IBM Spectrum Protect Plus on Microsoft Azure 10.1.7

Deployment Guide

Note:

Before you use this information and the product it supports, read the information in “Notices” on page 43.

Second edition (30th April 2021)

This edition applies to version 10, release 1, modification 7 of IBM Spectrum® Protect Plus (product number 5737-F11) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

This publication provides overview, planning, and deployment information for IBM Spectrum Protect Plus on Microsoft Azure.

Who should read this publication

This publication is intended for administrators who are responsible for deploying IBM Spectrum Protect Plus on Microsoft Azure.

In this publication, it is assumed that you have an understanding of IBM Spectrum Protect Plus and familiarity with the Azure services and components described in “Azure services and components” on page 13.

Chapter 1. IBM Spectrum Protect Plus on the Microsoft Azure cloud platform

IBM Spectrum Protect Plus on the Microsoft Azure cloud platform is a data protection solution for users who want to protect one or more databases that are running on Azure.

IBM Spectrum Protect Plus on Azure protects the following databases and file systems that are running on Azure:

- IBM® Db2®
- Microsoft SQL Server
- Microsoft Exchange Server
- Oracle
- MongoDB
- Microsoft 365
- Microsoft Windows Resilient® File System (RefS) and New Technology File System (NTFS)

You can deploy IBM Spectrum Protect Plus on Azure in one of the following configurations:

All-on-cloud environment
In this configuration, both the IBM Spectrum Protect Plus server and the vSnap server are deployed in Azure on an existing or new Virtual Network (VNet).

This option might benefit new IBM Spectrum Protect Plus users who want to protect databases on Azure 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 Azure on an existing or new VNet. The IBM Spectrum Protect Plus server is installed and maintained on premises or another location. This option might benefit existing 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 Azure for additional data protection. For example, you might want to use data that is protected at your on-premises site on Azure for DevOps, quality assurance, testing, and disaster recovery purposes.

Upgrading IBM Spectrum Protect Plus to a later version

The IBM Spectrum Protect Plus on Azure deployment includes IBM Spectrum Protect Plus version 10.1.7. If you want to use the current version of IBM Spectrum Protect Plus, follow the instructions in Updating IBM Spectrum Protect Plus components to complete an upgrade.

VNet deployment options

For both an all-on-cloud or hybrid environment, you can deploy IBM Spectrum Protect Plus to an existing or new VNet.

The deployment is automated by an Azure Resource Manager (ARM) template.

Deploying to an existing VNet

This option provisions the IBM Spectrum Protect Plus server and vSnap server (all on cloud) or only the vSnap server (hybrid) in the existing VNet. To deploy to an existing VNet, you must provide the VNet name and public and private subnet names during deployment. If you are connecting to the VNet by using a Bastion host, you must provide the IP address for the host.

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

Deploying to an existing VNet by using a Bastion host or VPN connection: If you have a virtual private network (VPN) connection to an existing VNet, a Bastion host is not required.

During the deployment of IBM Spectrum Protect Plus on Azure, a default security group that contains a role for the Bastion host is created. You can edit this security group and remove the role for the Bastion host to enable direct Secure Shell (SSH) access to the IBM Spectrum Protect Plus server and vSnap server.

Deploying to a new VNet

This option builds a new Azure environment consisting of the VNet, subnets, network address translation (NAT) gateways, security groups, public status IPs, Bastion host and other infrastructure components, and then deploys the IBM Spectrum Protect Plus server and vSnap server (all on cloud) or only the vSnap server (hybrid) in this new VNet.

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

Architecture

IBM Spectrum Protect Plus on Azure offers two types of configuration sets through an ARM template: all on cloud and hybrid.

All-on-cloud environment

In an all-on-cloud environment, the IBM Spectrum Protect Plus server and the vSnap server are hosted on Azure. 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 Blob object storage.

The following figure shows an all-on-cloud environment.

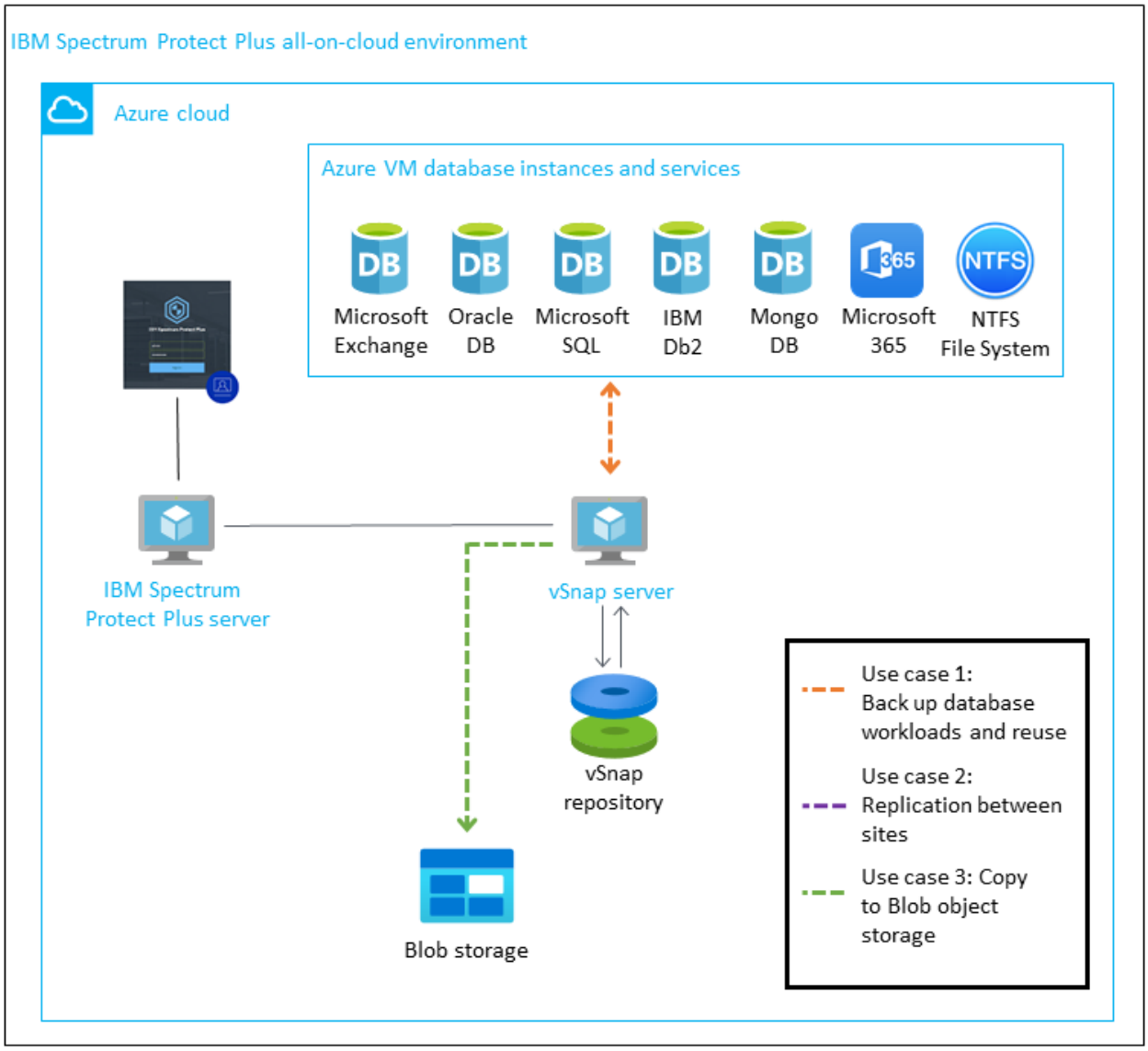


Figure 1. All-on-cloud environment

Components deployed by the ARM template

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

If you are deploying to an existing VNet, 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 VNet, the VNet 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 network security groups to restrict access to only necessary protocols and ports.
- A username and password for the vSnap server authentication.
- A username and password for the IBM Spectrum Protect Plus server authentication.
- A NAT gateway for outbound internet access from private subnets. *
- A static Public IP for NAT usage. *

- A VNet that spans one public and one private subnet. *
- A Linux Bastion host on a public subnet. The Bastion host enables secure shell (SSH) access to the vSnap server. *
- A virtual machine (VM) that is configured with the vSnap server by using the VM type that is recommended by the IBM Spectrum Protect Plus Blueprint.
- The vSnap server VM includes the following items:
  - A 70 GiB premium solid-state drive (SSD) disk volume for the root device
  - A premium SSD disk volume for the cloud cache as defined by the blueprint that corresponds to the vSnap server repository size
  - A dynamic number of disks to support the repository size during deployment. The type of disk is defined in the ARM template.
  - Logs and cache premium SSD disk volumes as defined by the blueprint that correspond to the vSnap server repository size
- A VM that is configured with the IBM Spectrum Protect Plus management server by using the VM module E8s_v4, which is recommended by the blueprint.
- The IBM Spectrum Protect Plus server VM includes the following items for internal use:
  - A 70 GiB premium SSD disk for the root device
  - A 50 Gib premium SSD disk for PostgresSQL
  - A 50 Gib premium SSD disk for MongoDB
  - A 150 Gib premium SSD disk for Lucene indexing

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

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 VNet

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

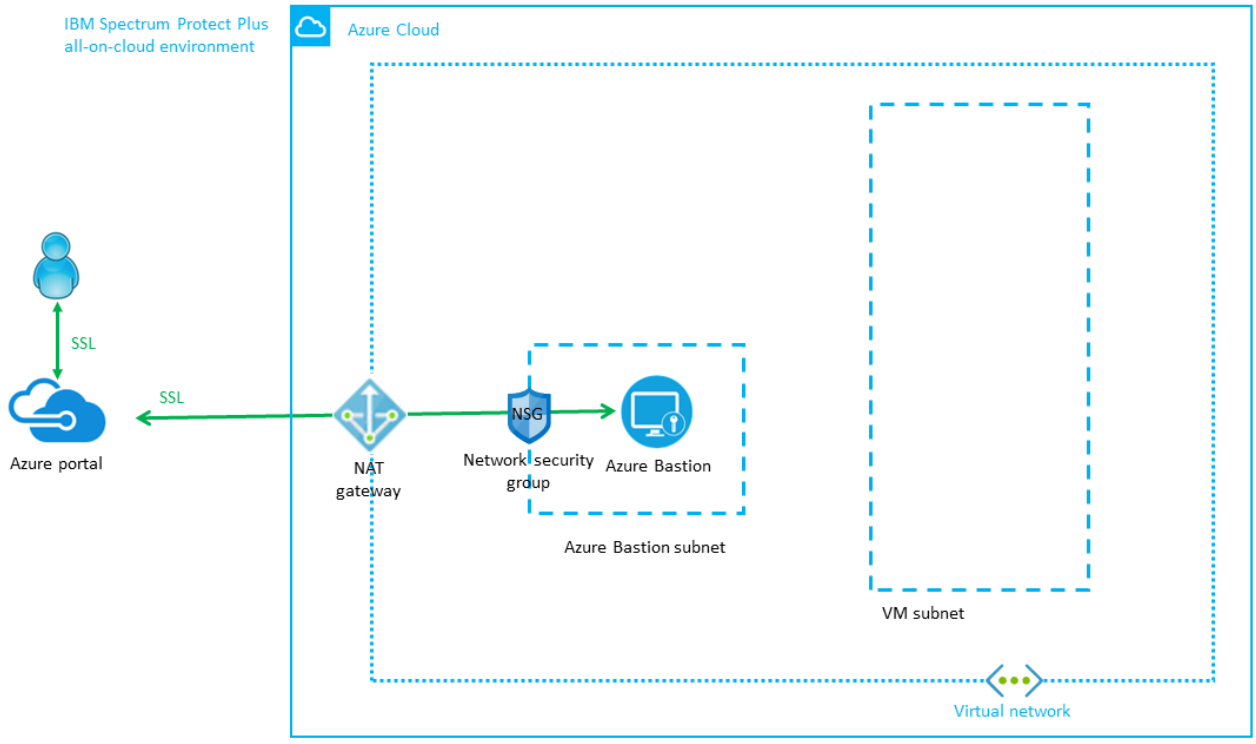


Figure 2. All-on-cloud environment, before deployment to an existing VNet

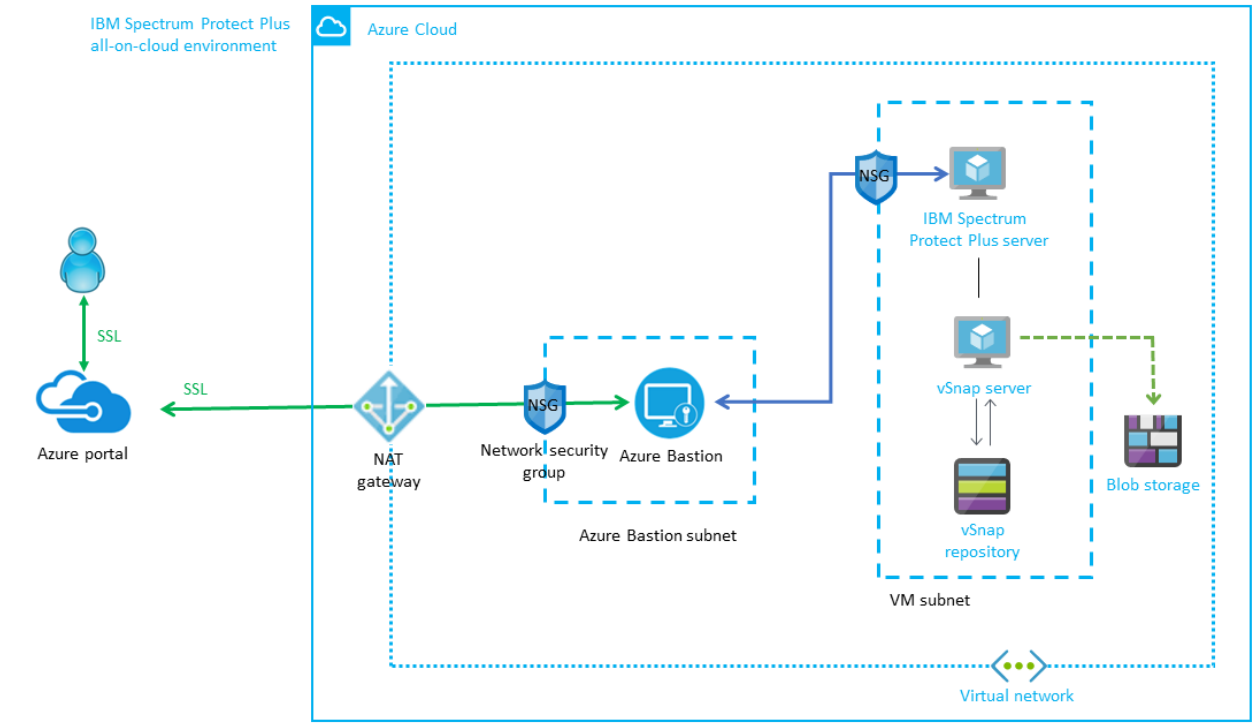


Figure 3. All-on-cloud environment, after deployment to an existing VNet

All On Cloud: Deploying to a New VNet

The following figures illustrate the Azure environment after IBM Spectrum Protect Plus is deployed to a new VNet.

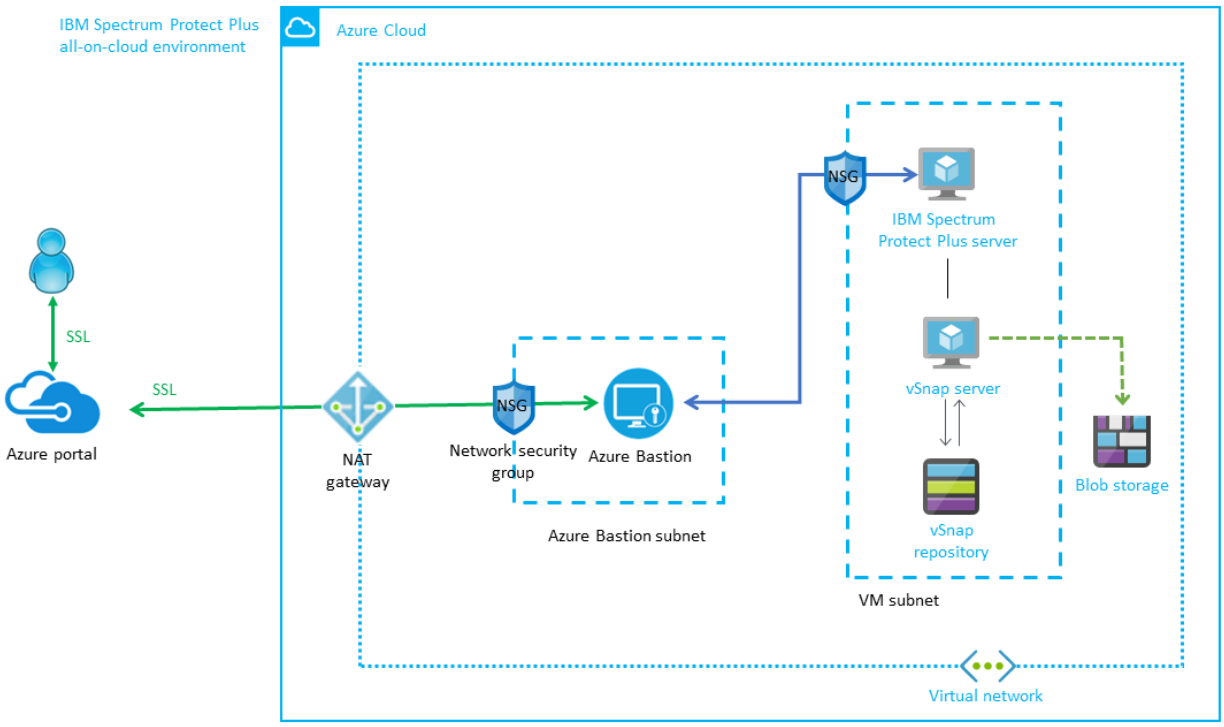


Figure 4. All-on-cloud environment, after deployment to a new VNet

Hybrid deployment

In a hybrid environment, a vSnap server is hosted on Azure and the IBM Spectrum Protect Plus server is on premises or another site. 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 Blob object storage.

As shown in the following figure, you can also have a vSnap server on premises in a hybrid environment. This configuration provides the option of backing up workloads to a vSnap server that is on premises.

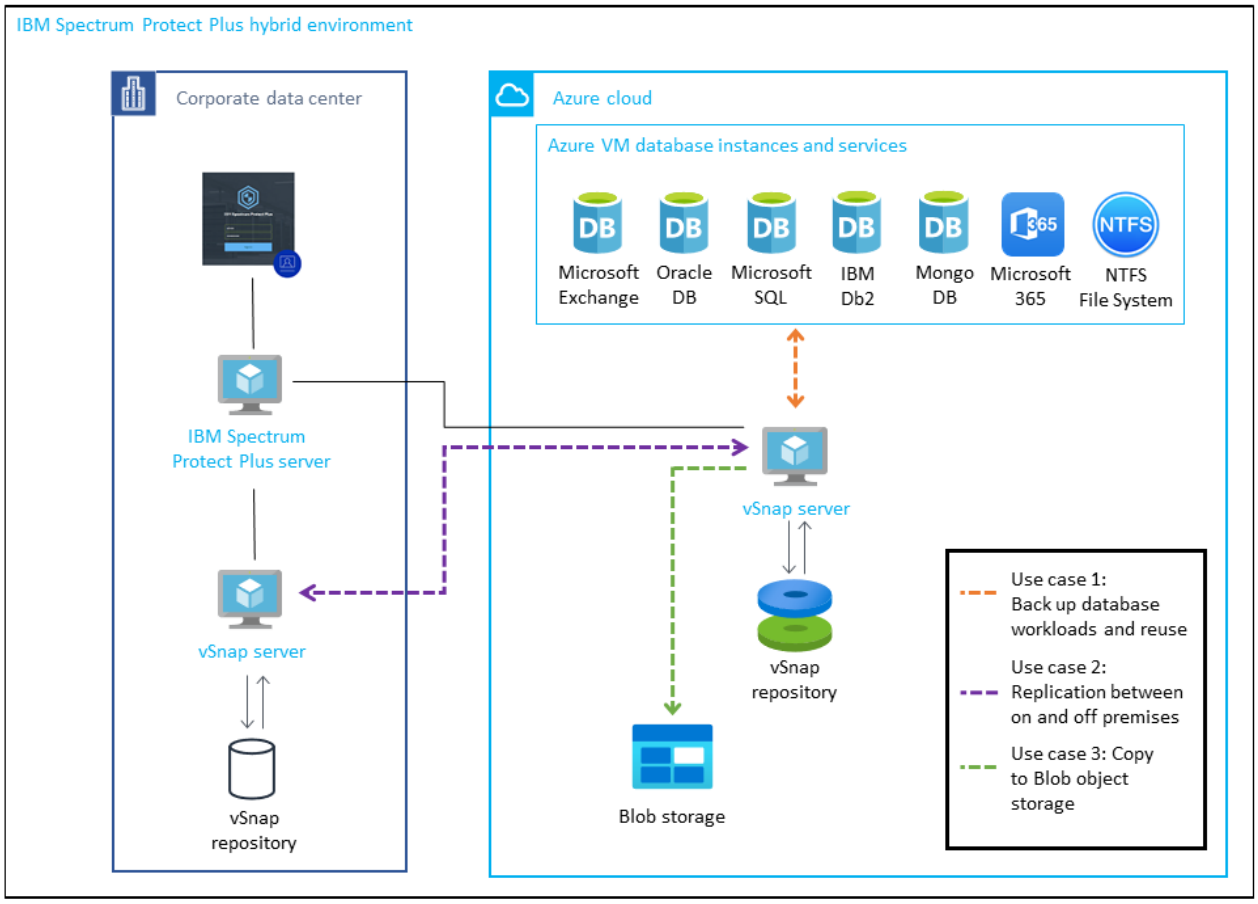


Figure 5. Hybrid environment

Components deployed by the ARM template

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

If you are deploying to an existing VNet, 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 VNet, the VNet 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.
- A network security group to restrict access to only necessary protocols and ports.
- A user name and password for the vSnap server authentication.
- A NAT gateway for outbound internet access from private subnets. *
- A static Public IP for NAT usage. *
- A VNet that spans one public and one private subnet. *
- A Linux Bastion host on a public subnet. The Bastion host enables secure shell (SSH) access to the vSnap server. *
- A virtual machine (VM) that is configured with the vSnap server by using the VM type that is recommended by the blueprint.
- The vSnap server VM includes the following items:
  - A 70 GiB premium solid-state drive (SSD) disk volume for the root device

- A premium SSD disk volume for the cloud cache as defined by the blueprint that corresponds to the vSnap server repository size
- A dynamic number of disks to support the repository size during deployment. The type of disk is defined in the ARM template.
- Logs and cache premium SSD disk volumes as defined by the blueprint that correspond to the vSnap server repository size

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

Establishing a VPN connection in a hybrid environment

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

Attention: If you do not establish this communication, the installation and configuration of the vSnap server on Azure fails.

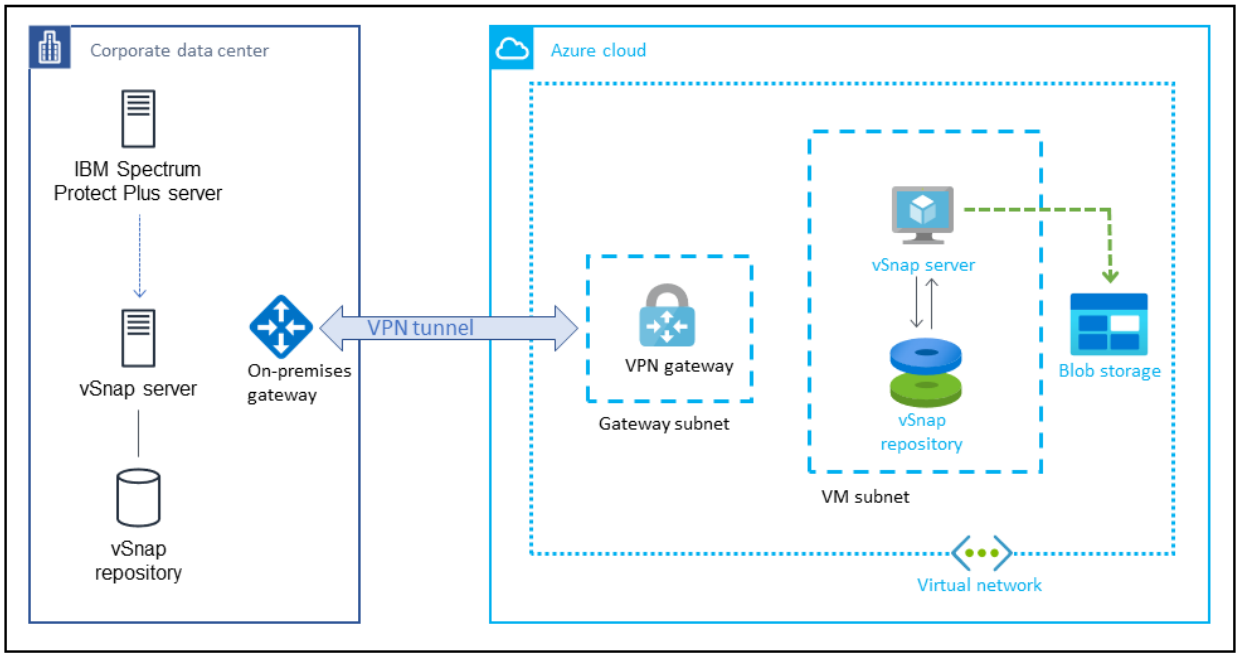


Figure 6. Communication between the vSnap server on Azure and the IBM Spectrum Protect Plus server on premises

If you are deploying the vSnap server in an existing VNet, ensure that you have the bidirectional VPN connection established between the VNet and the IBM Spectrum Protect Plus server before you set up and configure the Azure ARM 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 Azure and enables your on-premises IBM Spectrum Protect Plus server to recognize the vSnap server.

If you are deploying the vSnap server in an existing VNet, configure a bidirectional VPN connection between the VNet 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 “Testing an on-premises IBM Spectrum Protect Plus server with a vSnap server in a new Azure VNet” on page 31.

Hybrid: Deploying to an existing VNet

The following figures illustrate the on-premises and Azure environment before and after IBM Spectrum Protect Plus is deployed to an existing VNet.

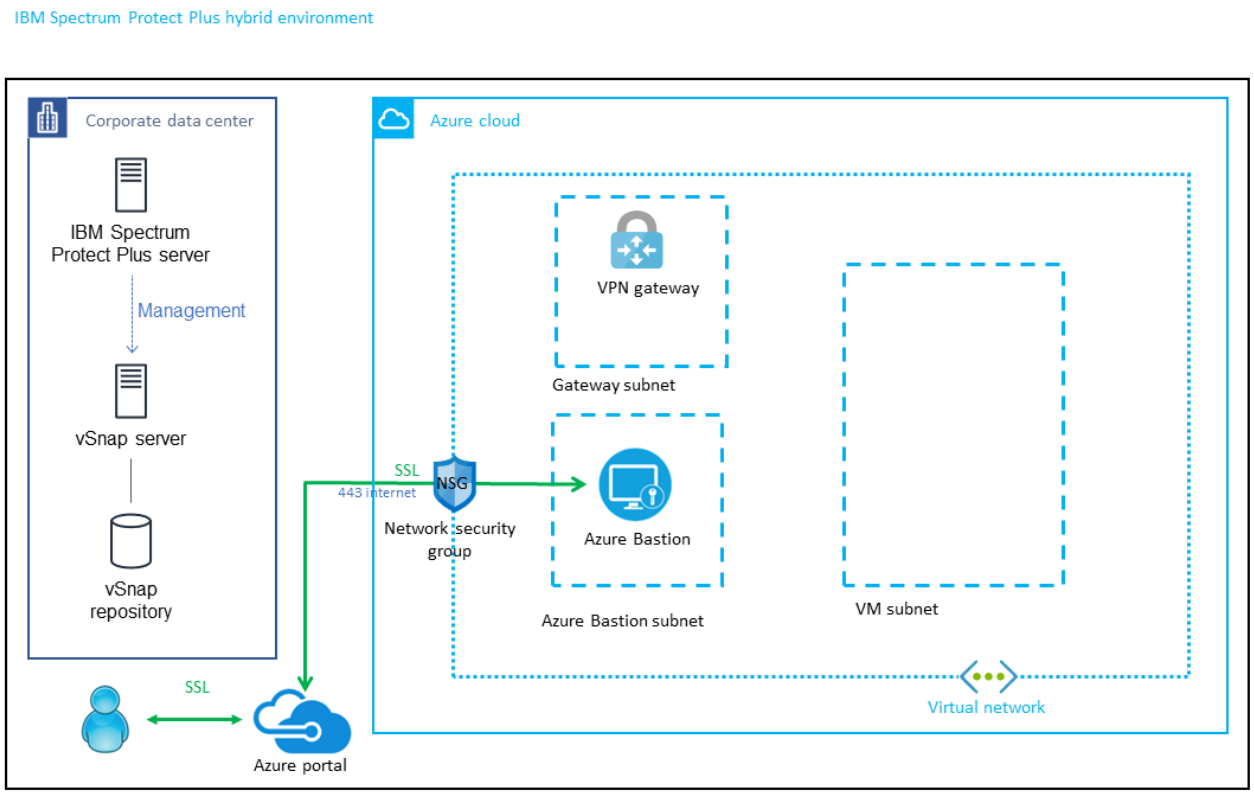


Figure 7. Hybrid environment, before deployment to an existing VNet

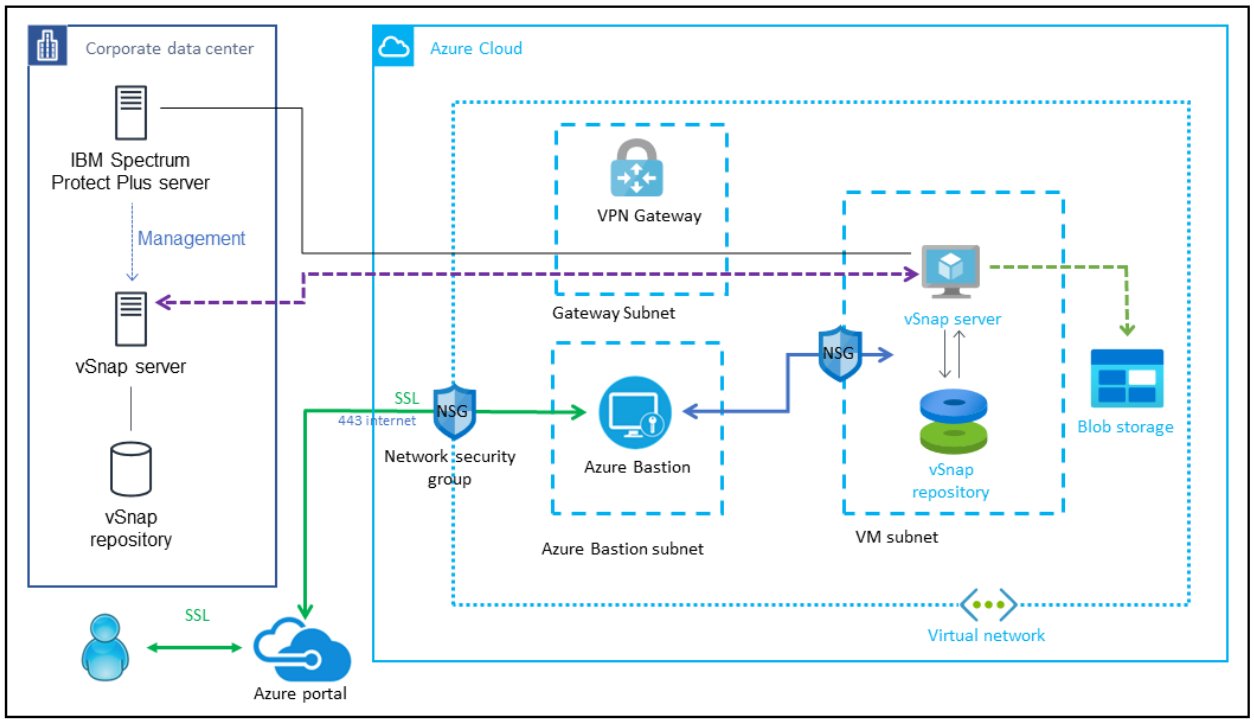


Figure 8. Hybrid environment, after deployment to an existing VNet

Hybrid: Deploying to a new VNet

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

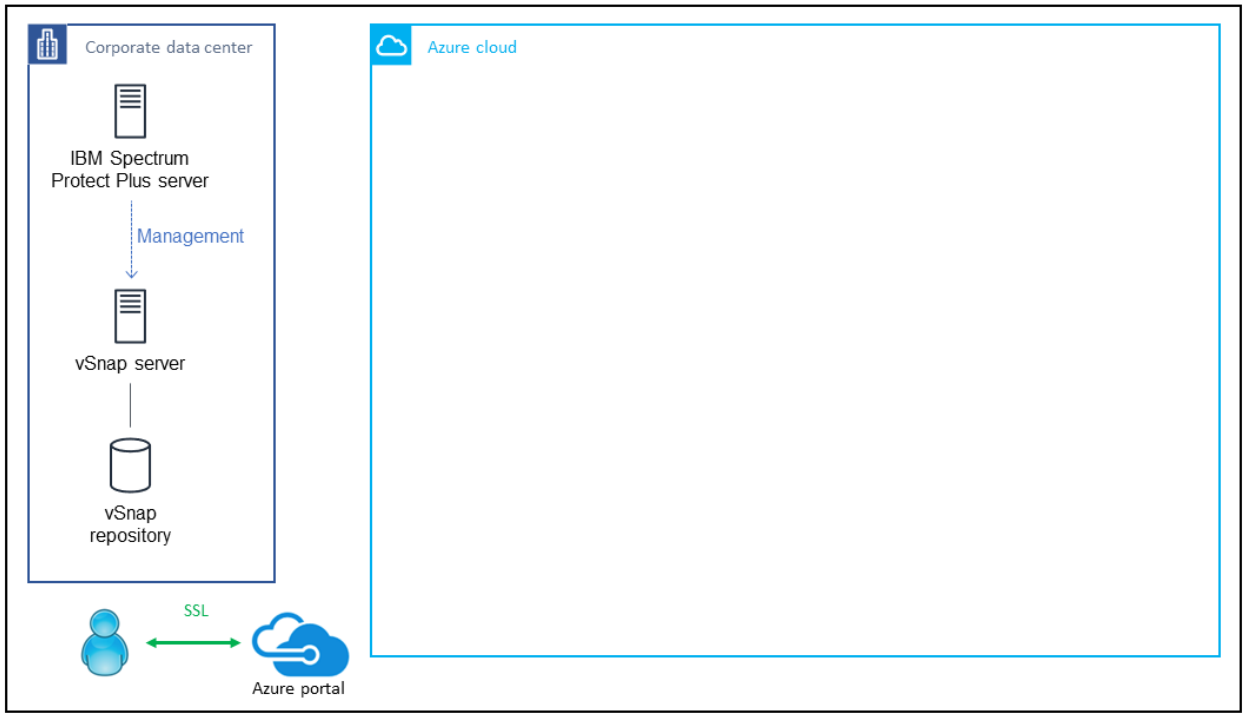


Figure 9. Hybrid environment, before deployment to a new VNet

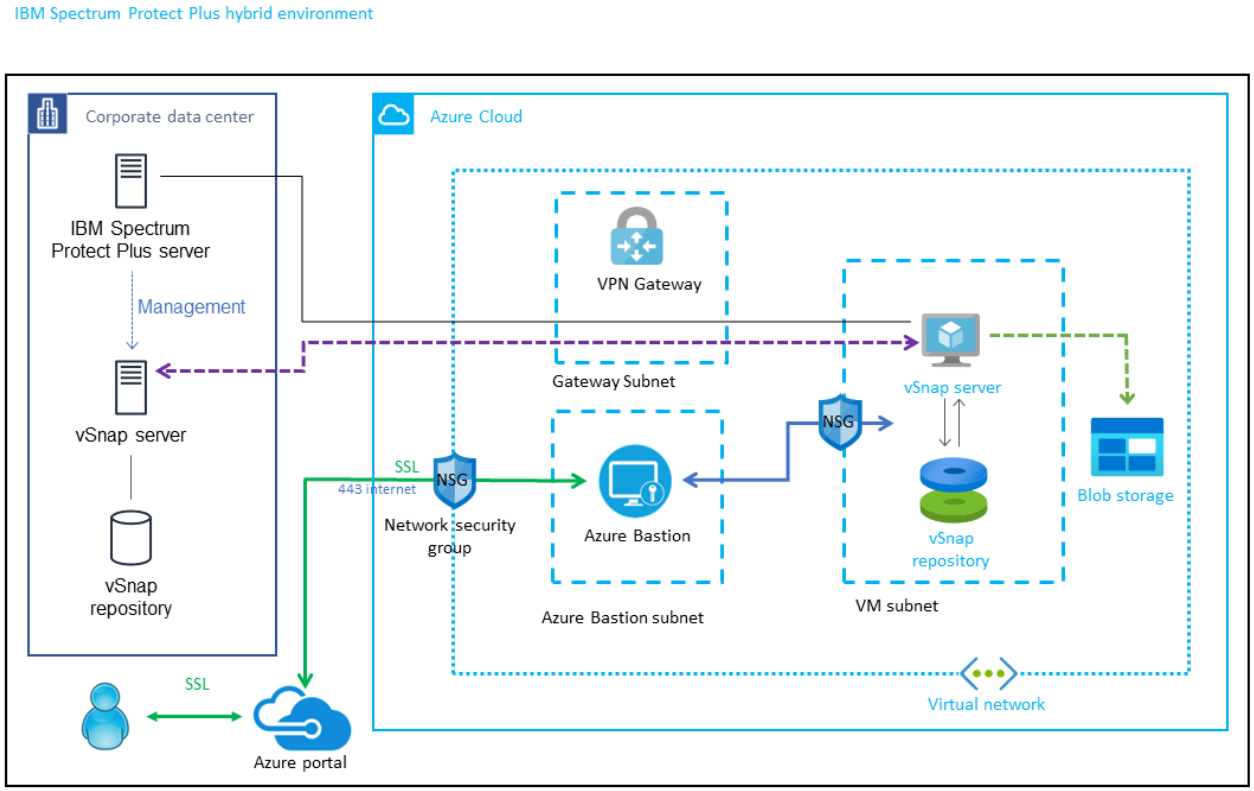


Figure 10. Hybrid environment, after deployment to a new VNet

Security

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

The following overview introduces some of the components of Azure security. For more information about security on Azure, see Azure Security Fundamentals.

Azure Identity and Access Management

Azure Identity and Access Management (IAM) manages and controls user identity. IAM includes security technologies and practices such as role-based access control (RBAC) to manage user access to Azure resources. You can use RBAC to grant users only the amount of access that they require to complete their tasks.

Operating system security

During deployment, a new sudo user is created for SSH and connection purposes. The root user is blocked from access.

The vSnap server VM can be accessed by either the SSH key or the user name and password that were provided during the deployment process. Azure does not store the SSH key or username and password. If you lose your SSH key or username and password, you can lose access to the vSnap server VM.

You must apply operating system patches on a periodic basis.

Security groups

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

The security groups created and assigned to the IBM Spectrum Protect Plus server and vSnap server VMs as part of this solution are restricted as much as possible while allowing access to the various functions needed by IBM Spectrum Protect Plus. Once the VM is up and running, review the security groups to further restrict access as required.

The Azure ARM template creates the following security group rules for the IBM Spectrum Protect Plus server and vSnap server:

- Open port 111 for all VNet 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 VNet IPs for NFS data transfer to and from the vSnap server
- Open port 3260 for all VNet IPs for iSCSI data transfer to and 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 VNet IPs and IBM Spectrum Protect Plus to allow ping tests

Additional open ports might be required to support IBM Spectrum Protect Plus features. For example, to back up Microsoft 365, you must manually open port 443 between the IBM Spectrum Protect Plus server and the proxy server. See the system requirements for the version of IBM Spectrum Protect Plus that you are using.

Chapter 2. Planning for deployment

Before deploying IBM Spectrum Protect Plus on Azure, you must have an Azure account and determine whether you want to deploy to an existing or new VNet.

Creating an Azure account

If you do not have an Azure account, create one at https://azure.microsoft.com by following the on-screen instructions.

Using an existing or new VNet

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

To deploy to an *existing* VNet, you must provide the VNet name and public and private subnet names during deployment. You must also provide a Bastion host IP address if you are connecting to the vNet by using a Bastion host rather than a VPN connection. For more information, see "Deploying to an existing VNet" on page 1.

To deploy to a *new* VNet, you must provide network parameters during deployment. An Azure environment is then created, which consists of the VNet, subnets, NAT gateways, security groups, Bastion host, and other infrastructure components.

Azure services and components

This documentation assumes that you are familiar with the Azure services and components.

If you are new to Azure, visit the Getting Started Resource Center and the Azure Training and Learning center for materials and programs that can help you develop the skills to design, deploy, and operate your infrastructure and applications on the azure Cloud.

Azure Virtual Machine (VM)

Azure Virtual Machines (VM) is one of several types of on-demand, scalable computing resources that Azure offers. Typically, you choose a VM when you need more control over the computing environment than the other choices offer.

An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it. However, you still need to maintain the VM by performing tasks, such as configuring, patching, and installing the software that runs on it.

Azure Virtual Network (VNet)

An Azure Virtual Network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription. You can use VNets to provision and manage VPNs in Azure and optionally, link the VNets with other VNets in Azure, or with your on-premises IT infrastructure to create hybrid or cross-premises solutions. Each VNet you create has its own CIDR block and can be linked to other VNets and on-premises networks as long as the CIDR blocks do not overlap. You also have control of DNS server settings for VNets, and segmentation of the VNet into subnets.

Azure Marketplace

The Microsoft Azure Marketplace is an online store that offers applications and services either built-in or designed to integrate with the Microsoft Azure public cloud.

The products and services offered through the Microsoft Azure Marketplace come from either Microsoft or its technology partners. Before they become available for purchase on the Marketplace, all services and products are certified through the Microsoft Azure Certified program to ensure compatibility with the Azure public cloud.

Azure Resource Manager (ARM)
Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account. You use management features, like access control, locks, and tags, to secure and organize your resources after deployment.

Azure Resource Group (RG)
A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Generally, add resources that share the same lifecycle to the same resource group so you can easily deploy, update, and delete them as a group.

Azure Blob storage
Azure Blob storage is the Microsoft object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data. Unstructured data is data that does not adhere to a particular data model or definition, such as text or binary data.

Bastion host
By including Bastion hosts in your VNet environment, you can 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 VNet through SSH connections on Linux. Bastion hosts are also configured with security groups to provide fine-grained ingress control.

Deploying to an existing VNet by using a Bastion host or VPN connection: If you have a virtual private network (VPN) connection to an existing VNet, a Bastion host is not required. For more information, see “Deploying to an existing VNet” on page 1.

Azure account technical requirements

Before you launch the ARM template, your account must have Azure IAM permissions to install and configure the resources that are required for IBM Spectrum Protect Plus.

The required resources are listed in the following table.

If you are deploying IBM Spectrum Protect Plus to an existing VNet, the resources that are indicated with an asterisk in the table must be pre-existing and are required for successful deployment. If you are deploying to a new VNet, the ARM template deploys these resources.

Resource	IBM Spectrum Protect Plus server and vSnap server deployment (all on cloud)	vSnap server only (hybrid)
Virtual Network (VNet) *	1	1
Public static IPs (pip) *	Up to 2	Up to 2
Security groups	2	1
Virtual machines (VM)	Up to 3	Up to 2
HDD disk volumes (standard LRS)	Up to 13	Up to 13
SSD disk volumes (premium LRS)	8	4
NAT gateways *	1	1
Subnets *	2	2
Blob storage	1	1

You might have to request service limit increases for the these resources. For example, if you 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 Azure documentation.

Regional requirements

The IBM Spectrum Protect Plus server and vSnap server require Azure v4 VMs.

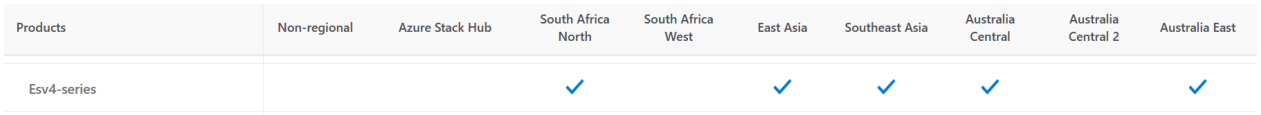
The following VMs are required to deploy IBM Spectrum Protect Plus on Microsoft Azure. You are asked to select a region when you are completing the ARM template for deployment as described in "Launch the ARM template" on page 19. You must select a region in which these VMs are available.

Resource	VM required	Disk Type
IBM Spectrum Protect Plus server	Esv4-series	The disk Standard_E8s_v4 is used for the IBM Spectrum Protect Plus server.
vSnap server	One of the following VMs: • Esv4-series • Bs-series	You are asked to select one of the following disk types when you are completing the vSnap server portion of the ARM template: • Standard_E4s_v4 • Standard_E8s_v4 • Standard_E16s_v4 • Standard_B8ms In the preceding list, 4, 8, and 16 specify the number of cores for the VM.

To view VMs that are available by region, go to Products available by region and complete the following steps:

1. Click **Browse**, and then click **Virtual Machines** in the **Virtual Machines** list.
2. Expand the **Regions** list, and then click **Select all/none**.

The availability of a VM in a region is indicated by a check mark as shown in the following figure for Esv4-series VMs. This figure shows a partial list of regions and is for example purposes.

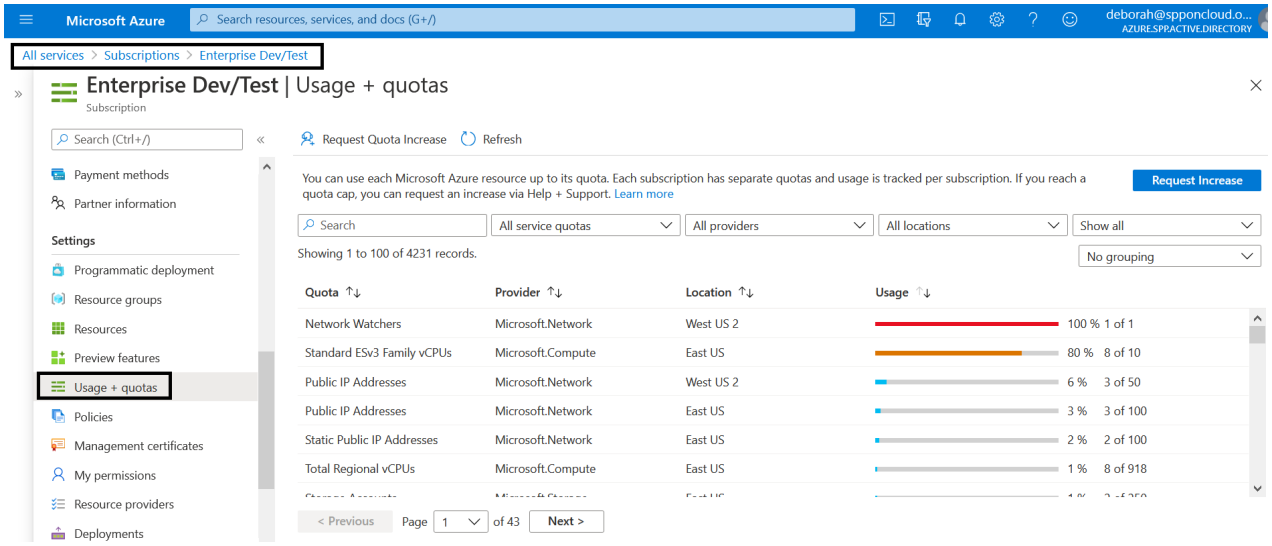


Quota requirements

Quotas are applied to resource groups, subscriptions, accounts, and other Azure components. You must have a sufficient quotas to accommodate IBM Spectrum Protect Plus on Azure.

If you are deploying an all-on-cloud solution, the quota for the Total Regional vCPUs must be 20 vCPUs or greater and you might be required to request a quota increase. In addition, other quotas might require an increase for your IBM Spectrum Protect Plus environment.

To view the quota consumption for a IBM Spectrum Protect Plus on Azure deployment, navigate to the subscription for the deployment in the Azure portal as shown in the following example:



To request a quota increase, click **Request Increase** and follow the instructions that are provided.

If you are new to Microsoft Azure, review the following information to learn about quotas:

- Azure subscription and service limits, quotas, and constraints
- Quota increase requests
- Requesting a quota increase

Costs and licenses

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

The ARM template that is used for deployment includes configuration parameters that you can customize. Some of these settings, such as VM types and storage layout types, will affect the cost of deployment. Prices are subject to change. For the price of each VM type, see the VM series and pricing.

The IBM Spectrum Protect Plus server, which can reside on the Azure Cloud or on premises, must be licensed for the physical data that is protected on the Azure environment. If you choose to have the IBM Spectrum Protect Plus server on Azure 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 Uploading the product key.

For additional licensing information, contact IBM Support.

IBM Spectrum Protect Plus planning and sizing tools

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.

The blueprints include a sizing worksheet that 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 Azure marketplace deployment.

Attention: When you deploy IBM Spectrum Protect Plus on Azure by using the ARM template, you must select a size for the vSnap server repository from a list. You cannot specify a disk size that is not on the list. Select the closest repository size that is larger than the size suggested by the sizing worksheet. For example, if the worksheet calculates a vSnap repository size of 10 TiB, select 12 TiB for the repository size.

This action prevents issues caused by attempting to combine multiple disk types and sizes and helps to keep your storage costs close to your requirements.

Related tasks

"Launch the ARM template" on page 19
Launch the ARM template to deploy IBM Spectrum Protect Plus on Azure

Chapter 3. Deploying IBM Spectrum Protect Plus on Azure

You can deploy IBM Spectrum Protect Plus on Azure as an all-on-cloud or hybrid data protection solution.

Complete the deployment tasks in the order presented in the following topics. Begin with “Launch the ARM template” on page 19.

Launch the ARM template

Launch the ARM template to deploy IBM Spectrum Protect Plus on Azure

Before you begin

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

About this task

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).

Deployment is determined by information and parameters that you enter for the ARM template. An example of a completed template is shown in “Example deployment” on page 26

Important: For a hybrid environment where only the vSnap server is deployed to a new VNet, make sure that the VNet has a bidirectional communication established to your on-premises IBM Spectrum Protect Plus server prior to running the template as described in “Hybrid deployment” on page 6. Otherwise, the template might fail during the attempt to automate the process.

Procedure

To deploy IBM Spectrum Protect Plus on Azure by using the ARM template, complete the following steps:

1. Sign in to your Azure account at https://azure.microsoft.com/en-us/.

   Make sure that the account has the right permissions to order Azure Marketplace products and to deploy ARM templates that create new VMs, disks, storage accounts, resource groups, and other components.
2. Open IBM Spectrum Protect Plus in Azure Marketplace and choose **Create**.

   A series of tabs are provided for you to enter the parameters for the ARM template. Complete each tab and then click **Next**.
3. On the **Basics** tab, enter the following parameters:

Parameter Field	Default Value	Description
Subscription	User provided	Select your Azure subscription. All resources in an Azure subscription are billed together.

Parameter Field	Default Value	Description
Resource Group	User provided	Enter a resource group or select an existing group. All the resources that will be created during deployment will be stored in the specified resource group.  **Attention:** The resource group must be empty prior to deployment.
Region	User provided	The region where all resources will be created.  **Attention:** The IBM Spectrum Protect Plus server and vSnap server require the Azure v4 VMs that are listed in “Regional requirements” on page 15. Ensure that the region you select provides these VMs.
Template name	User provided	Enter a template name. This name will be used as a prefix to many resources that will be deployed.
Instances to deploy	User provided	The instance to deploy. For an all-on-cloud solution, which deploys the IBM Spectrum Protect Plus and vSnap servers, select **All on cloud**. For a hybrid solution, which deploys only thevSnap server, select **Hybrid**
SSH username	User provided	The username that will be used to connect via SSH to your IBM Spectrum Protect Plus server, vSnap server instance, and Bastion host.
Authentication type	Password	The authentication type for the VM: **Password** or **SSH Public Key**. This authentication type is used to connect to your IBM Spectrum Protect Plus server, vSnap server instance, and Bastion host.

Parameter Field	Default Value	Description
Password	User provided	If you chose the authentication type **Password**, provide a password for the VM. The following rules are required for the password: • The minimum acceptable password length is 15 characters. • The new password must contain at least one character from each of the classes (numbers, uppercase letters, lowercase letters, and other). • The maximum number of identical consecutive characters that are allowed in the new password is three characters. • The maximum number of identical consecutive class of characters that are allowed in the new password is four characters.
Confirm password	User provided	Confirm the password.
SSH public key	User provided	If you chose the authentication type **SSH Public Key**, enter a public key. For information about using an SSH key, see Learn more about creating and using SSH keys in Azure.

4. On the **Networking** tab, enter the following parameters:

Parameter Field	Default Value	Description
Virtual network	User provided	Select an existing VNet or click **Create new** to create a new VNet by providing a new VNet name, IP ranges and subnets.
Public subnet	User provided	Select an existing public subnet or create a new public subnet in VNet.
Private subnet	User provided	Select an existing private subnet or create a new private subnet in VNet

Parameter Field	Default Value	Description
Allowed external access CIDR	If deploying to a new VNet, user provided	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.
Bastion host IP	If deploying to an existing VNet, user provided	The IP address of an existing Bastion host. This field cannot be blank. If you are deploying to an existing VNet and do not have an existing Bastion host, you can enter a value such as 10.0.0.0 and the deployment will complete. You can then change the IP address after deployment as described in “Update the SSH connection to the Bastion host (optional) ” on page 33. If you are using a VPN connection rather than a Bastion host, use the dummy IP address 1.1.1.1.

5. On the **IBM Spectrum Protect Plus Server configuration** tab, enter the following parameters:

Parameter Field	Default Value	Description
IBM Spectrum Protect Plus IP	User provided	The IP address of an existing IBM Spectrum Protect Plus server. This field is displayed only for a hybrid configuration on an existing VNet.

Parameter Field	Default Value	Description
IBM Spectrum Protect Plus username	administrator	The user name for the IBM Spectrum Protect Plus application. For an all-on-cloud configuration, this username is used for IBM Spectrum Protect Plus application configuration. For hybrid configuration, this username is used to register a new vSnap server on a IBM Spectrum Protect Plus server. This value cannot be blank, admin, test, or root. The user name can have a maximum of 32 characters.
IBM Spectrum Protect Plus password	User provided	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	User provided	Confirm the password.

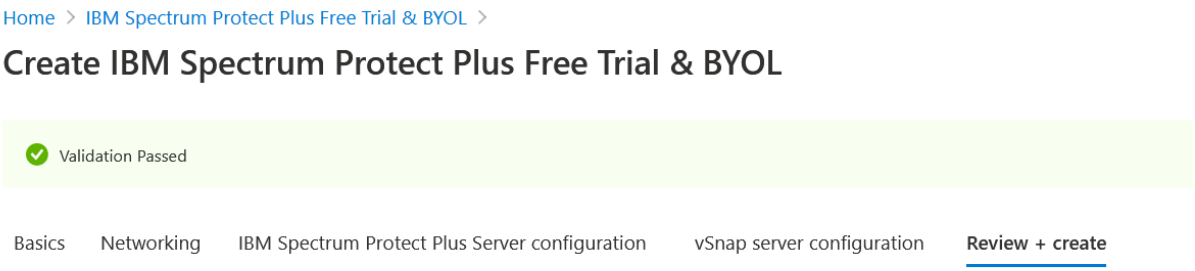
6. On the **vSnap server configuration** tab, enter the following parameters, and then click **Next: Review + create**:

Parameter Field	Default Value	Description
vSnap server repository size	12 TiB	Select the repository size in TiB.
Deduplication	Disable	This value permanently enables or disables data deduplication across the vSnap repository.
VSNAP server virtual machine type	Standard_E4s_v4	The vSnap server VM type. Choose a type that corresponds to the vSnap repository size and deduplication option.
Disk type in vSnap pool	Standard_HDD	The disk type for each disk in the vSnap pool. The options are: • Standard HDD (Standard_LRS) • Standard SSD (StandardSSD_LRS) • Preimium SSD (Premium_LRS)

Parameter Field	Default Value	Description
vSnap server user	admin	The username for the vSnap server application. This value cannot be serveradmin, blank, or root. A username can have a maximum of 32 characters.
vSnap server password	User provided	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	User provided	Confirm the password.
Blob container name	User provided, optional	To copy snapshots from the vSnap server to a Blob container, specify the name of the container. If a Blob container is specified, snapshots will be copied from the vSnap server to that container for a further level of data protection. If the Blob container does not exist, it is created during the deployment. To register the Blob container in the IBM Spectrum Protect Plus server, the deployment uses storage account access key and private keys. The keys are registered in the IBM Spectrum Protect Plus server and the Blob is scanned and registered. An SLA policy that defines the Blob container as a copy target is created. This policy is named AZURE_policy. You can assign database resources to this policy to ensure that backup snapshots of the resources are copied to the Blob container. This parameter does not appear for a hybrid configuration on a new VNet.

7. On the **Review + create** tab, review the parameters.

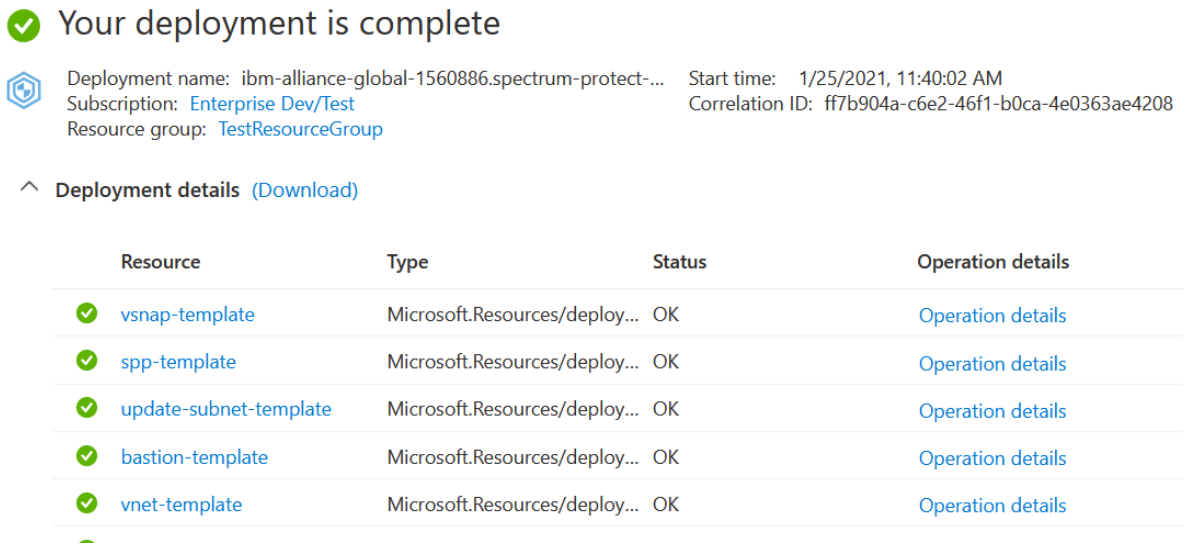
   A validation process is executed in the background. A messages is displayed showing the status of the validation as shown in the following example:



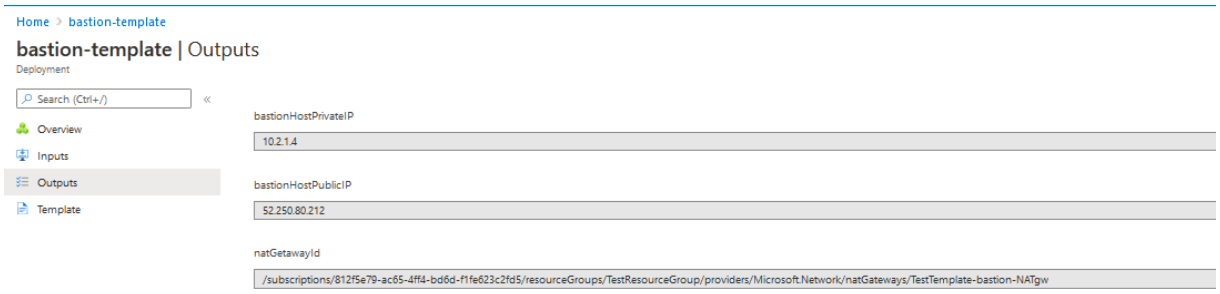
You can click **Previous** on this tab to return to any tab to make changes.

8. Click **Create** to start the deployment.
9. Monitor the status of the deployment.

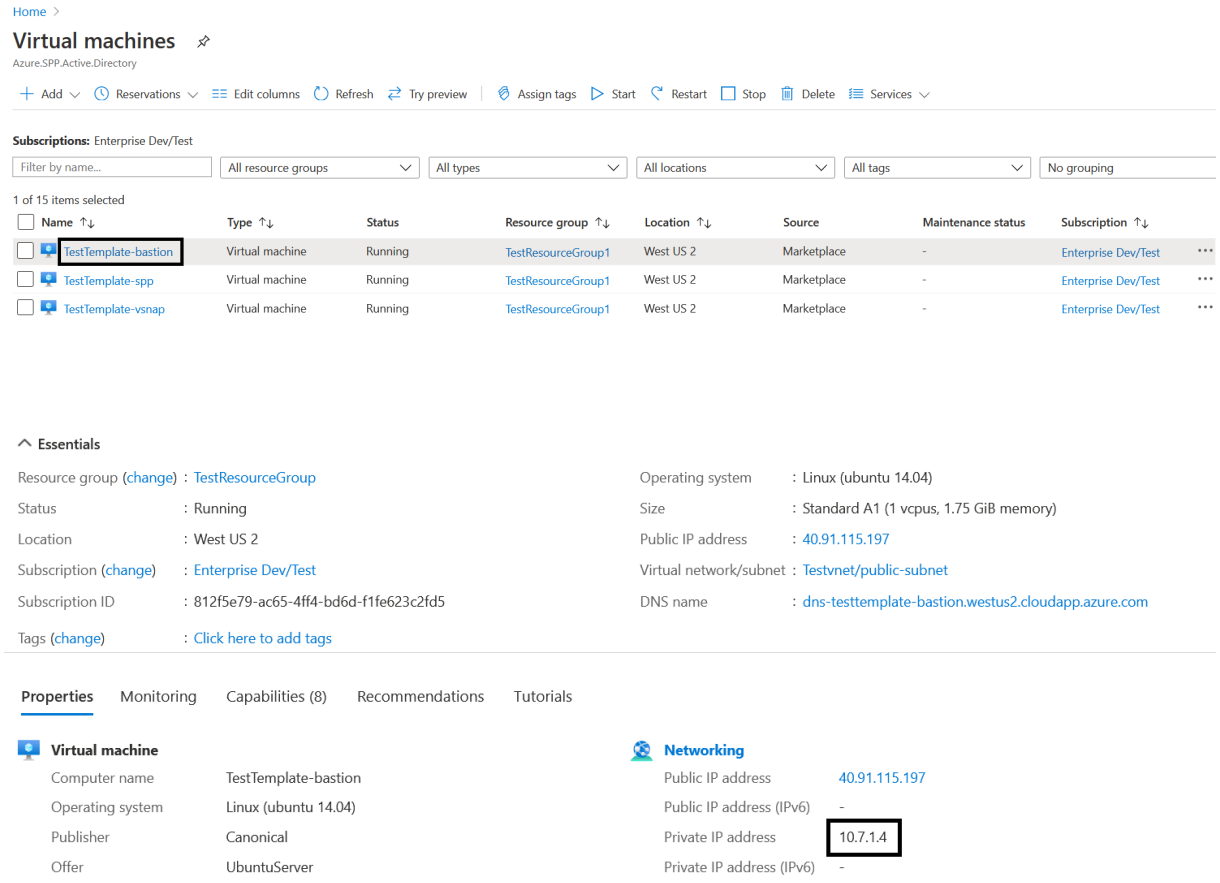
   The status **Your deployment is complete** is displayed when the deployment completes as shown in the following example. The status of each resource that is created by the template is shown. To view details about each resources, click **Operation details**.



10. Click **Outputs** to view the IP address or addresses for the resource. You are required to provide the IP addresses for the Bastion host, the IBM Spectrum Protect Plus server, and the vSnap server to complete the deployment. Note the addresses for reference when you are asked to provide these addresses. The following example figure shows the private and public IP addresses for the Bastion host.



11. To view information about the VM that is created for each resource, including the IP address for the VM, click **Home** > **Virtual Machines**, and then click the VM as shown in the following example:



Example deployment

Refer to an example of an all-all-cloud deployment in a new VNet.

About this task

This task is for example purposes. Refer to “Launch the ARM template” on page 19 for a description of the deployment parameters to determine the values that are required for your environment.

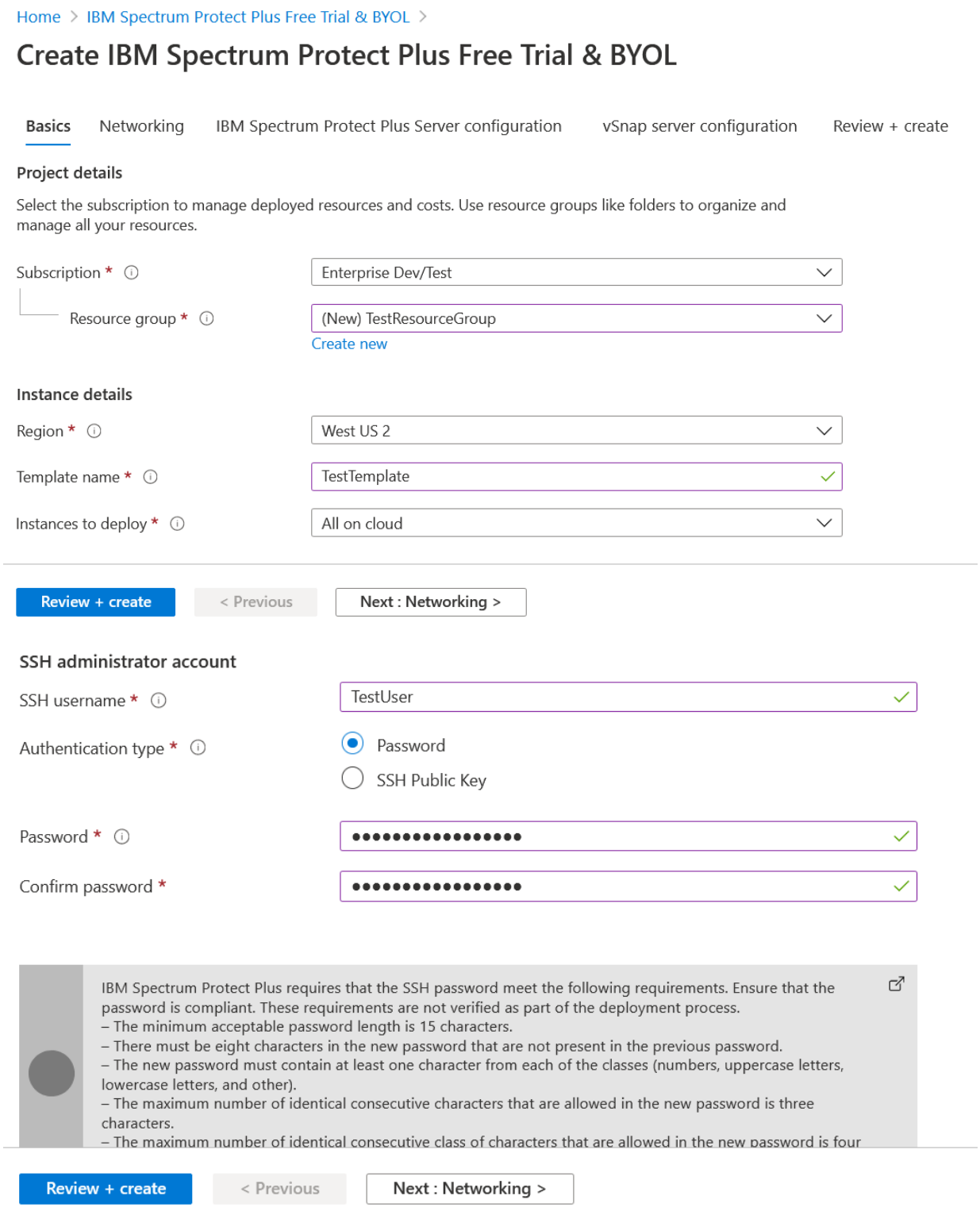
Procedure

1. Sign in to your Azure account at https://azure.microsoft.com/en-us/.
2. Open IBM Spectrum Protect Plus in Azure Marketplace and choose **Create**.

   A series of tabs are provided for you to enter the parameters for the ARM template. Complete each tab and then click **Next**.
3. On the **Basics** tab, enter the basic parameters for the deployment as shown in the following figure.

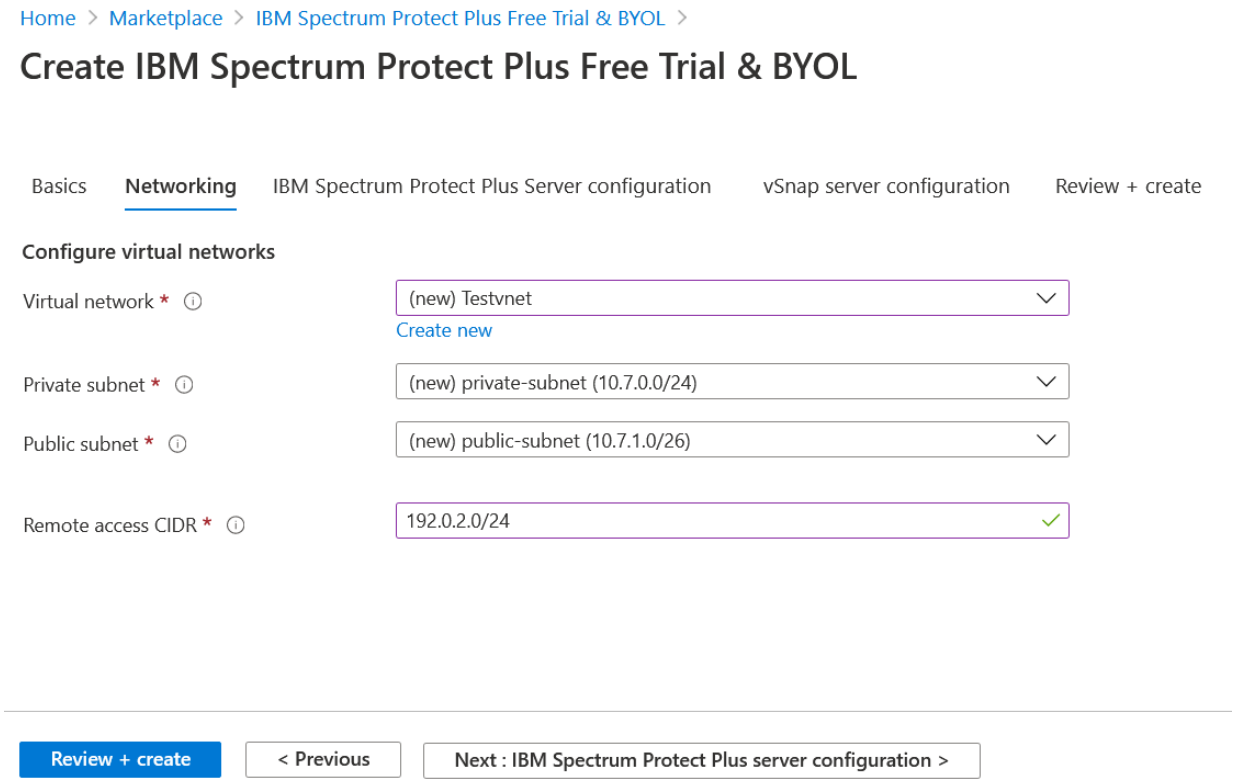
   In this example, note the following key parameters:

   - **All on cloud** is selected in the **Instances to deploy** field.
   - A new resource group named **TestResourceGroup** was created by clicking **Create new** for the **Resource group** field.
   - The template name is defined in the **Template name** field.
   - The user authentication method is **Password**.



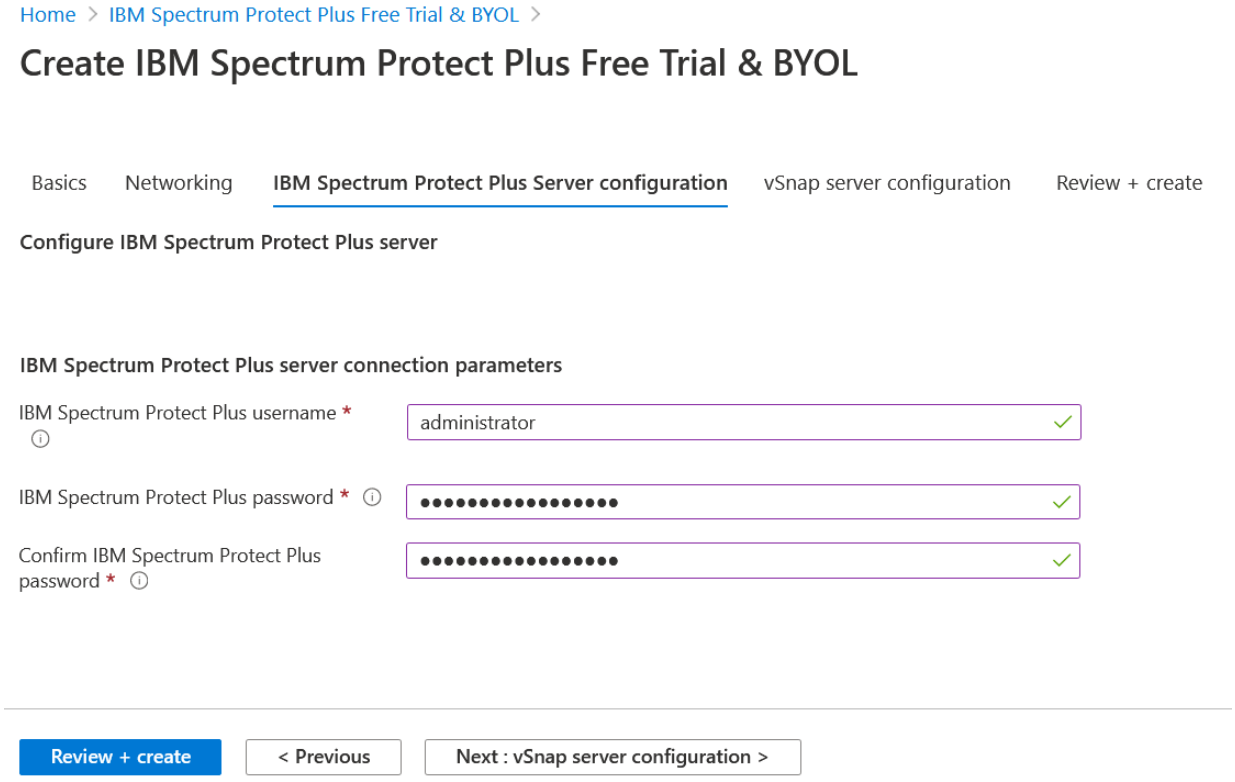
4. On the **Networking** tab, enter the networking parameters for the deployment as shown in the following figure.

   In this example, a new VNet named **Testvnet** was created by clicking **Create new**.

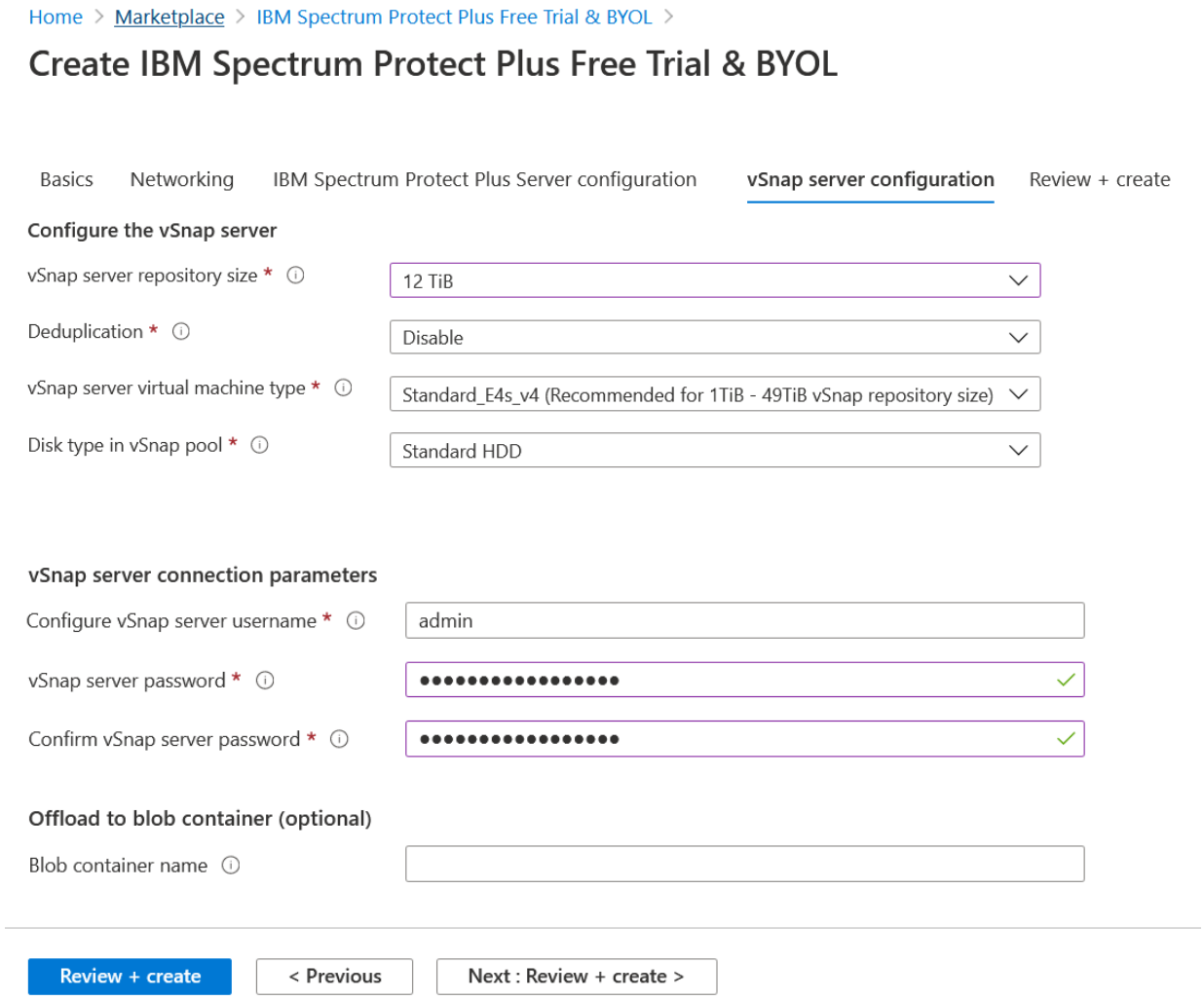


5. On the **IBM Spectrum Protect Plus server configuration** tab, enter the parameters for the server as shown in the following example.

   Parameter fields are not provided on this tab if you are deploying a hybrid environment on a new VNet.

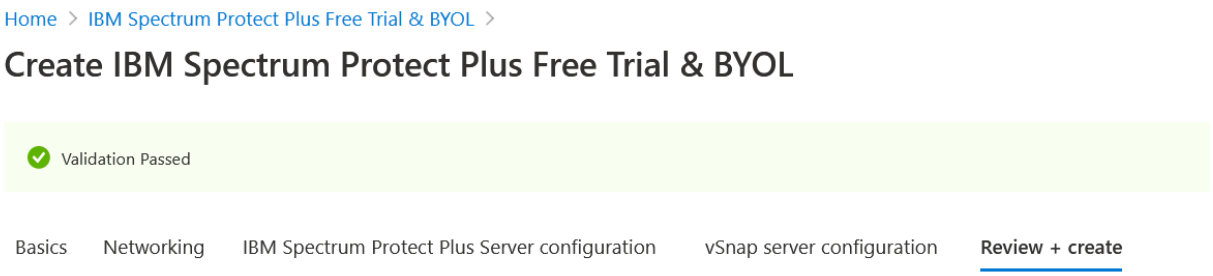


6. On the **vSnap server configuration** tab, enter the vSnap server parameters as shown in the following example, and then click **Next: Review + create**.



7. On the **Review + create** tab, review the parameters.

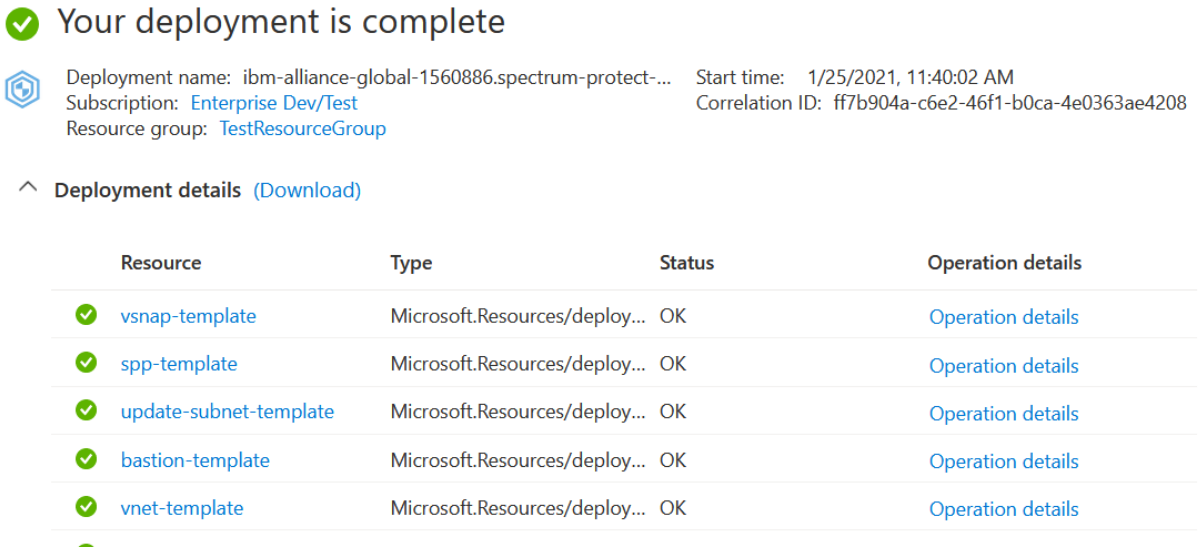
   A validation process is executed in the background. A messages is displayed showing the status of the validation as shown in the following example:



   You can click **Previous** on this tab to return to any tab to make changes.

8. Click **Create** to start the deployment.
9. Monitor the status of the deployment.

   The status **Your deployment is complete** is displayed when the deployment completes as shown in the following example. The status of each resource that is created by the template is shown. To view details about each resource, click **Operation details**.



Connect to the IBM Spectrum Protect Plus web application

If you are deploying IBM Spectrum Protect Plus server to a existing or new VNet for an all-on-cloud solution, you must connect to the IBM Spectrum Protect Plus web application.

Before you begin

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

Use one of the following options to connect the IBM Spectrum Protect Plus application by using a browser:

Option	Description
Configure a VPN connection between your organization and the Azure VNet	You can use the Azure 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 on any computer in your organization. For information about the Azure site-to-site feature, see What is Azure Site-to-Site VPN?.
Install a Windows bastion server with a public IP address on the VNet and use a Remote Desktop Protocol (RDP)	For information about RDP, see Azure Bastion connection to open a browser on the bastion server to connect to the IBM Spectrum Protect Plus application.
Configure SSH tunneling by using a Linux bastion server	For information about SSH tunneling, see Appendix B, “Access the IBM Spectrum Protect Plus web application using SSH tunneling,” on page 41.

Testing the deployment

The steps for testing the deployment depend on the type of deployment.

About this task

Refer to the following table for the steps required to test the deployment by type:

Deployment type	Description	Instructions
Hybrid: Existing IBM Spectrum Protect Plus server on premises, vSnap server deployed in a new Azure VNet	In this scenario, you must manually configure communication between the on-premises IBM Spectrum Protect Plus server and the vSnap server on Azure. You must also register the vSnap server with your on-premises IBM Spectrum Protect Plus server.	See "Testing an on-premises IBM Spectrum Protect Plus server with a vSnap server in a new Azure VNet" on page 31
Hybrid: Existing IBM Spectrum Protect Plus server on premises, the vSnap server deployed in an existing Azure VNet All On Cloud: IBM Spectrum Protect Plus server and vSnap server deployed in a new Azure VNet All On Cloud: IBM Spectrum Protect Plus server and vSnap server deployed in an existing Azure VNet	In these scenarios, after your vSnap server and repository are configured, the ARM 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 "Testing all other all-on-cloud and hybrid deployment types" on page 32

Testing an on-premises IBM Spectrum Protect Plus server with a vSnap server in a new Azure VNet

Before you begin

To complete this procedure, you must have the IP address for the vSnap server that you noted when you completed the instructions in "Launch the ARM template" on page 19.

Procedure

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 Azure as described in "Hybrid deployment" on page 6.
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.
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 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. On the **Disk Storage**, click **Add Disk Storage**.
6. Complete the fields in the **New Storage** pane to register the vSnap server with your on-premises IBM Spectrum Protect Plus server:

   Hostname/IP
   Enter the IP address for the vSnap server.

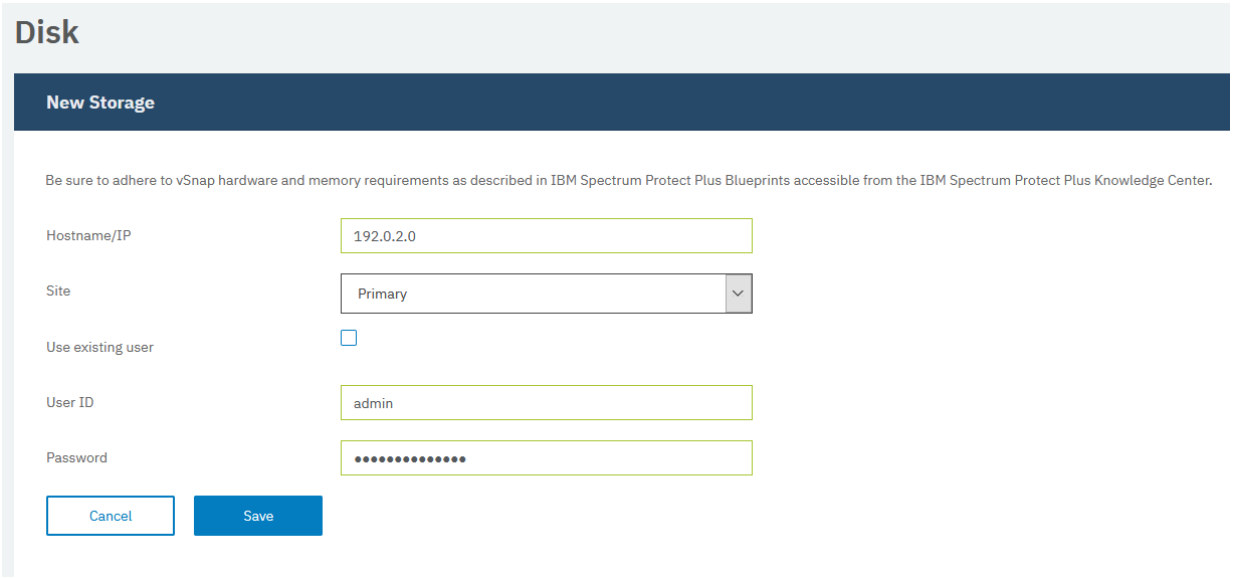
Site
Select **Primary**.

Use existing user
Select to use a a previously entered user name and password for the vSnap server.

Username
Enter the username for the vSnap server. This is the user name that you specified in the ARM template as described in “Launch the ARM template” on page 19.

Password
Enter the password for the user.

The following example figures shows completed fields for adding a vSnap server:



7. Click **Save** to add the vSnap server and return to the **Disk Storage** pane.
8. Find the IP address for the vSnap server. click the actions menu icon ⋮ that is associated with the server, and then select one of the following initialization methods:

   Initialize with Encryption
   Enable encryption of backup data on the vSnap server.

   Initialize
   Initialize the vSnap server without encryption enabled.

   The initialization process runs in the background and requires no further user interaction. The process might take 5 - 10 minutes to complete.

Testing all other all-on-cloud and hybrid deployment types

Procedure

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 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 and go to the *Browser support* section of the requirements.
2. In the IBM Spectrum Protect Plus navigation pane, click **System Configuration** > **Backup Storage** > **Disk**.
3. Confirm that the vSnap server is displayed in the list of disk storage in the **Disk Storage** pane.

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 VNet, 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.

Before you begin

Tip: Skip this topic if you are connecting to an existing VNet by using a VPN connection.

To complete this procedure, you must have the IP addresses for the Bastion host, IBM Spectrum Protect Plusserver, and vSnap server that you noted when you completed the instructions in "Launch the ARM template" on page 19.

About this task

If you are deploying in a new VNet, 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 VNet during deployment. If you are deploying to an existing VNet, you must provide the IP address for the Bastion host during deployment.

The Bastion host is the only server in the VNet that has public access.

If you are deploying in an existing VNet, 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 during deployment and the Bastion is not available or you want to increase or decrease the number of IP addresses that can access the Bastion host.

Procedure

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

1. Open the Azure portal and navigate to the **Virtual Machine** page.
2. Find the running VM that is named *your_ template_name*-bastion.
3. On VM view, click **Networking** to see the security group that associated with the Bastion Network Interface Card (NIC).

   You can add additional inbound and outbound rules from this interface.
4. To change an existing rule, click the relevant row in table.

   A modification window opens.
5. If SSH key authentication was chosen during deployment, add your private key to the ssh-agent by providing the path of the key file as an argument to the ssh-add command. The following steps show commands for a Linux shell. If you are using another shell, such as Windows PowerShell, the commands are similar.

   a) Activate the ssh-agent:

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

   b) Add your key to agent to store your credentials locally and temporarily:

   ```
   #ssh-add /path/key_pair_file
   ```

   where:

   The parameter *key_pair_file* is a .pem file that contains the private key that is required to connect to the Bastion host and the IBM Spectrum Protect Plus server and vSnap server instance.

6. If the authentication method that was chosen during deployment is username and password, 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 <username_provided_during_deployment>@bastion_host_ip_address

#ssh <username_provided_during_deployment>@server_ip_address
```

   where:

   The parameter *username_provided_during_deployment* is the chosen username that was provided during deployment. This user will be used to enable SSH connection to the Bastion host, IBM Spectrum Protect Plus server and vSnap server.

   The parameter *bastion_host_ip_address* is the IP address for the Bastion host.

   The parameter *server_ip_address* is the IP address for the IBM Spectrum Protect Plus instance.

   Provide the password when prompted.

Chapter 4. Troubleshooting

Troubleshooting procedures are available for diagnosis and resolution or issues that occur during the deployment process.

For information about common errors, see https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/common-deployment-errors.

If the deployment of IBM Spectrum Protect Plus to Azure fails, a message is displayed when the deployment operation completes. Review the logs and operation details to determine the cause of the failure.

If you require assistance resolving an issue that is related to Azure resource, contact Azure support. For example, if a deployment template attempts to create resources that exceed your Azure quotas, the deployment will fail. In this scenario, you can file a support issue requesting a quota increase by using the Azure portal as described in Troubleshoot common Azure deployment errors with Azure Resource Manager.

If you require assistance resolving an issue that is related to, such as incorrect parameter values in the deployment template, contact IBM Software Support. To assist the support team in the troubleshooting an issue, provide a log of the deployment activity.

Collecting log files for troubleshooting

To assist IBM Software Support in the troubleshooting a deployment issue, provide a log of the deployment activity.

You can use one of the following methods to collect a log file:

- The Azure portal
- The Azure CLI
- The Azure PowerShell CLI

Collecting log files by using the Azure portal

When the deployment operation completes, the status of deployment operation and individual resources is shown on the **Overview** page. You can download the log files to troubleshoot the issues that caused the deployment to fail.

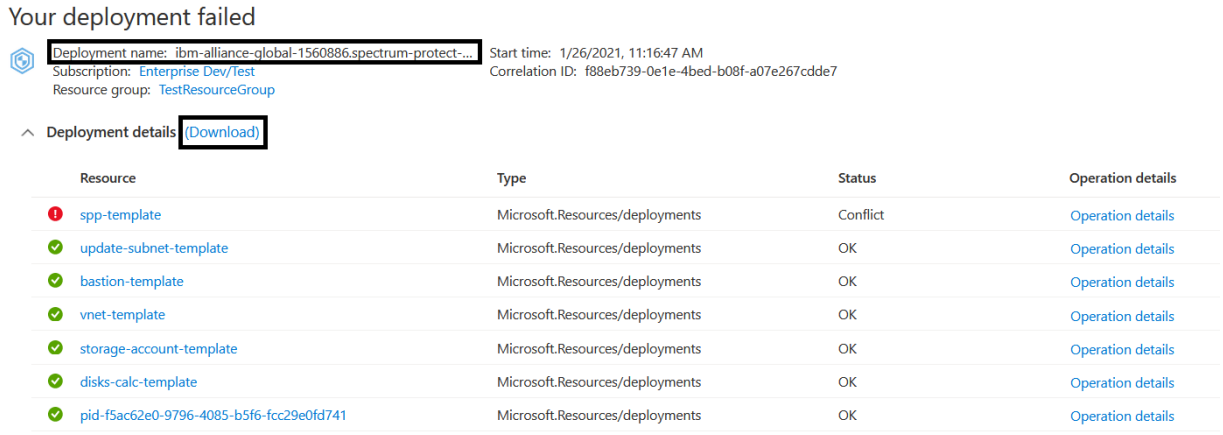
About this task

IBM Software Support requires the overall deployment log and the log for each resource that failed.

Procedure

To collect log files for a failed resource, complete the following steps:

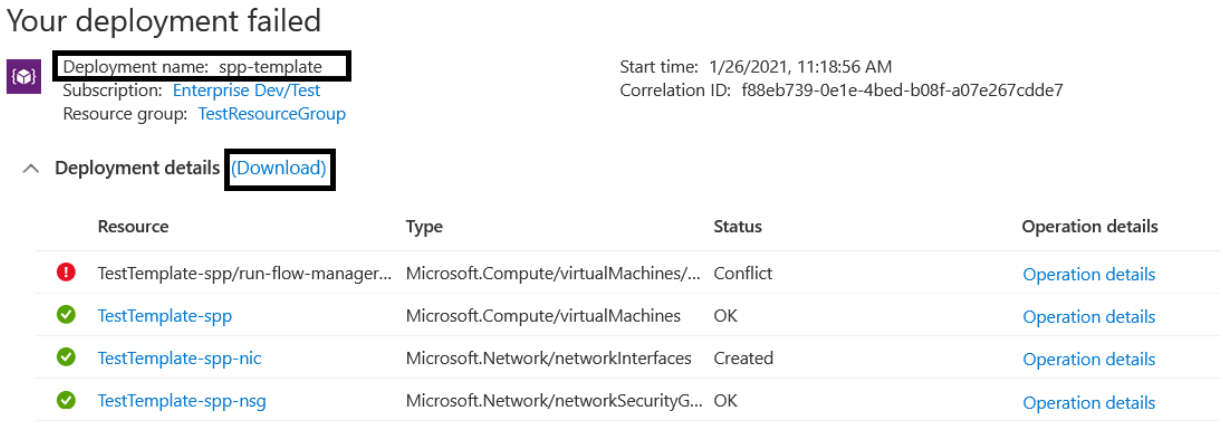
1. When the deployment operation completes, collect the log files by clicking **Download**.



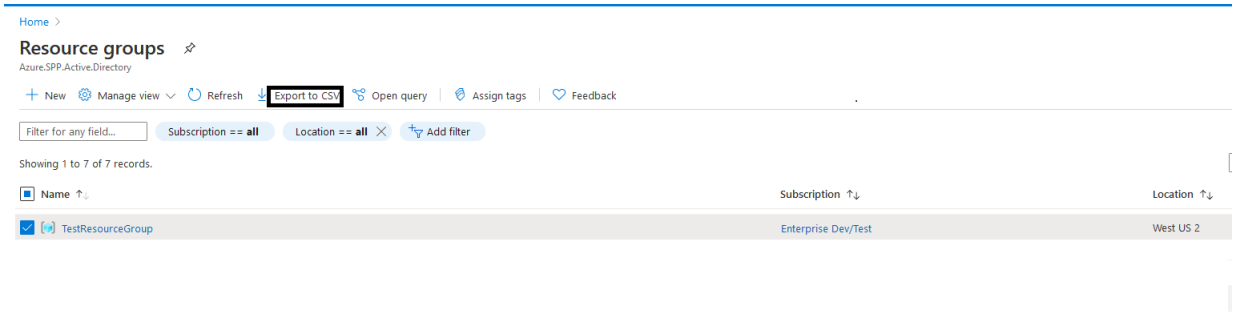
You can also click **Operation details** at any level of the resource navigation to view information about the failure.

2. For each failed resource, click the resource and click **Download** to collect the logs for that resource.

   In the preceding example, the failed resource is **spp-template**. .



3. Optional: You can also access log information by navigating to the resource group that was specified in the ARM template and clicking **Export to CSV**.



4. Submit the all files to IBM Software support.

Collecting log files by using the Azure CLI

You can use the Azure CLI to collect log files.

Before you begin

Ensure that you have the CLI installed on a Microsoft Windows, macOS, or Linux operating system.

Procedure

From the command line, enter the following commands:

```
#az monitor activity-log list -g {resource_group_name} -StartTime {YYYY-MM-DDTHH:MM}
-EndTime {YYYY-MM-DDTHH:MM} >  {output_success_file_name}
```

```
#az monitor activity-log list -g {resource_group_name} -StartTime {YYYY-MM-DDTHH:MM}
-EndTime {YYYY-MM-DDTHH:MM} --status Failed >  {output_failed_file_name}
```

```
#az monitor activity-log list -g {resource_group_name} -StartTime {YYYY-MM-DDTHH:MM}
-EndTime {YYYY-MM-DDTHH:MM>}--status Failed --query [].properties.statusMessage >
{output_query_failed_file_name}
```

where:

The parameter **resource_group_name** is the name of the resource group for the deployment.

The parameters **StartTime** and **EndTime** are the deployment start and end time (including the failure time).

The parameter **output_value** is the output file name.

Example

```
#az monitor activity-log list-g ExampleResourceGroup --start-time 2020-10-28 --end-time
2020-10-29 > output_deployment_log_success.txt
```

```
#az monitor activity-log list-g ExampleResourceGroup --start-time 2020-10-28T00:00--end-time
2020-10-29T12:00--status Failed > output_deployment_log_failed.txt
```

```
#az monitor activity-log list -g ExampleResourceGroup --status Failed --start-time 2020-10-28 --
end-time 2020-10-29 --query [].properties.statusMessage > output_deployment_log_query_failed.txt
```

Collecting log files by using the Azure Power Shell CLI

You can use the Azure PowerShell to collect log files.

Before you begin

Ensure that you have the Azure PowerShell installed on a Microsoft Windows, macOS, or Linux operating system.

Procedure

From the command line, enter the following commands:

```
#Get-AzLog -ResourceGroup {resource_group_name} -StartTime {YYYY-MM-DDTHH:MM}
-EndTime {YYYY-MM-DDTHH:MM} > {output_file_name}
```

where:

The parameter **ResoureceGroup** is the name of the resource group for the deployment.

The parameters **StartTime** and **EndTime** are the deployment start and end time (including the failure time).

The parameter **output_file_name** is the output file name.

Example

```
#Get-AzLog -ResourceGroup ExampleResourceGroup -StartTime 2020-10-28T00:00
-EndTime 2020-10-29T00:00 > output_deployment_log.txt
```

Deployment fails with exceeding regional cores quota error

If you attempt to deploy a VM with more cores than the permitted amount for a region, you receive an error that contains the text "exceeding total approved Regional Cores quota".

To resolve this issue, request a quota increase from the **Subscriptions** page of the Azure portal as described in “Quota requirements” on page 15.

When the quotas are increased, run the deployment operation again.

Deployment fails because the requested VM type is not available in the chosen region

The VM type that is required for the IBM Spectrum Protect Plus sever or vSnap server is not available in the chosen region.

The IBM Spectrum Protect Plus server and vSnap server require Azure v4 VMs. If the required VM type and size is not available in the region type that was selected in the ARM template, the deployment fails with an error message:

```
The requested VM size vm_disk_type is not available in the current region
```

For information about regions and VM availability, see “Regional requirements” on page 15.

Appendix A. Expand the vSnap server capacity post deployment procedure

You can expand an existing vSnap pool by ordering new disk volumes and attaching the volumes to the vSnap server on Azure. The IBM Spectrum Protect Plus server can be on premises or on Azure.

Procedure

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

1. Go to the Azure portal and select **Virtual machines**.
2. Choose the vSnap VM from the list.
3. On the **Virtual machines** page, under **Settings**, choose **Disks**.
4. On the **Disks** pane, under **Data disks**, select **Create and attach a new disk**.
5. Enter a name for your managed disk. Review the default settings, and update the **Storage type** and **Size (GiB)** fields.
6. When you are done, click **Save** at the top of the page to create the managed disk and update the VM configuration.

   Wait for the process to complete.
7. Open the IBM Spectrum Protect Plus server user interface.
8. In the navigation pane, click **System Configuration** > **Backup Storage** > **Disk**.
9. Find the IP address for the vSnap server, click the actions ⋮ menu that is associated with the server, and then click **Refresh**.

   The vSnap server scans the system for new volumes.
10. Click the tools icon ⚙ for the vSnap server.
11. Click the **Disks** tab, select the volumes that you want to add, and click **Save**.

    The new capacity is added to the vSnap pool.

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

You can access the IBM Spectrum Protect Plus web application by using SSH tunneling.

About this task

If you have an existing VPN connection configured, 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 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.

The following figure illustrates the SSH tunneling configuration:

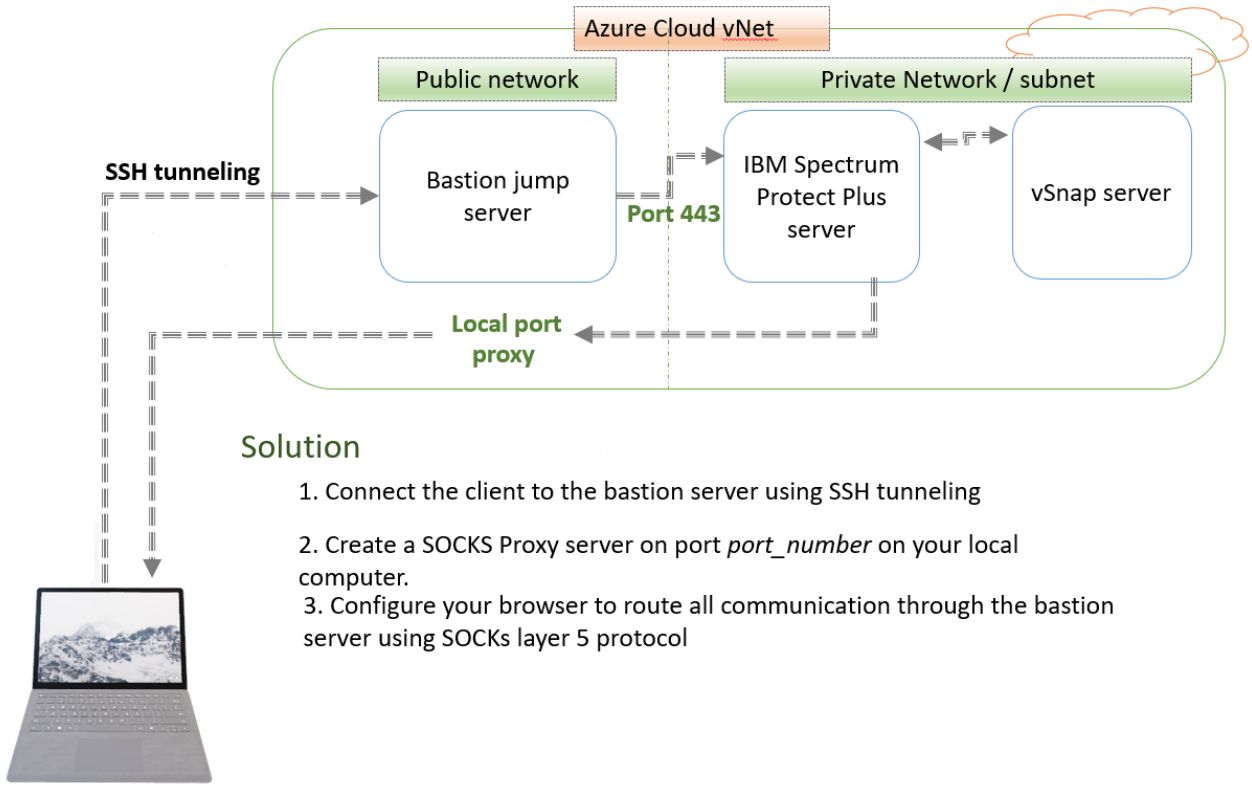


Figure 11. SSH tunneling

Procedure

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

1. Configure SSH dynamic port forwarding.

If SSH key authentication was chosen during deployment, enter the following command:

```
# ssh -i key_pair_file -D 1080 username@bastion-public-ip
```

If password authentication was selected during deployment, enter the following command:

```
# ssh -D 1080 username@bastion-public-ip
```

where:

The parameter *key_pair_file* is a .pem file that contains the private key that is required to connect to the Bastion host and the IBM Spectrum Protect Plus server and vSnap server instance.

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

2. Open a web browser.

   The following steps reflect Firefox. However, you can use any browser that supports proxy configuration.
3. Open **Options** in your browser.
4. Navigate to **Network Settings** and click **Settings**.
5. Configure the network settings to enable the proxy.
   a) Click **Manual proxy connection**.
   b) In the **SOCKS Host** field, enter `localhost`.
   c) In the **Port** field, enter `1080` (or the port number that you chose if other than 1080).
   d) In the **No proxy for** field, you can add internal sites for your organization that should not go through the Bastion host as a proxy server.
   e) Click **OK**. The networking settings are set and active.
6. Open a new web page and connect directly to the IBM Spectrum Protect Plus server 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.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open, LTO, and Ultrium are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Red Hat®, OpenShift®, Ansible®, and Ceph® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

A glossary is available with terms and definitions for the IBM Spectrum Protect family of products.

See the IBM Spectrum Protect glossary.

Index

SPP Reuse URLs

System requirements

System requirements

Creating catalog backup job

Permissions

Backing up the IBM Spectrum Protect Plus application

Adding a key

Adding a certificate

Backing up and restoring VMware data

Virtual machine privileges

Creating a user account for an individual user

SLA policies

Configuring global preferences

Managing SLA policies

Assigning a static IP address

VADP system requirements

Adding an access key

Installing a vSnap server

Tiering

Installing a physical vSnap

Creating jobs and job schedules

Job types

Product messages

Product Number: 5737-F11