

This article describes how to configure high availability and automatic failover for NetApp SnapCenter software within AWS.

# SnapCenter High Availability using Virtual IP on AWS

NetApp SnapCenter software is an easy-to-use enterprise platform to securely coordinate and manage data protection across applications, databases, virtual machines, and file systems. SnapCenter simplifies backup, restore, and clone lifecycle management by offloading these tasks to application owners without sacrificing the ability to oversee and regulate activity on the storage systems. And by leveraging storage-based data management, it enables increased performance and availability, as well as reduced testing and development times.

Note: SnapCenter supports only 2-node configuration.

## License

By accessing, downloading, installing or using the content in this repository, you agree the terms of the License laid out in License file.

Note that there are certain restrictions around producing and/or sharing any derivative works with the content in this repository. Please make sure you read the terms of the License before using the content. If you do not agree to all of the terms, do not access, download or use the content in this repository.

Copyright: 2024 NetApp Inc.

## Features

The solution provides the following features:

- Continuous health check of the SMcore, MYSQL service along with EC2 instance availability
- Automatic failover to secondary SnapCenter EC2 instance incase of primary instance failure
- Perform manual fallback using the lambda function

## Pre-requisites

Before you begin, ensure that the following prerequisites are met:

- SnapCenter software is installed and configured on AWS EC2 instances with HA configuration across multiple Availability Zones

Note: For information on how to install SnapCenter Server, see [SnapCenter Installation and Setup Guide \(https://docs.netapp.com/us-en/snapcenter/install/task\\_install\\_the\\_snapcenter\\_server\\_using\\_the\\_install\\_wizard.html\)](https://docs.netapp.com/us-en/snapcenter/install/task_install_the_snapcenter_server_using_the_install_wizard.html).

- Make sure that the repository path is identical on both nodes.
- Ensure the port numbers used for primary SnapCenter EC2 instance installation are also utilized for secondary SnapCenter EC2 instance installation
- Validate network connectivity between the SnapCenter EC2 instances

- Ensure that fully qualified domain names can be resolved to IPv4 addresses through DNS or local host configuration (c:\windows\system32\drivers\etc\hosts).
- Virtual IP address configured on both the EC2 instance's network interfaces (assuming an IP of 2.2.2.2)

1. Get the primary network adapter name of the EC2 instance by running the below command using command prompt or powershell

```
# net interface show interface
```

2. Enable DHCP static IP coexistence

```
# net interface ip set interface interface="Ethernet" dhcpstaticipcoexistence=enable
```

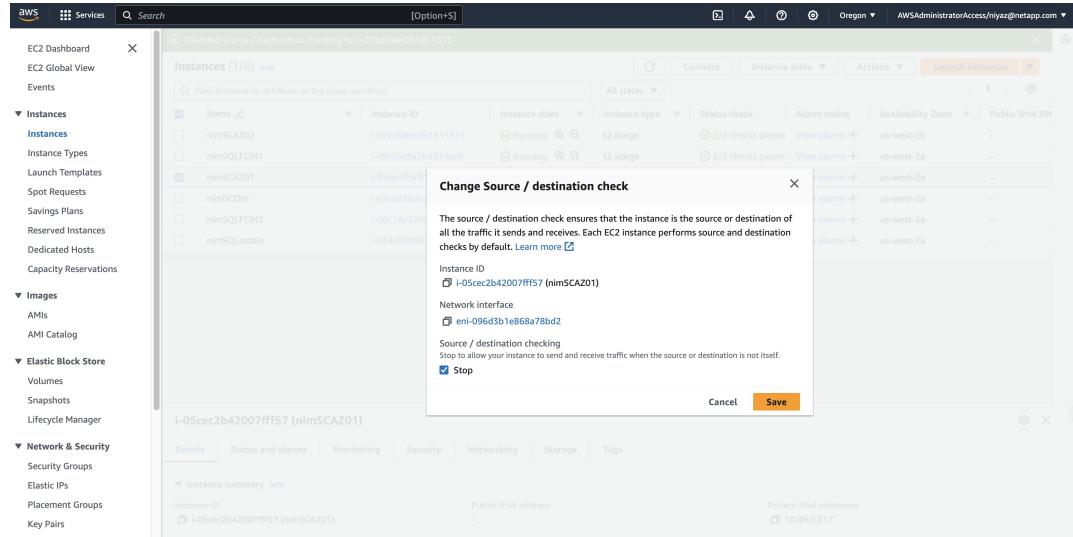
3. Add virtual IP with subnet mask (same as your primary subnet) to the primary network interface using netsh command

```
# netsh interface ip add address "Ethernet" 2.2.2.2 255.255.255.0
```

4. Update the appropriate route table to point to primary instance for the configured Virtual IP

- Disable source/destination check on SnapCenter EC2 instances using AWS Console or the CLI.

1. Login to AWS EC2 dashboard console
2. Select the SnapCenter HA server instances, click on Actions -> Networking -> Change source/destination check -> select stop -> save



Select Stop and click on Save (or)

3. Use AWS CLI command

```
# aws ec2 modify-instance-attribute --instance-id <instance-id> --source-dest-check "{\"Value\": false}"
```

- EC2 instances attached with instance IAM role with "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore" or similar permissions

## 1. Create EC2 instance IAM role

**Select trusted entity**

**Trusted entity type**

- AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account Allow entities in other AWS accounts belonging to you or a third party to perform actions in this account.
- SAML 2.0 Federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy Create a custom trust policy to enable others to perform actions in this account.
- Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

**Use case**

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

**Service or use case**

EC2

Choose a use case for the specified service.

Use case

- EC2 Allows EC2 instances to call AWS services on your behalf.
- EC2 Role for AWS Systems Manager Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- EC2 Spot Fleet Rule Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- EC2 - Spot Fleet Auto Scaling Allows EC2 Spot Fleet Auto Scaling to update EC2 spot fleets on your behalf.
- EC2 - Spot Fleet Tagging Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- EC2 - Spot Instances Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- EC2 - Spot Fleet Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- EC2 - Scheduled Instances Allows EC2 Scheduled Instances to manage instances on your behalf.

**Next**

Click on Next

**Add permissions**

**Permissions policies (1) Info**

The type of role that you selected requires the following policy.

Policy name	Type
AmazonSSMManagedInstanceCore	AWS managed

**Set permissions boundary - optional**

**Next**

Click on Next

**Name, review, and create**

**Role details**

**Role name** Enter a meaningful name to identify this role.  
snapcenter-instance-role

**Description** Add a short explanation for this role.  
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

**Step 1: Select trusted entities**

```
1: {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": "*",
      "Service": "ec2.amazonaws.com",
      "Action": "sts:AssumeRole"
    }
  ]
}
```

**Step 2: Add permissions**

**Permissions policy summary**

Policy name	Type	Attached as	Permissions policy
AmazonSSMManagedInstanceCore	AWS managed		

**Step 3: Add tags**

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with this resource.

Add new tag Info

You can add up to 50 more tags.

**Create role**

Create Role

## 2. Attach the EC2 instance role to both the SnapCenter servers

**Instances (1/6) Info**

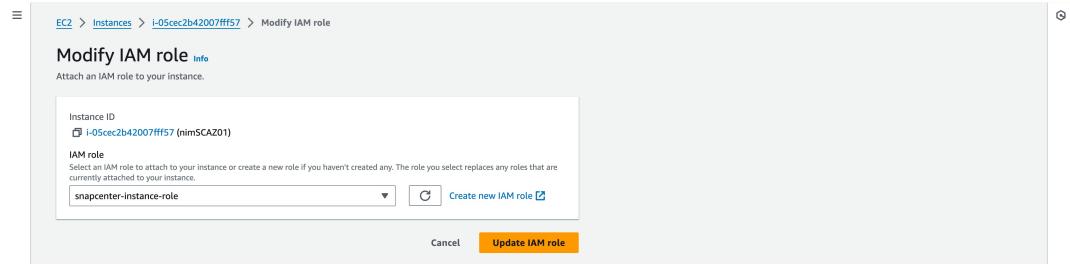
**Actions**

Connect View details Manage instance state Instance settings Networking Security Image and templates Monitor and troubleshoot

**Instances**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
nimSQLFCIN1	i-09fd5e8a2bdd7dae8	<span>Running</span>	t2.xlarge	<span>2/2 checks passed</span>	<span>View alarms +</span>	us-west-2a
<b>nimSCA201</b>	i-05cc2ba42007fff57	<span>Running</span>	t2.xlarge	<span>2/2 checks passed</span>	<span>Vi</span>	<span>Change security groups</span>
nimSCA202	i-07b2dec091411373	<span>Running</span>	t2.xlarge	<span>2/2 checks passed</span>	<span>Vi</span>	<span>Get Windows password</span>
nimDCore	i-03cd1b2bac7578bb	<span>Running</span>	t2.medium	<span>2/2 checks passed</span>	<span>Vi</span>	<span>Modify IAM role</span>
nimSQLFCIN2	i-00c1de72141a1be60d	<span>Running</span>	t2.xlarge	<span>2/2 checks passed</span>	<span>View alarms +</span>	us-west-2a
nimSQLstdalm	i-034d2089b0cca367d	<span>Running</span>	t2.xlarge	<span>2/2 checks passed</span>	<span>View alarms +</span>	us-west-2a

Click on Modify IAM role



Update IAM role

## Configuring MySQL HA

MySQL replication is a feature of MySQL Server that enables you to replicate data from one MySQL database server (master) to another MySQL database server (slave). SnapCenter supports MySQL replication for high availability only on two nodes.

Configure MySQL HA by running the following PowerShell cmdlets on designated primary SnapCenter EC2 instance:

```
Add-SmServerCluster -ClusterName <Cluster_Name> -ClusterIP <Cluster_IP> -PrimarySCServerIP <Node_1_IP_Address> -Verbose -Credential <Domain\User>
```

```
PS C:\Users\Administrator.NIMORG> Open-SmConnection
PS C:\Users\Administrator.NIMORG> Add-SmServerCluster -ClusterName nimscha -ClusterIP 2.2.2.2 -PrimarySCServerIP 10.49.0.217 -Verbose -Credential nimorg\administrator
VERBOSE: Start Add-SmServerCluster

Name      : Configure High Availability for SnapCenter Server
Id       : 4
StartTime : 
EndTime   : 
IsCancellable : False
IsRestatable : False
IsCompleted : False
IsVisible  : True
IsScheduled : False
PercentageCompleted : 0
Description : 
Status    : Running
Owner     : 
Error     : 
Priority  : None
Tasks     : {}
ParentJobID : 0
EventID   : 0
JobTypeID : 38
ApisJobKey : 
ObjectID  : 0
PluginCode : NONE
PluginName : NONE
HostId    : 0
RoleId    : 
JobIds   : {}
ScsJobId : 

Monitor the progress of job 4 in the Job Monitor page or by running the cmdlet: 'Get-SmJobSummaryReport -JobId 4'
VERBOSE: Add-SmServerCluster ended successfully.

PS C:\Users\Administrator.NIMORG>
```

```
Add-SmServer -ServerIP <Node_2_IP_Address> -Verbose -Credential <Domain\User>
```

```
PS C:\Users\Administrator.NIMORG> Add-SmServer -ServerName nimSCAZ02.nimorg.com -ServerIP 10.49.1.97 -Verbose -Credential nimorg\administrator
VERBOSE: Start Add-SmServer

Add-SmServer
Server 10.49.1.97 will be added as secondary node in the HA cluster and all the SnapCenter data on the server 10.49.1.97 will be discarded, if any. Do you want to continue?
[Y] Yes [A] Yes to All [N] No to All [S] Suspend [?] Help (default is "Y"); Y
WARNING: Make sure that the secondary SC server being added is identical to the primary SC server in terms of the SnapCenter version, installed port, SnapCenter Administrator, machine configuration and the domain.

Name      : Adding SC Server 10.49.1.97 to High Availability cluster
Id       : 15
StartTime : 
EndTime   : 
IsCancellable : False
IsRestatable : False
IsCompleted : False
IsVisible  : True
IsScheduled : False
PercentageCompleted : 0
Description : 
Status    : Running
Owner     : 
Error     : 
Priority  : None
Tasks     : {}
ParentJobID : 0
EventID   : 0
JobTypeID : 38
ApisJobKey : 
ObjectID  : 0
PluginCode : NONE
PluginName : NONE
HostId    : 0
RoleId    : 
JobIds   : {}
ScsJobId : 

Monitor the progress of job 15 in the Job Monitor page or by running the cmdlet: 'Get-SmJobSummaryReport -JobId 15'
VERBOSE: Add-SmServer ended successfully.

PS C:\Users\Administrator.NIMORG>
```

Run the below cmdlet to verify the state of HA configuration:

NetApp SnapCenter®

Jobs Schedules Events Logs

search by name

**Details** **Report** **Download Logs** **Cancel Job**

ID	Status	Name	Start date	End date	Owner
21		Package Installation on host 'nimsqstdaln.nimOrg.com'	07/11/2024 1:15:38 PM	07/11/2024 1:15:38 PM	NIMORGAdministrator
19		Add Host 'nimsqstdaln.nimOrg.com'	07/11/2024 1:15:26 PM	07/11/2024 1:15:26 PM	NIMORGAdministrator
17		Validate Host 'nimsqstdaln.nimOrg.com'	07/11/2024 1:15:19 PM	07/11/2024 1:15:26 PM	NIMORGAdministrator
15		Adding SC Server 10.49.1.97 to High Availability cluster	07/11/2024 1:10:06 PM	07/11/2024 1:11:49 PM	NIMORGAdministrator
11		Remove Host 'nimsqstdaln.nimOrg.com'	07/11/2024 1:25:29 PM	07/11/2024 1:01:37 PM	NIMORGAdministrator
9		Discover resources for host 'nimsqstdaln.nimOrg.com'	07/11/2024 12:55:01 PM	07/11/2024 12:55:31 PM	NIMORGAdministrator
7		Refresh for Host : nimsqstdaln.nimOrg.com	07/11/2024 12:54:42 PM	07/11/2024 12:55:02 PM	NIMORGAdministrator
5		Refresh for Host : nimsqstdaln.nimOrg.com	07/11/2024 12:53:10 PM	07/11/2024 12:53:49 PM	NIMORGAdministrator
4		Configure High Availability for SnapCenter Server	07/11/2024 12:49:20 PM	07/11/2024 12:49:40 PM	NIMORGAdministrator
3		Package Installation on host 'nimsqstdaln.nimOrg.com'	07/11/2024 12:43:46 PM	07/11/2024 12:55:03 PM	NIMORGAdministrator
2		Add Host 'nimsqstdaln.nimOrg.com'	07/11/2024 12:43:34 PM	07/11/2024 12:43:46 PM	NIMORGAdministrator
1		Validate Host 'nimsqstdaln.nimOrg.com'	07/11/2024 12:43:26 PM	07/11/2024 12:43:34 PM	NIMORGAdministrator

Total 12

### Job Details

Adding SC Server 10.49.1.97 to High Availability cluster

- ▾ Adding SC Server 10.49.1.97 to High Availability cluster
  - ▶ Configuring MySQL High Availability on Secondary SC Server
  - ▶ Configure SnapCenter for HA
  - ▶ Replicate MySQL Database
  - ▶ Backup MySQL server on host '10.49.0.217'
  - ▶ Prepare the host for MySQL replication
  - ▶ Restore MySQL server backup on host '10.49.1.97'
  - ▶ Configure MySQL replication
  - ▶ Configure Connection Strings
  - ▶ Synchronize Schedules on Secondary Server
  - ▶ Update SnapCenter Server URL

**Task Name:** Adding SC Server 10.49.1.97 to High Availability cluster **Start Time:** 07/11/2024 1:10:06 PM **End Time:** 07/11/2024 1:11:49 PM

**View Logs** **Cancel Job** **Close**

Get-SmServerConfig

```
PS C:\Users\Administrator.NIMORG> Get-SmServerConfig
```

```
SnapCenter Server High Availability Configuration

SnapCenterServerVersion : 5.0.0.3231
HighAvailabilityCluster : nimscA201 (2.2.2.2)
Servers : nimsCA201.nimOrg.com (10.49.0.217), nimsCA202.nimOrg.com (10.49.1.97)
ActiveRepository : nimsCA201.nimOrg.com (10.49.0.217)
ReplicationStatus : Healthy
ReplicationIssues :
LastSwitchoverTime : 7/11/2024 1:11:31 PM
```

```
PS C:\Users\Administrator.NIMORG>
```

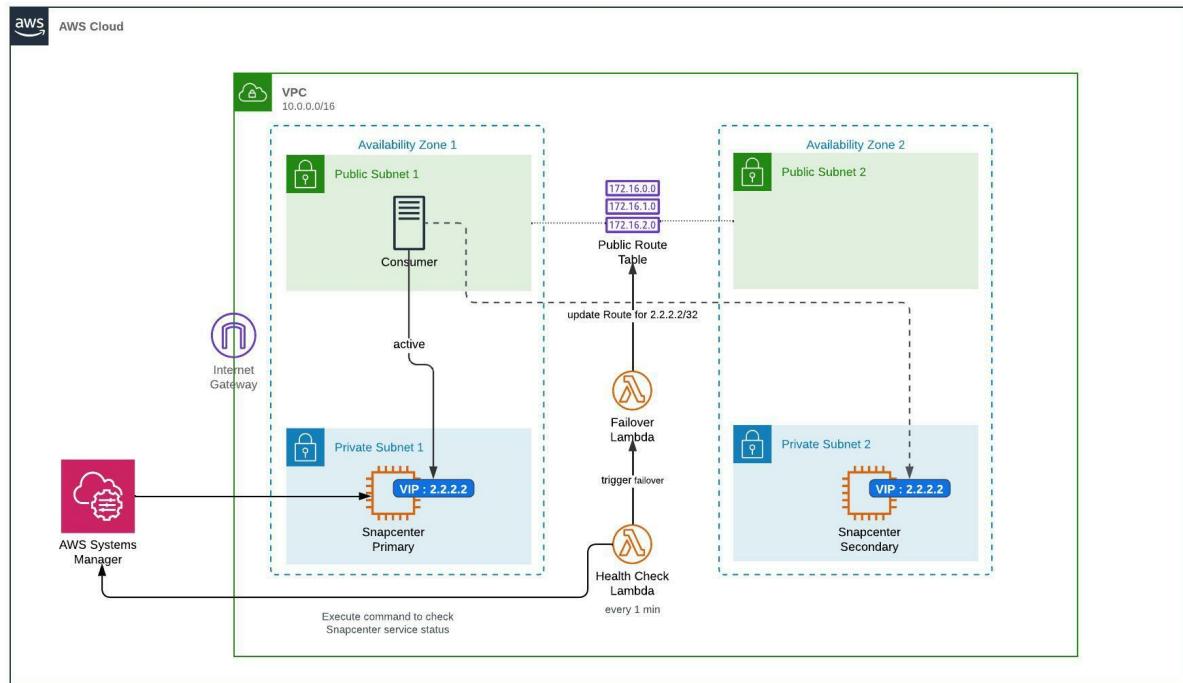
For information on how to run the cmdlets, see SnapCenter Software PowerShell Command Reference Guide.

**More Information:** SnapCenter performs read or write operations on the master repository and routes its connection to the slave repository when there is a failure on the master repository. The slave repository then becomes the master repository. SnapCenter also supports reverse replication, which is enabled only during failover.

SnapCenter provides the Get-SmRepositoryConfig and Set-SmRepositoryConfig PowerShell cmdlets to manage MySQL replication.

## Solution Architecture

Note : This solution is created based on the approach mentioned in this AWS blog -  
<https://aws.amazon.com/de/blogs/apn/making-application-failover-seamless-by-failing-over-your-private-virtual-ip-across-availability-zones/>



## Components

### 1. Health check lambda :

- Monitors the status of SnapCenter SMcore and MySQL service on the primary EC2 instance every 2 minutes by using AWS Systems Manager RunCommand service
- Triggers Failover lambda function in the event of primary EC2 instance failure
- Relyes on a SSM parameter "/snapcenter/ha/primary\_instance\_id"

## 2. Failover lambda :

- Updates the consumers Route table with the Virtual IP to point to the secondary SnapCenter EC2 instance
- After successful failover, it updates the "/snapcenter/ha/primary\_instance\_id" SSM parameter to reflect the current primary server

## 3. IAM Roles, permissions

### ● Health check lambda role

The screenshot shows the AWS IAM Role details page for the role `snapcenter-healthcheck-lambda-role`. The left sidebar shows the navigation menu for Identity and Access Management (IAM). The main content area displays the role's summary, including its creation date (July 11, 2024), last activity (17 minutes ago), ARN (arn:aws:iam::982589175402:role/snapcenter-healthcheck-lambda-role), and maximum session duration (1 hour). Below the summary, the `Permissions` tab is selected, showing attached policies: `AmazonSSMFullAccess` (AWS managed, 2 entities), `AWSLambdaBasicExecutionRole` (AWS managed, 6 entities), and `CustomPolicyWithFullAccess` (Customer inline, 0 entities). The JSON code for the `CustomPolicyWithFullAccess` policy is displayed:

```
1- {
2-     "Version": "2012-10-17",
3-     "Statement": [
4-         {
5-             "Action": [
6-                 "ec2:ReplaceRoute",
7-                 "ec2:CreateRoute",
8-                 "ec2:CreateNetworkInterface"
9-             ],
10-            "Effect": "Allow",
11-            "Resource": "*"
12-        }
13-    ]
14-}
```

CustomPolicy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:ReplaceRoute",
        "ec2>CreateRoute",
        "ec2>CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "EC2"
    },
    {
      "Action": [
        "ssm:GetParameter",
        "ssm:PutParameter",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "SSM"
    },
    {
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Resource": "arn:aws:lambda:us-west-2:982589175402:function:snap_center-failover-lambda",
      "Effect": "Allow",
      "Sid": "LambdaInvoke"
    }
  ]
}
```

- Failover lambda role

**Summary**

Creation date: July 11, 2024, 19:22 (UTC+05:30)  
Last activity: 47 minutes ago

ARN: arn:aws:iam::982589175402:role/snapcenter-failover-lambda-role  
Maximum session duration: 1 hour

**Permissions**

Policy name	Type	Attached entities
AmazonSSMReadOnlyAccess	AWS managed	2
AWSLambdaBasicExecutionRole	AWS managed	6
CustomPolicy	Customer inline	0

**CustomPolicy**

```

1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Action": [
5             "ec2:ReplaceRoute",
6             "ec2:CreateRoute",
7             "ec2:CreateNetworkInterface",
8             "ec2:DescribeNetworkInterfaces",
9             "ec2:DeleteNetworkInterface"
10        ],
11        "Resource": "*",
12        "Effect": "Allow",
13        "Sid": "EC2"
14    },
15    {
16        "Action": [
17            "ssm:GetParameter",
18            "ssm:PutParameter"
19        ],
20        "Resource": "*",
21        "Effect": "Allow",
22        "Sid": "SSM"
23    }
24]

```

## CustomPolicy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:ReplaceRoute",
        "ec2:CreateRoute",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "EC2"
    },
    {
      "Action": [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "SSM"
    }
  ]
}
```

# Deployment Guide

## Step 1 : Clone the GitHub repository

Clone the GitHub repository in your local system

```
# git clone https://github.com/NetApp/snapcenter-failover-automation.git
```

## Step 2 : Setup an AWS S3 Bucket

1. Navigate to AWS Console > S3 and click on Create bucket. Create the bucket with the default settings.
2. Once inside the bucket, click on Upload > Add files and upload the 2 zip files under the "deploy" directory from the cloned repository

The screenshot shows the AWS S3 console with the path 'Amazon S3 > Buckets > tme-sc-test-bucket > lambda/'. The 'Objects' tab is selected, displaying two items:

Name	Type	Last modified	Size	Storage class
failover.zip	zip	June 26, 2024, 11:04:14 (UTC+05:30)	1.5 KB	Standard
healthcheck.zip	zip	June 26, 2024, 16:42:22 (UTC+05:30)	1.6 KB	Standard

## Step 3 : AWS CloudFormation Deployment

1. Navigate to AWS Console > CloudFormation > Create stack > With New Resources (Standard). Select "snapcenter-ha-cf.yaml" file from the "deploy" directory from the cloned repository

The screenshot shows the AWS CloudFormation 'Create stack' wizard at Step 1: Prerequisite – Prepare template. The left sidebar shows steps: Step 1 (Create stack), Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review and create). The main area has three options for preparing a template:

- Choose an existing template: Upload or Choose an existing template.
- Use a sample template: Choose from our sample template library.
- Build from Application Composer: Create a template using a visual builder.

Below this, the 'Specify template' section shows:

**Template source**: Selecting a template generates an Amazon S3 URL where it will be stored.  
Options:

- Amazon S3 URL: Provide an Amazon S3 URL to your template.
- Upload a template file: Upload your template directly to the console.
- Sync from Git - new: Sync a template from your Git repository.

File uploaded: snapcenter-ha.yaml  
S3 URL: https://s3.us-west-2.amazonaws.com/cf-templates-90gla94i22sf-us-west-2/2024-07-08t120349.79426zr-snapcenter-ha.yaml

Buttons: Cancel, Next

Click on Next

- Enter the stack details. Click on Next and check the checkbox for "I acknowledge that AWS CloudFormation might create IAM resources" and click on Submit.

CloudFormation > Stacks > Create stack

Step 1  
Create stack

Step 2  
Specify stack details

Step 3  
Configure stack options

Step 4  
Review and create

### Specify stack details

#### Provide a stack name

Stack name

SnapCenterFailoverStack

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 23/128.

#### Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

CreateVPCEndpoints

Specify whether to create VPC endpoints for EC2, SSM, SSMMessages, EC2Messages, Lambda [Yes or No]? Select No if these VPC endpoints already exists for the VPC.

Yes

LambdaSSBucketName

Lambda SS bucket name

tmevc-test-bucket

PrivateSubnetId01

Private subnet ID 01

subnet-XXXXXX

PrivateSubnetId02

Private subnet ID 02

subnet-XXXXXX

RouteTableId

Route table ID

rtb-XXXXXX

SecurityGroupId

Security group ID

sg-XXXXXX

PrivateSubnetId03

subnet-XXXXXX

RouteTableId

Route table ID

rtb-XXXXXX

SecurityGroupId

Security group ID

sg-XXXXXX

SnapcenterDestinationCidrBlock

Snapcenter destination CIDR block

2.2.2.2/32

SnapcenterFailoverLambdaZipS3Key

Snapcenter failover lambda zip 53 key

lambda/failover.zip

SnapcenterHealthCheckLambdaZipS3Key

Snapcenter healthcheck lambda zip 53 key

lambda/heathcheck.zip

SnapcenterInstanceId01

Snapcenter instance ID 01

i-XXXXXX

SnapcenterInstanceId02

Snapcenter instance ID 02

i-XXXXXX

SnapcenterPrimaryInstanceId

Snapcenter primary instance ID

i-XXXXXX

VPCId

VPC ID

vpc-XXXXXX

Cancel Previous Next

Click on Next

- Once the CloudFormation stack deployment is completed, the health check of SnapCenter will begin and will failover in case of primary outage.

## Validated Environment

This solution was validated using Windows Server 2019 and NetApp SnapCenter version 5.0. The simulation of job within SnapCenter was performed using SQL Server as the application.

## Author Information

- [Pradeep Kumar](mailto:pradeep.kumar@netapp.com) - NetApp Solutions Engineering Team
- [Niyaz Mohamed](mailto:niyaz.mohamed@netapp.com) - NetApp Solutions Engineering Team