

Dell EMC NetWorker

Version 18.2

CloudBoost 18.2 Integration Guide

302-005-332

REV 01

Copyright © 2016-2018 Dell Inc. or its subsidiaries. All rights reserved.

Published December, 2018

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.” DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

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

CONTENTS

	PREFACE	7
Chapter 1	CloudBoost Integration	11
	About the CloudBoost appliance.....	12
	CloudBoost appliances with NetWorker software.....	12
	CloudBoost requirements and considerations.....	13
	On-Prem CloudBoost Management Console browser requirement....	13
	Direct back up to the cloud with Linux and Windows clients.....	14
	Backup Amazon EC2 data to Amazon S3 storage.....	14
	Backup a Microsoft Azure virtual machine data to Azure blob	
	storage.....	15
	Cloud best practices.....	15
	Supported private clouds.....	17
	Supported public clouds.....	17
	Supported Regions.....	18
	Firewall port requirements.....	19
Chapter 2	NetWorker with CloudBoost solution requirements	21
	Solution requirements.....	22
	WAN requirements.....	22
	Virtual CloudBoost appliance requirements (VMware ESX).....	22
	Virtual CloudBoost appliance requirements (Amazon Web Services	
	EC2).....	23
	Virtual CloudBoost appliance requirements for Microsoft Azure....	23
	NetWorker client host requirements.....	24
	CloudBoost sizing and performance considerations.....	24
	CloudBoost metadata storage requirements.....	24
	End-to-end bottlenecks.....	25
	Minimum WAN requirements.....	25
Chapter 3	Deploying the Virtual CloudBoost Appliance with VMware ESX	27
	Virtual CloudBoost appliance installation (VMware ESX).....	28
	Deploy the virtual CloudBoost appliance.....	28
	Configure network settings for a CloudBoost appliance.....	29
Chapter 4	Deploying the CloudBoost Appliance with Microsoft Azure	33
	Resource Manager	33
	Integrate the CloudBoost appliance with Microsoft Azure.....	34
	Download the VHD files and JSON template.....	34
	Configure and deploy the CloudBoost appliance	34
	Use the Azure PowerShell to configure Microsoft Azure for the	
	CloudBoost appliance.....	34
	Use the Azure CLI to configure the CloudBoost appliance.....	35
	Start the CloudBoost virtual machine.....	41
	Set the FQDN.....	41

	Check the Microsoft Azure audit logs.....	42
	Verify network setup and status of the appliance.....	42
Chapter 5	Deploying the CloudBoost Appliance in Amazon EC2	45
	Deploy the virtual CloudBoost appliance in Amazon EC2.....	46
	Start the CloudBoost virtual machine.....	47
	Set the FQDN.....	47
	Verify network setup and status of the appliance.....	48
Chapter 6	Configuring Network Settings for a CloudBoost Appliance	49
	Network settings for a CloudBoost appliance.....	50
	Configure network settings for a CloudBoost appliance.....	50
	Configure CloudBoost to use a proxy.....	52
Chapter 7	Configuring a New CloudBoost Appliance	55
	Create and manage cloud profile for CloudBoost appliance.....	56
	Cloud profiles.....	56
	Create a cloud profile.....	56
	Edit a cloud profile.....	56
	Validate cloud storage credentials.....	57
	Enable remote client mounts.....	58
	Configuring a new CloudBoost appliance.....	58
	Editing CloudBoost appliance configurations.....	60
Chapter 8	Configuring NetWorker with a CloudBoost appliance	61
	Configure a CloudBoost device by using an embedded NetWorker storage node.....	62
	Configure a CloudBoost device on an external storage node.....	65
	Troubleshoot CloudBoost device configuration issues.....	70
	Setting the configuration options for the CloudBoost SDK.....	70
	Improve clone performance.....	71
	Cannot retrieve the version of the CloudBoost appliance.....	72
	The selected CloudBoost appliance is unsupported for device type "CloudBoost".....	72
	Directory not found.....	72
	Unable to connect to the CloudBoost appliance: LOGON_FAILURE error.....	72
	Adding a CloudBoost 2.2.2 appliance fails with an error "unable to resolve".....	73
	Report information on cloud backup.....	73
Chapter 9	Perform a CloudBoost Appliance Recovery	75
	Recovering CloudBoost Appliance.....	76
Chapter 10	Monitoring, Managing, and Supporting a CloudBoost Appliance	77
	Monitoring CloudBoost.....	78
	Upgrade a CloudBoost appliance.....	78
	CloudBoost integration with EMC Secure Remote Services	79
	Registering EMC Secure Remote Services.....	79
	Installing the EMC Secure Remote Services gateway.....	79

Register CloudBoost with EMC Secure Remote Services.....	80
Configuring average chunk size.....	81
Specifications for the chunk size setting.....	81

PREFACE

As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

Note

This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website <https://www.dell.com/support>.

Purpose

This document describes the integration between the NetWorker software and the CloudBoost appliance.

Audience

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

Revision history

The following table presents the revision history of this document.

Table 1 Document revision history

Revision	Date	Description
01	December 14, 2018	First release of this document for NetWorker 18.2.

Related documentation

The following publications provide information about CloudBoost.

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

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

- *NetWorker Administration Guide*
Describes how to configure and maintain the NetWorker software.
- *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

The following conventions are used 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

The following type style conventions are used in this document:

Table 2 Style conventions

Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
<i>Italic</i>	Used for full titles of publications that are referenced in text.
Monospace	Used for: <ul style="list-style-type: none"> • System code • System output, such as an error message or script • Pathnames, file names, file name extensions, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Used for variables.
Monospace bold	Used for user input.
[]	Square brackets enclose optional values.
	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

You can use the following resources to find more information about this product, obtain support, and provide feedback.

Where to find product documentation

- <https://www.dell.com/support>
- <https://community.emc.com>

Where to get support

The Support website <https://www.dell.com/support> provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to <https://www.dell.com/support>.
2. In the search box, type a product name, and then from the list that appears, select the product.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

Live chat

To participate in a live interactive chat with a support agent:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

Service requests

To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.

Note

To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To get the details of a service request, in the *Service Request Number* field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

Online communities

For peer contacts, conversations, and content on product support and solutions, go to the Community Network <https://community.emc.com>. Interactively engage with customers, partners, and certified professionals online.

How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

CloudBoost Integration

This section contains the following topics:

• About the CloudBoost appliance	12
• CloudBoost appliances with NetWorker software	12
• Supported private clouds	17
• Supported public clouds	17
• Supported Regions	18
• Firewall port requirements	19

About the CloudBoost appliance

The CloudBoost appliance provides an integrated solution for existing supported backup environment by enabling the transfer of backups to public, hybrid, or private cloud storage. The CloudBoost appliance supports the following use cases: long-term retention to the cloud and backup to a private or public cloud.

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 read/write operations. All advanced data services, such as chunking, encryption, inline deduplication, compression, and bulk data transfers are performed separately from metadata storage.

CloudBoost is available as a VMware virtual appliance and as a virtual appliance that resides in supported public clouds.

CloudBoost appliances with NetWorker software

A NetWorker with CloudBoost environment can extend onsite data protection to the cloud through the following methods:

Backup to the cloud

NetWorker with CloudBoost allows direct backup of on-premises clients to a range of private, public, and hybrid clouds. This solution allows clients to send backups directly to the object store with only the metadata being stored in the CloudBoost appliance. This distributed model where the CloudBoost appliance is not in the data path provides enhanced backup performance, scale, and client-side data reduction. The solution supports Client Direct backup to the cloud for Linux and Windows file systems and a broad range of enterprise applications. For applications that do not support Client Direct, use an external or embedded NetWorker Storage Node to perform backups directly to the cloud.

Backup in public cloud

This solution allows protection of applications that run in public clouds such as AWS, AWS S3, Azure, and Azure blob storage. Similar to on-premises backups to the cloud, this solution allows Client Direct backup to the object store for applications that run in AWS EC2 and Azure compute instances. For applications that do not support Client Direct, use an external or embedded NetWorker Storage Node to perform backups directly to the cloud.

Long-term retention or cloning to cloud:

This solution allows clone backups from a backup target to the cloud for long-term retention. The operational copy for backup and restore operations remains on the Data Domain host or any other backup target. The copy that is cloned to the cloud by NetWorker and CloudBoost is used for long-term retention of data.

This table details the module support matrix for CloudBoost.

Table 3 CloudBoost module matrix

Module	Application	External or embedded Storage Node	Cloning	Client Direct	
				Linux x64	Microsoft Windows 64-bit
File System	Not applicable	Yes	Yes	Yes	Yes
Block Based Backup					
NetWorker Module for Databases and Applications (NMDA)	DB2	Yes	Yes	Yes	Yes
	Informix				Not applicable
	SAP IQ				
	Lotus				Yes
	MySQL			Yes, except for AWS	Not applicable
	Oracle				Yes
	Sybase			Yes	
NetWorker Module for Microsoft	Microsoft Exchange	Yes	Yes	Not applicable	Yes
	Microsoft Hyper-V				
	Microsoft SharePoint				
	Microsoft SQL				
NetWorker Module for SAP (NMSAP)	SAP HANA	Yes	Yes	Yes	Not applicable
	SAP with Oracle				Yes
NetWorker Snapshot Module (NSM)	Not applicable	Not applicable	Yes	Yes, only RHEL	Yes
VBA	VMware			Not applicable	Not applicable
vProxy	VMware				

CloudBoost requirements and considerations

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

Refer to the *NetWorker E-LAB Navigator* for the complete list of supported products and versions.

On-Prem CloudBoost Management Console browser requirement

The supported web browser for On-Prem CloudBoost Management Console is:

- Google Chrome
- Microsoft Internet Explorer
- Mozilla firefox

Direct back up to the cloud with Linux and Windows clients

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

Direct backup to the cloud is recommended for the following use cases:

- Where a high bandwidth pipe to the object store is required.
- When backing up non-critical applications that can tolerate a higher SLA for backup and restore operations.

This illustration displays Linux and Windows clients that are directly backed up to the cloud.

Figure 1 Clients backed up directly to the cloud

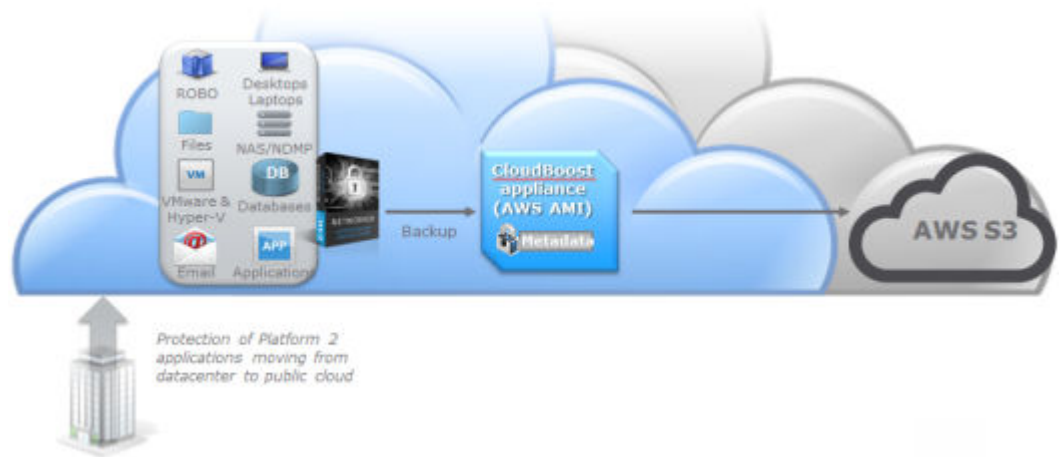


For clients that cannot back up directly to the cloud, you can send backups through the CloudBoost appliance or an external NetWorker storage node to the cloud. However, routing through either the CloudBoost appliance or the external NetWorker storage node limits performance. Having the data path go directly from the client to the cloud is the most scalable, efficient, and optimal performance deployment model.

Backup Amazon EC2 data to Amazon S3 storage

This use case is intended for workloads that run in public clouds and use S3 cloud object storage for backups, including short-term backups for operational recovery and long term retention backups for compliance.

The following illustration displays back up in Amazon EC2 to Amazon S3 storage.

Figure 2 Back up in Amazon EC2 to Amazon S3 storage

Backup a Microsoft Azure virtual machine data to Azure blob storage

This use case is intended for workloads that run in the public cloud and use Microsoft Azure blob storage for backups, including short-term backups for operational recovery and long-term retention backups for compliance.

You use the same NetWorker tools to manage both onsite and cloud-based data protection processes.

The following illustration illustrates backing up of Microsoft Azure virtual machine to Azure blob storage.

Figure 3 Back up to Microsoft Azure

Cloud best practices

Consider cloud best practices before you implement cloud backups.

Backups to a cloud storage device

NetWorker backups are saved in media pools which can contain one or more backup devices. When a backup is triggered, the NetWorker server sends it to one of the unused devices in the media pool.

When creating a media pool that contains CloudBoost devices, do not include backup devices from other CloudBoost appliances or any other type of backup device. Each CloudBoost appliance has its own deduplication database and cannot deduplicate against backups that are sent to other devices.

Concurrent backup and recovery operations

To support concurrent backup and recovery operations, you can create multiple NetWorker devices on a single CloudBoost appliance.

Each CloudBoost device type supports a minimum target session of 10 and a maximum session of 80. That means, each CloudBoost device supports a minimum of 10 concurrent streams and a maximum of 80 concurrent streams.

For example, to optimize performance you can mount the cloud volume on three cloud storage devices:

- One cloud storage device for backup (device CL1)
- One cloud storage device for recovery (device CL2)
- One cloud storage device for clone operations (device CL3)

You can create a maximum of 512 cloud devices per CloudBoost appliance, which is the maximum capacity of a NetWorker storage node. To optimize the backup and recovery performance, consider reducing the number of cloud devices per CloudBoost appliance. Each cloud device can handle a maximum of 80 concurrent streams.

Network dependencies

Cloud backups depend on the network connection that accesses the cloud service. Any disruption in connectivity or a slowdown in network speed can adversely affect cloud backups or recoveries.

The CloudBoost appliance requires proper DNS name resolution.

Consider the following points before you set up the network for cloud backups:

- If the latency between the source and cloud object store is higher than 50 ms, backup and restore throughput from the object store might be impacted. NetWorker can sustain 100 ms on the metadata path. However, packet loss significantly impacts the backup success rate.
- If there is a high-latency link and some packet loss between the NetWorker server, client, and the CloudBoost appliance, set a high client-retry value for the backup so backups are re-tried.
- An increase of 5 ms latency in the data path (clients to the cloud object store, the CloudBoost appliance, or the cloud object store), has the following impacts:
 - For the initial full backup, throughput is two to two and a half times slower.
 - Consecutive backups are about 20 percent slower compared to a full backup.
- A higher-latency link and higher packet losses might result in significantly slower backup operations.

Note

It is recommended that latency between the NetWorker client and the cloud object store be limited to less than 50 ms and that packet loss be less than 1 percent.

Supported private clouds

The following table lists the private clouds that CloudBoost appliances support.

Table 4 Supported private clouds

Cloud provider	Information that is required by the CloudBoost appliance
Elastic Cloud Storage (ECS) Appliance	<ul style="list-style-type: none"> ECS endpoint ECS access key ID ECS secret access key <hr/> <p>Note</p> <p>Elastic Cloud Storage (ECS) Community version is not supported with CloudBoost.</p>
Generic OpenStack Swift	<ul style="list-style-type: none"> Swift provider authentication endpoint Swift authentication type Region (optional) Swift credentials (specify the tenant name and the username separated by a colon, and then type the password) Swift secret key

Supported public clouds

The following table lists the public clouds that CloudBoost appliances support.

Table 5 Supported public clouds

Cloud provider	Information that is required by the CloudBoost appliance
Amazon Web Services (S3)	<ul style="list-style-type: none"> Storage region AWS access key ID AWS secret access key
Microsoft Azure Storage (supports general purpose and blob storage accounts with hot and cool tiers)	<ul style="list-style-type: none"> Azure account name Azure API key
Virtustream Storage Cloud	<ul style="list-style-type: none"> Access Key ID Secret Access Key Endpoint URL

Table 5 Supported public clouds (continued)

Cloud provider	Information that is required by the CloudBoost appliance
Scality Object Storage	<ul style="list-style-type: none"> • Access Key ID • Secret Access Key • Endpoint URL
Google Cloud Storage (Standard, DRA, Nearline)	<ul style="list-style-type: none"> • Access key • Secret key

Supported Regions

The following table lists the regions that are supported by AWS and Azure.

Table 6 Regions supported by the public cloud

Cloud provider	Supported regions
Amazon Web Services (EC2 and S3)	<ul style="list-style-type: none"> • Virginia • Ohio • California • Oregon • Mumbai • Seoul • Singapore • Sydney • Tokyo • Frankfurt • Ireland • South America (Sao Paulo)
Microsoft Azure Storage	<ul style="list-style-type: none"> • All the regions are supported in Microsoft Azure. <p>Note</p> <ul style="list-style-type: none"> ▪ ZRS replication is not supported. ▪ Special Azure regions are not supported.

Firewall port requirements

As with all networked software solutions, adhering to best practices for security is encouraged to protect the deployment. If the ports in the following table are not configured before you configure the CloudBoost appliance, restart the CloudBoost appliance.

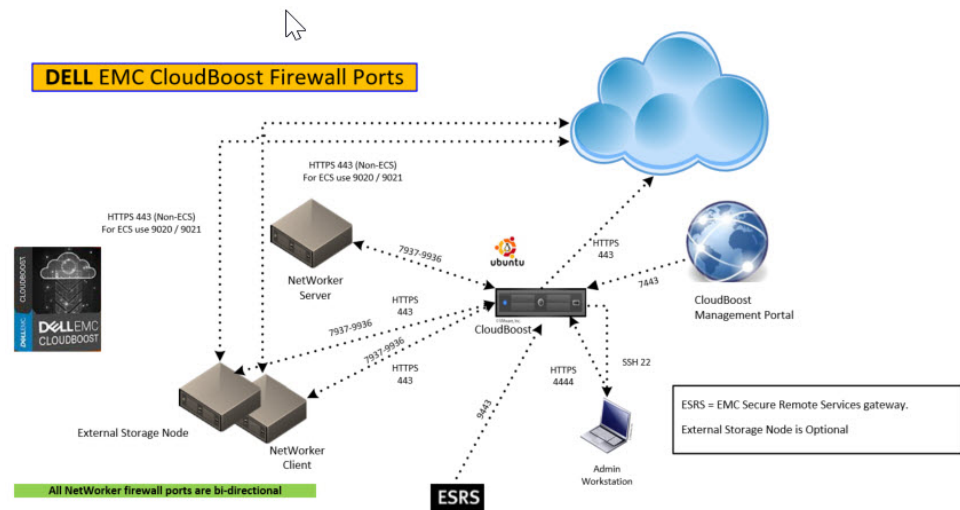
Note

It is not recommended to route outbound http traffic from the CloudBoost appliance through a proxy because it can create a performance bottleneck. In environments where outbound http traffic is restricted, create an exception for the appliance in the firewall after you consult with the IT security team. To configure a proxy, see [Configure CloudBoost to use a proxy](#).

The following table outlines the firewall port requirements.

Table 7 Firewall port requirements

Out	In	TCP port	Description
Administrator workstation	CloudBoost appliance	22	SSH for maintenance and troubleshooting
CloudBoost appliance	Cloud storage (public or private)	443	HTTPS to access object store (if supported)
CloudBoost appliance	On-Prem CloudBoost Management Console	7443	HTTPS to On-Prem CloudBoost Management Console.
NetWorker Server or NetWorker Client	CloudBoost appliance	7937-7942	The CloudBoost appliance has a pre-configured NetWorker SN. For a single CloudBoost device, a minimum of six ports must be opened on the CloudBoost appliance. The port range can be expanded based on the deployment type and the number of CloudBoost devices configured. The <i>NetWorker Security Configuration Guide</i> provides additional information on the NetWorker port requirements.
NetWorker client	<ul style="list-style-type: none"> Cloud Storage (public or private) CloudBoost appliance for metadata. 	443	HTTPS to access object store (if supported)
CloudBoost appliance	EMC Secure Remote Services gateway	9443	Communication from the CloudBoost appliance to the Secure Remote Services gateway

Figure 4 CloudBoost firewall ports

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

For information about NetWorker, refer to the *NetWorker Security Configuration Guide*.

CHAPTER 2

NetWorker with CloudBoost solution requirements

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

- [Solution requirements](#)..... 22
- [NetWorker client host requirements](#)..... 24
- [CloudBoost sizing and performance considerations](#)..... 24

Solution requirements

This section outlines the solution requirements for the CloudBoost appliance in the following environments.

- VMware ESX
- Amazon Web Services (AWS) EC2
- Microsoft Azure

For more information about metadata store, see [CloudBoost sizing and performance considerations](#) on page 24.

WAN requirements

The following points provide the WAN requirements for the CloudBoost appliance.

- Greater than or equal to 100 Mb/s bandwidth
- Less than or equal to 100 ms RTT latency

Virtual CloudBoost appliance requirements (VMware ESX)

The following section outlines the requirements and workflows that are supported for the VMware ESX virtual CloudBoost appliance.

Minimum deployment virtual machine requirements for VMware ESX

This table outlines the requirements.

Table 8 CloudBoost minimum requirements for VMware ESX

Workflow type	CPU	Memory	OS	Metadata space
Client direct backup	4	16 GB	50 GB	100 GB
Backup/clone via CloudBoost appliance	8	32 GB		
	16	64 GB		

Large CloudBoost deployment virtual machine requirements for VMware ESX

This table outlines the requirements.

Table 9 Large CloudBoost deployment requirements for VMware ESX

Workflow type	CPU	Memory	OS	Metadata space
Client direct backup	8	32 GB	50 GB	100 GB
Backup/clone via CloudBoost appliance	16	64 GB	50 GB	Extendable up to 3 TB
	16	64 GB	50 GB	Extendable up to 3 TB

Note

SSD is recommended for storage.

Virtual CloudBoost appliance requirements (Amazon Web Services EC2)

The following section outlines the requirements and workflows that are supported for the Amazon Web Services (AWS) EC2 virtual CloudBoost appliance.

Minimum deployment requirements for AWS EC2

This table outlines the minimum deployment requirements that apply to CloudBoost deployed on Amazon Web Services (AWS) EC2.

Table 10 Minimum deployment requirements for AWS EC2

Workflow type	CPU	Memory	OS	Metadata space
Client direct backup	4	16 GB	50 GB	100 GB
Backup/Clone via CloudBoost appliance	8	32 GB		

Use the AWS EC2 instance, type m4.xlarge, for small-client direct installations.

Note

For smaller environments, you can choose an instance with unified compute and storage such as AWS EC2 m3.xlarge, which includes 4 vCPUs, 15 GB memory, and 2x40 GB SSD storage.

Large deployment requirements for AWS EC2

This table outlines the requirements that apply to a large CloudBoost deployment on Amazon Web Services (AWS) EC2.

Table 11 Large deployment requirements for AWS EC2

CPU	Memory	OS	Metadata space
8	32 GB	50 GB	100 GB metadata space is required per 200 TB of logical capacity

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

Use the AWS EC2 instance type, m4.2xlarge, for Client Direct or for all installations of backup or clone operations through the CloudBoost appliance.

The CloudBoost appliance requires Amazon Elastic Block Store (AWS EBS) for the operating system disk and metadata database. Do not use the AWS EC2 instance default storage volumes with the CloudBoost appliance. The AWS EC2 instance default storage volumes are ephemeral.

Virtual CloudBoost appliance requirements for Microsoft Azure

The following section outlines the requirements and workflows that are supported for the Microsoft Azure virtual CloudBoost appliance.

Minimum deployment virtual machine requirements for Microsoft Azure

This table outlines the minimum requirements are supported for Microsoft Azure.

Table 12 Minimum requirements for Microsoft Azure

Workflow type	CPU	Memory	OS	Metadata space
Client direct backup	4	16 GB	50 GB	100 GB metadata is required per 200 TB of logical capacity
Backup/clone via CloudBoost appliance	8	32 GB	50 GB	100 GB metadata is required per 200 TB of logical capacity
	16	64 GB	50 GB	100 GB metadata is required per 200 TB of logical capacity

NetWorker client host requirements

This table outlines the NetWorker client host requirements for a virtual machine, public cloud, or private cloud.

Table 13 NetWorker client host requirements

Workflow type	Operating System		CPU	Memory
	Linux x64	Microsoft Windows 64-bit		
NetWorker file system backup	Yes	Yes	2	4 GB
NetWorker Module backup	Yes	Yes	See CloudBoost appliance with NetWorker software and the NetWorker Module documentation for specific requirements.	

CloudBoost sizing and performance considerations

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

CloudBoost metadata storage requirements

The amount of metadata storage that is required by a CloudBoost appliance depends on the average chunk size and data reduction ratio.

The virtual CloudBoost appliance requires a minimum of 100 GB of internal capacity for storing CloudBoost metadata. However, the amount of space that is provisioned for metadata directly affects the logical capacity addressable by the virtual CloudBoost appliance.

The ratio of metadata space to logical capacity ranges from 1:2000 to 1:500. For example, 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.

The virtual CloudBoost appliance assumes that the underlying storage is protected by using RAID or a similar technology. The virtual CloudBoost appliance does not provide protection against a failed virtual data disk.

Use the following formula to determine the CloudBoost metadata storage requirements:

```
Metadata storage = 100 GB (Reserved) + (512 / Data Reduction
ratio) * (Logical Capacity in TB / Chunk Size in KB)
```

where:

- The default chunk size is 256 KB, which is the default.
- Deduplication ratio for the CloudBoost appliance is 2x–8x.

Note

You must use an SSD for metadata storage.

Example 1 Examples

To address 6 PB of logical capacity with a dataset that has 4x data reduction, the CloudBoost appliance requires 3 TB of metadata storage.

To address 1 PB logical capacity with a dataset that has 4x data reduction, the CloudBoost appliance requires 500 GB for metadata.

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 in the virtual machine.

Object store ingest limits present 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 100 Mb/s to the cloud with a maximum latency of less than 100 ms RTT is recommended for the CloudBoost solution. Extremely low bandwidth links might result in backup and restore timeouts.

CHAPTER 3

Deploying the Virtual CloudBoost Appliance with VMware ESX

This section includes the following topics:

- [Virtual CloudBoost appliance installation \(VMware ESX\)](#)..... 28
- [Deploy the virtual CloudBoost appliance](#)..... 28
- [Configure network settings for a CloudBoost appliance](#)..... 29

Virtual CloudBoost appliance installation (VMware ESX)

This section applies to installing the virtual CloudBoost appliance on VMware ESX.

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

The procedure for deploying the virtual appliance differs for each cloud provider:

- To deploy the virtual CloudBoost appliance on Amazon EC2, see [Deploying the CloudBoost Appliance in Amazon EC2](#) on page 45.
- To deploy the virtual CloudBoost appliance on Microsoft Azure, see [Deploying the CloudBoost Appliance with Microsoft Azure Resource Manager](#) on page 33.

Deploy the virtual CloudBoost appliance

Deploy the virtual CloudBoost appliance in vSphere.

Before you begin

- Determine the location of the .OVA file that you must download. This location could be a URL or a location that is accessible from the computer, such as a local hard drive or a network share.

Procedure

1. In the vSphere client, click **File > Deploy OVF Template**.
2. Browse to the location of the OVA package, and then click **Next**.
3. Select the **Inventory Location** (the ESX cluster and host that runs the virtual machine), and then type the name of the virtual machine.
4. Select the datastore for the VMDK files, and then click **Next**.

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

5. On the **Ready to Complete** page of the wizard, review the deployment settings.
6. Clear **Power on after deployment**, and then click **Finish**.
7. In the vSphere client inventory, right-click the virtual machine:
 - a. Click **Edit Settings**.
 - b. On the **Resources** tab, click **Memory**.
 - c. Ensure that **Reservation** is set to **a11**.
 - d. Click **OK**.

Note

For performance, memory must be reserved and not shared.

8. Adjust the size of hard disk 2 as required:
 - a. In the vSphere client inventory, right-click the virtual machine.
 - b. Click **Edit Settings**.

- c. On the **Resources** tab, type the size of hard disk 2 in the required field.
- d. Click **OK**.

The virtual CloudBoost appliance installs.

Note

Before you can finish configuring the virtual appliance in the [On-Prem CloudBoost Management Console](#), you must set the appliance's IP address and network through the CLI.

Configure network settings for a CloudBoost appliance

Procedure

1. Connect to the CloudBoost CLI.
2. Authenticate with the default password, `password`.
3. Set the new administrator password.
4. To see the current network configuration of the appliance, type the following command.

```
status
```

```
admin@mag-fs> status
Host Configuration:
  Hostname:      hostname
  Domain:       domain
  FQDN:         fqdn
Version Information:
  Version:      version identifier
  Internal Version: version identifier
  Revision:     revision identifier
Network Interfaces:
  name          mode          address
  ----          -
  eth0          dhcp          10.x.x.123    address
Network Routes:
  prefix        netmask       gateway
  -----
  default       0.0.0.0       10.x.x.1
  10.x.x.0      address
DNS Configuration
  DNS Servers:  10.x.x.91
Appliance Configuration
Status:        Not Configured
Endpoint:      NA
```

5. If the IP address is dynamically assigned, then skip to [step 8](#). To statically set the IP address and netmask, type the following commands.

Note

If you have multiple networks, you must type the following commands for each network that is listed in the `status` command output.

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

For example:

```
net config eth0 xx.x.xx.xxx netmask 0.0.0.0
```

---

**6. Manually add the gateway by typing these commands.**

---

**Note**

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 xx.x.xx.x
```

---

**7. To manually set the DNS, type these commands:**

---

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

For example:

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

---

**8. (Mandatory) To set the Fully Qualified Domain Name (FQDN), type the following command:**

---

```
fqdn servername.yourcompanydomain
```

Consider the following:

- Custom *FQDN\_name* names are not supported.
- The *FQDN\_name* must be in lowercase.
- The *FQDN\_name* must not include the underscore character (`_`).

For example:

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

---

**Note**

You must set the FQDN to access the On-Prem CloudBoost Management Console.

---

9. To verify the networking setup and to see the status of the appliance, type the following command:

```
status
```

**Results**

After you have verified the system's basic networking settings, configure CloudBoost by using the On-Prem CloudBoost Management Console.

---

**Note**

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

---





# CHAPTER 4

## Deploying the CloudBoost Appliance with Microsoft Azure Resource Manager

Use the procedures in this section to deploy a CloudBoost appliance with Microsoft Azure Resource Manager (ARM).

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| • <a href="#">Integrate the CloudBoost appliance with Microsoft Azure</a> ..... | 34 |
| • <a href="#">Download the VHD files and JSON template</a> .....                | 34 |
| • <a href="#">Configure and deploy the CloudBoost appliance</a> .....           | 34 |
| • <a href="#">Start the CloudBoost virtual machine</a> .....                    | 41 |
| • <a href="#">Set the FQDN</a> .....                                            | 41 |
| • <a href="#">Check the Microsoft Azure audit logs</a> .....                    | 42 |
| • <a href="#">Verify network setup and status of the appliance</a> .....        | 42 |

## Integrate the CloudBoost appliance with Microsoft Azure

Integrating the CloudBoost appliance with the Microsoft Azure cloud platform employs Microsoft Azure low-cost blob storage to provide deduplication at the source, which minimizes bandwidth and storage consumption.

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

## Download the VHD files and JSON template

Network bandwidth and large file sizes might cause the VHD and JSON file download to be time-consuming.

### Procedure

1. Download the CloudBoost appliance from Online Support at <https://support.emc.com>.
2. Extract the files from the downloaded Zip file.

---

### Note

7zip was used to zip these files. To download the files, you might need to install a 7zip compatible extractor.

---

The Zip file contains the following files:

- Virtual Root Hard Disk (VHD) Zip file:  
`./installer/target/azure/root.vhd`  
The root VHD file is approximately 3 GB. As a sparse file, the root VHD file is 50 GB.
- lvm VHD Zip file:  
`./installer/target/azure/lvm.vhd`  
The lvm VHD is approximately 50 MB. As a sparse file, the lvm VHD is 40 GB.
- JSON Zip file:  
`./management/mgt_console/resources/scripts/autobuild/azuredeploy.json`
- MD5 check sums for the root VHD and lvm VHD files:  
`./installer/target/azure/azure_discs_md5sum.txt`

## Configure and deploy the CloudBoost appliance

You can use either the Microsoft CLI or Azure PowerShell to configure and deploy the CloudBoost appliance.

## Use the Azure PowerShell to configure Microsoft Azure for the CloudBoost appliance

### Before you begin

The following software and permissions are required:

- Microsoft Azure PowerShell
- Microsoft Azure account
- Azure subscription

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

### Procedure

1. Start Microsoft Azure PowerShell.
2. Type the following command:

```
Add-AzureAccount
```

3. Type the following command:

```
Select-AzureSubscription -SubscriptionName subscription-name
```

where *subscription-name* is the Microsoft Azure subscription account.

4. Respond to the following prompts:

```
$storage_account_name = account_name
```

```
$rg_name = resourcegroup_name
```

```
$storage_account_key = account_key
```

where:

- *account\_name* is the name of the Microsoft Azure subscription account.
- *resourcegroup\_name* is name of the resource group.
- *account\_key* is the Microsoft Azure account key.

5. To deploy the CloudBoost virtual machine, use the following template:

```
New-AzureRmResourceGroupDeployment -<resourcegroup_name>
$rg_name -<template_file> ./azure.json
```

where:

- *<resourcegroup\_name>* is name of the resource group.
- *<template\_file>* is the name of the Microsoft Azure template file.

## Use the Azure CLI to configure the CloudBoost appliance

Follow these steps to configure the CloudBoost appliance by using the Azure CLI.

## Configure Microsoft Azure for the CloudBoost appliance by using the Azure CLI

### Before you begin

The following software and permissions are required:

- Microsoft Azure account
- Azure CLI tools
- Azure utilities
- Go tools
- Git software

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

### Procedure

1. Authenticate Azure with the account.

- a. Open the Azure CLI, and then type the following command:

```
azure login
```

A device code appears with a link to the **Microsoft Azure Device Login** page.

- b. To open the **Microsoft Azure Device Login** page, click the link.

- c. In the **Code** field, type the device code.

2. In the Azure Resource Manager, perform the following steps:

- a. Create or use a storage account with the following properties:

- Deployment Model—Resource Manager
- Account Kind—General Purpose
- Replication—Select any type except ZRS.

- b. Set the deployment mode to Resource Mode. Type the following command:

```
azure config mode arm
```

3. In the Azure Resource Manager, 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 in the storage account.

4. At the Azure CLI, retrieve the Azure storage account information.

- To list the storage account name, type, location, and resource group, type the following command:

```
azure storage account list
```

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

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

5. Export or set the following environment variables that the Azure CLI will use. The procedure differs for Linux and Windows operating systems.

- On a Linux system, type the following commands:

```
export AZURE_STORAGE_ACCOUNT=<storage_account_name>
```

```
export AZURE_STORAGE_ACCESS_KEY=<primary_access_key>
```

---

#### Note

On a Linux OS, you can add these environment variables to the `.bashrc` file so you do not need to export the variables each time that you want to use them.

---

- On a Windows system, type the following commands:

```
set AZURE_STORAGE_ACCOUNT=<storage_account_name>
```

```
set AZURE_STORAGE_ACCESS_KEY=<primary_access_key>
```

## Methods for uploading the VHD files

You can use either the `azure-vhd-utils` Go tool or the Microsoft Azure CLI template to upload the VHD files to the Microsoft Azure storage account.

Uploading the files with the `azure-vhd-utils` Go tool is significantly faster than using the Microsoft Azure CLI template.

### Upload the .vhd files (azure-vhd-utils Go tool)

Upload the .vhd files by using the `azure-vhd-utils` Go tool that Microsoft provides.

#### Procedure

1. Install the latest version of the Go programming language software, which is available at the following link:  
<https://golang.org/dl/>
2. If required, install git.  
The git software is available at the following link: <https://git-scm.com/downloads>
3. Export or set the following PATH and GOPATH environment variables that the Azure CLI template will use. The procedure differs for Linux and Windows operating systems:

- On a Linux system, type the following commands:

```
export PATH=<Paths>;C:\Go\bin
```

```
export GOPATH=<GO_PATH>
```

---

#### Note

On Linux, you can add these environment variables to the `.bashrc` file, so you do not have to export the variables each time that you want to use them.

---

- On a Windows system, type the following commands:

```
set PATH=<Paths>;C:\Go\bin
```

```
set GOPATH=<GO_PATH>
```

The following site provides detailed information: <https://golang.org/doc/code.html#GOPATH>

4. Export or set the following environment variables that the Azure CLI template will use.

The procedure differs for Linux and Windows operating systems:

- On a Linux system, type the following commands:

```
export AZURE_STORAGE_ACCOUNT=<storage_account_name>
```

```
export AZURE_STORAGE_ACCESS_KEY=<storage_account_key>
```

where:

- `<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.
- 

#### Note

On Linux, you can add these environment variables to the `.bashrc` file, so you do not have to export the variables each time that you want to use them.

---

- On a Windows system, type the following commands:

```
set AZURE_STORAGE_ACCOUNT=<storage_account_name>
```

```
set AZURE_STORAGE_ACCESS_KEY=<storage_account_key>
```

where:

- `<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.

5. To get the Microsoft Azure utilities, type the following command:

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

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

```
azure-vhd-utils upload --localvhdpath <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 to the root VHD file.
- `<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.
- `<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.

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

```
azure-vhd-utils upload --localvhdpath <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 to the LVM VHD file.
- `<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.
- `<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 .vhd files (Microsoft Azure CLI template)

The CLI template method can take several hours to upload the VHD files to the Microsoft Azure storage account. The azure-vhd-utils Go tool method can take less than an hour to upload the VHD files.

---

### Note

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

---

### Procedure

1. Open the command prompt.
2. Upload the root and lvm VHDs to the storage account by typing the following command:

```
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-18.0.0.0-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-18.0.0-azure-root.vhd to
blob test-azure-root.vhd in container vhds
Percentage: 7.92% (3.69GB/50.00GB)
Average Speed: 1.86MB/S
Elapsed Time: 00:33:51 11
```

## Deploy the CloudBoost virtual machine with the JSON template

Deploy the CloudBoost virtual machine in Microsoft Azure by using the `azuredeploy.json` file that you downloaded from the Online Support at <https://support.emc.com>.

### Procedure

1. Deploy the CloudBoost virtual machine in Microsoft Azure. At the command prompt, type the following command:

```
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 deploys the virtual machine.



2. At the command prompt, type the following information:
  - For **vmName**, specify a unique name for the virtual machine.
  - For **storageAccountName**, specify the storage account name to associate with the virtual machine.
  - For **osDiskVhdUri**, type the destination URL of the following blob:  
`<URL_to_VHD_Azure_blob>/CloudBoost-18.0.0.0-azure-<root|lvm>.vhd`
  - For **metaDiskVhdUri**, type the destination URL of the following blob:  
`<URL_to_VHD_Azure_blob>/CloudBoost-18.0.0.0-azure-<root|lvm>.vhd`
3. To comply with the virtual machine size and location standards, adjust the JSON file. For detailed information about Azure virtual machine size, refer to the following Microsoft documentation:  
<https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-sizes>

## Start the CloudBoost virtual machine

### Procedure

1. Log in to Microsoft Azure.
2. Select and open the CloudBoost appliance.
3. Connect to the CloudBoost appliance using either of the following methods:
  - Use an SSH client.
  - Log in through a browser.

The CloudBoost CLI appears.

4. Authenticate with the default password, `password`.
5. Set a new administrator password.

## Set the FQDN

### Procedure

1. Open the Azure CLI.
2. Log in to Microsoft Azure.
3. Select and open the CloudBoost appliance.  
 The CloudBoost CLI appears.
4. Authenticate with the new, previously set, administration password.
5. Set the FQDN. At the command prompt, typing the following command:

```
fqdn <FQDN_name>
```

Consider the following:

- Ensure that the *FQDN\_name* is the same name as the DNS Label Name that Microsoft Azure provides.
- Custom *FQDN\_name* names are not supported.
- The *FQDN\_name* must be in lowercase letters.
- The *FQDN\_name* must not include the underscore character (\_).

## Check the Microsoft Azure audit logs

To check the Microsoft Azure audit logs, at the command prompt, type the following command:

```
azure group log show <resource_group> deployment
```

where *<resource\_group>* is the name of the resource group that was used to deploy the virtual machine.

## Verify network setup and status of the appliance

### Procedure

1. To configure network settings for the CloudBoost appliance, see [Configuring Network Settings for a CloudBoost Appliance](#) on page 49.
2. To verify the network setup and see the status of the appliance, type the following command:

```
status
```

For example:

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

eth0 dhcp 10.x.x.123 address

Network Routes:
 prefix netmask gateway

default 0.0.0.0 10.x.x.1
10.x.x.0 address *
```

DNS Configuration  
DNS Servers: 10.x.x.91  
Appliance Configuration

|           |                |
|-----------|----------------|
| Status:   | Not Configured |
| Endpoint: | NA             |

3. Configure the CloudBoost appliance, see [Configuring a New CloudBoost Appliance](#) on page 55.
4. To configure NetWorker with the CloudBoost appliance, see [Configuring NetWorker with a CloudBoost appliance](#) on page 61.



# CHAPTER 5

## Deploying the CloudBoost Appliance in Amazon EC2

This chapter includes the following topics:

- [Deploy the virtual CloudBoost appliance in Amazon EC2](#).....46
- [Start the CloudBoost virtual machine](#).....47
- [Set the FQDN](#).....47
- [Verify network setup and status of the appliance](#).....48

# Deploy the virtual CloudBoost appliance in Amazon EC2

## Before you begin

Ensure that Licensing has made the Amazon Machine Image (AMI) for the CloudBoost appliance available.

## Procedure

1. Log in to the Amazon Web Services console.
2. Click **EC2**.

For more information about supported regions, see [Supported Regions](#) on page 18

3. Under **Images**, perform the following steps:
  - a. Select **AMIs**.
  - b. Click **Owned by me** and then, select **Private Images** from the list box.
  - c. Select **Private images**.
  - d. Click the CloudBoost image.

4. Under **Instance Type**, select an instance type that exceeds the following minimum requirements:

- 4 CPUs
- 16 GB of memory

For more information about system requirement, see [Virtual CloudBoost appliance requirements \(Amazon Web Services EC2\)](#) on page 23

It is recommended that you use `m4.xlarge`.

5. Under **Configure Instance Details**, perform the following steps:
  - a. Type the number of instances to create.
  - b. Select the network and submask.
  - c. Select **Auto-assign Public IP**.

6. Under **Add Storage** for the **Root** section:

- a. Set **Size (GB)** to at least 50.

The default size for the added volume is 40 GB. Increase 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 10 keys to assist with AMI management and identification.

8. Under **Configure Security Group**:

- a. To allow or deny public access, select an existing security group. Security groups 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. You use this key to connect to the CloudBoost appliance.
11. Click **Launch instances**.
12. Before you can connect to the CloudBoost appliance, you must download the private key.

---

#### Note

Save the private key in a secure and accessible location. After the private key is created, you will be unable to download the private key again.

---

The CloudBoost appliance starts in Amazon EC2.

## Start the CloudBoost virtual machine

### Procedure

1. Log in to Amazon EC2.
2. Select the CloudBoost appliance, and then click **Connect**.
3. In the **Connect To Your Instance** wizard, connect with an SSH client.
4. Log in to the SSH terminal:

To log in to the SSH terminal as the Admin user, type the following command:

```
ssh -i "cloudboost_aws.pem" admin@ AWS FQDN_name or IP
```

Consider the following:

- Custom *FQDN\_name* names are not supported.
  - The *FQDN\_name* must be in lowercase.
  - The *FQDN\_name* must not include the underscore character (\_).
- 

#### Note

It is best practice to keep the DHCP configuration options that Amazon supplied.

---

5. Select and open the CloudBoost appliance.  
The CloudBoost CLI appears.
6. Authenticate with the default password, `password`.
7. Set the new administrator password.

## Set the FQDN

### Procedure

1. Connect to the CloudBoost CLI.
2. Authenticate with the new administrator password that you configured in the previous step.

3. Set the FQDN by typing the following command:

```
fqdn <FQDN_name>
```

Consider the following:

- Custom *FQDN\_name* names are not supported.
- The *FQDN\_name* must be in lowercase.
- The *FQDN\_name* must not include the underscore character (\_).

## Verify network setup and status of the appliance

### Procedure

1. To configure network settings for the CloudBoost appliance, see [Configuring Network Settings for a CloudBoost Appliance](#) on page 49.
2. To verify the network setup and see the status of the appliance, type the following command:

```
status
```

For example:

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

 eth0 dhcp 10.x.x.123 address

Network Routes:
 prefix netmask gateway
 ----- ----- -----
 default 0.0.0.0 10.x.x.1
 10.x.x.0 address *
DNS Configuration
 DNS Servers: 10.x.x.91
Appliance Configuration
Status: Not Configured
Endpoint: NA
```

3. Configure the CloudBoost appliance, see [Configuring a New CloudBoost Appliance](#) on page 55.
4. To configure NetWorker with the CloudBoost appliance, see [Configuring NetWorker with a CloudBoost appliance](#) on page 61.



# CHAPTER 6

## Configuring Network Settings for a CloudBoost Appliance

This section includes the following topics:

- [Network settings for a CloudBoost appliance](#) ..... 50
- [Configure network settings for a CloudBoost appliance](#).....50
- [Configure CloudBoost to use a proxy](#) ..... 52

## Network settings for a CloudBoost appliance

You must provide basic network settings information for a CloudBoost appliance at the CLI and complete initial configuration in the On-Prem CloudBoost Management Console.

### Note

In AWS, the CloudBoost AMI automatically uses the default VPC settings for the appliance IP address, DNS, and FQDN.

## Configure network settings for a CloudBoost appliance

### Procedure

1. Connect to the CloudBoost CLI.
2. Authenticate with the default password, `password`.
3. Set the new administrator password.
4. To see the current network configuration of the appliance, type the following command.

```
status
```

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

eth0 dhcp 10.x.x.123 address

Network Routes:
 prefix netmask gateway

default 0.0.0.0 10.x.x.1
10.x.x.0 address *
```

```
DNS Configuration
 DNS Servers: 10.x.x.91
Appliance Configuration
Status: Not Configured
Endpoint: NA
```

5. If the IP address is dynamically assigned, then skip to [step 8](#). To statically set the IP address and netmask, type the following commands.

---

**Note**

If you have multiple networks, you must type the following commands for each network that is listed in the `status` command output.

---

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

For example:

```
net config eth0 xx.x.xx.xxx netmask 0.0.0.0
```

6. Manually add the gateway by typing these commands.

Note

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 xx.x.xx.x
```

7. To manually set the DNS, type these commands:

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

For example:

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

8. (Mandatory) To set the Fully Qualified Domain Name (FQDN), type the following command:

```
fqdn servername.yourcompanydomain
```

Consider the following:

- Custom *FQDN_name* names are not supported.
- The *FQDN_name* must be in lowercase.
- The *FQDN_name* must not include the underscore character (`_`).

For example:

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

Note

You must set the FQDN to access the On-Prem CloudBoost Management Console.

9. To verify the networking setup and to see the status of the appliance, type the following command:

```
status
```

Results

After you have verified the system's basic networking settings, configure CloudBoost by using the On-Prem CloudBoost Management Console.

Note

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

Configure CloudBoost to use a proxy

CloudBoost can be configured to use a proxy to communicate with the On-Prem CloudBoost Management Console.

Do not route outbound http traffic from the CloudBoost appliance through a proxy because it can create a performance bottleneck. In environments where outbound http traffic is restricted, create an exception for the appliance in the firewall after you consult with the IT security team.

In a private cloud environment, excludes are used when the CloudBoost appliance is in a proxy or isolated network. In this scenario, the IP of the private cloud is excluded. Each time that you run the `http-proxy` command, you override an earlier setting for excludes.

Procedure

1. Connect to the CloudBoost CLI.
2. Authenticate with the administrator password.
3. Check the status of the CloudBoost appliance by typing the following command:

```
status
```

If a proxy is set, this command displays and lists what is excluded.

4. To remove the current proxy configuration, type the following command:

```
http-proxy reset
```

Use this command to clear the last proxy setting and excludes

5. To add a proxy exclude, type the following command:

```
http-proxy <IP>:<port> exclude <prefix>/<mask>
```

where:

- `<IP>` is the IP address of the proxy server.

- *<port>* is the port number of the proxy server.
- *<prefix>* is the range of the source IP addresses for which you want to bypass the proxy.
- *<mask>* specifies the size of the range that is identified by the prefix.

For example, this command sets the proxy to 10.8.196.10:3128 and excludes 10.8.*.*. Note that (*) is 0–255:

```
http-proxy 10.8.196.10:3128 exclude 10.8.0.0/16
```

6. To add exceptions for multiple exclusions, type the following command:

```
http-proxy <IP>:<Port> exclude <prefix>/<mask>,<prefix>/  
<mask>,...
```

where:

- *<IP>* is the IP address of the proxy server.
- *<port>* is the port number of the proxy server.
- *<prefix>* is the range of the source IP addresses for which you want to bypass the proxy.
- *<mask>* specifies the size of the range that is identified by the prefix.

For example, this command sets the proxy to 10.8.196.10:3128 and excludes 192.8.*.*.* and 100.9.22.24. Note that (*) is 0–255:

```
http-proxy 10.8.196.10:3128 exclude  
192.0.0.0/8,10.10.0.0/16,10.9.22.24/32
```


CHAPTER 7

Configuring a New CloudBoost Appliance

After you install a CloudBoost appliance and configure it at the CLI and complete its configuration in the On-Prem CloudBoost Management Console. You must create a cloud profile for the storage provider that the appliance will use before you can complete its configuration.

- [Create and manage cloud profile for CloudBoost appliance](#)..... 56
- [Validate cloud storage credentials](#)..... 57
- [Enable remote client mounts](#)..... 58
- [Configuring a new CloudBoost appliance](#)..... 58
- [Editing CloudBoost appliance configurations](#)..... 60

Create and manage cloud profile for CloudBoost appliance

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

Cloud profiles

Before you configure a CloudBoost appliance in the On-Prem CloudBoost Management Console, create a cloud profile for the storage that the appliance will use.

Create a cloud profile

Before you configure a CloudBoost appliance in the On-Prem CloudBoost Management Console, create a cloud profile for the storage the appliance uses.

Before you begin

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

Procedure

1. Use a web browser and sign in to the On-Prem CloudBoost Management Console as the administrator. Type the On-Prem CloudBoost Management Console address in the following format:

`https://<FQDN of the appliance>:7443`

Note

- The username is admin and use the password that you updated during deployment of CloudBoost.
-

2. In the left menu, click **Cloud Profiles**.

The **Cloud Profiles** page opens.

3. 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**.

Edit a cloud profile

Procedure

1. From the **On-Prem CloudBoost Management Console**, open the **Cloud Profiles** page.
2. 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**.

Validate cloud storage credentials

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

Before you begin

- Configure the CloudBoost appliance with a valid cloud storage provider.
- The NTP must be configured.

Note

If the date and time of the ESX host, CloudBoost virtual machine and object store are out of sync, then the validation fails. You can sync these to a specific time in the same zone or to an NTP.

Procedure

1. Connect to the CloudBoost CLI.
2. To see a list of valid cloud profiles, type the following command:

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

Note

The quotation marks are required.

The result should be similar to the following output, but with a list of available cloud profiles.

```
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 against the listed profiles, type the following command:

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

Note

The quotation marks are required.

The "1" represents the cloud profile to validate as listed in the result of Step 2.

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=s3
--identity=111111@example
```

```
--credential=1234ABCDE/xyz=
--endpoint=https://s3.ecs-fqdn.com validate
```

Enable remote client mounts

When you enable remote client mounts, you create the password that you must use for the task. Share the admin username and new password with anyone who needs to remotely mount with the client.

Procedure

1. Open a CLI window for the appliance.
2. Log in with the admin username and password.
3. Type the following command, where the value for *password* is the password that you created.

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

Configuring a new CloudBoost appliance

After you provide basic network information at the CLI, you must use a web browser to finish configuration in the On-Prem CloudBoost Management Console. You can change certain configuration information for an appliance after the initial configuration.

Before you begin

Define a cloud profile for use with this appliance.

Procedure

1. Use a web browser and sign in to the On-Prem CloudBoost Management Console as the administrator. Type the On-Prem CloudBoost Management Console address in the following format:

```
https://<FQDN of the appliance>:7443
```

Note

Only the administrator can log into the On-Prem CloudBoost Management Console.

2. In the left menu, click **CloudBoost Appliances**.
The **Appliances** page opens.
3. Click **CloudBoost Appliances**, click the appliance that you want to configure.
4. To change the display name for this appliance from the default FQDN that you set in the CLI, in the **Name** field, type the new display name.
5. To minimize clock drift:
 - a. Select **Enable NTP**.
 - b. Type the hostname or IP address for at least one NTP server.

Consider the following:

- Use the NTP details of the host system on which NetWorker server is installed.
- You can specify multiple servers to provide redundancy in case one or more time servers are unavailable. However, the NTP server validation is done only for one NTP server.
- If the NTP is not enabled, then the CloudBoost appliance inherits the time zone from the host ESXi server.

6. 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.

7. 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. Only this method of asymmetric key creation is supported for the CloudBoost appliance.
 - c. From the output file that is a result of step b, copy the entire public key and paste it into the text box below the instructions on the **Configure** tab.
 - d. From the output file that is a result of step b, copy the entire private key and paste it somewhere safe. If you created a pass phrase, copy that as well.
-

Note

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.

8. Review the selections and click **Save** to save these settings for the appliance. CloudBoost is configured.
9. Download the recovery metadata and the private key.
-

Note

- a. After editing the initial configurations, you must safely store the recovery files. They must be provided during a Disaster Recovery. Appliances that are backed up cannot be recovered without the private key and recovery metadata.
 - b. After you acknowledge, the recovery metadata file and private key will be purged from the CloudBoost. If you do not acknowledge, the file will be available for download in the **Pending Action**.
-

Editing CloudBoost appliance configurations

You can change certain configuration information for an appliance after the initial configuration.

Procedure

1. Use a web browser and sign in to the On-Prem CloudBoost Management Console as the administrator. Type the On-Prem CloudBoost Management Console address in the following format:

`https://<FQDN of the appliance>:7443`

Note

Only the administrator can log into the On-Prem CloudBoost Management Console.

2. In the left menu, click **CloudBoost Appliances**.

The **Appliances** page opens.

3. Click **Edit**
-

Note

You can edit only the NTP server field and the backup frequency.

4. Review the changes and click **Save** to save these settings for the appliance. CloudBoost is configured.
 5. Download the recovery metadata and the private key.
-

Note

- a. You must safely store the recovery metadata and the private key. They must be provided during a Disaster Recovery. Appliances that are backed up cannot be recovered without the private key and recovery metadata.
 - b. After you acknowledge, the recovery metadata file and private key is purged from the CloudBoost. If you do not acknowledge, the file will be available for download in the **Pending Action**.
-

CHAPTER 8

Configuring NetWorker with a CloudBoost appliance

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

The CloudBoost appliance has an embedded storage node which can be used with the NetWorker server. However, it is recommended that you install the NetWorker storage node on a separate Linux or Windows server and do not use the embedded NetWorker storage node on the CloudBoost appliance.

- [Configure a CloudBoost device by using an embedded NetWorker storage node](#)62
- [Configure a CloudBoost device on an external storage node](#).....65
- [Troubleshoot CloudBoost device configuration issues](#).....70
- [Report information on cloud backup](#).....73

Configure a CloudBoost device by using an embedded NetWorker storage node



To configure a CloudBoost device to receive backup or clone data, perform the following steps.

You do not require an external storage node when you back up Linux and Windows hosts by using Client Direct.

Procedure

1. In the **NetWorker Administration** interface
 - a. Click **View > Diagnostic Mode**.
 - b. Ensure that NetWorker **Client Direct** is selected.
Client Direct backups are enabled by default.
2. If remote client mounts are not configured, on the CloudBoost appliance, enable remote client mounts, and then 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.
3. Log in to the NMC GUI as an administrator of the NetWorker server.
4. On the taskbar, click the **Enterprise** icon .
5. In the navigation tree, highlight a host:
 - a. Right-click **NetWorker**.
 - b. Select **Launch Application**. The **NetWorker Administration** window appears.
6. On the taskbar, click the **Devices** button .
7. In the expanded left navigation pane:
 - a. Right-click **CloudBoost Appliances**.
 - b. Select **New Device Wizard**.
8. On the **Select the Device Type** page, select **CloudBoost**, and then click **Next**.
9. Review the **CloudBoost Preconfiguration Checklist** page, and then click **Next**.
10. On the **CloudBoost Configuration Options** page, perform the following tasks:
 - a. In the **CloudBoost Storage** group box:
 - a. Select **Use Embedded Storage Node**.
 - b. Select an embedded 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 then type a descriptive name.
- c. In the **Hostname (FQDN)** field, type 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 the file system on the CloudBoost appliance that NetWorker uses as the target data device:

Figure 5 Device Configuration Wizard: CloudBoost Configuration Options

CloudBoost Configuration Options

Specify the configuration options and the login credentials for the CloudBoost appliance.
Ensure that the NetWorker server can resolve hostname of the CloudBoost appliance.

CloudBoost Storage

☒ Use Embedded Storage
Default storage node of the Cloud Boost Appliance will be used.

☐ Use External Storage Node

CloudBoost Appliance

☒ Use an existing CloudBoost Appliance
ip-10-13-144-31.us-west-1.compute.internal

☐ Create new CloudBoost Appliance

CloudBoost Attributes

Hostname (FQDN): ip-10-13-144-31.us-west-1.compute.internal

CloudBoost Credentials

User name: remotebackup

Password:

Configuration Method

☒ Browse & Select (Recommended)
Browse the CloudBoost file system and select folders that NetWorker will use as a target device.

☐ Manual
Manually specify the path, in the `/mnt/magfs` directory, that NetWorker will use as a target device.

NetWorker automatically creates the storage node for the CloudBoost appliance during the device creation process.

- a. Select **Browse & Select**.
The **Browse and Select the CloudBoost Device Path** CloudBoost window appears.
- b. In the `/mnt/magfs/base` directory, create a folder with write access enabled. Use a unique name.
For example: `/mnt/magfs/base/CB01`

The CloudBoost appliance creates a share on `/mnt/magfs/base`. The NetWorker software requires that each CloudBoost device has a unique, customer named, folder.

Note

You cannot create folders outside of the `/mnt/magfs/base` directory.

- c. Select the folder that you just created.

NetWorker validates the CloudBoost username and password that you specified. NetWorker also updates the **NetWorker Device Name** and **Storage Path** fields with the information.

g. Click **Next**.

Figure 6 Device Configuration Wizard: Browse and Select the CloudBoost Device Path

The screenshot shows a file browser interface for selecting a storage path. At the top, there are buttons for 'New Folder' and 'Remove Folder'. The file tree shows a path: 'ip-10-13-144-31.us-west-1.compute.internal/mnt/magfs' containing a folder 'base', which contains a folder 'CloudBoost_Device_1'. Below the file tree, there is a table with two columns: 'NetWorker Device Name' and 'Storage Path'. The table contains one entry: 'ip-10-13-144-222.us-west-1.compute...' and 'base/CloudBoost_Device_1'. Below the table, there are two text input fields: 'NetWorker Device Name:' with the value 'ip-10-13-144-222.us-west-1.compute.internal:base/CloudBoost_Device_1' and 'Storage Path:' with the value 'base/CloudBoost_Device_1'. At the bottom right, there are '< Back' and 'Next >' buttons.

11. On the **CloudBoost Pool Configuration** page, perform the following steps:

Note

For detailed information about NetWorker media pools, refer to the *NetWorker Administration Guide*.

- a. Ensure that **Configure Media Pools for devices** option is selected.
- 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 type 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.

- e. Ensure that **Label and Mount device after creation** is selected.
- f. Click **Next**.

Figure 7 Device Configuration Wizard: Configure the CloudBoost Pool

Storage Path	NetWorker Device Name	Pool Type	Pool	Label
base/CloudBoost_De...	ip-10-13-144-222.us-west-1.com...	Backup	ip101314431uswest1...	✓

Pool Type

☒ Backup
☐ Backup Clone

Pool

☒ Create and use a new Pool
☐ Use an existing Pool

ip101314431uswest1computeinternal

Pool1

☒ Label and Mount device after creation

12. On the **Review the Device Configuration** page:
 - a. Review the settings.
 - b. Click **Configure**.
13. On the **Check results** page:
 - a. Review whether the devices were successfully configured or if any messages appeared.
 - b. Click **Finish**.
 - c. To change any of the settings, click **Back** to the correct wizard page.


After you finish


If the Device Configuration wizard does not create a CloudBoost device, manually create an embedded storage node that corresponds to the embedded storage node that you created with the wizard. After the nsrsnmd daemon starts on the CloudBoost appliance, create a CloudBoost device.

Configure a CloudBoost device on an external storage node

For large scale deployments, the recommendation is to use an external storage node.

Procedure

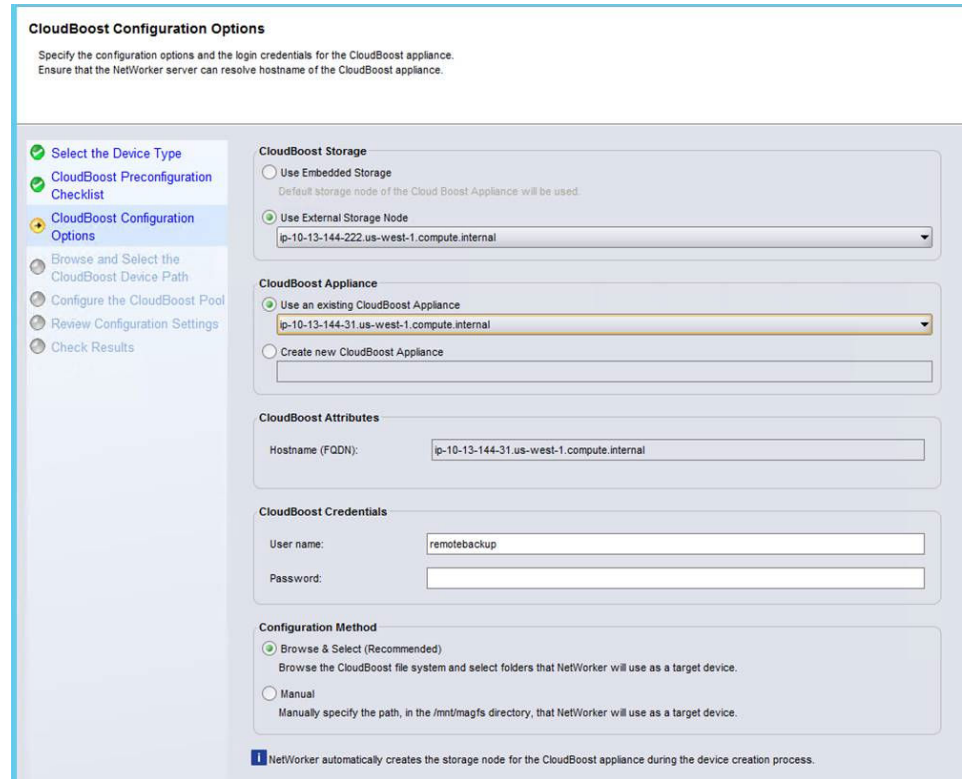
1. In the NetWorker Administration interface, click **View > Diagnostic Mode**, and ensure that **NetWorker Client Direct** is selected.
 Client Direct backups are enabled by default.
2. Log in to the NMC GUI as an administrator of the NetWorker server.
3. On the taskbar, click the **Enterprise** icon .
4. In the navigation tree, highlight a host:
 - a. Right-click **NetWorker**.
 - b. Select **Launch Application**. The **NetWorker Administration** window appears.

5. Create a storage node:
 - a. From the navigation tree, right-click **Storage Nodes** and select **New**.
The **Create Storage Node** windows appear with the **General** tab displayed.
 - b. Set the **Identity** attributes:
 - a. In the **Name** field, specify the hostname of the NetWorker storage node.
 - b. In the **Type of Storage Node** field, select **SCSI**.
 - c. In the **Status** attributes, review or set the storage node status:
 - **Storage node is configured** indicates that a device has been configured on this storage node.
 - **Enabled** indicates that the storage node is available for use:
 - **Yes** indicates an available state.
 - **No** indicates a service or disabled state. New device operations cannot begin and existing device operations might be canceled.
 - **Ready** indicates that the storage node is ready to accept device operations.
6. On the taskbar, click the **Devices** button .
7. Expand **Devices** in the left navigation pane:
 - a. Right-click the CloudBoost device.
 - b. Select **New Device Wizard**.
The **Device Configuration Wizard** window appears.
8. On the **Select the Device Type** page:
 - a. Select **CloudBoost**.
 - b. Click **Next**.
9. Review the **CloudBoost Preconfiguration Checklist** page, and then click **Next**.
10. On the **CloudBoost Configuration Options** page, perform the following tasks:
 - 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 the **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** page appears.

Figure 8 Device Configuration Wizard: CloudBoost Configuration Options



11. On the **Browse and Select the CloudBoost Device Path** page, 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. Use a unique name.

For example: `/mnt/magfs/base/CB01`

Configure the CloudBoost appliance to cloud profile, the CloudBoost appliance creates a share on `/mnt/magfs/base`. The NetWorker software requires that each CloudBoost device has a unique, customer named, folder.

Note

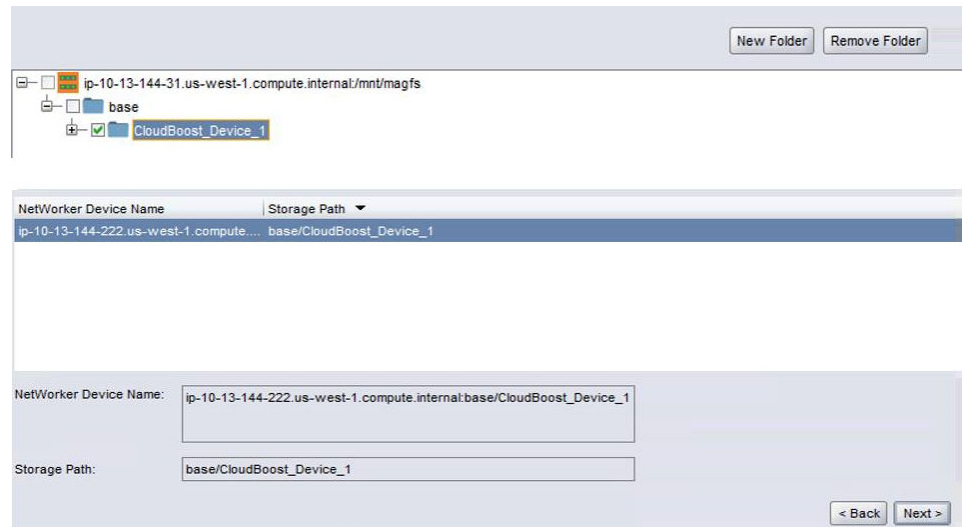
You cannot create folders outside of the `/mnt/magfs/base` directory.

- 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.

- e. Click **Next**.

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

12. On the **Configure the CloudBoost Pool** page, perform the following steps:

Note

For detailed information about NetWorker media pools, refer to the *NetWorker Administration Guide*.

- a. Ensure that the **Configure Media Pools for devices** is selected.
- 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 **Label and Mount device after creation** selected.
- f. Click **Next**.

Figure 10 Device Configuration Wizard: Configure the CloudBoost Pool

☒ Configure Media Pools for devices

Storage Path	NetWorker Device Name	Pool Type	Pool	Label
base/CloudBoost_De...	ip-10-13-144-222.us-west-1.com...	Backup	ip101314431uswest1...	✓

Pool Type

☒ Backup
☐ Backup Clone

Pool

☒ Create and use a new Pool
☐ Use an existing Pool

ip101314431uswest1computeinternal

Pool1

☒ Label and Mount device after creation

13. Review the configuration settings, and then click **Next**.
14. On the **Check Results** page, check and verify that the device configuration was successful.

Figure 11 Device Configuration Wizard: Check Results Page

Device Configuration Results
Results of device configuration.

- Select the Device Type
- CloudBoost Preconfiguration Checklist
- CloudBoost Configuration Options
- Browse and Select the CloudBoost Device Path
- Configure the CloudBoost Pool
- Review Configuration Settings
- Check Results**

Adding new directory on Storage Node ip-10-13-144-31.us-west-1.compute.internal

New Directory: /mnt/magfs/base/CloudBoost_Device_1

Adding new CloudBoost Device "rd=ip-10-13-144-222.us-west-1.compute.internal:base/CloudBoost_Device_1"

CloudBoost Device Name: rd=ip-10-13-144-222.us-west-1.compute.internal:base/CloudBoost_Device_1
 Device Access Information: ip-10-13-144-31.us-west-1.compute.internal:base/CloudBoost_Device_1
 User Name: remotebackup
 Password: *****
 Hostname(FQDN): ip-10-13-144-31.us-west-1.compute.internal

Adding new Label Template "ip101314431uswest1computeinternal"

Label Template Name: ip101314431uswest1computeinternal

Adding new Pool "ip101314431uswest1computeinternal"

Pool Name: ip101314431uswest1computeinternal
 Pool Type: Backup
 Label Template: ip101314431uswest1computeinternal
 Devices: rd=ip-10-13-144-222.us-west-1.compute.internal:base/CloudBoost_Device_1

Labeling device "rd=ip-10-13-144-222.us-west-1.compute.internal:base/CloudBoost_Device_1"

Device Name: rd=ip-10-13-144-222.us-west-1.compute.internal:base/CloudBoost_Device_1
 Pool Name: ip101314431uswest1computeinternal

Results

After the CloudBoost device has been configured with the NetWorker external storage node, the following information displays:

- The **Name** field points to the NetWorker external storage node.
- The **Device access information** field points to the CloudBoost appliance.
- The media type is specified as **CloudBoost**.

Figure 12 Device information

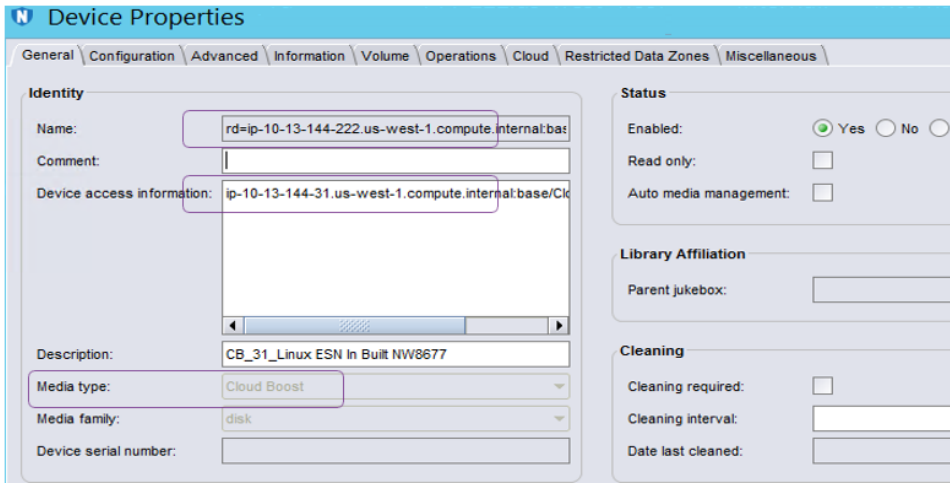
Devices

Showing: 0 of 0 items Clear All

Search name Search device access information Search volume name

Name	Device access information	Volume name
rd=ip-10-13-144-222.us-west-1.compute.i...	ip-10-13-144-31.us-west-1.compute.inte...	ip101314431uswest1compute...

Figure 13 Device properties



Troubleshoot 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.

Setting the configuration options for the CloudBoost SDK

You can set the configuration option for the CloudBoost SDK by creating the `nsrccbconfig` file to pass specific set of configuration option to CloudBoost library.

Procedure

1. Perform one of the following action sequences depending on the operating system:

Operating system	Procedure
Windows	<ol style="list-style-type: none">a. Open Notepad, and create the <code>nsrccbconfig</code> file with the configuration options.b. Save the file in <code><installation Directory>\Emc Networker\nsr\debug\</code> directory without an extension.
Linux	<ol style="list-style-type: none">a. Open the terminal.b. Create <code>nsrccbconfig</code> file without an extension in the <code>/nsr/debug/</code> directory and update the file with the configuration options.

You can add one or more configuration options from the following table.

Table 14 Configuration options

Configuration options	Description
v (lower case only)	Provides the capability of different log levels that ranges from 0-5. Greater the number, more the debug logs printed in <code>/nsr/logs/cloudboost/*</code>
maxLogFiles	Controls the number of log files that are retained in <code>/nsr/logs/cloudboost/</code> folder. The default value is 10. The maximum value is 50.
max_log_size	Limits the size of log files. When the value reaches the maximum file size, the files is zipped and the log continues in a new file. The default size of log file is 10 MB.
curlConnectTimeout	This is the timeout value for establishing connection to object store. This can be set to a higher value (in msec) if there are connection failures with an error message "BAD_NETWORK_PATH or Transfer error". The default value is 20000 msec.
cacheLocation	It is the directory where CloudBoost SDK stores the blob cache. You must create the directory incase if it does not exist. The default location is <code>/nsr/logs/cloudboost/</code> folder.
log_dir	It is the directory where the CloudBoost SDK writes log files. If it is not present, then you must create it. The default location is <code>/nsr/logs/cloudboost/</code> folder.

The following example creates a `nsrconfig` file in `/nsr/debug/nsrconfig` location.

```
[root@ip-xx-xx-xx-xx /]# cat /nsr/debug/nsrconfig
v=5
maxLogFiles=15
max_log_size=100
curlConnectTimeout=30000
```

Improve clone performance

For a new installation of NetWorker, the **Disable (RPS) Clone** attribute is selected by default. For NetWorker 9.0.1 and later, the **Disable (RPS) Clone** attribute is cleared by default. If you are upgrading to NetWorker 18.2, the **Disable (RPS) Clone** attribute keeps the previously assigned setting.

To improve clone performance, consider the following facts:

- For concurrent cloning workloads, select the **Disable (RPS) Clone** attribute.
- Ensure that the number of source and destination volumes match. This step avoids contention between the source and destination volumes and reduces the chances of clone failure.

To clear or select the **Disable (RPS) Clone** attribute, perform the following steps.

Procedure

1. Open the **Administration** window.

2. Right-click the NetWorker server name in the left pane.
3. Select **Properties**.
4. In the **Configuration** tab, clear or select the **Disable RPS Clone** attribute.

Cannot retrieve the version of the CloudBoost appliance

This error message appears when the NetWorker server cannot determine the version of NetWorker that is running on the CloudBoost appliance.

To resolve this issue, contact Technical Support for access to the CLI and ensure that the following criteria are met.

- The NetWorker daemon `nsrexecd` is started on the appliance:
 1. Log in to an SSH terminal with the Maginatics user account.
 2. Type the following command:


```
ps -ef | grep nsr
```
 3. Confirm that the `nsrexecd` process appears.
 4. If the `nsrexecd` daemon does not appear, type the following command to start the `nsrexecd` process on the appliance:


```
sudo service networker start
```
- 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"

If the NetWorker server and the CloudBoost appliance cannot communicate with each other, this error message appears.

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

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.

Note

For NetWorker 9.1.1 and later, the `/mnt/magfs/base` folder is validated when a CloudBoost device is created. You cannot create a device in a folder other than `/mnt/magfs/base`.

Unable to connect to the CloudBoost appliance: LOGON_FAILURE error

This error appears in the following scenarios:

- The password that is specified for the `remotebackup` user is incorrect.
- The `remotebackup` user does not exist on the CloudBoost appliance.

Adding a CloudBoost 2.2.2 appliance fails with an error “unable to resolve”

Perform the following steps to add a CloudBoost appliance 2.2.2 in the NetWorker server running on 18.0 or later in the absence of reverse DNS.

Procedure

1. Download the NetWorker client and storage node package for Linux from the Online Support website to a temporary location.
2. Stop the NetWorker process using the `nsr_shutdown` command.
3. Install the client and storage node by running the `dpkg` command: `dpkg -i package package..`

```
dpkg -i lgtoc1nt_18.0_amd64.deb lgtonode_18.0_amd64.deb
```

4. Start the NetWorker daemons by typing the following command:

Initialization system	Command
sysvinit	<code>/etc/init.d/networker start</code>
systemd	<code>systemctl start networker</code>

5. Add the CloudBoost appliance using the NetWorker character-based interface (nsradmin) and then, label and mount the appliance.

Report information on cloud backup

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

Cloud backup information can be obtained from the following sources:

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

CHAPTER 9

Perform a CloudBoost Appliance Recovery

This section includes the following topic:

- [Recovering CloudBoost Appliance](#) 76

Recovering CloudBoost Appliance

You can recover the CloudBoost appliance by using the recovery metadata and private key.

Before you begin

1. You must have the recovery metadata and the private key.
2. The recovery target appliance must be running the same version of the CloudBoost software as that of the failed appliance

Procedure

1. Deploy a second CloudBoost appliance to restore the metadata from backups that are stored in the cloud.
2. Connect to CloudBoost through CLI and validate whether the date and time are in sync between the ESX server, CloudBoost virtual machine and the object store.
3. Use a web browser to sign in to the On-Prem CloudBoost Management Portal.
4. In the left menu, click **Appliance Recovery**.
5. Upload the metadata file and the private key and click **Preview**
6. Review the recovery information and click **Start Recovery**.

After you finish

In the left menu, click CloudBoost Appliance and validate the configurations.

CHAPTER 10

Monitoring, Managing, and Supporting a CloudBoost Appliance

This section includes the following topics:

- [Monitoring CloudBoost](#) 78
- [Upgrade a CloudBoost appliance](#) 78
- [CloudBoost integration with EMC Secure Remote Services](#) 79
- [Register CloudBoost with EMC Secure Remote Services](#) 80
- [Configuring average chunk size](#) 81
- [Specifications for the chunk size setting](#) 81

Monitoring CloudBoost

CloudBoost is integrated with EMC Secure Remote Services (ESRS), which can be enabled to monitor the health of the appliances. If CloudBoost appliances are not registered with ESRS, you must monitor health, collect and review logs, and when necessary, contact Support.

Upgrade a CloudBoost appliance

You can upgrade the CloudBoost appliance software in the CLI. During the upgrade, the CloudBoost appliance is unavailable. The appliance will restart after the upgrade is complete.

To review the latest CloudBoost appliance supported features, refer to the following content available on the Support website at <https://support.emc.com>.

⚠ CAUTION

If the site cache is enabled in CloudBoost 18.1, then contact the DellEMC support to assist you in disabling the site cache and upgrade to CloudBoost 18.2.

Note

CloudBoost 18.2 does not support site-cache.

- The [CloudBoost Release Notes](#) contains information about new features and changes, fixed problems, known limitations, environment, and system requirements for the latest release.
- The *NetWorker E-LAB Navigator* provides a complete list of supported products and versions.

Procedure

1. Connect to CloudBoost using an SSH client.

For more information about connecting to CLI, see [Connect to the CloudBoost CLI](#).

2. Login to CloudBoost as an administrator and run the following command:

```
upgrade appliance <URL upgrade path>.
```

Note

You must host the image of CloudBoost that you want to upgrade to in your LAN environment. Since downloading the image from the support site requires authentication, CloudBoost will be unable to download the image from the link.

3. Review the warning message, and then type **yes**.
TheCloudBoost upgrade process initiates.
4. Monitor the progress of the upgrade.

Note

During an upgrade, some services might temporarily be down or the appliance might go red while it restarts. The services and appliance will return to a normal state after the restart completes.

Results

After the upgrade is complete, type `status` to view CloudBoost version.

After you finish

By default, the recovery files are saved as `recovery.key` and `recovery.meta`. To prevent accidental overwrite of existing recovery files, Dell EMC recommends that you save the recovery files with a different file name.

Note

You must download the recovery information immediately. If you fail to download the recovery file, then you will be unable to perform a disaster recovery on the upgraded CloudBoost appliance.

CloudBoost integration with EMC Secure Remote Services

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

Registering EMC Secure Remote Services

When the CloudBoost appliance is registered with the EMC Secure Remote Services gateway, the appliance continuously communicates with EMC Secure Remote Services, sending status information and reports on a predetermined schedule. Appliance alerts from EMC Secure Remote Services appear in the On-Prem CloudBoost Management Console. When necessary, 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 remote support activity, including the date and time of remote sessions, the ticket number, and the technician who provided the support.

Registering

You can allow or deny this remote activity for any reason. When a technical support agent starts a connection through EMC Secure Remote Services, an email that requests access is sent to you. You can choose to grant or deny the request.

If you choose not to register CloudBoost appliances with EMC Secure Remote Services, you must manually monitor the appliances. If any issues arise, contact Support.

Installing the EMC Secure Remote Services 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 On-Prem CloudBoost Management Console, you can then also register the appliance with EMC Secure Remote Services.

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

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

Note

At the CloudBoost CLI, when you register the appliance with EMC Secure Remote Services, you need to provide the SID from the email that is sent from EMC Secure Remote Services Support, along with the IP address or the URL and serial number. For information about registering the CloudBoost appliance with EMC Secure Remote Services, see [Register CloudBoost with EMC Secure Remote Services](#) on page 80.

Register CloudBoost with EMC Secure Remote Services

You can register a CloudBoost appliance with the EMC Secure Remote Services gateway to enable two-way remote communication with Customer Support. EMC Secure Remote Services gateway monitors system health and communicates alerts and issues to Customer Support.

Before you begin

The EMC Secure Remote Services gateway must be installed, and the CloudBoost appliance must be registered in the On-Prem CloudBoost Management Console. Remote access must be enabled for the appliance.

Note

If a firewall exists between the CloudBoost appliance and the EMC Secure Remote Services gateway server, certain ports such as port 9443, must be open.

Procedure

1. Find the EMC Secure Remote Services SID in the email from EMC Secure Remote Services Support.
2. Have the IP address or URL and the serial number of the installed Secure Remote Services gateway available.
3. Connect to the CloudBoost CLI.
4. Type the following command:

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

where:

- *esrs_gateway* is either the IP address or the FQDN for the EMC Secure Remote Services gateway virtual machine.
- *username* and *password* are the credentials that you used to set up the EMC Secure Remote Services gateway.
- *sid* is the EMC Secure Remote Services serial number that EMC Secure Remote Services Support provided in an email.

- `gateway_sn` is the serial number for the EMC Secure Remote Services gateway.

Note

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

Results

The CloudBoost appliance is registered with EMC Secure Remote Services, and continuous support monitoring begins.

Configuring average chunk size

You can adjust the chunk size in AWS and Azure to reduce API calls and improve backup, restore, and clone performance.

Procedure

1. Connect to the CloudBoost CLI.
2. Authenticate with the administrator password.
3. Check the current average chunk size appliance by typing the following command: `avgchunksize show`
4. To change the average chunk size, type the following command: `avgchunksize change xxx`

Where `xxx` is the new chunk size setting.

Specifications for the chunk size setting

You can adjust the chunk size in AWS and Azure to reduce API calls and improve backup, restore, and clone performance.

Consider the following specifications for the chunk size setting:

- The maximum chunk size is 4 MB.
- The maximum average chunk size is 1 MB.
- The minimum average chunk size is 256 KB.
- If the average chunk size is increased, object sizes increase which reduces the overall API calls.
- The compression rate of each chunk is data dependent. Changing the chunk size results in smaller objects from higher compression ratios.

This table lists the workload chunk size specifications.

Table 15 Specifications for work load types

Work load type	Chunk size			
	File system		SQL	
	256 K	1024 K	256 K	1024 K
Average chunk size in KB with Rabin finger print	282.29	1092.68	222	1347
Average chunk size in KB with transferring blob	294.2	1193.36	72	432

This table lists the compressed SQL data specifications.

Table 16 Specification with compressed SQL data

Work load type	Chunk size	
	256 K	1024 K
Average chunk size in KB with Rabin finger print	310	1240
Average chunk size in KB with transferring blob	172	686