IBM Spectrum Protect Plus Version 10.1.6 on the AWS Cloud

Deployment Guide
July 2020

Contents

Overview

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

> **Important** The IBM Spectrum Protect Plus on AWS deployment includes IBM Spectrum Protect Plus Version 10.1.6. To use a later version of IBM Spectrum Protect Plus, you must update the installed components to that version. For update 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 Updating IBM Spectrum Protect Plus components.

What is IBM Spectrum Protect Plus

IBM Spectrum Protect Plus is a modern data protection solution that simplifies data backup and recovery for virtual machines (VMs) and databases running on both virtual and physical machines. It unlocks the value of your data to facilitate data reuse and accelerate DevOps, analytics, and more. IBM Spectrum Protect Plus is designed to support rapid deployment and ease of maintenance. You can deploy the product as a virtual appliance and take advantage of the product's agentless architecture, which helps to simplify maintenance.

To facilitate rapid data recovery, IBM Spectrum Protect Plus creates and maintains a global catalog of protected VMs, files, databases, and applications, enabling administrators to see what is protected, and more importantly, what isn't. When data recovery is required, the catalog and search interface enable administrators to identify what they want to recover, eliminating the need to sort through hundreds of objects and recovery points.

Administrators can use a single data protection policy to govern data backup, replication, and copy operations. For data copy, IBM Spectrum Protect Plus integrates with Amazon S3 to provide cost-effective, long-term data retention and disaster recovery for all supported workloads (VMs, databases, and applications).

A centralized dashboard and policy-based templates streamline operations and help ensure compliance with service level agreements (SLAs). On the dashboard, you can view the state of your on-premises and AWS environment and identify failed jobs, capacity and device issues, and other areas of concern.

Representational State Transfer (REST) application programming interfaces (APIs) are available to automate data protection operations and to integrate third-party tools and solutions, such as Puppet and ServiceNow.

The primary components of IBM Spectrum Protect Plus are an IBM Spectrum Protect Plus server and one or more vSnap servers. The IBM Spectrum Protect Plus server manages all components in the system. The vSnap server is the primary snapshot backup location for IBM Spectrum Protect Plus.

Deploying IBM Spectrum Protect Plus to AWS

The purpose for deploying IBM Spectrum Protect Plus on AWS is to protect the following:

- One or more of the following databases that are running on AWS cloud:

    o IBM Db2

    o Microsoft SQL Server

    o Microsoft Exchange Server

    o Oracle

    o MongoDB

    o Office 365

- EC2 instances. You can backup, restore and reuse snapshots of all EC2 instances that are associated with your AWS account.

- Virtual machines that are managed by VMware Cloud (VMC) on AWS while having the IBM Spectrum Protect Plus server installed on VMC and the vSnap server installed on the AWS VPC. For more information about support for VMware Cloud on AWS, see IBM Spectrum Protect Plus for VMware Cloud on AWS.

You can deploy IBM Spectrum Protect Plus in AWS in one of the following configurations. Support for VMC on AWS is available only in a hybrid environment.

All-on-cloud environment: In this configuration, both the IBM Spectrum Protect Plus server and the vSnap server are deployed in AWS on an existing or new Virtual Private Cloud (VPC). An on-premises IBM Spectrum Protect Plus server and a Microsoft Hyper-V or VMware infrastructure are not required.

This option might benefit new IBM Spectrum Protect Plus users who want to protect databases on AWS and do not have IBM Spectrum Protect Plus running in an on-premises environment.

Hybrid environment: In this configuration, only the vSnap server is deployed in AWS on an existing or new VPC. The IBM Spectrum Protect Plus server is installed and maintained on premises or another location. This option might benefit IBM Spectrum Protect Plus users who want to continue protecting workloads that are running on premises and in the cloud environment.

In addition to backup and recovery operations, you can also use a hybrid environment to replicate and reuse data between your on-premises location and AWS for additional data protection. For example, you might want to use data that is protected at your on-premises site on AWS for DevOps, quality assurance, testing, and disaster recovery purposes.

USING AN EXISTING OR NEW VPC

For an all-on-cloud or hybrid environment, you can deploy IBM Spectrum Protect Plus to an existing VPC or a new VPC. The deployment to the VPC is automated by an AWS CloudFormation template.

To deploy IBM Spectrum Protect Plus to an existing or new VPC, one private subnet and one public subnet with a bastion host are required.

To deploy to an *existing* VPC, you must provide the VPC ID in the CloudFormation template and an existing bastion host IP address.

To deploy to a *new* VPC, you must provide network parameters in the CloudFormation template. An AWS environment is then created, which consists of the VPC, subnets, network address translation (NAT) gateways, security groups, and other infrastructure components.

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 and storage layout types, 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 can reside on the Amazon Cloud or on premises, must be licensed for the physical data that is protected on the AWS environment. If you choose to have the IBM Spectrum Protect Plus server on Amazon Cloud, the server is deployed in an evaluation mode for a limited time period of up to 30 days. A valid product key is required to enable IBM Spectrum Protect Plus features after the evaluation period.

PURCHASING AND REGISTERING AN IBM SPECTRUM PROTECT PLUS LICENSE

To purchase a license for IBM Spectrum Protect Plus and to choose a perpetual or monthly purchase order, go to [IBM Spectrum Protect Plus Pricing](#).

To register the license, see the instructions for [uploading the product key](#).

For additional licensing information, contact [IBM Support](#).

SUBSCRIBING TO THE AMI FOR IBM SPECTRUM PROTECT PLUS

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 offers two types of configuration sets through the CloudFormation templates: all on cloud and hybrid.

Option 1: All on cloud

In an all-on-cloud environment, the IBM Spectrum Protect Plus server and the vSnap server are hosted on AWS as shown in the following figure. The management, access control, and licensing features of IBM Spectrum Protect Plus are managed and maintained by the IBM Spectrum Protect Plus server, while the vSnap server stores the snapshot backups.

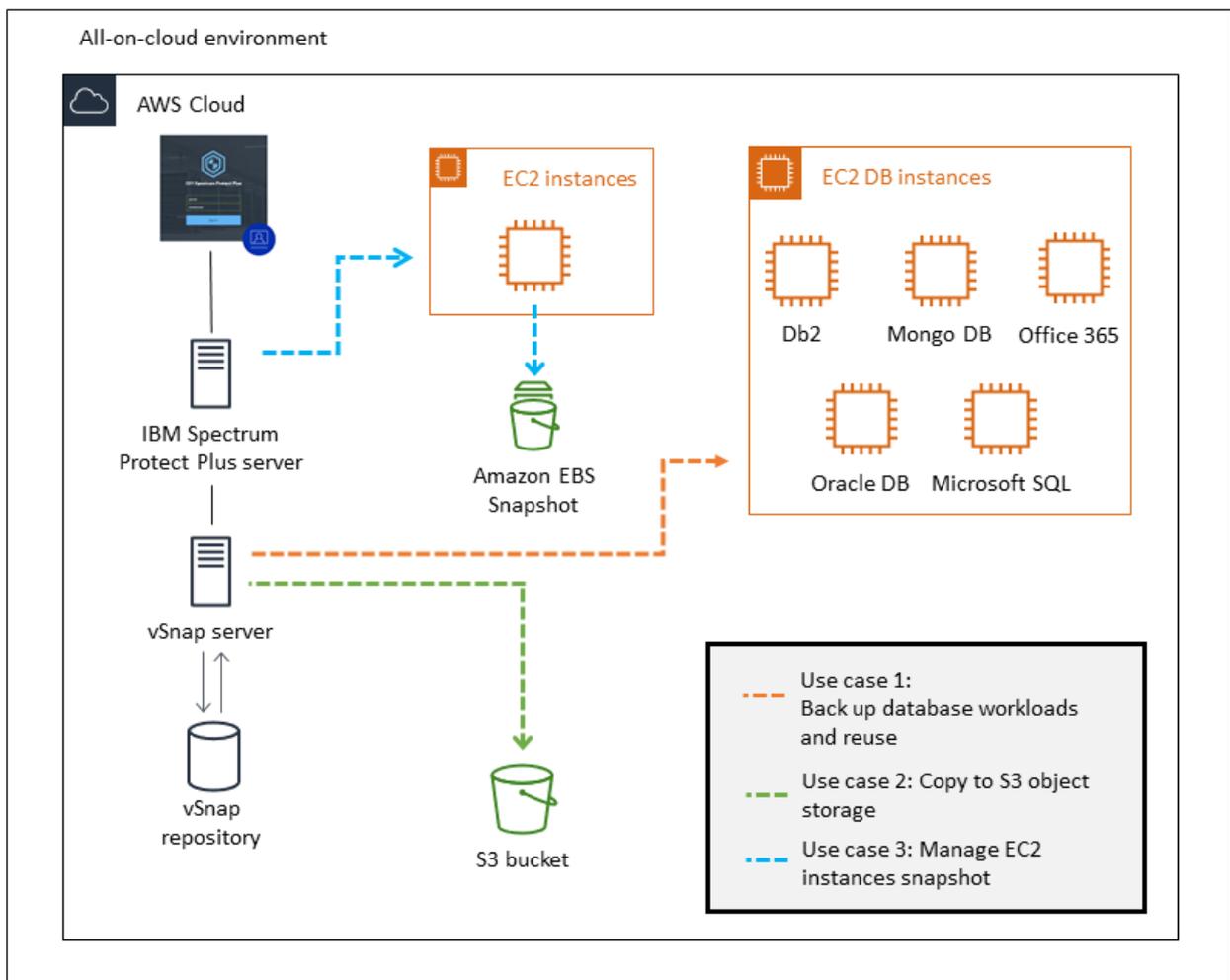Optionally, you can copy snapshots from the vSnap server to an S3 bucket.

Figure 1: Architecture for an all-on-cloud environment

You can deploy the IBM Spectrum Protect Plus server and vSnap server to an existing VPC or a new VPC. The deployment to the VPC is automated by an AWS CloudFormation template.

The components that are deployed by the template depend on whether you are deploying IBM Spectrum Protect Plus to an existing VPC or a new VPC.

If you are deploying to an existing VPC, the components that are indicated by an asterisk (*) in the following list must exist before you start the deployment.

If you are deploying to a new VPC, the VPC is created by the template and all of the components in the list are deployed.

- An IBM Spectrum Protect Plus server and a vSnap server that are mounted and provisioned for your repository size.

- Two security groups to restrict access to only necessary protocols and ports.

- A user name and password for the vSnap server authentication.

- A user name and password for the IBM Spectrum Protect Plus server authentication.

- A 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 required for the deployment process.

- An Amazon CloudWatch service to monitor AWS resources and logs.

- A VPC that spans one Availability Zone and includes one public and one private subnet. *

- An internet gateway to allow access to the internet. *

- A bastion host on a public subnet. The bastion host enables secure shell (SSH) access to the vSnap server. *

- An EC2 server instance that is configured with the vSnap server by using the instance type that is recommended by the [IBM Spectrum Protect Plus Blueprint](#).

  Each vSnap server EC2 instance will include the following items:

  - A 50 GiB Elastic Block Store (EBS) solid-state drive (SSD) volume for the root device

  - An EBS SSD volume for the cloud cache as defined by the blueprint that corresponds to the vSnap server repository size

  - A dynamic number of EBS sc1 volumes to support the repository size during deployment

  - Logs and cache disks as defined by the blueprint that correspond to the vSnap server repository size

- An EC2 server instance that is configured with the IBM Spectrum Protect Plus management server by using the instance type - r5a.2xlarge, which is recommended by the [IBM Spectrum Protect Plus Blueprint](#).

  Each IBM Spectrum Protect Plus server EC2 instance will include the following items:
  - A 70 GiB EBS SSD volume for the root device
  - A 50 Gib EBS SSD volume for PostgresSQL
  - A 50 Gib EBS SSD volume for MongoDB
  - A 150 Gib EBS SSD volume for Lucene indexing

The AWS CloudFormation template configures and builds a stack consisting of the IBM Spectrum Protect Plus server and the vSnap server and repository on AWS according to the size that you choose for the vSnap pool (up to 100 TiB).

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

When the IBM Spectrum Protect Plus server and vSnap server repository are configured, the template registers the vSnap server with the IBM Spectrum Protect Plus server.

ALL ON CLOUD: DEPLOYING TO AN EXISTING VPC

The following figures illustrate the AWS environment before and after IBM Spectrum Protect Plus is deployed to an existing VPC.

Before deployment
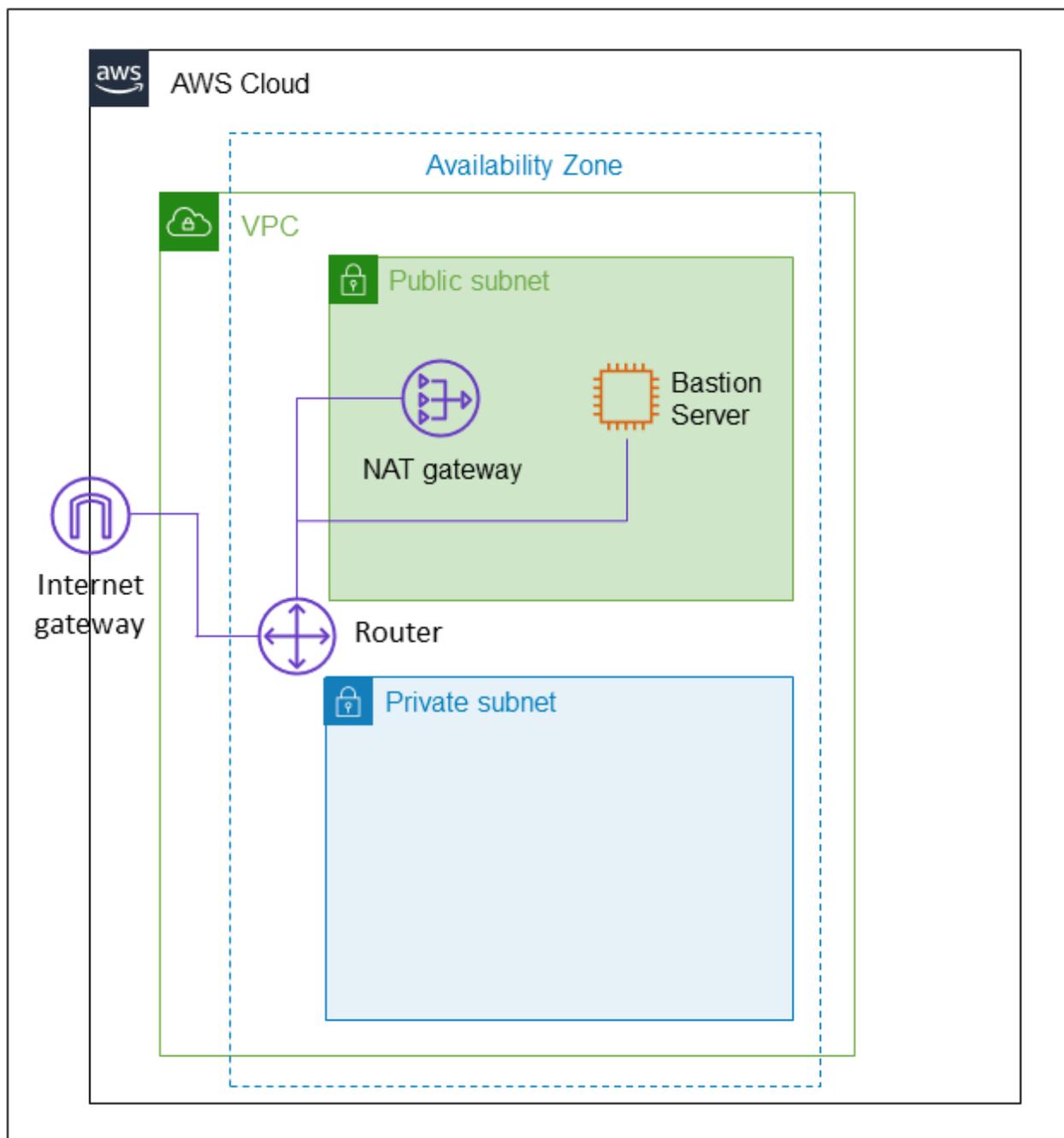

Figure 2: All-on-cloud environment, before deployment to an existing VPC
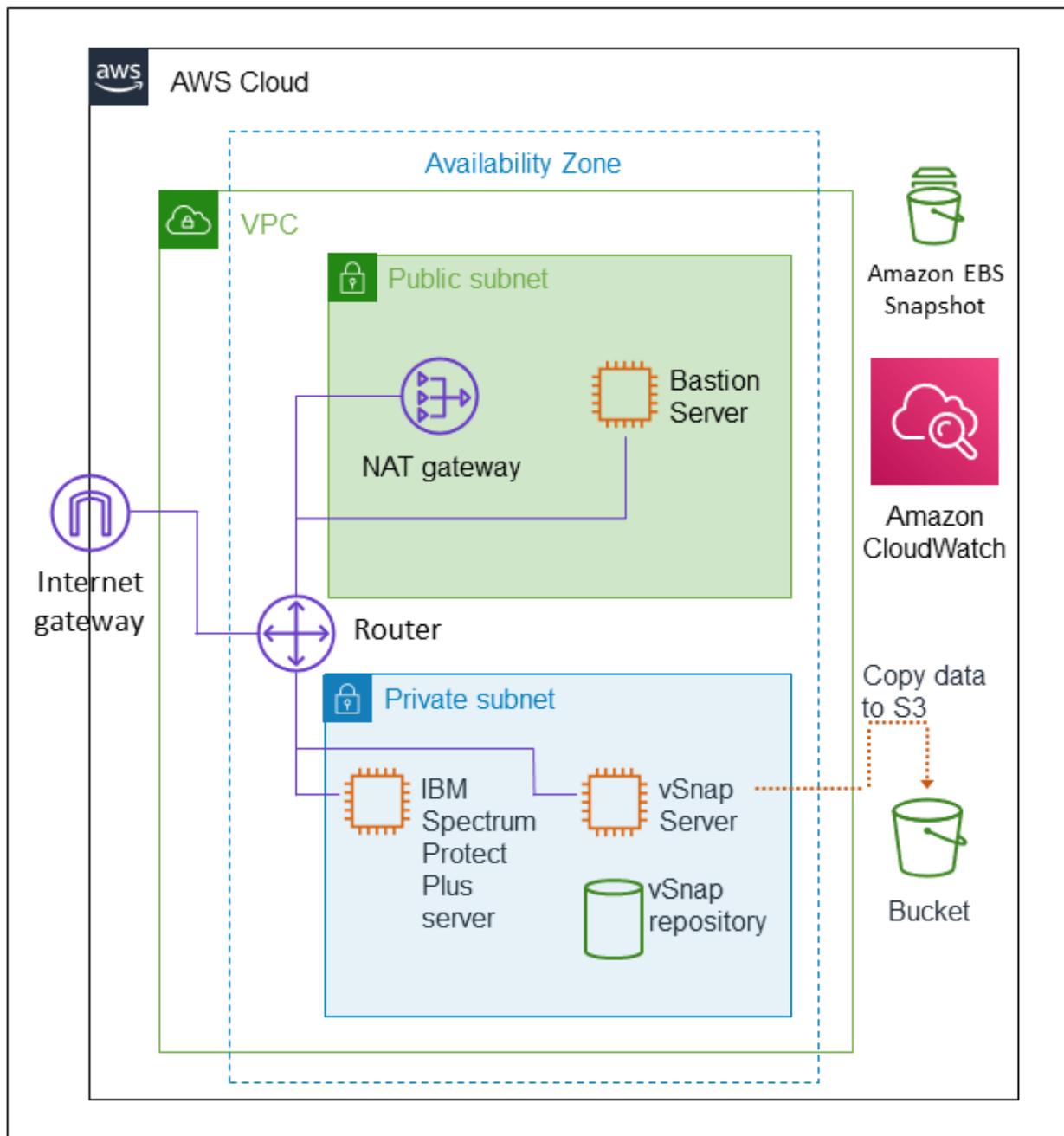
After deployment

Figure 3: All-on-cloud environment, after deployment to an existing VPC

ALL ON CLOUD: DEPLOYING TO A NEW VPC

The following figures illustrate the AWS environment after IBM Spectrum Protect Plus is deployed to a new VPC.
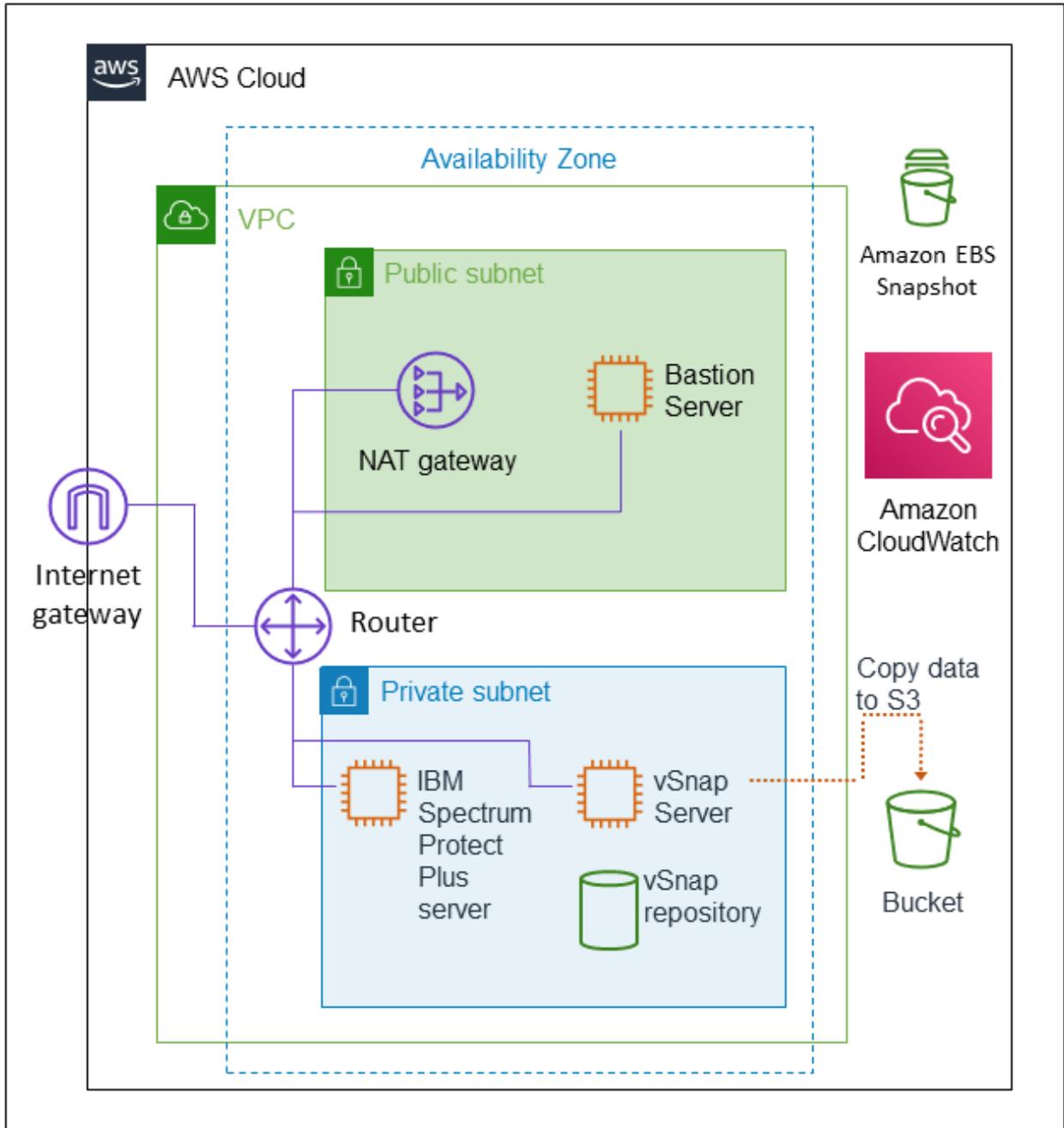
Figure 4: All-on-cloud environment, after deployment to a new VPC

Option 2: Hybrid

In a hybrid environment, a vSnap server is hosted on AWS and the IBM Spectrum Protect Plus server is on premises as shown in the following figure. The IBM Spectrum Protect Plus server provides management, access control, and licensing features, while the vSnap server stores the actual snapshot backups.

Optionally, you can copy snapshots from the vSnap server to an S3 bucket.

As shown in the following figures, you can also have a vSnap server on premises in a hybrid environment. This provides the option of backing up workloads to a vSnap server that is on premises.
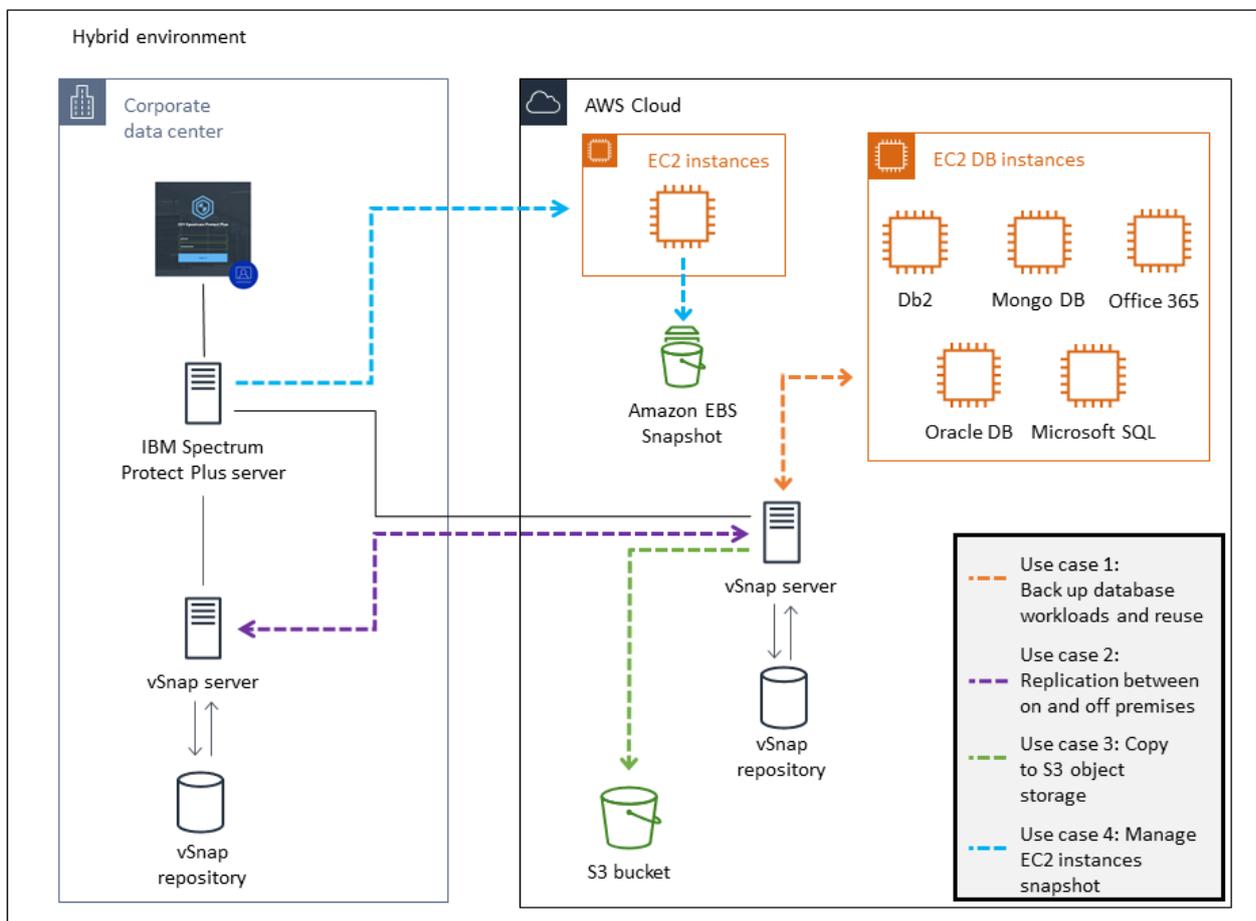
Figure 5: Architecture for a hybrid environment

You can deploy the vSnap server to an existing VPC or a new VPC. The deployment to the VPC is automated by an AWS CloudFormation template.

The components that are deployed by the template depend on whether you are deploying the vSnap server to an existing VPC or a new VPC.

If you are deploying to an existing VPC, the components that are indicated by an asterisk (*) in the following list must exist before you start the deployment.

If you are deploying to a new VPC, the VPC is created by the template and all of the components in the list are deployed.

- A vSnap server that is mounted and provisioned for your repository size.

- The appropriate security groups to restrict access to the required protocols and ports.

- A user name and password for the vSnap server authentication.

- A NAT gateway for outbound internet access from private subnets. *

- An Elastic IP (EIP) for NAT usage. *

- An IAM role with fine-grained permissions for access to AWS services that are necessary for the deployment process.

- An Amazon CloudWatch service to monitor AWS resources and logs.

- A VPC that spans one Availability Zone and includes one public and one private subnet. *

- An internet gateway to allow access to the internet. *

- A bastion host on a public subnet. The bastion host enables SSH access to the vSnap server. *

- An EC2 server instance that is configured with the vSnap server by using the instance type that is recommended by the [IBM Spectrum Protect Plus Blueprint](#).

  Each vSnap server EC2 instance will include the following items:

  - A 50 GiB EBS SSD volume for the root device

  - An EBS SSD volume for cloud cache as defined by the blueprint that corresponds to the vSnap server repository size

  - A dynamic number of EBS sc1 volumes to support the repository size during deployment

  - Logs and cache disks as defined by the blueprint that correspond to the vSnap server repository size

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 the vSnap pool (up to 100 TiB).

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

ESTABLISHING A VPN CONNECTION IN A HYBRID ENVIRONMENT

You must use a virtual private network (VPN) tunnel to establish bidirectional communication between the VPC that contains the vSnap server and the IBM Spectrum Protect Plus server, as shown in the following figure.

> **Important** If you do not establish this communication, the installation and configuration of the vSnap server on AWS fails.
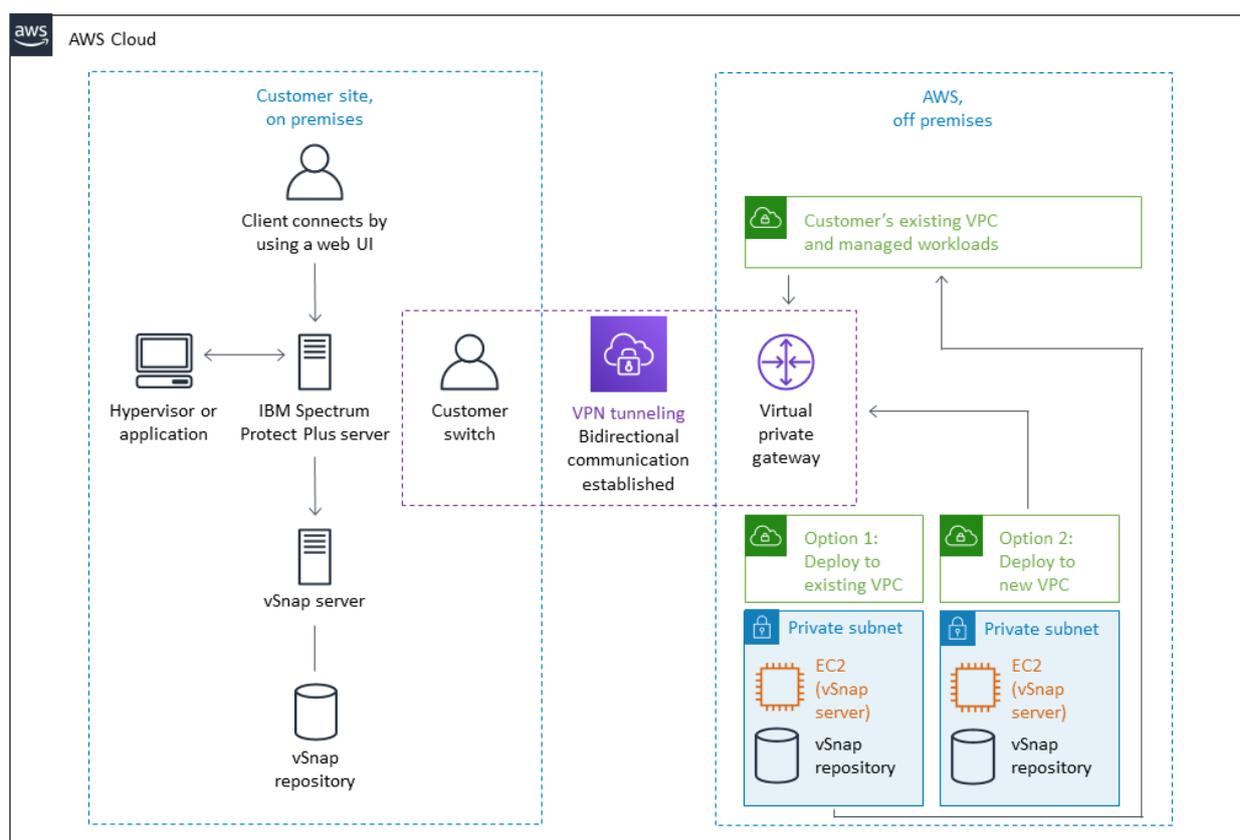
Figure 6: Communication between the vSnap server on AWS and the IBM Spectrum Protect Plus server on premises

If you are deploying the vSnap server in an existing VPC: Ensure that you have the bidirectional VPN connection established between the VPC and the IBM Spectrum Protect Plus server before you set up and configure the AWS CloudFormation template.

When the server and repository are configured, the template registers the new 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 the vSnap server in a new VPC: Configure a bidirectional VPN connection between the VPC and the IBM Spectrum Protect Plus server.

You must 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 (hybrid): Testing an on-premises IBM Spectrum Protect Plus server with a vSnap server in a new AWS VPC.](#)

For the complete steps to deploy the vSnap server to a new or existing VPC, including testing the deployment, see [Deployment steps.](#)

HYBRID: DEPLOYING TO AN EXISTING VPC

The following figures illustrate the on-premises and AWS environment before and after IBM Spectrum Protect Plus is deployed to an existing VPC.
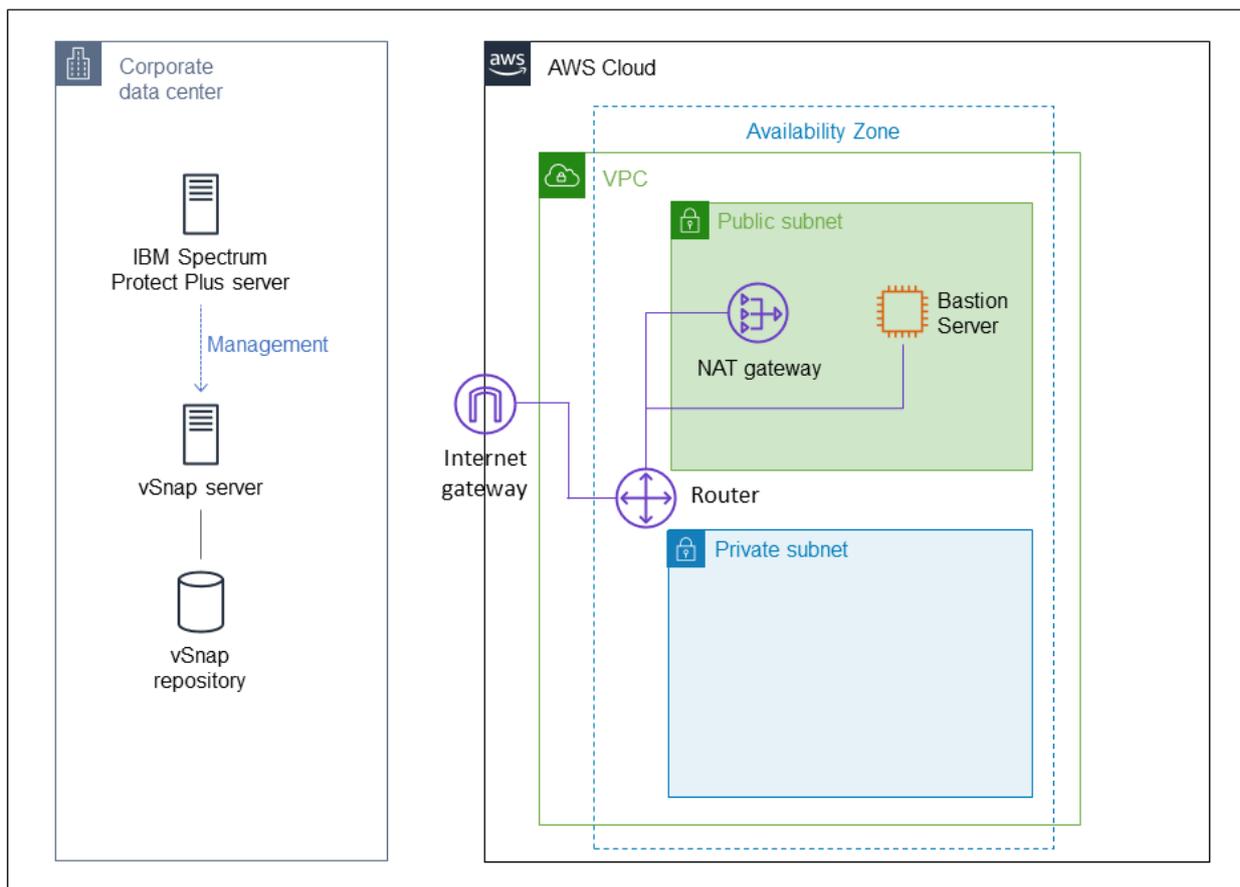
Before deployment

Figure 7: Hybrid environment, before deployment to an existing VPC
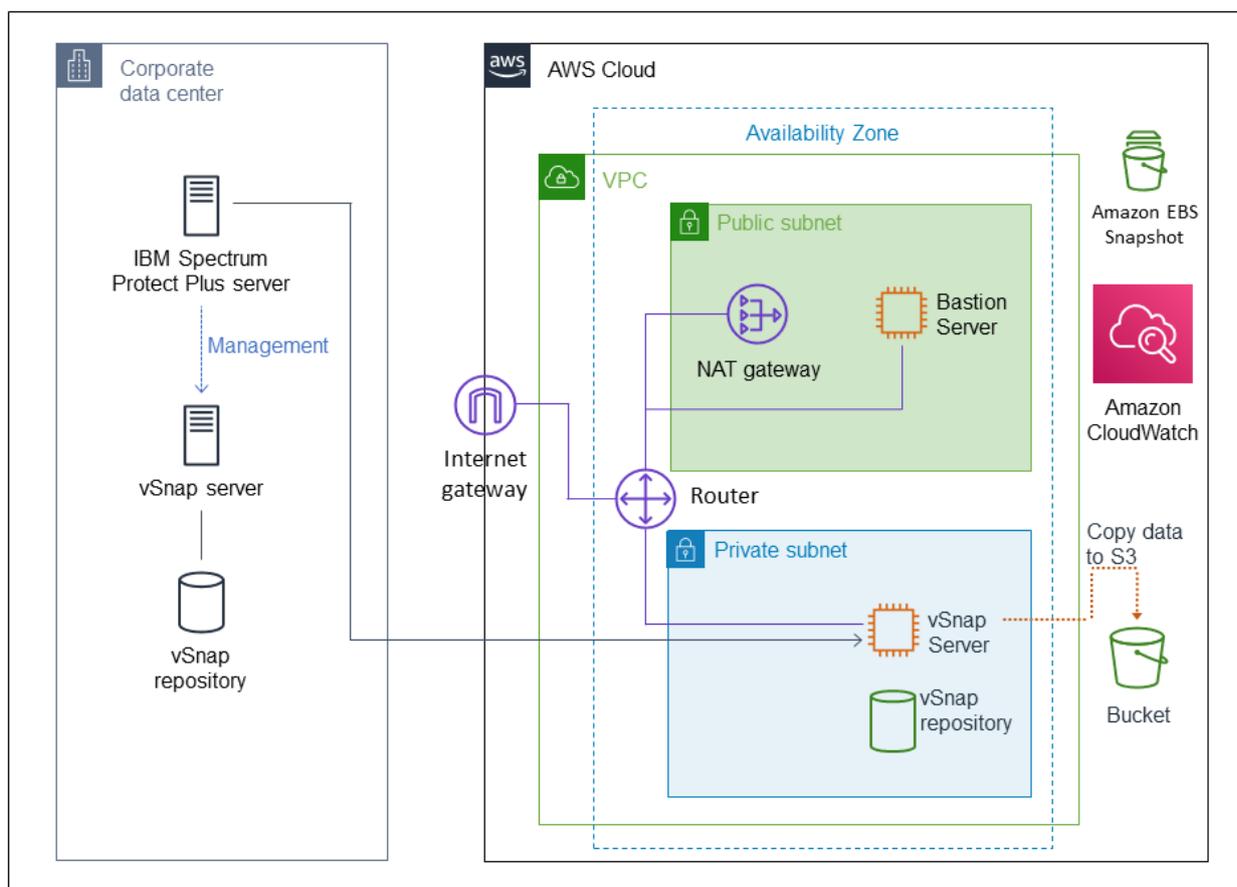
After deployment

Figure 8: Hybrid environment, after deployment to existing VPC

HYBRID: DEPLOYING TO A NEW VPC

The following figures illustrate the on-premises and AWS environment before and after IBM Spectrum Protect Plus is deployed to a new VPC.

Before deployment
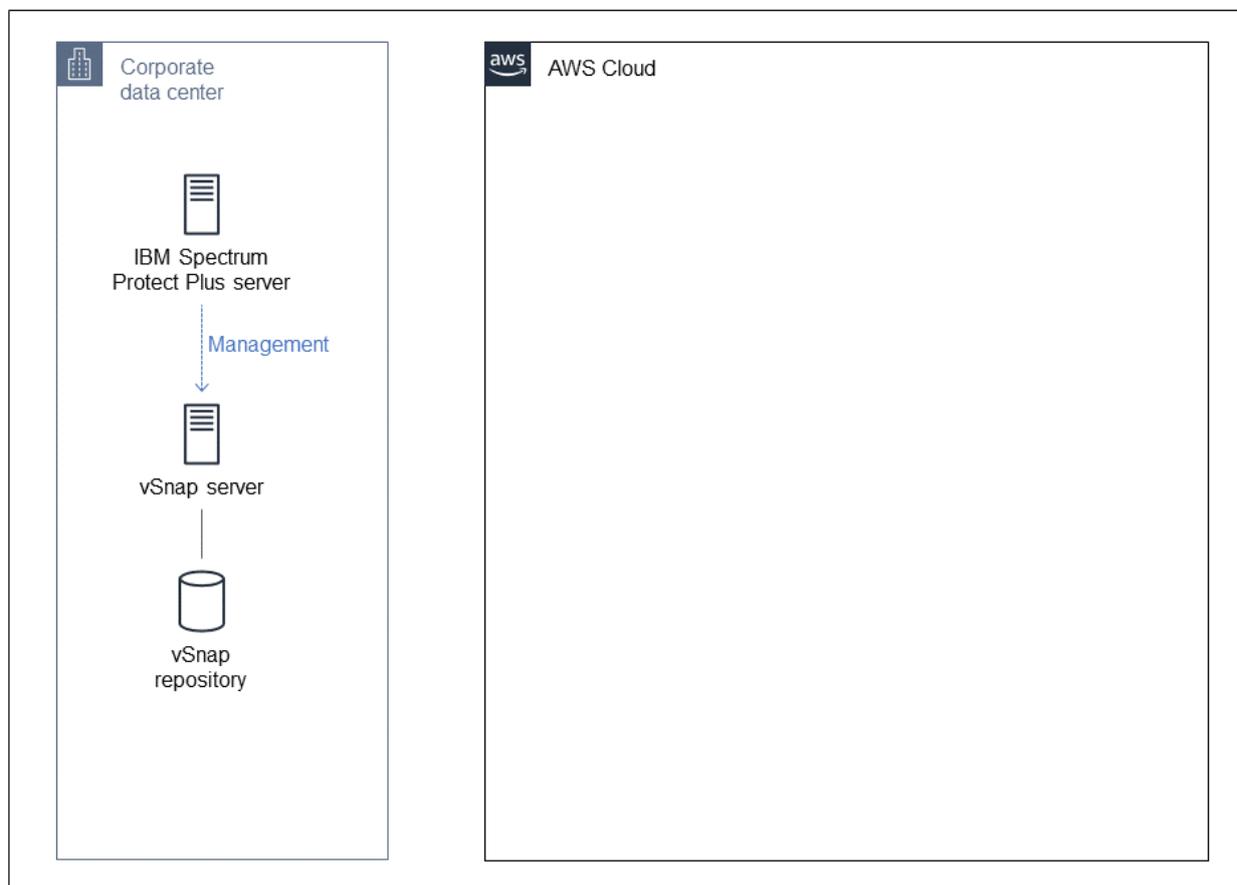
Figure 9: Hybrid environment, before deployment to a new VPC

After deployment

> **Reminder:** You must 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 (hybrid): Testing an on-premises IBM Spectrum Protect Plus server with a vSnap server in a new AWS VPC](#).
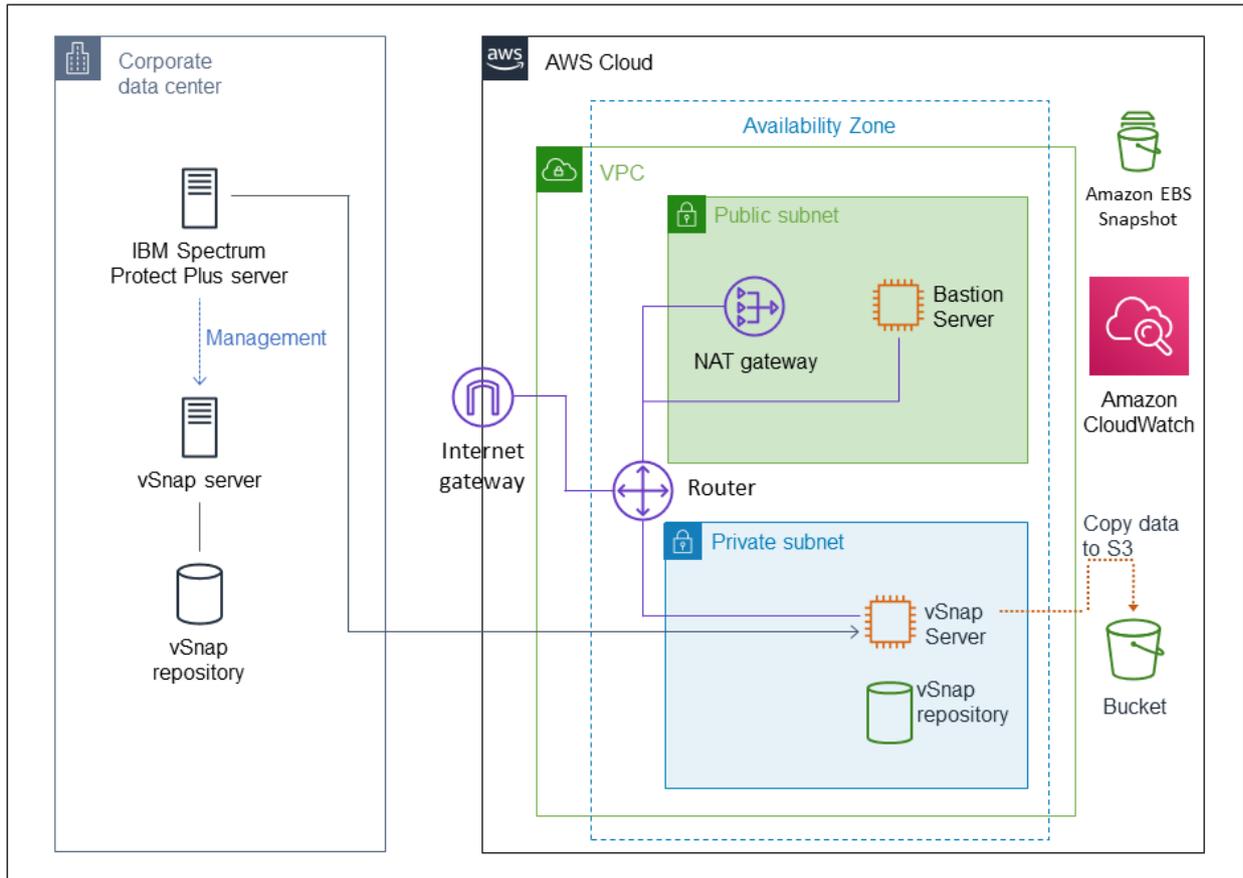
Figure 10: Hybrid environment, after deployment to a new VPC

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.

- **Bastion host -** Including bastion hosts in your VPC environment enables you to securely connect to your Linux instances without exposing your environment to the Internet. After you set up your bastion hosts, you can access the other instances in your VPC through SSH connections on Linux. Bastion hosts are also configured with security groups to provide fine-grained ingress control.

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.

For the price of each EC2 type, see the EC2 instance pricing list.

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	IBM Spectrum Protect Plus server and vSnap server deployment (all on cloud)	vSnap server only (hybrid)
Virtual Private Clouds (VPCs) *	1	1
Elastic IP addresses*	1	1
Security groups	2	1
IAM roles	Up to 3	Up to 3
Instances	Up to 3	Up to 2
HDD EBS Volumes (sc1)	Up to 16	Up to 16
SSD EBS Volumes (gp2)	9	5
NAT gateways *	1	1
Subnets *	2	2
S3 bucket	Up to 1	Up to 1
Internet Gateways *	1	1
Auto scaling group *	1	1

(*) 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.

| 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 to a new VPC or deploy to an existing VPC.

You can deploy both the IBM Spectrum Protect Plus server and the vSnap server in the new or existing VPC (all on cloud) or deploy only the vSnap server (hybrid).

- **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 the IBM Spectrum Protect Plus server and vSnap server or only the vSnap server in this new VPC.

  If you deploy only the vSnap server in the VPC, you must register the vSnap server with your on-premises IBM Spectrum Protect Plus server to complete the vSnap server installation.

- **Deploy IBM Spectrum Protect Plus in an existing VPC**. This option provisions the IBM Spectrum Protect Plus server and vSnap server or only the vSnap server in the existing VPC.

  If you deploy only the vSnap server in an existing VPC, the server installation is completed automatically and manual registration with the IBM Spectrum Protect Plus server is not required.

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 server and 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 choose **Continue to Subscribe**.

3. Review the terms and conditions for software usage, and then choose **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.

4. 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.

1. 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](#).

   Deploy • new VPC • workload

   Deploy • workload only

   [Deploy the IBM Spectrum Plus server and vSnap server or vSnap server only in a new VPC on AWS](#)

   [Deploy the IBM Spectrum Protect Plus server and vSnap server or vSnap server only in an existing VPC on AWS](#)

> **Important** For a hybrid environment where only the vSnap server is deployed to a new VPC, make sure that the 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 30 - 50 minutes to complete, depending on the vSnap server repository size and number of servers to deploy (bastion host, IBM Spectrum Protect Plus server, and vSnap server)

2. Verify the region that is displayed in the navigation bar, and change the region if necessary. The region specifies where the IBM Spectrum Protect Plus server and vSnap server (all on cloud) or vSnap server only (hybrid) and the 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:

- Option1: Parameters for deploying the IBM Spectrum Protect Plus server and vSnap server (all on cloud) or vSnap server only (hybrid) in a new VPC

- Options 2: Parameters for deploying the IBM Spectrum Protect Plus server and vSnap server (all on cloud) or vSnap server only (hybrid) in an existing VPC

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

OPTION 1: PARAMETERS FOR DEPLOYING IN A NEW VPC (ALL ON CLOUD OR HYBRID)

Instances to deploy:

Parameter label (name)	Default	Description
Instances (Instances)	*Requires input*	The instance to deploy. For an all-on-cloud solution, which deploys the IBM Spectrum Protect Plus and vSnap servers, select **AllOnCloud**. For a hybrid solution, which deploys only the vSnap server, select **Hybrid**.

VPC network configuration:

Parameter label (name)	Default	Description
VPC CIDR (VPCCIDR)	10.0.0.0/16	The range of IPv4 addresses for the VPC.
Public subnet CIDR (PublicSubnetCIDR)	10.0.0.0/24	The CIDR block for a public subnet located in the Availability Zone.
Private subnet CIDR (PrivateSubnetCIDR)	10.0.1.0/24	The CIDR block for a private subnet located in the Availability Zone.
Allowed External Access CIDR (**RemoteAccessCIDR**)	*Requires input*	The CIDR block that allows external SSH access to the bastion host. The value is similar to the following example: 192.0.2.0/24. For increased security, set this value to a trusted CIDR block. For example, you might want to restrict access so that only your corporate network can access the bastion host.

aws

EC2 general configuration:

Parameter label (name)	Default	Description
Key pair name (KeyPairName)	*Requires input*	A public and private key pair that will be used to connect securely to your IBM Spectrum Protect Plus server and vSnap server instances. This is the key pair you created in your preferred region, as described in Technical requirements.
Time zone (TimeZone)	US/Eastern	The time zone where the IBM Spectrum Protect Plus server and vSnap server instances are located.
Availability Zone (AvailabilityZone)	*Requires input*	The Availability Zone to use for the subnets in the VPC.

EC2 IBM Spectrum Protect Plus server configuration:

Parameter label (name)	Default	Description
IBM Spectrum Protect Plus user (SppUser)	administrator	The user name for the IBM Spectrum Protect Plus application. This parameter is used only for an all on cloud configuration. This parameter is ignored for a hybrid configuration because the VPC cannot communicate with the on-premises IBM Spectrum Protect Plus server to register the bucket that is on AWS. The connection from the VPC to the IBM Spectrum Protect Plus server must be configured after deployment. This value cannot be blank, admin, test, or root. The user name can have a maximum of 32 characters.
IBM Spectrum Protect Plus password (SppPassword)	*Requires input*	The user password for the IBM Spectrum Protect Plus application. The password cannot be blank or contain a back quote (`). This parameter is used only for an all-on-cloud configuration. This parameter is ignored for a hybrid configuration.
Confirm IBM Spectrum Protect Plus password (ConfirmSppPassword)	*Requires input*	Confirm the password for the IBM Spectrum Protect Plus application user.

EC2 vSnap server configuration:

Parameter label (name)	Default	Description
vSnap repository size (vSnapRepositorySize)	10000	The repository size in GiB. Enter a size value in the range 500 - 100,000 GiB (100 TiB).
Disk type in vSnap pool (vSnapDiskType)	sc1	The EBS volume type for each disk in the vSnap pool. The options are: General Purpose SSD (gp2), Throughput Optimized HDD (st1), and Cold HDD (sc1).
Deduplication (Deduplication)	Disable	This value permanently enables or disables data deduplication across the vSnap repository.
EC2 Snapshots (EC2snapshots)	Enable*	This value enables the EC2 snapshots feature on IBM Spectrum Protect Plus server.
Instance type (Instance Type)	r5.xlarge	The vSnap server EC2 instance type.
vSnap server user (vSnapUser)	admin	The user name for the vSnap server application. This value cannot be serveradmin, blank, or root. User names must start with a letter or an underscore, followed by 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: (?!^root$)^[a-zA-Z_]([a-zA-Z0-9_-]{0,31}\|[a-zA-z0-9_-]{0,30}\\$)$ A user name can have a maximum of 32 characters.
vSnap server password (vSnapPassword)	*Requires input*	The user password for the vSnap server application. The password must consist of ASCII characters (with the exception of whitespace character signs) and must be at least 8 characters long.
Confirm vSnap server password (ConfirmvSnapPassword)	*Requires input*	Confirm the password for the vSnap server application user.

* If EC2 Snapshots is enabled, a new IAM user with a role that is restricted to EC2 functions is created. The access key and secret key for the new IAM user are used to register the AWS account with the IBM Spectrum Protect Plus server.

An SLA policy that defines the options for EC2 snapshots, such as snapshot frequency and retention, is created. This policy is named AWS_policy_snapshot. You can assign EC2 instances to this policy to start storing snapshots.

S3 bucket configuration:

Parameter label (name)	Default	Description
S3 storage bucket (`S3BucketName`)	`replace-with-bucket-name` *	To copy snapshots from the vSnap server to an S3 bucket, specify the name of the bucket. If the bucket does not exist, it is created during the deployment. This parameter is used only for an all-on-cloud configuration. This parameter is ignored for a hybrid configuration because the VPC cannot communicate with the on-premises IBM Spectrum Protect Plus server to register the bucket that is on AWS. The connection from the VPC to the IBM Spectrum Protect Plus server must be configured after deployment. For the AWS rules for naming buckets, see Bucket Restrictions and Limitations.

* If an S3 bucket is specified, snapshots will be copied from the vSnap server to that bucket for a further level of data protection.

To register the bucket in the IBM Spectrum Protect Plus server, the deployment creates a IAM user with restricted roles to access the bucket. The access key and secret key of the new IAM user are used to register the S3 bucket with the IBM Spectrum Protect Plus server.

An SLA policy that defines the S3 bucket as a copy target is created. This policy is named AWS_policy. You can assign database resources to this policy to ensure that backup snapshots of the resources are copied to the S3 bucket.

OPTION 2: PARAMETERS FOR DEPLOYING IN AN EXISTING VPC (ALL ON CLOUD OR HYBRID)

Instances to deploy:

Parameter label (name)	Default	Description
Instances (Instances)	*Requires input*	The instance to deploy. For an all-on-cloud solution, which deploys the IBM Spectrum Protect Plus and vSnap servers, select **AllOnCloud**. For a hybrid solution, which deploys only the vSnap server, select **Hybrid**.

VPC network configuration:

Parameter label (name)	Default	Description
Existing VPC ID (VPCID)	*Requires input*	The ID that is used to deploy the Spectrum Protect Plus server and vSnap server in an existing VPC.
VPC private subnet ID (PrivateSubnetID)	*Requires input*	The ID of an existing private subnet in the VPC.
Bastion host IP (BastionIP)	10.0.0.0	The private IP address for the bastion host. This IP is used to allow SSH (port 22) connection to the IBM Spectrum Protect Plus and vSnap servers.

EC2 general configuration:

Parameter label (name)	Default	Description
Key pair name (KeyPairName)	*Requires input*	A public and private key pair that will be used to connect securely to your IBM Spectrum Protect Plus server and vSnap server instances. This is the key pair you created in your preferred region, as described in Technical requirements.
Time zone (TimeZone)	US/Eastern	The time zone where the IBM Spectrum Protect Plus server and vSnap server instances are located.

aws

EC2 IBM Spectrum Protect Plus server configuration:

Parameter label (name)	Default	Description
IBM Spectrum Protect Plus user (`SppUser`)	administrator	The user name for the IBM Spectrum Protect Plus application. For an all-on-cloud configuration, provide a user name. For a hybrid configuration, provide the user name for the IBM Spectrum Protect Plus application that is on premises. This value cannot be blank, admin, test, or root. The user name can have a maximum of 32 characters.
IBM Spectrum Protect Plus password (`SppPassword`)	*Requires input*	The user password for the IBM Spectrum Protect Plus application. The password cannot be blank or contain a back quote (`` ` ``).
Confirm IBM Spectrum Protect Plus password (`ConfirmSppPassword`)	*Requires input*	Confirm the password for the IBM Spectrum Protect Plus application user.
IBM Spectrum Protect Plus IP (`IBMSpectrumProtectPlusIP`)	*1.1.1.1*	The IP address of an existing IBM Spectrum Protect Plus server. This field is ignored if **AllOnCloud** is selected as the instance to deploy.

EC2 vSnap server configuration:

Parameter label (name)	Default	Description
vSnap repository size (vSnapRepositorySize)	10000	The repository size in GiB. Enter a size value in the range 500 - 100,000 GiB (100 TiB).
Disk type in vSnap pool (`vSnapDiskType`)	sc1	The EBS volume type for each disk in the vSnap pool. The options are: General Purpose SSD (gp2), Throughput Optimized HDD (st1), and Cold HDD (sc1).
Deduplication (`Deduplication`)	Disable	This value permanently enables or disables data deduplication across the vSnap repository.
EC2 Snapshots (**EC2snapshots**)	Enable *	This value enables the EC2 snapshots feature on IBM Spectrum Protect Plus server.
Instance type (Instance Type)	r5.xlarge	The vSnap server EC2 instance type.
vSnap server user (vSnapUser)	admin	The user name for the vSnap server application. This value cannot be serveradmin, blank, or root. User names must start with a letter or an underscore, followed by letters, digits, underscores, or dashes, and can end with a dollar sign. The regular expression terms that are used to validate the

Parameter label (name)	Default	Description
		user name are: (?!^root$)^[a-zA-Z_]([a-zA-Z0-9_-]{0,31}\|[a-zA-z0-9_-]{0,30}\\$)$ A user name can have a maximum of 32 characters.
vSnap server password (`vSnapPassword`)	*Requires input*	The user password for the vSnap server application. The password must consist of ASCII characters (with the exception of whitespace character signs) and must be at least 8 characters long.
Confirm vSnap server password (`ConfirmvSnapPassword`)	*Requires input*	Confirm the password for the vSnap server application user.

* If EC2 Snapshots is enabled, a new IAM user with a role that is restricted to EC2 functions is created. The access key and secret key for the new IAM user are used to register the AWS account with the IBM Spectrum Protect Plus server.

An SLA policy that defines the options for EC2 snapshots, such as snapshot frequency and retention, is created. This policy is named AWS_policy_snapshot. You can assign EC2 instances to this policy to start storing snapshots.

S3 bucket configuration:

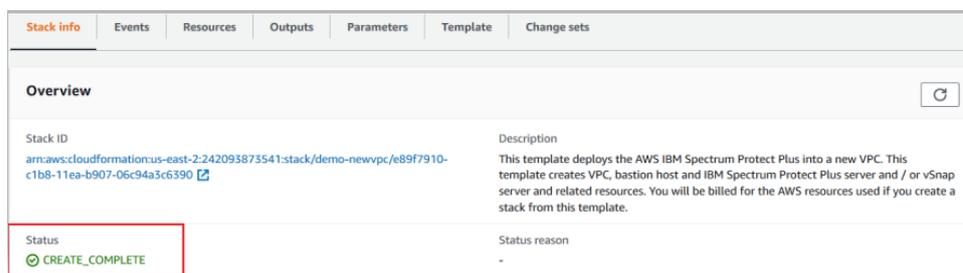| Parameter label (name)	Default	Description
S3 storage bucket (`S3BucketName`)	replace-with-bucket-name *	To copy snapshots from the vSnap server to an S3 bucket, specify the name of the bucket. If the bucket does not exist, it is created during the deployment. For the AWS rules for naming buckets, see Bucket Restrictions and Limitations.

* If an S3 bucket is specified, snapshots will be copied from the vSnap server to that bucket for a further level of data protection.

To register the bucket in the IBM Spectrum Protect Plus server, the deployment creates a IAM user with restricted roles to access the bucket. The access key and secret key of the new IAM user are used to register the S3 bucket with the IBM Spectrum Protect Plus server.

An SLA policy that defines the S3 bucket as a copy target is created. This policy is named AWS_policy. You can assign database resources to this policy to ensure that backup snapshots of the resources are copied to the S3 bucket.

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 checkbox to acknowledge that the template will create an IAM resource.
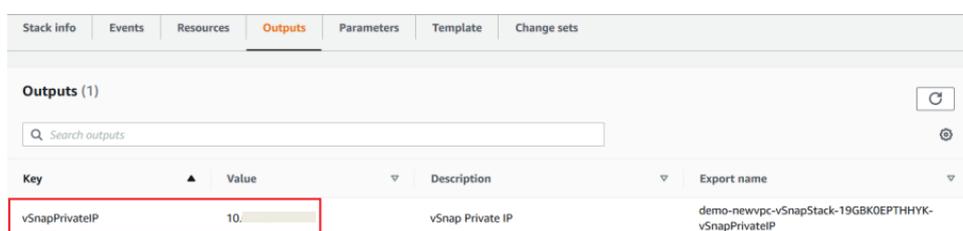
7. Click **Create** to deploy the stack.

aws

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.

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

Step 4. Connect to the IBM Spectrum Protect Plus web application

This step is required only if you are deploying the IBM Spectrum Protect Plus server to a VPC for an all-on-cloud solution. If you are deploying only a vSnap server for a hybrid solution, skip this step.

Use one of the following options to connect the IBM Spectrum Protect Plus application by using a browser in an all-on-cloud environment:

- Configure a VPN connection between your organization and the AWS VPC. You can use the AWS site-to-site VPN or any VPN connection software. When the VPN is running, you can access the IBM Spectrum Protect Plus web application using a browser any computer in your organization. For information about the AWS site-to-site feature, see What is AWS Site-to-Site VPN?.

- Install a Windows bastion server with a public IP address on the VPC and use a Remote Desktop Protocol (RDP) connection to open a browser on the bastion server to connect to the IBM Spectrum Protect Plus application. For information about RDP, see Remote Desktop Gateway on AWS.

- Configure SSH tunneling by using a Linux bastion server as described in Appendix B.

Step 5. Test the deployment

The steps for testing the deployment depend on the type of deployment, as shown in the following table:

| Deployment type	Description	Instructions
Hybrid: Existing IBM Spectrum Protect Plus server on premises, vSnap server deployed in a new AWS VPC	In this scenario, 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.	See Option 1 (hybrid): Testing an on-premises IBM Spectrum Protect Plus server with a vSnap server in a new AWS VPC
Hybrid: Existing IBM Spectrum Protect Plus server on premises, vSnap server deployed in an existing AWS VPC	In these scenarios, after your vSnap server and repository are configured, the CloudFormation template registers the new vSnap server in the IBM Spectrum Protect Plus server.

A new site that is named Cloud is created and the vSnap server is registered automatically as part of this site. | See Option 2: Testing all other all-on-cloud and hybrid deployment types |
| **All On Cloud: IBM Spectrum Protect Plus server and vSnap server deployed in a new AWS VPC** | | |
| **All On Cloud: IBM Spectrum Protect Plus server and vSnap server deployed in an existing AWS VPC** | | |

aws

OPTION 1 (HYBRID): TESTING AN ON-PREMISES IBM SPECTRUM PROTECT PLUS SERVER WITH A VSNAP SERVER IN A NEW AWS VPC

To confirm that communication is established and to register the vSnap server with the on-premises IBM Spectrum Protect Plus 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.
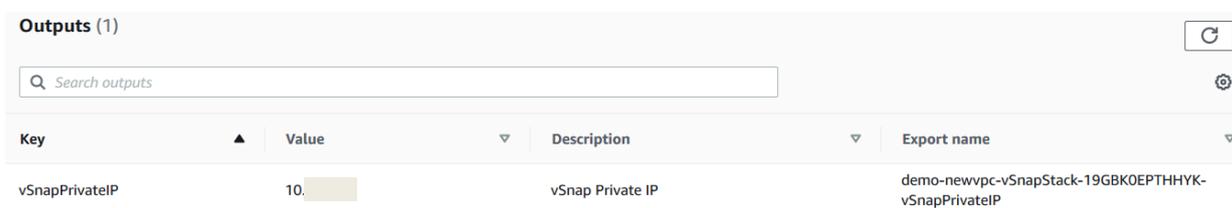
Outputs (1)				
Q *Search outputs*				
Key ▲	Value ▽	Description ▽	Export name ▽
vSnapPrivateIP	10.	vSnap Private IP	demo-newvpc-vSnapStack-19GBK0EPTHHYK-vSnapPrivateIP

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 supported browsers, go to the system requirements overview page and click the version of IBM Spectrum Protect Plus that you are using. Then, click **System requirements: IBM Spectrum Protect Plus V10.1.6** and go to the **Browser support** section of the requirements.

4. In the IBM Spectrum Protect Plus 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:

Disk Storage

		Name	Hostname/IP	Site	Version	Status/Capacity	VADP Proxy	
🗑 ✎ ⚙		172.	172.	Cloud	10.1.6-1735	390 GB/9.8 TB 4% ▮		⋮

OPTION 2: TESTING ALL OTHER ALL-ON-CLOUD AND HYBRID DEPLOYMENT TYPES

To ensure that the vSnap server was successfully registered with the IBM Spectrum Protect Plus server, 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 supported browsers, go to the system requirements overview page and click the version of IBM Spectrum Protect Plus that you are using. Then, click **System requirements** and go to the **Browser support** section.

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

		Name	Hostname/IP	Site	Version	Status/Capacity	VADP Proxy	
🗑 ✎ ⚙		172.	172.	Cloud	10.1.6-1735	390 GB/9.8 TB 4% ▮		⋮

aws

Step 6. Update the SSH connection to the bastion host (optional)

In most cases, the IBM Spectrum Protect Plus user interface is used to manage the IBM Spectrum Protect Plus server and the vSnap server and that communication is managed by the REST API. However, if you want to connect to the servers from an IP address outside of the VPC, for example, to download the .run file to upgrade the vSnap server to a later version, the SSH connection can be enabled by using a bastion host.

If you are deploying in a new VPC, a new bastion host is created. However, you must provide the external IP range that will be used to access the bastion host from outside of the VPC in the CloudFormation template. If you are deploying to an existing VPC, you must provide the IP address for the bastion host in the CloudFormation template.
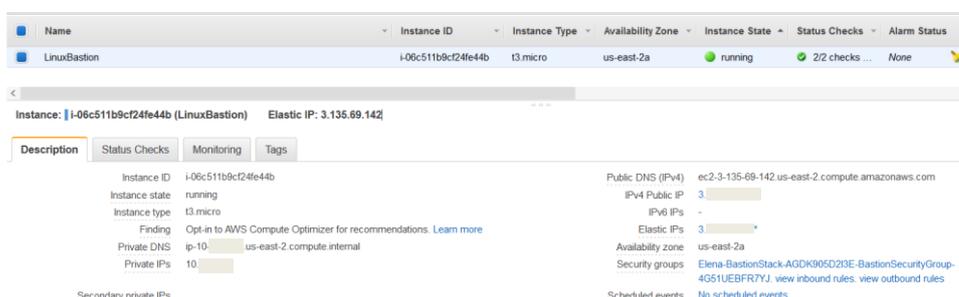
The bastion host is the only server in the VPC that has public access.
If you are deploying in an existing VPC, the IBM Spectrum Protect Plus server and the vSnap server have access to the bastion host through their security groups.

In some situations, you might want to update the security group for the bastion host. For example, if the incorrect IP address or CIDR block range was provided for the bastion host in the CloudFormation template and the bastion is not available or you want to increase or decrease the number of IP addresses that can access the bastion host.

To update the bastion security group, complete the following steps:

1. Open the AWS EC2 console and navigate to the Instance page.

2. Look for a running instance named **LinuxBastion**.

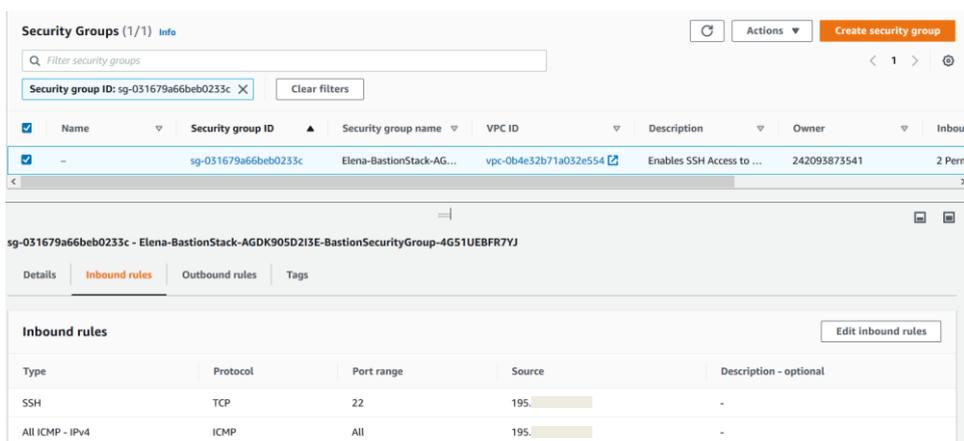3. In the description on the instance, select the security group that is associated with the instance.

4. On the **Inbound rules** tab, click **Edit inbound rules**.

5. Click **Add rule** to add a new inbound rule for SSH and specify the CIDR from which you want to provide SSH access to the bastion host, and then click **Save rules**.
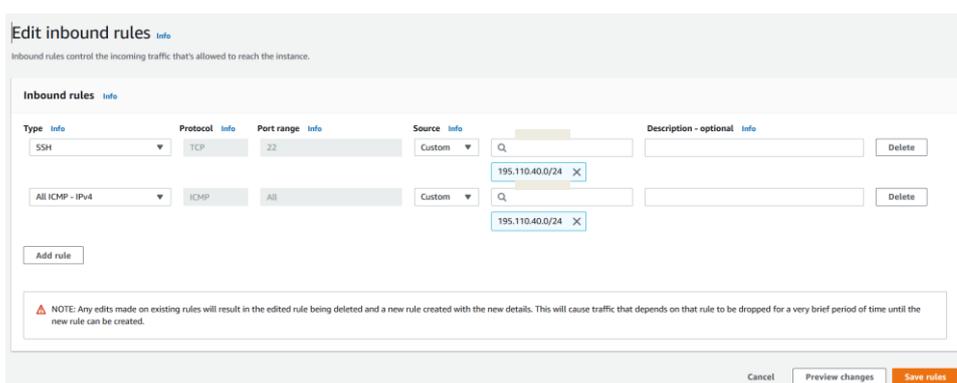
6. To enable an SSH connection to the IBM Spectrum Protect Plus server and vSnap server instances, add your key pair file that was chosen during deployment to the ssh-agent by providing the path of the key file as an argument to ssh-add.

First, activate the ssh-agent:`

```
#eval 'ssh-agent'
```

Then, add your key to agent to store your credentials locally and temporarily:

```
#ssh-add /path_to/key_pair_file
```

where:

- The parameter *key_pair_file* is a .pem file that contains the public and private keys that are required to connect to the bastion host and the IBM Spectrum Protect Plus server and vSnap server instance.

7. Issue the following commands to enable SSH connection to the bastion host and then to the IBM Spectrum Protect Plus server and vSnap server instance:

```
ssh -A ec2_user@bastion_host_ip_address
ssh -A serveradmin@server_ip_address
```

where:

- The parameter *ec2_user* is a default AWS user to login into EC2 servers.

- The parameter *bastion_host_ip_address* is the IP address for the bastion host.

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

- The parameter *server_ip_address* is the IP address for the IBM Spectrum Protect Plus server or vSnap server instance.

Tip To find the IP address for the IBM Spectrum Protect Plus or vSnap server instance, select the relevant stack for the instance and then click the **Outputs** tab. Each server has a unique IP address.

For the IBM Spectrum Protect Plus server IP address, see the SPPPrivateIP key.
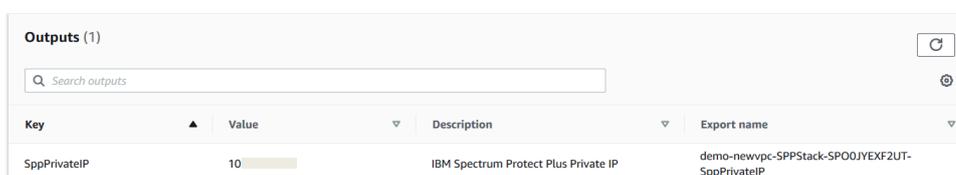
Key		Value		Description		Export name	
SppPrivateIP		10		IBM Spectrum Protect Plus Private IP		demo-newvpc-SPPStack-SPO0JYEXF2UT-SppPrivateIP	

Outputs (1)

Q Search outputs

aws

For the vSnap server IP address, see the key vSnapPrivateIP.

Outputs (1)

Search outputs

Key	▲	Value	▽	Description	▽	Export name	▽
vSnapPrivateIP		10.		vSnap Private IP		demo-newvpc-vSnapStack-19GBK0EPTHHYK-vSnapPrivateIP	

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 IBM Spectrum Protect Plus server and vSnap server instances as part of this solution are 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 the IBM Spectrum Protect Plus server and vSnap server:

- 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 bastion host only.

- 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 copy 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

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

How can a resolve this issue?

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 IBM Spectrum Protect Plus server and vSnap server instances are left running so that you can troubleshoot the issue. Review the log file **/root/SPP/bin/aws/flow_manager/deploy.log** for additional information.

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

Or

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

Or

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

How can I resolve this issue?

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, choose **Create Case > Service Limit Increase > EC2 instances**, and then complete the fields in the form.

aws

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)

How can I resolve this issue?

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

How can I resolve this issue?

A. Stack creation might fail for many reasons when installing and configuring the servers.

All IBM Spectrum Protect Plus server and vSnap server configuration logs are available in AWS CloudWatch.

aws

To review the logs in AWS CloudWatch:

1. Select the stack for the IBM Spectrum Protect Plus server or vSnap server instance in the AWS CloudFormation console, and then click the **Resources** tab.

2. Find the instance in the Logical ID column and copy the ID. The following figure shows the ID for the vSnap server.

Resources (20)

	Logical ID ▼	Physical ID ▼	Type ▼
		7add-11e9-baf2-12ece74fd46e /vSnapWaitHandle	WaitCondition
	vSnapSecurityGroup	sg-0a35032468fd06fdc ☑	AWS::EC2::SecurityGrou p
	vSnapInstance	i-0ec32e29025bffc4f ☑	AWS::EC2::Instance

3. Open the AWS CloudWatch console, and click **Log groups** in the navigation pane.

4. Paste the instance ID in the **Filter** field.

Billing
Logs
| **Log groups**
Insights
Metrics
Events

Create Metric Filter   Actions ▾

Filter: i-0e2c26e3dfad6e7fa   ×

Log Groups

○   i-0e2c26e3dfad6e7fa/10.0.1.145

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

Log streams (2)

Filter log streams

	Log stream ▽	Last event time
☐	cloud_init_output.log	7/12/2020, 3:06:14 PM
☐	deploy.log	7/12/2020, 2:56:50 PM

For additional details about the failure, review the deploy.log file.

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

13 May 2019 09:39:42	PrivateSubnet	⊗ 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)

How can I resolve this issue?

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 Subnets.

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

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

How can I resolve this issue?

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.

aws

Q. A CREATE_FAILED error occurred for the operation to create an IAM user:

2019-12-25 14:33:14 UTC+0200	CreateS3User	⊗ CREATE_FAILED	Failed to create resource. See the details in CloudWatch Log Stream: 2019/12 /25/[$LATEST]046d6dc32de54de99f2d4aca2dac56 07

How can I resolve this issue?

A: When an S3 bucket name is provided in the CloudFormation template, a dedicated IAM user is created during deployment.

If the user name is in use, the deployment process makes 10 attempts to create the user by appending the numbers 1 – 10 to the user name: that is, SPP_user_for_s3_1 to SPP_user_for_s3_10. If all 10 IAM user names exist, the deployment fails.

To resolve the error, use IAM to delete or rename the users as needed for your AWS environment.

The following is an example error from the createS3User Lambda logs:

[INFO] 2019-12-25T12:33:13.46Z 800a7c05-ba67-4363-b61f-c5dad898d66a Failed to create IAM user for S3: An error occurred (EntityAlreadyExists) when calling the CreateUser operation: User with name SPP_user_for_s3_1 already exists.

Appendix A: Expand the vSnap server capacity post deployment procedure

For IBM Spectrum Protect Plus V10.1.5 and later, you can order new EBS volumes, attach the volumes to an existing vSnap server on AWS, and expand an existing vSnap pool.

The IBM Spectrum Protect Plus server can be on premises or on AWS.

To increase the capacity of a vSnap server, complete the following steps:

1. Stop the vSnap server EC2 instance.

2. Create new EBS volumes by following the instructions in <u>Creating an Amazon EBS Volume.</u> Create the volumes in the same Availability Zone as the vSnap server EC2 instance.

3. Attach the new volumes to an existing vSnap server by following the instructions in <u>Creating an Amazon EBS Volume.</u>

4. Power on the vSnap server.

5. Start the IBM Spectrum Protect Plus server GUI.

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

7. Find the IP address for the vSnap server and click the actions menu ⋮ and then click **Rescan.** The vSnap server scans the system for new volumes.
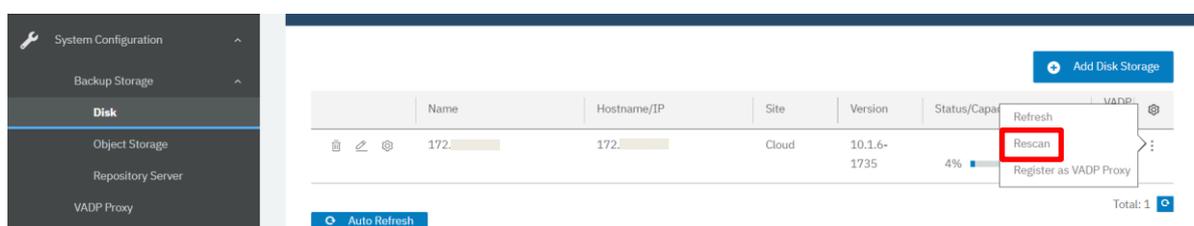
8. Click the tools icon ⚙ for the vSnap server. Click the Disks tab and select the volumes that you want to add, and click **Save**.

| Options | Disks | Partners | Active Directory | Advanced Options |

Add New Disks to Backup Storage
Select one or more unused disks to add to the storage pool

Select	Disk	Size	Vendor	Model
☐	/dev/nvme3n1	500 GiB	Unknown	Amazon Elastic Block Store

The new capacity is added to the vSnap pool.

aws

Appendix B: Access the IBM Spectrum Protect Plus web application using SSH tunneling

Configure SSH tunneling through a bastion host to get to the IBM Spectrum Protect Plus web application.

If you have an existing VPN connection configures, SSH tunneling is not required because you should have direct access to the IBM Spectrum Protect Plus web application.

SSH port forwarding is a mechanism ~~in SSH~~ for tunneling application ports from the client machine to the server machine, or vice versa. It can be used for adding encryption to legacy applications, going through firewalls, and some system administrators and IT professionals use it for opening backdoors into the internal network from their home machines.

The following steps use the SSH -D option, which specifies a local dynamic application-level port forwarding. This option works by allocating a socket to listen to a local port, optionally bound to the specified *bind_address* (a bastion host public IP address). Whenever a connection is made to this port, the connection is forwarded over the secure channel, and the application protocol is then used to determine where to connect to from the remote machine. Currently, the SOCKS5 protocol is supported, and SSH acts as a SOCKS server.

To access the IBM Spectrum Protect Plus web application using SSH tunneling, complete the following steps:

1. Record the IBM Spectrum Protect Plus server private IP address and bastion host server public address. (To find the IP address, navigate to the Stacks page of the AWS CloudFormation console. Select the stack for the sever instance and then click the **Outputs** tab.)

2. Make sure that you have a regular SSH access to bastion host using a PEM key file by running the following command:
   ```
   # ssh –i pem_key_file ec2-user@bastion_public_ip
   ```

3. Configure SSH dynamic port forwarding by running the following command:
   ```
   # ssh –i pem_key_file –D 1080 ec2-user@bastion-public-ip
   ```



```
$ ssh -i vered_key_TLV_virginia.pem -D 1080 ec2-user@52.44.221.84
Last login: Tue Feb 11 10:02:06 2020 from nesher17.haifa.il.ibm.com

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
17 package(s) needed for security, out of 33 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-23 ~]$
```
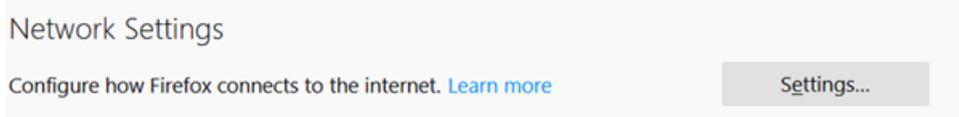
aws

Note that 1080 is the default port used for port forwarding. You can change the port number to any available port in your network.

4. Open a web browser. In this example, the browser is Firefox, you can use any browser that supports proxy configuration.
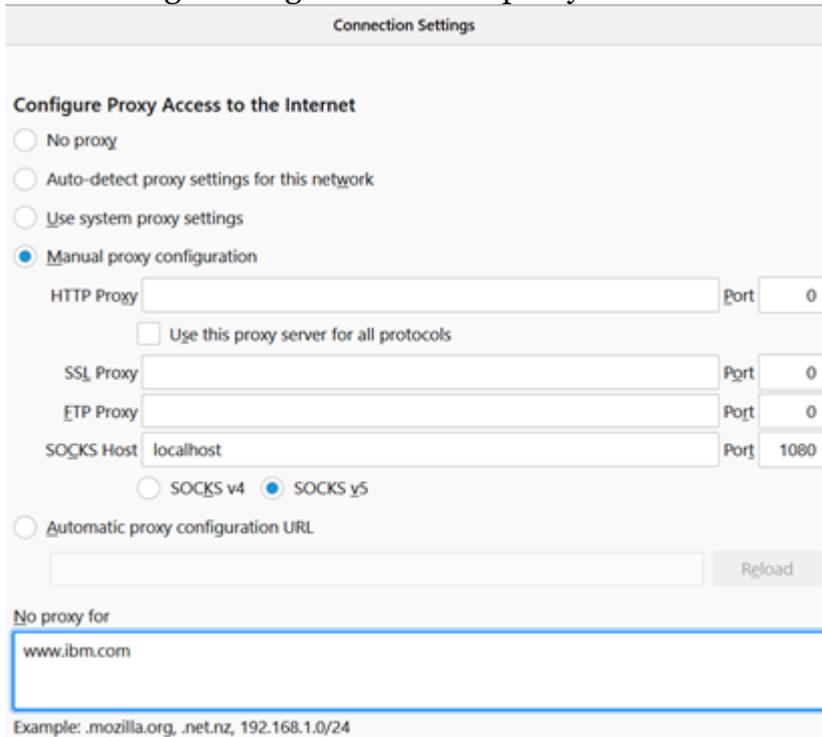
5. Find **Options** in your browser:
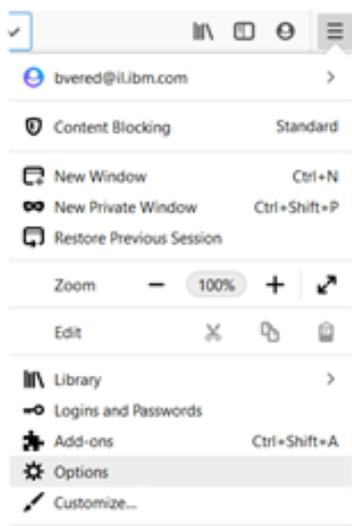
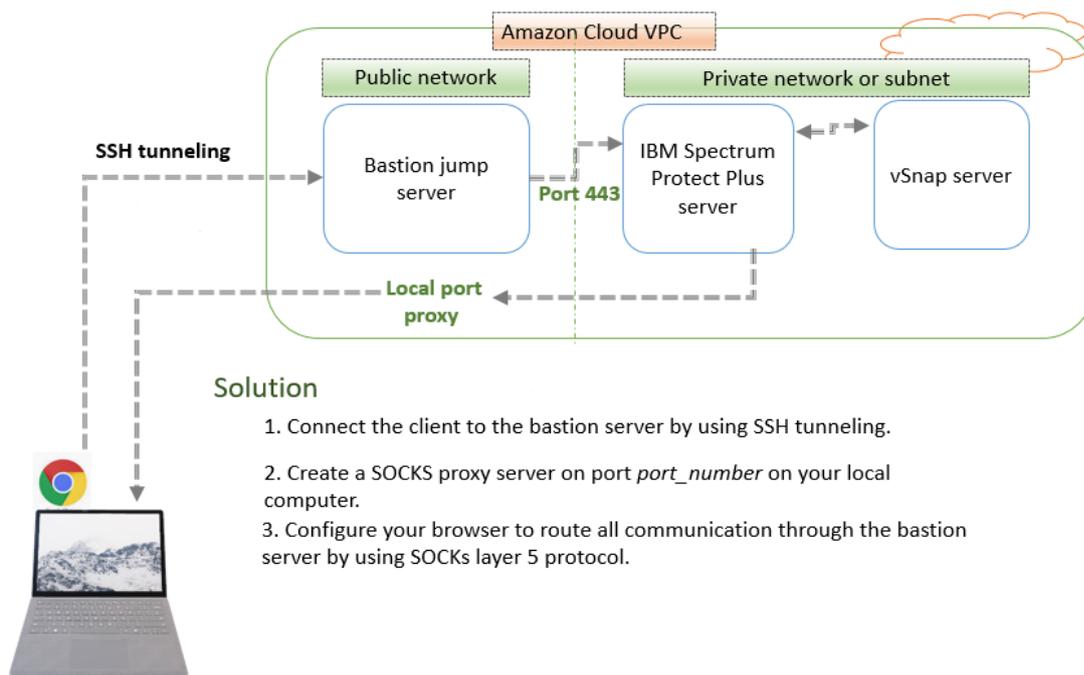6. Navigate to **Network Settings** and click **Settings**:

7. Configure the network settings to enable the proxy.

a. Click **Manual proxy connection**.

b. In the **SOCKS Host** field, enter localhost and enter port 1080 (or the port number that you chose if other than 1080).

c. In the **No proxy for** field, you can add internal sites for your organization that should not go through bastion as a proxy server.

Connection Settings

Configure Proxy Access to the Internet
- ○ No proxy
- ○ Auto-detect proxy settings for this network
- ○ Use system proxy settings
- ● Manual proxy configuration

HTTP Proxy		Port	0
	☐ Use this proxy server for all protocols		
SSL Proxy		Port	0
FTP Proxy		Port	0
SOCKS Host	localhost	Port	1080
	○ SOCKS v4 ● SOCKS v5		

- ○ Automatic proxy configuration URL

              [Reload]

No proxy for

> www.ibm.com

Example: .mozilla.org, .net.nz, 192.168.1.0/24

d. Click **OK**. The networking settings are set and active.

8. Open a new web page and connect directly to the IBM Spectrum Protect Plus private IP address (https://*private_ip_address*). You should be able to access the IBM Spectrum Protect Plus web application directly through bastion proxy server.

Solution

1. Connect the client to the bastion server by using SSH tunneling.

2. Create a SOCKS proxy server on port *port_number* on your local computer.
3. Configure your browser to route all communication through the bastion server by using SOCKs layer 5 protocol.

aws

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**.
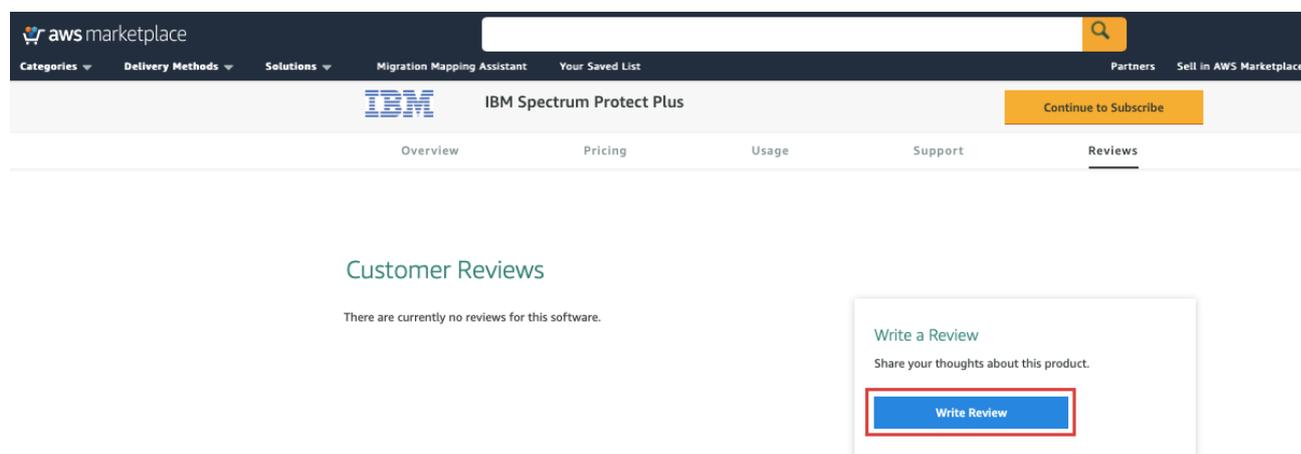
Additional resources

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 product documentation](#)

Document revisions

Date	Change	In sections
July 2020	Initial publication	—