NetBackup™ Marketplace Deployment on AWS

Release 11.2.0.1

COHESITY

NetBackup™ Marketplace Deployment on AWS

Last updated: 2026-09-09

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

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. COHESITY 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.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 NetBackup marketplace deployment on AWS 6

About Cohesity 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 NetBackup 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: Cloud Recovery server only 13

Chapter 4 NetBackup configuration parameters 15

NetBackup configuration parameters 15
Instance configuration parameters 15
VPC and Subnet details for deployment in existing VPC 16
VPC and Subnet configuration for deployment in new VPC 17
NetBackup installation parameters for the primary server 18
IAM role required for the primary server 19
NetBackup installation parameters for Media server 20
NetBackup installation parameters for Cloud Recovery server 20
IAM role required for Cloud Recovery Server 22

Chapter 5 Deploying Snapshot Manager 24

Deploying Snapshot Manager server using the marketplace offer 24
Prerequisites for using the Snapshot Manager template 25
Resources created by the Snapshot Manager template 26
Snapshot Manager EC2 instance configuration details 28
Instance failures and Auto Scaling Group behavior 28
NetBackup installation parameters for Snapshot Manager server 29

Chapter 6 Encryption enabled NetBackup primary server 38

Additional steps on CRS if encryption is enabled NetBackup primary server 38

Chapter 7 Accessing the NetBackup servers 40

How to access the NetBackup servers 40

Chapter 8 Upgrade NetBackup Snapshot Manager from AWS Marketplace 41

Upgrade NetBackup Snapshot Manager from AWS Marketplace 41
Upgrade Snapshot Manager deployment using new AWS CloudFormation stack 43

Chapter 9 Troubleshooting 47

Troubleshooting 47

Chapter 1

NetBackup marketplace deployment on AWS

This chapter includes the following topics:

- About Cohesity NetBackup Marketplace Deployment on AWS
- Before you begin the deployment
- Network configuration

About Cohesity NetBackup Marketplace Deployment on AWS

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

Supported platforms:

- The NetBackup deployment on Red Hat Enterprise Linux (RHEL) 8.8.
- The Snapshot Manager deployment on Red Hat Enterprise Linux (RHEL) 8.8.
- The Cloud Recovery server that is supported on Red Hat Enterprise Linux (RHEL) 8.8.

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, Snapshot Manager server, and Cloud Recovery server as independent components; or configuring a combination of two or more components in a single deployment.

- Proxy settings for Snapshot Manager server: You can configure the Snapshot Manager component to be accessible through a proxy server, if required.
- Other mandatory specifications such as AWS instance, the virtual environment and network, and the server-specific configuration details.

Note: The NetBackup is deployed with 60 day evaluation license by default. After successful installation of the NetBackup, connect to the web UI to add the production license. If the license is not added within 60 days, NetBackup may stop working.

This document provides the instructions for deploying Cohesity NetBackup on the 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.
2. You have a valid key pair for the region in which you want to deploy NetBackup.
3. For the primary server deployment, the IAM user you login with, need Secret Manager read, write privileges. You need to attach the following policies to IAM user.
   - SecretsManagerReadWrite
   - IAMFullAccess
4. For Primary Server deployment, you need to have an existing IAM role. For permissions required for the IAM role, refer see See “IAM role required for the primary server” on page 19.
5. 5. For Cloud Recovery Server deployment, you need to have an existing IAM role. For permissions required for the IAM role, refer See “IAM role required for Cloud Recovery Server” on page 22.
6.

   Note: for the primary server deployment, IAM Role can be deleted after successful deployment.
   ---
7. 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.

Chapter 2

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. 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 (CRS optional)
   - b. NetBackup Media server
   - c. NetBackup Primary and Media Servers

Note: To deploy Cloud Recovery Server, choose the delivery method as NetBackup Primary Server (CRS optional).

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.

Chapter 3

Deployment options (Delivery methods) for NetBackup on AWS cloud

This chapter includes the following topics:

- Deployment options (Delivery methods) for NetBackup on AWS cloud
- Option 1: Primary server only
- Option 2: Media server only
- Option 3: Primary and Media servers
- Option 4: Cloud Recovery server only

Deployment options (Delivery methods) for NetBackup 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:** 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 15.
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 17.

   See “VPC and Subnet details for deployment in existing VPC” on page 16.
4. Provide the primary server configuration details.

   See “NetBackup installation parameters for the primary server” on page 18.
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 15.
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 16.
4. Provide the media server configuration details.

   See “NetBackup installation parameters for Media server” 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 theNetBackup primary server name and the Instance Configuration Parameters as applicable.

   See “NetBackup installation parameters for the primary server” on page 18.

   See “Instance configuration parameters” on page 15.
3. Provide theNetBackup Media server name and the Instance Configuration Parameters as applicable.

   See “NetBackup installation parameters for Media server” on page 20.

   See “Instance configuration parameters” on page 15.
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 16.

   See “VPC and Subnet configuration for deployment in new VPC” on page 17.
5. Provide the NetBackup Service Username.

   See “NetBackup installation parameters for the primary server” on page 18.
6. Click **Next** and tag your stack for identification.
7. Review all the details and initiate the launch.

Option 4: Cloud Recovery server only

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

Note: For deploying CRS server, choose the delivery method as NetBackup Primary Server (CRS optional).

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 server" on page 20.
3. Click **Next** to tag your stack for identification.
4. Review all the details and initiate the launch.

Chapter 4

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 the primary server
- NetBackup installation parameters for Media server
- NetBackup installation parameters for Cloud Recovery server

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 NetBackup 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
NetBackup server configuration	Select the configuration type for the NetBackup server. Default is Primary server.
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.
Subnet ID	Select the subnet that is within the selected VPC, where the NetBackup server should be deployed.

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

Parameters	Description
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
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

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

Parameters	Description
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 the primary server

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

Table 4-4 NetBackup installation parameters for the primary server

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 (!@#$%^&*).
Confirm NetBackup Web User Password	Password must be at least 8 characters long which includes a number, a lower case, an upper case and a special character (!@#$%^&*).

Table 4-4 NetBackup installation parameters for the primary server *(continued)*

Parameters	Description
NetBackup Server Name	Provide a name for the NetBackup server. Must be a valid name with a minimum length of 8 characters and it should not start with minus sign (-), dot (.) and a number.
User for Services on NetBackup Server	Provide a non-root Service Username. It is used to run NetBackup services and is set as database user as well. It will not be accessible via SSH. Most services on the server run as this user. User gets created and gets associated with the 'nbwebgrp' user group as the secondary group. Refer to the *Running NetBackup services with non-privileged user (service user) account* chapter in the NetBackup Security and Encryption Guide.
IAM Role	Name of the existing IAM role to be attached to the NetBackup primary server instance. The role must have all required permissions and include policy for Secrets Manager to store password for Web UI user.See "IAM role required for the primary server" on page 19.

IAM role required for the primary server

Below table states the details of permission of IAM role required for the primary server:

Table 4-5 Permission of IAM role required for the primary server

Action	Resource
■ secretsmanager:GetResourcePolicy ■ secretsmanager:GetSecretValue ■ secretsmanager:DescribeSecret ■ secretsmanager:DeleteSecret ■ secretsmanager:ListSecretVersionIds	*

Note: Refer IAMRoleCreation and IAMPolicyCreation for creating IAM role and policies.

NetBackup installation parameters for Media server

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

Table 4-6 NetBackup installation parameters for Media server

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 Service Username on Media Server	Provide a Service Username. Most services on the server will run as this user. If a non-root username is provided, then the user will be created. Refer to the *Running NetBackup services with non-privileged user (service user) account* chapter in the *NetBackup Security and Encryption Guide*. It is recommended to provide the non-root user for service user on Media Server.
NetBackup Token	Enter the NetBackup authorization token key for the media server generated from an existing the primary server. Refer to the *NetBackup Security and Encryption Guide*.

NetBackup installation parameters for Cloud Recovery server

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

Table 4-7 NetBackup installation parameters for Cloud Recovery server

Parameters	Description
Instance Configuration Parameters	
NetBackup Server Configuration	Select the configuration type for the Netbackup Server. Choose CRS server to deploy CRS server.

Table 4-7 NetBackup installation parameters for Cloud Recovery server *(continued)*

Parameters	Description
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
Use an Existing VPC?	Select **True** if you want to deploy the Cloud Recovery server into an existing VPC. Select **False** to deploy the Cloud Recovery server in a new VPC that will be created during the deployment.
VPC and Subnet details for deployment in existing VPC	
See "VPC and Subnet details for deployment in existing VPC" on page 16.	
VPC and Subnet configuration for deployment in new VPC (Required only if new VPC has been selected above)	
See "VPC and Subnet configuration for deployment in new VPC" on page 17. **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	
IAM Role Name	Name of existing IAM role for Cloud Recovery server. The role must have all required permissions.See "IAM role required for Cloud Recovery Server" on page 22.
NetBackup Server Name	Provide a name for the Primary server. Must be a valid name with a minimum length of 8 characters and it should not start with minus sign (-), dot (.) and a number.

Table 4-7 NetBackup installation parameters for Cloud Recovery server *(continued)*

Parameters	Description
User for Services on NetBackup Server	Provide a non-root Service Username. It is used to run NetBackup services and is set as database user as well. It will not be accessible via SSH. Most services on the server is run as this user. User gets created and is associated with the 'nbwebgrp' user group as the secondary group. For more details, refer to the *Running NetBackup services with non-privileged user (service user) account* chapter in the NetBackup Security and Encryption Guide..
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.
Service Host	Service host is required for NetBackup MSDP Disk pool configuration. **Note:** Ensure that you select the service host for the same region where Cloud Recovery Server deployment is being performed.

IAM role required for Cloud Recovery Server

Below table states the details of the permissions of IAM role required for Cloud Recovery Server:

Table 4-8 IAM roles for Cloud Recovery Server

■ ec2:CreateTags ■ ec2:DescribeImportImageTasks ■ ec2:ImportImage ■ ec2:DescribeImages ■ iam:ListRolePolicies ■ iam:ListRoles ■ iam:GetRole ■ iam:GetRolePolicy ■ iam:CreateRole ■ iam:PutRolePolicy ■ s3:ListAllMyBuckets	*
■ s3:*	Give this access only to the bucket and its objects where MSDP images are stored.

Note: Refer IAMRoleCreation and IAMPolicyCreation for creating IAM role and policies.

Chapter 5

Deploying Snapshot Manager

This chapter includes the following topics:

- Deploying Snapshot Manager server using the marketplace offer

Deploying Snapshot Manager server using the marketplace offer

From version , Snapshot Manager server is deployed as a separate offer on the marketplace. You need to follow the steps to deploy the Snapshot Manager on the AWS cloud.

To deploy Snapshot Manager server

1. Visit the AWS Marketplace at link.
2. Locate and access the **Veritas NetBackup Snapshot Manager (BYOL)**.
3. On the offer page, click **Continue to Subscribe**.
4. 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.
6. Provide a name for the Stack.
7. Provide the various configurations for NetBackup Snapshot Manager system, network, server, KMS, security etc. Refer to the section See "NetBackup installation parameters for Snapshot Manager server" on page 29.
8. Click Next to tag your stack for identification.
9. Review all the details and initiate the launch.

Prerequisites for using the Snapshot Manager template

Ensure that you configure the following before you launch a Snapshot Manager CloudFormation stack:

- Set up AWS SNS notifications by creating an SNS topic for the Snapshot Manager stack. This allows you to receive notification emails each time the Auto Scaling Group (ASG) is updated. The SNS topic must be configured in the same AWS region where the Snapshot Manager instance is being deployed.
  Getting started with Amazon SNS
- Create a key pair in the region where you want to launch the Snapshot Manager stack.
  Amazon EC2 key pairs and Linux instances
- If desired, set up a AWS customer master key (CMK) if you want to use AWS KMS with Snapshot Manager. This is not a mandatory requirement.
  Creating keys
- Create an AWS IAM role and assign permissions that are required by Snapshot Manager.
  See "Configuring AWS permissions for Snapshot Manager" on page 25.
  Snapshot Manager requires that you use AWS IAM for authenticating Snapshot Manager operations on the assets in the AWS cloud.
  Refer to the AWS documentation for more information on IAM roles.
  IAM roles for Amazon EC2

Configuring AWS permissions for Snapshot Manager

To protect your Amazon Web Services (AWS) assets, Snapshot Manager must first have access to them. You must associate a permission policy with each Snapshot Manager user who wants to work with AWS assets.

Ensure that the user account or role is assigned the minimum permissions required for Snapshot Manager.

To configure permissions on Amazon Web Services

1. Create or edit an AWS user account from Identity and Access Management (IAM).
2. Do one of the following.
   - To create a new AWS user account, do the following:
     - From IAM, select the **Users** pane and click **Add user**.
     - In the **User name** field, enter a name for the new user.

- Select the **Access** type. This value determines how AWS accesses the permission policy. (This example uses Programmatic access).
- Select **Next: Permissions**.
- On the **Set permissions for username** screen, select **Attach existing policies directly**.
- Select the previously created permission policy (shown below) and select **Next: Review**.
- On the **Permissions summary** page, select **Create user**.
- Obtain the **Access Key** and **Secret Key** for the newly created user.

- To edit an AWS user account, do the following:
  - Select **Add permissions**.
  - On the **Grant permissions** screen, select **Attach existing policies directly**.
  - Select the previously created permission policy (shown below), and select **Next: Review**.
  - On the **Permissions summary** screen, select **Add permissions**.

3 To configure the AWS plug-in for the created or edited user, refer to the plug-in configuration notes.

Resources created by the Snapshot Manager template

The following resources are created when you launch a Snapshot Manager stack using the Snapshot Manager CloudFormation template:

Table 5-1 Snapshot Manager CloudFormation template resources

Resource	Description
EBS Volume **(AWS::EC2::Volume)**	The volume size and availability zone are specified during the stack creation process.
EC2 Instance **(AWS::EC2::Instance)**	The instance type along with the required network and security configuration settings are specified during the stack creation process.
VolumeAttachment **(AWS::EC2::VolumeAttachment)**	An EBS volume gets attached to the Snapshot Manager EC2 instance that is created.

Table 5-1 Snapshot Manager CloudFormation template resources *(continued)*

Resource	Description
Instance Profile **(AWS::IAM::InstanceProfile)**	A new profile is created for the Snapshot Manager EC2 instance. This profile then assigns the specified IAM role to the EC2 instance.
IAM Role **(AWS::IAM::Role)**	A new IAM role is created and attached to the Snapshot Manager instance during the stack creation process. The role is assigned all the AWS permissions that Snapshot Manager requires. This new role is created only if you have not specified any existing IAM role name in the CFT form (the Snapshot Manager System Configuration > IAM Role field is empty).
Security Group **(AWS::EC2::SecurityGroup)**	An AWS security group is created internally for the Snapshot Manager deployment. The security group contains rules that allow inbound and outbound traffic for the following: ■ SSH on port 22 ■ RabbitMQ on port 5671 ■ HTTPS on port 443 Refer to the AWS documentation for more information on security groups: Control traffic to resources using security groups
Launch Configuration **(AWS::AutoScaling::LaunchConfiguration)**	A new launch configuration is created and is then used by the Auto Scaling Group (ASG) to scale the instance if the original Snapshot Manager EC2 instance status is marked as unhealthy.

Table 5-1 Snapshot Manager CloudFormation template resources *(continued)*

Resource	Description
Auto Scaling Group **(AWS::AutoScaling::AutoScalingGroup)**	A new Auto Scaling Group (ASG) is created and the Snapshot Manager instance is attached to it. If the original Snapshot Manager EC2 instance becomes unhealthy, this ASG automatically creates a new Snapshot Manager instance and attaches the existing Snapshot Manager metadata volume to the new instance.

Snapshot Manager EC2 instance configuration details

When you deploy a Snapshot Manager stack using the CloudFormation template, the following configuration is created on the EC2 instance where Snapshot Manager is deployed:

- A disk is attached to the instance and a file system of type ext4 is created on the disk.
- The file system is mounted as a folder mount at `/cloudpoint`.
- Snapshot Manager is installed and the specified user account is configured as the Snapshot Manager administrator.
- The Snapshot Manager AWS plug-in is configured with the Source Account configuration. The IAM role that is attached to the Snapshot Manager instance is used for the plug-in configuration.

Instance failures and Auto Scaling Group behavior

The Amazon EC2 Auto Scaling Group (ASG) monitors the Snapshot Manager EC2 instance periodically. The ASG determines the status of the instance using the default status checks or via custom health checks. After the instance passes the status checks, the instance is marked as healthy. If the state of the instance changes due to an external event, for example--if a disaster causes a loss of the instance, or if you manually stop the instance, the ASG immediately marks the instance as unhealthy and schedules it for a replacement.

The ASG creates a new instance from the same Amazon Machine Instance (AMI) and uses the same configuration as that of the original instance that was configured earlier. The ASG creates a new EBS volume using the snapshot, attaches that volume to the new EC2 instance, and then brings Snapshot Manager up on that instance. You can suspend the health check process if you do not want ASG to

replace the instance, for example in cases where you want to stop the instance for maintenance purposes.

For more information on how the Amazon EC2 Auto Scaling works, refer to the following Amazon AWS documentation:

Health checks for Auto Scaling instances

NetBackup installation parameters for Snapshot Manager server

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

Table 5-2 NetBackup installation parameters for Snapshot Manager server

Parameters	Description
Snapshot Manager System Configuration	
EC2 Instance Type	Select the EC2 instance type that you want to use for the Snapshot Manager instance.
Volume Size	Enter the size (in GB) of the EBS volume that will be attached to the Snapshot Manager instance.
IAM Role	Name of the role to be attached to the Snapshot Manager instance (A new IAM Role will be created if this field is left empty). Following permissions are required for the IAM role.See "IAM role required for Snapshot Manager instance" on page 32.
Snapshot Manager Upgrade Configuration (Applicable only in case of upgrade)	
EBS Volume ID	ID of an existing EBS volume
Volume Snapshot ID	ID of the Snapshot Manager metadata volume snapshot.
Network Configuration	
Snapshot Manager VPC	Select ID of existing VPC where Snapshot Manager instance will be deployed.
Snapshot Manager Subnet	Select ID of existing subnet in your VPC where Snapshot Manager instance will be deployed.

Table 5-2 NetBackup installation parameters for Snapshot Manager server *(continued)*

Parameters	Description
Availability Zone	Name of an existing EC2 Availability Zone in which the Snapshot Manager instance will be created.
Snapshot Manager Domain Name	Domain name must correspond to an existing Route53 Hosted Zone associated with this VPC, or it must be a new domain for which a Hosted Zone will be created with the deployment.
Inbound Access CIDR	If you choose to create a new virtual network, you can provide the CIDR block from which the Snapshot Manager server can be accessed.
Elastic IP	Elastic IP to be assigned to Snapshot Manager instance.
HTTP Proxy	Provide the HTTP proxy value to configure Snapshot Manager with proxy server.
HTTPS Proxy	Provide the HTTPS proxy value to configure Snapshot Manager 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`
Snapshot Manager Configuration	
Snapshot Managerserver name	Provide the server name with which you want to enable the access to Snapshot Manager. The installer uses this name to generate a TLS certificate for the Snapshot Manager host.
Port	Select the port through which the Snapshot Manager server can communicate. Default is port 443.
Snapshot Manager Recovery Notification Configuration	

Table 5-2 NetBackup installation parameters for Snapshot Manager server *(continued)*

Parameters	Description
SNS Topic ARN	ARN of the SNS Topic to get notifications on any update in the Snapshot Manager Auto Scaling Group (Leave this field blank if notifications are not required)
Snapshot Manager KMS configuration	
CMK ID	ID of the customer master key using which KMS would be configured with Snapshot Manager (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 Snapshot Manager is being deployed)
Security configuration	
Key Pair Name	Snapshot Manager instance
Snapshot Manager Registration with NetBackup	
NetBackup server	Provide a Fully Qualified Domain Name of the existing the primary server to which the Snapshot Manager server needs to be associated. Configuration fails if the FQDN is not resolvable from this Snapshot Manager server.
NetBackup API Key	As a NetBackup user, provide a valid API key generated from the existing the primary server to validate the communication between the primary server and the Snapshot Manager server. The user generating API keys must have permission to add the Snapshot Manager server. Creating and managing API keys for users (Administrators) Adding and managing your API key (Users)

IAM role required for Snapshot Manager instance

Table 5-3 IAM roles for Snapshot Manager instance

SID	Effect	Action	Resource
EC2AutoScaling	Allow	■ autoscaling:UpdateAutoScalingGroup ■ autoscaling:AttachInstances	*
KMS	Allow	■ kms:ListKeys ■ kms:Encrypt ■ kms:Decrypt ■ kms:ReEncryptTo ■ kms:DescribeKey ■ kms:ListAliases ■ kms:GenerateDataKey ■ kms:GenerateDataKeyWithoutPlaintext ■ kms:ReEncryptFrom ■ kms:CreateGrant	*
RDSBackup	Allow	■ rds:DescribeDBSnapshots ■ rds:DescribeDBClusters ■ rds:DescribeDBClusterSnapshots ■ rds:DeleteDBSnapshot ■ rds:CreateDBSnapshot ■ rds:CreateDBClusterSnapshot ■ rds:ModifyDBSnapshotAttribute ■ rds:DescribeDBSubnetGroups ■ rds:DescribeDBInstances ■ rds:CopyDBSnapshot ■ rds:CopyDBClusterSnapshot ■ rds:DescribeDBSnapshotAttributes ■ rds:DeleteDBClusterSnapshot ■ rds:ListTagsForResource ■ rds:AddTagsToResource ■ rds:DescribeDBClusterParameterGroups	*

Table 5-3 IAM roles for Snapshot Manager instance *(continued)*

SID	Effect	Action	Resource
RDSRecovery	Allow	■ rds:ModifyDBInstance' ■ rds:ModifyDBClusterSnapshotAttribute' ■ rds:RestoreDBInstanceFromDBSnapshot' ■ rds:ModifyDBCluster ■ rds:RestoreDBClusterFromSnapshot ■ rds:CreateDBInstance ■ rds:RestoreDBClusterToPointInTime' ■ rds:CreateDBSecurityGroup ■ ds:CreateDBCluster ■ rds:RestoreDBInstanceToPointInTime	*

Table 5-3 IAM roles for Snapshot Manager instance *(continued)*

SID	Effect	Action	Resource
EC2Backup	Allow		*

Table 5-3 IAM roles for Snapshot Manager instance *(continued)*

SID	Effect	Action	Resource
		■ sts:GetCallerIdentity ■ ec2:CreateSnapshot ■ ec2:DescribeInstances' ■ ec2:DescribeInstanceStatus ■ ec2:ModifySnapshotAttribute ■ ec2:CreateImage ■ ec2:CopyImage ■ ec2:CopySnapshot' ■ ec2:DescribeSnapshots ■ ec2:DescribeVolumeStatus ■ ec2:DescribeVolumes ■ ec2:RegisterImage ■ ec2:DescribeVolumeAttribute ■ ec2:DescribeSubnets ■ ec2:DescribeVpcs ■ ec2:DeregisterImage ■ ec2:DeleteSnapshot ■ ec2:DescribeInstanceAttribute ■ ec2:DescribeRegions ■ ec2:ModifyImageAttribute ■ ec2:DescribeAvailabilityZones ■ ec2:ResetSnapshotAttribute ■ ec2:DescribeHosts ■ ec2:DescribeImages ■ ec2:AssociateAddress ■ ec2:DescribeNetworkInterfaces ■ ec2:DescribeSecurityGroups ■ ec2:AuthorizeSecurityGroupEgress ■ ec2:AuthorizeSecurityGroupIngress ■ ec2:CreateSnapshots ■ ec2:GetEbsEncryptionByDefault ■ ec2:DescribeKeyPairs ■ ec2:ModifyInstanceMetadataOptions ■ secretsmanager:GetResourcePolicy ■ secretsmanager:GetSecretValue ■ secretsmanager:DescribeSecret ■ secretsmanager:RestoreSecret ■ secretsmanager:PutSecretValue	

Table 5-3 IAM roles for Snapshot Manager instance *(continued)*

SID	Effect	Action	Resource
		■ secretsmanager:DeleteSecret ■ secretsmanager:UpdateSecret	
SSM	Allows	■ ssm:CreateDocument ■ ssm:DescribeDocument ■ ssm:DescribeInstanceInformation ■ ssm:GetCommandInvocation ■ ssm:SendCommand ■ ssm:UpdateDocumentDefaultVersion ■ ssm:UpdateDocument	
EC2Recovery	Allows	■ ec2:RunInstances ■ ec2:AttachNetworkInterface ■ ec2:DetachVolume ■ ec2:AttachVolume ■ ec2:DeleteTags ■ ec2:CreateTags ■ ec2:StartInstances ■ ec2:StopInstances ■ ec2:TerminateInstances ■ ec2:CreateVolume ■ ec2:DeleteVolume ■ ec2:DescribeIamInstanceProfileAssociations ■ ec2:AssociateIamInstanceProfile ■ ec2:DescribeInstanceTypeOfferings	*
SNS	Allow	■ sns:Publish ■ sns:GetTopicAttributes	*
IAM	Allow	■ iam:SimulatePrincipalPolicy ■ iam:ListAccountAliases	*
EBS	Allow	■ ebs:ListSnapshotBlocks ■ ebs:StartSnapshot ■ ebs:CompleteSnapshot ■ ebs:PutSnapshotBlock ■ ebs:ListChangedBlocks ■ ebs:GetSnapshotBlock	*

Table 5-3 IAM roles for Snapshot Manager instance *(continued)*

SID	Effect	Action	Resource
Route53	Allow	■ route53:CreateHostedZone ■ route53:ListHostedZones ■ route53:GetHostedZone ■ route53:ListResourceRecordSets ■ route53:ChangeResourceRecordSets ■ route53:ListResourceRecordSets ■ route53:ListHostedZonesByName	*

AWS endpoints used by Snapshot Manager

When Snapshot Manager connects to AWS, it uses the following endpoints:

Endpoints

secretsmanager.*.amazonaws.com

eks.*.amazonaws.com

autoscaling.*.amazonaws.com

ec2.*.amazonaws.com

sts.amazonaws.com

rds.*.amazonaws.com

kms. *.amazonaws.com

ebs.*.amazonaws.com

iam.amazonaws.com

Chapter 6

Encryption enabled NetBackup primary server

This chapter includes the following topics:

- Additional steps on CRS if encryption is enabled NetBackup primary server

Additional steps on CRS if encryption is enabled NetBackup primary server

Below are the additional steps to be done on Cloud Recovery Server, if the encryption is enabled on Netbackup primary server.

When KMS encryption is enabled, you can share the images in S3 bucket to the Cloud Recovery Server host with manual KMS key transfer.

On-premises KMS key changes:

In case of KMS key changes, for the given group for on-premises storage server after the Cloud Recovery Server host is set up, you must export the key file from on-premises KMS server and import that key file on the cloud recovery host.

On-premises NetBackup master server: Exports the key group with a passphrase to a file:

```
/usr/openv/netbackup/bin/admincmd/nbkmsutil -export -key_groups
<key-group-name> -path <key file path>
```

Cloud Recovery Server host (cloud side):

1. Copy the exported key to the Cloud Recovery Server host.
2. Config KMS server:

```
/usr/openv/netbackup/bin/nbkms -createemptydb
/usr/openv/netbackup/bin/nbkms /usr/openv/netbackup/bin/nbkmscmd
-discovernbkms -autodiscover
```

3. Import keys to KMS service.

   ```
   /usr/openv/netbackup/bin/admincmd/nbkmsutil -import -path <key
   file path> -preserve_kgname
   ```

4. Once this is done we need to restart the NetBackup.

   Refer below link for more details.

Chapter 7

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 as follows:

Launch the NetBackup Web UI using https://<primaryserver>/webui/login.

You can access the primary server Web UI using the hostname of the deployed NetBackup primary server. Make sure that the hostname is resolvable from the server where you are accessing the Web UI.

There are more ways to access the NetBackup Web UI. Refer to the *Sign in to the NetBackup Web UI* section in the *NetBackup Web UI Administrator's Guide*, and start managing and protecting your assets.

Chapter 8

Upgrade NetBackup Snapshot Manager from AWS Marketplace

This chapter includes the following topics:

- Upgrade NetBackup Snapshot Manager from AWS Marketplace
- Upgrade Snapshot Manager deployment using new AWS CloudFormation stack

Upgrade NetBackup Snapshot Manager from AWS Marketplace

The upgrade process is similar to when you are deploying a new instance using the Snapshot Manager CFT. Upgrading a Snapshot Manager CloudFormation stack difference is in some of the parameters where you are required to specify the values used in the existing Snapshot Manager deployment.

Prerequisites for the upgrade:

Perform the following steps before you proceed with the upgrade:

1. Gather the following details about the existing Snapshot Manager instance; these are required later during the actual upgrade:
   - Snapshot Manager metadata volume ID.
     Perform the following steps to get the volume ID
     - In the AWS Console, from the menu on the left, click Services, and then from under Management & Governance, click CloudFormation

- From the list of stacks, click on the Snapshot Manager stack and then click the Resources tab.
- From the list of resources displayed, locate a volume of type of AWS::EC2::Volume and Logical ID as NewVolume. This is the volume that contains the Snapshot Manager metadata.
- Copy the entry that appears in the Physical ID column. The entry is of the format vol-123456abc789 and it represents the volume ID.

- Snapshot Manager metadata disk snapshot ID.
  Using the Snapshot Manager metadata volume ID that you noted earlier, perform the following steps to find out the metadata disk's snapshot ID:
  - In the AWS console, from the menu on the left, click **Services**, and then from under **Compute**, click **EC2**.
  - From the EC2 dashboard navigation menu on the left, under **Elastic Block Store**, click **Snapshots**.
  - Search for the snapshot ID using the Snapshot Manager metadata volume ID as the search parameter.
  - Copy the snapshot ID listed under the Snapshot ID column.
- AWS IAM role that is attached to the Snapshot Manager configuration.
- AWS Elastic IP that is associated with the Snapshot Manager instance.
- AWS SNS Topic ARN that is created for the existing Snapshot Manager stack. If required, you can also use another SNS topic ARN altogether.

2. Verify that there are no protection policy snapshot or other operations in progress.
3. Login to NetBackup and disable the Snapshot Manager.

4 Stop Snapshot Manager gracefully. Log on to the Snapshot Manager instance and then run the following command:

```
# sudo podman run --rm -it -v /cloudpoint:/cloudpoint -v
/var/run/podman.sock:/var/run/podman.sock
veritas/flexsnap-deploy:current_version stop
```

OR

```
# flexsnap_configure stop
```

The Snapshot Manager containers are stopped one by one. Messages similar to the following appear on the command line:

```
Stopping the services

Stopping container: flexsnap-agent.e425d969dd4 ...done

Stopping container: flexsnap-agent.4704fd318322 ...done

Stopping container: flexsnap-fluentd ...done

Stopping container: flexsnap-mongodb ...done

Stopping container: flexsnap-rabbitmq ...done

Stopping container: flexsnap_configure ... done
```

Wait for all the Snapshot Manager containers to be stopped.

5 Unmount the Snapshot Manager file system on the instance and then detach the Snapshot Manager metadata volume mounted at `/cloudpoint`. Type the following command on the instance:

```
# umount /cloudpoint
```

6 Disassociate the AWS Elastic IP that is assigned to the existing Snapshot Manager instance. From the AWS console, click on the EC2 Service and then from under Network and Security, select Elastic IPs. Select the Elastic IP address assigned to the instance and then click **Actions > Disassociate address** and then confirm the action. You will associate the same IP address with the newer instance later during the upgrade.

Upgrade Snapshot Manager deployment using new AWS CloudFormation stack

Note: Enter the above collected information against the respective attributes in Snapshot Manager Upgrade Configuration.

1. **Deploy the product**

- On clicking the Action button, you will see an option to **Launch CloudFormation Stack**, which will lead to the Launch page. Another option is, after searching for the product, you may directly on **Launch CloudFormation Stack**, which will lead to the Launch page. Select the delivery method, software version and region from the dropdown appearing on the screen.
- Click on **Continue to Launch** button after selecting the above fields.
- On the next page, you can review the configuration selected and choose how you wish to launch the software.
- From the "Choose Action" drop-down, select **Launch CloudFormation** and click on **Launch**.
- This will take you to the CloudFormation service page, where template source would be pre -filled. Click on **Next**.

2. **Fill in the CloudFormation Template**
   - **Stack Name**
     Unique stack name has to be provided. The name you specify would be the name of the stack created.
   - **Snapshot Manager System Configuration**
     - **EC2 Instance type (Mandatory):** Select a type from the drop down that appears. The default being t3.large.
     - **Volume Size (Mandatory):** Size of the volume which would be created as part of stack for CP metadata. Default is 60 GB.
     - **IAM role (Optional):** Specify IAM role name, which would be attached to the CP instance. Otherwise it would be created with the required permissions and would be attached to the CP instance.
   - **Snapshot Manager Upgrade Configuration**
     - EBS Volume ID (Optional): This is used in case of upgrade. Existing Volume ID which has Snapshot Manager metadata must be specified, which would be attached to the Snapshot Manager instance.
     - Volume Snapshot (Optional): This is used in case of upgrade. Existing Snapshot Manager metadata disk's snapshot ID must be specified. Volume would be created and attached to the Snapshot Manager instance from the snapshot.
   - **Network Configuration**
     - **Snapshot Manager VPC (Mandatory)**: Select a Virtual private network where you want to deploy Snapshot Manager instance. The drop-down

lists down the VPC IDs in the region where you are deploying Snapshot Manager.

- **Snapshot Manager Subnet (Mandatory):**From the drop down, select the ID of existing subnet in your VPC where you want to deploy Snapshot Manager instance. The drop -down lists down the subnet IDs in the region where you are deploying Snapshot Manager.
- **Availability Zone (Mandatory):** From the drop down that appears, choose a zone in which the volume or snapshot exists for upgrade
- **Snapshot Manager Domain Name (Mandatory):** Domain name must correspond to an existing Route53 Hosted Zone associated with this VPC, or it must be a new domain for which a Hosted Zone will be created with the deployment.
- **Inbound Access CIDR(Mandatory):**The Inbound Access CIDR would be used to create a Security Group for Snapshot Manager. The traffic from the CIDR mentioned would be allowed to the Snapshot Manager.
- **Elastic IP (Optional):**Specify an Elastic IP which was dissociated from the previous deployment in case the selected network type is Public, which would be assigned to Snapshot Manager instance.
- **HTTP Proxy (Optional):**Specify HttpProxy environment variable to configure Snapshot Manager with proxy server
- **HTTPS Proxy (Optional):** Specify HttpsProxy environment variable to configure Snapshot Manager with proxy server.
- **No Proxy (Optional):** Specify NoProxy environment variable to configure Snapshot Manager with proxy server.

- **Snapshot Manager Configuration**
  - Snapshot Manager server name (Optional): Provide the server name with which you want to enable the access to Snapshot Manager. The installer uses this name to generate a TLS certificate for the Snapshot Manager host.
- **Security Configuration**
  - SNS Topic ARN (Optional): The ARN of a SNS topic to receive notifications when ASG scales to address the disaster.
- **Snapshot Manager Recovery Notification Configuration**
  - SNS Topic ARN (Optional): The ARN of a SNS topic to receive notifications when ASG scales to address the disaster.
- **Snapshot Manager KMS Configuration**

- Customer's Mater Key ID (Optional): ID of the customer's master key to configure KMS with Snapshot Manager, if KMS need to be configured.
- Customer's Master Key's Region (Optional): The region in which the above mentioned key is present. Optional, if the region is same as the region in which Snapshot Manager is deployed.

- **Snapshot Manager Registration with NetBackup**
  - Provide a Fully Qualified Domain Name (FQDN) of the existing the primary server to which the Snapshot Managerserver needs to be associated. Configuration fails if the FQDN is not resolvable from this Snapshot Managerserver.
  - **NetBackup server name and NetBackup API Key :** Provide a valid API key generated from the existing the primary server to validate the communication between the primary server and the Snapshot Managerserver. The user generating API keys must have permission to add the Snapshot Manager server.

3. **Confirm and Create the stack**
   - In the next page, user needs to specify information such as Tags, Permissions, Rollback Triggers, and some other additional options for the stack, like notification options and a stack policy.
   - The next page allows you to review your inputs and asks for the acknowledgment that the AWS CFT may create some IAM resources.
   - Click on the **Create** button.
   - This will now take you the page where all the stacks are listed. You can view the status of the stack you just created.

Perform the following steps before you proceed with the upgrade:

1 Check for the status of the CloudFormation stack created.

2 Delete the stack created by the previous deployment.

3 After the stack creation is successful, perform any one of the action from the below:

- a. If the hostname of the Snapshot Manager server remains same, enable the Snapshot Manager server from the NetBackup primary server.
- b. If the hostname of the Snapshot Manager server is changed, you will have to upgrade the NetBackup to the latest version and then again add the Snapshot Manager to the upgraded NetBackup primary server.

Chapter 9

Troubleshooting

This chapter includes the following topics:

- Troubleshooting

Troubleshooting

This section lists the troubleshooting issues and their respective workaround for different deployment issues.

Deployment logs

Table 9-1 Deployment logs for NetBackup and Snapshot Manager

Product name	Path
NetBackup	The NetBackup installation logs can be found at `/root/NBSetup/userdata.log` on the appliance. . While the installation is going on, one can SSH to the server with `ec2-user` and check the logs using command `tail -f /var/log/userdata.log`.
Snapshot Manager	Path for log failures - `"/var/log/cfn-init-cmd.log` These are explicit log failures required while deploying Snapshot Manager through cloud formation template.

Unable to login with NetBackup Web Username provided while deploying the primary server

Steps to resolve the issue:

- Edit the security group of the NetBackup server to allow SSH access on port 22. Ensure that 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.
- 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.

No assets are displayed post NetBackup and Snapshot Manager deployment

Resolution:

When no assets are listed under the Virtual Machines tab for Cloud Workload, but you see your region configured for AWS provider, then as part of deployment trigger a manual discovery for the attached Snapshot Manager.