Veritas NetBackup CloudPoint™ Quick Start Guide for AWS

What is NetBackup CloudPoint?

Veritas NetBackup CloudPoint is an integrated cloud-native feature of NetBackup, a leading enterprise data protection solution that's simple to deploy, easy to scale, and cost-effective to run. NetBackup CloudPoint is available to all users deploying NetBackup 8.3 or newer at no additional cost.

Highlights:

- Easy to deploy.
- NetBackup integration: Natively integrates with NetBackup for centralized visibility, reporting, Role Based Access Control (RBAC) and compliance across physical, virtual, and cloud workloads.
- Disk, File and Database level recovery, application consistent snapshot.
- Replicate across AWS regions and accounts for DR readiness. Allow Rollback, Original and Alternate location restores.
- Modular architecture for rapid workload integration

KEY FEATURES

- Snapshot-based data protection
- Automated scheduling and creation
- Multi-cloud visibility and orchestration
- Auto-deletion of expired snapshots
- Fast RPO and RTO
- Deep integration with storage arrays, and public cloud platforms
- Modular architecture for rapid workload proliferation
- Intuitive interface and reporting
- NetBackup integration

Deploy NetBackup CloudPoint from AWS Marketplace

1 Deploy the product

- On clicking the Action button, you will see an option to "Launch

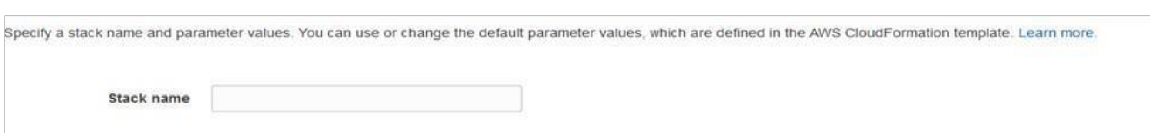
  CloudFormation Stack", which will lead to the Launch page. Another option is, after searching for the product, you may directly on "Launch CloudFormation Stack", which will lead to the Launch page. Select the delivery method, software version and region from the dropdown appearing on the screen.

- 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.



- CloudPoint System Configuration

  ○ OS type (Mandatory):

  Select an OS from the drop down that appears.

  ○ EC2 Instance type (Mandatory):

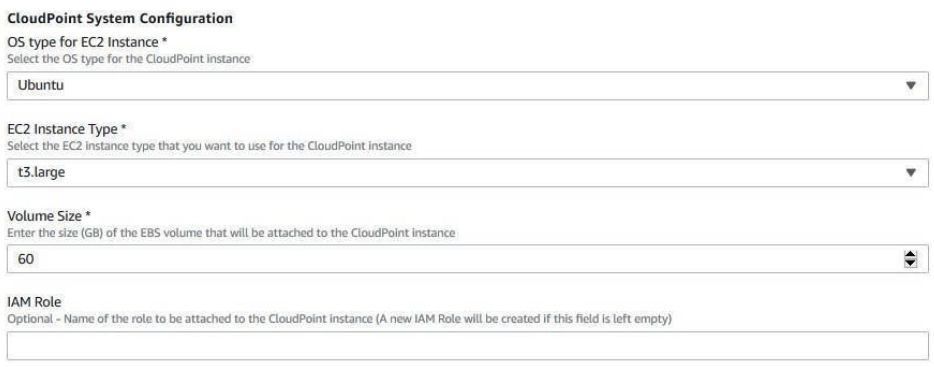
  Select a type from the drop down that appears. The default being t3.large.

  ○ 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.



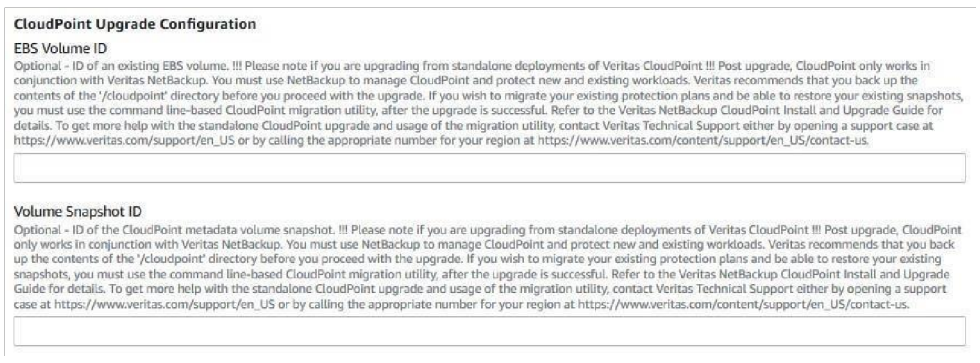
- CloudPoint Upgrade Configuration

○ EBS Volume ID (Optional):

This is used in case of upgrade. Existing Volume ID which has CP metadata must be specified, which would be attached to the CP instance.

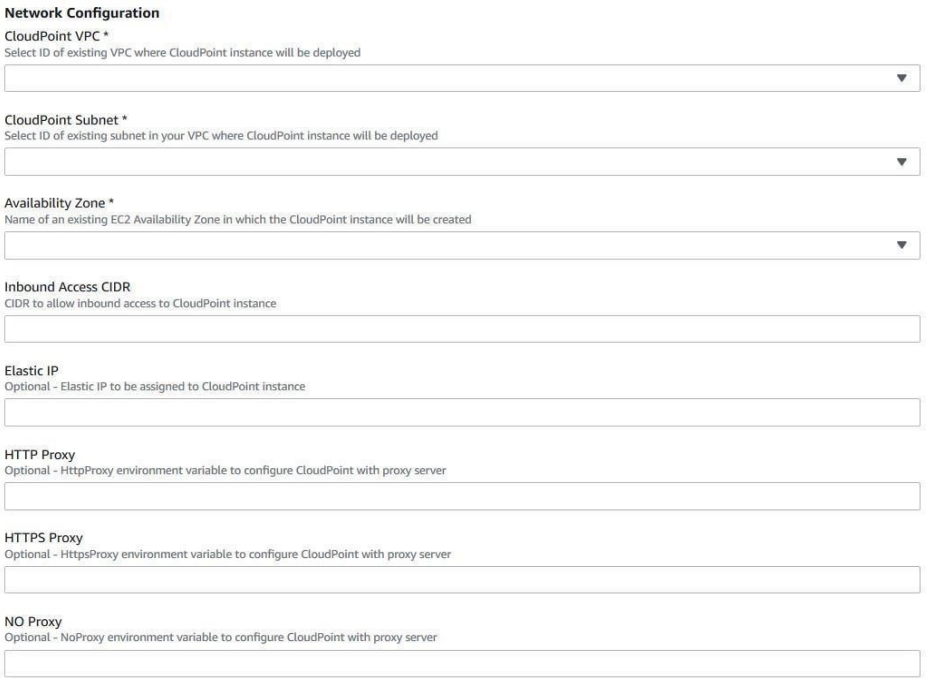
○ Volume Snapshot (Optional):

This is used in case of upgrade. Existing CP metadata disk's snapshot ID must be specified. Volume would be created and attached to the CP instance from the snapshot.

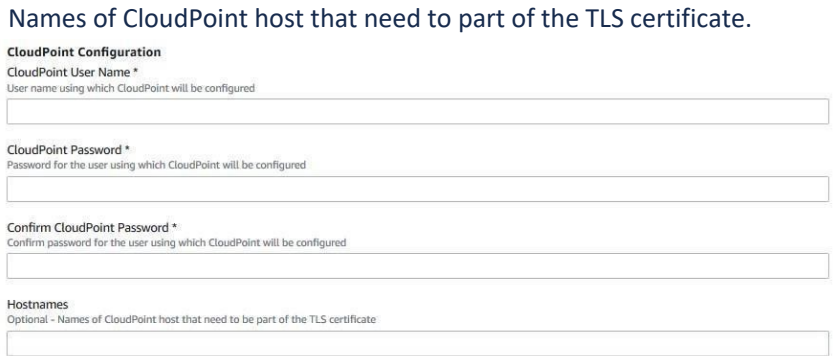


- Network Configuration

- CloudPoint VPC (Mandatory):
  Select a Virtual private network where you want to deploy CloudPoint instance. The drop-down lists down the VPC IDs in the region where you are deploying CP.
- CloudPoint Subnet (Mandatory):
  From the drop down, select the ID of existing subnet in your VPC where you want to deploy CloudPoint instance. The drop-down lists down the subnet IDs in the region where you are deploying CP.
- Availability Zone (Mandatory):
  From the drop down that appears, choose a zone in which the volume or snapshot exists for upgrade.
- Inbound Access CIDR(Mandatory):
  The Inbound Access CIDR would be used to create a Security Group for CloudPoint. The traffic from the CIDR mentioned would be allowed to the CloudPoint.
- 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 CloudPoint instance.
- HTTP Proxy (Optional):
  Specify HttpProxy environment variable to configure CloudPoint with proxy server
- HTTPS Proxy (Optional):
  Specify HttpsProxy environment variable to configure CloudPoint with proxy server
- No Proxy (Optional):
  Specify NoProxy environment variable to configure CloudPoint with proxy server



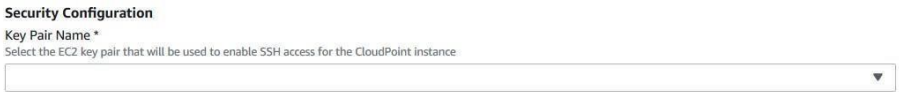
- CloudPoint Configuration
- CloudPoint username (Mandatory):
  The email of user using which CloudPoint would be configured. In case of upgrades, provide the email used in the previous deployment.
- CloudPoint password (Mandatory):
  Password for the user using which CloudPoint would be configured. In case of upgrades, provide the password used in the previous deployment.
- Confirm CloudPoint Password (Mandatory):
  Confirm password for the user using which CloudPoint would be configured. In case of upgrades, provide the password used in the previous deployment.
- Hostnames (Optional):
  Names of CloudPoint host that need to part of the TLS certificate.



Security Configuration

- SNS Topic ARN (Optional):

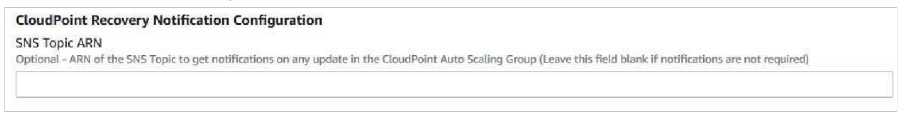
The ARN of a SNS topic to receive notifications when ASG scales to address the disaster.



CloudPoint Recovery Notification Configuration

- SNS Topic ARN (Optional):

The ARN of a SNS topic to receive notifications when ASG scales to address the disaster.



• CloudPoint KMS Configuration

- Customer's Mater Key ID (Optional):
  ID of the customer's master key to configure KMS with CloudPoint, 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 CloudPoint is deployed.

4 Confirm and Create the stack

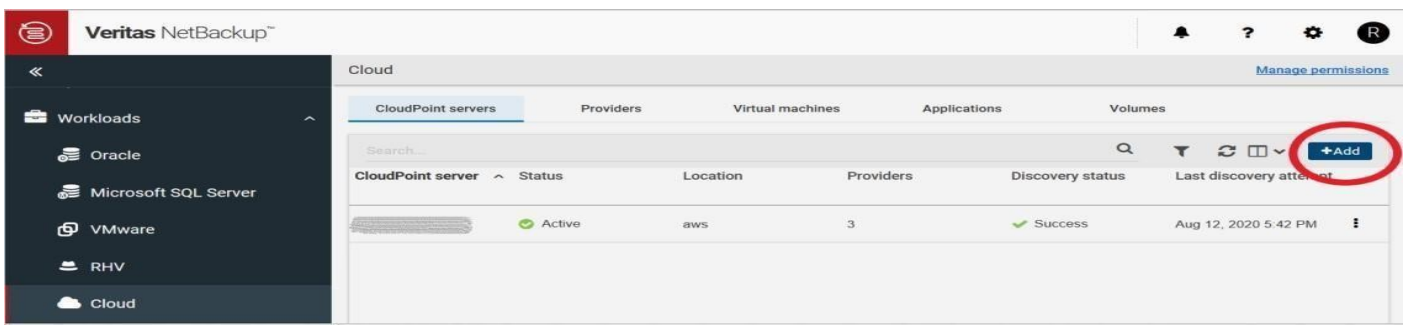
- In the next page, user needs to specify information such as Tags, Permissions, Rollback Triggers, and some other additional options for the stack, like notification options and a stack policy.
- The next page allows you to review your inputs and asks for the acknowledgement that the AWS CFT may create some IAM resource s.
- 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.

Register CloudPoint to NetBackup

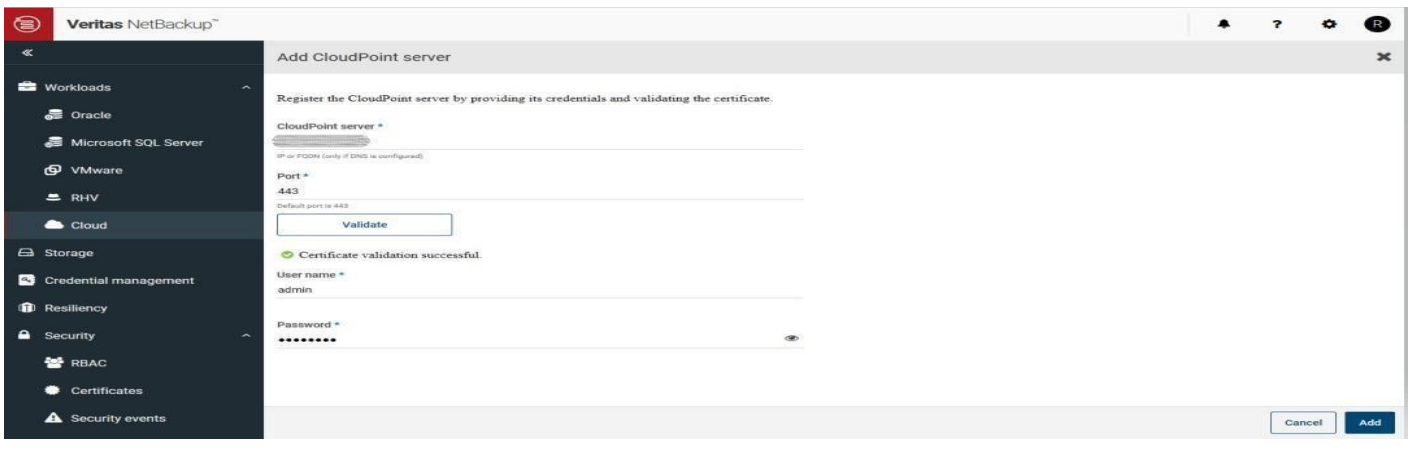
1 Add CloudPoint Server in NetBackup

- Login to NetBackup https://<nertbackupserver>/webui

  Go to Cloud section under Workloads tab and click "+Add" to add a new CloudPoint server.



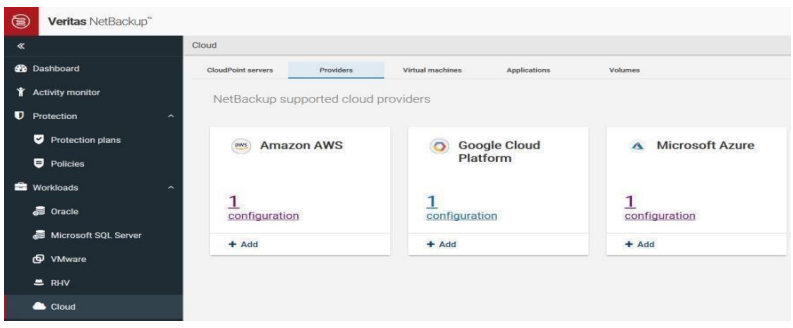
- Add CloudPoint server



- Wait the discovery status is successful for the newly added CloudPoint server.

2 Add Providers

- Add configurations for any of the cloud providers by clicking “+Add” below the Cloud provider to add a configuration for that cloud.

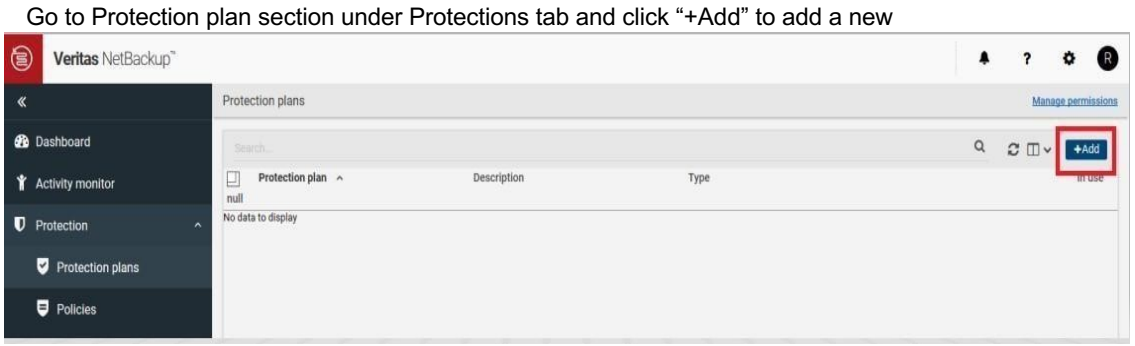


- Once the providers have been added successfully, you would see the providers against that cloud has been incremented accordingly and the status of discovery is successful.

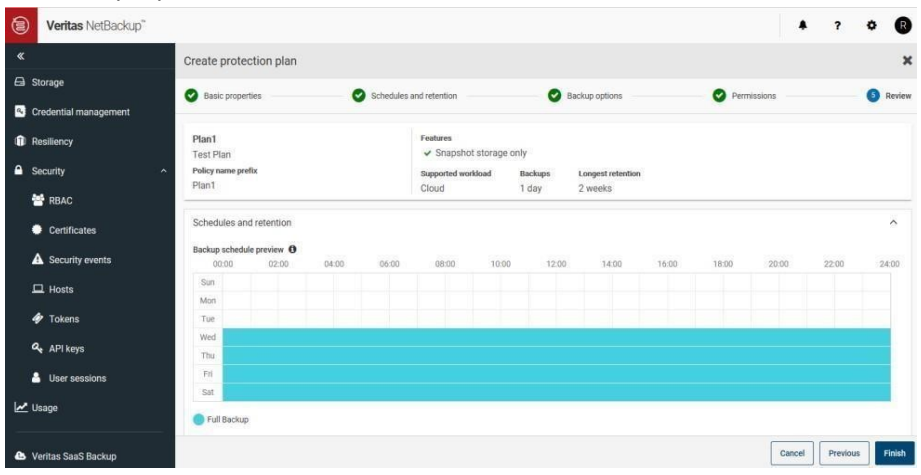
Protect an asset

1 Create a protection plan

- Go to Protection plan section under Protections tab and click “+Add” to add a new



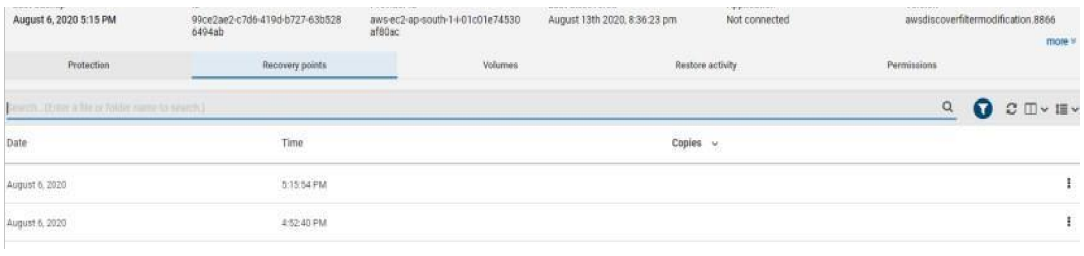
- Set the properties for the Protection Plan and click Finish to create a new.



2 Protect Assets

- Once the Protection Plan has been created you may select any asset form the virtual Machine tab of cloud section to protect a VM and add the Protection Plan for scheduled backups or do a “Backup now” and select the protection plan using which you want to back up the VM. Similarly, you may protect any volume/application.

- You may recover the assets by selecting the asset and going to the recovery section of the asset, and recover from the list of recovery points.



Upgrade NetBackup CloudPoint from AWS Marketplace

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

Prerequisites for the upgrade :

Perform the following steps before you proceed with the upgrade:

1. Gather the following details about the existing CloudPoint instance; these are required later during the actual upgrade:
   - CloudPoint 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 CloudPoint 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 CloudPoint 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.
   - CloudPoint metadata disk snapshot ID.
     Using the CloudPoint 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 CloudPoint 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 CloudPoint configuration.
   - AWS Elastic IP that is associated with the CloudPoint instance.
   - CloudPoint administrator username and password.
   - AWS SNS Topic ARN that is created for the existing CloudPoint 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. Stop CloudPoint gracefully. Log on to the CloudPoint instance and then run the following command:
   # sudo docker run --rm -it -v /cloudpoint:/cloudpoint -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-cloudpoint:current_version stop The CloudPoint 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
   Wait for all the CloudPoint containers to be stopped.
4. Unmount the CloudPoint file system on the instance and then detach the CloudPoint metadata volume mounted at /cloudpoint. Type the following command on the instance:
   # umount /cloudpoint
5. Disassociate the AWS Elastic IP that is assigned to the existing CloudPoint 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 with the newer instance later during the upgrade.

Perform the following steps to upgrade a CloudPoint deployment using a new AWS CloudFormation stack.

Note: Enter the above collected information against the respective attributes in **CloudPoint Upgrade Configuration**.

1 Deploy the product

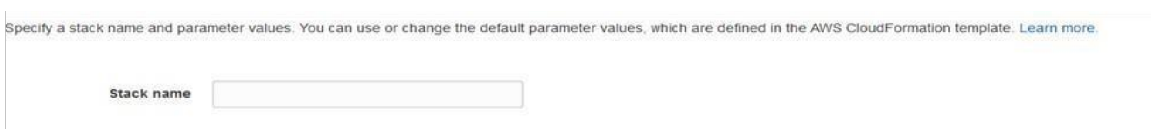
- On clicking the Action button, you will see an option to "Launch

  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".

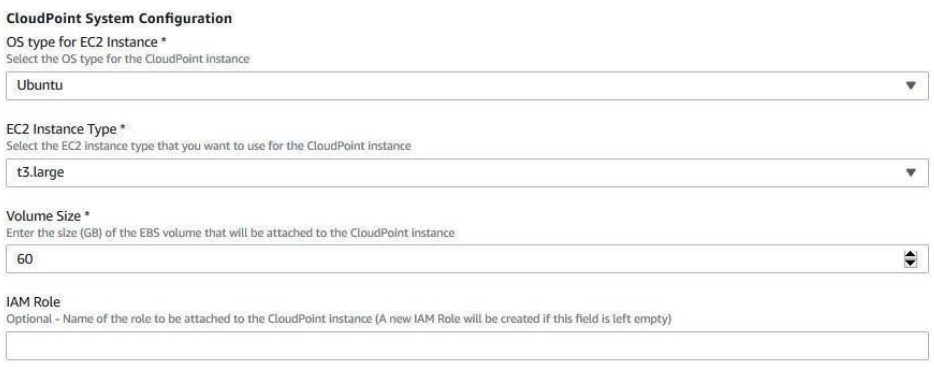
2 Fill in the CloudFormation Template

- Stack Name
  - Unique stack name has to be provided. The name you specify would be the name of the stack created.



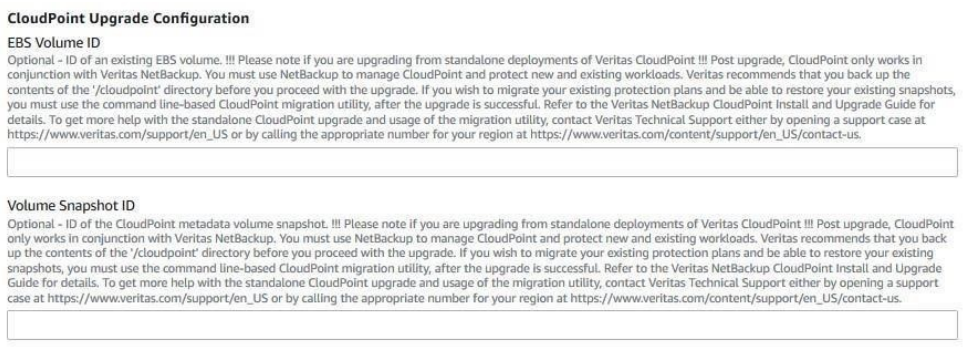
- CloudPoint System Configuration
    - OS type (Mandatory):
      Select an OS from the drop down that appears.
    - EC2 Instance type (Mandatory):

      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.



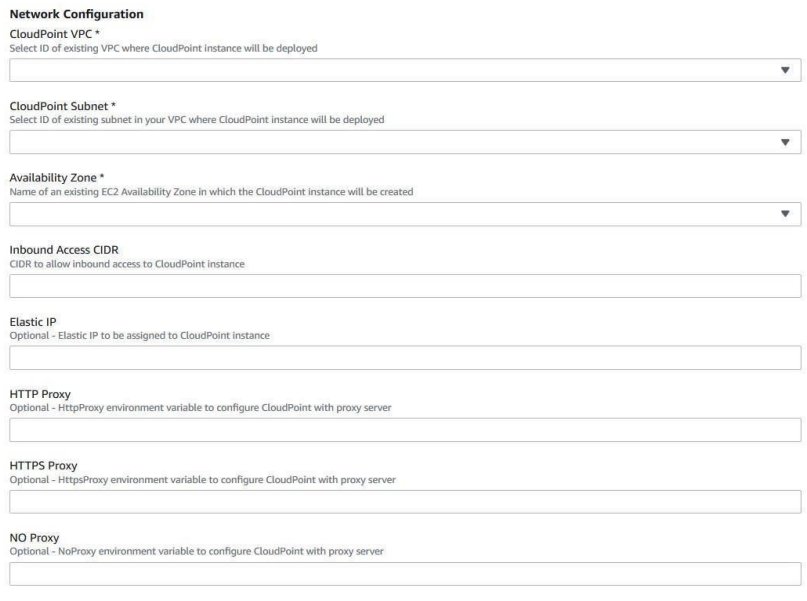
- CloudPoint Upgrade Configuration

- EBS Volume ID (Optional):
  This is used in case of upgrade. Existing Volume ID which has CP metadata must be specified, which would be attached to the CP instance.
- Volume Snapshot (Optional):
  This is used in case of upgrade. Existing CP metadata disk's snapshot ID must be specified. Volume would be created and attached to the CP instance from the snapshot.



- Network Configuration

- CloudPoint VPC (Mandatory):
  Select a Virtual private network where you want to deploy CloudPoint instance. The drop-down lists down the VPC IDs in the region where you are deploying CP.
- CloudPoint Subnet (Mandatory):
  From the drop down, select the ID of existing subnet in your VPC where you want to deploy CloudPoint instance. The drop-down lists down the subnet IDs in the region where you are deploying CP.
- Availability Zone (Mandatory):
  From the drop down that appears, choose a zone in which the volume or snapshot exists for upgrade.
- Inbound Access CIDR(Mandatory):
  The Inbound Access CIDR would be used to create a Security Group for CloudPoint. The traffic from the CIDR mentioned would be allowed to the CloudPoint.
- 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 CloudPoint instance.
- HTTP Proxy (Optional):
  Specify HttpProxy environment variable to configure CloudPoint with proxy server
- HTTPS Proxy (Optional):
  Specify HttpsProxy environment variable to configure CloudPoint with proxy server
- No Proxy (Optional):
  Specify NoProxy environment variable to configure CloudPoint with proxy server



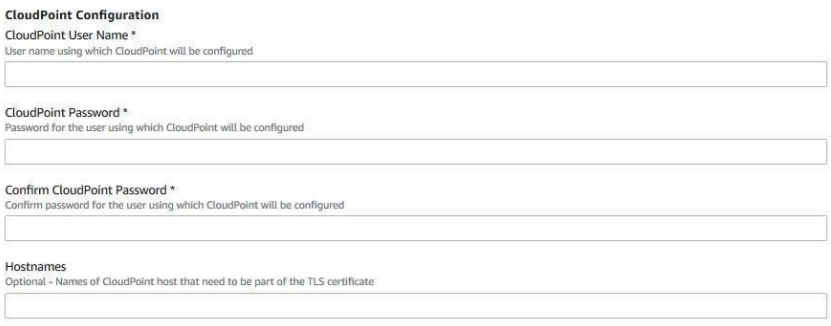
- CloudPoint Configuration

- CloudPoint username (Mandatory):
  The email of user using which CloudPoint would be configured. In case of upgrades, provide the email used in the previous deployment.

- CloudPoint password (Mandatory):
  Password for the user using which CloudPoint would be configured. In case of upgrades, provide the password used in the previous deployment.

- Confirm CloudPoint Password (Mandatory):
  Confirm password for the user using which CloudPoint would be configured. In case of upgrades, provide the password used in the previous deployment.

- Hostnames (Optional):
  Names of CloudPoint host that need to part of the TLS certificate.



Security Configuration

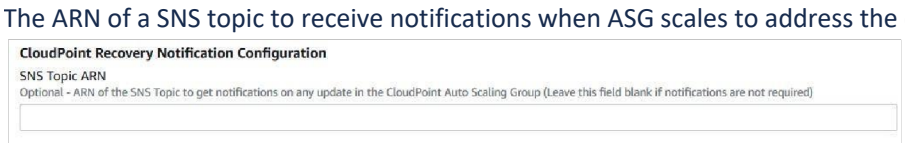
- SNS Topic ARN (Optional):

The ARN of a SNS topic to receive notifications when ASG scales to address the disaster.

CloudPoint Recovery Notification Configuration

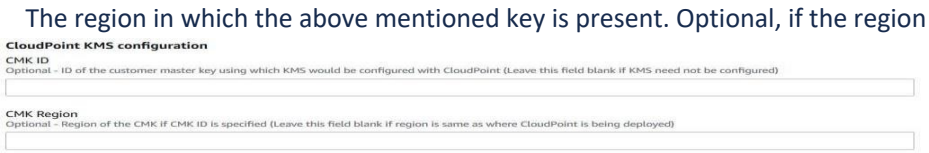
- SNS Topic ARN (Optional):

The ARN of a SNS topic to receive notifications when ASG scales to address the disaster.



- CloudPoint KMS Configuration

- Customer's Mater Key ID (Optional):
  ID of the customer's master key to configure KMS with CloudPoint, 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 CloudPoint is deployed.



4 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 acknowledgement 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:

- Check for the status of the CloudFormation stack created.
- Delete the stack created by the previous deployment.
- After the stack creation is successful, enable the CloudPoint server from NetBackup.

VERITAS The truth in information.