

# IBM Spectrum Protect Plus on the AWS Cloud

## Deployment Guide

*June 2019*

### Contents

Overview .....	2
Cost and licenses .....	3
Architecture .....	4
Planning the deployment .....	8
IBM Spectrum Protect Plus sizing tool.....	9
AWS account .....	9
Technical requirements .....	10
Deployment options.....	11
Deployment steps.....	11
Step 1. Sign in to your AWS account.....	11
Step 2. Subscribe to the IBM Spectrum Protect Plus AMI.....	11
Step 3. Launch the AWS CloudFormation template .....	12
Option 1: Parameters for deploying IBM Spectrum Protect Plus in a new VPC .....	13
Option 2: Parameters for deploying IBM Spectrum Protect Plus in an existing VPC.....	14
Step 4. Test the deployment .....	17
Option 1: Testing deployment of IBM Spectrum Protect Plus in a new VPC .....	17
Option 2: Testing deployment of IBM Spectrum Protect Plus in an existing VPC .....	19
Step 5. Enable SSH connection to vSnap server (optional) .....	20
Best practices for using IBM Spectrum Protect Plus on AWS.....	22

Security .....	22
AWS Identity and Access Management (IAM).....	22
OS Security.....	23
Security Groups.....	23
Troubleshooting .....	24
Send us feedback .....	29
Additional resources .....	29
Document revisions.....	30

## Overview

This deployment guide provides step-by-step instructions for deploying IBM Spectrum Protect Plus on the Amazon Web Services (AWS) Cloud.

The IBM Spectrum Protect Plus on AWS deployment includes IBM Spectrum Protect Plus Version 10.1.3. To use a later version of IBM Spectrum Protect Plus, you must upgrade to that version. For upgrade instructions, go to the [IBM Spectrum Protect Plus documentation](#), click the version of IBM Spectrum Protect Plus that you are using, and then search for Updating IBM Spectrum Protect Plus components.

The deployment is an automated process that is intended for users who run IBM Spectrum Protect Plus on premises, but want to protect any of the following databases that are running on AWS:

- IBM Db2
- Microsoft SQL Server
- Microsoft Exchange Server
- Oracle
- MongoDB

IBM Spectrum Protect Plus simplifies the backup and recovery of your database data on AWS.

With IBM Spectrum Protect Plus, you can create custom policies that define the parameters that are applied to backup jobs. These parameters include the frequency, retention period, and target site for backup operations. Optional parameters are available to enable data replication between disk storage pools in your IBM Spectrum Protect Plus environment. You can also offload data to cloud storage such as Amazon S3 for cost-efficient, long-term data retention.

To facilitate rapid data recovery, IBM Spectrum Protect Plus offers a global catalog that enables you to see what resources are protected, and more importantly, what resources are not protected. When data recovery is required, the catalog and search interface enable you to quickly identify the data that you want to recover, eliminating the need to sort through hundreds of objects and recovery points.

You can use the REST APIs to automate data protection operations and to integrate third-party tools and solutions, such as Puppet and ServiceNow.

When you deploy IBM Spectrum Protect Plus to AWS, you can take advantage of a hybrid on-premises and off-premises architecture to protect your database data, while managing your workloads from a single dashboard. On the dashboard, you can quickly view the health of your on-premises and AWS environment and identify failed jobs, capacity and device issues, and other areas of concern.

In addition to backup and recovery operations, you can also use IBM Spectrum Protect Plus to replicate backup data between your on-premises location and AWS for additional data protection.

You can also reuse data between your on-premises location and AWS. For example, you might want to use data that is protected on your on-premises site on AWS for DevOps, quality assurance, or testing purposes.

## Cost and licenses

You are responsible for the cost of the AWS services used while deploying IBM Spectrum Protect Plus.

The deployment is automated by an AWS CloudFormation template. AWS CloudFormation provides a way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.

The AWS CloudFormation template includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment.

For cost estimates, see the pricing pages for each AWS service that you will use. Prices are subject to change.

**Tip** After you deploy the AWS CloudFormation template, it is useful to enable the [AWS Cost and Usage Report](#) to track costs that are associated with the deployment. This report delivers billing metrics to an S3 bucket in your account. It provides cost estimates based on usage throughout each month and finalizes the data at the end of the month. For more information about the report, see the [AWS documentation](#).

The IBM Spectrum Protect Plus server, which is on premises, must be licensed for the physical data that is protected on the AWS environment. Contact IBM for licensing information.

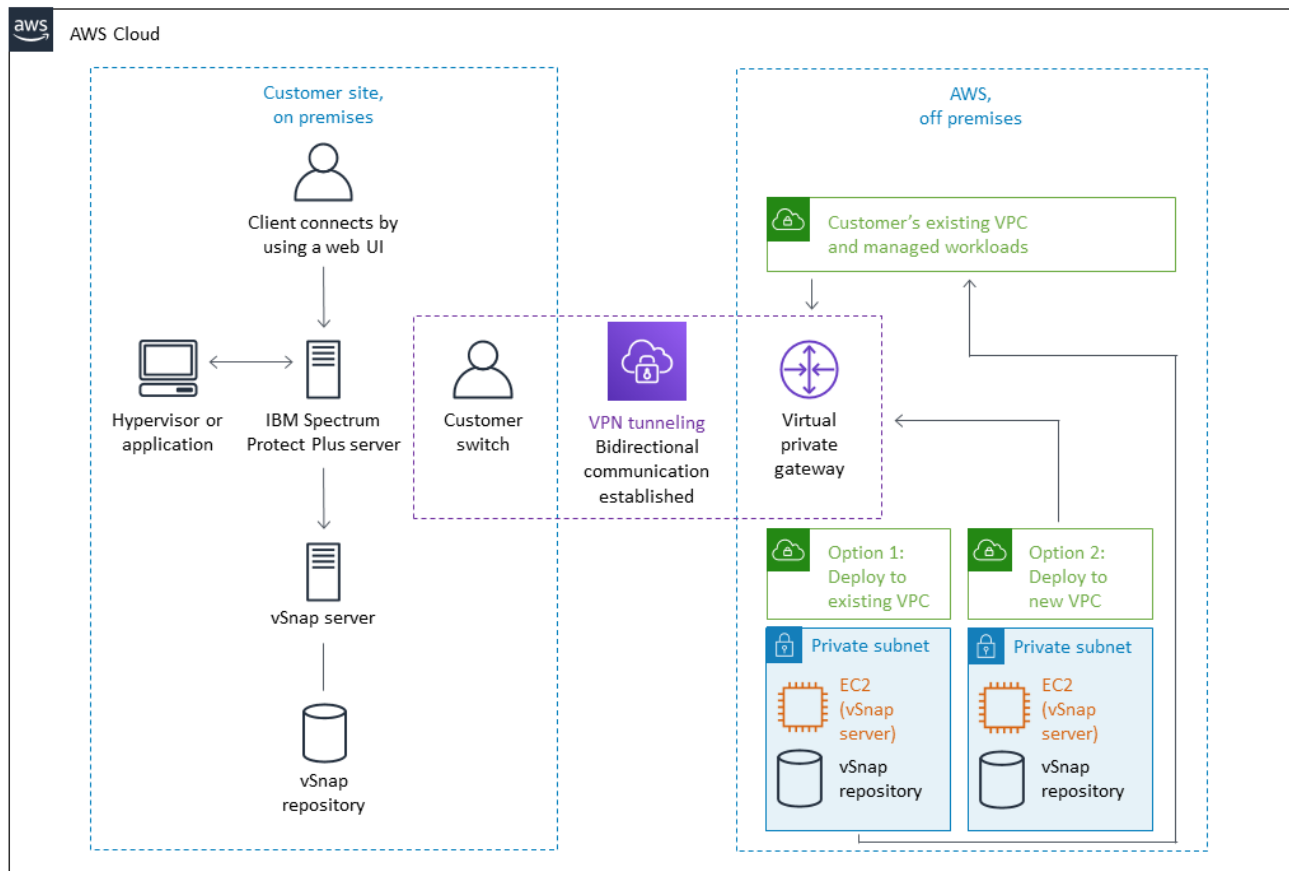
The deployment also requires a subscription to the Amazon Machine Image (AMI) for IBM Spectrum Protect Plus. The AMI is available from [AWS Marketplace](#), and additional pricing, terms, and conditions might apply. For instructions, see [step 2](#) in the deployment section.

## Architecture

IBM Spectrum Protect Plus on AWS is a hybrid solution in which the vSnap server is hosted on AWS and the IBM Spectrum Protect Plus server is on premises. The management, access control, and licensing features of IBM Spectrum Protect Plus are managed and maintained by the IBM Spectrum Protect Plus server.

You must use a virtual private network (VPN) tunnel to establish bidirectional communication between the vSnap server and the IBM Spectrum Protect Plus server before you set up and configure the AWS CloudFormation template.

**Important** If you do not establish this communication, the installation and configuration of the vSnap server on AWS will fail.



**Figure 1: Communication between AWS and the IBM Spectrum Protect Plus server**

To test the communication, follow the instructions in [Step 4. Test the Deployment](#).

The AWS CloudFormation template configures and builds a stack of a single vSnap server and repository on AWS according to the size that you choose for vSnap workloads (up to 100 TiB).

If you delete this stack, the entire IBM Spectrum Protect Plus deployment is deleted.

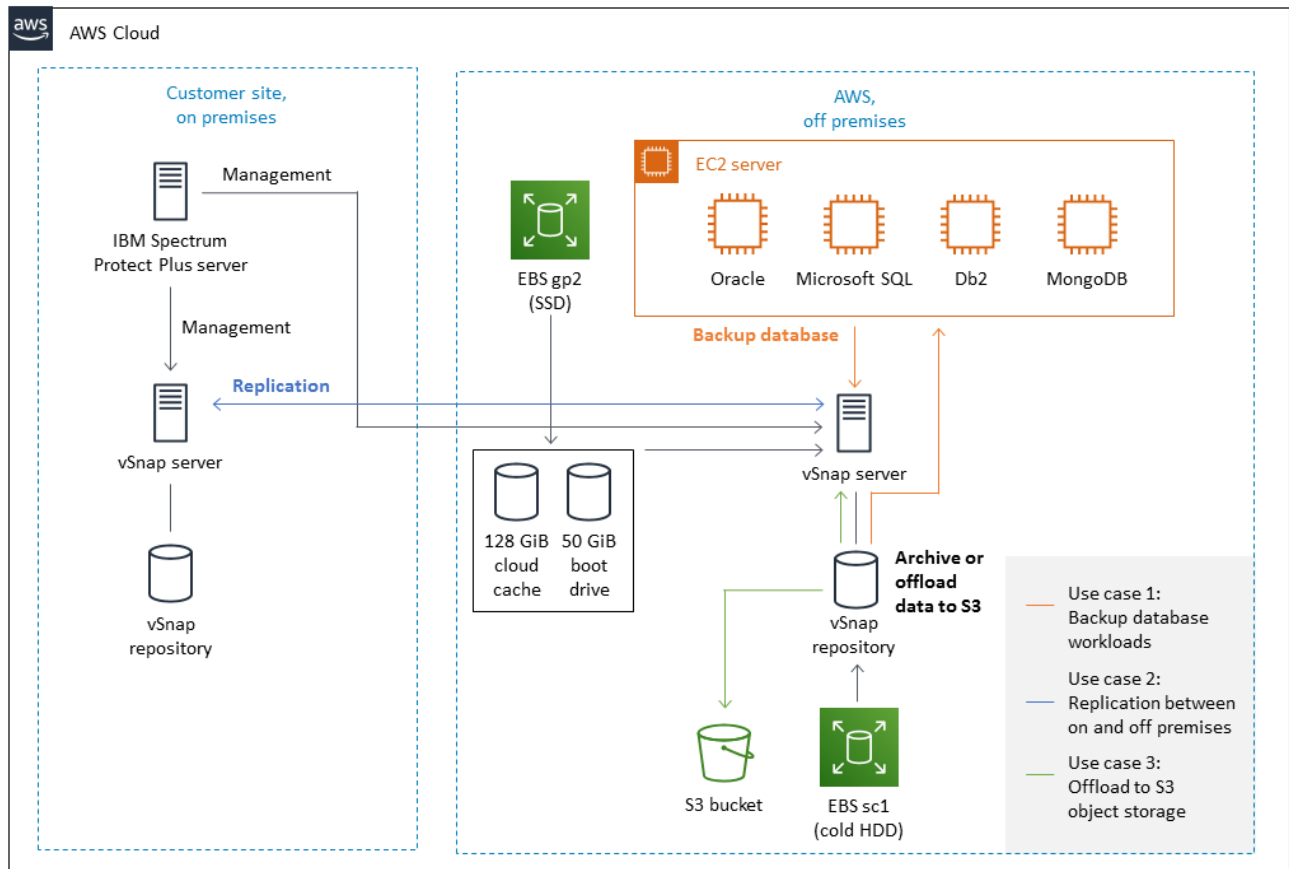
If you are deploying IBM Spectrum Protect Plus in an existing Virtual Private Cloud (VPC), when your vSnap server and repository are configured, the template registers the new vSnap server with your on-premises IBM Spectrum Protect Plus server. This process completes the installation of the vSnap server on AWS and enables your on-premises IBM Spectrum Protect Plus server to recognize the vSnap server.

If you are deploying IBM Spectrum Protect Plus in a new VPC, you must take the following actions to complete the installation of the vSnap server:

- Configure a bidirectional VPN communication between the new vSnap server and your on-premises IBM Spectrum Protect Plus server.

- Register the new vSnap server with your on-premises IBM Spectrum Protect Plus server to complete the vSnap server installation. For the steps required to register the vSnap server, see [Option 1: Testing deployment of IBM Spectrum Protect Plus in a new VPC](#).

Deploying the template builds the following IBM Spectrum Protect Plus on AWS environment:



**Figure 2: Architecture for IBM Spectrum Protect Plus on AWS**

The deployment sets up and configures the following components:

- A vSnap server that is mounted and provisioned for your repository size.
- The appropriate security groups to restrict access to only necessary protocols and ports.
- A user name and password for vSnap server authentication.

- A Network Address Translation (NAT) gateway for outbound internet access from private subnets. \*
- An Elastic IP (EIP) for NAT usage. \*
- An Identity and Access Management (IAM) role with fine-grained permissions for access to AWS services that are necessary for the deployment process.
- A Cloud Watch service to monitor AWS resources and logs.
- A VPC that spans 1 Availability Zone and includes one public and one private subnet. \*
- An internet gateway to allow access to the internet. \*
- An EC2 server instance that is configured with the vSnap components server by using the instance type that is recommended by the [IBM Spectrum Protect Plus blueprint](#).

Each vSnap server EC2 instance will have:

- A 50 GiB Amazon Elastic Block Store (EBS) SSD volume for the root device.
- A 128 GiB EBS SSD volume for a cloud cache to support offload and restore operations.
- A dynamic number of EBS sc1 volumes to support the given repository size during deployment.
- Logs and cache disks as defined by the blueprint that correspond to the vSnap server repository size.

\* If you are deploying IBM Spectrum Protect Plus to an existing VPC, these components must be pre-existing and are required for successful deployment. The CloudFormation template will not deploy these components.

## Planning the deployment

This guide assumes that you are familiar with IBM Spectrum Protect Plus and that you have a moderate level of familiarity with AWS services and components listed below.

If you're new to AWS, visit the [Getting Started Resource Center](#) and the [AWS Training and Certification website](#) for materials and programs that can help you develop the skills to design, deploy, and operate your infrastructure and applications on the AWS Cloud.

- **Amazon EC2** – The Amazon EC2 service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or import your own virtual machine images.
- **Amazon VPC** – The Amazon VPC service lets you provision a private, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, subnet creation, and configuration of route tables and network gateways
- **AWS CloudFormation** – AWS CloudFormation gives you an easy way to create and manage a collection of related AWS resources, and provision and update them in an orderly and predictable way. You use a template to describe all the AWS resources (for example, EC2 instances) that you want. You don't have to create and configure the resources or figure out dependencies; AWS CloudFormation handles all of that.
- **IAM** – AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. With IAM, you can manage users, security credentials such as access keys, and permissions that control which AWS resources users can access, from a central location.
- **CloudWatch** – Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications that you run on AWS. You can use CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.
- **Amazon S3** – Amazon Simple Storage Service (Amazon S3) is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web. You can accomplish these tasks using the simple and intuitive web interface of the AWS Management Console.



## IBM Spectrum Protect Plus sizing tool

Use the IBM Spectrum Protect Plus sizing worksheet that is available with the [IBM Spectrum Protect Plus blueprint](#) to architect your IBM Spectrum Protect Plus environment.

The worksheet provides the estimated size of vSnap server that is required to optimally use IBM Spectrum Protect Plus to protect your environment.

You will use sizing results when you set the parameters in the AWS CloudFormation template.

## AWS account

If you don't already have an AWS account, create one at <https://aws.amazon.com> by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

Your AWS account is automatically signed up for all AWS services. You are charged only for the services you use.

## Technical requirements

Before you launch the AWS CloudFormation template, your account must be configured as specified in the following table. Otherwise, deployment might fail.

### [Resources](#)

If necessary, request [service limit increases](#) for the following resources. You might need to do this if you already have an existing deployment that uses these resources, and you think you might exceed the default limits with this deployment. For default limits, see the [AWS documentation](#).

[AWS Trusted Advisor](#) offers a service limits check that displays your usage and limits for some aspects of some services.

Resource	This deployment uses
<b>Virtual Private Clouds (VPCs)</b>	1
<b>Elastic IP addresses</b>	1
<b>Security groups</b>	1
<b>IAM roles</b>	2
<b>Instances</b>	1
<b>HDD EBS Volumes (sc1)</b>	Up to 16
<b>SSD EBS Volumes (gp2)</b>	Up to 4
<b>NAT gateways</b>	1
<b>Subnets</b>	2
<b>Internet Gateways</b>	1

### [Key pair](#)

Make sure that at least one Amazon EC2 key pair exists in your AWS account in the region where you are planning to deploy the template. Make note of the key pair name. You'll be prompted for this information during deployment. To create a key pair, follow the [instructions in the AWS documentation](#).

If you're deploying the AWS CloudFormation template for testing or proof-of-concept purposes, we recommend that you create a new key pair instead of specifying a key pair that's already being used by a production instance.

### [IAM permissions](#)

To deploy the AWS CloudFormation template, you must log in to the AWS Management Console with IAM permissions for the resources and actions the templates will deploy. The *AdministratorAccess* managed policy within IAM provides sufficient permissions, although your organization may choose to use a custom policy with more restrictions.

## Deployment options

There are two options for deploying IBM Spectrum Protect Plus on AWS:

- **Deploy IBM Spectrum Protect Plus in a new VPC.** This option builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, and other infrastructure components, and then deploys IBM Spectrum Protect Plus in this new VPC.

This option *does not* register the vSnap server with the on-premises IBM Spectrum Protect Plus server automatically.

- **Deploy IBM Spectrum Protect Plus in an existing VPC.** This option provisions IBM Spectrum Protect Plus in your existing AWS infrastructure.

This option registers the vSnap server with the on-premises IBM Spectrum Protect Plus server automatically.

Separate AWS CloudFormation templates are used to implement the two options. With these templates, you can configure Classless Inter-Domain Routing (CIDR) blocks, instance types, and IBM Spectrum Protect Plus vSnap server settings, as discussed later in this guide.

## Deployment steps

### Step 1. Sign in to your AWS account

1. Sign in to your AWS account at <https://aws.amazon.com> with an IAM user role that has the necessary permissions. For details, see [AWS account](#) earlier in this guide.
2. Make sure that your AWS account is configured correctly, as discussed in the [Technical requirements](#) section.

### Step 2. Subscribe to the IBM Spectrum Protect Plus AMI

This deployment requires a subscription to the AMI for IBM Spectrum Protect Plus in AWS Marketplace.

1. Sign in to your AWS account.
2. Open the [IBM Spectrum Protect Plus](#) page in AWS Marketplace, and then click **Continue to Subscribe**.
3. Review the terms and conditions for software usage, and then click **Accept Terms**.

You will get a confirmation page, and an email confirmation will be sent to the account owner. For detailed subscription instructions, see the [AWS Marketplace documentation](#).

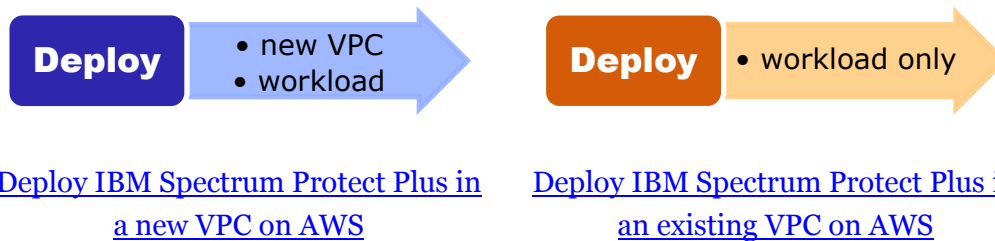
- When the subscription process is complete, exit out of AWS Marketplace without further action. **Do not** provision the software from AWS Marketplace—the AWS CloudFormation template will deploy the AMI for you.

### Step 3. Launch the AWS CloudFormation template

**Notes** The instructions in this section reflect the older version of the AWS CloudFormation console. If you're using the redesigned console, some of the user interface elements might be different.

You are responsible for the cost of the AWS services used while running this deployment. However, there is no additional cost for using the AWS CloudFormation template. For full details, see the pricing pages for each AWS service that you will be using. Prices are subject to change.

- Sign in to your AWS account, and choose one of the following options to launch the AWS CloudFormation template. For help choosing an option, see [Deployment options](#) earlier in this guide.



**Important** If you're deploying IBM Spectrum Protect Plus in an existing VPC, make sure that your VPC has a bidirectional communication established to your on-premises IBM Spectrum Protect Plus server prior to running the template. Otherwise, the template might fail during the attempt to automate the process and roll back the stack.

Each deployment takes approximately 15-40 minutes to complete, depending on the vSnap server size.

2. Check the region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the vSnap server and its relevant components for IBM Spectrum Protect Plus will be built.
3. On the Select Template page, keep the default setting for the template URL, and then click **Next**.
4. On the Specify Details page, set the stack name. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary.

In the following tables, parameters are listed by category and described separately for the two deployment options:

- [Parameters for deploying IBM Spectrum Protect Plus in a new VPC](#)
- [Parameters for deploying IBM Spectrum Protect Plus in an existing VPC](#)

When you finish reviewing and customizing the parameters, click **Next**.

### OPTION 1: PARAMETERS FOR DEPLOYING IBM SPECTRUM PROTECT PLUS IN A NEW VPC

*VPC network configuration:*

Parameter label (name)	Default	Description
<b>VPC CIDR</b> (VPCCIDR)	10.0.0.0/16	The range of IPv4 addresses for the VPC.
<b>Public subnet CIDR</b> (PublicSubnet1CIDR)	10.0.1.0/24	The CIDR block for a public subnet located in the Availability Zone.
<b>Private subnet CIDR</b> (PrivateSubnet1CIDR)	10.0.3.0/24	The CIDR block for a private subnet located in the Availability Zone.
<b>Availability Zone</b> (AvailabilityZone)	<i>Requires input</i>	The Availability Zone to use for the subnets in the VPC. Only one Availability Zone is used for this deployment.

*EC2 (vSnap server) configuration:*

Parameter label (name)	Default	Description
<b>Key pair name</b> (KeyPairName)	<i>Requires input</i>	A public and private key pair, which allows you to connect securely to your vSnap server instance after it launches. This is the key pair you created in your preferred region, as described in <a href="#">Technical requirements</a> .
<b>vSnap repository size</b> (vSnapRepositorySize)	10000	The repository size in GiB. Enter a size value in the range 500 - 100,000 GiB (100 TiB).

Parameter label (name)	Default	Description
<b>Instance type</b> (Instance Type)	t2.xlarge	The vSnap server EC2 instance type.
<b>vSnap server user</b> (vSnapUser)	admin	<p>The user name for the vSnap server application. This value cannot be blank or root.</p> <p>User names must start with a lowercase letter or an underscore, followed by lowercase letters, digits, underscores, or dashes, and can end with a dollar sign.</p> <p>The regular expression terms that are used to validate the user name are <code>[a-z_][a-z0-9_-]*[\$]?</code></p> <p>A user name can have a maximum of 32 characters.</p>
<b>vSnap server password</b> (vSnapPassword)	<i>Requires input</i>	The user password for the vSnap server application. The password must consist of ASCII characters and must be at least 8 characters long.
<b>Confirm vSnap server password</b> (ConfirmvSnapPassword)	<i>Requires input</i>	Confirm the password for the vSnap server application user.
<b>Time zone</b> (TimeZone)	US/Eastern	The time zone where the vSnap server instance is located.

## OPTION 2: PARAMETERS FOR DEPLOYING IBM SPECTRUM PROTECT PLUS IN AN EXISTING VPC

*VPC network configuration:*

Parameter label (name)	Default	Description
<b>Existing VPC ID</b> (VPCID)	<i>Requires input</i>	The ID that is used to deploy the vSnap server in an existing VPC.
<b>VPC private subnet ID</b> (VPCPrivateSubnet)	<i>Requires input</i>	The ID of an existing private subnet in the VPC.
<b>Availability Zone</b> (AvailabilityZone)	<i>Requires input</i>	The Availability Zone to use for the subnets in the VPC. Only one Availability Zone is used for this deployment.

*EC2 (vSnap server) configuration:*

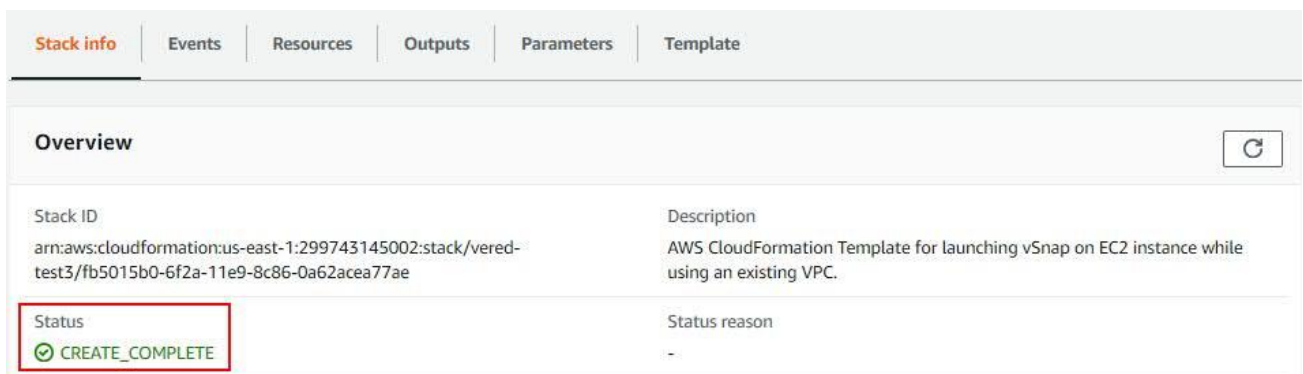
Parameter label (name)	Default	Description
<b>Key pair name</b> (KeyPairName)	<i>Requires input</i>	A public/private key pair, which allows you to connect securely to your vSnap server instance after it launches. This is the key

Parameter label (name)	Default	Description
		pair that you created in your preferred region, as described in <a href="#">Technical requirements</a> .
<b>vSnap repository size</b> (vSnapRepositorySize)	10000	The repository size in GiB. Enter a size value in the range 500 - 100,000 GiB (100 TiB).
<b>Instance type</b> (Instance Type)	t2.xlarge	The vSnap server EC2 instance type.
<b>vSnap server user</b> (vSnapUser)	admin	The user name for the vSnap server application. This value cannot be blank or root.  User names must start with a lowercase letter or an underscore, followed by lowercase letters, digits, underscores, or dashes, and can end with a dollar sign.  The regular expression terms that are used to validate the user name are [a-z_][a-z0-9_-]*[\$]?  A user name can have a maximum of 32 characters.
<b>vSnap server password</b> (vSnapPassword)	<i>Requires input</i>	The user password for the vSnap server application. The password must consist of ASCII characters and must be at least 8 characters long.
<b>Confirm vSnap server password</b> (ConfirmvSnapPassword)	<i>Requires input</i>	Confirm the password for the vSnap server application user.
<b>Time zone</b> (TimeZone)	US/Eastern	The time zone where the vSnap server instance is located.

### IBM Spectrum Protect Plus Parameters:

Parameter label (name)	Default	Description
<b>IBM Spectrum Protect Plus IP address</b> (SppIP)	<i>Requires input</i>	The private IP address for the IBM Spectrum Protect Plus server.
<b>IBM Spectrum Protect Plus user</b> (SppUser)	admin	The user name for the IBM Spectrum Protect Plus application.
<b>IBM Spectrum Protect Plus password</b> (SppPassword)	<i>Requires input</i>	The user password for the IBM Spectrum Protect Plus application.
<b>Confirm IBM Spectrum Protect Plus password</b> (ConfirmSppPassword)	<i>Requires input</i>	Confirm the password for the IBM Spectrum Protect Plus application user.

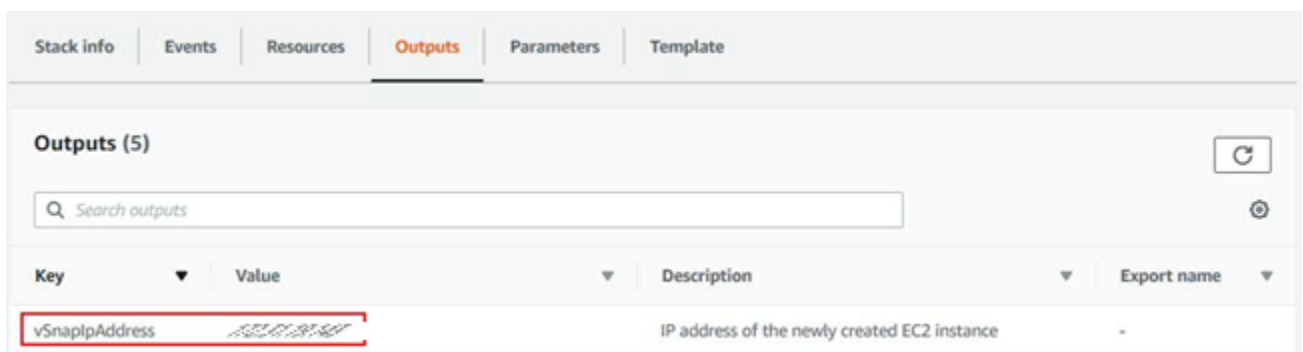
5. On the Options page, you can [specify tags](#) (key-value pairs) for resources in your stack and [set advanced options](#). When you're done, click **Next**.
6. On the Review page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create an IAM resource.
7. Click **Create** to deploy the stack.
8. Monitor the status of the stack on the **Stack info** tab. When the status is **CREATE\_COMPLETE**, the IBM Spectrum Protect Plus vSnap server is ready.



The screenshot shows the AWS CloudFormation console with the 'Stack info' tab selected. The 'Overview' section displays the following information:

Property	Value
Stack ID	arn:aws:cloudformation:us-east-1:299743145002:stack/vered-test3/fb5015b0-6f2a-11e9-8c86-0a62acea77ae
Description	AWS CloudFormation Template for launching vSnap on EC2 instance while using an existing VPC.
Status	CREATE_COMPLETE
Status reason	-

9. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.



The screenshot shows the AWS CloudFormation console with the 'Outputs' tab selected. The 'Outputs (5)' section displays the following information:

Key	Value	Description	Export name
vSnapIpAddress	10.0.1.10	IP address of the newly created EC2 instance	-



## Step 4. Test the deployment

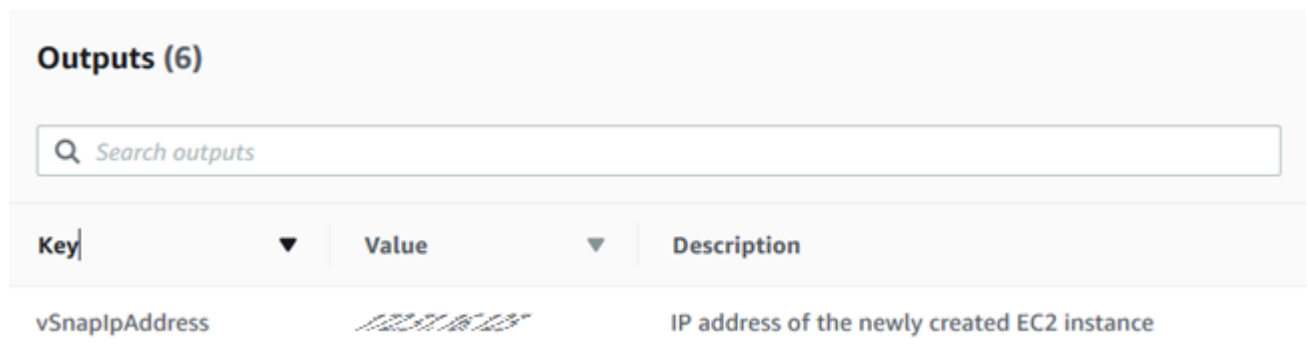
### OPTION 1: TESTING DEPLOYMENT OF IBM SPECTRUM PROTECT PLUS IN A NEW VPC

When you deploy IBM Spectrum Protect Plus in a new VPC, you must manually configure communication between the on-premises IBM Spectrum Protect Plus server and the vSnap server on AWS. You must also register the vSnap server with your on-premises IBM Spectrum Protect Plus server.

To confirm that communication is established and to register the vSnap server, complete the following steps:

1. Ensure that a bidirectional VPN connection is configured between the on-premises IBM Spectrum Protect Plus server and the vSnap server on AWS.
2. From the on-premises system that is running the IBM Spectrum Protect Plus server, ping the system that hosts the vSnap server instance and vice versa.

To find the IP address for the vSnap server instance, navigate to the Stacks page of the AWS CloudFormation console. Select the stack for the instance and then click the Outputs tab.



Outputs (6)		
<input type="text" value="Search outputs"/>		
Key	Value	Description
vSnapIpAddress	172.31.16.125	IP address of the newly created EC2 instance

3. In a supported web browser, start the IBM Spectrum Protect Plus user interface by entering the host name or IP address of the machine where IBM Spectrum Protect Plus is deployed.

For a list of browsers that are supported by each IBM Spectrum Protect Plus version, go to the [system requirements](#) overview page and click the version of IBM Spectrum Protect Plus that you are using. Then click System requirements > Browser support.

4. In the navigation pane, click **System Configuration > Backup Storage > Disk**.

5. Register and initialize the vSnap server with your on-premises IBM Spectrum Protect Plus server.



For instructions, go to the IBM Spectrum Protect Plus product documentation, click the version of IBM Spectrum Protect Plus that you are using, and then search for the following topics:

- Adding a vSnap server as a backup storage provider
- Completing a simple initialization

6. Confirm that the vSnap server is displayed in the list of disk storage as shown in the following example:



The screenshot shows a 'Disk Storage' interface with a table of storage providers. The table has the following columns: Hostname/IP, Site, Version, Status/Capacity, and Actions. There are three rows of data. The third row is highlighted with a black box. The 'Status/Capacity' column for the third row also has a '0%' label highlighted with a black box.

	Hostname/IP	Site	Version	Status/Capacity	
  	localhost	Primary	10.1.3-269	0% 	Actions ▾
  	...	Primary	10.1.3-269	0% 	Actions ▾
  	...	Primary	10.1.3-566	0% 	Actions ▾

## OPTION 2: TESTING DEPLOYMENT OF IBM SPECTRUM PROTECT PLUS IN AN EXISTING VPC

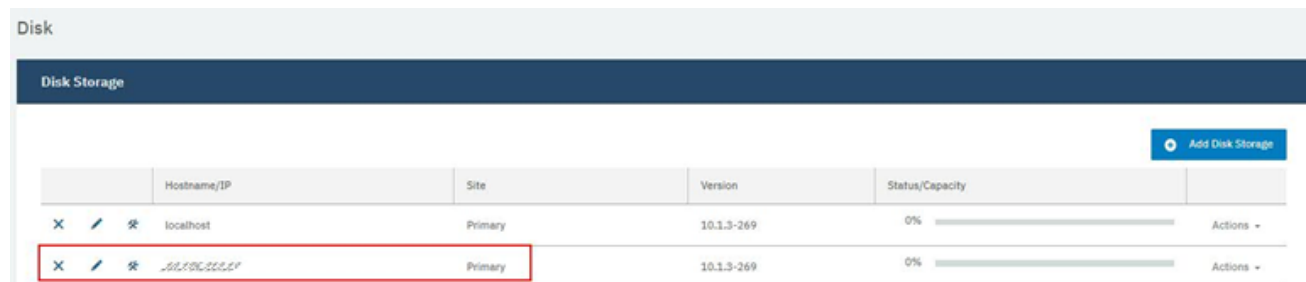
When you deploy IBM Spectrum Protect Plus in an existing VPC, after your vSnap server and repository are configured, the template registers the new vSnap server in your on-premises IBM Spectrum Protect Plus server.

To ensure that the vSnap server was successfully registered as a backup storage device, complete the following steps:










1. In a supported web browser, start the IBM Spectrum Protect Plus user interface by entering the host name or IP address of the machine where IBM Spectrum Protect Plus is deployed.

For a list of browsers that are supported by each IBM Spectrum Protect Plus version, go to the [system requirements](#) overview page and click the version of IBM Spectrum Protect Plus that you are using. Then click **System requirements > Browser support**.

2. In the navigation pane, click **System Configuration > Backup Storage > Disk**.
3. Confirm that the vSnap server is shown in the list of disk storage as shown in the following example:



Disk Storage

	Hostname/IP	Site	Version	Status/Capacity	
  	localhost	Primary	10.1.3-269	0% 	Actions 
  	10.1.3.269	Primary	10.1.3-269	0% 	Actions 

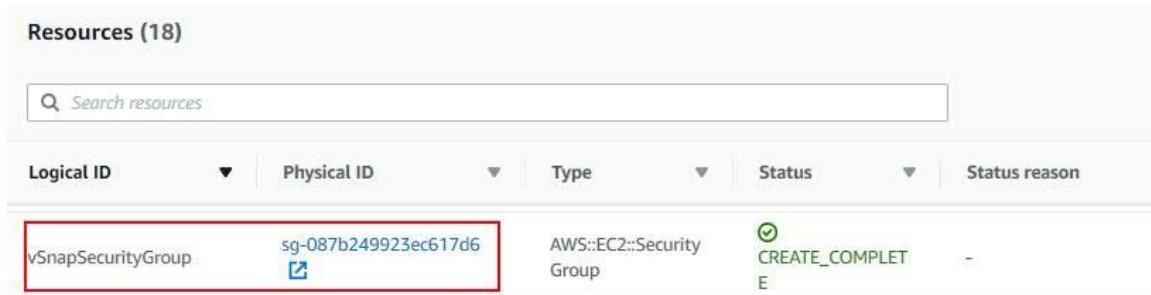
## Step 5. Enable SSH connection to vSnap server (optional)

In most cases, the IBM Spectrum Protect Plus user interface is used to manage the vSnap server and that communication is managed by the REST API. However, if you want to connect to the vSnap server from a server that has an IP address that is outside of the VPC, for example, to download the .run file to upgrade the vSnap server to a later version, you must update the vSnap server security group and enable a Secure Shell (SSH) connection.

By default, security group blocks any SSH connections from servers that are outside of the VPC.

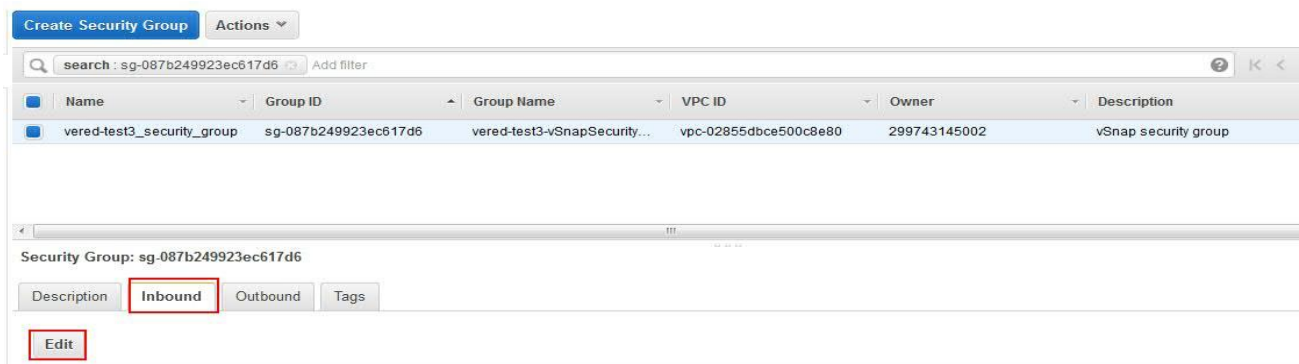
To update the security group, complete the following steps:

1. Open the AWS CloudFormation console and navigate to the Stacks page.
2. Select the stack for the vSnap server instance and then click the **Resources** tab.
3. Find vSnapSecurityGroup in the Logical ID column, and then click the ID in the **Physical ID** column to open the security group instance.



Logical ID	Physical ID	Type	Status	Status reason
vSnapSecurityGroup	sg-087b249923ec617d6	AWS::EC2::Security Group	CREATE_COMPLETE	-

4. On the **Create Security Group** tab, click **Inbound > Edit**.



Create Security Group Actions

search : sg-087b249923ec617d6 Add filter

Name	Group ID	Group Name	VPC ID	Owner	Description
vered-test3_security_group	sg-087b249923ec617d6	vered-test3-vSnapSecurity...	vpc-02855dbce500c8e80	299743145002	vSnap security group

Security Group: sg-087b249923ec617d6

Description Inbound Outbound Tags

Edit

5. Add a new inbound rule for SSH and specify the CIDR from which you would like to provide SSH access to the vSnap server.

Type <small>(i)</small>	Protocol <small>(i)</small>	Port Range <small>(i)</small>	Source <small>(i)</small>
SSH <small>▼</small>	TCP	22	Custom <small>▼</small> 192.0.2.0/24

6. Issue the following command to enable an SSH connection to the vSnap server:

```
ssh -I key-pair-file serveradmin@ip-address
```

where:

The parameter *key-pair-file* is a .pem file that contains the public and private keys that are required to connect to the vSnap server.

The parameter *serveradmin* is the required user name. This user has sudo privilege. The root user is blocked from access.

The parameter *ip-address* is the IP address for the vSnap server instance.

To find the IP address for the vSnap server instance, select the stack for the instance and then click the **Outputs** tab.

Stack info	Events	Resources	Outputs	Parameters	Template
<b>Outputs (5)</b>					
<input type="text" value="Search outputs"/>					
Key <small>▼</small>	Value <small>▼</small>	Description <small>▼</small>			
vSnapIpAddress	192.0.2.10	IP address of the newly created EC2 instance			

## Best practices for using IBM Spectrum Protect Plus on AWS

Use the [IBM Spectrum Protect Plus blueprint](#) to help you optimize your IBM Spectrum Protect Plus environment.

The blueprint provides guidance on how to build an IBM Spectrum Protect Plus solution with a focus on how to properly size, build, and place storage components in your environment.

### Security

The AWS Cloud provides a scalable, highly reliable platform that helps customers deploy applications and data quickly and securely.

When you build systems on the AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, you assume responsibility and management of the guest operating system (including updates and security patches), other associated applications, as well as the configuration of the AWS-provided security group firewall. For more information about security on AWS, visit the [AWS Security Center](#).

### AWS Identity and Access Management (IAM)

This solution leverages an IAM role with least privileged access. It is not necessary or recommended to store SSH keys, secret keys, or access keys on the provisioned instances.

A new IAM role is created to enable the usage of Cloud-Watch and Lambda scripts.

When you launch the AWS CloudFormation template, if you select the check box to acknowledge that the template will create IAM resources under **Capabilities**, AWS CloudFormation will automatically acquire the IAM resources.

 The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more.](#)

I acknowledge that AWS CloudFormation might create IAM resources.

## OS Security

The root user is blocked from access. Use the serveradmin user, which has sudo privilege, for SSH and connection purposes.

The vSnap server instance can be accessed only by using the SSH key that is specified during the deployment process. AWS doesn't store the SSH key. If you lose your SSH key, you can lose access to the vSnap server instance. Operating system patches are your responsibility and should be performed on a periodic basis.

## Security Groups

A security group acts as a firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time. The new rules are automatically applied to all instances that are associated with the security group.

The security groups created and assigned to the vSnap server instance as part of this solution is restricted as much as possible while allowing access to the various functions needed by IBM Spectrum Protect Plus. We recommend reviewing security groups to further restrict access as needed once the instance is up and running.

The AWS CloudFormation template creates the following security group rules for IBM Spectrum Protect Plus:

- Open port 111 for all VPC IPs to allow clients to discover ports that Open Network Computing (ONC) clients require to communicate with ONC servers (internal).
- Open port 22 for all VPC IPs for OpenSSH.  
Note – by default, the vSnap server SSP connection is blocked for any address outside the VPC.
- Open port 2049 and 20048 for all VPC IPs for NFS data transfer to/from the vSnap server
- Open port 3260 for all VPC IPs for iSCSI data transfer to/from the vSnap server
- Open port 8900 for IBM Spectrum Protect Plus IP to allow communication for vSnap server REST APIs
- Open ICMP port for VPC IPs and IBM Spectrum Protect Plus to allow ping tests

It's very likely that additional ports must be open to support IBM Spectrum Protect Plus features. For example, port 9000 is required to offload data to IBM Spectrum Protect server. See the [system requirements](#) for the version of IBM Spectrum Protect Plus that you are using.

## Troubleshooting

**Q.** A `CREATE_FAILED` error occurred with a timeout message when the AWS CloudFormation template was launched.

Logical ID	Status Reason
NatTets2	The following resource(s) failed to create: [vSnapWaitCondition].
vSnapWaitCondition	WaitCondition timed out. Received 0 conditions when expecting 1

**A.** If the AWS CloudFormation template fails to create the stack, relaunch the template with the **Rollback on failure** option set to **No**. (This setting is under **Advanced** on the Options page when you create or update a stack in the AWS CloudFormation console.) This option retains the state of the stack and the vSnap server instance is left running so that you can troubleshoot the issue. Review the log files `/var/log/cloud-init-output.log` and `/root/SPP/log/aws_vsnap_config.log`.



**Important** When you set **Rollback on failure** to **No**, you will continue to incur AWS charges for this stack. When you finish troubleshooting, delete the stack.

One of the most common failures occurs when the NAT gateway is not configured properly during an attempt to use the template for deployment in an existing VPC. If this error occurs, connect to the vSnap server and try to ping to 8.8.8.8. If the ping fails, there is no routing occurring from your VPC. Fix this issue before you retry to create the stack.


For additional information, see [Troubleshooting AWS CloudFormation](#) on the AWS website.




**Q.** A `LimitExceeded` error occurred for a stack event and the stack creation failed.

RESS			
13 May 2019 07:17:20	myVPC	 <code>CREATE_FAILED</code>	The maximum number of VPCs has been reached. (Service: AmazonEC2; Status Code: 400; Error Code: <code>VpcLimitExceeded</code> ; Request ID: 69d0024f-0679-4c35-a7ed-380d183478cd )
13 May 2019 07:17:20	NATEIP	 <code>CREATE_FAILED</code>	The maximum number of addresses has been reached. (Service: AmazonEC2; Status Code: 400; Error Code: <code>AddressLimitExceeded</code> ; Request ID: aaddb219-cf60-4ec5-8b5d-3d450a6eede7)

Or

13 May 2019 07:28:13	NATEIP	 <code>CREATE_FAILED</code>	The maximum number of addresses has been reached. (Service: AmazonEC2; Status Code: 400; Error Code: <code>AddressLimitExceeded</code> ; Request ID: 78a11d4f-10b0-41e9-b2ba-1c252e42ddd4 )
----------------------	--------	--	---

Or

13 May 2019 07:30:53	NAT	 <code>CREATE_FAILED</code>	Performing this operation would exceed the limit of 5 NAT gateways (Service: AmazonEC2; Status Code: 400; Error Code: <code>NatGatewayLimitExceeded</code> ; Request ID: 8952998b-fee2-475d-ba27-0c4d364cb42c )
----------------------	-----	--	---

**A.** You might encounter this error if you try to deploy a service that exceeds your account's limits. To address this problem, [request a service limit increase](#) for the EC2 instance types that you intend to deploy. In the AWS Support Center, click **Create Case > Service Limit Increase > EC2 instances**, and then complete the fields in the form.

**Q.** When using an AWS CloudFormation template for deployment to an existing VPC, stack creation fails with the message that the Availability Zone is invalid.

13 May 2019 07:08:35	vered-test-main1	⊗ ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [vSnapInstance]. . Rollback requested by user.
13 May 2019 07:08:34	vSnapInstance	⊗ CREATE_FAILED	Value (us-east-2a) for parameter availabilityZone is invalid. Subnet 'subnet-0a75f223662babf20' is in the availability zone us-east-2c (Service: AmazonEC2; Status Code: 400; Error Code: InvalidParameterValue; Request ID: b4f1a1de-eb72-4028-ad66-2e88d4123a44 )

**A.** The subnet and the Availability Zone that you provided in the AWS CloudFormation template do not correspond. The subnet exists in a different Availability Zone. Choose the correct Availability Zone for the subnet and run the template again. To find the Availability Zone for the subnet, navigate to the Subnets page of the AWS VPC console.

**Q.** Stack creation failed with a message to see a CloudWatch log.

05 May 2019 12:47:03	Elena2	⊗ CREATE_FAILED	The following resource(s) failed to create: [vSnapWaitCondition].
05 May 2019 12:47:01	vSnapWaitCondition	⊗ CREATE_FAILED	WaitCondition received failed message: 'Failed to run aws_register_vsnap.py, could be due to (Invalid input parameter, Failed to register external vSnap), For more information please refer to the cloudwatch log' for uniqueId: i-06249e69749e26739

Or

13 May 2019 09:57:07	vSnapWaitCondition	⊗ CREATE_FAILED	WaitCondition received failed message: 'Failed to run create_vsnap_pool.py, could be due to (Invalid input parameter, No disks for assigned for vSnap pool, rescan disks failed, list pools failed, failed expanding pool, failed enabling dedupe), For more information please refer to the cloudwatch log' for uniqueId: i-041b8da866152c53d
----------------------	--------------------	-----------------	--

Or

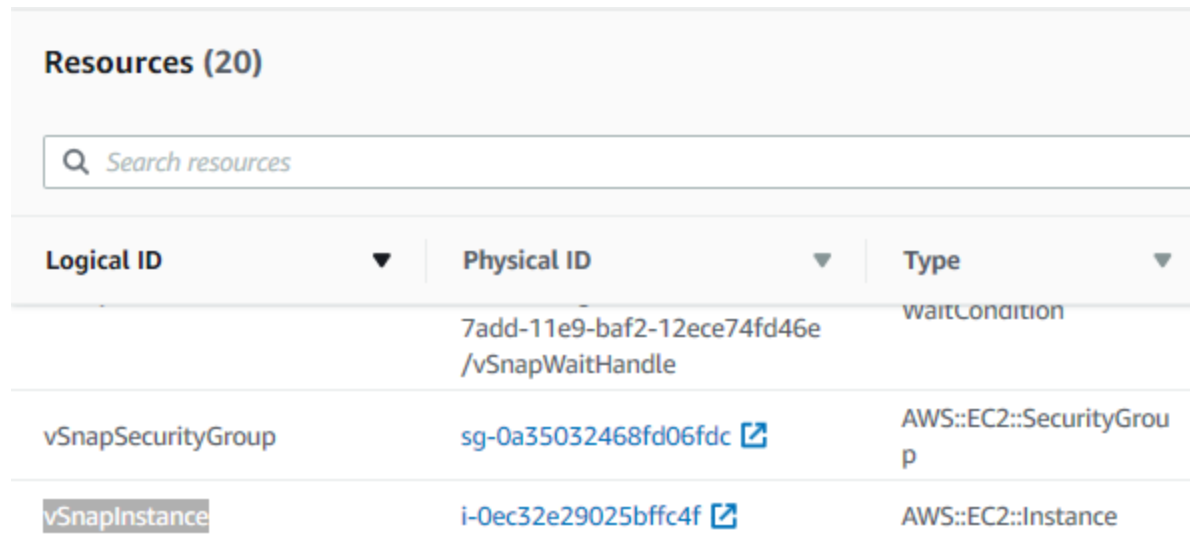
13 May 2019 11:04:43	ElenaForOded	⊗ CREATE_FAILED	The following resource(s) failed to create: [vSnapWaitCondition].
13 May 2019 11:04:42	vSnapWaitCondition	⊗ CREATE_FAILED	WaitCondition received failed message: 'Failed to run vsnap_init.py' for uniqueId: i-08b9b441bd8399d52

**A.** Stack creation might fail for many reasons when installing and configuring the vSnap server.

All vSnap server configuration logs are available in AWS CloudWatch.

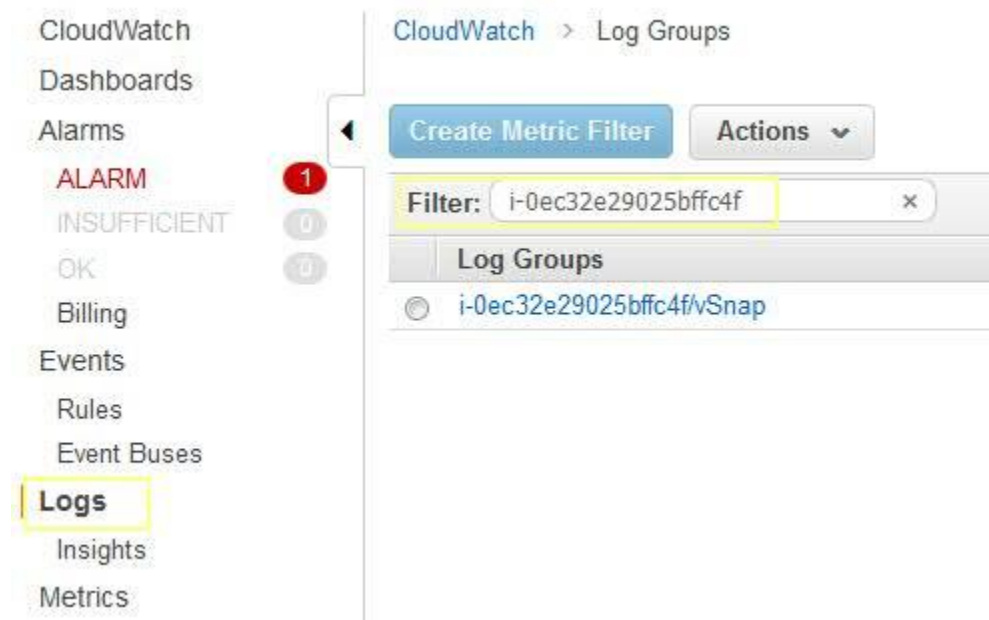
To review the logs in AWS CloudWatch:

1. Select the stack for the vSnap server instance in the AWS CloudFormation console, and then click the **Resources** tab.
2. Find vSnapInstance in the Logical ID column and copy the ID.



Logical ID	Physical ID	Type
	7add-11e9-baf2-12ece74fd46e /vSnapWaitHandle	waitCondition
vSnapSecurityGroup	sg-0a35032468fd06fdc <a href="#">↗</a>	AWS::EC2::SecurityGroup
<b>vSnapInstance</b>	i-0ec32e29025bffc4f <a href="#">↗</a>	AWS::EC2::Instance

3. Open the AWS CloudWatch console, and click **Logs** in the navigation pane.
4. Paste the instance ID in the **Filter** field.



CloudWatch > Log Groups

Create Metric Filter Actions

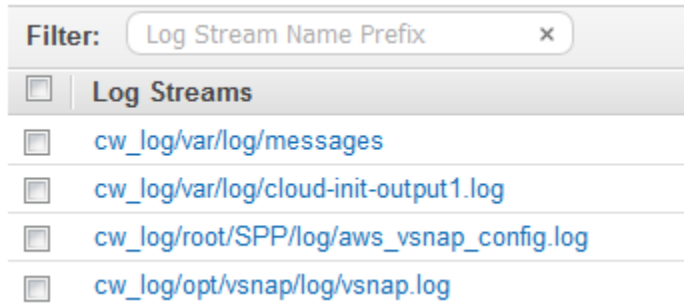
Filter: i-0ec32e29025bffc4f x

Log Groups

- i-0ec32e29025bffc4f/vSnap

Navigation pane: CloudWatch, Dashboards, Alarms, ALARM, INSUFFICIENT, OK, Billing, Events, Rules, Event Buses, **Logs**, Insights, Metrics

5. Click the log group that is found and review logs to view information about the installation and configuration process and failures.



For additional details about the failure, review the `aws_vsnap_config.log` file.

**Q.** Stack creation failed because the CIDR range is invalid.

13 May 2019 09:39:42	PrivateSubnet	<span style="color: red;">⊗</span> CREATE_FAILED	The CIDR '9.0.3.0/24' is invalid. (Service: AmazonEC2; Status Code: 400; Error Code: InvalidSubnet.Range; Request ID: 64af0bbd-a50c-48f2-a16e-99cec30a4d23)
----------------------	---------------	--	---

**A.** The subnet CIDR that you provided in the AWS CloudFormation template does not match the VPC CIDR.

Run the stack creation again and provide corresponding VPC and subnet CIDRs. For additional information, see [VPC and Subnet on AWS](#).

**Q.** Launching the AWS CloudFormation template fails with following message:

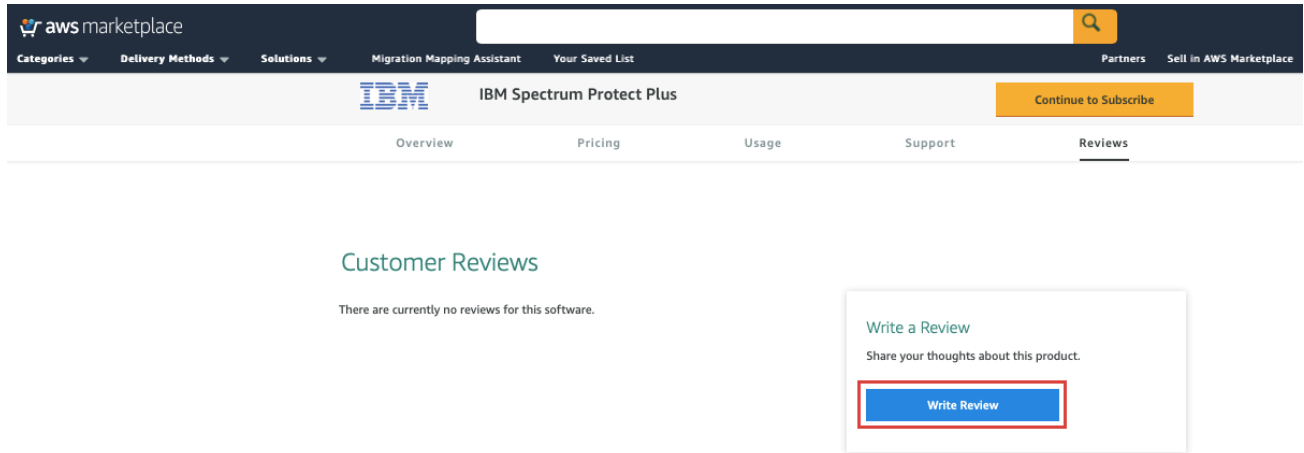
⊗ Template error: Unable to get mapping for Region2Principal::us-west-1::EC2Principal

**A.** The region that you are trying to deploy to is not supported because the IBM Spectrum Protect Plus AMI does not exist in this region.

Change the region and run the template again.

## Send us feedback

To post feedback, submit feature ideas, or report bugs, open the [IBM Spectrum Protect Plus](#) page in AWS Marketplace, and then click **Write Review**.



## Additional resources

### AWS resources

- [Getting Started Resource Center](#)
- [AWS General Reference](#)
- [AWS Glossary](#)

### AWS services

- [AWS CloudFormation](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [IAM](#)
- [Amazon VPC](#)

### IBM Spectrum Protect Plus documentation

- [IBM Spectrum Protect Plus Knowledge Center](#)

© 2019, Amazon Web Services, Inc. or its affiliates, and IBM. All rights reserved.

### **Notices**

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at <http://aws.amazon.com/apache2.0/> or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

## Document revisions

Date	Change	In sections
June 2019	Initial publication	—