

# Cloud NetBackup™ Marketplace Deployment on AWS

# Cloud NetBackup™ Marketplace Deployment on AWS

Last updated: 2022-04-22

## Legal Notice

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

2625 Augustine Drive  
Santa Clara, CA 95054

<http://www.veritas.com>

## Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

Japan

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

## Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

## Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

[NB.docs@veritas.com](mailto:NB.docs@veritas.com)

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

## Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# Contents

Chapter 1	NetBackup marketplace deployment on AWS	6
	.....	6
	About Veritas NetBackup Marketplace Deployment on AWS .....	6
	Before you begin the deployment .....	7
	Network configuration .....	8
Chapter 2	Deploying NetBackup on AWS Cloud using the marketplace offer .....	9
	Deploying NetBackup on AWS Cloud using the marketplace offer .....	9
Chapter 3	Deployment options (Delivery methods) for NetBackup on AWS cloud .....	11
	Deployment options (Delivery methods) for &ProductName; on AWS cloud .....	11
	Option 1: Primary server only .....	12
	Option 2: Media server only .....	12
	Option 3: Primary and Media servers .....	13
	Option 4: CloudPoint server only .....	13
	Option 5: Primary, Media, and CloudPoint servers .....	14
	Option 6: Cloud Recovery server only .....	15
Chapter 4	NetBackup configuration parameters .....	16
	NetBackup configuration parameters .....	16
	Instance configuration parameters .....	16
	VPC and Subnet details for deployment in existing VPC .....	17
	VPC and Subnet configuration for deployment in new VPC .....	18
	NetBackup installation parameters for Primary sever .....	19
	NetBackup installation parameters for Media sever .....	20
	NetBackup installation parameters for CloudPoint Sever .....	21
	IAM role required for CloudPoint instance .....	24
	NetBackup installation parameters for Cloud Recovery Sever .....	28

Chapter 5	Accessing the NetBackup servers .....	31
	How to access the NetBackup servers .....	31
Chapter 6	Troubleshooting section .....	32
	Troubleshooting .....	32
	Deployment Logs .....	33

# NetBackup marketplace deployment on AWS

This chapter includes the following topics:

- [About Veritas NetBackup Marketplace Deployment on AWS](#)
- [Before you begin the deployment](#)
- [Network configuration](#)

## About Veritas NetBackup Marketplace Deployment on AWS

Veritas NetBackup provides the integrated deployment solution on the Amazon Web Services (AWS) Marketplace. The integrated offer facilitates an automated deployment of NetBackup, CloudPoint, and Cloud Recovery components on AWS using a CloudFormation template.

### Supported platforms:

- NetBackup deployment on Red Hat Enterprise Linux (RHEL) 7.x
- CloudPoint deployment on Red Hat Enterprise Linux (RHEL) 7.x, 8.x and Ubuntu 20.04 LTS
- Cloud Recovery server supported on Red Hat Enterprise Linux (RHEL) 7.x

The template lets you specify the following details for the NetBackup deployment:

- Deployment options (Delivery Methods): You have the flexibility of configuring the NetBackup Primary server, Media server, CloudPoint server, and Cloud Recovery server as independent components; or configuring a combination of two or more components in a single deployment.

- NetBackup license key: To be used to validate your NetBackup entitlement.
- NetBackup Usage Insights customer registration key: To be used to track your license usage and entitlement.
- Proxy settings for CloudPoint server: You can configure the CloudPoint component to be accessible through a proxy server, if required.
- Other mandatory specifications such as, the AWS instance, the virtual environment and network, and the server-specific configuration details.

This document provides the instructions for deploying Veritas NetBackup on AWS cloud by using a CloudFormation template. The intended audience for this document includes backup administrators, cloud administrators, architects, and system administrators.

## Before you begin the deployment

Before you begin deploying the NetBackup on AWS, ensure the following:

1. You have an AWS account with an active subscription, with privileges to create a new VPC and an m4.xlarge EC2 or higher instance.
2. You have a valid key pair for the region in which you want to deploy NetBackup.
3. For Cloud Recovery deployment, you may require the privileges to create an IAM role in the AWS account.
4. For Primary server deployment, you may require the privileges to create an IAM role in the AWS account. You need to attach the following Secrets Manager related policies to IAM user.
  - [SecretsManagerReadWrite](#)
  - [IAMFullAccess](#)
5. For Primary Server deployment, if you are adding an existing IAM role, you need to have following policies of Secret Manager assigned to the IAM role.
  - `secretsmanager:GetResourcePolicy`
  - `secretsmanager:GetSecretValue`
  - `secretsmanager:DescribeSecret`
  - `secretsmanager>DeleteSecret`
  - `secretsmanager:ListSecretVersionIds`

---

**Note:** For Primary server deployment, IAM Role can be deleted after successful deployment.

---

6. You have a valid NetBackup license key.
7. You have a NetBackup Usage Insights Customer Registration key for your account.
8. Meet system and instance requirements. Refer to the compatibility lists [NetBackup Compatibility List for all versions](#)

## Network configuration

The NetBackup instances need access to the public Internet for the product to function. If you are deploying NetBackup components in an existing VPC ensure that the subnet used to deploy the NetBackup instances has outbound access to the Internet, either through an internet gateway or a NAT gateway.

If you do not have a properly configured VPC available, you can choose to create a new one during the deployment. The VPC will be created with a public and a private subnet. The NetBackup Primary server will be deployed in the public subnet so that you can access the NetBackup UI from a machine outside the VPC. NetBackup Media servers can be deployed in the private subnet for greater security.



# Deploying NetBackup on AWS Cloud using the marketplace offer

This chapter includes the following topics:

- [Deploying NetBackup on AWS Cloud using the marketplace offer](#)

## Deploying NetBackup on AWS Cloud using the marketplace offer

You need to follow below mentioned steps to deploy NetBackup on AWS cloud.

### To deploy NetBackup on AWS

- 1 Visit the AWS Marketplace at [link](#).
- 2 Locate and access the **Veritas NetBackup (BYOL)**.
- 3 On the offer page, click **Continue to Subscribe**.
- 4 You may review the Terms and Conditions and click **Continue to Configuration**.
- 5 This opens the selection page which lets you select and launch the CloudFormation Template for the NetBackup component you want to install.

Select from the following deployment options under **Delivery Method**:

- a. NetBackup Primary server
- b. NetBackup Media server
- c. NetBackup CloudPoint server

- d. NetBackup Cloud Recovery server
  - e. For Primary + Media + CloudPoint full deployment: NetBackup Primary, Media and CloudPoint servers
  - f. For Primary + Media server deployment: NetBackup Primary and Media servers
- 6 Select the version and select the region in which you want to deploy the component.
  - 7 On the **Launch this software** page that opens, select **Launch CloudFormation** under **Choose Action** to begin configuration using the AWS CloudFormation console.
  - 8 This opens the **Create Stack** page where the template URL is pre-populated for you. Click **Next**.
  - 9 Then on the **Specify stack details** page that opens, specify a name for the stack (deployment) and provide the configuration details.  
  
Refer to the individual configuration sections that correspond to the delivery method you selected.
  - 10 On the next page, for **Configure stack option**, change the **Stack failure options** to preserve the successfully provisioned resources. This helps in preserving the created resources and troubleshoot issues in case of stack failure.

# Deployment options (Delivery methods) for NetBackup on AWS cloud

This chapter includes the following topics:

- [Deployment options \(Delivery methods\) for &ProductName; on AWS cloud](#)
- [Option 1: Primary server only](#)
- [Option 2: Media server only](#)
- [Option 3: Primary and Media servers](#)
- [Option 4: CloudPoint server only](#)
- [Option 5: Primary, Media, and CloudPoint servers](#)
- [Option 6: Cloud Recovery server only](#)

## Deployment options (Delivery methods) for &ProductName; on AWS cloud

There are multiple options to deploy NetBackup on AWS cloud.

- **Option 1:** Primary server only
- **Option 2:** Media server only
- **Option 3:** Primary and Media servers
- **Option 4:** CloudPoint server only

- **Option 5:** Primary, Media, and CloudPoint servers
- **Option 6:** Cloud Recovery server only

## Option 1: Primary server only

Refer to this section if you intend to configure the NetBackup Primary server only in a single deployment.

### Steps to configure:

- 1 Provide a name for the Stack.
- 2 Provide the Instance Configuration Parameters.  
See [“Instance configuration parameters”](#) on page 16.
- 3 Provide the VPC and Subnet details, depending on whether you are deploying the primary server in an existing VPC or in a new VPC.  
See [“VPC and Subnet configuration for deployment in new VPC”](#) on page 18.  
See [“VPC and Subnet details for deployment in existing VPC ”](#) on page 17.
- 4 Provide the Primary sever configuration details.  
See [“NetBackup installation parameters for Primary sever”](#) on page 19.
- 5 Click **Next** and tag your stack for identification.
- 6 Review all the details and initiate the launch.

## Option 2: Media server only

Refer to this section if you intend to configure the NetBackup Media server only in a single deployment.

### Steps to configure:

- 1 Provide a name for the Stack.
- 2 Provide the Instance Configuration Parameters as applicable.  
See [“Instance configuration parameters”](#) on page 16.
- 3 Provide the VPC and Subnet details as applicable, in which the Primary server is deployed. See VPC and Subnet details for deployment in existing VPC  
See [“VPC and Subnet details for deployment in existing VPC ”](#) on page 17.
- 4 Provide the Media server configuration details.  
See [“NetBackup installation parameters for Media sever”](#) on page 20.

- 5 Click Next and tag your stack for identification.
- 6 Review all the details and initiate the launch.

## Option 3: Primary and Media servers

Refer to this section if you intend to configure the NetBackup Primary and Media servers both, in a single deployment.

### Steps to configure:

- 1 Provide a name for the Stack.
- 2 Provide the NetBackup Primary server name and the Instance Configuration Parameters as applicable.  
  
See [“NetBackup installation parameters for Primary sever”](#) on page 19.  
See [“Instance configuration parameters”](#) on page 16.
- 3 Provide the NetBackup Media server name and the Instance Configuration Parameters as applicable.  
  
See [“NetBackup installation parameters for Media sever”](#) on page 20.  
See [“Instance configuration parameters”](#) on page 16.
- 4 Provide the VPC and Subnet details, depending on whether you are deploying the servers in an existing VPC or in a new VPC.  
  
See [“VPC and Subnet details for deployment in existing VPC ”](#) on page 17.  
See [“VPC and Subnet configuration for deployment in new VPC”](#) on page 18.
- 5 Provide the NetBackup Service Username, License Key, and Usage Insights key.  
  
See [“NetBackup installation parameters for Primary sever”](#) on page 19.
- 6 Click **Next** and tag your stack for identification.
- 7 Review all the details and initiate the launch.

## Option 4: CloudPoint server only

Refer to this section if you intend to:

- Configure the NetBackup CloudPoint server in a single deployment
- Upgrade your existing CloudPoint server to 10.0

**Steps to configure:**

- 1 Provide a name for the Stack.
- 2 Provide the various configurations for NetBackup CloudPoint system, network, server, KMS, security etc.  
See [“NetBackup installation parameters for CloudPoint Sever”](#) on page 21.
- 3 Click **Next** to tag your stack for identification.
- 4 Review all the details and initiate the launch.

## Option 5: Primary, Media, and CloudPoint servers

Refer to this section if you are performing the full deployment that includes configuring the NetBackup Primary, Media, and CloudPoint servers, in a single deployment. The deployment can take approximately 25 minutes.

The servers are deployed in the following order:

1. Primary server
2. Media server
3. CloudPoint server

**Steps to configure:**

- 1 Provide a name for the Stack.
- 2 Provide the NetBackup Primary server name and the Instance Configuration Parameters as applicable.  
See [“NetBackup installation parameters for Primary sever”](#) on page 19.  
See [“Instance configuration parameters”](#) on page 16.
- 3 Provide the NetBackup Media server name and the Instance Configuration Parameters as applicable.  
See [“NetBackup installation parameters for Media sever”](#) on page 20.  
See [“Instance configuration parameters”](#) on page 16.
- 4 Provide the NetBackup CloudPoint server Instance Configuration Parameters.  
See [“NetBackup installation parameters for CloudPoint Sever”](#) on page 21.
- 5 Provide the Common Instance Configuration Parameters.  
See [“Instance configuration parameters”](#) on page 16.

- 6 Provide the VPC and Subnet details, depending on whether you are deploying the servers in an existing VPC or in a new VPC.  
See [“VPC and Subnet details for deployment in existing VPC ”](#) on page 17.  
See [“VPC and Subnet configuration for deployment in new VPC”](#) on page 18.
- 7 Provide the NetBackup Service Username, License Key, and Usage Insights key.  
See [“NetBackup installation parameters for Primary sever”](#) on page 19.
- 8 Provide the NetBackup CloudPoint Installation Parameters.  
See [“NetBackup installation parameters for CloudPoint Sever”](#) on page 21.
- 9 Click **Next** to tag your stack for identification.
- 10 Review all the details and initiate the launch.

## Option 6: Cloud Recovery server only

Refer to this section if you are configuring only the NetBackup Cloud Recovery server in a single deployment.

### Steps to configure:

- 1 Provide a name for the Stack.
- 2 Provide the various configuration details for NetBackup Cloud Recovery server instance, VPC and subnet, installation parameters etc.  
See [“NetBackup installation parameters for Cloud Recovery Sever”](#) on page 28.
- 3 Click **Next** to tag your stack for identification.
- 4 Review all the details and initiate the launch.

# NetBackup configuration parameters

This chapter includes the following topics:

- [NetBackup configuration parameters](#)
- [Instance configuration parameters](#)
- [VPC and Subnet details for deployment in existing VPC](#)
- [VPC and Subnet configuration for deployment in new VPC](#)
- [NetBackup installation parameters for Primary sever](#)
- [NetBackup installation parameters for Media sever](#)
- [NetBackup installation parameters for CloudPoint Sever](#)
- [NetBackup installation parameters for Cloud Recovery Sever](#)

## NetBackup configuration parameters

Refer to the following tables and provide the configuration details depending on the NetBackup component deployment you want to perform.

See See [“Deployment options \(Delivery methods\) for &ProductName; on AWS cloud”](#) on page 11.

## Instance configuration parameters

Below table states the instance configuration parameters:



**Table 4-1** Instance configuration parameters details

Parameters	Description
IAM Role	Name of the existing role to be attached to the NetBackup Primary server instance. The role must include policy for Secrets Manager to store password for Web UI user. A new role will be created if this field is kept blank.
NetBackup server Instance Type	Select a supported instance type from the drop-down list, based on the size of your deployment.
SSH Key Pair	Select an existing SSH key pair to be used for SSH access to the NetBackup server you are deploying.
NetBackup Installation Volume Size	Specify the storage space that should be assigned to NetBackup, based on the size of your deployment.  The installation volume size for media server is 250 GB, for primary server 50 GB and for Cloud Recovery server 200 GB.
Use an existing VPC?	Select True to deploy the NetBackup server in an existing VPC in your account.  Select False to deploy the NetBackup server in a new VPC that will be created during the deployment.

# VPC and Subnet details for deployment in existing VPC

Below table states the details of VPC and subnet for deploying in existing VPC:

**Table 4-2** VPC and Subnet details for deployment

Parameters	Description
VPC ID	Specify the ID of the VPC in your account where the NetBackup server is to be deployed.

**Table 4-2** VPC and Subnet details for deployment (*continued*)

Parameters	Description
Subnet ID	Select the subnet that is within the selected VPC, where the NetBackup server should be deployed.
VPC CIDR Block	Specify the CIDR block contained in the selected VPC. This information is used to create security group rules for the NetBackup server.
Create New DHCP Option Set for this VPC?	Select True only if you want the deployment to create a new DHCP Option set for your VPC. Select False if you already have a DHCP Option set associated with your VPC that can resolve Route 53 host names using an Amazon provided DNS server. Selecting True will override any existing DHCP options associated with the VPC.
NetBackup server Domain Name	Route53 DNS is configured with this domain name and a Record is updated in the corresponding Hosted Zone with the private IP of the NetBackup server.
Is there an Existing Hosted Zone for this Domain?	Select True if a Route53 Hosted Zone associated with the selected VPC already exists for the domain name entered above. Select False to create a new Hosted Zone along with the deployment.

# VPC and Subnet configuration for deployment in new VPC

Below table states the details of VPC and subnet for deploying in new VPC:

**Table 4-3** VPC and Subnet configuration details

Parameters	Description
New VPC CIDR Block	Specify the CIDR block that will be used to create the new VPC and security group rules for the new server. Ex. 172.31.0.0/16

**Table 4-3** VPC and Subnet configuration details (*continued*)

Parameters	Description
CIDR Block for Public Subnet	Select the CIDR block within the VPC CIDR block that will be used for the public subnet created in the VPC. Ex. 172.31.0.0/24
CIDR Block for Private Subnet	Select the CIDR block within the VPC CIDR block that will be used for the private subnet created in the VPC. Ex. 172.31.1.0/24
NetBackup server Domain Name	A Route53 Hosted Zone for this domain name will be created. Then a DNS is configured with this domain name and a Record is updated in the Hosted Zone with the private IP of the NetBackup server.

**Note:** : If you have selected a new VPC and subnet configuration to be created, you still need to provide a VPC ID and Subnet ID in the section “VPC and Subnet details for deployment in existing VPC” above. This is because, AWS does not permit these fields to be blank. Any values you provide in these fields will be ignored if you have selected to create a new VPC and subnet.

# NetBackup installation parameters for Primary sever

Below table states the details of NetBackup installation parameters for Primary server:

**Table 4-4** NetBackup installation parameters for Primary sever

Parameters	Description
NetBackup Web Username	Provide a 'Web user' name. If a non-root username is provided, then the user will be created. This user will be created on the Primary server instance during deployment and will only be used to access NetBackup Web UI. Administrator role will be associated with web user.
NetBackup Web User Password	Password must be at least 8 characters long which includes a number, a lower case, an upper case and a special character (!@#\$\$%^&*).

**Table 4-4** NetBackup installation parameters for Primary sever (*continued*)

Parameters	Description
Confirm NetBackup Web User Password	Password must be at least 8 characters long which includes a number, a lower case, an upper case and a special character (!@#\$\$%^&*).
Primary server Name	Provide a name for the Primary server.
NetBackup Service Username	Provide a 'service user' name. Most services on the server will run as this user. If a non-root username is provided, then the user will be created, and associated with the 'nbwebgrp' user group as the secondary group. Refer to "Running NetBackup services with non-privileged user (service user) account" in the <a href="#">Veritas NetBackup™ Security and Encryption Guide</a>
NetBackup License Key	Provide your NetBackup license key. When copy/pasting the license key, ensure that it is copied completely, including the hyphens. See <a href="#">Veritas NetBackup™ Installation Guide</a>
NetBackup Usage Insights Customer Registration Key	Copy and paste entire contents of the JSON file containing the NetBackup Usage Insights customer registration key. See <a href="#">Enable Veritas Usage Insights</a> documentation.

## NetBackup installation parameters for Media sever

Below table states the details of NetBackup installation parameters for Media server:

**Table 4-5** NetBackup installation parameters for Media sever

Parameters	Description
Media server Name	Provide a name for the Media server.
Primary server Name	Provide the name of a NetBackup Primary server to which the Media server should connect. The Primary server needs to have been deployed in the same domain and the VPC, where you are trying to deploy the Media server.
NetBackup License Key	Provide your NetBackup license key. When copy/pasting the license key, ensure that it is copied completely, including the hyphens. Refer <a href="#">Veritas NetBackup™ Installation Guide</a>

**Table 4-5** NetBackup installation parameters for Media sever *(continued)*

Parameters	Description
NetBackup Token	Enter the NetBackup authorization token key for the Media server generated from an existing Primary server. Refer <a href="#">Veritas NetBackup™ Security and Encryption Guide</a>

# NetBackup installation parameters for CloudPoint Sever

If you have chosen the deployment option that includes the NetBackup CloudPoint server deployment, provide the following details as applicable.

**Table 4-6** NetBackup installation parameters for CloudPoint server

Parameters	Description
<b>CloudPoint System Configuration</b>	
OS type for EC2 Instance	Select the OS type for the CloudPoint instance.
EC2 Instance Type	Select the EC2 instance type that you want to use for the CloudPoint instance.
Volume Size	Enter the size (in GB) of the EBS volume that will be attached to the CloudPoint instance.
IAM Role	Name of the role to be attached to the CloudPoint instance (A new IAM Role will be created if this field is left empty). Following permissions are required for the IAM role. See <a href="#">"IAM role required for CloudPoint instance"</a> on page 24.
<b>CloudPoint Upgrade Configuration (Applicable only in case of upgrade)</b>	
EBS Volume ID	ID of an existing EBS volume
Volume Snapshot ID	ID of the CloudPoint metadata volume snapshot.
<b>Network Configuration</b>	
CloudPoint VPC	Select ID of existing VPC where CloudPoint instance will be deployed.

**Table 4-6** NetBackup installation parameters for CloudPoint server  
(continued)

Parameters	Description
CloudPoint Subnet	Select ID of existing subnet in your VPC where CloudPoint instance will be deployed.
Availability Zone	Name of an existing EC2 Availability Zone in which the CloudPoint instance will be created.
Inbound Access CIDR	If you choose to create a new virtual network, you can provide the CIDR block from which the CloudPoint server can be accessed.
Elastic IP	Elastic IP to be assigned to CloudPoint instance.
HTTP Proxy	Provide the HTTP proxy value to configure CloudPoint with proxy server.
HTTPS Proxy	Provide the HTTPS proxy value to configure CloudPoint with proxy server.
NO Proxy	Specify the hosts that should be allowed to bypass the proxy server. You can mention multiple, comma-separated values. For example:  localhost,mycompany.com,192.168.0.10:80
<b>CloudPoint Configuration</b>	
CloudPoint Username	Specify a username for the CloudPoint administrator user account to be created.
CloudPoint Password	Specify a password for the administrator user.
Confirm CloudPoint Password	Confirm the administrator user password.

**Table 4-6** NetBackup installation parameters for CloudPoint server  
(continued)

Parameters	Description
Hostnames	Specify the IP address or the Fully Qualified Domain Name (FQDN) of the CloudPoint host. You can mention multiple, comma-separated values. If you want to connect to the host using different names (for example, myserver, myserver.mydomain, or myserver.mydomain.mycompany.com), then ensure that you add all the names here if you want to enable CloudPoint access using those names.  The installer uses these names to generate a TLS certificate for the CloudPoint host.
Port	Select the port through which the CloudPoint server can communicate. Default is port 443.
<b>CloudPoint Recovery Notification Configuration</b>	
SNS Topic ARN	ARN of the SNS Topic to get notifications on any update in the CloudPoint Auto Scaling Group (Leave this field blank if notifications are not required)
<b>CloudPoint KMS configuration</b>	
CMK ID	ID of the customer master key using which KMS would be configured with CloudPoint (Leave this field blank if KMS need not be configured)
CMK Region	Region of the CMK if CMK ID is specified (Leave this field blank if region is same as where CloudPoint is being deployed)
<b>Security configuration</b>	
Key Pair Name	CloudPoint instance
<b>CloudPoint Registration with NetBackup</b>	

**Table 4-6** NetBackup installation parameters for CloudPoint server  
(continued)

Parameters	Description
NetBackup server	Provide a Fully Qualified Domain Name of the existing Primary server to which the CloudPoint server needs to be associated. Configuration fails if the FQDN is not resolvable from this CloudPoint server.
NetBackup API Key	<p>As a NetBackup user, provide a valid API key generated from the existing Primary server to validate the communication between the Primary server and the CloudPoint server. The user generating API keys must have permission to add the CloudPoint server.</p> <p><a href="#">Creating and managing API keys for users (Administrators)</a></p> <p><a href="#">Adding and managing your API key (Users)</a></p>

## IAM role required for CloudPoint instance

**Table 4-7** IAM roles for CloudPoint instance

SID	Effect	Action	Resource
EC2AutoScaling	Allow	<ul style="list-style-type: none"> <li>autoscaling:UpdateAutoScalingGroup</li> <li>autoscaling:AttachInstances</li> </ul>	*
KMS	Allow	<ul style="list-style-type: none"> <li>kms:ListKeys</li> <li>kms:Encrypt</li> <li>kms:Decrypt</li> <li>kms:ReEncryptTo</li> <li>kms:DescribeKey</li> <li>kms:ListAliases</li> <li>kms:GenerateDataKey</li> <li>kms:GenerateDataKeyWithoutPlaintext</li> <li>kms:ReEncryptFrom</li> <li>kms&gt;CreateGrant</li> </ul>	*



**Table 4-7** IAM roles for CloudPoint instance (*continued*)

SID	Effect	Action	Resource
RDSBackup	Allow	<ul style="list-style-type: none"> <li>■ rds:DescribeDBSnapshots</li> <li>■ rds:DescribeDBClusters</li> <li>■ rds:DescribeDBClusterSnapshots</li> <li>■ rds&gt;DeleteDBSnapshot</li> <li>■ rds&gt;CreateDBSnapshot</li> <li>■ rds&gt;CreateDBClusterSnapshot</li> <li>■ rds:ModifyDBSnapshotAttribute</li> <li>■ rds:DescribeDBSubnetGroups</li> <li>■ rds:DescribeDBInstances</li> <li>■ rds:CopyDBSnapshot</li> <li>■ rds:CopyDBClusterSnapshot</li> <li>■ rds:DescribeDBSnapshotAttributes</li> <li>■ rds&gt;DeleteDBClusterSnapshot</li> <li>■ rds:ListTagsForResource</li> <li>■ rds:AddTagsToResource</li> <li>■ rds:DescribeDBClusterParameterGroups</li> </ul>	*
RDSRecovery	Allow	<ul style="list-style-type: none"> <li>■ rds:ModifyDBInstance'</li> <li>■ rds:ModifyDBClusterSnapshotAttribute'</li> <li>■ rds:RestoreDBInstanceFromDBSnapshot'</li> <li>■ rds:ModifyDBCluster</li> <li>■ rds:RestoreDBClusterFromSnapshot</li> <li>■ rds&gt;CreateDBInstance</li> <li>■ rds:RestoreDBClusterToPointInTime'</li> <li>■ rds&gt;CreateDBSecurityGroup</li> <li>■ ds&gt;CreateDBCluster</li> <li>■ rds:RestoreDBInstanceToPointInTime</li> </ul>	*

**Table 4-7** IAM roles for CloudPoint instance *(continued)*

SID	Effect	Action	Resource
EC2Backup	Allow		*

**Table 4-7** IAM roles for CloudPoint instance (*continued*)

SID	Effect	Action	Resource
		<ul style="list-style-type: none"> <li>■ sts:GetCallerIdentity</li> <li>■ ec2:CreateSnapshot</li> <li>■ ec2:DescribeInstances'</li> <li>■ ec2:DescribeInstanceStatus</li> <li>■ ec2:ModifySnapshotAttribute</li> <li>■ ec2:CreateImage</li> <li>■ ec2:CopyImage</li> <li>■ ec2:CopySnapshot'</li> <li>■ ec2:DescribeSnapshots</li> <li>■ ec2:DescribeVolumeStatus</li> <li>■ ec2:DescribeVolumes</li> <li>■ ec2:RegisterImage</li> <li>■ ec2:DescribeVolumeAttribute</li> <li>■ ec2:DescribeSubnets</li> <li>■ ec2:DescribeVpcs</li> <li>■ ec2:DeregisterImage</li> <li>■ ec2&gt;DeleteSnapshot</li> <li>■ ec2:DescribeInstanceAttribute</li> <li>■ ec2:DescribeRegions</li> <li>■ ec2:ModifyImageAttribute</li> <li>■ ec2:DescribeAvailabilityZones</li> <li>■ ec2:ResetSnapshotAttribute</li> <li>■ ec2:DescribeHosts</li> <li>■ ec2:DescribeImages</li> <li>■ ec2:AssociateAddress</li> <li>■ ec2:DescribeNetworkInterfaces</li> <li>■ ec2:DescribeSecurityGroups</li> <li>■ ec2:AuthorizeSecurityGroupEgress</li> <li>■ ec2:AuthorizeSecurityGroupIngress</li> <li>■ ec2:CreateSnapshots</li> <li>■ ec2:GetEbsEncryptionByDefault</li> <li>■ ec2:DescribeKeyPairs</li> <li>■ secretsmanager:GetResourcePolicy</li> <li>■ secretsmanager:GetSecretValue</li> <li>■ secretsmanager:DescribeSecret</li> <li>■ secretsmanager:RestoreSecret</li> <li>■ secretsmanager:PutSecretValue</li> <li>■ secretsmanager&gt;DeleteSecret</li> </ul>	

**Table 4-7** IAM roles for CloudPoint instance (*continued*)

SID	Effect	Action	Resource
		<ul style="list-style-type: none"> <li>secretsmanager:UpdateSecret</li> </ul>	
EC2Recovery	Allows	<ul style="list-style-type: none"> <li>ec2:RunInstances</li> <li>ec2:AttachNetworkInterface</li> <li>ec2:DetachVolume</li> <li>ec2:AttachVolume</li> <li>ec2&gt;DeleteTags</li> <li>ec2:CreateTags</li> <li>ec2:StartInstances</li> <li>ec2:StopInstances</li> <li>ec2:TerminateInstances</li> <li>ec2:CreateVolume</li> <li>ec2&gt;DeleteVolume</li> <li>ec2:DescribeIamInstanceProfileAssociations</li> <li>ec2:AssociateIamInstanceProfile</li> <li>ec2:DescribeInstanceTypeOfferings</li> </ul>	*
SNS	Allow	<ul style="list-style-type: none"> <li>sns:Publish</li> <li>sns:GetTopicAttributes</li> </ul>	*
IAM	Allow	<ul style="list-style-type: none"> <li>iam:SimulatePrincipalPolicy</li> <li>iam:ListAccountAliases</li> </ul>	*
EBS	Allow	<ul style="list-style-type: none"> <li>ebs:ListSnapshotBlocks</li> <li>ebs:StartSnapshot</li> </ul>	*
Route53	Allow	<ul style="list-style-type: none"> <li>route53:CreateHostedZone</li> <li>route53:ListHostedZones</li> <li>route53:GetHostedZone</li> <li>route53:ListResourceRecordSets</li> <li>route53:ChangeResourceRecordSets</li> <li>route53:ListResourceRecordSets</li> <li>route53:ListHostedZonesByName</li> </ul>	*

## NetBackup installation parameters for Cloud Recovery Server

Below table states the details of NetBackup installation parameters for Cloud Recovery Server:

**Table 4-8** NetBackup installation parameters for Cloud Recovery Server

Parameters	Description
<b>Instance Configuration Parameters</b>	
NetBackup server Instance Type	Select the instance type for the NetBackup server from the dropdown list.
SSH Key Pair	Select an existing EC2 Key Pair in the region, to enable SSH access to the instance.
NetBackup Installation Volume Size	Specify the storage space that should be assigned to NetBackup, based on the size of your deployment. For the Cloud Recovery server the volume size must be minimum 200 GB
Create IAM Role for Cloud Recovery server?	Cloud Recovery server requires a role with specific IAM privileges to be assigned to the NetBackup instance. Select <b>Yes</b> to create a new role or 'No' to use an existing role. Make sure that you have 'iam:CreateRole' permission to create new role.
IAM Role Name	Name of existing or new IAM role for Cloud Recovery server.  <b>Note:</b> If you have selected 'Yes' to create a new role above, and if a role already exists with the same name, then the deployment will fail.
Use an Existing VPC?	Select <b>True</b> if you want to deploy the Cloud Recovery server into an existing VPC. Select <b>False</b> to deploy the Cloud Recovery server in a new VPC that will be created during the deployment.
<b>VPC and Subnet details for deployment in existing VPC</b>	
See <a href="#">"VPC and Subnet details for deployment in existing VPC "</a> on page 17.	
<b>VPC and Subnet configuration for deployment in new VPC (Required only if new VPC has been selected above)</b>	

Table 4-8

NetBackup installation parameters for Cloud Recovery Server

(continued)

Parameters	Description
See <a href="#">“VPC and Subnet configuration for deployment in new VPC”</a> on page 18.	
<b>Note:</b> If you have selected a new VPC and subnet configuration to be created, you still need to provide a VPC ID and Subnet ID in the section “VPC and Subnet details for deployment in existing VPC” above. This is because, AWS does not permit these fields to be blank. Any values you provide in these fields will be ignored if you have selected to create a new VPC and subnet.	
<b>NetBackup Installation Parameters</b>	
Master server Name	Provide a Fully Qualified Domain Name of the existing Primary server to which the Cloud Recovery server needs to be associated. Configuration fails if the FQDN is not resolvable from this server.
NetBackup License Key	Provide your NetBackup license key. When copy/pasting the license key, ensure that it is copied completely, including the hyphens. <a href="#">Veritas NetBackup™ Installation Guide</a>
NetBackup Usage Insights Customer Registration Key	Copy and paste entire contents of the JSON file containing the NetBackup Usage Insights customer registration key. <a href="#">Enable Veritas Usage Insights</a> documentation.
S3 Bucket Name	Name of the bucket where MSDP images are stored.
Bucket Subfolder	Enter the path of the subfolder in the S3 bucket above where the MSDP images are stored.

# Accessing the NetBackup servers

This chapter includes the following topics:

- [How to access the NetBackup servers](#)

## How to access the NetBackup servers

After the successful deployment, you can access the NetBackup servers if you are an authorized user.

### How to access NetBackup servers

- 1 Use the 'NetBackup Web Username' user and 'NetBackup Web User Password' to log on to the NetBackup console (Java or Remote Administration Console).
- 2 Launch the NetBackup Web UI using [link](#).

The Web UI Primary server can be accessed using the hostname of the NetBackup Primary server that you have deployed. Make sure that the hostname is resolvable from the server where you are accessing the Web UI. Or, connect to the Web UI using the NetBackup Java Console.

If you want to connect to the NetBackup java console, ensure that you SSH using a client that has X11 forwarding enabled.

There are more ways to access the NetBackup Web UI. Refer to section *Sign in to the NetBackup web UI* in the latest version of [NetBackup™ Web UI Administrator's Guide](#) , and start managing and protecting your assets.

# Troubleshooting section

This chapter includes the following topics:

- [Troubleshooting](#)
- [Deployment Logs](#)

## Troubleshooting

1. **Unable to login with 'NetBackup Web Username' provided in while deploying Primary server.**

Steps to resolve the issue:

- Edit the security group of the NetBackup server to allow SSH access on port 22. Make sure you only allow access from the trusted sources in your network.
- Go to the Output section in the CloudFormation Stack and note down the NetBackup server private/public IP.
- SSH connect to the NetBackup server using the username for the ec2-user, and the PEM file corresponding to the key pair selected during deployment.
- Use the command `sudo passwd root` to set a password for the root user.
- Use the root user and password to log on to the NetBackup console (Java or Remote Administration Console).
- Launch the NetBackup Web UI using **`https://<primaryserver>/webui/login`**.

---

**Note:** The primaryserver is the host name or IP address of the NetBackup primary server that you want to sign in to.

---



# Deployment Logs

The NetBackup installation logs can be found at `/root/NBSetup/userdata.log` on the appliance.

.

The NetBackup installation logs can be found at `/root/NBSetup/userdata.log` on the appliance. While installation going on, one can SSH to the server with `ec2-user` and check the logs using command `tail -f /var/log/userdata.log`.