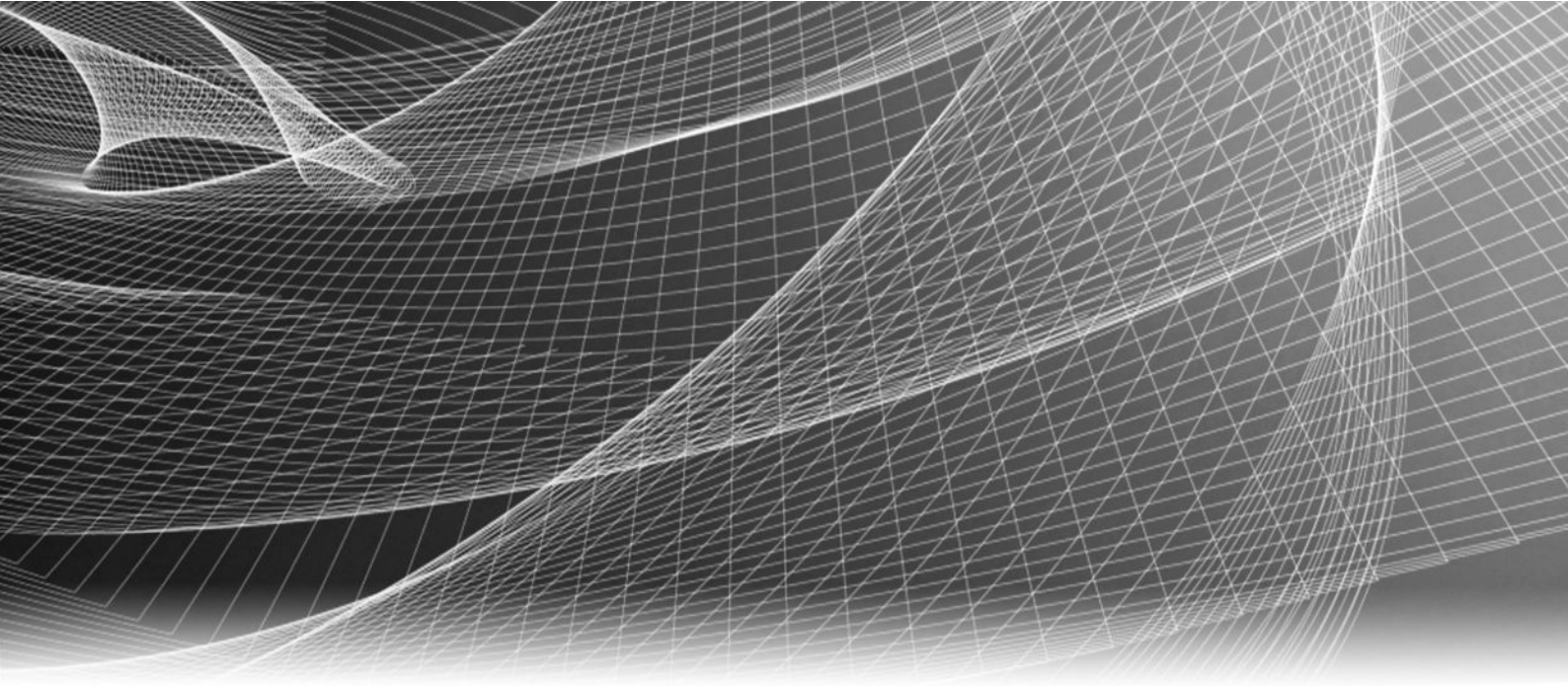

EMC® NetWorker with EMC® CloudBoost

Version 1.0.1

Integration Guide

P/N 302-001-736

REV 02

EMC²

Published April, 2015

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

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

CONTENTS

TABLES

Preface

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 (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This document describes the integration of NetWorker with CloudBoost.

Audience

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

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	March 11, 2015	Initial release of EMC CloudBoost 1.0
02	April 13, 2015	Updated for the release of EMC CloudBoost 1.0.1. In Solution requirements on page 14, changed the labels of several cloud storage providers to reflect changes made on the Cloud Storage Profile page of the CloudBoost management console. Added Preface to enable inclusion of this revision history.

Related documentation

The CloudBoost documentation set includes the following publications.

- *EMC CloudBoost Release Notes*
  Contains information about new features and changes, fixed problems, known limitations, environment and system requirements for the latest CloudBoost release.

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

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

Where to get 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. You will see several options for contacting EMC Technical Support. 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

Visit 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.

CHAPTER 1

Introduction to NetWorker with CloudBoost

This chapter contains the following topics:

NetWorker with CloudBoost

NetWorker with CloudBoost enables long term storage provisioning via the cloud.

NetWorker sends a backup clone to the CloudBoost virtual appliance. The CloudBoost virtual appliance translates these into generic objects which are sent to an object store, which can be public, private, or hybrid. The CloudBoost virtual appliance presents itself as a NetWorker Advanced File Type Device. The enabled workflow is a clone operation to the cloud; it is not a backup to the cloud. With this low cost tape replacement solution, each CloudBoost virtual appliance can support up to 400 TB of addressable back end storage.

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

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

System architecture and components

The CloudBoost virtual appliance is deployed as a single virtual machine (VM) comprised of these core components.

- The 8.2.1 versions of the NetWorker Storage Node and Advanced File type Device are pre-installed on the Cloudboost VM as the primary transport mechanism for cloning backups from local NetWorker targets to Cloudboost.
- The *management server* is a monitoring component for collecting instantaneous and historical statistics. It also provides a web-based console for system management.
- The *discovery service* allows the CloudBoost clients to locate and access the shares and learn the IP address of the metadata Server exporting them.

CloudBoost sizing and performance considerations

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

CloudBoost sizing

The CloudBoost virtual appliance requires 750 GB of internal capacity for storing CloudBoost metadata. SSDs are recommended for optimal performance. Additionally, the virtual appliance requires a single 4-core CPU with minimum 16 GB of memory (32 GB of memory recommended).

De-duplication and cloud capacity

A CloudBoost virtual appliance supports up to 400 TB of addressable back-end capacity in object storage. This is the total amount of unique capacity in the object store after de-duplication. Based on preliminary test data, CloudBoost expects to achieve a 2x–4x range of de-duplication. Backups of file systems, applications, and databases where file sizes are typically small are expected to achieve close to 2x de-duplication on average. Backups of virtual machines where typical virtual disks sizes are larger could see up to 4x de-duplication. Based on this range of de-duplication, each CloudBoost virtual appliance

can support 800 TB–1.6 PB of logical client capacity. That said, proof of concept testing, or testing with up-to-date, real data is recommended.

End-to-end bottlenecks

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

Minimum WAN requirements

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

Multiple clone sessions

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

CHAPTER 2

Provision and Deploy the CloudBoost Virtual Appliance

This chapter contains the following topics:

Solution requirements

Requirements for CloudBoost.

Table 2 Supported public clouds

Cloud provider	Information required by CloudBoost
Amazon Web Services (S3)	Storage Region, Amazon Web Access Key ID, AWS Secret Access Key
AT&T Synaptic Storage	Synaptic Subtenant ID, AT&T User ID, Synaptic Secret Key
EMC Elastic Cloud Storage Service	Access Key ID, Secret Access Key
Google Cloud Storage	Access Key, Secret
Microsoft Azure Storage	Azure Account Name, Azure API Key

Table 3 Supported private clouds

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

Supported server versions

- NetWorker Server 8.1.x, 8.2.x

For supported clients, see the Software Compatibility Guides at http://compatabilityguide.emc.com:8080/CompGuideApp/.

Hardware

- 750 GB SSD
- 4-core CPU
- 16 GB of memory

WAN

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

Pre-installation requirements

Perform these tasks before you install CloudBoost for NetWorker.

- Obtain the necessary credentials for your cloud storage profile, such as the endpoint URL, the token ID or access key, and the secret key.

- Obtain the blobstore validator and the supporting `.JAR` file. Run nslookup to validate name resolution and the blobstore validator to validate the cloud credentials.
- Obtain the CloudBoost storage node `.OVA`.
- Determine the fully qualified domain name of the CloudBoost management server.
- Obtain a static IP address for the CloudBoost management server, and determine the subnet mask, the gateway, and the forward and reverse DNS servers.
- Register the CloudBoost hostname/IP address in DNS. The hostname/IP address must be statically registered in DNS regardless of any mappings created by DHCP. Failure to do this may result in indeterministic service unavailability and downtime.
- Open the necessary ports. For more information, see Port access restrictions on page 15.
- Plan and prepare your SSL Certificate usage for testing and production environments. For more information, see Manage SSL Certificates on page 41.

Firewall port requirements

As with all networked software solutions, adhering to best practices for security is encouraged to protect your deployment.

Table 4 Firewall port requirements

From	To	TCP Port	Description
Administrator workstation	CloudBoost storage node	22	SSH for maintenance and troubleshooting
CloudBoost storage node	Cloud storage (public or private)	443	HTTPS to access object store (if supported)
Administrator workstation	CloudBoost storage node	4444	HTTPS/HTTP to CloudBoost management console/API
NetWorker server	CloudBoost storage node	7937	NetWorker client service daemon (nsrexecd)
NetWorker server	CloudBoost storage node	7938	NetWorker port mapper
CloudBoost storage node	site cache servers	8443	Site cache

For more information about NetWorker firewall ports, refer to the documentation for NetWorker.

Provision the CloudBoost virtual appliance on vSphere

Before you can install the CloudBoost virtual appliance, you must ensure proper integration with the DHCP, DNS, and Active Directory.

- Obtain a static IP address for the CloudBoost server, and determine the subnet mask and the gateway.
- Register the CloudBoost hostname/IP address in DNS.

- If necessary for integration with Active Directory, create a new username in the domain for the CloudBoost administrator, register a Service Principal Name (SPN) for it, and generate a keytab file for that SPN.

Note

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

Installing the CloudBoost virtual appliance

Install the CloudBoost virtual appliance in vSphere.

Before you begin

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

Procedure

1. In the vSphere client, click **File** › **Deploy OVF Template**, browse to the location of the OVA package, and then click **Next**.
2. Select the **Inventory Location** (the ESX cluster and host that will run the VM), and then enter 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.
4. On the **Ready to Complete** page of the wizard, review the deployment settings.
5. Select the **Power on after deployment checkbox**, and then click **Finish**.
6. To ensure that the CloudBoost virtual appliance has 16 GB of memory reserved, right click on the VM and click **Edit Settings**.
   a. On the **Resources** tab, click **Memory** and ensure that **Reservation** is set to `16384 MB`, and then click **OK.**

Results

The CloudBoost virtual appliance is installed

After you finish

You must use the CLI to initially configure the VM before you can start it and complete the CloudBoost deployment.

Configuring the CloudBoost virtual appliance

After the CloudBoost virtual appliance is installed, you must initially configure it before you can use its management console to complete the deployment.

You must configure the IP settings and hostname for CloudBoost from the VM console in the vSphere client.

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

Note

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

After the CloudBoost virtual appliance has the correct IP address (either via DHCP or manual configuration), you must configure its Fully Qualified Domain Name (FQDN), such as **`example.company.com`**. The FQDN must be registered in your DNS with both forward and reverse domain name resolutions. You can then create shares within that FQDN, for example at `\\example.company.com\sales`.

Note

This is required for the CloudBoost virtual appliance to work properly and must be configured exactly as the DNS name for this VM.

You must also change the default password for the CloudBoost management console to one of your own choosing.

Procedure

1. In the vSphere client, right-click **VM › Open Console**.
2. To manually set a static IP address and DNS, run this command.

   ```
   $ ip-address static <Address> netmask <Netmask> gateway <Gateway>
   ```

3. To configure DNS, run these commands.

   ```
   $ dns set primary <IP address>
   $ dns set secondary <IP address>
   $ dns set tertiary <IP address>
   ```

4. To configure the FQDN, run this command.

   ```
   $ fqdn <servername.yourcompanydomain>
   ```

   For example: `$ fqdn example.example.com`

5. To change the default as-installed password for the management console, run this command, where the value for *‹current_password›* is **`password`**.

   ```
   $ password <current_password> <new_password>
   ```

   For example: `$ password password P@ssword123`

6. To verify the configuration, run this command.

   ```
   $ status
   ```

Results

After you have verified the system's basic IP configuration, you can deploy the CloudBoost virtual appliance using a Web browser.

Note

Other troubleshooting commands (such as diagnostics nslookup, diagnostics ping) are also available from the command line. To get help, type **`$ help`** or **`$ ?`**.

Deploying the CloudBoost virtual appliance

After you configure the CloudBoost virtual appliance at the vSphere CLI, you can log in to the CloudBoost management console to configure its deployment settings.

Before you begin

- Configure the CloudBoost virtual appliance. For more information, see Configuring the CloudBoost virtual appliance on page 16.
- Understand SSL Certificate management for CloudBoost. For more information, see Manage SSL Certificates for the CloudBoost Virtual Appliance on page 41.

Procedure

1. Use a Web browser to log in to the Cloudboost virtual appliance at `https://<FQDN>:4444`, where *‹FQDN›* is the fully qualified domain name specified at the vSphere CLI with the default username, **`local\admin`**, and the password specified during initial configuration.

   If a password was not specified at the vSphere CLI during initial configuration, the default password is **`password`**. You must immediately change this default password.

2. Click **Get Started**, and on the License Agreement page, click **I Agree**.

   The Deployment page opens.

3. Review the network and host settings you defined at the vSphere CLI.

   For more information, see Configuring the CloudBoost virtual appliance on page 16.

4. In the **Deployment Type** field, select **Standard Deployment**, and then click **Save and Continue**.

5. On the **Licenses** page click **New License**, paste the key you've been given into the **Add a License** text box, click **Add**, and then click **Save and Continue**.

   The Outbound HTTP Proxy page opens.

6. If an HTTP proxy must be used to reach the cloud storage service from the VM, select the **Enable Outbound HTTP Proxy** checkbox, enter the hostname and port in the **HTTP Proxy hostname and port** fields, and then click **Save and Continue**.

   The Cloud Storage Profile page opens.

7. Click **New Profile**, provide the required information for this cloud storage profile, click **Add**, and then click **Save and Continue**.

   While you may select **EMC object store**, it may not be available yet. Your EMC pre-sales professional services representative can help you learn more about this.

   The System Backup and Restore page opens.

8. Select the cloud profile to which the CloudBoost virtual appliance will be backed up.

   a. To specify a container, click **advanced settings**, then type the name of an existing container in the **Container for the backup files** field.

   b. Click **Save and Continue**.

   The SSL Certificates page opens.

9. Provide your SSL certificate information, and then click **Save and Continue**.

   The NTP (Network Time Protocol) page opens.

10. To minimize clock drift, select the **Enable NTP** checkbox, enter the FQDN or IP address for at least one NTP server, and then click **Save and Continue**.

    It is best for this NTP server to be in sync with the one used by the object store.

    The Notifications page opens.

11. To enable email notifications of system events, select the **Enable notifications for system events** checkbox.

    Note

    Your network and firewall must be configured to allow traffic through the SMTP port you specify for the notification service.

    a. In the **SMTP Server** and **Port** fields, specify the server name and port number.

    b. In the **Sender Address** field, specify the email address from which event notifications are sent.

       example_alerts@example.com

    c. If your SMTP provider operates an authenticated service, provide the necessary credentials in the **Username** and **Password** fields.

    d. If necessary, select the **Use TLS when connecting to the mail server** checkbox.

    e. To subscribe recipients to event notification emails, click any event level to select or deselect it, enter an email address for each recipient for the selected notification event levels, and then click **Save**.

    f. Click **Save and Continue**.

    The External Access page opens.

12. To enable access to the management console from a secure HTTP port (443), select the **Enable external access** checkbox, and then click **Save and Continue**.

Results

The CloudBoost virtual appliance is deployed with all the settings you specified.

After you finish

Download the CloudBoost encryption key. For more information, see Download the CloudBoost encryption keys on page 38.

Configuring a CloudBoost share

After you deploy the CloudBoost virtual appliance, you must configure the shared data store.

Before you begin

Configure and deploy the CloudBoost virtual appliance. For more information, see Deploying the CloudBoost virtual appliance on page 18.

Procedure

1. Use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Shares** in the top menu.

2. Click **Configure Share**.

   The Configure Share page opens.

3. In the **Cloud Storage Profile** field, select the cloud storage account to use for storing the share.

4. To specify a container for the share data, click **advanced settings**, then type the name of an existing container in the **Container for the Share Data** field.

   This name is used to access the share. Share names cannot contain spaces or any of these characters: `\ " / [ ] : | < > + = ; , ?`

   Note

   If you specify a container in this way, that container is not automatically deleted by CloudBoost when deleting the share.

5. To improve data transfer performance by making use of a geographical read cache, select the **Enable Cloud Delivery Cache** checkbox.

   The separate CloudBoost planes for data and metadata allow data caches to be deployed with no impact on file system consistency. The metadata path remains real-time for all users.

6. Select a database for storing the share's metadata, and then click **Configure Share**.

   The Shares page opens, showing progress and details while the share initializes.

After you finish

Download the CloudBoost encryption key if you have not already done so. For more information, see Download the CloudBoost encryption keys on page 38.

Connecting NetWorker to CloudBoost

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

Before you begin

You can refer to NetWorker documentation for information about installing and configuring NetWorker, storage nodes, and advanced file type devices (AFTDs). For more information, refer to the *EMC NetWorker Installation Guide* and the *EMC NetWorker Administration Guide*.

Procedure

1. In the NetWorker administration interface, create a new storage node as an AFTD device and provide the FQDN for CloudBoost.

   This must be a sub-directory under `/mnt/magfs/base`, for example, `/mnt/magfs/base/device0`.

2. Create or choose a NetWorker backup clone to be sent to CloudBoost.

   The backup clone is sent to CloudBoost according to the scheduling settings in NetWorker.

After you finish

Download the CloudBoost encryption key if you have not already done so. For more information, see Download the CloudBoost encryption keys on page 38.

Verify that CloudBoost is receiving clones from NetWorker

Verify that CloudBoost is receiving clones from NetWorker.

To verify that CloudBoost is receiving clones from NetWorker, open the CloudBoost management console and click **Dashboard**. Storage consumption for data sent to the share and received by CloudBoost is reflected there. For more information, see CloudBoost Dashboard on page 24.

If you have not already done so, download the CloudBoost encryption key and store it off-box so you can recover in the event of a disaster. For more information, see Downloading the CloudBoost encryption keys on page 38.

You may also test restoring data from the share by using the NetWorker Recovery Wizard. For more information, see Restore from the Cloud on page 29.

CHAPTER 3

Monitor and Manage the CloudBoost Virtual Appliance

This chapter contains the following topics:

CloudBoost Dashboard

The CloudBoost Dashboard shows the current status of the management server and its critical services.

You can monitor the health of the systems and obtain basic statistics such as the amount of de-duplicated data, number of users, etc.

Some of the Dashboard counters and charts display dashes (--) or `No Data To Show` until the system has been running for 30 minutes, or until user activity has been registered.

Monitoring services and loads

You can monitor services and loads on the CloudBoost virtual appliance from the Dashboard page.

To open the Dashboard page, use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Dashboard** in the top menu of the CloudBoost management console.

Green indicates a healthy system, yellow indicates an area of concern and red indicates a serious issue.

Table 5 Monitoring services for the CloudBoost virtual appliance

Service	Description
Discovery Service	Not applicable
Statistics Service	A data collector for instantaneous and historical statistical collection along with graphing for reporting.

Table 6 Monitoring loads on the CloudBoost virtual appliance

Load Monitoring	Description
Load-Short	A measure of the average amount of computational work on the virtual machine, monitored over a rolling one-minute window. The maximum height of the graph is linked to the number of CPUs available. A value of `0` indicates that the CloudBoost virtual appliance is under no load.
Mem Free	A numerical indication of the total amount of available memory. The graph is inverted, meaning that low bars indicate a low amount of available memory.
Disk Free	A numerical indication of the total amount of available disk space. The graph is inverted, meaning that low bars indicate a low amount of available disk space.

Monitoring services for shares

You can monitor CloudBoost shares from the Dashboard page of the CloudBoost management console.

To open the Dashboard page, use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Dashboard** in the top menu of the CloudBoost management console.

Table 7 Monitoring services for a CloudBoost share

Share Service	Description
Metadata Service	The logical control plane for metadata pertaining to the location and state of all data in the namespace.
Database Service	Operates configuration information for the share and provides a storage layer for metadata.

Table 8 Monitoring loads on the CloudBoost share

Load Monitoring	Description
Load-Short	A measure of the average amount of computational work on the virtual machine, monitored over a rolling one-minute window. The maximum height of the graph is linked to the number of CPUs available. A value of `0` indicates that the CloudBoost virtual appliance is under no load.
Mem Free	A numerical indication of the total amount of available memory. The graph is inverted, meaning that low bars indicate a low amount of available memory.
Disk Free	A numerical indication of the total amount of available disk space. The graph is inverted, meaning that low bars indicate a low amount of available disk space.

To see graphs showing user connection activity or object store usage, click the **details** link.

The default view, Share Size and Blobstore usage, shows the current share size and object store usage over time.

To see the number of users connected to the share over time, click **Share Size and Blobstore Usage**, and then select **Connected Users**.

The default time period for these graphs is to show usage over the last hour. You can modify the time window by selecting the drop down at the top right of the graph, and then choosing **Last hour**, **Last day**, **Last week**, **Last month**, or **Last year**.

Monitoring events

You can monitor system events for the CloudBoost virtual appliance from the Dashboard page.

To open the Dashboard page, use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Dashboard**. The Event log appears on the right side of the Dashboard page.

Table 9 System event levels

Event level	Description
Info	Informational messages indicate success of a major event on the CloudBoost virtual appliance, such as `Share Create`.
Warn	Warning messages indicate that a non-major event was registered by the CloudBoost virtual appliance. These messages are typically helpful when supporting debugging.
Error	Error messages indicate the failure of major events registered by the CloudBoost virtual appliance, such as `Share Create—failed`. These messages are critical when reporting or tracking issues.

You can filter the event log by clicking on the info, warn, or error buttons at the top of the list. Inactive buttons are gray.

Events triggered by an administrative user (those which are not automatic system events) include the name of the user who triggered the event.

Managing notifications

Subscribe to email notifications of system events based on event level.

Before you begin

Your network and firewall must be configured to allow traffic through the SMTP port you specify for the notification service.

You can enable notifications of system events during initial deployment of the CloudBoost virtual appliance or at any time afterward. If you do not enable notifications, all users see all notifications for all system events on the Dashboard page of the management console.

The notifications service sends emails when there are new system events. You can subscribe recipients to events based on the event levels, which are info, warning, and error.

Procedure

1. Use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name.
2. Click **Settings** › **Notifications**.
3. To enable notifications, select the **Enable notifications for system events** checkbox.
   a. In the **SMTP Server** and **Port** fields, specify the server name and port number.
   b. In the **Sender Address** field, specify the email address from which event notifications are sent.

      example_alerts@example.com

   c. If your SMTP provider operates an authenticated service, provide the necessary credentials in the **Username** and **Password** fields.
   d. If necessary, select the **Use TLS when connecting to the mail server** checkbox.

   The notification service is set up with mail server information.
4. Subscribe recipients to event notification emails.

a. Warn and error events are selected by default. Click any event level to select or deselect it.

b. Enter an email address for each recipient for the selected notification event levels, and then click **Save**.

5. To send a test message, click the envelope icon for a recipient.
6. To delete an email recipient, click the trashcan icon for a recipient.

Monitoring CloudBoost share status and performance history

You can monitor the status and performance history of a CloudBoost share.

Procedure

1. Use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Shares** in the top menu.

   The Shares page opens.

2. For a share, click **Manage VM disk** next to **disk space**.

   The Virtual Machines page opens.

3. Click the graph icon below the IP address of any share.

   A performance graph appears showing IOPS, CPU, network packets, disk ops and load over time. You can alter the reporting window, selecting from 30s, 5m, 15m, 1h and 24h views.

4. To open an SSH session with a share, click the terminal icon next to the share name.

Adding space to a CloudBoost share

You can add to the available system volume to support a growing share.

Before you begin

Make a new disk or EBS volume available to the VM.

Procedure

1. Use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Shares** in the top menu.

   The Shares page opens.

2. For a share, click **Manage VM disk** next to **disk space**.

   The Virtual Machines page opens.

3. Next to the space utilization information, click **Add**.
4. Select any available volume and then click **Add Volume**.

CHAPTER 4

Restore from the Cloud

This chapter contains the following topics:

Restore files from NetWorker

You can restore files from the cloud using NetWorker.

You can find complete information about the NetWorker Recovery Wizard in the *EMC NetWorker Administration Guide*.

Creating a new recover configuration

The Recovery Wizard allows you to create and save a configuration that you can reuse or modify later.

Procedure

1. Use NMC to connect to the NetWorker server.
2. Click **Protection** from the left navigation pane, then select **Clients**.
3. Right-click the client from which you want to recover the data, then select **Recover**. The Recovery Wizard appears.
4. Navigate through the Recovery Wizard screens and define the configuration for the recover job. Online help describes how to use the Recovery Wizard.

Troubleshooting Recovery Wizard

At the start time for a Recovery resource, `nsrd` uses an `nsrtask` process on the NetWorker server to start the recover job. The `nsrtask` process requests that the `nsrjobd` process on the NetWorker server run the recovery job on the destination client, then `nsrtask` monitors the job.

Once the recover job starts:

- The log files on the NetWorker server contain stdout and stderr information for the recover job. NetWorker stores the logs files in the following location, by default:
  - Windows: `C:\Program Files\EMC NetWorker\nsr\logs\recover`
  - UNIX: `/nsr/logs/recover`

  Note

  NetWorker names the log file according to the name of the recover resource and the time of the recovery job: *recover_resource_name_YYYYMMDDHHMMSS*
- The jobsdb contains job status information for the recover job.

Debugging recover job failures from NMC

To troubleshoot a recovery issue by using NMC, configure the Recovery resource to display greater detail in the log file, then retry the recover configuration in debug mode:

Procedure

1. In the **Recover** window, right-click the recover configuration and select **Recover Again**.
2. Click the **Back** button until you reach the **Select the Recover Options** window.
3. Select **Advanced Options**.

4. Increase the value in the **Debug level** attribute to enable debugging. The higher the value, the more the debug output that appears in the recover log file.
5. Click **Next** until you reach the **Perform the Recover** window.
6. In the **Recover name** field, provide a new name for the recover configuration.
7. Click **Run Recover**.
8. Monitor the status of the recover job in the option in the **Recover** window.
9. When the recover completes, review the recover log file.

CHAPTER 5

Disaster Recovery

This chapter contains the following topics:

CloudBoost disaster recovery

In the event of a disaster, you can deploy a second CloudBoost virtual appliance to restore metadata.

⚠ CAUTION

Disaster recovery requires the encryption key file for system backups. Immediately after the original CloudBoost virtual appliance was deployed, you should have downloaded and safeguarded the encryption key and its password to be prepared for disaster recovery. You can download this key any time after deployment. For information, see **Download the CloudBoost encryption key on page 38****.**

If the CloudBoost virtual appliance encounters a failure, you must deploy a second CloudBoost virtual appliance to restore the metadata from backups stored in the cloud. Backups of the CloudBoost metadata are automatically taken every 12 hours and stored in the same object store as the data. The recovery process requires this metadata to be restored to the newly deployed CloudBoost virtual appliance.

For disaster recovery testing, you must deploy a second CloudBoost appliance using the test recovery mode. A CloudBoost virtual appliance deployed using the test recovery mode is read only. You cannot use it to clone backups to the cloud. It can only be used for restores from cloud to verify backups as part of the disaster recovery testing process. The workflow is similar to the standard disaster recovery except for the recovery mode.

Testing CloudBoost disaster recovery

You can test the disaster recovery process for the CloudBoost virtual appliance.

Procedure

1. Install a CloudBoost virtual appliance and configure it using CLI commands.

   The new deployment can have a different name and IP from the original deployment. For more information, see Provision and Deploy the Cloudboost Virtual Appliance on page 13.

2. Use a Web browser to log in to the Cloudboost virtual appliance at `https://<FQDN>:4444`, where *‹FQDN›* is the fully qualified domain name specified during Step 1, with the default username **`local\admin`** and the password set during Step 1.

   If a password was not specified during Step 1, the default password is **`password`**. You must immediately change this default password.

3. Click **Get Started**, and on the License Agreement page, click **I Agree**.

   The Deployment page opens.

4. Review the network and host settings you defined in Step 1.

   For more information, see Configuring the CloudBoost virtual appliance on page 16.

5. In the **Deployment Type** field, select **Disaster Recovery**, and then click **Save and Continue**.

6. On the Recovery Mode page, select **Test Recovery**.

7. If an HTTP proxy must be used to reach the cloud storage service from the CloudBoost virtual appliance, select the **Enable Outbound HTTP Proxy** checkbox, enter the hostname and port in the **HTTP Proxy hostname and port** fields, and then click **Save and Continue**.

The Cloud Storage Profile page opens.

8. To retrieve the most recent metadata backup from the cloud, specify the encryption key file and the key file password, and then click **Continue**.

   This is encryption key file for system backups which was downloaded after the original CloudBoost virtual appliance was deployed, along with the password set during download of the file.

9. On the Recover Deployment page, select the metadata backup to retrieve from cloud.
10. When the recovery of metadata is complete, click **View Share**.

    The Shares page opens, where you can verify that the status is **Active**.

11. Log in to the NetWorker administration console and add the newly-deployed CloudBoost virtual appliance as a storage node.

    Because this is a test, the new deployment must have a different name and IP from the original deployment. For more information, see Connecting NetWorker to CloudBoost on page 20.

12. Add a new AFTD device and specify its mount point.

    This mount point should be the same as the mount point of the AFTD device on the original CloudBoost virtual appliance. You can enter the mount point manually or browse to it using the AFTD browse option. The mount point for an AFTD device needs to be a sub-directory under `/mnt/magfs/base`.

13. Deselect the **label and mount device after creation** checkbox.

    ⚠ CAUTION

    Do not label the AFTD device. If the AFTD device is labeled, backups taken using this device will be deleted from the cloud.

14. If the original CloudBoost virtual appliance had multiple AFTD devices, recreate each device individually.
15. After the AFTD device is created, manually mount the device.
16. Recover backups from the cloud to an alternate path on a client.

    Repeat this for a couple of clients and savesets and verify that the disaster recovery testing virtual appliance sees all backups and can restore them.

17. Unmount the AFTD device, remove the storage node from NetWorker administrative console and delete the test disaster recovery virtual appliance.

    The test disaster recovery virtual appliance is read-only and cannot be used for any cloning operations.

Deploying CloudBoost for disaster recovery

You can deploy a second CloudBoost virtual appliance to recover from failure of the original CloudBoost virtual appliance.

Procedure

1. Install a CloudBoost virtual appliance and configure it using CLI commands.

   The new deployment can have a different name and IP from the original deployment. For more information, see Provision and Deploy the Cloudboost Virtual Appliance on page 13.

2. Use a Web browser to log in to the Cloudboost virtual appliance at `https://<FQDN>:4444`, where *‹FQDN›* is the fully qualified domain name specified during Step 1, with the default username **`local\admin`** and the password set during Step 1.

   If a password was not specified during Step 1, the default password is **`password`**. You must immediately change this default password.

3. Click **Get Started**, and on the License Agreement page, click **I Agree**.

   The Deployment page opens.

4. Review the network and host settings you defined in Step 1.

   For more information, see Configuring the CloudBoost virtual appliance on page 16.

5. In the **Deployment Type** field, select **Disaster Recovery**, and then click **Save and Continue**.

6. On the Recovery Mode page, select **Disaster Recovery**.

7. If an HTTP proxy must be used to reach the cloud storage service from the CloudBoost virtual appliance, select the **Enable Outbound HTTP Proxy** checkbox, enter the hostname and port in the **HTTP Proxy hostname and port** fields, and then click **Save and Continue**.

   The Cloud Storage Profile page opens.

8. To retrieve the most recent metadata backup from the cloud, specify the encryption key file and the key file password, and then click **Continue**.

   This is encryption key file for system backups which was downloaded after the original CloudBoost virtual appliance was deployed, along with the password set during download of the file.

9. On the Recover Deployment page, select the metadata backup to retrieve from cloud.

10. When the recovery of metadata is complete, click **View Share**.

    The Shares page opens, where you can verify that the status is **Active**.

11. Log in to the NetWorker administrative console and add the newly-deployed CloudBoost virtual appliance as a storage node.

    For more information, see Connecting NetWorker to CloudBoost on page 20

12. Add a new AFTD device and specify its mount point.

    This mount point should be the same as the mount point of the AFTD device on the original CloudBoost virtual appliance. You can enter the mount point manually or browse to it using the AFTD browse option. The mount point for an AFTD device needs to be a sub-directory under `/mnt/magfs/base`.

13. Deselect the **label and mount device after creation** checkbox.

    ⚠ CAUTION

    Do not label the AFTD device. If the AFTD device is labeled, backups taken using this device will be deleted from the cloud.

14. If the original CloudBoost virtual appliance had multiple AFTD devices, recreate each device individually.

15. After the AFTD device is created, manually mount the device and restart any failed backups from the NetWorker administrative console.

CHAPTER 6

Support and Troubleshooting for the CloudBoost Virtual Appliance

This chapter contains the following topics:

Request assistance

You can find tools for managing and debugging the CloudBoost deployment within the management console.

Log in to the CloudBoost management console and click **Support** in the top menu. To request assistance, click the **EMC Product Support Site** link next to Contacting Us.

Downloading the CloudBoost encryption keys

At the earliest opportunity, download and securely store your CloudBoost encryption keys so they will be available in the event you need to recover your system from a backup.

It is best to download your encryption keys as soon as possible, though you can download them at any time. You must securely store the downloaded encryption keys separately from the location of any backed up objects. You will use these keys if you ever need to recover your system from a backup. For information about disaster recovery, see Disaster Recovery on page 33.

⚠ CAUTION

There is no way to retrieve your encryption keys after a system failure.

Procedure

1. Use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Support** in the top menu.

   The Support page opens.
2. Next to Encryption Keys, provide and confirm a strong password to protect the key file.
3. Click **Download Encryption Keys**.

   The keys are downloaded.
4. Securely store the downloaded encryption keys separately from the location of any backed up objects.

Managing and downloading CloudBoost log files

You can download log files to diagnose problems with a CloudBoost share, and change logging levels to either increase the amount of information collected or to improve share performance.

Log files are an important tool when investigating issues. Each share operates its own independent logging. You can change the log level for any share.

While increasing the logging level may assist in diagnosing a reported problem, it will decrease the performance of the share.

Procedure

1. Use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Support** in the top menu.

   The Support page opens.

2. To change the level of logging for a share, select the appropriate share next to Log Level, and then select the log level for that share.
   - **normal (info)**, the default log level.
   - **high (debug)**
   - **higher (trace)**
3. Click **Change Log Level** to confirm your selections, and then click **OK**.
4. To download an archive of the logs and other system information, click either **Download Recent Log Files** or **Download All Log Files** next to Download Logs.

   A `.zip` file is downloaded. The time this takes depends upon the quantity and size of the log files.

Results

When an elevated log level is no longer needed for diagnosing and troubleshooting issues with a share, you can reduce the level to normal and thereby improve performance of the share.

Enabling support data for proactive care

You can choose to send data about your CloudBoost deployment to support to enable receipt of proactive system care.

You can enable data to be sent to support, so that you can receive proactive care from EMC for your deployment of CloudBoost. Alerts include notifications when you run low on system resources or licensed capacity, and information about new features or updates to existing features.

You may choose to send data to EMC anonymously, which removes FQDN and share naming information. Anonymous data may enable faster support response to issues, but it can limit the proactive support you receive.

All data sent to support is encrypted, regardless of whether it is anonymous. Support data is sent to EMC once each day.

Procedure

1. Use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Support** in the top menu.

   The Support page opens.
2. Next to Support Data, select the **Allow support data to be sent to EMC for proactive care** checkbox.
3. To send the support data anonymously, select the **Anonymize data** checkbox.

Results

Upgrading the CloudBoost virtual appliance

On the Support page, you can see what version of CloudBoost is currently running, and you can upgrade the CloudBoost virtual appliance.

Before you begin

- Determine the location of the upgrade `.tar` file. This file may be made available from a URL or in a local network location the CloudBoost virtual appliance may browse to.

- Schedule a time for the upgrade, during which all managed shares will be unavailable. The upgrade takes several minutes.

Procedure

1. Use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Support** in the top menu.

   The Support page opens.
2. Next to Upgrading, review the version currently running and whether any version is currently staged for installation.
3. Ensure that no tasks are currently running.

   For more information, see Monitoring and Managing the Cloudboost Virtual Appliance on page 23.
4. Click **Load New Upgrade File**.
5. Choose one of these methods to provide the upgrade file.
   - Provide a URL to the location of the upgrade `.tar` file, then click **Fetch File**.
   - Click **select file**, and then browse to the locally-available location of the upgrade `.tar` file.

   The specified `.tar` file is imported, its integrity is automatically verified, and it is staged for installation.
6. To install the version shown as staged for installation, click **Install version *x.x.x***.

   A verification is performed to determine whether an upgrade to the target version is actually required.
7. On the Upgrade Confirmation message, click **Upgrade**.

   All services are stopped while the upgrade is applied, stopping access to all shares.

   Note

   The service that runs the management console is upgraded along with the services on the management server. The management console will be unresponsive until the reboot has completed, though some client-side scripting minimizes the impact and provides some status information. When the service restarts, the management console resumes responding and reflects real-time information.
8. On the Upgrade Complete message, click **OK**.

Results

The system automatically restarts and all services resume.

CHAPTER 7

Manage SSL Certificates for the CloudBoost Virtual Appliance

This chapter contains the following topics:

SSL certificate requirements

SSL certificates are used to establish trust between machines.

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

The CA-signed wildcard certificate must be suitable for SSL server usage and must cover all the host names in the CloudBoost deployment. Certificates that do not cover all of the VMs in your 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 across the top of every page of the CloudBoost management console 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

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

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

Note

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

Selecting **Self-signed certificate** in the CloudBoost management console 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 in the CloudBoost management console.

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 = www.foo.com
DNS.2 = www.bar.org
```

2. Save the file.
3. Enter this command to generate a valid private RSA key: `$ openssl genrsa 2048 > host.key`

   Once the private key is generated, a Certificate Signing Request can be generated.
4. Enter this command to use the CSR to self-sign the CSR: `$ openssl req –new –key host.key –out host.csr –config config.cnf`
5. Self-sign the certificate request, setting a life-span of the certificate: `$ openssl x509 –req –days 365 –in host.csr –signkey host.key –out host.crt –extensions v3_req –extfile config.cnf`
6. Combine the files to generate a valid `.pem` file: `$ 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 in the CloudBoost management console.

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).

Procedure

1. In a Linux terminal, execute this command: `$ openssl pkcs12 -export -chain -CAfile foo.com.chain.pem -in magfs.io.pem -inkey foo.com.key -passout file:passphrase.txt -out foo.com.chain.p12`

   Where:

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

Verifying your certificate

Verify an SSL certificate before providing it to the CloudBoost management console.

OpenSSL provides tools to verify an SSL certificate. It is best practice to verify your certificate before providing it to the CloudBoost management console.

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

Procedure

1. From a Linux terminal, execute this command, replacing *host.crt* with the appropriate certificate filename: `$ openssl verify -purpose sslserver host.crt`

Providing an SSL certificate

You can provide a self-signed or a CA-signed SSL certificate in the CloudBoost management console.

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

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

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

Procedure

1. Use a Web browser to log in to the CloudBoost virtual appliance at `https://<FQDN>:444`, where *‹FQDN›* is your fully qualified domain name, and then click **Settings › Certificates**.

2. Select the type of SSL certificate and provide the necessary certificate information.

Option	Description
Self-signed certificate	Generate a self-signed certificate.
CA-signed certificate	Upload a CA-signed wildcard certificate in the form of a `.p12` or `.pfx` file and if necessary, type the encryption pass phrase.