOUNT=<storage_account_name>

export AZURE_STORAGE_ACCESS_KEY=<primary_access_key>
```

In Linux, you can add these commands in `.bashrc`.

**Downloading the VHDs and JSON template**

Depending on network bandwidth, downloading these files might be time consuming because of their large size.

**Procedure**

1. Download the CloudBoost appliance from the Dell EMC online support site.
2. Extract the files from the downloaded zip file.

The zip file contains the following files:

- **Virtual Root Hard Disk (VHDs) zip file:**
  CloudBoost-2.1.3-azure-root.zip
  
  The root VHD is approximately 3 GB, but as a sparse file it is 50 GB.

- **lvm VHD zip file:**
  CloudBoost-2.1.3-azure-lvm.zip
  
  The lvm VHD is approximately 50 MB, but as a sparse file it is 40 GB.

- **azuredeploy.json**

**Uploading the VHDs**

There are two different methods of uploading the VHDs to the Microsoft Azure storage account.

The azure-vhd-utils GO tool method can take less than an hour to upload the VHDs.

The command template method can take several hours to upload the VHDs.

- Upload the VHDs by using the azure-vhd-utils GO tool that is provided by Microsoft.
This method takes less time than by using the Microsoft Azure command template.

1. Install the latest version of the Go programming language software available at the following link:
   https://golang.org/dl/

2. Set the GOPATH and PATH environment variables as specified at:
   https://golang.org/doc/code.html#GOPATH

3. Run the following command:

   ```
   go get github.com/Microsoft/azure-vhd-utils
   ```

4. Upload the root VHD by typing the following command on one line:

   ```
   azure-vhd-utils upload --localvhdpth <root.vhd_path> --stgaccountname <storage_account_name> --stgaccountkey <storage_account_key> --containername <container_name> --blobname <dest_blob_name>
   ```

   where:
   - `<root.vhd_path>` is the file path of the root VHD.
   - `<storage_account_name>` is the name of the storage account where the blob is to be uploaded.
   - `<storage_account_key>` is the storage account key information that was obtained earlier.
   - `<container_name>` is the destination location of the container in the storage account.
   - `<dest_blob_name>` is the name of the blob in which to upload the VHD file.

5. Upload the LVM VHD by typing the following command on one line:

   ```
   azure-vhd-utils upload --localvhdpth <lvm.vhd_path> --stgaccountname <storage_account_name> --stgaccountkey <storage_account_key> --containername <container_name> --blobname <dest_blob_name>
   ```

   where:
   - `<lvm.vhd_path>` is the file path of the LVM VHD.
   - `<storage_account_name>` is the name of the storage account where the blob is to be uploaded.
   - `<storage_account_key>` is the storage account key information that was obtained earlier.
   - `<container_name>` is the destination location of the container in the storage account.
   - `<dest_blob_name>` is the name of the blob in which to upload the VHD file.

- Upload the root and LVM VHDs to the storage account by using the following command template:
Note

Depending on network bandwidth, uploading these files might be time consuming because of their large size.

```bash
azure storage blob upload <image_to_upload> <container_name> <blob_name>
```

where:

- `<image_to_upload>` is the root or LVM VHD file to upload.
- `<container_name>` is the destination location of the container in the storage account.
- `<blob_name>` is the name of the blob in which to upload the VHD file.

An output similar to the following appears:

```
$ azure storage blob upload CloudBoost-2.1.3-azure-root.vhd
vhds test -azure-root.vhd
info: Executing command storage blob upload
+ Checking blob test-azure-root.vhd in container vhds
+ Uploading CloudBoost-2.1.3-azure-root.vhd to blob test-azure-root.vhd in container vhds
Percentage: 9.0% (3.69GB/41.00GB) Average Speed: 1.86MB/S
Elapsed Time: 00:33:51 11
```

### Deploying CloudBoost with the JSON template

**Procedure**

1. Deploy the CloudBoost virtual machine in Microsoft Azure by using the `azuredeploy.json` file that was downloaded from the Dell EMC online support site.
   
   a. Type the following command:

   ```bash
   azure group deployment create -n <deployment_name> -f azuredeploy.json -g <resource_group>
   ```

   where:

   - `<deployment_name>` is the name of the deployment. Use a unique name.
   - `<resource_group>` is the name of the resource group that was used to deploy the virtual machine.

   b. At the prompt, provide the following information:

   - For the `vmName` field, specify a unique name for the virtual machine.
   - For the `storageAccountName` field, specify the storage account name to associate with the virtual machine.
   - For the `osDiskVhdUri` field, type the destination URL of the following blob:

   ```bash
   <URL_to_VHD_Azure_blob>/CloudBoost-2.1.3-azure-root.vhd
   ```
For the metaDiskVhdUri field, type the destination URL of the following blob:
<URL_to_VHD_Azure_blob>/CloudBoost-2.1.3-azure-lvm.vhd

2. Start the virtual machine and perform the following steps:
   a. Log in as admin with the default password.
      Note
      The default password is password.
   b. Set the new admin password.
   c. Set the FQDN by typing the following command:

      fqdn <FQDN_name>

      Note
      Use the FQDN_name provided by Microsoft Azure. Custom FQDN names are not supported.

3. To check the Microsoft Azure audit logs, type the following command:

   azure group log show <resource_group> --last deployment

   Where <resource_group> is the name of the resource group that was used to deploy the virtual machine.

Verifying networking setup and status of the appliance

Procedure

1. To configure network settings for the CloudBoost appliance, see Configure Network Settings for a CloudBoost Appliance on page 49.
2. To verify the networking setup and see the status of the appliance, type 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:

<table>
<thead>
<tr>
<th>name</th>
<th>mode</th>
<th>address</th>
</tr>
</thead>
<tbody>
<tr>
<td>netmask</td>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>------</td>
<td>eth0</td>
<td>static 10.5.96.123</td>
</tr>
</tbody>
</table>

Network Routes:

<table>
<thead>
<tr>
<th>prefix</th>
<th>netmask</th>
<th>gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>0.0.0.0</td>
<td>10.5.96.1</td>
</tr>
</tbody>
</table>

DNS Configuration

DNS Servers: 10.8.192.91
Appliance status: Not yet registered
Domain name: domain name

3. To register and configure the CloudBoost appliance, see Register and Configure a New CloudBoost Appliance on page 55.

4. To configure NetWorker with the CloudBoost appliance, see Configure NetWorker with CloudBoost on page 63.
CHAPTER 5

Deploying the CloudBoost Appliance in Amazon EC2

This chapter includes the following topics.

- Deploying the CloudBoost appliance in Amazon EC2 ........................................ 46
- Verifying networking setup and status of the appliance ................................. 47
Deploying the CloudBoost appliance in Amazon EC2

Before you begin

Once EMC Licensing has made the Amazon machine image (AMI) for the CloudBoost appliance available to you, you can start the deployment.

Procedure

1. Log in to the AWS console.
2. Click EC2.
3. Under Images, perform the following steps:
   a. Select AMIs.
   b. Click Owned by me and open the drop-down.
   c. Select Private images.
   d. Find and launch the CloudBoost image.
4. Under Instance Type, choose an instance type that exceeds the following minimum requirements:
   - 4 CPUs
   - 6 GB of memory
   EMC recommends using the m4.xlarge.
5. Under Configure Instance Details, perform the following steps:
   a. Type the number of instances to create.
   b. Choose the network and submask.
   c. Enable Auto-assign Public IP.
6. Under Add Storage for the Root section:
   a. Set Size (GiB) to at least 41.
      The default size for the added volume is 40 GB. Increased the default size for the added volume based on a 1:2000 ratio. This storage is used for the metadata store.
   b. Add an EBS volume for metadata.
7. Under Tag Instance, define up to ten keys to assist with AMI management and identification.
8. Under Configure Security Group:
   a. To allow or deny public access, create or select from an existing security group which are a set of firewall rules.
   b. Consider the port requirements for the CloudBoost appliance.
9. Review information about the instance.
10. Select an existing key pair or create a new key pair to use when connecting to the CloudBoost appliance.
11. Click Launch instances.
12. Download the private key before you can connect.
Save the private key in a secure and accessible location as you will not be able to download the private key again after it is created.

The CloudBoost appliance is launched and running in Amazon EC2.

Verifying networking setup and status of the appliance

Procedure

1. To configure network settings for the CloudBoost appliance, see Configure Network Settings for a CloudBoost Appliance on page 49.
2. To verify the networking setup and see the status of the appliance, type 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
   0.0.0.0      address
   DNS Configuration
   DNS Servers: 10.8.192.91
   Appliance status: Not yet registered
   Domain name: domain name

3. To register and configure the CloudBoost appliance, see Register and Configure a New CloudBoost Appliance on page 55.
4. To configure NetWorker with the CloudBoost appliance, see Configure NetWorker with CloudBoost on page 63.
Deploying the CloudBoost Appliance in Amazon EC2
CHAPTER 6

Configure Network Settings for a CloudBoost Appliance

This section includes the following topics:

- About configuring network settings for a CloudBoost appliance .................. 50
- Configuring network settings for a CloudBoost appliance .......................... 50
About configuring network settings for a CloudBoost appliance

You must provide basic network settings information for a EMC 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.

Configuring network settings for a CloudBoost appliance

Procedure

1. Open a CLI window on the CloudBoost appliance. The procedures differ depending on where the CloudBoost appliance CLI is to be opened.

   Use the following table for instructions on how to open the CLI on different platforms.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere</td>
<td>In the vSphere client, right-click VM &gt; Open Console.</td>
</tr>
<tr>
<td>client</td>
<td></td>
</tr>
<tr>
<td>EC2</td>
<td>a. Log in to EC2, select the CloudBoost appliance, and then click <strong>Connect</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. In the <strong>Connect To Your Instance</strong> wizard, choose whether to connect with an SSH client or from the browser, and then follow the instructions.</td>
</tr>
<tr>
<td></td>
<td>c. In the SSH terminal, type the following command:</td>
</tr>
<tr>
<td></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td>ssh -i &quot;private key&quot; admin@AWS FQDN or IP</td>
</tr>
<tr>
<td></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td>where <strong>private key</strong> is the private key you used as the key pair when you installed your CloudBoost AMI.</td>
</tr>
<tr>
<td>Microsoft</td>
<td>a. Log in to Microsoft Azure, select, and open the CloudBoost appliance.</td>
</tr>
<tr>
<td>Azure</td>
<td>b. Connect to the CloudBoost appliance using either of the following methods:</td>
</tr>
<tr>
<td></td>
<td>• Use an SSH client</td>
</tr>
<tr>
<td></td>
<td>• Log in through a browser</td>
</tr>
</tbody>
</table>

Note

It is best practice to keep the DHCP configuration options supplied by Amazon.
The CloudBoost CLI appears.

Figure 5 CLI for CloudBoost

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
  ------- ----         -------
  eth0    dhcp    10.5.96.123
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. For CloudBoost 2.1, if the network interface card was not configured when the CloudBoost appliance was installed in the ESX server, run the following command to add a new virtual LAN on the appliance:

```
net create interface interface vlan vlan_id
```
6. To statically set the IP address and netmask, run these commands.
   If you have multiple networks, you must run this command for each network
   that is listed in the status command.
   - For CloudBoost 2.1:
     
     ```bash
     net config interface static IP address netmask netmask
     address
     ```
     
     For example,
     
     ```bash
     net config eth0 10.5.96.123 netmask 0.0.0.0
     ```
   - For CloudBoost 2.0:
     
     ```bash
     ip-address static <ip_address> netmask <netmask> gateway <gateway>
     ```
     
    7. For CloudBoost 2.1, manually add the gateway by running these commands.
   If you have multiple networks, you must also add multiple routes to the
   gateways.
   
   ```bash
   route add IP address netmask netmask address gw gateway address
   ```
   
   For example,
   
   ```bash
   route add 0.0.0.0 netmask 0.0.0.0 gw 10.5.96.1
   ```
   
    8. To manually set the DNS, type these commands:
   
   ```bash
   dns set primary primary IP address
   dns set secondary secondary IP address
   dns set tertiary tertiary IP address
   ```
   
   For example:
   
   ```bash
   dns set primary 10.5.96.91
   dns set secondary 10.5.96.92
   dns set tertiary 10.5.96.93
   ```
   
   9. To set the FQDN, type this command:

   ```bash
   fqdn servername.yourcompanydomain
   ```

   **Note**

   The FQDN must be in lowercase.
For example:

```
fqdn cloudbost.example.com
```  

10. To verify the networking setup and see the status of the appliance, type 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
    0.0.0.0         0.0.0.0         10.5.96.1
    default        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 by using the EMC Cloud Portal.

Note

Other commands are also available from the command line. To get help, type `help` or `?`. 
Configure Network Settings for a CloudBoost Appliance
CHAPTER 7

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.

- Creating and managing cloud profiles for CloudBoost ........................................ 56
- Validate cloud storage credentials ....................................................................... 57
- Registering a CloudBoost appliance ................................................................... 59
- Enable remote client mounting ........................................................................... 60
- Disable remote client mounting ........................................................................... 60
- Configuring a new CloudBoost appliance ........................................................... 60
Creating and managing cloud profiles for CloudBoost

The following topics describe how to create and manage cloud profiles for CloudBoost.

About cloud profiles

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

For Virustream deployments, consider the following:

- If the account was provisioned with Virtustream Storage Cloud by EMC Sales, the 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.

Note
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.

Creating a cloud profile

Before you begin
Obtain the necessary credentials for the cloud provider you intend to use.

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials that you created from the invitation.
   https://console.dpccloud.com
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 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 cloud provider.
   c. In the fields that appear for the selected cloud provider, provide the credentials and any additional information that is required to access this particular cloud object store.
   d. Click Save.

Results
The cloud profiles that are listed can be used by CloudBoost appliances.
Editing a cloud profile

Procedure

1. 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.

2. To delete an existing cloud profile, click Delete.
   A cloud profile that is used by an appliance cannot be deleted.

Validate cloud storage credentials

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 the CloudBoost appliance with a valid cloud storage provider.

Note

The quotation marks are required.

Procedure

1. Open a CLI window on the CloudBoost appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere client</td>
<td>In the vSphere client, right-click VM &gt; Open Console.</td>
</tr>
<tr>
<td>EC2</td>
<td>a. Log in to EC2, select the CloudBoost appliance, and then click Connect.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>c. In the SSH terminal, run this command,</td>
</tr>
<tr>
<td></td>
<td><code>ssh -i &quot;private key&quot; admin@AWS FQDN or IP</code></td>
</tr>
<tr>
<td></td>
<td>where private key is the private key you used as the key pair when you installed the CloudBoost AMI.</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>a. Log in to Microsoft Azure, select, and open the CloudBoost appliance.</td>
</tr>
<tr>
<td></td>
<td>b. Connect to the CloudBoost appliance using either of the following methods:</td>
</tr>
<tr>
<td></td>
<td>• Use an SSH client</td>
</tr>
<tr>
<td></td>
<td>• Log in through a browser</td>
</tr>
</tbody>
</table>
The CloudBoost CLI appears.

**Figure 6 CLI for CloudBoost**

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

```bash
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 that are listed as a result of Step 1, type this command:

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

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

**Note**

The quotation marks are required.

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=05832cb9d39a40af96aafdf4a4066a6f/A8581914817a4a8c264d --credential=fXPGEkxSCo9Zt6QHLtg05I/axjc= --endpoint=https://api.atmosonline.com 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.
- You must have accepted the invitation to create an account in the EMC Cloud Portal.

Procedure
1. Establish an SSH session to the IP address for the CloudBoost appliance:
   a. Log in with the username admin.
   b. Type the password that you set earlier.
2. Run this command:

   `register`

   If the host and DNS entries were not correctly updated between the CloudBoost appliance and the NetWorker server, the following error message appears:

   Registration failed, please try again. If registration fails again, contact the support staff

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 that you created from the invitation.
5. In the upper right-most corner of any portal page:
   a. Click (Services Menu).
   b. Click Register a CloudBoost Appliance.
6. In the Claim code field:
   a. Type the claim code.
   b. 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 77.

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 75.

Enable remote client mounting

When you enable 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 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
   ```

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. Type this command.

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

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 87. 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 the invitation:
   https://console.dpccloud.com
2. Click **Cloud Portal**, and then click **CloudBoost**.
3. In the left menu, click **Appliances**.
   The **Appliances** page opens.

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 77.

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, type the display name in the **Name** field.
7. In the **Cloud Profile** field, select one of the cloud profiles that was previously set up.

   **Note**

   The **Cloud Profile** field cannot be changed after initial configuration.

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

   **Note**

   This cannot be changed after initial configuration.
9. To use a CA-signed certificate:
   a. Select **Provide a CA-signed certificate**.
   b. Select a PKCS12 certificate file to upload.
      CA-signed certificate information must be provided in lowercase.
   c. If required, provide the key file password.

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

10. To minimize clock drift:
    a. Select **Enable NTP** checkbox.
    b. Type the hostname 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:
    a. Select **Enable backup encryption with asymmetric keys**.
    b. Refer to the displayed instructions to help you create the private and public encryption keys. This is the only method of asymmetric key creation that is supported for the CloudBoost appliance.
    c. Copy the entire public key from the resulting output file and paste it into the text box below the instructions on the **Configure** tab.
    d. 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 the private key and pass phrase. They must be provided to decrypt a recovered backup. Appliances that are backed up using the public key that is provided on the Configure tab cannot be recovered without the private key and pass phrase.

13. Review the selections and click **Update Configuration** to save these settings for the appliance.

**Results**
The appliance is configured and a backup immediately begins.
CHAPTER 8

Configure NetWorker with CloudBoost

This chapter applies to configuring NetWorker with a CloudBoost appliance using backup to cloud. Cloud-based data protection occurs over a TCP/IP network.

You can compress and encrypt the data. It is recommended that you install the NetWorker Storage Node on a separate Linux server, and not use the NetWorker Storage Node on the CloudBoost appliance.

- Creating a CloudBoost Device.................................................................64
- Adding a NetWorker Storage Node to back up multiple Windows hosts......66
- Troubleshooting CloudBoost device configuration issues........................73
- Report information on cloud backup.........................................................73
Creating a CloudBoost Device

Perform the following steps to configure a CloudBoost device to receive backup or clone data.

You do not require a storage node when backing up Linux hosts by using Client Direct.

Procedure

1. If not already configured, enable remote client mounting on the CloudBoost appliance, and define a password for the `remotebackup` user account:
   a. Connect to the CloudBoost appliance with the admin account.
   b. Type the following command:

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

   where `password` is the new password for the `remotebackup` user.

2. Log in to the NMC GUI as an administrator of the NetWorker server.
3. Click the Enterprise button 🌐 on the taskbar.
4. Highlight a host in the navigation tree:
   a. Right-click NetWorker.
   b. Select Launch Application. The NetWorker Administration window appears.
5. Click the Devices button 🌐 on the taskbar.
6. In the expanded left navigation pane:
   a. Right-click CloudBoost Appliances.
   b. Select New Device Wizard.
7. On the Select the Device Type window, select CloudBoost, and then click Next.
8. Review the CloudBoost Preconfiguration Checklist window, and then click Next.
9. On the CloudBoost Configuration Options window, perform the following tasks:
   a. In the CloudBoost appliance group box, select one of the following options:
      - To use a CloudBoost appliance that you have previously configured on the NetWorker server, select Use an existing CloudBoost appliance.
      - To create a CloudBoost appliance, select Create a new CloudBoost appliance and specify a descriptive name.
   b. In Hostname (FQDN) field, specify the Fully Qualified Domain Name (FQDN) of the CloudBoost appliance.
   c. In the Username field, type remotebackup.
   d. In the Password field, type the password for the `remotebackup` account, which you defined on the CloudBoost appliance by using the `remote-mount` command.
e. In the **Configuration Method** group box, select the file system on the CloudBoost appliance that NetWorker uses as the target data device:

   a. Select **Browse & Select**.
   
   b. Create a folder in the `/mnt/magfs/base` directory. For example: `/mnt/magfs/base/CBO1`
   
   c. Select the folder that you just created.

   NetWorker validates the CloudBoost username and password that you specified.

10. Click **Next**.

11. Create the NetWorker device on the CloudBoost appliance:

   - Ensure that the storage path that you specify exists in a subfolder in the `/mnt/magfs/base` directory with write access enabled.
   
   - Use the **New Folder** option to create a device folder.

   NetWorker updates the **NetWorker Device Name** and **Storage Path** fields with the information.

12. Click **Next**.

13. In the **CloudBoost Pool Configuration** window, perform the following steps:

   a. Leave the **Configure Media Pools for devices** option enabled.
   
   b. In the **Devices** table, select the NetWorker device for the CloudBoost appliance.
   
   c. In the **Pool Type** box, depending on the use case, select one of the following:
      
      - **Backup**
      - **Backup Clone**
   
   d. In the **Pool** box:
      
      - To use a new pool, select **Create and use a new Pool** and then specify a pool name.
      - To use an existing pool, select **Use an existing Pool** and choose a pool that contains at least one CloudBoost device.

   **Note**

   The pool that you select cannot contain other device types such as AFTD and DD Boost devices.

14. Click **Next**.

15. In the **Review the Device Configuration** page:

   a. Review the settings.
   
   b. Click **Configure**.

16. In the **Check results** page:

   a. Review whether the devices were successfully completed or any messages.
Adding a NetWorker Storage Node to back up multiple Windows hosts

Use the following procedures to offload resource-intensive activities from the CloudBoost appliance when backing up several Windows hosts.

You must configure a Linux storage node host to manage the CloudBoost backup activities.

Procedure

1. Ensure that the storage node software and required enabler codes have been installed on the host.
2. In the NetWorker server Administration interface, click the Devices view.
3. From the navigation tree, right-click Storage Nodes, and select New.

The Create Storage Node window appears, with the General tab displayed.

4. Set the Identity attributes:
   a. In Name, specify the hostname of the NetWorker storage node.
   b. In Type of Storage Node, select SCSI.
5. In the Status attributes, review or set the storage node status:
   a. Storage node is configured indicates whether a device has already been configured on this storage node.
   b. Enabled indicates whether the storage node is available for use.
Configure NetWorker with CloudBoost

6. Set the Device Management attributes:
   a. In Max active devices, set the maximum number of devices that NetWorker may use from this storage node in a DDS environment.
   b. In AFTD allowed directories, for AFTD devices, type the pathnames of directories on the storage host where AFTDs are allowed to be created.
   c. In mmds for disabled devices, select a nsrmmd (data mover) option:
      - To start nsrmmd processes for disabled devices, select Yes.
      - To not start nsrmmd processes for disabled devices, select No.
   d. In Dynamic nsrmmds, for AFTD or DD Boost devices, select whether nsrmmd processes on the storage node devices are started dynamically.
      - Selected (Dynamic mode): NetWorker starts one nsrmmd process per device and adds more only on demand, for example, when a device's Target sessions is reached.
      - Unselected (Static mode): NetWorker runs all available nsrmmd processes.
      In environments where unattended firewall ports must be restricted for security reasons, the storage node settings for mmds for disabled devices and Dynamic nsrmmds unselected (static mode) offer more control because they cause all available nsrmmd firewall ports to be attended by running nsrmmd processes.

7. Select the Configuration tab.

8. In Scanning, set the attributes for SCSI library target devices on this storage node:
   a. In Device Sharing Mode, select an option:
      - Server Default uses the NetWorker server setting for device sharing.
      - Maximal Sharing allows sharing of all devices.
      - No Sharing disables device sharing.
   b. In Search all LUNs, select an option:
      - For NetWorker to detect all LUNs (logical unit numbers), select Yes. Detection can be time consuming.
      - For NetWorker to stop searching at the first available LUN, select No (the default).
   c. In Use persistent names, choose whether NetWorker uses persistent device names specific to the storage host operating system when performing device discovery and autoconfiguration operations.
   d. In Skip SCSI targets field:
      - If the storage node type is set to SCSI, list any SCSI targets to exclude from backup operations, one per line.
• The format is bus.target.lun where the target and LUN fields are optional.
• You can exclude a maximum of 63 targets.

9. For AFTD or DD Boost devices, configure the following settings in **Advanced Devices**:
   • In **Server network interface**, type the unique network interface hostname of the NetWorker server to be used by the storage nodes.
   • In **Clone storage nodes**, list by priority the hostnames of the storage nodes to be used for the save or “write source” side of clone operations originating from this storage node as the “read source.” The clone operation selects the first storage node in this list that has an enabled device and a functional nsrmmd process.
     - If the **Clone storage nodes** attribute does not contain a value, then the device operations use the value that is defined in the **Clone storage nodes** attribute for the Storage Node resource that was created for the NetWorker server.
     - If the **Clone storage nodes** attribute for the storage node resource is empty, then device operations use the values that are defined in **Storage nodes** attribute for the client resource that was created for the NetWorker server.

In backup-to-disk environments, it is possible for a single backup volume to be shared by multiple storage devices on different storage nodes. This can result in an ambiguous clone write source.

10. Click **OK**.

### Configuring a CloudBoost device on an external storage node

The procedures for configuring a device by using an external storage node for the CloudBoost appliance differ depending on the installed NetWorker software version.

**NetWorker 9.1: Configuring a device by using an external storage node for CloudBoost**

**Procedure**

1. Log in to the NMC GUI as an administrator of the NetWorker server.
2. Click the **Enterprise** button on the taskbar.
3. Highlight a host in the navigation tree:
   a. Right-click **NetWorker**.
   b. Select **Launch Application**. The **NetWorker Administration** window appears.
4. Click the **Devices** button on the taskbar.
5. Expand **Devices** in the left navigation pane:
   a. Right-click the CloudBoost device.
   b. Select **New Device Wizard**.
   The **Device Configuration Wizard** window appears.
6. On the **Select the Device Type** window:
   a. Select **CloudBoost**.
b. Click Next.

7. Review the CloudBoost Preconfiguration Checklist window, and then click Next.

8. On the CloudBoost Configuration Options window, perform the following tasks:

**Figure 8 Device Configuration Wizard: CloudBoost Configuration Options**

a. In the CloudBoost Storage group box:
   a. Select Use External Storage Node.
   b. Select an external storage node.

b. In the CloudBoost Appliance group box, select one of the following options:
   - To use a CloudBoost appliance that you have previously configured on the NetWorker server, select **Use an existing CloudBoost appliance**.
   - To create a CloudBoost appliance, select **Create a new CloudBoost appliance** and specify a descriptive name.

c. In **Hostname (FQDN)** field, specify the Fully Qualified Domain Name (FQDN) of the CloudBoost appliance.

d. In the **Username** field, type `remotebackup`.

e. In the **Password** field, type the password for the `remotebackup` account, which you defined on the CloudBoost appliance by using the `remote-mount` command.

f. In the **Configuration Method** group box, select **Browse & Select**.

The Browse and Select the CloudBoost Device Path window appears.
9. In the **Browse and Select the CloudBoost Device Path** window, select the file system on the CloudBoost appliance that NetWorker uses as the target data device.

   a. Select **New Folder**.

   b. Create a folder in the `/mnt/magfs/base` directory. 

      For example: `/mnt/magfs/base/CBO1`

   c. Select the folder that you just created.

   d. Ensure that the storage path that you specify exists in a subfolder in the `/mnt/magfs/base` directory with write access enabled.

      NetWorker updates the **NetWorker Device Name** and **Storage Path** fields with the required information.

**Figure 9 Device Configuration Wizard: Browse and Select the CloudBoost Device Path**

10. Click **Next**.

11. On the **Configure the CloudBoost Pool** page, perform the following steps:
Figure 10 Device Configuration Wizard: Configure the CloudBoost Pool

a. Leave the **Configure Media Pools for devices** option enabled.

b. In the **Devices** table, select the NetWorker device for the CloudBoost appliance.

c. In the **Pool Type** box, depending on the deployment, select either of the following:
   - Backup
   - Backup Clone

d. In the **Pool** box perform either of the following steps:
   - To use a new pool, select **Create and use a new Pool** and specify a pool name.
   - To use an existing pool, select **Use an existing Pool** and select a pool that contains at least one CloudBoost device.

**Note**

The pool that you select cannot contain other device types such as AFTD and DD Boost devices.

e. Leave the **Label and Mount device after creation** option enabled.

f. Click **Next**.

12. Review the configuration settings and click **Next**.

13. Check and verify that the device configuration was successful in the **Check Results** window.
NetWorker 9.0.1: Configuring a device by using an external storage node for CloudBoost

**Procedure**

1. Click the **Devices** button on the taskbar.
2. Expand **Devices** in the left navigation pane:
   a. Right-click the CloudBoost device.
   b. Select **Copy**.

   The **Create Device** window appears.
3. In the **Create Device** window, perform the following steps:
   a. In the **Name** field:
      a. Specify the hostname of the new storage node.
      b. Specify a new device path in the following format:
         ```
         rd=hostname:device_path
         ```
         For example, `rd=nwsn01.emc.com:ms_server_backups`
   b. For the **Device access information** field:
      a. Specify the hostname of the CloudBoost appliance.
      b. Specify the device path that you specified in the **Name** field in the following format:
         ```
         hostname:device_path
         ```
         For example, `cb01.emc.com:ms_server_backups`
   c. Click **OK**.

   **Note**
   During device creation, the NetWorker software automatically creates the device path on the CloudBoost appliance.
4. Right-click the device and select **Label**.
   The **Label** window appears.
a. Select a pool from the Pool list.
b. Click OK.

Troubleshooting CloudBoost device configuration issues

This section provides information about the error messages that might appear when you configure a NetWorker device for the CloudBoost appliance.

Cannot retrieve the version of the CloudBoost appliance

This error message appears when the NetWorker server cannot determine the version of NetWorker running on the CloudBoost appliance. To resolve this issue, contact EMC Support for access to the CLI and ensure that:

- The NetWorker daemon nsrexed is started on the appliance. Log in to an SSH terminal with the maginatics user account and type `ps -ef | grep nsr`. Confirm that the nsrexed process appears. If the nsrexed daemon does not appear, type `sudo service networker start` to start the nsrexed process on the appliance.
- Forward and reverse name resolution is correctly configured for the CloudBoost appliance and the NetWorker server host.

The selected CloudBoost appliance is unsupported for device type "CloudBoost"

The host and DNS entries were not updated between the CloudBoost appliance and the NetWorker server.

Directory not found

This error appears when the NetWorker server cannot access the file system on the CloudBoost appliance. To resolve this issue, ensure that the `/mnt/magfs` folder exists on the CloudBoost appliance and is mounted.

Unable to connect to the CloudBoost appliance: LOGON_FAILURE error

This error appears in the following scenarios:

- The password specified for the remotebackup user is not correct.
- The remotebackup user does not exist on the CloudBoost appliance.
- The user credentials that were specified for the NetWorker device are not the same credentials that were used to register the CloudBoost appliance.

Report information on cloud backup

Use cloud backup information to monitor backup costs and help optimize your cloud backups.

Cloud backup information can be obtained from the following sources:

- Cloud backup and recover reports in NMC.
- The `mminfo` command
  Use the `mminfo -avot` command to get information on how much data is consumed in a cloud backup. The *EMC NetWorker Command Reference Guide* and
the UNIX man pages provide more information about how to use the mminfo command.
CHAPTER 9

Monitor, Manage, and Support CloudBoost

This section includes the following topics:

- About monitoring CloudBoost ................................................................. 76
- CloudBoost reporting ........................................................................... 76
- Upgrading a CloudBoost appliance ....................................................... 77
- CloudBoost integration with EMC Secure Remote Services ............... 78
- Registering CloudBoost with EMC Secure Remote Services .............. 78
- Increasing the CloudBoost appliance site cache .................................. 79
- Changing log levels for CloudBoost debugging ..................................... 80
- Restarting a CloudBoost appliance ....................................................... 80
- Recovering a CloudBoost appliance .................................................... 81
- Deleting a CloudBoost appliance ......................................................... 84
About monitoring CloudBoost

You can review 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 need to manually monitor the health, collect and review logs, and contact EMC Support.

CloudBoost reporting

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

Appliances
To view the list of appliances, its status and available upgrades, sign in to the EMC Cloud Portal and click Cloud Portal > CloudBoost > Appliances.

To filter the list of appliances, type a portion of the name of the appliance or appliances you want to see.

Figure 12 Appliances page

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

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

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

**History**

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

**Storage Use History**

**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 that is used over the course of days, weeks, months, or years.

---

**Upgrading a CloudBoost appliance**

You can upgrade CloudBoost appliance software within the EMC Cloud Portal. During the installation, the CloudBoost appliance is 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 the invitation:
   ```
   https://console.dpccloud.com
   ```
2. Click **Cloud Portal**, and then click **CloudBoost**.
3. Select the appliance to upgrade.
4. On the **Overview** tab, click **Choose Upgrade** under the **About** section.
5. Select the version to upgrade to, and then click **Start Upgrade**.

![Figure 13 Upgrade Window](image)

6. Review the warning message, then click **Confirm**.

   The **Appliances** page appears.

7. Monitor the progress of the upgrade.
Results
After the upgrade is complete, view the upgrade history under the History section.

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.

About registering ESRS

When registered with your ESRS gateway, the CloudBoost appliance continuously communicates with ESRS, sending it status information and reports on a schedule. 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.

Auditing
You can audit EMC remote support activity, including the date and time of remote sessions, the ticket number, the EMC technician, and more.

Registering
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.

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.

About installing the ESRS gateway

You can install the EMC Secure Remote Services gateway version 3.6.0 or later in a VM separate from the CloudBoost appliance. After the 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_EMCCloudBoost](https://support.emc.com/products/37716_EMCCloudBoost)
- [https://support.emc.com/products/37716_EMCCloudBoostTopics/pg58757/](https://support.emc.com/products/37716_EMCCloudBoostTopics/pg58757/)

Note
When you install the ESRS gateway, make note of the IP address or URL and the serial number. You 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 the CloudBoost appliance with ESRS, see Registering CloudBoost with EMC Secure Remote Services on page 78.

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 78.

**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 18.

**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. Type 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.

**Note**

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 that is collected for their use in troubleshooting.

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 the invitation:
   
   ![https://console.dpccloud.com](https://console.dpccloud.com)

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 improve performance.

### Restarting a CloudBoost appliance

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

You may restart an appliance within the EMC Cloud Portal or at the CLI.
Procedure
1. If the CloudBoost appliance that 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 appliance, and then click Commands.
   d. Select Reboot Appliance.
2. If you cannot restart the appliance 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. Type 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.

Preparing to recover the CloudBoost appliance

Procedure
1. Ensure that the recovery target appliance is running the same version of the CloudBoost software that the failed appliance was running.
2. If required, upgrade the target appliance 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 77.

   Note

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

3. If a CloudBoost appliance fails, you must deploy a second CloudBoost appliance to restore the metadata from backups that are 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.

4. The recovery process requires the backup metadata to be restored to the newly deployed CloudBoost appliance.
5. For testing purposes, you can force recovery for an active appliance.
Performing a recovery of the CloudBoost appliance

Procedure

1. Use a web browser to sign in to the EMC Cloud Portal with the credentials you created from the invitation:
   https://console.dpccloud.com

2. Click Cloud Portal, and then click CloudBoost.

3. On the Appliances page, verify that an unconfigured appliance is available to recover the failed appliance to.

   Figure 14 New, unconfigured appliance

4. Verify that the unconfigured appliance is running the same version as the failed appliance. Upgrade if necessary.

5. Recover the failed appliance.

   a. Find the inactive appliance on the Appliances page.

   Figure 15 Appliance to recover

   The Recover tab opens.
6. If the appliance being recovered had been configured to use asymmetric encryption, provide the private key that is required to decrypt the backed up data.

   If a pass phrase was created to use with the private key, type that pass phrase.

7. Select the CloudBoost appliance to be used as the recovery target.

   Consider the following:
   
   • Ensure that the recovery target appliance is running the same version of the CloudBoost software as the appliance being recovered.
   
   • Use the same IP and hostname so that the NetWorker software can find the device.

   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**.

9. If the recovered appliance used asymmetric encryption, you can rotate the encryption keys:

   a. Open the **Configure** tab for the recovered appliance.
   
   b. Enable backup encryption with asymmetric keys.
   
   c. Create the public and private keys.

   For more information, see **Configuring a new CloudBoost appliance** on page 60.
Deleting a CloudBoost appliance

You can delete an appliance so that it can be deployed once again, as if it were a new EMC CloudBoost 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, and the Recover and Delete buttons appear for that appliance. When you select such an appliance, the status at the top of the appliance detail page is Down.

Figure 17 Down appliance

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 delete it.

Procedure

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere client</td>
<td>In the vSphere client, right-click VM &gt; Open Console.</td>
</tr>
<tr>
<td>EC2</td>
<td>a. Log in to EC2, select the CloudBoost appliance, and then click Connect.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>c. In the SSH terminal, run this command,</td>
</tr>
<tr>
<td></td>
<td><code>ssh -i &quot;private key&quot; admin@AWS FQDN or IP</code></td>
</tr>
<tr>
<td></td>
<td>where <code>private key</code> is the private key you used as the key pair when you installed your CloudBoost AMI.</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>a. Log in to Microsoft Azure, select, and open the CloudBoost appliance.</td>
</tr>
<tr>
<td></td>
<td>b. Connect to the CloudBoost appliance using either of the following methods:</td>
</tr>
</tbody>
</table>
|              |   • Use an SSH client
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Log in through a browser</td>
</tr>
</tbody>
</table>

The CloudBoost CLI appears.

**Figure 18** CLI for CloudBoost

3. To delete all the data in the cloud, run this command:
   
   `destroy-appliance`

4. To perform a factory reset, 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.

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.
Monitor, Manage, and Support 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 EMC 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**...............................................................................88
- **Converting a PEM file to PKCS #12**.................................................................89
- **Verifying your certificate**...................................................................................90
- **Manage the SSL certificate for an appliance**......................................................90
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 deployments of EMC CloudBoost.

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. Open a Linux terminal.
2. Run the following 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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>foo.com.chain.pem</td>
<td>is the concatenation of the intermediate certificate (root is the last)</td>
</tr>
<tr>
<td>foo.com.pem</td>
<td>is the *.foo.com certificate</td>
</tr>
<tr>
<td>foo.com.key</td>
<td>is the private key for the above certificate</td>
</tr>
<tr>
<td>passphrase.txt</td>
<td>contains the pass phrase to use for the .p12 file</td>
</tr>
</tbody>
</table>

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](http://www.openssl.org/docs/apps/verify.html).

Procedure

1. Open a Linux terminal.
2. Run the following command and replace host.crt with the appropriate certificate filename:

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

Manage the SSL certificate for an 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, use a 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, update the SSL certificate.

Procedure

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

   https://console.dpccloud.com

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use the default self-signed certificate</strong></td>
<td>This is selected by default. This is acceptable in test environments, but should not be used in a production environment.</td>
</tr>
<tr>
<td><strong>Provide a CA-signed certificate</strong></td>
<td>Upload a CA-signed wildcard certificate in the form of a .p12 or .pfx file and if necessary, type the key file password.</td>
</tr>
</tbody>
</table>

**Note**

CA certificate information must be provided in lowercase.

5. Click **Update Configuration**.
CHAPTER 11

Common Cloud Portal Tasks

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

- Resetting your personal Cloud Portal password at sign-in .................. 94
- Editing your personal Cloud Portal account profile ............................ 94
- Manage Cloud Portal users ............................................................... 94
- Changing the event notification settings in the Cloud Portal ................. 99
- Events history in the Cloud Portal .................................................... 100
- Getting help inside the Cloud Portal .................................................. 100
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 EMC Cloud 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 Cloud Portal, select **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 95.
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 97.

Delete a User
You can delete one or more user accounts with the User Management function in the Cloud 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 98.

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 a 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.
3. Click Invite Users.

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

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.

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.
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 95 or Deleting a Cloud Portal account invitation on page 97.

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 97.
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 95 or Resending a Cloud Portal account invitation on page 96.
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.
3. Click **Users**, and then in the User email list, select the email address of the user account you want to edit.
   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 95 or Deleting a Cloud Portal user account on page 98.
4. Click **Edit User**.

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.

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

### Reseting a Cloud Portal user account password

As a EMC 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**.

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.

   **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 95 or *Deleting a Cloud Portal user account* on page 98.

4. Click **Edit User**.

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 98.

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 95 and Editing a Cloud Portal user account on page 97.

4. Delete the user account using either of two methods.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click Delete User.</td>
<td>Use this method to delete the user account directly from the View Users page.</td>
</tr>
<tr>
<td>Click Edit User &gt; &gt; Delete User.</td>
<td>Use this method to delete the user account if you decide to do so while in the Edit User mode.</td>
</tr>
</tbody>
</table>

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

Changing the event notification settings in the Cloud Portal

You can configure the 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>
<thead>
<tr>
<th>Table 10 How events are prioritized in Events History</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5 (no icon)</td>
</tr>
</tbody>
</table>

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 the 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 19** 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) 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 EMC 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.