# IBM Spectrum Protect Plus
# Version 10.1.1

*Installation and User's Guide*

**Note:**

Before you use this information and the product it supports, read the information in “Notices” on page 117.

**Third edition (May 2018)**

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

# Contents

# What's new in Version 10.1.1

IBM Spectrum Protect Plus Version 10.1.1 introduces new features and updates.

For a list of new features and updates in this release, see IBM Spectrum Protect Plus updates.

# Chapter 1. IBM Spectrum Protect Plus overview

IBM Spectrum Protect Plus is a data protection and availability solution for virtual environments that can be deployed in minutes and protect your environment within an hour.

IBM Spectrum Protect Plus can be implemented as a stand-alone solution or integrate with your IBM Spectrum Protect environment to offload copies for long-term storage and governance with scale and efficiency.

To access the IBM Spectrum Protect Plus online help system, click the user icon from any page in the user interface, and then select **Help**.

### Getting started

- For IBM Spectrum Protect Plus system requirements, see "System requirements" on page 5.
- For IBM Spectrum Protect Plus installation procedures, see "Installing IBM Spectrum Protect Plus as a VMware virtual appliance" on page 6 and "Installing IBM Spectrum Protect Plus as a Hyper-V virtual appliance" on page 7.
- To install virtual or physical vSnap backup destinations, see "Installing vSnap servers" on page 19.
- To configure VADP proxies, which enable load sharing and load balancing for jobs in Linux environments, see "Managing VADP backup proxies" on page 89.

## IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus is available as an IBM Cloud for VMware Solutions service, IBM Spectrum Protect Plus on IBM Cloud.

IBM Cloud for VMware Solutions enables you to integrate or migrate your on-premises VMware workloads to the IBM Cloud by using the scalable IBM Cloud infrastructure and VMware hybrid virtualization technology.

IBM Cloud for VMware Solutions provides the following major benefits:

**Global reach**
Expand your hybrid cloud footprint to up to 30 enterprise-class IBM Cloud datacenters around the world.

**Seamless integration**
Seamlessly integrate across the hybrid cloud with the IBM Cloud infrastructure.

**Rapid provisioning**
Quickly deploy an enterprise-class VMware environment with on-demand IBM Cloud Bare Metal Servers and virtual servers by using automated deployment and configuration of the VMware environment.

**Simplification**
Use a VMware cloud platform without identifying, procuring, deploying, and managing the underlying physical compute, storage, and network infrastructure, and software licenses.

**Expansion and contraction flexibility**
Easily expand and contract your VMware workloads according to your business needs.

**Single management console**
Use a single console to deploy, access, and manage the VMware environments on IBM Cloud.

### Available features in IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus supports both VMware and Microsoft Hyper-V environments.

However, IBM Spectrum Protect Plus on IBM Cloud supports only VMware environments.

This documentation includes topics about features that are specific to Hyper-V. These features are not available if you are using IBM Spectrum Protect Plus on IBM Cloud.

The current version of IBM Spectrum Protect Plus and IBM Spectrum Protect Plus on IBM Cloud might not be the same. To find the documentation for the version of IBM Spectrum Protect Plus on IBM Cloud that you are using, go to the online product documentation and select the product version.

**For more information**

For information about how to order, install, and configure IBM Spectrum Protect Plus on IBM Cloud, see the following documentation. An IBMid is required to access the documentation.

- Getting started with IBM Cloud for VMware Solutions
- Components and considerations for IBM Spectrum Protect Plus on IBM Cloud
- Managing IBM Spectrum Protect Plus on IBM Cloud

# Chapter 2. Dashboard

The dashboard displays an overview of your IBM Spectrum Protect Plus environment. Use the dashboard to quickly review the status of your jobs, backup storage utilization, and restore points.

The dashboard overview displays the number of protected and unprotected virtual machines and databases in your environment, along with the number of failed and running jobs Additional widgets include:

**Backup Storage Utilization**
This widget displays the usage of your available vSnap servers as well as their capacity. Additional vSnap servers can be added to the IBM Spectrum Protect Plus environment through the Backup Storage window.

**Backup Storage Summary**
This widget displays your data utilization and the total capacity of your backup storage. Additionally it displays these data reduction ratios:

**Data Deduplication Ratio**
The ratio of the amount of data that is protected compared with the physical space required to store it, due to removal of duplicates.

**Data Compression Ratio**
The ratio of the amount of data that is protected compared with the physical space required to store it, due to data compression.

**Protection by Policy**
This widget displays the total number of protected resources per SLA Policy. Use this widget to see an overview of your SLA Policy usage. The display includes SLA Policies that have been deleted but for which recovery points still exist.

**System Information**
This widget displays system resource utilization, including CPU, memory, Configuration, Recovery, and File Catalogs.

# Chapter 3. Installation and setup

The topics in the following section cover installing IBM Spectrum Protect Plus and system requirements.

## System requirements

Details of the system requirements can change over time. For current requirements, see technote 2013790.

This technote provides links to the following IBM Spectrum Protect Plus documents:

- System requirements
- File indexing and restore requirements
- Database backup and restore requirements

## Obtaining the IBM Spectrum Protect Plus installation files

You can obtain the IBM Spectrum Protect Plus installation files from an IBM download site. These packages contain a file that is required to install or update the IBM Spectrum Protect Plus components.

**Before you begin**

See technote 4044571 for the list of components.

**Procedure**

To run the installation files:

1. Download the appropriate installation files.

   Different installation files are provided for installation on VMware and Hyper-V systems and for installation on physical or virtual machines. Ensure that you download the correct files for your environment.
2. Follow the instructions in the installation or update topics for each component.

**Related tasks**

"Installing IBM Spectrum Protect Plus as a VMware virtual appliance" on page 6
To install IBM Spectrum Protect Plus in a VMware environment, deploy an OVF template. Deploying an OVF template creates a virtual appliance containing the application on a VMware host such as an ESX or ESXi server. To run IBM Spectrum Protect Plus, access the newly created virtual machine. A local vSnap server that is already named and registered is also installed on the virtual machine.

"Installing IBM Spectrum Protect Plus as a Hyper-V virtual appliance" on page 7
To install the IBM Spectrum Protect Plus in a Microsoft Hyper-V environment, import a Hyper-V template. Importing a template creates a virtual appliance containing the IBM Spectrum Protect Plus application on a Hyper-V virtual machine. A local vSnap server that is already named and registered is also installed on the virtual machine.

"Installing vSnap servers" on page 19
A vSnap server is as the primary backup destination for IBM Spectrum Protect Plus. In either a VMware or Hyper-V environment, one vSnap server with the name localhost is automatically installed at the time that the IBM Spectrum Protect Plus appliance is initially deployed. In larger backup enterprise environments, additional vSnap servers might be required.

"Updating the IBM Spectrum Protect Plus virtual appliance" on page 31
Use the IBM Spectrum Protect Plus administrative console to update the virtual appliance.

"Updating vSnap servers" on page 32

The default vSnap server is updated with the IBM Spectrum Protect Plus appliance. You must update additional vSnap servers that are installed on either virtual or physical appliances separately.

## Installing IBM Spectrum Protect Plus as a VMware virtual appliance

To install IBM Spectrum Protect Plus in a VMware environment, deploy an OVF template. Deploying an OVF template creates a virtual appliance containing the application on a VMware host such as an ESX or ESXi server. To run IBM Spectrum Protect Plus, access the newly created virtual machine. A local vSnap server that is already named and registered is also installed on the virtual machine.

**Before you begin**

Note the following procedures and considerations before installing IBM Spectrum Protect Plus:

- Review the IBM Spectrum Protect Plus system requirements. See technote 2013790.
- Download the `.ova` template installation file from Passport Advantage Online. For information about downloading files, see technote 4044571.
- Before deployment, run MD5 Checksum on the downloaded `.ova` file. Ensure that the generated checksum matches the one provided in the MD5 Checksum file, which is part of the software download.
- You might need to configure an IP address pool that is associated with the VM network where you plan to deploy IBM Spectrum Protect Plus. Correct configuration of the IP address pool includes the setup of IP address range (if used), netmask, gateway, DNS search string, and a DNS server IP address.
- To use DHCP instead of a static IP address, leave all fields blank when prompted to enter network properties. If you don't have access to a DHCP server and want to use a static IP address, assign a static IP by using the NetworkManager text user interface (nmtui) tool. For more information, see “Assigning a static IP address” on page 9.
- To change the IP address allocation type after IBM Spectrum Protect Plus deploys, redeploy the virtual machine.
- If the hostname of the IBM Spectrum Protect Plus appliance changes after deployment, either through user intervention or if a new IP address is acquired through DNS, the IBM Spectrum Protect Plus appliance must be restarted.
- For later versions of vSphere, the vSphere Web Client might be required to deploy IBM Spectrum Protect Plus appliances.
- IBM Spectrum Protect Plus has not been tested for IPv6 environments.

**Procedure**

To install IBM Spectrum Protect Plus as a virtual appliance, complete the following steps:

1. Use the vSphere Client to deploy IBM Spectrum Protect Plus. From the **File** menu, choose **Deploy OVF Template**. If using the vSphere Web Client, click **Create/Register VM**, then select **Deploy a virtual machine from an OFV or OVA file**. Click **Next**.
2. Specify the location of the `.ova` template installation file and select it. Click **Next**.
3. Review the template details and accept the End User License Agreement. Click **Next**.
4. Provide a meaningful name for the template, which becomes the name of your virtual machine. Identify an appropriate location to deploy the virtual machine. Click **Next**.
5. Identify the datacenter, server, and resource pool for deployment. When prompted to select storage, select from datastores already configured on the destination host. The virtual machine configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine and all of its virtual disk files. Click **Next**.
6. Select a disk format to store the virtual disks. It is recommended that you select thick provisioning, which is preselected for optimized performance. Thin provisioning requires less disk space, but may impact performance. Click **Next**.

7. Select networks for the deployed template to use. Several available networks on the ESX server may be available by clicking Destination Networks. Select a destination network that allows you to define the appropriate IP address allocation for the virtual machine deployment. Click **Next**.
8. Enter network properties for the virtual machine default gateway, DNS, IP address, and network prefix. It is recommended that you work with your network administrator when configuring network properties.

   If you are using DHCP instead of static IP address, bypass the fields in this dialog, and click **Next**. If you don't have access to a DHCP server and want to use a static IP address, assign a static IP by using the nmtui tool.

   Note that a default gateway must be configured properly before deployment. Multiple DNS strings are supported, and must be separated by commas without the use of spaces.

   The network prefix should be specified by a network administrator. The network prefix must be entered using CIDR notation; valid values are 1 - 32.
9. Click **Next**.
10. Review your template selections. Click **Finish** to exit the wizard and to start deployment of the OVF template. Deployment might take significant time.
11. After OVF template deployment completes, power on your newly created virtual machine. You can power on the virtual machine from the vSphere Client.

    **Important:** The virtual machine must remain powered on for the IBM Spectrum Protect Plus application to be accessible.
12. Record the IP address of the newly created virtual machine.

    The IP address is required to log on to the application. Find the IP address in vSphere Client by clicking your newly created virtual machine and looking in the **Summary** tab.

    **Important:** Wait several minutes for IBM Spectrum Protect Plus to initialize completely.

**What to do next**
After you install the virtual appliance, complete the following actions:

| Action | How to |
|---|---|
| If you use a static IP address instead of DHCP, restart the virtual appliance. | Refer to the documentation for the virtual appliance. |
| Upload the product key. | See “Uploading the product key” on page 9. |
| Start IBM Spectrum Protect Plus from a supported web browser. | See “Starting IBM Spectrum Protect Plus” on page 10. |

## Installing IBM Spectrum Protect Plus as a Hyper-V virtual appliance

To install the IBM Spectrum Protect Plus in a Microsoft Hyper-V environment, import a Hyper-V template. Importing a template creates a virtual appliance containing the IBM Spectrum Protect Plus application on a Hyper-V virtual machine. A local vSnap server that is already named and registered is also installed on the virtual machine.

**Before you begin**
Note the following procedures and considerations before installing IBM Spectrum Protect Plus:

- Review the IBM Spectrum Protect Plus system requirements. See technote 2013790.
- Download the `.exe` installation file from Passport Advantage Online. For information about downloading files, see technote 4044571.
- Review additional Hyper-V system requirements. See https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows.

- Before deployment, run MD5 Checksum on the downloaded installation file. Ensure the generated checksum matches the one provided in the MD5 Checksum file, which is part of the software download.
- Assign a static IP address by using the NetworkManager text user interface (nmtui) tool. For more information, see “Assigning a static IP address” on page 9.
- If the hostname of the IBM Spectrum Protect Plus appliance changes after deployment, either through user intervention or if a new IP address is acquired through DNS, the IBM Spectrum Protect Plus appliance must be restarted.
- All Hyper-V servers, including cluster nodes, must have the Microsoft iSCSI Initiator Service running in their Services list. Set the service to Automatic so that it is available when the machine boots.

**Procedure**

To install IBM Spectrum Protect Plus as a virtual appliance, complete the following steps:

1. Copy the `.exe` installation file to your Hyper-V server.
2. Start the installer and complete the installation steps.
3. Once complete, close the installer.
4. Open Hyper-V Manager and select the required server.
5. From the **Actions** menu in Hyper-V Manager, click **Import Virtual Machine**, then click **Next**. The Locate Folder dialog opens.
6. Browse to the location you designated during the installation and select the Virtual Machines folder.
7. Click **Next**. The Select Virtual Machine dialog opens.
8. Select **SPP-{release}**, then click **Next**. The Choose Import Type dialog opens.
9. Choose the following import type: **Register the virtual machine in place**. Click **Next**.
10. If the Connect Network dialog opens, specify the virtual switch to use, then click **Next**. The Completing Import dialog opens.
11. Review the description, then click **Finish** to complete the import process and close the Import Virtual Machine wizard. The virtual machine is imported.
12. Right-click the newly deployed VM, then click **Settings**.
13. Under the section named IDE Controller 0, select **Hard Drive**.
14. Click **Edit**, then click **Next**.
15. In the Choose Action screen, choose **Convert** then click **Next**.
16. For the Disk Format, choose **VHDX**.
17. For the Disk Type, choose **Fixed Size**.
18. For the Configure Disk option, give the disk a new name and optionally, a new location.
19. Review the description, then click **Finish** to complete the conversion.
20. Once the conversion completes, click **Browse**, then locate and select the newly created VHDX.
21. Repeat steps 15 through 20 for each disk under the SCSI Controller section.
22. Power on the virtual machine from the Hyper-V Manager.
23. Use Hyper-V Manager to identify the IP address of the new virtual machine if automatically assigned. To assign a static IP to the virtual machine, use the nmtui tool.

**What to do next**

After you install the virtual appliance, complete the following actions:

| Action | How to |
|---|---|
| Restart the virtual appliance. | Refer to the documentation for the virtual appliance. |
| Upload the product key. | See “Uploading the product key” on page 9. |

| Action | How to |
|---|---|
| Start IBM Spectrum Protect Plus from a supported web browser. | See “Starting IBM Spectrum Protect Plus” on page 10. |

When uninstalling IBM Spectrum Protect Plus in a Hyper-V environment, it is recommended to delete the IBM Spectrum Protect Plus appliance from Hyper-V first before running the uninstaller.

## Assigning a static IP address

If you do not have access to a DHCP server and want to use a static IP address for the installation of the virtual appliance, a network administrator can assign a static IP address by using the NetworkManager text user interface (nmtui) tool. Sudo privileges are required to run nmtui.

### Procedure

To assign a static IP address, ensure that the IBM Spectrum Protect Plus virtual machine is powered on and complete the following steps:

1. Log on to the virtual machine console as the root user.
   The initial root password is sppDP758.
2. From a CentOS command line, enter `nmtui` to open the interface.
3. From the main menu, select **Edit a connection**, and then click **OK**.
4. Select the network connection, then click **Edit**.
5. On the **Edit Connection** screen, enter an available static IP address that is not already in use.
6. Click **OK** to save the static IP configuration, then restart the IBM Spectrum Protect Plus appliance.

### Related tasks

“Installing IBM Spectrum Protect Plus as a VMware virtual appliance” on page 6
To install IBM Spectrum Protect Plus in a VMware environment, deploy an OVF template. Deploying an OVF template creates a virtual appliance containing the application on a VMware host such as an ESX or ESXi server. To run IBM Spectrum Protect Plus, access the newly created virtual machine. A local vSnap server that is already named and registered is also installed on the virtual machine.

“Installing IBM Spectrum Protect Plus as a Hyper-V virtual appliance” on page 7
To install the IBM Spectrum Protect Plus in a Microsoft Hyper-V environment, import a Hyper-V template. Importing a template creates a virtual appliance containing the IBM Spectrum Protect Plus application on a Hyper-V virtual machine. A local vSnap server that is already named and registered is also installed on the virtual machine.

## Uploading the product key

A valid product key is required to access IBM Spectrum Protect Plus and all of its features

### Before you begin

Save the product key to a computer with Internet access and record the location of the key.

### Procedure

To upload the product key, complete the following steps:

1. From a supported browser, enter the following URL:

   ```
   https://HOSTNAME:8090/
   ```

   Where *HOSTNAME* is the IP address of the virtual machine where the application is deployed.

2. In the login window, select **Authentication Type** > **System**. Enter your password to access the Administration Console. The default password is sppadLG235.

   You are prompted to enter a new password to access the Administrative Console upon first log in.

   **Installing IBM**
3. Click **Manage your licenses**.
4. Click **Choose File**, and then browse for the product key on your computer,
5. Click **Upload new license**.
6. Click **Logout**.

**What to do next**
After you upload the product key, complete the following action:

| Action | How to |
|---|---|
| Start IBM Spectrum Protect Plus from a supported web browser. | See "Starting IBM Spectrum Protect Plus" on page 10. |

## Starting IBM Spectrum Protect Plus

Launch IBM Spectrum Protect Plus to begin using the application and its features.

**Before you begin**
Note the following considerations before starting IBM Spectrum Protect Plus:

- IBM Spectrum Protect Plus must be installed prior to starting the application.
- The System Administrator must provide you with the IP address for the virtual appliance and the IBM Spectrum Protect Plus user name and password.

**Procedure**

To start IBM Spectrum Protect Plus, complete the following steps:

1. In a supported web browser, enter the following URL:

   ```
   https://host_name
   ```

   Where *host_name* is the IP address of the virtual machine where the application is deployed. This connects you to IBM Spectrum Protect Plus.
2. In the logon dialog, enter your user name and password. If this is your first time logging on to IBM Spectrum Protect Plus, the initial user name is `admin` and the initial password is `password`. You will be prompted to reset the default admin password.
3. Click **Sign In**. The application launches.

   A vSnap server serves as a backup target, and is required to perform backup and restore jobs. By default, a vSnap installation is present on the IBM Spectrum Protect Plus appliance. Before the storage can be used, additional software components will be initialized and a storage pool will be created. You will be prompted to start the vSnap initialization process upon first login to the user interface. For more information about vSnap installations, see "Installing vSnap servers" on page 19.

**Related tasks**
"Installing IBM Spectrum Protect Plus as a VMware virtual appliance" on page 6
To install IBM Spectrum Protect Plus in a VMware environment, deploy an OVF template. Deploying an OVF template creates a virtual appliance containing the application on a VMware host such as an ESX or ESXi server. To run IBM Spectrum Protect Plus, access the newly created virtual machine. A local vSnap server that is already named and registered is also installed on the virtual machine.

"Installing IBM Spectrum Protect Plus as a Hyper-V virtual appliance" on page 7

To install the IBM Spectrum Protect Plus in a Microsoft Hyper-V environment, import a Hyper-V template. Importing a template creates a virtual appliance containing the IBM Spectrum Protect Plus application on a Hyper-V virtual machine. A local vSnap server that is already named and registered is also installed on the virtual machine.

## Configuring SLA policies

SLA Policies allow administrators to create customized templates for the key processes involved in the creation and use of Backup jobs. Parameters are configured in SLA Policies, which can be used and re-used in Backup jobs.

### Before you begin

If a virtual machine is associated with multiple SLA Policies, ensure that the policies are not scheduled to run concurrently. Either schedule the SLA Policies to run with a significant amount of time between them, or combine them into a single SLA Policy.

### Procedure

To create an SLA policy, complete the following steps:

1. From the navigation menu, click **SLA Policy**.
2. Click the add icon . The New SLA Policy pane opens.
3. In the **Name** field, enter a name that provides a meaningful description of the SLA Policy.
4. In the **Backup Storage** section, define the recovery point objective to determine the frequency and interval with which backups must be made. In the **Retention** field, enter the number of copies to keep either by number of days or number of snapshots. In the **Frequency** field, set the backup frequency and interval.
5. In the **Target Site** field, select a primary or secondary backup destination. Target sites are designated as primary or secondary through the Backup Storage pane. If more than one Primary or Secondary Backup Storage is available to IBM Spectrum Protect Plus, the vSnap backup destination with the largest amount of available storage will be used first.
6. Expand the **Backup Storage Replication** section to display replication options.

   Backup storage replication allows you to complete asynchronous replication of backup data from one vSnap server, such as the primary site, to another, such as the secondary site.
7. Select **Enable Backup Storage Replication**, and complete the following fields:

   **Frequency**

   Enter the backup frequency and interval through the associated menus.

   **Target Site**

   Select a replication target site.

   **Same retention as source selection**

   Select to use the same retention as the source vSnap server. Clear this option to set a new retention schedule.

   Replication partnerships are established through the **Backup Storage** pane. For more information, see “Establishing a replication partnership for a vSnap server” on page 26.

   To create one-to-many replication scenarios, where a single set of backup data is replicated to multiple vSnap servers, create multiple SLA policies for each replication site. In each SLA Policy, set the Backup Storage Target to the primary site, then set each Backup Storage Replication Target Site to the available replication sites.
8. Expand the **IBM Spectrum Protect Offload** section to display IBM Spectrum Protect offload options.

Offloading essentially creates two backups of your data – one on the vSnap server for short term protection, and one on the IBM Spectrum Protect server for longer term protection. Select **Offload to IBM Spectrum Protect** to enable offloading. Enter the backup frequency and interval through the associated pulldown menus.

If **Leverage most recent backup** is selected, the offload occurs from the ESX original host or cluster directly, and the latest backup image on the vSnap server is mounted. Note that incremental backups are not supported if selected.

**Important:** Microsoft Hyper-V is not currently supported for offloading.

9. When you are satisfied that the SLA Policy-specific information is correct, click **Save**. The SLA Policy can now be applied to Backup job definitions.

**What to do next**

After you create an SLA policy, complete the following actions:

| Action | How to |
|---|---|
| Assign user permissions to the SLA policy. | See "Creating a user role" on page 110. |
| Create a Backup job definition that utilizes the SLA policy. | See "Creating a VMware backup job" on page 43 or "Creating a Hyper-V backup job" on page 54. |

**Related concepts**

"Offloading to IBM Spectrum Protect " on page 12

IBM Spectrum Protect Plus contains built-in capabilities surrounding long term retention. The protection policies of IBM Spectrum Protect Plus leverage those capabilities.

## Offloading to IBM Spectrum Protect

IBM Spectrum Protect Plus contains built-in capabilities surrounding long term retention. The protection policies of IBM Spectrum Protect Plus leverage those capabilities.

IBM Spectrum Protect Plus enables users to easily create protection policies that address scheduling, RPO's, retention, and other parameters. When defining a protection policy in IBM Spectrum Protect Plus, the user has the option to offload the snapshots to IBM Spectrum Protect, essentially creating two backups of the data – one on the vSnap server, and one on the IBM Spectrum Protect server for longer term protection.

Two methods for offloading are available.

**Method 1**

With the default method (method 1), the offload happens from the hypervisor directly. Incremental backups are supported.

**Method 2**

With the alternative method (method 2), the offload happens from the vSnap server. Incremental backups are not supported.

The decision regarding which offload method to choose is based upon use case and environment. Factors to consider include speed, impact on production hypervisor servers, and storage needs.

**Important:** Microsoft Hyper-V is not currently supported for offload for either method.

To indicate that a backup snapshot is to be offloaded, select the **Offload to IBM Spectrum Protect** method on the IBM Spectrum Protect Plus SLA Policy screen. A dialog requesting details about the offload method, the offload backup schedule, and retention parameters opens.

**Important:**

- Review the IBM Spectrum Protect for Virtual Environments vmname restrictions for the vmcli Backup command. Go to the online product documentation, select the product version, and type `backup command` in the **Search IBM Knowledge Center** field.
- Review unsupported characters in VM or datacenter names. Go to the online product documentation, select the product version, and type `troubleshooting` in the **Search IBM Knowledge Center** field.
- The user that registers the IBM Spectrum Protect for Virtual Environments server in IBM Spectrum Protect Plus must have "Log on as a service" rights enabled to run remote commands. For more information about the "Log on as a service" right, see https://technet.microsoft.com/en-us/library/cc794944.aspx.
- Your IBM Spectrum Protect server and data mover should be configured with the same time zone.
- Offloading requires that vCenters and IBM Spectrum Protect for Virtual Environments are registered in IBM Spectrum Protect Plus as a pair, or configured so that all datacenters in vCenter are registered in IBM Spectrum Protect for Virtual Environments. The scope for offloaded backups is limited to the vCenter configured with the IBM Spectrum Protect for Virtual Environments server. Backups and restores are limited to the same vCenter. Alternatively, virtual machines selected for backup should be restricted to the datacenters configured in IIBM Spectrum Protect for Virtual Environments.
- A single data mover supports one command at a time. If a data mover is performing a backup operation, it cannot perform a restore operation until the backup operation completes.
- A single data mover supports one command at a time, but can support multiple virtual machines. When selecting multiple virtual machines for offloading, select the virtual machines from a single datacenter per policy. The virtual machines will be distributed among the available datamovers, and will offload in a parallel sequence. If creating multiple offload jobs for virtual machines on the same datacenter, schedule the jobs so that they do not overlap.
- For Linux-based IBM Spectrum Protect for Virtual Environments servers, the user must have sufficient permissions to run a shell as the tdpvmware user. Typically, root is used as the user when registering a Linux-based IBM Spectrum Protect for Virtual Environments server.
- To enable back up and offloading of virtual machine templates, you must include the VMENABLETEMPLATEBACKUPS option in the data mover options file. A backup of a templates can be completed only as a Full type backup. For more information about configuring your environment for backing up virtual machine templates, see Vmenabletemplatebackups.
- Instant Disk Restore jobs utilizing offloading are not supported.

The following concepts summarize the salient points about the IBM Spectrum Protect Plus offload operation:

**Backup**

- The vSnap server is the primary target for IBM Spectrum Protect Plus backups.
- An IBM Spectrum Protect server is the target for offloaded IBM Spectrum Protect Plus backups.
- IBM Spectrum Protect Plus triggers the offload operation. If you select offload method 1, the offload happens from the hypervisor directly. If you select offload method 2, the offload happens from the vSnap server. Method 1 is the default.
- The offload operation uses data movers from IBM Spectrum Protect for Virtual Environments configured nodes, not VADP proxies.
- IBM Spectrum Protect Plus records the offloaded backup in its catalog.
- For primary backups and for backups using offload method 1, block level incremental backups are supported. For offloaded backups using method 2, all backups are full backups.

**Restore**

- Both restores from vSnap and recoveries of offloaded data are triggered from IBM Spectrum Protect Plus.
- IBM Spectrum Protect Plus is used to restore the snapshots from vSnap to the original or alternate hypervisor.

- IBM Spectrum Protect for Virtual Environments is used to recover snapshots from IBM Spectrum Protect servers to the original or alternate hypervisor.
- When restoring from an offload-based SLA Policy, you must select specific recovery points. Offload-based restores are not compatible with “Use latest version” recovery points.

**Related tasks**

“Configuring SLA policies” on page 11
SLA Policies allow administrators to create customized templates for the key processes involved in the creation and use of Backup jobs. Parameters are configured in SLA Policies, which can be used and re-used in Backup jobs.

## Setting up Data Protection for VMware for integration with IBM Spectrum Protect Plus

Use a checklist to guide you through the tasks that are required to set up IBM Spectrum Protect for Virtual Environments: Data Protection for VMware for use with IBM Spectrum Protect Plus.

It is assumed that IBM Spectrum Protect Plus and the IBM Spectrum Protect server are operational and that you have an understanding of these applications.

For information about Data Protection for VMware, see the online product documentation.

**Deployment checklist**

| | Action | Description |
|---|---|---|
| ☐ | Download the IBM Spectrum Protect for Virtual Environments: Data Protection for VMware installation package. | Obtain the installation package from the Passport Advantage Online web site.<br>**Related documentation**<br>Obtaining the Data Protection for VMware installation package |
| ☐ | Determine the number of data movers that are required to protect your vSphere environment. | A data mover is a software component of Data Protection for VMware that moves data to and from the IBM Spectrum Protect server. Multiple data movers might be required to protect your vSphere environment.<br>To determine the number of data movers that are required, see technote 2007197. This technote also includes considerations for using virtual or physical machines for data movers and for data mover locality.<br>**Related documentation**<br>How IBM Spectrum Protect nodes are used in a virtual environment |
| ☐ | Review the hardware and software requirements for the Data Protection for VMware components | To view the hardware and software requirements for the Data Protection for VMware components:<br>1. Go to the product Support Portal and type `all requirements` in the search field.<br>2. Open the *IBM Spectrum Protect for Virtual Environments - All Requirements Doc* to find links to system requirements by version.<br>**Related documentation**<br>Planning to install Data Protection for VMware |

| | Action | Description |
|---|---|---|
| ☐ | Contact your IBM Spectrum Protect server administrator to create a policy domain for use with IBM Spectrum Protect Plus | The policy domain specifies the number of days to retain backup and archive copies on the server storage. Contact your IBM Spectrum Protect server administrator to create a policy domain. |
| ☐ | Install Data Protection for VMware | To install Data Protection for VMware:<br>1. Start the installation program by using the instructions for your operating system:<br>• **Windows:** Double-click the spinstall.exe file.<br>• **Linux:** From the root of the installation folder, change directories to `CD/Linux/DataProtectionForVMware`.<br>From a command line, enter the following command:<br>`./install-Linux.bin`<br>2. In the installation wizard, select **Typical Installation** for Windows operating systems or **Complete** from the **Install Set** list for Linux operating systems and follow the steps in the wizard to complete the installation.<br>**Related documentation**<br>Installing the Data Protection for VMware components |
| ☐ | Configure Data Protection for VMware | When the installation wizard completes, the Data Protection for VMware vSphere GUI configuration wizard opens to enable you to set up communication with the IBM Spectrum Protect server.<br>Follow the instructions in the wizard to complete the configuration. For additional assistance using the configuration wizard, refer to the GUI help.<br>**Tips:**<br>• During the configuration, you are asked to specify the nodes that are used in your Data Protection for VMware environment. On the **Node Definition Options** page of the configuration wizard, you can enter a prefix to identify the nodes as common nodes. For example, you could enter ISPP for IBM Spectrum Protect Plus. On all node configuration pages of the wizard, the prefix is automatically added to the node name.<br>You also use the **Node Definition Options** page to select the policy domain to use when registering new nodes. Use the domain that your IBM Spectrum Protect server administrator created for IBM Spectrum Protect Plus.<br>• You define the data mover or data movers for your environment on the **Data Mover Nodes** page of the configuration wizard.<br>**Related documentation**<br>Configuring a new installation with the wizard |

| | Action | Description |
|---|---|---|
| ☐ | Install and configure additional data movers on remote systems if required | You can install data movers on remote systems to redistribute the backup workload among multiple systems.<br>To install a data mover on a remote system:<br>1. Start the Data Protection for VMware installation program and complete the following steps for your operating system:<br>• **Windows:** Select **Advanced Installation** > **Install the data mover or mount proxy** in the configuration wizard.<br>• **Linux:** Select **Custom** from the **Install Set** list in the configuration wizard. Ensure that **Data Protection for VMware data mover** is selected. This option is selected by default.<br>2. When the installation is complete, follow the instructions in Setting up the data mover nodes in a vSphere environment to set up the data movers. |
| ☐ | Start IBM Spectrum Protect Plus | To start IBM Spectrum Protect Plus:<br>1. Open a web browser and enter the URL for the virtual machine where IBM Spectrum Protect Plus is deployed. For example:<br>`http://hostname`<br>Where hostname is the IP address of the virtual machine.<br>2. Enter your user name and password. If you are logging on to IBM Spectrum Protect Plus for the first time, the initial user name is `admin` and the initial password is `password`. You will be prompted to reset the default password.<br>3. Click **Sign in**.<br>**Related documentation**<br>“Starting IBM Spectrum Protect Plus” on page 10 |

| | Action | Description |
|---|---|---|
| ☐ | Define the IBM Spectrum Protect server to use for offload operations | Offloading data to the IBM Spectrum Protect server provides long-term data protection in addition to the short-term protection provided by backup to the vSnap server.<br>To specify the IBM Spectrum Protect server that you want to use for offloading data from a vCenter:<br>1. From the navigation menu in the IBM Spectrum Protect Plus GUI, expand **Hypervisor** > **VMware**, and then click **Backup**.<br>2. Click **Manage vCenter**, and then click the add icon  .<br>3. In the **vCenter Properties** pane, complete the fields to add a vCenter.<br>4. Expand **IBM Spectrum Protect vStorage Backup Server Settings**.<br>5. Click **Link to IBM Spectrum Protect** and enter the information for the vStorage Backup Server.<br>**Related documentation**<br>"Offloading to IBM Spectrum Protect " on page 12<br>"Adding a VMware provider" on page 36 |
| ☐ | Create an SLA policy that includes offloading to the IBM Spectrum Protect server | SLA policies allow storage and virtualization administrators to create customized templates for the key processes that are involved in the creation and use of backup jobs.<br>To configure and SLA policy that offloads to the IBM Spectrum Protect server:<br>1. From the navigation menu in the IBM Spectrum Protect Plus GUI, click **SLA Policy**, and then click the add icon  .<br>2. In the **New SLA Policy** pane, configure the backup retention, frequency, and target site settings.<br>**Tip:** If **Offload to IBM Spectrum Protect** is selected, IBM Spectrum Protect Plus offloads data to the IBM Spectrum Protect server. The retention policy that is defined in the server policy domain created by your IBM Spectrum Protect server administrator is used for offloads to the server rather than the policy that is set in the **Retention** field. The policy in the **Retention** field applies only to backups to the vSnap server.<br>3. Expand **IBM Spectrum Protect Offload**, and click **Offload to IBM Spectrum Protect**.<br>4. Set the frequency for offloading data to the IBM Spectrum Protect server.<br>5. If **Leverage most recent backup** is selected, the offload occurs from the ESX original host or cluster directly, and the latest backup image on the vSnap server is mounted. Note that incremental backups are not supported if this option is selected.<br>**Related documentation**<br>"Configuring SLA policies" on page 11. |

| | Action | Description |
|---|---|---|
| ☐ | Create a backup job definition that uses the SLA policy | To create a backup job definition that uses the SLA policy:<br>1. From the navigation menu in the IBM Spectrum Protect Plus GUI, expand **Hypervisor** > **VMware**, and then click **Backup**.<br>2. Select a vCenter and click **Select SLA Policy** to add the SLA policy to the job definition<br>**Related documentation**<br>“Creating a VMware backup job” on page 43. |

# Chapter 4. vSnap installation and setup

Every installation of IBM Spectrum Protect Plus requires at least one vSnap server. The vSnap server serves as the primary backup destination. Disk storage is connected to the vSnap servers.

In either a VMware or Hyper-V environment, one vSnap server with the name localhost is automatically installed at the time that the IBM Spectrum Protect Plus appliance is initially deployed. The default vSnap server resides on a partition of the IBM Spectrum Protect Plus appliance. The default vSnap server is registered in IBM Spectrum Protect Plus and initialized as well. In smaller backup environments, that default vSnap server might be sufficient.

In larger backup enterprise environments, additional vSnap servers might be required. These can be installed on either virtual or physical appliances any time after the IBM Spectrum Protect Plus appliance is installed and deployed. After installation, some registration and configuration steps are required for these stand-alone vSnap servers.

In summary, the process for setting up a stand-alone vSnap server is:

- Install the vSnap server
- Register the vSnap server as a backup storage target in IBM Spectrum Protect Plus
- Initialize the system and create a storage pool

**Note:** If performing a custom (non-OVA) installation to a VMware virtual machine, the virtual disk UUIDs must be visible to the operating system in order for vSnap to detect the disks and use them in a storage pool. Edit the VM settings, add the advanced configuration parameter **disk.enableUUID** and set its value to **TRUE**.

## Installing vSnap servers

A vSnap server is as the primary backup destination for IBM Spectrum Protect Plus. In either a VMware or Hyper-V environment, one vSnap server with the name localhost is automatically installed at the time that the IBM Spectrum Protect Plus appliance is initially deployed. In larger backup enterprise environments, additional vSnap servers might be required.

**Before you begin**

Review the vSnap system requirements. See technote 2013790.

Download the installation file. Different installation files are provided for installation on physical or virtual machines. Ensure that you download the correct files for your environment. For information about downloading files, see technote 4044571.

### Installing a physical vSnap server in a VMware or Hyper-V environment

A Linux operating system that supports physical vSnap installations is required to install a vSnap server on a physical machine.

**Procedure**

To install a physical vSnap server:

1. Install a Linux operating system that supports physical vSnap installations. See technote 2013790 for system requirements.

   The minimal install configuration is sufficient, but you can also install additional packages including a graphical user interface (GUI). The root partition must have at least 8 GB of free space after installation.
2. Edit the file `/etc/selinux/config`, change the SELinux mode to Permissive.
3. Run `setenforce 0` to apply the setting immediately without requiring a restart.

4. Download the vSnap `.run` installation file from Passport Advantage Online. For information about downloading files, see technote 4044571.
5. Before running the vSnap installation file, ensure that your system is up to date by running the **`yum update`** command.
6. Make the file executable through the command `chmod +x` *`file_name`*`.run`, and then run the executable. The vSnap packages are installed, plus all of dependencies.

**What to do next**

After you install the vSnap server, complete the following action:

| Action | How to |
|---|---|
| Configure the vSnap environment | See "Configuring the vSnap environment" on page 22. |

## Installing a virtual vSnap server in a VMware environment

To install a vSnap server in a VMware environment, deploy an OVF template. This creates a virtual appliance containing the vSnap server on a Hyper-V virtual machine.

**Procedure**

To install vSnap server in a VMware environment:

1. Download the `.ova` template installation file from Passport Advantage Online. For information about downloading files, see technote 4044571
2. Use the vSphere Client to deploy the vSnap server. From the **File** menu, choose **Deploy OVF Template**. If using the vSphere Web Client, click **Create/Register VM**, then select **Deploy a virtual machine from an OFV or OVA file**. Click **Next**.
3. Specify the location of the IBM Spectrum Protect Plus OVA template installation file and select it. Click **Next**.
4. Review the template details and accept the End User License Agreement. Click **Next**.
5. Provide a meaningful name for the template, which becomes the name of your virtual machine. Identify an appropriate location to deploy the virtual machine. Click **Next**.
6. Identify the datacenter, server, and resource pool for deployment. When prompted to select storage, select from datastores already configured on the destination host. The virtual machine configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine and all of its virtual disk files. Click **Next**.
7. Select a disk format to store the virtual disks. It is recommended that you select thick provisioning, which is preselected for optimized performance. Thin provisioning requires less disk space, but may impact performance. Click **Next**.
8. Select networks for the deployed template to use. Several available networks on the ESX server may be available by clicking Destination Networks. Select a destination network that allows you to define the appropriate IP address allocation for the virtual machine deployment. Click **Next**.
9. Enter network properties for the virtual machinedefault gateway, DNS, IP address, and network prefix. It is recommended to work with your network administrator when configuring network properties.

   If you are using DHCP instead of static IP address, bypass the fields in this dialog, and click **Next**. If you don't have access to a DHCP server and want to use a static IP address, assign a static IP by using the NetworkManager text user interface (nmtui) tool. For more information, see "Assigning a static IP address" on page 9.

   Note that a default gateway must be configured properly before deployment. Multiple DNS strings are supported, and must be separated by commas without the use of spaces.

   The network prefix should be specified by a network administrator. The network prefix must be entered using CIDR notation; valid values are 1 - 32.

10. Click **Next**.
11. Review your template selections. Click **Finish** to exit the wizard and to start deployment of the OVF template. Deployment might take significant time.
12. After OVF template deployment completes, power on your newly created virtual machine. You can power on the virtual machine from the vSphere Client.

    **Important:** The virtual machine must remain powered on for the IBM Spectrum Protect Plus application to be accessible.
13. Record the IP address of the newly created virtual machine.

    The IP address is required to access and register the vSnap server. Find the IP address in vSphere Client by clicking your newly created virtual machine and looking in the **Summary** tab.

**What to do next**

After you install the vSnap server, complete the following action:

| Action | How to |
|---|---|
| Configure the vSnap environment | See "Configuring the vSnap environment" on page 22. |

## Installing a virtual vSnap server in a Hyper-V environment

To install a vSnap server in a Hyper-V environment, import a Hyper-V template. This creates a virtual appliance containing the vSnap server on a Hyper-V virtual machine.

**Before you begin**

All Hyper-V servers, including cluster nodes, must have the Microsoft iSCSI initiator service running in their Services list. Set the service to Automatic so that it is available when the machine is restarted.

**Procedure**

To install vSnap server in a Hyper-V environment:

1. Download the `.exe` vSnap installation file from Passport Advantage Online. For information about downloading files, see technote 4044571.
2. Copy the installation file to your Hyper-V server.
3. Start the installer and complete the installation steps.
4. Once complete, close the installer.
5. Open Hyper-V Manager and select the required server. For Hyper-V system requirements see https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows.
6. From the **Actions** menu in Hyper-V Manager, click **Import Virtual Machine**, then click **Next**. The Locate Folder dialog opens.
7. Browse to the location of the Virtual Machines folder within the unzipped vSnap folder. Click **Next**. The Select Virtual Machine dialog opens.
8. Select vSnap, then click **Next**. The Choose Import Type dialog opens.
9. Choose the following import type: **Register the virtual machine in place**. Click **Next**.
10. If the Connect Network dialog opens, specify the virtual switch to use, then click **Next**. The Completing Import dialog opens.
11. Review the description, then click **Finish** to complete the import process and close the Import Virtual Machine wizard. The virtual machine is imported.
12. Right-click the newly deployed VM, then click **Settings**.
13. Under the section named IDE Controller 0, select **Hard Drive**.
14. Click **Edit**, then click **Next**.
15. In the Choose Action screen, choose **Convert** then click **Next**.

16. For the Disk Format, choose **VHDX**.
17. For the Disk Type, choose **Fixed Size**.
18. For the Configure Disk option, give the disk a new name and optionally, a new location.
19. Review the description, then click **Finish** to complete the conversion.
20. Once the conversion completes, click **Browse**, then locate and select the newly created VHDX.
21. Repeat steps 13 through 19 for each disk under the SCSI Controller section.
22. Power on the virtual machine from the Hyper-V Manager. If prompted, select the option where the kernel boots in rescue mode.
23. Use Hyper-V Manager to identify the IP address of the new virtual machine if automatically assigned. To assign a static IP to the virtual machine using NetworkManager Text User Interface, see the following section.
24. Use Hyper-V Manager to identify the IP address of the new virtual machine if automatically assigned. To assign a static IP to the virtual machine, use the NetworkManager text user interface (nmtui) tool. For more information, see "Assigning a static IP address" on page 9.

**What to do next**
After you install the vSnap server, complete the following action:

| Action | How to |
|---|---|
| Configure the vSnap environment | See "Configuring the vSnap environment" on page 22. |

When uninstalling IBM Spectrum Protect Plus in a Hyper-V environment, it is recommended to delete the IBM Spectrum Protect Plus appliance from Hyper-V first before running the uninstaller.

# Configuring the vSnap environment

Before you can use a new installation of vSnap, you must complete initial configuration tasks.

## Registering the vSnap server as a backup storage target

The default, or on-board, vSnap server is registered in IBM Spectrum Protect Plus with the name localhost when the appliance is deployed. You must register additional vSnap servers that are installed on either virtual or physical appliances.

**Procedure**

To register the vSnap server, complete the following steps:

1. Log in to the vSnap server console as the root user and run the **`vsnap user create`** command. The initial root password is sppDP758.
2. Enter a user name and password when prompted.
3. Log in to the IBM Spectrum Protect Plus user interface. From the navigation menu select **Backup Storage**, then register the vSnap server using the credentials of this new user. For more information, see "Adding a vSnap server as a backup storage provider" on page 24.

## Initializing the vSnap system

The initialization process prepares a new vSnap system for use by loading and configuring software components and initializing the internal configuration. This is a one-time process that you must run only for new installations.

### About this task

As part of the initialization process, vSnap creates a storage pool using any available unused disks on the system. The OVA-based deployments of vSnap each contain a default 100 GB unused virtual disk which is used to create the pool.

If no unused disks are found, the initialization process completes without creating a pool.

For information about how to expand, create, and administer storage pools, see "Storage management" on page 27.

### Completing a simple initialization

The following is the recommended procedure for initializing virtual deployments of vSnap.

### Procedure

1. Log in to the IBM Spectrum Protect Plus user interface.
2. For the default on-board vSnap installation that is registered as part of an IBM Spectrum Protect Plus installation, you are prompted to start the initialization process the first time you log in to the user interface. No further steps are required.
3. For any other vSnap servers, register the servers as described in "Registering the vSnap server as a backup storage target" on page 22, then from the **Actions** menu, select **Initialize** for each server.

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

### Completing an advanced initialization

The following is the recommended procedure for initializing physical deployments of vSnap. It gives you the flexibility of creating a storage pool using advanced redundancy options and a specific list of disks.

### Procedure

1. Log in to the vSnap server console as the root user (or alternatively, as the user you created previously using the **`vsnap user create command`**). The initial root password is sppDP758.
2. Run the **`vsnap system init --skip_pool`** command. The command requires no further interaction and performs all initialization tasks except for the creation of a storage pool. The process might take 5 - 10 minutes to complete.

### What to do next

After you complete the initialization, complete the following action:

| Action | How to |
|---|---|
| Create a storage pool | See "Storage management" on page 27. |

# Managing vSnap servers

To enable Backup and Restore jobs, at least one IBM Spectrum Protect Plus appliance and at least one vSnap server is required. The vSnap server can be located on the IBM Spectrum Protect Plus appliance or on its own appliance, or it can be a physical vSnap installation. Each vSnap server location must be added so that IBM Spectrum Protect Plus recognizes it.

## Adding a vSnap server as a backup storage provider

In larger backup enterprise environments, additional vSnap servers might be required. These can be installed on either virtual or physical appliances any time after the IBM Spectrum Protect Plus appliance is installed and deployed.

### Before you begin

After you add a vSnap server as a backup storage provider, you might have to configure and administer certain aspects of vSnap, such as network configuration or storage pool management. For more information, see “vSnap server administration reference ” on page 26.

### Procedure

To add a vSnap server as a backup storage device, complete the following steps:

1. From the navigation menu, click **Backup Storage**.
2. Click the add icon  .
3. Complete the fields in the **Storage Properties** pane:

   **Hostname/IP**

   Enter the resolvable IP address or hostname of the backup storage.

   **Site**

   Select a site for the backup storage. Available options are **Primary**, **Secondary**, or **Add a new site**. If more than one primary, secondary, or user-defined site is available to IBM Spectrum Protect Plus, the site with the largest amount of available storage is used first.

   **Username**

   Enter your username for the backup storage device.

   **Password**

   Enter your password for the backup storage device.
4. Click **Save**.

   IBM Spectrum Protect Plus confirms a network connection and adds the backup storage device to the database.
5. From the **Actions** menu associated with the newly added backup storage device, select **Initialize**. The initialization process runs in the background and requires no further user interaction. Note that the process might take 5 - 10 minutes to complete.

### What to do next

After you add a backup storage provider, complete the following action:

| Action | How to |
|---|---|
| Expand the vSnap storage pool. | See “Expanding a vSnap storage pool” on page 25. |
| After you add a vSnap server as a backup storage provider, you might have to configure and administer certain aspects of vSnap, such as network configuration or storage pool management. | “vSnap server administration reference ” on page 26 |

### Related tasks

“Creating a VMware backup job” on page 43

Use a Backup job to back up VMware data including virtual machines, datastores, folders, vApps, and datacenters with snapshots.

"Creating a Hyper-V backup job" on page 54
Use a Backup job to backup Hyper-V data with snapshots.

## Setting vSnap storage options

You can set additional storage-related options for a vSnap server.

### Procedure

To set the options for a vSnap server, complete the following steps:

1. From the navigation menu, click **Backup Storage**.
2. Click the manage icon that is associated with the vSnap server, and then expand the **Storage Options** section. Set the storage options.

   **Enable Compression**

   If enabled, each incoming block of data is compressed using a compression algorithm before it is written to the storage pool. Compression consumes a moderate amount of additional CPU resources.

   **Enable Deduplication**

   If enabled, each incoming block of data is hashed and compared against existing blocks in the storage pool. If compression is enabled, the data is compared after it is compressed. Duplicate blocks are skipped instead of being written to the pool. Deduplication is disabled by default because it consumes a large amount of memory resources (proportional to the amount of data in the pool) to maintain the deduplication table of block hashes.

   **Synchronous Write Mode**

   Disabling synchronous writes can lead to data loss and silent corruption of backup data if the storage server experiences an abrupt shutdown or reboot during a backup job. Do not disable this option unless the storage server resides in a stable environment that is adequately secured against hardware and power failures.
3. Click **Save**.

## Expanding a vSnap storage pool

To expand a vSnap storage pool, you must first add virtual or physical disks on the vSnap server, either by adding virtual disks to the vSnap virtual machine or adding physical disks to the vSnap physical server. See vSphere documentation for information about creating additional virtual disks.

### Procedure

To set the expand a vSnap storage pool, complete the following steps:

1. From the navigation menu, click **Backup Storage**.
2. Select **Actions** > **Rescan** for the vSnap server that you want to rescan.
3. Click the manage icon that is associated with the vSnap server, and then expand the **Add New Disks to Backup Storage** section.
4. Add and save the selected disks. The vSnap pool expands by the size of the disks that are added.

## Establishing a replication partnership for a vSnap server

Backup storage replication allows you to perform asynchronous replication of backup data from one vSnap server to another.

### Before you begin

Backup storage replication is enabled through SLA policies by selecting **Enable Backup Storage Replication**. For more information, see "Configuring SLA policies" on page 11.

### Procedure

To set the establish a replication partnership, complete the following steps:

1. From the navigation menu, click **Backup Storage**.
2. Click the manage icon that is associated with the vSnap server that you want to add a replication partnership to, and then expand the **Configure Storage Partner(s)** section.
3. Click the add icon.
4. From the **Select Partner** list, select a vSnap server with which to establish a replication partnership.
5. Click **Add Partner**.

# vSnap server administration reference

Once the vSnap server has been installed, registered, and initialized, IBM Spectrum Protect Plus automatically manages its use as a backup target. Volumes and snapshots are created and managed automatically based on the SLA Policies that are defined in IBM Spectrum Protect Plus.

However, you might still have to configure and administer certain aspects of vSnap, such as network configuration or storage pool management.

### Managing vSnap using the command line interface

The vSnap command-line interface is the primary means of administering vSnap. Run the **vsnap** command to access the command line interface. The command can be invoked as the root user or any other operating system user who has vSnap admin privileges. Use the **vsnap user create** command to create additional operating system users that have these privileges. The initial root password is sppDP758.

The command line interface consists of several commands and subcommands that manage various aspects of the system. Refer to Storage Management on page 57 and Network Management on page 59 for details on using these commands. You can also pass the **--help** flag to any command or subcommand to view usage help, for example, **vsnap --help** or **vsnap pool create --help.**

### Managing vSnap using the IBM Spectrum Protect Plus user interface

Some of the most common operations can also be completed from the IBM Spectrum Protect Plus user interface. Log in to the user interface and select **Backup Storage** from the navigation menu. Click the manage icon for a vSnap server to manage it.

### Related tasks

"Installing vSnap servers" on page 19
A vSnap server is as the primary backup destination for IBM Spectrum Protect Plus. In either a VMware or Hyper-V environment, one vSnap server with the name localhost is automatically installed at the time that the IBM Spectrum Protect Plus appliance is initially deployed. In larger backup enterprise environments, additional vSnap servers might be required.

"Configuring the vSnap environment" on page 22

Before you can use a new installation of vSnap, you must complete initial configuration tasks.

"Adding a vSnap server as a backup storage provider" on page 24
In larger backup enterprise environments, additional vSnap servers might be required. These can be installed on either virtual or physical appliances any time after the IBM Spectrum Protect Plus appliance is installed and deployed.

## Storage management

Configure and administer storage pools for a vSnap server.

### Managing disks

vSnap creates a storage pool using disks provisioned to the vSnap server. In the case of virtual deployments, the disks can be RDM or virtual disks provisioned from datastores on any backing storage. In the case of physical deployments, the disks can be local or SAN storage attached to the physical server. The local disks may already have external redundancy enabled via a hardware RAID controller, but if not, vSnap can also create RAID-based storage pools for internal redundancy.

Disks that are attached to vSnap servers must be thick provisioned. If disks are thin provisioned, the vSnap server will not have an accurate view of free space in the storage pool, which might lead to data corruption if the underlying datastore runs out of space.

If vSnap was deployed as part of a virtual appliance, it already contains a 100 GB starter virtual disk that can be used to create a pool. You can add more disks before or after creating a pool and accordingly use them to create a larger pool or expand an existing pool.

### Detecting disks

If you add disks to a vSnap server, use the command line or the IBM Spectrum Protect Plus user interface to detect the newly attached disks.

**Command line:** Run the **`vsnap disk rescan`** command.

**User interface:** Select **Backup Storage** from the navigation menu, and then click the **Actions** menu next to the relevant vSnap server and select **Rescan**.

### Showing disks

Run the **`vsnap disk show`** command to list all disks that are on the vSnap system,

The USED AS column in the output shows whether each disk is in use. Any disk that is unformatted and unpartitioned is marked as unused, otherwise they are marked as used by the partition table or filesystem that is discovered on them.

Only disks that are marked as unused are eligible for creating or adding to a storage pool. If a disk that you plan to add to a storage pool is not seen as unused by vSnap, it might be because it was previously in use and thus contains remnants of an older partition table or filesystem. You can correct this by using system commands like **`parted`** or **`dd`** to wipe the disk partition table.

### Showing storage pool information

Run the **`vsnap pool show`** command to view information about each storage pool.

### Creating a storage pool

If you completed the simple initialization procedure described in "Completing a simple initialization" on page 23, a storage pool was created automatically and the information in this section is not applicable.

To complete an advanced initialization, use the **`vsnap pool create`** command to create a storage pool manually. Before you run the command, ensure that one or more unused disks are available as described

in “Showing disks” on page 27. For information about available options, pass the **--help** flag for any command or subcommand.

Specify a user-friendly display name for the pool and a list of one or more disks. If no disks are specified, all available unused disks are used. You can choose to enable compression and deduplication for the pool during creation. You can also update the compression/deduplication settings at a later time by using the **vsnap pool update** command.

The pool type that you specify during the creation of the storage pool dictates the redundancy of the pool:

**raid0**
This is the default option when no pool type is specified. In this case vSnap assumes your disks have external redundancy, for example, if you use virtual disks on a datastore backed by redundant storage. In this case, the storage pool will have no internal redundancy.

Once a disk has been added to a raid0 pool it cannot be removed. Disconnecting the disk will result in the pool becoming unavailable, which can be resolved only by destroying and recreating the pool.

**raid5**
When you select this option, the pool is comprised of one or more RAID5 groups each consisting of three or more disks. The number of RAID5 groups and the number of disks in each group depends on the total number of disks you specify during pool creation. Based on the number of available disks, vSnap chooses values that maximize total capacity while also ensuring optimal redundancy of vital metadata.

**raid6**
When you select this option, the pool is comprised of one or more RAID6 groups each consisting of four or more disks. The number of RAID6 groups and the number of disks in each group depends on the total number of disks that you specify during pool creation. Based on the number of available disks, vSnap chooses values that maximize total capacity while also ensuring optimal redundancy of vital metadata.

### Expanding a storage pool

Before expanding a pool, ensure that one or more unused disks are available as described in “Showing disks” on page 27.

Use the command line or the IBM Spectrum Protect Plus user interface to expand a storage pool.

**Command line:** Run the **vsnap pool expand** command. For information about available options, pass the **--help** flag for any command or subcommand.

**User interface:** Select **Backup Storage** from the navigation menu. Click the manage icon  for a vSnap server to manage it, and then expand the **Add New Disks** tab. The tab displays all unused disks discovered on the system. Select one or more disks and click **Save** to add them to the storage pool.

## Network management

Configure and administer network services for a vSnap server.

### Showing network interface information

Run the **vsnap network show** command to list network interfaces and the services that are associated with each interface.

By default, the following vSnap services are available of all network interfaces:

**mgmt**
This service is used for management traffic between IBM Spectrum Protect Plus and vSnap.

**nfs**
This service is used for data traffic when backing up data using NFS (currently used for VMware backups).

**iscsi**
This service is used for data traffic when backing up data using iSCSI (currently used for Hyper-V backups).

**smb**
This service is used for data traffic when backing up data using SMB/CIFS (currently not used, reserved for future use.)

### Modifying services associated with network interfaces

Run the **`vsnap network update`** command to modify services that are associated with an interface. For example, if you are using a dedicated interface for data traffic to improve performance.

The following options are required:

**`--id <id>`**
Enter the ID of the interface to update.

**`--services <services>`**
Specify `all` or a comma-separated list of services to enable on the interface. The following are valid values: `mgmt`, `nfs`, `smb`, and `iscsi`.

If a service is available on more than one interface, IBM Spectrum Protect Plus can use any one of the interfaces.

Ensure that the mgmt service remains enabled on the interface that was used to register the vSnap server in IBM Spectrum Protect Plus.

# Chapter 5. Updating

You can update IBM Spectrum Protect Plus from a previous version or release to get the latest features and enhancements. Software patches and updates are installed by using the IBM Spectrum Protect Plus administrative console.

The steps in the following sections describe how to update the IBM Spectrum Protect Plus virtual appliance, the vSnap server, and the VADP proxy. For information about available update files and how to obtain them from an IBM download site, see technote 4044571.

Note the following procedures and considerations before updating IBM Spectrum Protect Plus:

- You must update vSnap servers or VADP proxies that are not on IBM Spectrum Protect Plus virtual appliance separately.
- A patch might not require updates for all IBM Spectrum Protect Plus components. The update files that are available in each patch might vary.
- After IBM Spectrum Protect Plus updates, it cannot roll back to a previous version without a virtual machine snapshot. Create a virtual machine snapshot of your environment before updating. Then, if necessary, complete a snapshot rollback to return to a previous version of IBM Spectrum Protect Plus.
- The update process through the Administrative Console updates IBM Spectrum Protect Plus features and the underlying infrastructure components including the operating system and file system. Do not use another method to update these components.
- Do not update any of the underlying components for IBM Spectrum Protect Plus unless the component is provided in an IBM Spectrum Protect Plus update package. Infrastructure updates are managed by IBM update facilities. The administrator console is the primary means for updating IBM Spectrum Protect Plus features and underlying infrastructure components including the operating system and filesystem.
- Ensure that there are no active jobs scheduled to run during the IBM Spectrum Protect Plus virtual appliance update procedure. Once associated jobs complete or are in an idle state, navigate to **System** > **Job Monitor**, and then select **Hold Schedule** from the **Actions** list for each job. Once the update completes, select **Release Schedule** for each job to resume the associated schedule.

## Updating the IBM Spectrum Protect Plus virtual appliance

Use the IBM Spectrum Protect Plus administrative console to update the virtual appliance.

### Before you begin

Updating your IBM Spectrum Protect Plus environment from version 10.1.0 to version 10.1.1 requires an update to the IBM Spectrum Protect Plus application as well as the operating system of the IBM Spectrum Protect Plus virtual appliance. Download the `.iso` update files to a directory on the computer that is running the browser for the administrative console.

For a list of download images, including the required operating system update for the virtual appliance, see technote 4044571. Note that you must update the virtual appliance before you update the operating system.

### Procedure

To update the IBM Spectrum Protect Plus virtual appliance:

1. From a supported web browser, access the administrative console at the following address:

   ```
   https://hostname:8090/
   ```

   Where *hostname* is the IP address of the virtual machine where the application is deployed.

2. In the login window, select one of the following authentication types in the **Authentication Type** list:

| Authentication Type | Login information |
|---|---|
| **IBM Spectrum Protect Plus** | To log in as an IBM Spectrum Protect Plus user with SYSADMIN privileges, enter your administrator user name and password. |
| **System** | To login as a system user, enter the system password. The default password is `sppadLG235`. You are prompted to change this password during the first login. |

3. Click **Manage updates**.
4. Click **Browse** to browse for the update file for the virtual appliance, and then click **Upload Update Image**.

   The update process begins once the update image is uploaded to the appliance.
5. When the update completes, the virtual machine where the application is deployed automatically restarts.
6. Start the administrative console, and click **Manage updates**.
7. Click **Browse** to browse for the update file for the virtual appliance operating system, and then click **Upload Update Image**.

   The update process begins when the update image is uploaded to the appliance.
8. When the update is complete, navigate to the **Perform System Actions** page on the administrative console to restart the appliance.

   HTML content from previous versions of IBM Spectrum Protect Plus might be stored in your browser cache. Clear the cache before logging in to an updated version of IBM Spectrum Protect Plus to ensure that you are viewing the latest content changes.

   **Important:** If you update IBM Spectrum Protect Plus from V10.1.0 to version V10.1.1, or V10.1.1 to V10.1.1 patch 1, you must update any external vSnap servers in your environment. If you do not update external vSnap servers, authentication errors will occur during log backup operations.

**Related tasks**

"Updating vSnap servers" on page 32

The default vSnap server is updated with the IBM Spectrum Protect Plus appliance. You must update additional vSnap servers that are installed on either virtual or physical appliances separately.

## Updating vSnap servers

The default vSnap server is updated with the IBM Spectrum Protect Plus appliance. You must update additional vSnap servers that are installed on either virtual or physical appliances separately.

**Before you begin**

Download the self-extracting archive `.run` update file to a temporary location on the vSnap server. For information about downloading files, see technote 4044571.

**Procedure**

To update a vSnap server:

1. Ensure that there are no active jobs that use the vSnap server.
2. Navigate to the **System** > **Job Monitor** page in IBM Spectrum Protect Plus.
3. When the associated jobs are complete or in an idle state, select **Hold Schedule** from the **Actions** list for each job.
4. On the vSnap server, open a terminal.

5. From the folder where the `.run` file is located, make the file executable and run the installer by using the following commands:

   ```
   chmod +x file_name.run
   ```

   ```
   ./file_name.run
   ```

   The vSnap packages are installed.
6. On the **Job Monitor** page, select **Release Schedule** from the **Actions** list for the jobs that are associated with the vSnap server.

## Updating VADP proxies

The default VADP proxy is updated with the IBM Spectrum Protect Plus appliance. You must update additional VADP proxies separately.

### Procedure

To update a VADP proxy:

1. Navigate to the **System** > **VADP Proxy** page in IBM Spectrum Protect Plus.
2. The **VADP Proxy** page displays each proxy server. If a newer version of the VADP Proxy software is available, an update icon displays in the **Status** field.
3. Ensure that there are no active jobs that use the proxy, and then click the update icon.

   The proxy server enters a suspended state and installs the latest update. When the update completes, the VADP Proxy server automatically resumes and enters an enabled state.

# Chapter 6. Backup and restore operations

IBM Spectrum Protect Plus is a high-performance data protection and recovery solution for virtual server environments. IBM Spectrum Protect Plus ensures that an organization's virtual machines and their contents are protected quickly, completely, and safely.

Resources that IBM Spectrum Protect Plus needs to recognize are registered in the IBM Spectrum Protect Plus user interface with a one-time operation when defining a backup job. Items that are registered include:

- The hypervisors that contain the components to be backed up. VMware vCenters and Microsoft Hyper-V servers are both supported hypervisors.
- The vSnap Storage Applicances that serve as the primary target for the backup.
- The IBM Spectrum Protect server, which serves as the secondary target for the backup.

Related features of IBM Spectrum Protect Plus include auto-discovery and the product catalog. Auto-discovery recognizes when new virtual machines on a registered hypervisor are added to the environment. The feature ensures that all data in your virtualized environment is protected.

The IBM Spectrum Protect Plus catalog, which inventories and indexes all virtual machine snapshots, enables an administrator to easily see what is and is not protected. When the need to recover arises, this global catalog allows the administrator to quickly search and identify what objects they want to recover, and from which recovery point.

The catalog is stored and maintained on the IBM Spectrum Protect Plus appliance. Periodic maintenance jobs are run to cleanse the catalog of metadata for snapshots that have passed the retention period or are otherwise expired.

## Backing up and restoring VMware data

To protect content on a VMware server, first register the server so that IBM Spectrum Protect Plus recognizes it. Then create backup and restore job definitions, including SLA requirements such as job schedule and retention policies.

### Support for VMware tags

IBM Spectrum Protect Plus supports VMware virtual machine tags. Tags are applied in vSphere and allow users to assign metadata to virtual machines. Once applied in vSphere and added to the IBM Spectrum Protect Plus inventory, virtual machine tags can be viewed through the **View** > **Tags & Categories** filter when you create a job definition. For more information about VMware tagging, see https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vcenterhost.doc/GUID-E8E854DD-AA97-4E0C-8419-CE84F93C4058.html.

### Support for encryption

Backing up and restoring encrypted virtual machines is supported in vSphere 6.5 environments and later. Encrypted virtual machines can be backed up and restored at the virtual machine-level to their original location. If restoring to an alternate location, the encrypted virtual machine is restored without encryption, and must be encrypted manually through vCenter after the restore completes.

The following vCenter privileges are required to enable operations for encrypted virtual machines:

- Cryptographer.Access
- Cryptographer.AddDisk
- Cryptographer.Clone

## Adding a VMware provider

Providers are servers that host objects and attributes. Once a provider is registered, an inventory of the provider is captured and added to IBM Spectrum Protect Plus, enabling you to perform backup and restore jobs, as well as run reports.

### Procedure

To register a VMware provider, complete the following steps.

1. From the navigation menu, expand **Hypervisor**, then **VMware**. Click **Backup**.
2. Click **Manage vCenter**.
3. Click the add icon  .
4. Populate the fields in the **vCenter Properties** pane:

   **Hostname/IP**

   Enter the resolvable IP address or a resolvable path and machine name.

   **Use existing user**

   Enable to select a previously entered user name and password for the provider.

   **Username**

   Enter your user name for the provider.

   **Password**

   Enter your password for the provider.

   **Port**

   Enter the communications port of the provider you are adding. Select the **Use SSL** check box to enable an encrypted Secure Socket Layer connection. The typical default port is 80 for non SSL connections or 443 for SSL connections.
5. Expand **Options** to configure additional options:

   **Maximum number of VMs to process concurrently per ESX server**

   Set the maximum number of concurrent VM snapshots to process on the ESX server.
6. Optionally, expand **IBM Spectrum Protect vStorage Backup Server Settings** to configure an associated vStorage Backup Server for IBM Spectrum Protect offload functionality.

   Offloading essentially creates two backups of your data – one on the vSnap server for short term protection, and one on the IBM Spectrum Protect storage server for longer term protection. Once configured here, offloading is enabled through SLA Policies. The offload operation uses data movers from IBM Spectrum Protect for Virtual Environments configured nodes.

   Select **Link to IBM Spectrum Protect**.

   Populate the fields in the vStorage Backup Server section:

   **vStorage Backup Server**

   Enter the location of the system where the IBM Spectrum Protect for Virtual Environments client GUI and VMCLI are installed.

   **OS Type**

   Select the operating system type of the vStorage Backup Server. Available options include Windows and Linux.

   **vStorage Backup Server Username**

   Enter your login for the vStorage Backup Server.

   **vStorage Backup Server Password**

Enter your password for the vStorage Backup Server.

7. Click **Save**. IBM Spectrum Protect Plus confirms a network connection, adds the provider to the database, then catalogs the provider.

   If a message appears indicating that the connection is unsuccessful, review your entries. If your entries are correct and the connection is unsuccessful, contact a system administrator to review the connections.

   To troubleshoot a connection to a hypervisor virtual machine, use the **Test** function. The **Test** function verifies communication with the virtual machine and tests DNS settings between the IBM Spectrum Protect Plus appliance and the virtual machine. To test a connection, select a single virtual machine, then click **Select Options**. Select **Use existing user** and select a previously entered user name and password for the resource. The **Test** button displays to the right of the **Save** button in the **Options** section. Click **Test**.

   Providers are automatically cataloged after registration. IBM Spectrum Protect Plus creates a high-level Inventory job and catalogs the objects on the provider. To manually run an Inventory job, click **Run Inventory** from the **Backup** pane.

**What to do next**

After you add the VMware provider, complete the following action:

| Action | How to |
|---|---|
| Assign user permissions to the hypervisor. | See "Creating a user role" on page 110. |

**Related concepts**

"Managing identities" on page 95

Some features in IBM Spectrum Protect Plus require credentials to access your resources. For example, IBM Spectrum Protect Plus connects to Oracle servers as the local operating system user that is specified during registration to complete tasks like cataloging, data protection, and data restore.

**Related tasks**

"Creating a VMware backup job" on page 43

Use a Backup job to back up VMware data including virtual machines, datastores, folders, vApps, and datacenters with snapshots.

"Creating a VMware restore job" on page 46

VMware Restore jobs support Instant VM Restore and Instant Disk Restore scenarios, which are created automatically based on the selected source.

## Virtual machine privileges

vCenter Server privileges are required for the virtual machines that are associated with a VMware provider. These privileges are included in the vCenter Administrator role.

If the user that is associated with the provider is not assigned to the Administrator role for an inventory object, the user must be assigned to a role that has the following required privileges. Ensure that the privileges are propagated to child objects. For instructions, refer to the VMware documentation about adding a permission to an inventory object.

| vCenter Server Object | Required Privileges |
|---|---|
| Datacenter | • Create datacenter<br>• Reconfigure datacenter |

| vCenter Server Object | Required Privileges |
|---|---|
| Datastore | • Allocate space<br>• Browse datastore<br>• Configure datastore<br>• Low level file operations<br>• Remove file<br>• Update virtual machine files |
| Datastore Cluster | • Configure a datastore cluster |
| Distributed switch | • Create<br>• Delete<br>• Host operation<br>• Modify<br>• Move<br>• Network I/O Control operation<br>• Policy operation<br>• Port configuration option<br>• Port setting operation<br>• VSPAN operation |
| ESX Agent Manager | • Config<br>• Modify<br>• View |
| Extension | • Register extension |
| Folder | • Create folder<br>• Delete folder<br>• Move folder<br>• Rename folder |
| Global | • Cancel task<br>• Diagnostics (used for troubleshooting, not required for operations)<br>• Disable methods<br>• Enable methods<br>• Licenses<br>• Log event<br>• Manage custom attributes<br>• Set custom attribute<br>• Settings |
| Host > Configuration | • Advanced settings<br>• Storage partition configuration |

| vCenter Server Object | Required Privileges |
| --- | --- |
| Inventory Service > vSphere Tagging | • Assign or Unassign vSphere Tag<br>• Create vSphere Tag<br>• Create vSphere Tag Category<br>• Modify UsedBy Field for Category<br>• Modify UsedBy Field for Tag |
| Network | • Assign network<br>• Configure<br>• Move network<br>• Remove |
| Resource | • Apply recommendation<br>• Assign a vApp to resource pool<br>• Assign virtual machine to resource pool<br>• Create resource pool<br>• Migrate powered off VM<br>• Migrate powered on VM<br>• Modify resource pool<br>• Move resource pool<br>• Query vMotion<br>• Remove resource pool<br>• Rename resource pool |
| Sessions | • View and stop sessions |
| Storage views | • Configure service<br>• View |
| Tasks | • Create task<br>• Update task |

| vCenter Server Object | Required Privileges |
| --- | --- |
| Virtual Machine > Configuration | • Add existing disk<br>• Add new disk<br>• Add or remove device<br>• Advanced<br>• Change CPU count<br>• Change resource<br>• Configure managedBy<br>• Disk change tracking<br>• Disk lease<br>• Display connection settings<br>• Extend virtual disk<br>• Host USB device<br>• Memory<br>• Modify device settings<br>• Query Fault Tolerance compatibility<br>• Query unowned files<br>• Raw device<br>• Reload from path<br>• Remove disk (detach and remove virtual disk)<br>• Rename<br>• Reset guest information<br>• Set annotation<br>• Settings<br>• Swapfile placement<br>• Unlock virtual machine<br>• Upgrade virtual machine compatibility |
| Virtual Machine > Guest Operations | • Guest Operation Modifications<br>• Guest Operation Program Execution<br>• Guest Operation Queries |

| vCenter Server Object | Required Privileges |
| --- | --- |
| Virtual Machine > Interaction | • Answer question<br>• Backup operation on virtual machine<br>• Configure CD media<br>• Configure floppy media<br>• Console interaction<br>• Create screenshot<br>• Defragment all disks<br>• Device connection<br>• Disable Fault Tolerance<br>• Enable Fault Tolerance<br>• Guest operating system management by VIX API<br>• Inject USB HID scan codes<br>• Perform wipe or shrink operations<br>• Power Off<br>• Power On<br>• Record session on VM<br>• Replay session on VM<br>• Reset<br>• Resume Fault Tolerance<br>• Suspend<br>• Suspend Fault Tolerance<br>• Test failover<br>• Test restart Secondary VM<br>• Turn Off Fault Tolerance<br>• Turn On Fault Tolerance<br>• VMware Tools install |
| Virtual Machine > Inventory | • Create from existing<br>• Create new<br>• Move<br>• Register<br>• Remove<br>• Unregister |

| vCenter Server Object | Required Privileges |
| --- | --- |
| Virtual Machine > Provisioning | • Allow disk access<br>• Allow read-only disk access<br>• Allow virtual machine download<br>• Allow virtual machine files upload<br>• Clone template<br>• Clone virtual machine<br>• Create template from virtual machine<br>• Customize<br>• Deploy template<br>• Mark as template<br>• Mark as virtual machine<br>• Modify customization specification<br>• Promote disks<br>• Read customization specifications |
| Virtual Machine > Service configuration | • Allow notifications<br>• Allow polling of global event notifications<br>• Manage service configurations<br>• Modify service configurations<br>• Query service configurations<br>• Read service configurations |
| Virtual Machine > Snapshot management | • Create snapshot<br>• Remove snapshot<br>• Rename snapshot<br>• Revert to snapshot |
| Virtual Machine > vSphere Replication | • Configure replication<br>• Manage replication<br>• Monitor replication |

| vCenter Server Object | Required Privileges |
|---|---|
| vApp | • Add VM (to vApp)<br>• Assign resource pool to vApp<br>• Assign vApp (to another vApp)<br>• Clone<br>• Create<br>• Delete<br>• Export<br>• Import<br>• Move<br>• Power Off<br>• Power On<br>• Rename<br>• Suspend<br>• Unregister<br>• View OVF Environment<br>• vApp application configuration<br>• vApp instance configuration<br>• vApp managedBy configuration<br>• vApp resource configuration |

## Creating a VMware backup job

Use a Backup job to back up VMware data including virtual machines, datastores, folders, vApps, and datacenters with snapshots.

### Before you begin

Review the following procedures and considerations before you create a backup job definition:

- Register the providers that you want to back up. For more information, see “Adding a VMware provider” on page 36.
- Configure an SLA Policy. For more information, see “Configuring SLA policies” on page 11.
- Before an IBM Spectrum Protect Plus user can implement backup and restore operations, roles must be assigned to the user. Grant users access to hypervisors and backup and restore operations through the **Access** pane. Roles and associated permissions are assigned during user account creation. For more information, see Chapter 10, “User access,” on page 105 and “Managing user accounts” on page 112.
- If a virtual machine is associated with multiple SLA Policies, ensure that the policies are not scheduled to run concurrently. Either schedule the SLA Policies to run with a significant amount of time between them, or combine them into a single SLA Policy.
- If your vCenter is a virtual machine, it is recommended to have the vCenter on a dedicated datastore and backed up in a separate backup job.
- In some cases, VMware backup jobs fail with “failed to mount” errors. To resolve, increase the maximum number of NFS mounts to at least 64 through the NFS.MaxVolumes (vSphere 5.5 and later) and NFS41.MaxVolumes (vSphere 6.0 and later) values, as described in the following procedure, https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2239.

### Procedure

To create a VMware Backup job definition, complete the following steps.

1. From the navigation menu, expand **Hypervisor**, then **VMware**. Click **Backup**.
2. Select resources to back up

   Use the search function to search for available resources and toggle the displayed resources through the **View** filter. Available options are **VMs and Templates**, **VM(s)**, **Datastore**, and **Tags & Categories**. Tags are applied in vSphere, and allow a user to assign metadata to virtual machines.
3. Click **Select SLA Policy** to add an SLA Policy to the job definition that meets your backup data criteria.
4. To create the job definition by using default options, click **Save**.

   The job runs as defined by your SLA Policy, or can be run manually from the **Job Monitor** pane.

   Once the job definition is saved, available virtual machine disks (VMDKs) in a virtual machine are discovered and are shown when **VMs and Templates** is selected in the **View** filter. By default, these VMDKs are assigned to the same SLA Policy as the virtual machine. If you want a more granular backup, you can exclude individual VMDKs from the SLA Policy, see "Excluding VMDKs from the SLA Policy for a job" on page 46.
5. To edit options before you create the job definition, click **Select Options**. Set the job definition options.

   **Make VM snapshot application/file system consistent**

   Turn on application or file system consistency for the virtual machine snapshot.

   **Skip Read-only datastores**

   Skip datastores that are mounted as read-only.

   **Skip temporary datastores mounted for Instant Access**

   Exclude temporary Instant Access datastores from the backup job definition.

   **Catalog file metadata**

   Turn on file indexing for the associated snapshot. When file indexing is completed, individual files can be restored through the File Restore pane in IBM Spectrum Protect Plus. Credentials must be established for the associated virtual machine through the **Guest OS Username** and **Guest OS Password** options within the backup job definition. Ensure that the virtual machine can be accessed from the IBM Spectrum Protect Plus appliance either through DNS or host name.

   **Note:** File indexing and file restore are not supported from recovery points that were offloaded to IBM Spectrum Protect storage.

   **Truncate SQL logs**

   To truncate application logs for SQL Server during the backup job, enable the **Truncate SQL logs** option. The credentials must be established for the associated virtual machine through the Guest OS user name and Guest OS Password option within the backup job definition. When the virtual machine is attached to a domain, the user identity follows the default domain\Name format. If the user is a local administrator, the format <local administrator> is used.

   The user identity must have local administrator privileges. On the SQL Server server, the system login credential must have the following permissions:

   - SQL Server sysadmin permissions must be enabled.
   - "Log on as a service" privilege must be set.

   These permissions are assigned through the **Administrative Tools** pane on the local system, see **Local Security Policy > Local Policies > User Rights Assignment > Log on as a service**. For more information about the "Log on as a service" right, see https://technet.microsoft.com/en-us/library/cc794944.aspx.

   IBM Spectrum Protect Plus generates log files for the log truncation function and copies them to the following location on the IBM Spectrum Protect Plus appliance:

   ```
   /data/log/guestdeployer/<Latest-Date>/<Latest-Entry>/<VM name>
   ```

**Important:** File indexing and file restore are not supported from recovery points that were offloaded to IBM Spectrum Protect server.

**VM Snapshot retry attempts**

Set the number of times that IBM Spectrum Protect Plus attempts to snapshot a virtual machine before the job is canceled.

**VADP Proxy**

Select a specific VADP Proxy for load sharing and load balancing.

**Use existing user**

Select a previously entered user name and password for the provider.

**Guest OS Username/Password**

For some tasks (such as cataloging file metadata, file restore, and IP reconfiguration), credentials must be established for the associated virtual machine. Enter the user name and password, and ensure that the virtual machine can be accessed from the IBM Spectrum Protect Plus appliance either through DNS or host name.

6. To troubleshoot a connection to a hypervisor virtual machine, use the **Test** function.

   The **Test** function verifies communication with the virtual machine and tests DNS settings between the IBM Spectrum Protect Plus appliance and the virtual machine. To test a connection, select a single virtual machine, then click **Select Options**. Select **Use existing user** and select a previously entered user name and password for the resource. The **Test** button displays to the right of the **Save** button in the **Options** section. Click **Test**.

7. When you are satisfied that the job-specific information is correct, click **Save**.

   The job runs as defined by your SLA Policy, or can be run manually from the **Job Monitor** pane.

8. To configure additional options, click the **Options** field that is associated with the job in the **SLA Policy Status** section. If no additional options are currently configured for the job, **Not Configured** is shown in the field. Set the following additional job options, and then click **Save**:

   **Pre-scripts and Post-scripts**

   In the **Pre-script** or **Post-script** section, select an uploaded script and a script server where the script will run. Scripts and script servers are configured through the **System** > **Script** pane.

   Pre-scripts and post-scripts are scripts that can be run before or after a job runs at the job level. Windows-based machines support Batch and PowerShell scripts while Linux-based machines support shell scripts.

   Select **Continue scripts on error** to continue running the job if the script associated with the job fails.

   When this option is enabled, if a Pre-script or Post-script completes with a non-zero return code, the backup or restore is attempted and the Pre-script task status returns COMPLETED. If a Post-script completes with a non-zero return code, the Post-script task status returns COMPLETED.

   When this option is disabled, the backup or restore is not attempted, and the Pre-script or Post-script task status returns FAILED.

   **Exclude Resources**

   Exclude specific resources from the backup job through single or multiple exclusion patterns. Resources can be excluded through an exact match or with wildcard asterisks specified before the pattern (*test) or after the pattern (test*).

   Multiple asterisk wildcards are also supported in a single pattern. Patterns support standard alphanumeric characters as well as the following special characters: - _ and *.

   Separate multiple filters with a semicolon.

**What to do next**

After you create the backup job definition, complete the following actions:

| Action | How to |
|---|---|
| If you are using a Linux environment, consider creating VADP proxies to enable load sharing. | See “Creating VADP backup proxies” on page 90. |
| Create a VMware Restore job definition. | See “Creating a VMware restore job” on page 46. |

**Excluding VMDKs from the SLA Policy for a job**
Once a Backup job definition is saved, you can exclude individual VMDKs in a virtual machine from the SLA Policy that is assigned to job.

**Procedure**

To exclude VMDKs from the SLA policy:

1. From the navigation menu, expand **Hypervisor**, then **VMware**. Click **Backup**.
2. Select **VMs and Templates** in the **View** filter.
3. Click the link for the vCenter, and then click the link for the virtual machine that contains the VMDKs that you want to exclude.
4. Select one or more VMDKs, and then click **Select SLA Policy**.
5. Clear the check box for the selected SLA Policy, and then click **Save**.

**Backing up a Linux-based vCenter virtual machine**
To back up a Linux-based vCenter virtual machine by using a backup job, you must first modify the VMware scripts `pre-freeze-script` and `post-thaw-script` on the virtual machine to avoid corrupted vCenter backups.

**Procedure**

To modify the scripts, complete the following steps:

1. On the virtual machine, navigate to the `/usr/sbin` directory and replace the content of the script `pre-freeze-script` with the following content:

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Start of creation consistent state" >> ${log}
#execute freeze command
cmd="echo \"SELECT pg_start_backup('${today}', true);\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log}
2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Finished freeze script" >> ${log}
```

2. Replace the content of the script `post-thaw-script` with the following content:

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Start of creation consistent state" >> ${log}
#execute freeze command
cmd="echo \"SELECT pg_start_backup('${today}', true);\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log}
2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Finished freeze script" >> ${log}
```

## Creating a VMware restore job

VMware Restore jobs support Instant VM Restore and Instant Disk Restore scenarios, which are created automatically based on the selected source.

**Before you begin**
Note the following procedures and considerations before creating a Restore job definition:

- Create and run a VMware Backup job. For more information, see “Creating a VMware backup job” on page 43.
- Before an IBM Spectrum Protect Plus user can perform backup and restore operations, roles must be assigned to the user. Grant users access to hypervisors and backup and restore operations through the **Access** pane. Roles and associated permissions are assigned during user account creation. For more information, see Chapter 10, “User access,” on page 105 and “Managing user accounts” on page 112.
- When selecting virtual machines for recovery, recovery points offloaded to the IBM Spectrum Protect server cannot be recovered in Test Mode.
- Recovery points that were offloaded to the IBM Spectrum Protect server cannot be used to recover VMDKs.
- The size of the virtual machine restored from a vSnap offload to a Spectrum Protect recovery point will be equal to the thick provisioned size of the virtual machine, regardless of source provisioning due to the use of NFS datastores during the offload. The full size of the data must be transferred even if it is unallocated in the source virtual machine.
- When selecting a destination for a Restore job definition, note that the destination must be registered in IBM Spectrum Protect Plus. This includes Restore jobs that restore data to original hosts or clusters.

### About this task

If a VMDK is selected for restore, IBM Spectrum Protect Plus automatically presents options for an Instant Disk Restore job, which provides instant writable access to data and application recovery points. An IBM Spectrum Protect Plus snapshot is mapped to a target server where it can be accessed or copied as required.

All other sources are restored through Instant VM Restore jobs, which can be run in the following modes:

#### Test Mode

Test Mode creates temporary virtual machines for development/testing, snapshot verification, and disaster recovery verification on a scheduled, repeatable basis without affecting production environments. Test machines are kept running as long as needed to complete testing and verification and are then cleaned up after testing and verification completes. Through fenced networking, you can establish a safe environment to test your jobs without interfering with virtual machines used for production. Virtual machines created through Test mode are also given unique names and identifiers to avoid conflicts within your production environment. For more information about creating a fenced network, see “Creating a fenced network through a VMware restore job” on page 50.

#### Clone Mode

Clone Mode creates copies of virtual machines for use cases requiring permanent or long-running copies for data mining or duplication of a test environment in a fenced network. Virtual machines created through Clone Mode are also given unique names and identifiers to avoid conflicts within your production environment. With clone mode you must be sensitive to resource consumption, since clone mode creates permanent or long-term virtual machines.

#### Production Mode

Production Mode enables disaster recovery at the local site from primary storage or a remote disaster recovery site, replacing original machine images with recover images. All configurations are carried over as part of the recovery, including names and identifiers, and all copy data jobs associated with the virtual machine continue to run.

You can also set an IP address or subnet mask for virtual machines to be repurposed for development/testing or disaster recovery use cases. Supported mapping types include IP to IP, IP to DHCP, and subnet to subnet.

### Procedure

To create a VMware Restore job definition, complete the following steps.

1. From the navigation menu, expand **Hypervisor**, then **VMware**. Click **Restore**.

2. In the Restore pane, review the available recovery points of your VMware sources, including virtual machines, VM templates, datastores, folders, and vApps. Use the search function and filters to fine-tune your selection across specific recovery site types. Expand an entry in the Restore pane to view individual recovery points by date.
3. To select the latest recovery point, click the add to restore list icon at the resource level. Then, from the **Restore from site list**, select the site associated with the backup storage server that you want to recover from.

   To restore a specific recovery point from a specific site, expand a resource in the **Restore** pane, and then click the add to restore list icon that is associated with the recovery point. Adding the latest recovery points and specific recovery points to the **Restore List** is not supported. Click the remove icon to remove recovery points from the **Restore List**.
4. To run the job now using default options, click **Restore**. To schedule the job to run using default options, click **Manage Jobs** and define a trigger for the job definition.
5. To edit options before creating the job definition, click **Options**. Set the job definition options.

   **Destination**

   Set the VMware destination:

   **Original ESX Host or Cluster** - Select to restore to the original host or cluster.

   **Alternate ESX Host or Cluster** - Select to restore to a local destination different from the original host or cluster, then select the alternate location from available resources. Test and Production networks can be configured on the alternate location to create a fenced network, which keeps virtual machines used for testing from interfering with virtual machines used for production. From the vCenter section, select an alternate location. Selections can be filtered by either hosts or clusters.

   **ESX Host if vCenter is down** - Select to bypass the vCenter and restore directly to the ESX host. In other restore scenarios, actions are completed through vCenter. If vCenter is unavailable, this option restores the vCenter virtual machine or virtual machines that the vCenter is dependent on.

   **Restore Type**

   Set the VMware Restore job to run in Test, Production, or Clone mode by default. Once the job is created, it can be run in Production or Clone mode through the Job Sessions or Active Clones sections of the Restore pane. Test mode is not available for long distance restores.

   **Network Settings**

   Set the network settings for a restore to an original ESX host or cluster:

   **Allow system to define IP configuration** - Select to allow your operating system to define the destination IP address. During a Test Mode restore, the destination virtual machine receives a new MAC address along with an associated NIC. Depending on your operating system, a new IP address can be assigned based on the original NIC of the virtual machine, or assigned through DHCP. During a Production Mode restore the MAC address does not change, therefore the IP address should be retained.

   **Use original IP configuration** - Select to restore to the original host or cluster using your predefined IP address configuration. During a restore, the destination virtual machine receives a new MAC address, but the IP address is retained.

   Set the network settings for a restore to an alternate or long distance ESX host or cluster:

   From the **Production** and **Test** fields, set virtual networks for production and test restore job runs. Destination network settings for production and test environments should be different locations to create a fenced network, which keeps virtual machines used for testing from interfering with virtual machines used for production. The networks associated with Test and Production will be utilized when the restore job is run in the associated mode.

Set an IP address or subnet mask for virtual machines to be re-purposed for development/testing or disaster recovery use cases. Supported mapping types include IP to IP, IP to DHCP, and subnet to subnet. Virtual machines containing multiple NICs are supported.

By default, the **Use system defined subnets and IP addresses for VM guest OS on destination** option is enabled. To use your predefined subnets and IP addresses, select **Use original subnets and IP addresses for VM guest OS on destination**.

To create a new mapping configuration, select **Add mappings for subnets and IP addresses for VM guest OS on destination**, then click **Add Mapping**. Enter a subnet or IP address in the **Source** field. In the destination field, select **DHCP** to automatically select an IP and related configuration information if DHCP is available on the selected client. Select **Static** to enter a specific subnet or IP address, subnet mask, gateway, and DNS. Note that **Subnet / IP Address**, **Subnet Mask**, and **Gateway** are required fields. If a subnet is entered as a source, a subnet must also be entered as a destination.

IP reconfiguration is skipped for VMs if a static IP is used but no suitable subnet mapping is found, or if the source machine is powered off and there is more than one associated NIC. In a Windows environment, if a VM is DHCP only, then IP reconfiguration is skipped for that VM. In a Linux environment all addresses are assumed to be static, and only IP mapping will be available.

**Destination Datastore** - Set the destination datastore for a restore to an alternate ESX host or cluster.

**VM Folder Destination** - Enter the VM folder path on the destination datastore. Note that the directory will be created if it does not exist. Use "/" as the root VM folder of the targeted datastore.

**Script Settings**

In the **Pre-script** or **Post-script** section, select an uploaded script and a script server where the script will run. Scripts and script servers are configured through the **System** > **Script** pane.

Pre-scripts and post-scripts are scripts that can be run before or after a job runs at the job level. Windows-based machines support Batch and PowerShell scripts while Linux-based machines support shell scripts.

Select **Continue scripts on error** to continue running the job if the script associated with the job fails.

When this option is enabled, if a Pre-script or Post-script completes with a non-zero return code, the backup or restore is attempted and the Pre-script task status returns COMPLETED. If a Post-script completes with a non-zero return code, the Post-script task status returns COMPLETED.

When this option is disabled, the backup or restore is not attempted, and the Pre-script or Post-script task status returns FAILED.

**Advanced Options**

Set the advanced job definition options:

**Power on after recovery** - Toggle the power state of a VM after a recovery is performed. VMs are powered on in the order they are recovered, as set in the Source step. Note that restored VM templates cannot be powered on after recovery.

**Overwrite virtual machine** - Enable to allow the restore job to overwrite the selected VM. By default this option is disabled.

**Continue with restore even if it fails** - Toggle the recovery of a resource in a series if the previous resource recovery fails. If disabled, the Restore job stops if the recovery of a resource fails.

**Rollback all the changes on failure** - Enable to automatically clean up allocated resources as part of a restore if the VM recovery fails.

**Allow to overwrite and force clean up of pending old sessions** - Enable this option to allow a scheduled session of a recovery job to force an existing pending session to clean up associated resources so the new session can run. Disable this option to keep an existing test environment running without being cleaned up.

**Fix VMX file for missing disk** - If individual disks are excluded from a backup, the associated VM will fail to start. Enable this option to remove the entries for excluded disks from the VMX configuration file and ensure the restored VM starts as part of an Instant VM Restore job.

**Restore VM tags** - Enable this option to restore tags applied to VMs through vSphere.

Click **Save** to save the policy options.

6. To run the job now, click **Restore**. To schedule the job click **Manage Jobs** and define a trigger for the job definition.
7. Once the job completes successfully, select one of the following options from the **Actions** menu on the Jobs Sessions or Active Clones sections on the Restore pane:

   **Cleanup**

   Destroys the VM and cleans up all associated resources. Since this is a temporary/testing VM, all data is lost when the VM is destroyed.

   **Move to Production (vMotion)**

   Migrates the VM through vMotion to the Datastore and the Virtual Network defined as the "Production" network.

   **Clone (vMotion)**

   Migrates the VM through vMotion to the Datastore and Virtual Network defined as the "Test" network.

**Related tasks**

“Adding a VMware provider” on page 36
Providers are servers that host objects and attributes. Once a provider is registered, an inventory of the provider is captured and added to IBM Spectrum Protect Plus, enabling you to perform backup and restore jobs, as well as run reports.

### Creating a fenced network through a VMware restore job

Through fenced networking, you can establish a safe environment to test your jobs without interfering with virtual machines that are used for production. Fenced networking can be used with with jobs running in Test Mode and Production Mode.

#### Before you begin

Review the following procedures and considerations before you create a fenced network:

- Create and run a VMware Restore job. For more information, see “Creating a VMware restore job” on page 46.
- When selecting virtual machines for recovery, recovery points offloaded to the IBM Spectrum Protect server cannot be recovered in Test Mode.
- Recovery points that were offloaded to the IBM Spectrum Protect server cannot be used to recover VMDKs.

#### Procedure

To create a fenced network, complete the following steps:

1. From the navigation menu, expand **Hypervisor**, then **VMware**. Click **Restore**.
2. In the Restore pane, review the available recovery points of your VMware sources, including virtual machines, VM templates, datastores, folders, and vApps. Use the search function and filters to fine-tune your selection across specific recovery site types. Expand an entry in the Restore pane to view individual recovery points by date.
3. Select recovery points and click the add to restore list icon to add the recovery point to the Restore List.Click the remove icon to remove items from the Restore List.
4. Click **Options** to set the job definition options.
5. Select **Alternate ESX Host or Cluster**, then select an alternate host or cluster from the vCenter list.

6. Expand the **Network Settings** section. From the **Production** and **Test** fields, set virtual networks for production and test Restore job runs. Destination network settings for production and test environments should be different locations to create a fenced network, which keeps virtual machines used for testing from interfering with virtual machines used for production. The networks associated with Test and Production will be utilized when the restore job is run in the associated mode.The IP address(es) of the target machine can be configured through the following options:

   **Use system defined subnets and IP addresses for VM guest OS on destination** - Select to allow your operating system to define the destination IP address. During a Test Mode restore, the destination virtual machine receives a new MAC address along with an associated NIC. Depending on your operating system, a new IP address can be assigned based on the original NIC of the virtual machine, or assigned through DHCP. During a Production Mode restore the MAC address does not change, therefore the IP address should be retained.

   **Use original subnets and IP addresses for VM guest OS on destination** - Select to restore to the original host or cluster using your predefined IP address configuration. During a restore, the destination virtual machine receives a new MAC address, but the IP address is retained.

   Set the network settings for a restore to an alternate or long distance ESX host or cluster:

   From the **Production** and **Test** fields, set virtual networks for production and test restore job runs. Destination network settings for production and test environments should be different locations to create a fenced network, which keeps virtual machines used for testing from interfering with virtual machines used for production. The networks associated with Test and Production will be utilized when the restore job is run in the associated mode.

   Set an IP address or subnet mask for virtual machines to be re-purposed for development/testing or disaster recovery use cases. Supported mapping types include IP to IP, IP to DHCP, and subnet to subnet. Virtual machines containing multiple NICs are supported.

   By default, the **Use system defined subnets and IP addresses for VM guest OS on destination** option is enabled. To use your predefined subnets and IP addresses, select **Use original subnets and IP addresses for VM guest OS on destination**.

   To create a new mapping configuration, select **Add mappings for subnets and IP addresses for VM guest OS on destination**, then click **Add Mapping**. Enter a subnet or IP address in the **Source** field. In the destination field, select **DHCP** to automatically select an IP and related configuration information if DHCP is available on the selected client. Select **Static** to enter a specific subnet or IP address, subnet mask, gateway, and DNS. Note that **Subnet / IP Address**, **Subnet Mask**, and **Gateway** are required fields. If a subnet is entered as a source, a subnet must also be entered as a destination.

   IP reconfiguration is skipped for virtual machines if a static IP is used but no suitable subnet mapping is found, or if the source machine is powered off and there is more than one associated NIC. In a Windows environment, if a virtual machine is DHCP only, then IP recoh, onfiguration is skipped for that virtual machine. In a Linux environment all addresses are assumed to be static, and only IP mapping will be available.

   **Destination Datastore** - Set the destination datastore for a restore to an alternate ESX host or cluster.

   **VM Folder Destination** - Enter the VM folder path on the destination datastore. Note that the directory will be created if it does not exist. Use "/" as the root VM folder of the targeted datastore.
7. Click **Save** to save the policy options.
8. Once the job completes successfully, select one of the following options from the **Actions** menu on the Jobs Sessions or Active Clones sections on the Restore pane:

   **Cleanup**

   Destroys the virtual machine and cleans up all associated resources. Since this is a temporary/testing virtual machine, all data is lost when the virtual machine is destroyed.

   **Move to Production (vMotion)**

   Migrates the virtual machine through vMotion to the Datastore and the Virtual Network defined as the "Production" Network.

**Clone (vMotion)**

Migrates the virtual machine through vMotion to the Datastore and Virtual Network defined as the "Test" network.

**Related tasks**

“Adding a VMware provider” on page 36
Providers are servers that host objects and attributes. Once a provider is registered, an inventory of the provider is captured and added to IBM Spectrum Protect Plus, enabling you to perform backup and restore jobs, as well as run reports.

# Backing up and restoring Hyper-V data

To protect content on a Hyper-V server, first register the server so that IBM Spectrum Protect Plus recognizes it. Then create backup and restore job definitions, including SLA requirements such as job schedule and retention policies.

## Adding a Hyper-V provider

Providers are servers that host objects and attributes. Once a provider is registered, an inventory of the provider is captured and added to IBM Spectrum Protect Plus, enabling you to perform backup and restore jobs, as well as run reports.

**Before you begin**

Note the following considerations and procedures before adding a Hyper-V server to IBM Spectrum Protect Plus:

- Hyper-V servers can be registered using a DNS name or IP address. DNS names must be resolvable by IBM Spectrum Protect Plus. If the Hyper-V server is part of a cluster, all nodes in the cluster must be resolvable through DNS. If DNS is not available, the server must be added to the `/etc/hosts` file on the IBM Spectrum Protect Plus appliance. If more than one Hyper-V server is set up in a cluster environment, all of the servers must be added to`/etc/hosts`. When registering the cluster in IBM Spectrum Protect Plus, register the Failover Cluster Manager.
- All Hyper-V servers, including cluster nodes, must have the Microsoft iSCSI initiator Service running in their Services list. Set the service to Automatic so that it is available when the machine boots.
- Add the user to the local administrator group on the Hyper-V server.

**Procedure**

To register a Hyper-V provider, complete the following steps.

1. From the navigation menu, expand **Hypervisor**, then **Hyper-V**. Click **Backup**.
2. Click **Manage Hyper-V Server**.
3. Click the add icon  .
4. Populate the fields in the **Server Properties** pane:

   **Hostname/IP**

   Enter the resolvable IP address or a resolvable path and machine name.

   **Use existing user**

   Enable to select a previously entered user name and password for the provider.

   **Username**

   Enter your user name for the provider.

   **Password**

   Enter your password for the provider.

**Port**

Enter the communications port of the provider you are adding. The typical default port is 5985.

Select the **Use SSL** check box to enable an encrypted Secure Socket Layer (SSL) connection.

To enable an SLL connection, you must add the self-signed SSL certificate for the Hyper-V server or a certificate authority (CA) certificate. To upload a certificate, see "Uploading an SSL certificate from the administrative console" on page 98 certificate.

If you do not select **Use SSL** you must complete additional steps on the Hyper-V server. See "Enabling WinRM for connection to Hyper-V hosts" on page 53

5. Expand **Options** to configure additional options:

   **Maximum number of VMs to process concurrently per Hyper-V server**

   Set the maximum number of concurrent virtual machine snapshots to process on the Hyper-V server.

6. Click **Save**. IBM Spectrum Protect Plus confirms a network connection, adds the provider to the database, and then catalogs the provider.

   If a message appears indicating that the connection is unsuccessful, review your entries. If your entries are correct and the connection is unsuccessful, contact a system administrator to review the connections.

   To troubleshoot a connection to a hypervisor virtual machine, use the **Test** function. The **Test** function verifies communication with the virtual machine and tests DNS settings between the IBM Spectrum Protect Plus appliance and the virtual machine. To test a connection, select a single virtual machine, then click **Select Options**. Select **Use existing user** and select a previously entered user name and password for the resource. The **Test** button displays to the right of the **Save** button in the **Options** section. Click **Test**.

   Providers are automatically cataloged after registration. IBM Spectrum Protect Plus creates a high-level Inventory job and catalogs the objects on the provider. To manually run an Inventory job, click **Run Inventory** from the **Backup** pane.

**What to do next**

After you add the Hyper-V provider, complete the following action:

| Action | How to |
|---|---|
| Assign user permissions to the hypervisor. | See "Creating a user role" on page 110. |

**Related tasks**

"Creating a Hyper-V backup job" on page 54
Use a Backup job to backup Hyper-V data with snapshots.

"Creating a Hyper-V restore job " on page 56
Hyper-V Restore jobs support Instant VM Restore and Instant Disk Restore scenarios, which are created automatically based on the selected source.

**Enabling WinRM for connection to Hyper-V hosts**

If you cannot use SSL to enable encrypted network traffic between IBM Spectrum Protect Plus Hyper-V hosts, you must configure WinRM on the host to allow unencrypted network traffic. Ensure that you understand the security risks that are associated with allowing unencrypted network traffic.

**Procedure**

To configure WinRM for connection to Hyper-V hosts:

1. On the Hyper-V host system, log in with an administrator account.
2. Open a Windows command prompt. If User Account Control (UAC) is enabled, you must open the command prompt with elevated privileges by running with the "Run as administrator" option enabled.

3. Enter the following command to configure WinRM to allow unencrypted network traffic:

```
winrm s winrm/config/service @{AllowUnencrypted="true"}
```

4. Verify that the AllowUnencrypted option is set to true through the following command:

```
winrm g winrm/config/service
```

## Creating a Hyper-V backup job

Use a Backup job to backup Hyper-V data with snapshots.

### Before you begin

Note the following procedures and considerations before creating a Backup job definition:

- Register the providers that you want to back up. For more information see “Adding a Hyper-V provider” on page 52
- Configure an SLA Policy. For more information, see “Configuring SLA policies” on page 11.
- Hyper-V Backup and Restore jobs require the installation of the latest Hyper-V integration services. For Microsoft Windows environments, https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-windows-guest-operating-systems-for-hyper-v-on-windows. For Linux environments, see https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-linux-and-freebsd-virtual-machines-for-hyper-v-on-windows.
- All Hyper-V servers, including cluster nodes, must have the Microsoft iSCSI initiator Service running in their Services list. Set the service to Automatic so that it is available when the machine boots.
- Before an IBM Spectrum Protect Plus user can complete backup and restore operations, roles must be assigned to the user. Grant users access to hypervisors and backup and restore operations through the **Access** pane. Roles and associated permissions are assigned during user account creation. For more information, see Chapter 10, “User access,” on page 105 and “Managing user accounts” on page 112.
- If a virtual machine is associated with multiple SLA Policies, ensure that the policies are not scheduled to run concurrently. Either schedule the SLA Policies to run with a significant amount of time between them, or combine them into a single SLA Policy.
- If the IP address of the IBM Spectrum Protect Plus appliance is changed after an initial Hyper-V base backup is created, the target IQN of the Hyper-V resource may be left in a bad state. To correct this issue, from the Microsoft iSCSI Initiator tool, click the **Discovery** tab. Select the old IP address, then click **Remove**. Click the **Target** tab and disconnect the reconnecting session.

### Procedure

To create a Hyper-V Backup job definition, complete the following steps.

1. From the navigation menu, expand **Hypervisor**, then **Hyper-V**. Click **Backup**.
2. Select resources to back up

   Use the search function to search for available resources and toggle the displayed resources through the **View** filter. Available options are **VMs** and **Datastore**.
3. Click **Select SLA Policy** to add an SLA Policy to the job definition that meets your backup data criteria.
4. To create the job definition using default options, click **Save**.

   The job runs as defined by your SLA Policy, or can be run manually from the **Job Monitor** pane.
5. To edit options before creating the job definition, click **Select Options**. Set the job definition options.

   **Make VM snapshot application/file system consistent**

   Enable to turn on application or file-system consistency for the virtual machine snapshot.

   **Skip Read-only datastores**

   Enable to skip datastores mounted as read-only.

   **Skip temporary datastores mounted for Instant Access**

Enable to exclude temporary Instant Access datastores from the backup job definition.

**Catalog file metadata**

To turn on file indexing for the associated snapshot, enable the Catalog file metadata option. Once file indexing completes, individual files can be restored through the File Restore pane in IBM Spectrum Protect Plus. Note that credentials must be established for the associated virtual machine through the Guest OS Username and Guest OS Password option within the backup job definition. Ensure that the virtual machine can be accessed from the IBM Spectrum Protect Plus appliance either through DNS or host-name.

**Truncate SQL logs**

To truncate application logs for SQL during the Backup job, enable the **Truncate SQL logs** option. Note that credentials must be established for the associated virtual machine through the Guest OS Username and Guest OS Password option within the backup job definition. The user identity follows the default domain\Name format if the virtual machine is attached to a domain. The format <local administrator> is used if the user is a local administrator.

The user identity must have local administrator privileges. Additionally, on the SQL server, the system login credential must have SQL sysadmin permissions enabled, as well as the ""Log on as a service"" right, which is assigned through the Administrative Tools control panel on the local machine (**Local Security Policy > Local Policies > User Rights Assignment > Log on as a service**). For more information about the ""Log on as a service"" right, see https://technet.microsoft.com/en-us/library/cc794944.aspx.

IBM Spectrum Protect Plus generates logs pertaining to the log truncation function and copies them to the following location on the IBM Spectrum Protect Plus appliance:

```
/data/log/guestdeployer/<Latest-Date>/<Latest-Entry>/<VM name>
```

**Important:** File indexing and file restore are not supported from recovery points that were offloaded to IBM Spectrum Protect server.

**VM Snapshot retry attempts**

Set the number of times IBM Spectrum Protect Plus should attempt to snapshot a virtual machine before canceling the job.

**Use existing user**

Enable to select a previously entered username and password for the provider.

**Guest OS Username/Password**

For some tasks (such as cataloging file metadata, file restore, and IP reconfiguration), credentials must be established for the associated virtual machine. Enter the username and password, and ensure that the virtual machine can be accessed from the IBM Spectrum Protect Plus appliance either through DNS or hostname.

The default security policy uses the Windows NTLM protocol, and the user identity follows the default domain\Name format if the Hyper-V virtual machine is attached to a domain. The format .\<local administrator> is used if the user is a local administrator.

6. To troubleshoot a connection to a hypervisor virtual machine, use the **Test** function.

   The **Test** function verifies communication with the virtual machine and tests DNS settings between the IBM Spectrum Protect Plus appliance and the virtual machine. To test a connection, select a single virtual machine, then click **Select Options**. Select **Use existing user** and select a previously entered user name and password for the resource. The **Test** button displays to the right of the **Save** button in the **Options** section. Click **Test**.
7. When you are satisfied that the job-specific information is correct, click **Save**.

   The job runs as defined by your SLA Policy, or can be run manually from the **Job Monitor** pane.

8. To configure additional options, click the **Options** field that is associated with the job in the **SLA Policy Status** section. If no additional options are currently configured for the job, **Not Configured** is shown in the field. Set the following additional job options, and then click **Save**:

   **Pre-scripts and Post-scripts**

   In the **Pre-script** or **Post-script** section, select an uploaded script and a script server where the script will run. Scripts and script servers are configured through the **System** > **Script** pane.

   Pre-scripts and post-scripts are scripts that can be run before or after a job runs at the job level. Windows-based machines support Batch and PowerShell scripts while Linux-based machines support shell scripts.

   Select **Continue scripts on error** to continue running the job if the script associated with the job fails.

   When this option is enabled, if a Pre-script or Post-script completes with a non-zero return code, the backup or restore is attempted and the Pre-script task status returns COMPLETED. If a Post-script completes with a non-zero return code, the Post-script task status returns COMPLETED.

   When this option is disabled, the backup or restore is not attempted, and the Pre-script or Post-script task status returns FAILED.

   **Exclude Resources**

   Exclude specific resources from the backup job through single or multiple exclusion patterns. Resources can be excluded through an exact match or with wildcard asterisks specified before the pattern (*test) or after the pattern (test*).

   Multiple asterisk wildcards are also supported in a single pattern. Patterns support standard alphanumeric characters as well as the following special characters: - _ and *.

   Separate multiple filters with a semicolon.

**What to do next**
After you create the backup job definition, complete the following action:

| Action | How to |
|---|---|
| Create a Hyper-V Restore job definition. | See “Creating a Hyper-V restore job ” on page 56. |

## Creating a Hyper-V restore job

Hyper-V Restore jobs support Instant VM Restore and Instant Disk Restore scenarios, which are created automatically based on the selected source.

**Before you begin**
Note the following procedures and considerations before creating a Restore job definition:

- Create and run a Hyper-V Backup job. For more information, see “Creating a Hyper-V backup job” on page 54.
- When selecting a destination for a Restore job definition, note that the destination must be registered in IBM Spectrum Protect Plus. This includes Restore jobs that restore data to original hosts or clusters.
- Hyper-V Backup and Restore jobs require the installation of the latest Hyper-V integration services. For Microsoft Windows environments, https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-windows-guest-operating-systems-for-hyper-v-on-windows. For Linux environments, see https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-linux-and-freebsd-virtual-machines-for-hyper-v-on-windows.
- Before an IBM Spectrum Protect Plus user can perform backup and restore operations, roles must be assigned to the user. Grant users access to hypervisors and backup and restore operations through the **Access** pane. Roles and associated permissions are assigned during user account creation. For more information, see Chapter 10, “User access,” on page 105 and “Managing user accounts” on page 112.

### About this task

If a VHD is selected for restore, IBM Spectrum Protect Plus automatically presents options for an Instant Disk Restore job, which provides instant writable access to data and application recovery points.

An IBM Spectrum Protect Plus snapshot is mapped to a target server where it can be accessed or copied as required. All other sources are restored through Instant VM Restore jobs, which can be run in the following modes:

#### Test Mode

Test Mode creates temporary virtual machines for development/testing, snapshot verification, and disaster recovery verification on a scheduled, repeatable basis without affecting production environments. Test machines are kept running as long as needed to complete testing and verification and are then cleaned up after testing and verification completes. Through fenced networking, you can establish a safe environment to test your jobs without interfering with virtual machines used for production. Virtual machines created through Test mode are also given unique names and identifiers to avoid conflicts within your production environment.

#### Clone Mode

Clone Mode creates copies of virtual machines for use cases requiring permanent or long-running copies for data mining or duplication of a test environment in a fenced network. Virtual machines created through Clone Mode are also given unique names and identifiers to avoid conflicts within your production environment. With clone mode you must be sensitive to resource consumption, since clone mode creates permanent or long-term virtual machines.

#### Production Mode

Production Mode enables disaster recovery at the local site from primary storage or a remote disaster recovery site, replacing original machine images with recover images. All configurations are carried over as part of the recovery, including names and identifiers, and all copy data jobs associated with the virtual machine continue to run.

**Note:** Moving from Test mode to Production mode is not supported for Hyper-V.

### Procedure

To create a Hyper-V Restore job definition, complete the following steps.

1. From the navigation menu, expand **Hypervisor**, then **Hyper-V**. Click **Restore**.
2. In the Restore pane, review the available recovery points of your VMware sources, including virtual machines, VM templates, datastores, folders, and vApps. Use the search function and filters to fine-tune your selection across specific recovery site types. Expand an entry in the Restore pane to view individual recovery points by date.
3. To select the latest recovery point, click the add to restore list icon at the resource level. Then, from the **Restore from site list**, select the site associated with the backup storage server that you want to recover from.

   To restore a specific recovery point from a specific site, expand a resource in the **Restore** pane, and then click the add to restore list icon that is associated with the recovery point. Adding the latest recovery points and specific recovery points to the **Restore List** is not supported. Click the remove icon to remove recovery points from the **Restore List**.
4. To run the job now using default options, click **Restore**. To schedule the job to run using default options, click **Manage Jobs** and define a trigger for the job definition.
5. To edit options before creating the job definition, click **Options**. Set the job definition options.

   **Destination**

   Set the Hyper-V destination:

   **Original Hyper-V Host or Cluster** - Select to restore to the original host or cluster.

**Alternate Hyper-V Host or Cluster** - Select to restore to a local destination different from the original host or cluster, then select the alternate location from available resources.

**Restore Type**

Set the Hyper-V Restore job to run in Test, Production, or Clone mode by default. Once the job is created, it can be run in Test, Production, or Clone mode through the Job Sessions pane.

**Network Settings**

Set the network settings for a restore to an alternate Hyper-V host or cluster:

- From the Production and Test fields, set virtual networks for production and test restore job runs. Destination network settings for production and test environments should be different locations to create a fenced network, which keeps virtual machines used for testing from interfering with virtual machines used for production. The networks associated with Test and Production will be utilized when the restore job is run in the associated mode.
- Set an IP address or subnet mask for virtual machines to be re-purposed for development/testing or disaster recovery use cases. Supported mapping types include IP to IP, IP to DHCP, and subnet to subnet. Virtual machines containing multiple NICs are supported.

**Destination Datastore**

Set the destination datastore for a restore to an alternate Hyper-V host or cluster.

**VM Folder Destination**

Enter the VM folder path on the destination datastore. Note that the directory will be created if it does not exist. Use "/" as the root VM folder of the targeted datastore.

**Script Settings**

In the **Pre-script** or **Post-script** section, select an uploaded script and a script server where the script will run. Scripts and script servers are configured through the **System** > **Script** pane.

Pre-scripts and post-scripts are scripts that can be run before or after a job runs at the job level. Windows-based machines support Batch and PowerShell scripts while Linux-based machines support shell scripts.

Select **Continue scripts on error** to continue running the job if the script associated with the job fails.

When this option is enabled, if a Pre-script or Post-script completes with a non-zero return code, the backup or restore is attempted and the Pre-script task status returns COMPLETED. If a Post-script completes with a non-zero return code, the Post-script task status returns COMPLETED.

When this option is disabled, the backup or restore is not attempted, and the Pre-script or Post-script task status returns FAILED.

**Advanced Options**

Set the advanced job definition options:

**Power on after recovery** - Toggle the power state of a virtual machine after a recovery is performed. Virtual machines are powered on in the order they are recovered, as set in the Source step. Note that restored VM templates cannot be powered on after recovery.

**Overwrite virtual machine** - Enable to allow the restore job to overwrite the selected virtual machine. By default this option is disabled.

**Continue with restore even if it fails** - Toggle the recovery of a resource in a series if the previous resource recovery fails. If disabled, the Restore job stops if the recovery of a resource fails.

**Rollback all the changes on failure** - Enable to automatically clean up allocated resources as part of a restore if the virtual machine recovery fails.

**Allow to overwrite and force clean up of pending old sessions** - Enable this option to allow a scheduled session of a recovery job to force an existing pending session to clean up associated

resources so the new session can run. Disable this option to keep an existing test environment running without being cleaned up.

Click **Save** to save the policy options.

6. To run the job now, click **Restore**. To schedule the job click **Manage Job(s)** and define a trigger for the job definition.
7. Once the job completes successfully, select one of the following options from the **Actions** menu on the Jobs Sessions or Active Clones sections on the Restore pane:

**Cleanup**

Destroys the virtual machine and cleans up all associated resources. Since this is a temporary/testing virtual machine, all data is lost when the virtual machine is destroyed.

**Clone (migrate)**

Migrates the virtual machine to the Datastore and Virtual Network defined as the "Test" network.

**Related tasks**

“Creating a Hyper-V backup job” on page 54
Use a Backup job to backup Hyper-V data with snapshots.

“Adding a Hyper-V provider” on page 52
Providers are servers that host objects and attributes. Once a provider is registered, an inventory of the provider is captured and added to IBM Spectrum Protect Plus, enabling you to perform backup and restore jobs, as well as run reports.

## Backing up and restoring SQL Server data

To protect content on a SQL Server server, first register the server so that IBM Spectrum Protect Plus recognizes it. Then create backup and restore job definitions, including SLA requirements such as job schedule and retention policies.

### Registration and authentication

Register each SQL Server server as a provider in IBM Spectrum Protect Plus by name or IP address. When registering a SQL Server Cluster (AlwaysOn) node, register each node by name or IP address. Note that the IP addresses must be public-facing and listening on port 5985. The fully qualified domain name and virtual machine node DNS name must be resolvable and route-able from the IBM Spectrum Protect Plus appliance.

The user identity must have sufficient rights to install and start the IBM Spectrum Protect Plus Tools Service on the node. This includes "Log on as a service" rights. For more information about the "Log on as a service" right, see https://technet.microsoft.com/en-us/library/cc794944.aspx.

The default security policy uses the Windows NTLM protocol, and the user identity format follows the default domain\Name format.

### Kerberos requirements

Kerberos-based authentication can be enabled through a configuration file on the IBM Spectrum Protect Plus appliance. This will override the default Windows NTLM protocol.

For Kerberos-based authentication only, the user identity must be specified in the username@FQDN format. The username must be able to authenticate using the registered password to obtain a ticket-granting ticket (TGT) from the key distribution center (KDC) on the domain specified by the fully qualified domain name.

Kerberos authentication also requires that the clock skew between the Domain Controller and the IBM Spectrum Protect Plus appliance is less than five minutes.

The default Windows NTLM protocol is not time dependent.

**Privileges**

On the SQL Server server, the system login credential must have public and sysadmin permissions enabled, plus permission to access cluster resources in a SQL Server AlwaysOn environment. If one user account is used for all SQL Server functions, a Windows login must be enabled for the SQL Server server, with public and sysadmin permissions enabled.

Every SQL Server instance can use a specific user account to access the resources of that particular instance.

To perform log backup operations, the SQL Server user registered with IBM Spectrum Protect Plus must have the sysadmin permission enabled to manage SQL Server agent jobs.

## Adding a SQL Server provider

Providers are servers that host objects and attributes. Once a provider is registered, an inventory of the provider is captured and added to IBM Spectrum Protect Plus, enabling you to perform backup and restore jobs, as well as run reports.

**Procedure**

To register a SQL Server provider, complete the following steps.

1. From the navigation menu, expand **Application**, then **SQL**. Click **Backup**.
2. Click **Manage Application Servers**.
3. Click the add icon .
4. Populate the fields in the **Application Properties** pane:

   **Host Address**

   Enter the resolvable IP address or a resolvable path and machine name.

   **Use existing user**

   Enable to select a previously entered user name and password for the provider.

   **Username**

   Enter your user name for the provider. The user identity follows the default domain\Name format if the virtual machine is attached to a domain. The format <local administrator> is used if the user is a local administrator.

   For Kerberos-based authentication only, the user identity must be specified in the username@FQDN format. The user name must be able to authenticate using the registered password to obtain a ticket-granting ticket (TGT) from the key distribution center (KDC) on the domain that is specified by the fully qualified domain name.

   **Password**

   Enter your password for the provider.
5. Click **Save**. IBM Spectrum Protect Plus confirms a network connection, adds the provider to the database, and then catalogs the provider.

   To troubleshoot an application server after registration, use the **Actions** > **Test** function. This function verifies communication with the server, tests DNS settings between theIBM Spectrum Protect Plus appliance and the server, and installs the necessary agent on the server.

   Providers are automatically cataloged after registration. IBM Spectrum Protect Plus creates a high-level Inventory job and catalogs the objects on the provider. To manually run an Inventory job, click **Run Inventory** from the **Backup** pane.

**What to do next**

After you add the SQL Server provider, complete the following action:

| Action | How to |
|---|---|
| Assign user permissions to the hypervisor. | See “Creating a user role” on page 110. |

**Related concepts**

“User access” on page 105
Role-based access control allows you to set the resources and permissions available to IBM Spectrum Protect Plus user accounts.

**Related tasks**

“Creating a SQL Server backup job” on page 61
Use a backup job to back up SQL Server environments with snapshots.

“Creating a SQL Server restore job” on page 63
Use a restore job to restore SQL Server environments from snapshots. Your SQL Server clones can be utilized and consumed instantly through IBM Spectrum Protect Plus Instant Disk Restore jobs. IBM Spectrum Protect Plus catalogs and tracks all cloned instances.

## Creating a SQL Server backup job

Use a backup job to back up SQL Server environments with snapshots.

### Before you begin

During the initial base backup, IBM Spectrum Protect Plus creates a new vSnap volume and creates an NFS share. During incremental backups, the previously created volume is reused. The IBM Spectrum Protect Plus agent mounts the share on the SQL Server server where the backup is to be completed.

When the backup is complete, the IBM Spectrum Protect Plus agent unmounts the share from the SQL Server server and creates a vSnap snapshot of the backup volume.

Review the following procedures and considerations before you create a backup job definition:

- Register the providers that you want to back up. For more information, see “Adding a SQL Server provider” on page 60.
- Configure an SLA Policy. For more information, see “Configuring SLA policies” on page 11.
- Before an IBM Spectrum Protect Plus user can implement backup and restore operations, roles and resource groups must be assigned to the user. Grant users access to resources and backup and restore operations through the **Access** pane. For more information, see Chapter 10, “User access,” on page 105.
- Microsoft iSCSI Initiator must be enabled and running on the Windows server. An iSCSI route must be enabled between the SQL system and vSnap server. For more information, see https://technet.microsoft.com/en-us/library/ee338476(v=ws.10).aspx.
- Avoid configuring log backup for a single SQL database through multiple backup jobs. Logs are truncated during log backup operations. If a single SQL database is added to multiple job definitions with log backup enabled, a log backup from one job will truncate a log before it is backed up by the next job. This might cause point-in-time restore jobs to fail.
- IBM Spectrum Protect Plus does not support log backup of Simple recovery models.
- An AlwaysOn of a replica of a SQL Server cluster instance is not supported. Replicas are limited standalone SQL Server servers and instances.
- Failover of a SQL cluster instance during backup is not supported.

### Procedure

To create a SQL backup job definition, complete the following steps.

1. From the navigation menu, expand **Application**, then **SQL**. Click **Backup**.
2. Select a SQL Server instance to back up.

Use the search function to search for available instances and toggle the displayed instances through the **View** filter. The available options are **Standalone/Failover Cluster** and **AlwaysOn**.

3. Click **Select SLA Policy** to add an SLA Policy to the job definition that meets your backup data criteria.
4. To create the job definition by using default options, click **Save**. The job runs as defined by your SLA Policy, or can be run manually from the **Job Monitor** pane.
5. To edit options before you create the job definition, click **Select Options**. Set the job definition options.

   **Enable Log Backup**

   Select to enable IBM Spectrum Protect Plus to back up transaction logs and then protect the underlying disks.

   IBM Spectrum Protect Plus automatically truncates post log backups of databases that it backs up. If database logs are not backed up with IBM Spectrum Protect Plus, logs are not truncated by IBM Spectrum Protect Plus and must be managed separately.

   When SQL backup job completes with log backups enabled, all transaction logs up to the point of the job completing are purged from the SQL Server server. Log purging occurs only if the SQL Backup job completes successfully. If log backups are disabled during a rerun of the job, log purging does not occur.

   If a source database is overwritten, all old transaction logs up to that point are placed in a “condense” directory once the restoration of the original database completes. When the next run of the SQL Backup job completes, the contents of the condense folder is removed.

   To complete log backups, the SQL Server agent service user must be a local Windows administrator and must have the sysadmin permission enabled to manage SQL Server agent jobs. The agent will use that administrator account to enable and access log backup jobs. The IBM Spectrum Protect Plus SQL Server agent service user must also be the same as the SQL Server service and SQL Server agent service account for every SQL Server instance to be protected.

   To enable log backup schedule creation for multiple databases on the same SQL Server instance, ensure that all databases are added to the same SLA policy.

   When this option is selected, point-in-time restore options are available for SQL restore operations.

   **Maximum Parallel Streams per Database**

   Set the maximum data stream per database to the backup storage. This setting applies to each database in the job definition. Multiple databases can be backed up in parallel if the value of the option is set to **1**. Multiple parallel streams might improve backup speed, but high bandwidth consumption might affect overall system performance.
6. When you are satisfied that the job-specific information is correct, click **Save**.

   The job runs as defined by your SLA Policy, or can be run manually from the Job Monitor pane.
7. To configure additional options, click the **Options** field that is associated with the job in the **SLA Policy Status** section. If no additional options are currently configured for the job, **Not Configured** is shown in the field. Set the additional job options, and then click **Save**:

   **Pre-scripts and Post-scripts**

   In the **Pre-script** or **Post-script** section, select an uploaded script and a script server where the script will run. Scripts and script servers are configured through the **System** > **Script** pane.

   Pre-scripts and post-scripts are scripts that can be run before or after a job runs at the job level. Batch and PowerShell scripts are supported.

   Select **Continue scripts on error** to continue running the job if the script associated with the job fails.

   When this option is enabled, if a Pre-script or Post-script completes with a non-zero return code, the backup or restore is attempted and the Pre-script task status returns COMPLETED. If a Post-script completes with a non-zero return code, the Post-script task status returns COMPLETED.

   When this option is disabled, the backup or restore is not attempted, and the Pre-script or Post-script task status returns FAILED.

**Exclude Resources**

Exclude specific resources from the backup job through single or multiple exclusion patterns. Resources can be excluded through an exact match or with wildcard asterisks specified before the pattern (*test) or after the pattern (test*).

Multiple asterisk wildcards are also supported in a single pattern. Patterns support standard alphanumeric characters as well as the following special characters: - _ and *.

Separate multiple filters with a semicolon.

**What to do next**
After you create the backup job definition, complete the following action:

| Action | How to |
|---|---|
| Create a SQL Restore job definition. | See "Creating a SQL Server restore job" on page 63. |

**Related concepts**
"Configuring scripts for backup and restore operations" on page 74
Prescripts and postscripts are scripts that can be run before or after Backup and Restore jobs run at the job level. Supported scripts include shell scripts for Linux-based machines and Batch and PowerShell scripts for Windows-based machines. Scripts are created locally, uploaded to your environment through the **Scripts** pane, and then applied to job definitions.

## Creating a SQL Server restore job

Use a restore job to restore SQL Server environments from snapshots. Your SQL Server clones can be utilized and consumed instantly through IBM Spectrum Protect Plus Instant Disk Restore jobs. IBM Spectrum Protect Plus catalogs and tracks all cloned instances.

**Before you begin**
Note the following procedures and considerations before creating a restore job definition:

- Create and run a SQL Backup job. For more information, see "Creating a SQL Server backup job" on page 61.
- Review the SQL Server system requirements. See technote 2013790.
- Before an IBM Spectrum Protect Plus user can implement backup and restore operations, roles and resource groups must be assigned to the user. Grant users access to resources and backup and restore operations through the **Access** pane. For more information, see Chapter 10, "User access," on page 105.
- When completing a production restore to a SQL Server failover cluster, the root volume of the alternate file path must be eligible to host database and log files. The volume should belong to the destination SQL Server cluster server resource group, and be a dependency of the SQL Server cluster server.
- A restore to an NTFS or FAT compressed volume is not supported because of SQL Server database restrictions. For more information see https://support.microsoft.com/en-us/help/231347/description-of-support-for-sql-server-databases-on-compressed-volumes.
- When completing a point-in-time recovery, ensure that both the restore target SQL instance service and the IBM Spectrum Protect Plus SQL Server service use the same user account.
- When restoring to an alternate location, the SQL Server destination must be running the same version of SQL Server or a later version. For more information, see https://docs.microsoft.com/en-us/sql/t-sql/statements/restore-statements-transact-sql?view=sql-server-2017#compatibility-support.

### About this task

Instant Disk Restore leverages iSCSI or fibre channel protocols to provide immediate mount of LUNs without transferring data. Snapshotted databases are cataloged and instantly recoverable with no physical transfer of data.

The following restore modes are supported:

**Instant Access Mode**
In Instant Access Mode, no further action is taken after mounting the share. Users can perform any custom recovery using the files in the vSnap volume. An Instant Access restore of an AlwaysOn database is restored to the local destination instance.

**Test Mode**
In Test Mode, the agent creates a new database using the data files directly from the vSnap volume.

**Production Mode**
In Production Mode, the agent first restores the files from the vSnap volume back to primary storage and then spins up the new database using the restored files.

### Procedure

To create a SQL Restore job definition, complete the following steps:

1. From the navigation menu, expand **Application**, then **SQL**. Click **Restore**.
2. In the **Restore** pane, review the available recovery points of your SQL Servers servers.
3. Use the search function to search for available instances and toggle the displayed instances through the **View** filter. The available options are **Standalone/Failover Cluster** and **AlwaysOn**.
4. To select the latest recovery point, click the add to restore list icon at the resource level. Then, from the **Restore from site** list, select the site that is associated with the backup storage server that you want to recover from.

   To restore a specific recovery point from a specific site, expand a resource in the **Restore** pane, and then click the add to restore list icon that is associated with the recovery point. Click the delete icon to remove recovery points from the **Restore List**.
5. When log backup is enabled through a SQL backup job definition, point-in-time restore options are available for creating a SQL restore job definition.

   To complete a point-in-time recovery from a latest recovery point, add the recovery point to the **Restore List**, and complete the following steps:

   a) Click the point-in-time icon .

   The **Configure Point in Time** window opens.

   b) Select one of the following options, and then click **Save**:

   **By Time**
   Select this option to configure a point-in-time recovery by a specific date and time.

   **By Transaction ID**
   Select this option to configure a point-in-time recovery by transaction ID.

   In a standalone restore, IBM Spectrum Protect Plus finds the recovery points that directly proceed and follow the selected point-in-time. During the recovery, the older data backup volume and the newer log backup volume are mounted. A temporary recovery point is created if the point-in-time is after the last backup.

   In an AlwaysOn restore operation that is running in Test mode, the restored database is joined to the instance where the availability group resides. In an AlwaysOn restore operation that is running in Production mode, the restored primary database is joined to the availability group. The secondary database is restored by using the NORECOVERY option, and is kept in the target standalone instance.

6. To run the job now using default options, click **Restore**. To schedule the job to run using default options, click **Manage Jobs** and define a trigger for the job definition.
7. To edit options before you create the job definition, click **Options**. Set the job definition options.

   **Destination**

   Set the restore destination.

   **Restore to original location**

   Select to restore to the original server.

   **Restore to alternate location**

   Select to restore to a local destination different from the server, then select the alternate location from available servers.

   **New Database Name**

   Click the **New Database Name** field to enter an optional alternate name for the database.

   **Restore Type**

   Set the SQL Restore job to run in Test, Production, or Instant Access Mode by default. Once the job is created, it can be run in Test, Production, or Instant Access Mode through the **Job Sessions** pane.

   **Advanced Options**

   Set the advanced job definition options:

   **Rollback all the changes on failure** - Enable to automatically clean up allocated resources as part of a restore if the recovery fails.

   **Allow session overwrite** - Select this option to replace an existing database with the same name during recovery. When an Instant Disk Restore is performed for a database and another database with the same name is already running on the destination host/cluster, IBM Spectrum Protect Plus shuts down the existing database before starting up the recovered database. If this option is not selected, the restore job fails when IBM Spectrum Protect Plus encounters an existing running database with the same name.

   **Continue with restore even if it fails** - Toggle the recovery of a resource in a series if the previous resource recovery fails. If disabled, the Restore job stops if the recovery of a resource fails.

   **Overwrite existing database** - Enable to allow the restore job to overwrite the selected database. By default this option is disabled.

   **Recovery Mode** - If a database is restored with the **No recovery** option selected, the database is set to a restoring state. If managing transaction log backups without using IBM Spectrum Protect Plus, you can manually restore log files, and add the database to an availability group, assuming that the log sequence number of the secondary and primary database copies meet the criteria. The NORECOVERY option does not support Production mode restores to SQL AlwaysOn groups.

   **Protocol Priority (Instant Access only)** - If more than one storage protocol is available, select the protocol to take priority in the job. Available protocols are **iSCSI** and **Fibre Channel**.

   **Script Settings**

   In the **Pre-script** or **Post-script** section, select an uploaded script and a script server where the script will run. Scripts and script servers are configured through the **System** > **Script** pane.

   Pre-scripts and post-scripts are scripts that can be run before or after a job runs at the job level. Batch and PowerShell scripts are supported.

   Select **Continue scripts on error** to continue running the job if the script associated with the job fails.

   When this option is enabled, if a Pre-script or Post-script completes with a non-zero return code, the backup or restore is attempted and the Pre-script task status returns COMPLETED. If a Post-script completes with a non-zero return code, the Post-script task status returns COMPLETED.

When this option is disabled, the backup or restore is not attempted, and the Pre-script or Post-script task status returns FAILED.

8. Click **Save**.
9. To run the job now, click **Restore**. To schedule the job click **Manage Jobs** and define a trigger for the job definition.

**Related concepts**

"Configuring scripts for backup and restore operations" on page 74
Prescripts and postscripts are scripts that can be run before or after Backup and Restore jobs run at the job level. Supported scripts include shell scripts for Linux-based machines and Batch and PowerShell scripts for Windows-based machines. Scripts are created locally, uploaded to your environment through the **Scripts** pane, and then applied to job definitions.

**Related tasks**

"Adding a SQL Server provider" on page 60
Providers are servers that host objects and attributes. Once a provider is registered, an inventory of the provider is captured and added to IBM Spectrum Protect Plus, enabling you to perform backup and restore jobs, as well as run reports.

"Creating a SQL Server backup job" on page 61
Use a backup job to back up SQL Server environments with snapshots.

# Backing up and restoring Oracle data

To protect Oracle content, first register the application server so that IBM Spectrum Protect Plus recognizes it. Then create backup and restore job definitions, including SLA requirements such as job schedule and retention policies.

## Adding an Oracle provider

Providers are servers that host objects and attributes. Once a provider is registered, an inventory of the provider is captured and added to IBM Spectrum Protect Plus, enabling you to perform backup and restore jobs, as well as run reports.

**Procedure**

To register an Oracle provider, complete the following steps.

1. From the navigation menu, expand **Application**, then **Oracle**. Click **Backup**.
2. Click **Manage Application Servers**.
3. Click the add icon  .
4. Populate the fields in the **Application Properties** pane:

   **Host Address**

   Enter the resolvable IP address or a resolvable path and machine name.

   **Use existing user**

   Enable to select a previously entered user name and password for the provider.

   **Username**

   Enter your user name for the provider. The user identity follows the default domain\Name format if the virtual machine is attached to a domain. The format <local administrator> is used if the user is a local administrator.

   For Kerberos-based authentication only, the user identity must be specified in the username@FQDN format. The user name must be able to authenticate using the registered password to obtain a ticket-granting ticket (TGT) from the key distribution center (KDC) on the domain that is specified by the fully qualified domain name.

**Password**

Enter your password for the provider.

5. Click **Save**. IBM Spectrum Protect Plus confirms a network connection, adds the provider to the database, then catalogs the provider.

   To troubleshoot an application server after registration, use the **Actions** > **Test** function. This function verifies communication with the server, tests DNS settings between theIBM Spectrum Protect Plus appliance and the server, and installs the necessary agent on the server.

   Providers are automatically cataloged after registration. IBM Spectrum Protect Plus creates a high-level Inventory job and catalogs the objects on the provider. To manually run an Inventory job, click **Run Inventory** from the **Backup** pane.

**What to do next**

After you add the VMware provider, complete the following action:

| Action | How to |
|---|---|
| Assign user permissions to the hypervisor. | See "Creating a user role" on page 110. |

**Related concepts**

"User access" on page 105
Role-based access control allows you to set the resources and permissions available to IBM Spectrum Protect Plus user accounts.

**Related tasks**

"Creating an Oracle backup job" on page 67
Use a Backup job to back up Oracle environments with snapshots.

"Creating an Oracle restore job" on page 69
Use a Restore job to restore Oracle environments from snapshots. IBM Spectrum Protect Plus creates a vSnap clone from the version selected during the job definition creation and creates an NFS share. The IBM Spectrum Protect Plus agent then mounts the share on the Oracle server where the restore is to be performed. In the case of Oracle RAC, the restore is performed on all nodes in the cluster.

## Creating an Oracle backup job

Use a Backup job to back up Oracle environments with snapshots.

**Before you begin**

During the initial base backup, IBM Spectrum Protect Plus creates a new vSnap volume and creates an NFS share. During incremental backups, the previously created volume is reused. The IBM Spectrum Protect Plus agent mounts the share on the Oracle server where the backup is to be completed.

In the case of Oracle RAC, the backup is completed from any one node in the cluster. When the backup is complete, the IBM Spectrum Protect Plus agent unmounts the share from the Oracle server and creates a vSnap snapshot of the backup volume

Review the following procedures and considerations before you create a backup job definition:

- Register the providers that you want to back up. For more information, see "Adding an Oracle provider" on page 66.
- Configure an SLA Policy. For more information, see "Configuring SLA policies" on page 11.
- Before an IBM Spectrum Protect Plus user can implement backup and restore operations, roles and resource groups must be assigned to the user. Grant users access to resources and backup and restore operations through the **Access** pane. For more information, see Chapter 10, "User access," on page 105.
- To ensure that filesystem permissions are retained correctly when IBM Spectrum Protect Plus moves Oracle data between servers, ensure that the user and group IDs of the Oracle users (for example,

oracle, oinstall, dba) are consistent across all the servers. Refer to Oracle documentation for recommended uid and gid values.

- If an Oracle Inventory job runs at the same time or short period after an Oracle Backup job, copy errors might occur because of temporary mounts that are created during the Backup job. As a best practice, schedule Oracle Inventory jobs so that they do not overlap with Oracle Backup jobs.
- Point-in-time recovery is not supported when one or more datafiles are added to the database in the period between the chosen point-in-time and the time that the preceding Backup job ran.

**Procedure**

To create an Oracle backup job definition, complete the following steps.

1. From the navigation menu, expand **Application**, then **Oracle**. Click **Backup**.
2. Select Oracle homes, databases and ASM diskgroups to back up. Use the search function to search for available instances.
3. Click **Select SLA Policy** to add an SLA Policy to the job definition that meets your backup data criteria.
4. To create the job definition by using default options, click **Save**. The job runs as defined by your SLA Policy, or can be run manually from the **Job Monitor** pane.
5. To edit options before you create the job definition, click **Select Options**. Set the job definition options.

   **Enable Log Backup**

   Select to enable IBM Spectrum Protect Plus to automatically create a log backup volume and mount it to the application server. IBM Spectrum Protect Plus then uses cron to configure a scheduled job that completes a transaction log backup to that volume at the frequency specified through the **Frequency** setting.

   For Oracle Real Application Clusters (RAC), IBM Spectrum Protect Plus mounts the volume and configures the cron job on each of the cluster nodes. When the schedule is triggered, the jobs internally coordinate to ensure that any one active node completes the log backup and the other nodes take no action.

   IBM Spectrum Protect Plus automatically manages the retention of logs in its own log backup volume. After a successful database backup, older logs are deleted automatically from this log backup volume.

   IBM Spectrum Protect Plus does not manage the retention of other archived log locations. Administrators must continue to manage those logs using their existing log retention policies.

   When this option is selected, point-in-time restore options are available through for Oracle restore operations.

   **Maximum Parallel Streams per Database**

   Set the maximum data stream per database to the backup storage. This setting applies to each database in the job definition. Multiple databases can be backed up in parallel if the value of the option is set to **1**. Multiple parallel streams might improve backup speed, but high bandwidth consumption might affect overall system performance.
6. When you are satisfied that the job-specific information is correct, click **Save**.
7. To configure additional options, click the **Options** field that is associated with the job in the **SLA Policy Status** section. If no additional options are currently configured for the job, **Not Configured** is shown in the field. Set the additional job options, and then click **Save**:

   **Pre-scripts and Post-scripts**

   In the **Pre-script** or **Post-script** section, select an uploaded script and a script server where the script will run. Scripts and script servers are configured through the **System** > **Script** pane.

   Pre-scripts and post-scripts are scripts that can be run before or after a job runs at the job level. Windows-based machines support Batch and PowerShell scripts while Linux-based machines support shell scripts.

   Select **Continue scripts on error** to continue running the job if the script associated with the job fails.

When this option is enabled, if a Pre-script or Post-script completes with a non-zero return code, the backup or restore is attempted and the Pre-script task status returns COMPLETED. If a Post-script completes with a non-zero return code, the Post-script task status returns COMPLETED.

When this option is disabled, the backup or restore is not attempted, and the Pre-script or Post-script task status returns FAILED.

**Exclude Resources**

Exclude specific resources from the backup job through single or multiple exclusion patterns. Resources can be excluded through an exact match or with wildcard asterisks specified before the pattern (*test) or after the pattern (test*).

Multiple asterisk wildcards are also supported in a single pattern. Patterns support standard alphanumeric characters as well as the following special characters: - _ and *.

Separate multiple filters with a semicolon.

**What to do next**

After you create the backup job definition, complete the following action:

| Action | How to |
|---|---|
| Create an Oracle Restore job definition. | See "Creating an Oracle restore job" on page 69. |

**Related concepts**

"Configuring scripts for backup and restore operations" on page 74

Prescripts and postscripts are scripts that can be run before or after Backup and Restore jobs run at the job level. Supported scripts include shell scripts for Linux-based machines and Batch and PowerShell scripts for Windows-based machines. Scripts are created locally, uploaded to your environment through the **Scripts** pane, and then applied to job definitions.

## Creating an Oracle restore job

Use a Restore job to restore Oracle environments from snapshots. IBM Spectrum Protect Plus creates a vSnap clone from the version selected during the job definition creation and creates an NFS share. The IBM Spectrum Protect Plus agent then mounts the share on the Oracle server where the restore is to be performed. In the case of Oracle RAC, the restore is performed on all nodes in the cluster.

**Before you begin**

Note the following procedures and considerations before creating a Restore job definition:

- Create and run an Oracle Backup job. For more information, see "Creating an Oracle backup job" on page 67.
- Review the Oracle system requirements. See technote 2013790.
- Before an IBM Spectrum Protect Plus user can implement backup and restore operations, roles and resource groups must be assigned to the user. Grant users access to resources and backup and restore operations through the **Access** pane. For more information, see Chapter 10, "User access," on page 105.
- Point-in-time recovery is not supported when one or more data files are added to the database in the period between the chosen point-in-time and the time that the preceding backup job ran.

**About this task**

The following restore modes are supported:

**Instant Access Mode**

In Instant Access Mode, no further action is taken after mounting the share. Users can perform any custom recovery using the files in the vSnap volume. An Instant Access restore of an AlwaysOn database is restored to the local destination instance.

**Test Mode**
In Test Mode, the agent creates a new database using the data files directly from the vSnap volume.

**Production Mode**
In Production Mode, the agent first restores the files from the vSnap volume back to primary storage and then spins up the new database using the restored files.

### Procedure

To create an Oracle Restore job definition, complete the following steps:

1. From the navigation menu, expand **Application**, then **Oracle**. Click **Restore**.
2. In the **Restore** pane, review the available recovery points of your Oracle instances.
3. Use the search function to search for available instances and toggle the displayed instances through the **View** filter.
4. To select the latest recovery point, click the add to restore list icon at the resource level. Then, from the **Restore from site** list, select the site that is associated with the backup storage server that you want to recover from.

   To restore a specific recovery point from a specific site, expand a resource in the **Restore** pane, and then click the add to restore list icon that is associated with the recovery point. Click the delete icon to remove recovery points from the **Restore List**.
5. When log backup is enabled through an Oracle backup job definition, point-in-time restore options are available for creating an Oracle restore job definition.

   To complete a point-in-time recovery from a latest recovery point, add the recovery point to the **Restore List** and complete the following steps:

   a) Click the point-in-time icon .

   The **Configure Point in Time** window opens.

   b) Select one of the following options, and then click **Save**:

   **By Time**
   Select this option to configure a point-in-time recovery by a specific date and time.

   **By SCN**
   Select this option to configure a point-in-time recovery by System Change Number (SCN).

   IBM Spectrum Protect Plus finds the recovery points that directly proceed and follow the selected point-in-time. During the recovery, the older data backup volume and the newer log backup volume are mounted. A temporary recovery point is created if the point-in-time is after the last backup.
6. To run the job now using default options, click **Restore**. To schedule the job to run using default options, click **Manage Jobs** and define a trigger for the job definition.
7. To edit options before you create the job definition, click **Options**. Set the job definition options.

   **Destination**

   Set the restore destination.

   **Restore to original location**

   Select to restore to the original server.

   **Restore to alternate location**

   Select to restore to a local destination different from the server, then select the alternate location from available servers.

   **New Database Name**

   Click the **New Database Name** field to enter an optional alternate name for the database.

   **Restore Type**

Set the Oracle Restore job to run in Test, Production, or Instant Access Mode by default. Once the job is created, it can be run in Test, Production, or Instant Access Mode through the **Job Sessions** pane.

**Advanced Options**

Set the advanced job definition options:

**Rollback all the changes on failure** - Enable to automatically clean up allocated resources as part of a restore if the recovery fails.

**Allow session overwrite** - Select this option to replace an existing database with the same name during recovery. When an Instant Disk Restore is performed for a database and another database with the same name is already running on the destination host/cluster, IBM Spectrum Protect Plus shuts down the existing database before starting up the recovered database. If this option is not selected, the restore job fails when IBM Spectrum Protect Plus encounters an existing running database with the same name.

**Continue with restore even if it fails** - Toggle the recovery of a resource in a series if the previous resource recovery fails. If disabled, the Restore job stops if the recovery of a resource fails.

**Overwrite existing database** - Enable to allow the restore job to overwrite the selected database. By default this option is disabled.

**Init Params** - This option controls the initialization parameters that are used to start up the recovered database in Oracle Test and Production workflows.

**Source:** This is the default option. IBM Spectrum Protect Plus uses the same initialization parameters as the source database, but with the following changes:

- Parameters that contain paths such as control_files, db_recovery_file_dest, or log_archive_dest_* are updated to reflect the new paths based on the renamed mount points of the recovered volumes.
- Parameters such as audit_file_dest and diagnostic_dest are updated to point to the appropriate location under the Oracle Base directory on the destination server if the path differs from the source server.
- The db_name and db_unique_name are updated to reflect the new name of the database if a new name is specified.
- Cluster-related parameters such as instance_number, thread, and cluster_database are set automatically by IBM Spectrum Protect Plus depending on the appropriate values for the destination.

**Target:** Customize the initialization parameters by specifying a template file containing the initialization parameters that IBM Spectrum Protect Plus should use.

The specified path must be to a plain text file that exists on the destination server and is readable by the IBM Spectrum Protect Plus user. The file must be in Oracle pfile format, consisting of lines in the form name = value. Comments beginning with the # character are ignored.

IBM Spectrum Protect Plus reads the template pfile and copies the entries to the new pfile that will be used to start up the recovered database. However, the following parameters in the template are ignored. Instead, IBM Spectrum Protect Plus sets their values to reflect appropriate values from the source database or to reflect new paths based on the renamed mount points of the recovered volumes.

- control_files
- db_block_size
- db_create_file_dest
- db_recovery_file_dest
- log_archive_dest
- spfile
- undo_tablespace

Additionally, cluster-related parameters like instance_number, thread, and cluster_database are set automatically by IBM Spectrum Protect Plus depending on the appropriate values for the destination.

**Protocol Priority (Instant Access only)** - If more than one storage protocol is available, select the protocol to take priority in the job. Available protocols are **iSCSI** and **Fibre Channel**.

**Script Settings**

In the **Pre-script** or **Post-script** section, select an uploaded script and a script server where the script will run. Scripts and script servers are configured through the **System** > **Script** pane.

Pre-scripts and post-scripts are scripts that can be run before or after a job runs at the job level. Windows-based machines support Batch and PowerShell scripts while Linux-based machines support shell scripts.

Select **Continue scripts on error** to continue running the job if the script associated with the job fails.

When this option is enabled, if a Pre-script or Post-script completes with a non-zero return code, the backup or restore is attempted and the Pre-script task status returns COMPLETED. If a Post-script completes with a non-zero return code, the Post-script task status returns COMPLETED.

When this option is disabled, the backup or restore is not attempted, and the Pre-script or Post-script task status returns FAILED.

8. Click **Save**.
9. To run the job now, click **Restore**. To schedule the job click **Manage Jobs** and define a trigger for the job definition.

   **Note:** To perform a granular restore, first perform an Instant Access recovery. Doing this will mount a copy of the database to a temporary mount point at the following path: `/mnt/spp/vsnap/vpool/XX/fsYY`, where XX and YY are specific to your environment. This path will not be the same as the backup path because it is a new volume cloned from an older snapshot at the storage layer.

   Once the Instant Access volume is mounted, make a note of the new path which is shown in the job log. Using RMAN, run `catalog start with '<new path>'`. This will force RMAN to scan the new path and recognize the backups stored at that location. Granular restore commands, such as `restore datafile` should now work as expected.

**Related concepts**

“Configuring scripts for backup and restore operations” on page 74
Prescripts and postscripts are scripts that can be run before or after Backup and Restore jobs run at the job level. Supported scripts include shell scripts for Linux-based machines and Batch and PowerShell scripts for Windows-based machines. Scripts are created locally, uploaded to your environment through the **Scripts** pane, and then applied to job definitions.

**Related tasks**

“Adding an Oracle provider” on page 66
Providers are servers that host objects and attributes. Once a provider is registered, an inventory of the provider is captured and added to IBM Spectrum Protect Plus, enabling you to perform backup and restore jobs, as well as run reports.

## Catalog backup and restore operations

The IBM Spectrum Protect Plus catalog inventories and indexes all virtual machine snapshots. You can back up and restore the catalog.

Backing up the IBM Spectrum Protect Plus catalog protects the underlying databases.

### Creating a catalog backup job

Back up the IBM Spectrum Protect Plus catalog to protect underlying databases for disaster recovery scenarios. When running a Catalog Backup job, IBM Spectrum Protect Plus configuration settings,

recovery points, search data, and job information are backed up to a vSnap server that is defined in the associated SLA Policy.

**Before you begin**

It is recommended that you create SLA Policies specifically for backing up the catalog.

**Procedure**

To back up the catalog:

1. From the navigation menu, expand **System**, then **Catalog**. Click **Backup**.
2. Select one or more SLA Policies that meet your backup data criteria.
3. Click **Save** to create the job definition.

**Results**

The job runs as defined by your SLA Policy, or you can manually run the job from the **Job Monitor** pane.

**Related tasks**

"Configuring SLA policies" on page 11

SLA Policies allow administrators to create customized templates for the key processes involved in the creation and use of Backup jobs. Parameters are configured in SLA Policies, which can be used and re-used in Backup jobs.

## Creating a catalog restore job

Use a catalog restore job to restore the IBM Spectrum Protect Plus configuration settings, recovery points, search data, and job information that were backed up through catalog backup job. A catalog can be restored to the same location or another IBM Spectrum Protect Plus location.

**About this task**

**Attention:** A catalog restore overwrites all data in the IBM Spectrum Protect Plus virtual appliance and alternate virtual appliance. All IBM Spectrum Protect Plus operations stop while the catalog is being restored. The user interface is not accessible, and all jobs that are running are canceled. All snapshots that are created after the catalog backup ran are not saved.

**Procedure**

To restore the catalog:

1. From the navigation menu, expand **System**, then **Catalog**. Click **Restore**.
2. Select a vSnap server.

   A catalog can be restored to the same location, or an alternate location in disaster recovery scenarios.

   Available catalog snapshots for the server display.
3. Click **Restore** for the catalog snapshot that you want to restore.
4. Select one of the following restore modes:

   **Restore the catalog and suspend all scheduled jobs**
   The catalog is restored and all scheduled jobs are left in a suspended state. No scheduled jobs are started, which allows for the validation and testing of catalog entries and the creation of new jobs. Typically, this option is used in DevOps use cases.

   **Restore the catalog**
   The catalog is restored and all scheduled jobs continue to run as captured in the catalog backup. Typically, this option is used in disaster recovery.
5. Click **Restore**.
6. A confirmation dialog box displays. Click **Yes** to restore the catalog.

## Managing restore points in the catalog

Use the **Catalog Retention** pane to search for restore points in the IBM Spectrum Protect Plus catalog by Backup job name, view their creation and expiration dates, and override the assigned retention. The restore point is removed during the next run of the Maintenance job.

### Procedure

To restore for a restoration point and set it to expire:

1. From the navigation menu, expand **System**, then **Catalog**. Click **Retention**.
2. Enter a search string to search for a restore point by name. For more information about using the search function, see "Search guidelines" on page 115.
3. Use filters to fine-tune your search across job types (Hypervisor Backup, Application Backup, and Catalog Backup) and date range in which the associated backup job started.
4. Click the search icon .
5. Select **Actions** > **Expire** for the restore point that you want to expire.
6. Click **Yes** in the confirmation dialog box.

### Results

### Related concepts

"Maintenance job" on page 100
The Maintenance job removes resources and associated objects that are created by IBM Spectrum Protect Plus when a job that is in a pending state is deleted.

# Configuring scripts for backup and restore operations

Prescripts and postscripts are scripts that can be run before or after Backup and Restore jobs run at the job level. Supported scripts include shell scripts for Linux-based machines and Batch and PowerShell scripts for Windows-based machines. Scripts are created locally, uploaded to your environment through the **Scripts** pane, and then applied to job definitions.

### Considerations for hypervisors

Review the following considerations for using scripts with hypervisors:

- The user who is running the script must have the "Log on as a service" right enabled, which is required for running prescripts and postscripts. For more information about the "Log on as a service" right, see https://technet.microsoft.com/en-us/library/cc794944.aspx.
- Windows Remote Shell (WinRM) must be enabled.

## Uploading a script

Supported scripts include shell scripts for Linux-based machines and Batch and PowerShell scripts for Windows-based machines. Scripts must be created using the associated file format for the operating system.

### Procedure

Complete the following steps to upload a script:

1. From the navigation menu, expand **System**, and then click **Script**.
2. In the scripts section, click the add icon .
   The **Upload Script** pane displays.
3. Click **Browse** to select a local script to upload.
4. Click **Save**.

The script displays in the **Scripts** table and can be applied to supported jobs.

**What to do next**
After you upload the script, complete the following action:

| Action | How to |
|---|---|
| Add the script to a server from which it will run. | See "Adding a script to a server" on page 75. |

## Adding a script to a server

Add the script to a server from which it will run.

**Procedure**

Complete the following steps to designate a script to a server:

1. From the navigation menu, expand **System**, and then click **Script**.
2. In the script server section, click the add icon .
   The **Script Server Properties** pane displays.
3. Set the server options.

   **Host Address**

   Enter the resolvable IP address or a resolvable path and machine name.

   **Use existing user**

   Enable to select a previously entered user name and password for the provider.

   **Username**

   Enter your username for the provider. If entering a SQL server, the user identity follows the default domain\Name format if the virtual machine is attached to a domain. The format <local administrator> is used if the user is a local administrator.

   **Password**

   Enter your password for the provider.

   **OS Type**

   Select the operating system of the application server.
4. Click **Save**.

# Restoring a file

Recover files from a snapshot created through IBM Spectrum Protect Plus Backup jobs. Files can be restored to their original or alternate location.

**Before you begin**
Note the following procedures and considerations before restoring a file:

- Review the file indexing and restore requirements. See technote 2013790.
- Run a Backup job with Catalog file metadata enabled. Note that credentials must be established for the associated virtual machine as well as the alternate virtual machine destination through the Guest OS Username and Guest OS Password option within the backup job definition. Ensure the virtual machine can be accessed from the IBM Spectrum Protect Plus appliance either through DNS or hostname. In a Windows environment, the default security policy uses the Windows NTLM protocol, and the user identity follows the default domain\Name format if the Hyper-V virtual machine is attached to a domain. The format <local administrator> is used if the user is a local administrator.

**General considerations**

Encrypted Windows file systems are not supported for file cataloging or file restore.

For a file restore to complete successfully, ensure that the user on the target machine has the necessary ownership permissions of the file being restored. If a file was created by a user that differs from the user restoring the file based on their Windows security credentials, the file restore will fail.

File indexing and file restore are not supported from recovery points that were offloaded to IBM Spectrum Protectserver.

When restoring files in a Resilient File System (ReFS) environment, restores from newer versions of Windows Server to earlier versions are not supported. For example, restoring a file from Windows Server 2016 to Windows Server 2012 R2.

It is recommended that the IBM Spectrum Protect Plus appliance, storage arrays, hypervisors and application servers in your environment use an NTP server to synchronize the time zones across resources. If the clocks on the various systems are significantly out of sync, you may experience errors during application registration, metadata cataloging, Inventory, Backup, or Restore/File Restore jobs. For more information about identifying and resolving timer drift, see https://kb.vmware.com/s/article/1006072.

**Hyper-V considerations**

Only volumes on SCSI disks are eligible for file cataloging and file restore.

**Linux considerations**

If data resides on LVM volumes, the *lvm2-lvmetad* service must be disabled as it can interfere with the ability of IBM Spectrum Protect Plus to mount and re-signature volume group snapshots/clones. To disable:

- **`systemctl stop lvm2-lvmetad`**
- **`systemctl disable lvm2-lvmetad`**
- Edit the file `/etc/lvm/lvm.conf` and set **`use_lvmetad = 0`**

If data resides on XFS file systems and the version of xfsprogs is between 3.2.0 and 4.1.9, the file restore can fail due to a known issue in xfsprogs that causes corruption of a clone/snapshot file system when its UUID is modified. To resolve this issue, update xfsprogs to version 4.2.0 or above. For more information, see https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=782012.

**Procedure**

To restore a file, complete the following steps.

1. From the navigation menu, click **File Restore**.
2. Enter a search string to search for a file by name, and then click the search icon . For more information about using the search function, see “Search guidelines” on page 115.
3. Optional: Use filters to fine-tune your search across specific virtual machines, date range in which the file was protected, and virtual machine operating system types.

   Searches can also be limited to a specific folder through the **Folder path** field. The **Folder path** field supports wildcards. Position wildcards at the beginning, middle, or end of a string. For example, enter `*Downloads` to search within the `Downloads` folder without entering the preceding path.
4. To restore the file using default options, click **Restore**. The file is restored to its original location.
5. To edit options before restoring the file, click **Options**. Set the file restore options.

   **Overwrite existing files/folder**

   Replace the existing file or folder with the restored file or folder.

   **Destination**Select to replace the existing file or folder with the restored file or folder.

   Restore the file to its original location by selecting **Restore file(s) to original location**. Select **Restore file(s) to alternative location** to restore to a local destination different from the original location, then select the alternate location from available resources through the navigation tree or through the search function.

**Note:** If restoring to an alternate location, credentials must be established for the alternate virtual machine through the Guest OS Username and Guest OS Password option within the backup job definition.

Enter the VM folder path on the alternate destination in the **Destination Folder** field. Note that the directory will be created if it does not exist.

Click **Save** to save the options.

6. To restore the file using defined options, click **Restore**.

**Related tasks**

“Creating a VMware backup job” on page 43
Use a Backup job to back up VMware data including virtual machines, datastores, folders, vApps, and datacenters with snapshots.

“Creating a VMware restore job” on page 46
VMware Restore jobs support Instant VM Restore and Instant Disk Restore scenarios, which are created automatically based on the selected source.

# Chapter 7. Reports

IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

Before a user can run reports, permissions must be assigned to the user through a user role. See “Creating a user role” on page 110.

**Related concepts**

“User access” on page 105
Role-based access control allows you to set the resources and permissions available to IBM Spectrum Protect Plus user accounts.

## Types of reports

IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

Reports are based on the data that is collected by the most recent Inventory job. You can generate reports after all cataloging jobs and subsequent database condense jobs are completed. You can run the following types of reports:

- Backup storage utilization reports
- Protection reports
- System reports
- Virtual Machine environment reports

Reports include interactive elements, such as searching for individual values within a report, vertical scrolling, and column sorting.

### Backup storage utilization reports

IBM Spectrum Protect Plus provides backup storage utilization reports that display the storage utilization and status of your backup storage, such as vSnap servers.

Complete the following steps to view backup storage utilization reports:

1. Ensure that the user permissions for this report type are correct. See “Permission types ” on page 111.
2. Click **Report** from the navigation menu.
3. Expand **Backup Storage Utilization** in the Report pane.

The following reports are available:

**vSnap Storage Utilization Report**

Review the storage utilization of your vSnap servers, including the availability status, free space, and used space. The vSnap Storage Utilization displays both an overview of your vSnap servers and a detailed view of the individual virtual machines and databases that are protected on each vSnap server.

Use the report options to filter specific vSnap servers to display. For a detailed view of the individual virtual machines and databases that are protected on each vSnap server, select **Show Resources protected per vSnap Storage**. This area of the report displays the names of the virtual machines, associated hypervisor, location, and the compression/deduplication ratio of the vSnap server.

**Related concepts**

“Types of reports” on page 79

IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

## Protection reports

IBM Spectrum Protect Plus provides protection reports that display the protection status of your resources, and help ensure that your data is protected through user-defined recovery point objective parameters.

Complete the following steps to view protection reports:

1. Ensure that the user permissions for this report type are correct. See “Permission types ” on page 111.
2. Click **Report** from the navigation menu.
3. Expand **Protection** in the Report pane.

The following reports are available:

**Protected VMs report**

Run the Protected VMs report to view the protection status of your virtual machines. You can modify the report to show unprotected virtual machines and display the total number of virtual machines added to the IBM Spectrum Protect Plus inventory before backup jobs are started. Use the report options to filter by Hypervisor type and specific Hypervisors to display. To include unprotected virtual machines in the report, select **Show Unprotected VMs**. The **Summary View** displays an overview of your virtual machine protection status, including the number of unprotected and protected virtual machines and the managed capacity of the protected virtual machines. The managed capacity is the used capacity of a virtual machine. The **Detail View** provides further information about the protected and unprotected virtual machines, included names and location.

**Protected Databases report**

Run the Protected Databases report to view the protection status of your databases. You can modify this report to show unprotected databases, which will display the total number of databases added to the IBM Spectrum Protect Plus inventory before running backup jobs.

Use the report options to filter by database type and specific databases to display. To include unprotected databases in the report, select **Show Unprotected Databases**. To view databases that are protected through hypervisor-based backup jobs, select **Show Databases Protected as part of Hypervisor Backup**.

The **Summary View** displays an overview of your application server protection status, including the number of unprotected and protected databases, as well as the front end capacity of the protected databases. The front end capacity is the used capacity of a database. The **Detail View** provides further information about the protected and unprotected databases, included their names and location

**VM Backup History report**

Run the VM Backup History report to review the protection history of specific virtual machines. To run the report, at least one virtual machine must be specified in the **VMs** option. You can select multiple virtual machine names.

Use the report options to filter by failed or successful jobs and time of the last backup. The report can be further filtered by specific Service Level Agreement (SLA) policies. In **Detail View**, click the plus icon  next to an associated job to view further job details, such as the reason why a job failed or the size of a successful backup.

**Database Backup History report**

Run the Database Backup History report to review the protection history of specific databases. To run the report, at least one database must be specified in the **Databases** option. You can select multiple databases.

Use the report options to filter by failed or successful jobs and time of the last backup. The report can be further filtered by specific SLA policies. In **Detail View**, click the plus icon  next to an associated job to view further job details, such as the reason why a job failed or the size of a successful backup.

**VM SLA Policy Compliance report**

The VM SLA Policy Compliance report displays virtual machines in relation to recovery point objectives as defined in SLA policies. The report displays the following information:

- Virtual machines in compliance
- Virtual machines not in compliance
- Virtual machines in which the last backup job session failed

Use the report options to filter by Hypervisor type and specific Hypervisors to display. The report can be further filtered by virtual machines that are in compliance or not in compliance with the defined RPO.

**Database SLA RPO Compliance report**

The Database SLA RPO Compliance report displays databases in relation to recovery point objectives as defined in SLA policies. The report displays the following information:

- Databases in compliance
- Databases not in compliance
- Databases in which the last backup job session failed

Use the report options to filter by application type and specific application servers to display. The report can be further filtered by databases that are in compliance or not in compliance with the defined RPO, or by protection type, including data that was backed up to vSnap or by using replication.

**Related concepts**

"Types of reports" on page 79

IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

## System reports

IBM Spectrum Protect Plus provides system reports that display an in-depth view of the status of your configuration, including storage system information, jobs, and job status.

Complete the following steps to view system reports:

1. Ensure that the user permissions for this report type are correct. See "Permission types " on page 111.
2. Click **Report** from the navigation menu.
3. Expand **System** in the Report pane.

The following reports are available:

**Configuration report**

Review the configuration of the Hypervisor providers and Backup Storage available. Use the report options to filter the configuration types to display including Backup Storage, Hypervisors, or all. The report displays the name of the resource, resource type, associated site, and the SSL connection status.

**Job Report**

Review the available jobs in your configuration. Run the Job report to view jobs by type, their average runtime, and their successful run percentage. Use the report options to filter the job types to display and display jobs that run successfully over a period of time. The **Summary View** lists jobs by type along with the number of times a job session is run, completed, or failed. Job sessions listed as Other are jobs that are aborted, partially run, are currently running, skipped, or stopped. In the **Detail View**, click the plus icon  next to an associated job to view further job details such as virtual machines protected by a Backup job, the average runtime, and the next scheduled runtime if the job is scheduled.

**License Report**

Review the configuration of your IBM Spectrum Protect Plus environment in relation to licensed features. The following sections and fields display in the License report:

**Virtual Machine Protection**
The **Total Number of VMs** field displays the total number of virtual machines protected through hypervisor backup jobs, plus the number of virtual machines hosting application databases protected through application backup jobs (not hypervisor backup jobs). The **Front End Capacity** field displays the used size of these virtual machines.

**Virtual Machine ProtectionPhysical Machine Protection**
The **Total Number of Physical Servers** field displays the total number of physical application servers hosting databases protected through application backup jobs. The **Front End Capacity** field displays the used size of these physical application servers.

**Backup Storage Utilization (vSnap)**
The **Total Number of vSnap Servers** field displays the number of vSnap server configured in IBM Spectrum Protect Pluss as a backup destination. The **Target Capacity** field displays the total used capacity of the vSnap servers, excluding replica destination volumes.

**Related concepts**
"Types of reports" on page 79
IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

## VM Environment reports

IBM Spectrum Protect Plus provides VM environment reports to display the storage utilization and status of your virtual machines and datastores.

Complete the following steps to view VM environment reports:

1. Ensure that the user permissions for this report type are correct. See "Permission types " on page 111.
2. Click **Report** from the navigation menu.
3. Expand **VM Environment** in the Report pane.

The following reports are available:

**VM Datastores report**

Review the storage utilization of your datastores, including the total free space, provisioned space, and capacities. Run the VM Datastores report to view your datastores, the number of virtual machines on the datastores, and the percentage of space available. Use the report options to filter by Hypervisor type and specific Hypervisors to display. The **Detail View Filter** controls the datastores to display in the Detail View based on the percentage of space used. Use the **Show Only Orphaned Datastores** filter to view datastores that do not have any virtual machines assigned to them, or virtual machines that are in an inaccessible state. The reason for a datastore to be in an orphaned state is displayed in the Datastore field in the Detail View.

**VM LUNs report**

Review the storage utilization of your VM LUNs. Run the VM LUNs report to view your LUNs, associated datastores, capacities, and storage vendors. Use the report options to filter by Hypervisor type and specific Hypervisors to display. Use the **Show Only Orphaned Datastores** filter to view datastores that do not have any virtual machines assigned to them, or virtual machines that are in an inaccessible state.

**VM Snapshot Sprawl report**

The VM Snapshot Sprawl report displays the age, name, and number of snapshots that are used to protect your Hypervisor resources. Use the report options to filter by Hypervisor type and specific Hypervisors to display. Use the **Snapshot Creation Time** filter to display snapshots from specific periods of time.

**VM Sprawl report**

Review the status of your virtual machines, including virtual machines that are powered off, powered on, or suspended. Run the VM Sprawl report to view unused virtual machines, the date and time they were powered off, and virtual machine templates. Use the report options to filter by Hypervisor type

and specific Hypervisors to display. The report can be further filtered by power state over time, including Days Since Last Powered Off and Days Since Last Suspended. The Quick View section displays a pie chart of used and free space on your virtual machines based on power state. Use the Hypervisor parameter to display virtual machines on all hosts or a specific host. The Detail Views are categorized by power state, and a separate table for VM templates.

**VM Storage report**

Review your virtual machines and associated datastores through the VM Storage report. View associated

datastores and provisioned space of the datastores. Use the report options to filter by Hypervisor type and specific Hypervisors to display. The Detail View displays associated datastores and the amount of space on the datastore that is allocated for virtual disk files.

**Related concepts**

"Types of reports" on page 79
IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

# Report actions

You can run, save, or schedule reports in IBM Spectrum Protect Plus.

## Running a report in IBM Spectrum Protect Plus

You can run IBM Spectrum Protect Plus reports with predefined default parameters or run customized reports that are driven by custom parameters.

### Before you begin

Before you run reports, ensure that the user permissions for this report type are correct. See "Permission types " on page 111.

### Procedure

Complete the following steps to run a report in IBM Spectrum Protect Plus:

1. From the navigation menu, click **Report**.
2. Expand a report type and select a report to run.
3. Run the report either with custom parameters or default parameters:
   - To run the report with custom parameters, click **Options**, set the report parameters, and click **Run**. Parameters are unique to each report.
   - To run the report with default parameters, click **Run**.

### What to do next

Review the report in the **Report** pane.

**Related concepts**

"Reports" on page 79

IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

## Saving a report in IBM Spectrum Protect Plus

You can modify predefined reports with custom parameters in IBM Spectrum Protect Plus and save the customized reports.

### Before you begin

Before you run reports, ensure that the user permissions for this report type are correct. See “Permission types ” on page 111.

### Procedure

Complete the following steps to save a report in IBM Spectrum Protect Plus:

1. From the navigation menu, click **Report**.
2. Select a predefined report.
3. Set your customized parameters.
4. Define the report to run in one of the following circumstances:
   - Run on demand.
   - Create a schedule to run the report as defined by the parameters of the schedule.
5. Save the report with a customized name.

### What to do next

Run the report and review the report in the **Report** pane.

### Related concepts

“Reports” on page 79
IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

## Scheduling a report in IBM Spectrum Protect Plus

You can schedule customized reports in IBM Spectrum Protect Plus to run at specific times.

### Before you begin

Before you run reports, ensure that the user permissions for this report type are correct. See “Permission types ” on page 111.

### Procedure

Complete the following steps to save a report in IBM Spectrum Protect Plus:

1. From the navigation menu, click **Report**.
2. Select a report type.
3. Select the report that you want to schedule.
4. Click **Options** to edit the report parameters.
5. Enter values in the **Name** and **Description** fields for the report.
6. Set the parameters for the report.
7. Click **Schedule Report** to expand the schedule editor.
8. Define a trigger for the report.
9. Enter an address to receive the scheduled report in the email field, and then click **Add a recipient**.
10. Click **Save**.

### What to do next

After the report runs to schedule, review the report in the email that you receive from the scheduled report.

### Related concepts

“Reports” on page 79
IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

# Chapter 8. System management

You use the **System** menu to configure and monitor your IBM Spectrum Protect Plus environment.

You use the **System** menu to complete the following tasks:

- Create and configure accounts.
- View scheduled jobs.
- View audit logs.
- Monitor the status of your VADP proxies.

**Related concepts**

“Types of reports” on page 79
IBM Spectrum Protect Plus provides a number of predefined reports that you can customize to meet your specific reporting requirements.

## Managing providers

You can register SMTP providers or LDAP providers in the IBM Spectrum Protect Plus system environment. You can also create VDAP proxies.

**Related concepts**

“Managing user accounts” on page 112
Before a user can log on to IBM Spectrum Protect Plus and use the available functions, an administrator must add the user account to IBM Spectrum Protect Plus.

### Registering an SMTP provider in IBM Spectrum Protect Plus

System administrators can add an SMTP provider to IBM Spectrum Protect Plus to enable email communications. You can associate only one SMTP server with IBM Spectrum Protect Plus.

#### Before you begin

Ensure that you have one of the following levels of user privileges:

- Native Administrator
- Administrator

#### Procedure

Complete the following steps to register an SMTP server in IBM Spectrum Protect Plus:

1. From the navigation menu, expand **System** and click **LDAP / SMTP**.
2. From the SMTP table, click **Add**.
3. Populate the following fields in the **SMTP Settings** pane:

**Host Address**

The IP address of the host or the path and host name.

**Port**

The communications port of the provider that you are adding. The typical default port is 25 for non SSL connections or 443 for SSL connections.

**Username**

The name that is used to access the provider.

**Password**

The password that is associated with the user name.

**Timeout**

Set the email timeout value in milliseconds.

**From Address**

Set the address that is associated with email communications from IBM Spectrum Protect Plus.

**Subject Prefix**

Set a prefix to add to the email subject lines sent from IBM Spectrum Protect Plus.

4. Click **Save**.
   IBM Spectrum Protect Plus completes the following actions:
   a. Confirms that a network connection is made.
   b. Adds the provider to the database.

**What to do next**

If a message is returned indicating that the connection is unsuccessful, review your entries. If your entries are correct and the connection is unsuccessful, contact a system administrator to review the connections.

**Related concepts**

"Managing user accounts" on page 112
Before a user can log on to IBM Spectrum Protect Plus and use the available functions, an administrator must add the user account to IBM Spectrum Protect Plus.

## Registering LDAP providers in IBM Spectrum Protect Plus

System administrators can add LDAP providers to enable users to be provisioned and access IBM Spectrum Protect Plus by using LDAP user names and passwords. You can associate only one LDAP server with IBM Spectrum Protect Plus.

**Before you begin**

Ensure that you have one of the following levels of user privileges:

- Native Administrator
- Administrator

**Procedure**

Complete the following steps to register an LDAP server in IBM Spectrum Protect Plus:

1. From the navigation menu, expand **System** and click **LDAP / SMTP**.
2. From the LDAP table, click **Add**.
3. Populate the following fields in the **SMTP Settings** pane:

   **Host Address**

   The IP address of the host or logical name of the LDAP server.

   **Port**

   The port on which the LDAP server is listening. The typical default port is 389 for non SSL connections or 636 for SSL connections.

   **SSL**

   Enable the SSL option to establish a secure connection to the LDAP server.

**Bind Name**

The Bind Distinguished Name that is used for authenticating the connection to the LDAP server. IBM Spectrum Protect Plus supports simple bind.

**Password**

The password that is associated with the Bind Distinguished Name.

**Base DN**

The location where users and groups can be found.

**User Filter**

A filter to select only those users in the Base DN that match certain criteria. An example of a valid default user filter is `cn={0}`.

**Tips:**

- To enable authentication by using the **sAMAccountName** Windows user naming attribute, set the filter to `samaccountname={0}`. When this filter is set, users log in to IBM Spectrum Protect Plus by using only a user name. A domain is not included.
- To enable authentication using the user principal name (UPN) naming attribute, set the filter to `userprincipalname={0}`. When this filter is set, users log in to IBM Spectrum Protect Plus by using the username@domain format.
- To enable authentication by using an email address that is associated with LDAP, set the filter to `mail={0}`.

The **User Filter** setting also controls the type of user name that appears in the IBM Spectrum Protect Plus display of users.

**User RDN**

The relative distinguished path for the user. Specify the path where user records can be found. An example of a valid default RDN is `cn=Users`.

**Group RDN**

The relative distinguished path for the group. If the group is at a different level than the user path, specify the path where group records can be found.

4. Click **Save**.

   IBM Spectrum Protect Plus completes the following actions:

   a. Confirms that a network connection is made.

   b. Adds the provider to the database.

**What to do next**

If a message is returned indicating that the connection is unsuccessful, review your entries. If your entries are correct and the connection is unsuccessful, contact a system administrator to review the connections.

**Related concepts**

“Managing user accounts” on page 112

Before a user can log on to IBM Spectrum Protect Plus and use the available functions, an administrator must add the user account to IBM Spectrum Protect Plus.

## Managing VADP backup proxies

In IBM Spectrum Protect Plus, you can create proxies to run VMware backup jobs through vStorage API for Data Protection (VADP) in Linux environments. The proxies reduce demand on system resources by enabling load sharing and load balancing.

The backup of a VMware virtual machine includes the following files:

- VMDKs corresponding to all disks. The base backup captures all allocated data, or all data if disks are on NFS datastores. Incremental backups will capture only changed blocks since the last successful backup.
- Virtual machine templates
- VMware files with the following extensions:
  - .vmx
  - .vmfx (if available)
  - .nvram (stores the state of the virtual machine BIOS)

If proxies exist, the entire processing load is shifted off the host system and onto the proxies. If proxies do not exist, the entire load stays on the host. Within a backup job, the processing load for any single VM is shifted to a single proxy system; multiple VMs are shifted to multiple proxies if they are available.

If a proxy server goes down or is otherwise unavailable before the start of the job, the other proxies take over and the job completes. If no other proxies exist, the host takes over the job. If a proxy server becomes unavailable when a job is running, the job might fail.

### Creating VADP backup proxies

You can create VADP proxies to run VMware backup jobs with IBM Spectrum Protect Plus in Linux environments.

#### Before you begin

Note the following considerations before creating VADP proxies:

- Review the IBM Spectrum Protect Plus system requirements. See technote 2013790.
- The IBM Spectrum Protect Plus version of the VADP Proxy installer includes Virtual Disk Development Kit (VDDK) version 6.5. This version of the VADP proxy installer provides the external VADP Proxy support with vSphere 6.5.

#### Procedure

To create VMware VADP proxies, complete the following steps.

1. From the navigation menu, expand **System**, and then click **VADP Poxy**.
2. Click the add icon  .
3. Complete the following fields in the **Install VADP Proxy** pane:

   **Hostname/IP**

   Enter the resolvable IP address or a resolvable path and machine name.

   **Username**

   Enter the user name for the VADP proxy server.

   **Password**

   Enter the password name for the VADP proxy server.
4. Click **Install**.

   The proxy is added to the **VADP Proxy** table.
5. From the **Site** field, select a site to associate with the proxy.
6. Click **Register** to register the proxy server.

   You can unregister or suspend the server by using the **Actions** menu. Suspending a proxy prevents upcoming backup jobs from using the proxy, and jobs that use a suspended or unregistered proxy will run locally, which may impact performance. You can complete maintenance tasks on the proxy while it is suspended. To resume usage of the proxy, select **Actions** > **Resume** .

   After successful registration, the service vadp is started on the proxy machine. A log file `vadp.log` is generated in `/opt/IBM/SPP/logs` directory.

7. Repeat the previous steps for each proxy you want to create.

**What to do next**

After you create the VADP proxies, complete the following actions:

| Action | How to |
|---|---|
| Run the VMware backup job. | See "Creating a VMware backup job" on page 43.<br>The proxies are indicated in the job log by a log message similar to the following text:<br>`Run remote vmdkbackup of MicroService: http://<proxy`<br>*`nodename`*`, IP:`*`proxy_IP_address`* |
| Uninstall the proxies when you cease running the VMware backup jobs. | To uninstall a proxy, run the following command on the host system from the uninstall subdirectory of the installation directory `/opt/IBM/SPP`:<br>`./uninstall_vmdkbackup` |

**Related tasks**

"Setting options for VADP backup proxies" on page 91
You can create VADP proxies to run VMware backup jobs with IBM Spectrum Protect Plus in Linux environments.

**Setting options for VADP backup proxies**

You can create VADP proxies to run VMware backup jobs with IBM Spectrum Protect Plus in Linux environments.

**Procedure**

To set options for VMware VADP proxies, complete the following steps.

1. From the navigation menu, expand **System**, and then click **VADP Poxy**.
2. Select **Actions** > **Set Options** for the proxy:
3. Complete the following fields in the **Set VADP Proxy Options** pane:

   **Site**

   Assign a site to the proxy.

   **Transport Modes**

   Set the transport modes to be used by the proxy. For more information about VMware transport modes, see https://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkDataStruct.5.5.html.

   **Enable NBDSSL Compression**

   If you selected the NBDSSL transport mode, enable compression to increase the performance of data transfers.

   To turn off compression, select **disabled**.

   **Log retention in days**

   Set the number of days to retain logs before they are deleted.

   **Read and write buffer size**

   Set the buffer size of the data transfer, measured in bytes.

   **Block size of NFS volume**

Set the block size to be used by the mounted NFS volume, measured in bytes.

**What to do next**

After you create the VADP proxies, complete the following actions:

| Action | How to |
|---|---|
| Run the VMware backup job. | See "Creating a VMware backup job" on page 43.<br>The proxies are indicated in the job log by a log message similar to the following text:<br>`Run remote vmdkbackup of MicroService: http://<proxy`<br>*`nodename`*`, IP:`*`proxy_IP_address`* |
| Uninstall the proxies when you cease running the VMware backup jobs. | To uninstall a proxy, run the following command on the host system from the uninstall subdirectory of the installation directory `/opt/IBM/SPP`:<br>`./uninstall_vmdkbackup` |

**Related tasks**

"Creating VADP backup proxies" on page 90
You can create VADP proxies to run VMware backup jobs with IBM Spectrum Protect Plus in Linux environments.

# Managing user activities

Users can run job sessions on demand in IBM Spectrum Protect Plus, pause, or cancel running jobs, and hold all future scheduled instances of a job. You can also collect searchable audit logs for user activities in IBM Spectrum Protect Plus.

## Starting jobs in IBM Spectrum Protect Plus

Users with an account in IBM Spectrum Protect Plus can start jobs on demand.

**Before you begin**

Ensure that you have a valid user account in IBM Spectrum Protect Plus.

**Procedure**

Complete the following steps to start jobs in IBM Spectrum Protect Plus:

1. From the navigation menu, expand **System** and click **Job Monitor**.
2. To start the job session, click the **Actions** menu that is associated with the job that you want to start and click **Start**.
3. Click **Expand** next to the running job session to view the job session details.

   The following items are included in the job session details:

   - Duration of the job
   - Start time of the job
   - End time of the job
   - Total number of protected VMs
   - Total number of failed VMs

**Related concepts**

"Managing user accounts" on page 112
Before a user can log on to IBM Spectrum Protect Plus and use the available functions, an administrator must add the user account to IBM Spectrum Protect Plus.

## Holding and releasing jobs in IBM Spectrum Protect Plus

Users with an account in IBM Spectrum Protect Plus can start jobs on demand.

**Before you begin**

Ensure that you have a valid user account in IBM Spectrum Protect Plus.

**Procedure**

Complete the following steps to hold and release jobs in IBM Spectrum Protect Plus:

1. From the navigation menu, expand **System** and click **Job Monitor**.
2. To hold a scheduled job, click the **Actions** menu that is associated with the job that you want to hold and click **Hold Schedule**.
3. To release the scheduled job, click the **Actions** menu that is associated with the job that you want to release and click **Release Schedule**.

**Related concepts**

"Managing user accounts" on page 112
Before a user can log on to IBM Spectrum Protect Plus and use the available functions, an administrator must add the user account to IBM Spectrum Protect Plus.

## Collecting audit logs for actions in IBM Spectrum Protect Plus

Users with an account in IBM Spectrum Protect Plus can collect searchable audit logs for actions that are completed in IBM Spectrum Protect Plus.

**Before you begin**

Ensure that you have a valid user account in IBM Spectrum Protect Plus.

**Procedure**

Complete the following steps to collect audit logs for actions in IBM Spectrum Protect Plus.

1. From the navigation menu, expand **System** and click **Audit log**.
2. Review the following information in the **Audit Log** pane:
   - A log of actions that were completed in IBM Spectrum Protect Plus.
   - The users who completed the actions.
   - A description of each action.
3. To search for the actions of a specific user in IBM Spectrum Protect Plus, enter the user name in the search user field.
4. Optional: Expand the **Filters** section to further filter the displayed logs. Enter specific action descriptions and a date range in which the action was completed.
5. Click the search icon .
6. To download the audit log as a `.csv` file, click **Download**, and then select a location to save the file.

**Related concepts**

"Managing user accounts" on page 112

Before a user can log on to IBM Spectrum Protect Plus and use the available functions, an administrator must add the user account to IBM Spectrum Protect Plus.

## Managing sites

A site is a user-defined grouping of backup storage servers that is generally based on location to help quickly identify and interact with backup data. Once sites are created in IBM Spectrum Protect Plus, they can be applied to your backup storage servers.

### Adding a site

Once sites are added in IBM Spectrum Protect Plus, they can be applied to your backup storage servers.

**Procedure**

To add a site, complete the following steps:

1. From the navigation menu, expand **System**, and then click **Site**.
2. Click the add icon .
   The **Site Properties** pane displays.
3. Enter a site name, and then click **Save**.
   The site displays in the **Site** table and can be applied to new and existing backup storage servers.

### Editing a site

Revise site names and descriptions to reflect changes in your IBM Spectrum Protect Plus environment.

**Procedure**

To edit a site, complete the following steps:

1. From the navigation menu, expand **System**, and then click **Site**.
2. Click the edit icon that is associated with a site.
   The **Site Properties** pane displays.
3. Revise the site name, and then click **Save**.
   The revised site appears in the **Site** table and can be applied to new and existing backup storage.

### Deleting a site

Delete a site when it becomes obsolete. Ensure that you reassign your backup storage to different sites before deleting the site.

**Procedure**

To delete a site, complete the following steps:

1. From the navigation menu, expand **System**, and then click **Site**.
2. Click the delete icon that is associated with a site.
3. Click **Yes** to delete the site.

# Managing identities

Some features in IBM Spectrum Protect Plus require credentials to access your resources. For example, IBM Spectrum Protect Plus connects to Oracle servers as the local operating system user that is specified during registration to complete tasks like cataloging, data protection, and data restore.

User names and passwords for your resources can be added and edited through the **Identity** pane. Then when utilizing a feature in IBM Spectrum Protect Plus that requires credentials to access a resource, select **Use existing user**, and select an identity from the drop-down menu.

## Adding an identity

Add an identity to provide user credentials.

### Procedure

To add an identity, complete the following steps:

1. From the navigation menu, expand **System**, and then click **Identity**.
2. Click the add icon .
3. Complete the fields in the **Identify Properties** pane:

   **Name**

   Enter a meaningful name to help identify the identity.

   **Username**

   Enter the user name that is associated with a resource, such as a SQL or Oracle server.

   **Password**

   Enter the password that is associated with a resource.
4. Click **Save**.

   The identity displays in the **Identity** table and can be selected when utilizing a feature that requires credentials to access a resource through the **Use existing user** option.

## Editing an identity

Revise an identity to change the user name and password used to access an associated resource.

### Procedure

To edit an identity, complete the following steps:

1. From the navigation menu, expand **System**, and then click **Identity**.
2. Click the edit icon that is associated with an identity.

   The **Identify Properties** pane displays.
3. Revise the identity name, user name, and password.
4. Click **Save**.

   The revised identity displays in the **Identity** table and can be selected when utilizing a feature that requires credentials to access a resource through the **Use existing user** option.

## Deleting an identity

Delete an identity when it becomes obsolete.

### Procedure

To delete an identity, complete the following steps:

1. From the navigation menu, expand **System**, and then click **Identity**.

2. Click the delete icon  that is associated with an identity.
3. Click **Yes** to delete the identity.

# Chapter 9. Maintenance

System administrators can perform maintenance tasks on the IBM Spectrum Protect Plus application. Maintenance tasks include collecting logs, updating the application, and reviewing the configuration of the virtual appliance.

In most cases, IBM Spectrum Protect Plus is installed on a virtual appliance. The virtual appliance contains the application and the Inventory. Maintenance tasks are performed in vSphere Client, through the IBM Spectrum Protect Plus command line, or through a web-base management console.

Maintenance tasks are performed by a system administrator. A system administrator is usually a senior-level user who designed or implemented the vSphere and ESX infrastructure, or a user with an understanding of IBM Spectrum Protect Plus, VMware, and Linux command-line usage.

Infrastructure updates are managed by IBM's update facilities. The Administrative Console serves as the primary means for updating IBM Spectrum Protect Plus features and underlying infrastructure components, including the operating system and file system. ZFS update packages are also provided for vSnap stand-alone instances.

**CAUTION:** Update underlying components of IBM Spectrum Protect Plus only by using IBM's update facilities.

## Managing the Administrative Console

Log on to the Administrative Console to review the configuration of the IBM Spectrum Protect Plus virtual appliance. Available information includes general system settings, network, and proxy settings.

### Procedure

To manage the Administrative Console, complete the following steps:

1. From a supported browser, enter the following URL:

   ```
   https://HOSTNAME:8090/
   ```

   Where *HOSTNAME* is the IP address of the virtual machine where the application is deployed.
2. In the login window, select one of the following authentication types in the **Authentication Type** list:

| Authentication Type | Login information |
|---|---|
| **IBM Spectrum Protect Plus** | To log in as an IBM Spectrum Protect Plus user with SYSADMIN privileges, enter your administrator user name and password. |
| **System** | To login as a system user, enter the system password. The default password is sppadLG235. You are prompted to change this password during the first login. |

3. Review the available options for the virtual appliance.

**Related concepts**

"Managing user roles" on page 109

Roles define the actions that can be completed for the resources that are defined in a resource group. While a resource group defines the resources that are available to an account, a role sets the permissions to interact with the resources that are defined in the resource group.

## Setting the time zone

Use the Administrative Console to set the time zone of the IBM Spectrum Protect Plus appliance.

### Procedure

To set the time zone, complete the following steps:

1. From a supported browser, enter the following URL:

   ```
   https://HOSTNAME:8090/
   ```

   Where *HOSTNAME* is the IP address of the virtual machine where the application is deployed.
2. In the login window, select one of the following authentication types in the **Authentication Type** list:

| Authentication Type | Login information |
|---|---|
| **IBM Spectrum Protect Plus** | To log in as an IBM Spectrum Protect Plus user with SYSADMIN privileges, enter your administrator user name and password. |
| **System** | To login as a system user, enter the system password. The default password is `sppadLG235`. You are prompted to change this password during the first login. |

3. Click **Perform System Actions**.
4. In the **Change Time Zone** section, select your time zone.

   A message stating that the operation was successful displays. All IBM Spectrum Protect Plus logs and schedules will reflect the selected time zone. The selected time zone will also display on the IBM Spectrum Protect Plus appliance when logged in as a root user.
5. To view the current time zone, select **Product Information** from the main page of the Administrative Console.

## Uploading an SSL certificate from the administrative console

To establish secure connections in IBM Spectrum Protect Plus, you can upload an SSL certificate such as an HTTPS or LDAP certificate by using the administrative console.

### About this task

For HTTPS certificates, PEM encoded certificates with `.cer` or `.crt` extensions are supported.

For LDAP/Hyper-V certificates, DER encoded certificates with `.cer` or `.crt` extensions are supported. If you are uploading an LDAP SSL certificate, ensure that IBM Spectrum Protect Plus has connectivity to the LDAP server and that the LDAP server is running.

ASCII and binary format certificates are accepted with the standard `.pem`, `.cer`, and `.crt` file extensions. However, the administrative console certificate import function cannot be used to update the appliance SSL web server communications; however, SSL can be updated using the procedure in “Uploading an SSL certificate from the command line” on page 99

### Procedure

To upload an SSL certificate, complete the following steps:

1. Contact your network administrator for the name of the certificate to export.
2. From a supported browser, export the certificate to your computer. Make note of the location of the certificate on your computer. The process of exporting certificates varies based on your browser.
3. From a supported browser, enter the following URL:

   ```
   https://HOSTNAME:8090/
   ```

   where *HOSTNAME* is the IP address of the virtual machine where the application is deployed.
4. In the login window, select one of the following authentication types in the **Authentication Type** list:

| Authentication Type | Login information |
|---|---|
| **IBM Spectrum Protect Plus** | To log in as an IBM Spectrum Protect Plus user with SYSADMIN privileges, enter your administrator user name and password. |
| **System** | To login as a system user, enter the system password. The default password is `sppadLG235`. You are prompted to change this password during the first login. |

5. Click **Manage your certificates**.
6. Click **Browse**, and select the certificate that you want to upload.
7. Click **Upload SSL certificate for HTTPS**.
8. Restart the virtual machine where the application is deployed.

## Uploading an SSL certificate from the command line

ASCII and binary format certificates are accepted with the standard `.pem`, `.cer`, and `.crt` file extensions.

### About this task

This process requires that you package the private key, public key, and chain certificates into a PKCS12 format file (often referred to as PFX file with .p12 extension) and import this manually into the IBM Spectrum Protect Plus Java keystore. The procedure assumes you already have the private, public, and all supporting security objects provided by your security vendor packaged into a PKCS12 format file named *name*`.p12`.

If you do not have this file, you must work with your security vendor using a separate server and/or OpenSSL to generate the necessary certificate signing request. Once received, package the resulting private, public, and chain certificate objects into the required file referenced below.

### Procedure

To import the *name*`.p12` file, complete the following steps:

1. Log in as root user on the IBM Spectrum Protect Plus virtual appliance.
2. At the command line execute the following command:

   ```
   /usr/java/latest/bin/keytool -importkeystore -deststorepass ecx-beta -
   destkeystore /opt/virgo/configuration/keystore -srckeystore NAME.p12 -
   srcstoretype PKCS12
   ```
3. Restart the virtual appliance.

## Maintenance job

The Maintenance job removes resources and associated objects that are created by IBM Spectrum Protect Plus when a job that is in a pending state is deleted.

The cleanup procedure reclaims space on your storage devices, cleans up your IBM Spectrum Protect Plus catalog, and removes related snapshots. The Maintenance job also removes cataloged data that is associated with deleted jobs. By default, the Maintenance job runs once a day. The job cannot be deleted.

The Maintenance job performs cleanup operations only after a job in a pending state is deleted. All logs that are associated with the deleted job are removed from IBM Spectrum Protect Plus, so it is advised to download job logs before the Maintenance job's next run. The job can be stopped and resumed; all pending operations set to occur before the job was stopped will resume upon the next job run.

After the Maintenance job deletes a pending job, all associated copy data, including recovery points, are deleted. The Maintenance job removes all VM Copies and Primary copies that are associated with deleted VMware Backup and Restore jobs. After the Maintenance job completes, data that was copied as part of the backup job cannot be recovered. Any data that is related to the deleted job is not recoverable.

## Logging on to the virtual appliance

Log on to the IBM Spectrum Protect Plus virtual appliance through vSphere Client to access the command line. You can access the command line in a VMware environment or in a Hyper-V environment.

### Accessing the virtual appliance in VMware

In a VMware environment, log on to the IBM Spectrum Protect Plus virtual appliance through vSphere Client to access the command line.

#### Procedure

To access the virtual appliance command line in a VMware environment, complete the following steps:

1. In vSphere Client, select the virtual machine where IBM Spectrum Protect Plus is deployed.
2. On the **Summary** tab, select **Open Console** and click in the console.
3. Select **Login**, and enter your user name and password. The default user name is `administrator` and the default password is `sppadLG235`.

#### What to do next

Enter commands to administer the virtual appliance. To log off, enter `exit`.

### Accessing the virtual appliance in Hyper-V

In a Hyper-V environment, log on to the IBM Spectrum Protect Plus virtual appliance through vSphere Client to access the command line.

#### Procedure

To access the virtual appliance command line in a Hyper-V environment, complete the following steps:

1. In Hyper-V Manager, select the virtual machine where IBM Spectrum Protect Plus is deployed.
2. Right-click the virtual machine and select **Connect**.
3. Select **Login**, and enter your user name and password. The default user name is `administrator` and the default password is `sppadLG235`.

#### What to do next

Enter commands to administer the virtual appliance. To log off, enter **exit**.

## Collecting log files for troubleshooting

To troubleshoot the IBM Spectrum Protect Plus application, you can download an archive of log files that are generated by IBM Spectrum Protect Plus.

**Before you begin**

Contact Technical Support to determine whether they need a log collection file for troubleshooting.

**Procedure**

To collect log files for troubleshooting, complete the following steps:

1. Click the user icon and select **Download System Logs**.
2. Select the location where you want to save the archive file.

   **Archived log files:** The following log files are added to the archive file and saved to your local system:

   - `mongo`
   - `rabbitmq`
   - `virgo`

**What to do next**

Contact Technical Support to inform them that you created a log collection file for troubleshooting. Send the compressed log collection file to Technical Support.

## Data disk expansion

You can add new virtual disks (hard disks) on your IBM Spectrum Protect Plus virtual machine through vCenter.

When you deploy the IBM Spectrum Protect Plus virtual appliance, you can deploy all virtual disks to one datastore that you specify at the time of deployment. You can add a disk within the virtual machine and configure it as a Logical Volume Manager (LVM). You can then mount the new disk as a new volume or attach the new disk to the existing volumes within the virtual appliance.

You can review the disk partitions by using the **`fdisk -l`** command. You can review the physical volumes and the volume groups on the IBM Spectrum Protect Plus virtual appliance by using the **`pvdisplay`** and **`vgdisplay`** commands.

### Adding a disk to the virtual appliance

To add a disk to the virtual appliance, use the vCenter client to edit the settings of the virtual machine.

**Before you begin**

To run commands, you must connect to the IBM Spectrum Protect Plus appliance's command line by using SSH and log in as the root account. The default initial password is sppDP758 and you are prompted to change the password when you log in for the first time.

**Procedure**

To add a disk to an IBM Spectrum Protect Plus virtual machine, complete the following steps from the vCenter client:

1. From the vCenter client, complete the following steps:
   a) On the Hardware tab, click **Add...**.
   b) Select **Create a new virtual disk**.

c) Select the required Disk Size. In the Location section, select one of the following options:

- To use the current datastore, select **Store with the virtual machine**
- To specify one or more datastores for the virtual disk, select **Specify a datastore or datastore cluster** Click **Browse...** to select the new datastores.

d) Leave the default values in the Advanced Options tab.

e) Review and save your changes.

f) Click the **Edit Settings** option for the virtual machine to view the new hard disk.

2. Add the new SCSI device without rebooting the virtual machine. From the console of the IBM Spectrum Protect Plus virtual machine, issue the following command:

```
echo "-- -" > /sys/class/scsi_host/host#/scan
```

where # is the latest host number.

## Adding storage capacity from a new disk to the appliance volume

After you add a disk to the virtual appliance, you can attach the new disk to the existing volumes within the virtual appliance.

### Before you begin

To run commands, you must connect to the IBM Spectrum Protect Plus appliance's command line by using SSH and log in as the root account. The default initial password is sppDP758 and you are prompted to change the password when you log in for the first time.

### About this task

You need to complete this task only if you want to add the storage capacity from a new disk to an existing appliance volume. If you added the disk as a new volume, you do not need to complete this task.

### Procedure

To add storage capacity from a new disk to the appliance volume, complete the following steps from the console of the virtual appliance:

1. Complete the following steps to set up a partition for the new disk and set the partition to be of type Linux LVM:

a) Open the new disk by using the **fdisk** command:

```
[root@localhost ~]# fdisk /dev/sdd
```

The **fdisk** utility starts in interactive mode. Output similar to the following output is displayed:

```
Device contains neither a valid DOS partition table, nor Sun, SGI or
OSF disklabel
Building a new DOS disklabel with disk identifier 0xb1b293df.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
Warning: invalid flag 0x0000 of partition table 4 will be corrected by
w(rite)
WARNING: DOS-compatible mode is deprecated. It's strongly recommended
to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
Command (m for help):
```

a) At the **fdisk** command line, enter the **n** subcommand to add a partition.

```
Command (m for help): n
```

The following command action choices are displayed:

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
```

b) Enter the **p** command action to select the primary partition.
You are prompted for a partition number:

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
Partition number (1-4):
```

c) At the partition number prompt, enter the partition number 1.

```
Partition number (1-4): 1
```

The following prompt is displayed:

```
First cylinder (1-2610, default 1):
```

d) Do not type anything at the First cylinder prompt. Press the **Enter** key.
The following output and prompt is displayed:

```
First cylinder (1-2610, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
```

e) Do not type anything in the Last cylinder prompt. Press the **Enter** key.
The following output is displayed:

```
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
Using default value 2610
Command (m for help):
```

f) At the **fdisk** command line, enter the **t** subcommand to change a partition's system ID.

```
Command (m for help): t
```

You are prompted for a hex code that identifies the partition type:

```
Selected partition 1
Hex code (type L to list codes):
```

g) At the Hex code prompt, enter the hex code 8e to specify the Linux LVM partition type.
The following output is displayed:

```
Hex code (type L to list codes): 8e
Changed system type of partition 1 to 8e (Linux LVM)
Command (m for help):
```

h) At the **fdisk** command line, enter the **w** subcommand to write the partition table and to exit the **fdisk** utility.

```
Command (m for help): w
```

The following output is displayed:

```
Command (m for help): w (write table to disk and exit)
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
```

2. To review the changes to the disk, issue the **fdisk -1** command.
3. To review the current list of Physical Volumes (PV), issue the **pvdisplay** command.
4. To create a new Physical Volume (PV), issue the **pvcreate /dev/sdd1** command.
5. To view the new PV from /dev/sdd1, issue the **pvdisplay** command.
6. To review the Volume Group (VG), issue the **vgdisplay** command.
7. To add the Physical Volume (PV) to the Volume Group (VG) and increase its space, issue the following command:

```
vgextend data_vg /dev/sdd1
```

8. To verify that data_vg is extended, and that free space available for logical volumes (or /data volume) to use, issue the **vgdisplay** command.
9. To review the Logical Volume (LV) /data, issue the **lvdisplay** command. The usage of the /data volume displays.
10. To add space to the LV /data to the total volume capacity, issue the **lvextend** command. Be sure to reduce the amount of space added by 1 GB.
    In this example, 20 GB of space is being added to a 100 GB volume. First, the amount of space to add is reduced by 1 GB. Then, it is added to the overall volume capacity. In this example, the new size of the LV is specified as 119 GB.

```
[root@localhost ~]# lvextend -L119gb -r /dev/data_vg/data
Size of logical volume data_vg/data changed from 100.00 GiB (25599
extents) to 119.00 GiB (30464 extents).
Logical volume data successfully resized
resize2fs 1.41.12 (date)
Filesystem at /dev/mapper/data_vg-data is mounted on /data; on-line
resizing required
old desc_blocks = 7, new_desc_blocks = 8
Performing an on-line resize of /dev/mapper/data_vg-data to 31195136
(4k) blocks.
The filesystem on /dev/mapper/data_vg-data is now 31195136 blocks
long.
```

    After you run the preceding command, the size of the /data volume is displayed in **lvdisplay** command output as 119 GB:

```
[root@localhost ~]# lvdisplay
--- Logical volume ---
LV Path: /dev/data_vg/data
LV Name: data
VG Name: data_vg
LV UUID: [uuid]
LV Write Access: read/write
LV Creation host, time localhost.localdomain, [date, time]
LV Status: available
# open: 1
LV Size: 119.00 GiB
Current LE: 30208
Segments : 2
Allocation inherit
Read ahead sectors: auto
- currently set to: 256
Block device: 253:1
[root@localhost ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda3 14G 2.6G 11G 20% /
tmpfs 16G 0 16G 0% /dev/shm
/dev/sda1 240M 40M 188M 18% /boot
/dev/mapper/data_vg-data
118G 6.4G 104G 6% /data
/dev/mapper/data2_vg-data2
246G 428M 234G 1% /data2
```

# Chapter 10. User access

Role-based access control allows you to set the resources and permissions available to IBM Spectrum Protect Plus user accounts.

Through role-based access control, you can tailor IBM Spectrum Protect Plus for individual users, giving them access to the features and resources they require.

Once resources are available to IBM Spectrum Protect Plus, they can be added to a resource group along with high level IBM Spectrum Protect Plus features such as hypervisors and individual screens.

Roles are then configured to define the actions that can be performed by the user associated with the resource group. These parameters are then associated with one or more user accounts.

Use the following sections of the **Access** pane to configure role-based access:

**Resource Groups**
A resource group defines the resources that are available to a user. Every resource added to IBM Spectrum Protect Plus can be included in a resource group, along with individual IBM Spectrum Protect Plus functions and screens. This gives you the ability to finely-tune the experience of a user. For example, a resource group could include an individual hypervisor, with access to only backup and reporting functionality. When the resource group is associated with a role and a user, the user will only see the screens associated with backup and reporting for the assigned hypervisor.

**Roles**
Roles define the actions that can be performed on the resources defined in a resource group. While a resource group defines the resources that will be made available to an account, a role sets the permissions to interact with the resources defined in the resource group. For example, if a resource group is created that includes Backup and Restore jobs, the role determines how a user can interact with the jobs.

Permissions can be set to allow a user to create, view, and run the Backup and Restore jobs defined in a resource group, but not delete them. Similarly, permissions can be set to create administrator accounts, allowing a user to create and edit other accounts, set up sites and resources, and interact with all of the available IBM Spectrum Protect Plus features.

**Users**
A user account associates a resource group with a role. To enable a user to log in to IBM Spectrum Protect Plus and use its functions, you must first add the user as an individual user (referred to as a native user) or as part of an imported group of LDAP users, and then assign resource groups and roles to the user account. The account will have access to the resources and features that are defined in the resource group as well as the permissions to interact with the resources and features defined in the role.

The user account `admin` is used to set up IBM Spectrum Protect Plus. You cannot modify the credentials for this user other than to change to the password and you cannot delete the account. This account is assigned to the SUPERUSER role, which has access to all functions of the product.

# Managing user resource groups

A resource group defines the resources that will be made available to a user. Every resource added to IBM Spectrum Protect Plus can be included in a resource group, along with individual IBM Spectrum Protect Plus functions and screens.

## Creating a resource group

An administrator can create a resource group to define the resources that are available to a user.

### Procedure

Complete the following steps to create a resource group:

1. From the navigation menu, expand **Access**, and then click **Resource Group**.
2. Click **Create Resource Group**. The **Create Resource Group** pane displays.
3. Enter a name for the resource group.
4. From the **I would like to create a resource group** menu, select one of the following options:

| Option | Actions |
|---|---|
| **New** | a. Select a resource type from the **Choose a resource type** menu.<br>b. Select resource subtypes, and then click **Add Resources**. Resources are added to the **Selected Resources** view. |
| **From template** | a. Select a resource group from the **Which resource group would you like to use as a template?** list. Resources from the selected template are added to the **Selected Resources** view.<br>b. You can add resources by using the **Choose a resource type** list and its associated lists.<br>To view available resource types and their usage, see “Resource types ” on page 107 |

   If you want to delete resources from the group, click the delete icon  that is associated with a resource or click **Delete All** to delete all resources.
5. When you are finished adding resources, click **Create resource group**.

### Results

The resource group displays in the **RESOURCE GROUP** table and can be associated with new and existing user accounts.

### What to do next

After you add the resource group, complete the following action:

| Action | How to |
|---|---|
| Create roles to define the actions that can be performed by the user account that is associated with the resource group. Roles are used to define permissions to interact with the resources that are defined in the resource group.. | See “Creating a user role” on page 110. |

**Resource types**

Resource types are selected when resource groups are created and determine the resources that are available to a user assigned to a group.

The following resource types and subtypes are available:

| Resource Type | Subtype | Description |
|---|---|---|
| Access | • Role<br>• User | Used to grant access to roles and users through the **Access** pane. |
| Application | • Oracle<br>• SQL Standalone/Failover Cluster<br>• SQL Always On | Used to grant access to viewing individual application databases on an application server in IBM Spectrum Protect Plus. |
| Application Server | • SQL<br>• Oracle | Used to grant access to application servers in IBM Spectrum Protect Plus without access to individual databases. |
| Backup Storage | None | Used to grant access to vSnap backup storage servers. |
| Hypervisor | • VMware<br>• Hyper-V | Used to grant access to hypervisor resources. |
| Job | None | Used to grant access to Inventory, Backup, and Restore jobs. The Job resource group is mandatory for all Backup and Restore operations, including assigning SLA Policies to resources. |
| Report | • Backup Storage Utilization<br>• Protection<br>• System<br>• VE Environment | Used to grant access to report types and individual reports. |
| Screen | None | Used to grant or deny access to screens in the IBM Spectrum Protect Plus interface. If certain screens are not included in a resource group for a user, the user will not be able to access the functionality provided on the screen, regardless of the permissions granted to the user. |
| SLA Policy | None | Used to grant access to SLA Policies for Backup operations. |
| System | Identity | Used to grant access to the credentials required to access your resources. Identity functionality is available through the **System** > **Identity** pane. |

| Resource Type | Subtype | Description |
|---|---|---|
| System | LDAP | Used to grant access to LDAP servers for user registration. |
| System | Logs | Used to grant access to viewing and downloading Audit and System logs. |
| System | Script | Used to grant access to uploaded prescripts and postscripts. |
| System | Script Server | Used to grant access to script servers, where scripts are run during a Backup or Restore job. |
| System | Site | Used to grant access to sites, which are assigned to vSnap backup storage servers. |
| System | SMTP | Used to grant access to SMTP servers for job notifications. |
| System | VADP Proxy | Used to grant access to VADP proxy servers. |

## Editing a resource group

An administrator can edit a resource group to change the resources and IBM Spectrum Protect Plus features that are assigned to the group. Updated resource group settings take affect when user accounts that are associated with the resource group log in to IBM Spectrum Protect Plus.

### Before you begin

Note the following considerations before editing a resource group:

- If a user is logged in when their permissions or access rights are changed, the user must log out and log in again for the updated permissions to take affect.
- An administrator can edit any resource group that is not designated as **Cannot be modified**.

### Procedure

Complete the following steps to edit a resource group:

1. From the navigation menu, expand **Access**, and then click **Resource Group**.
2. Click the edit icon for the resource group. The **Modify Resource Group** pane displays.
3. Revise the resource group selections.
4. Click **Update Resource Group**.

## Deleting a resource group

An administrator can delete any resource group that is not designated as **Cannot be modified**.

### Procedure

Complete the following steps to delete a resource group

1. From the navigation menu, expand **Access**, and then click **Resource Group**.
2. Click the delete icon that is associated with the resource group, and then click **Yes**.

## Managing user roles

Roles define the actions that can be completed for the resources that are defined in a resource group. While a resource group defines the resources that are available to an account, a role sets the permissions to interact with the resources that are defined in the resource group.

For example, if a resource group is created that includes Backup and Restore jobs, the role determines how a user can interact with the jobs. Permissions can be set to allow a user to create, view, and run the Backup and Restore jobs that are defined in a resource group, but not delete them.

Similarly, permissions can be set to create administrator accounts, allowing a user to create and edit other accounts, set up sites and resources, and interact with all of the available IBM Spectrum Protect Plus features.

The functionality of a role is dependent on a properly configured resource group. When selecting a predefined role or configuring a custom role, you must ensure that access to necessary IBM Spectrum Protect Plus operations, screens, and resources align with the proposed usage of the role.

The following user account roles are available:

**SYSADMIN**

The SYSADMIN role is the administrator role. This role provides access to all resources and privileges.

Users with this role can add users and complete the following actions for all users other than the `admin` user, which is assigned to the SUPERUSER role. The only action that is allowed for the SUPERUSER role is to change the user password.

- Modify and delete user accounts.
- Change user passwords.
- Assign user roles.

An administrator can also access the Administrative Console by selecting **IBM Spectrum Protect Plus** from the **Authentication Type** list in the console login window and entering administrator credentials.

From the Administrative Console, the administrator can apply software updates, restart the IBM Spectrum Protect Plus appliance, and set the local time zone.

For more information about using the Administrative Console, see "Managing the Administrative Console" on page 97

**Application Admin**

The Application Admin role allows a user to register and modify application database resources that are delegated by an administrator, as well as associate application databases to assigned SLA policies, perform backup and restore operations, and run and schedule reports delegated by an administrator.

Access to specific application servers must be granted by an administrator through the **Access** > **Resource Group** pane. This step is also required if the **All Resources** resource group is selected because access to application servers are not included by default.

**Backup Only**

The Backup Only role allows users to complete the following actions:

- Run, edit, and monitor backup operations.
- View, create, and edit SLA Policies that are delegated by an administrator.

Access to resources, including specific backup jobs, must be granted by an administrator through the **Access** > **Resource Group** pane.

**Application Admin**

The Application Admin role allows users to complete the following actions:

- Register and modify application database resources that are delegated by an administrator.
- Associate application databases to assigned SLA policies.
- Complete backup and restore operations.

- Run and schedule reports that delegated by an administrator.

Access to resources must be granted by an administrator through the **Access** > **Resource Group** pane.

**Restore Only**

The Restore Only role allows users to complete the following actions:

- Run, edit, and monitor restore operations.
- View, create, and edit SLA Policies that are delegated by an administrator.

Access to resources, including specific restore jobs, must be granted by an administrator through the **Access** > **Resource Group** pane.

**Self Service**

The Self Service role allows users to monitor existing backup and restore operations that are delegated by an administrator.

Access to resources, including specific jobs, must be granted by an administrator through the **Access** > **Resource Group** pane.

**VM Admin**

The VM Admin role allows a users to complete the following actions:

- Register and modify hypervisor resources that are delegated by an administrator.
- Associate hypervisors to SLA.
- Complete backup and restore operations.
- Run and schedule reports that are delegated by an administrator.

Access to resources must be granted by an administrator through the **Access** > **Resource Group** pane.

## Creating a user role

An administrator can create roles to define the actions that can be completed by the user of an account that is associated with a resource group. Roles are used to define permissions to interact with the resources that are defined in the resource group.

### Procedure

Complete the following steps to create a user role:

1. From the navigation menu, expand **Access**, and then click **Role**.
2. Click **Create role**. The **The Create Role** pane displays.
3. From the **I would like to create a role** list, select one of the following options:

| Option | Actions |
|---|---|
| **New** | Select permissions to apply to the role. By default, none of the permissions are pre-selected. |
| **From template** | a. Select a role from the **Which role would you like to use as a template?** menu. Permissions that are associated with the template role are selected by default.<br>b. Select additional permissions to apply to the role.<br>To view available permissions and their usage, see “Permission types ” on page 111. |

4. Enter a name for the role, and then click **Create role**.

### Results

The new role displays in the **ROLE** table and can be applied to new and existing user accounts.

**Permission types**
Permission types are selected when user accounts are created and determine the permissions that are available to the user.

The following permissions are available:

| Name | Permissions | Description |
|---|---|---|
| Application | View | Used to view individual application databases on an application server in IBM Spectrum Protect Plus. |
| Application Server | Register, view, edit, deregister | Used to interact with application servers, such as SQL or Oracle servers, without access to individual databases. |
| Hypervisor | Register, view, edit, deregister, options | Used to interact with hypervisor virtual machines, such as VMware or Hyper-V virtual machines. |
| Identity | Create, view, edit, delete | Used to interact with the credentials required to access your resources. Identity functionality is available through the System > Identity pane. |
| LDAP | Register, view, edit, deregister | Used to interact with LDAP servers for user registration. |
| Log | View | Used to view Audit and System logs. |
| Job | Create, view, edit, run, delete | Used to interact with Inventory, Backup, and Restore jobs. |
| VADP Proxy | Register, view, edit, deregister | Used to interact with VADP |
| Report | Create, view, edit, delete | Used to interact with reports. |
| Resource Group | Create, view, edit, delete | Used to interact with resource groups, which define the IBM Spectrum Protect Plus resources that are made available to a user. |
| Role | Create, view, edit, delete | Used to interact with roles, which define the actions that can be performed on the resources defined in a resource group. |
| Script | Upload, view, replace, delete | Used to interact with prescripts and postscripts that are added to IBM Spectrum Protect Plus and run before or after a job. |
| Site | Create, view, edit, delete | Used to interact with sites, which are assigned to vSnap backup storage servers. |
| SMTP | Register, view, edit, deregister | Used to interact with SMTP servers for job notifications. |

| Name | Permissions | Description |
|---|---|---|
| Storage | Register, view, edit, deregister | Used to interact with vSnap backup storage servers. |
| SLA Policy | Create, view, edit, delete | Used to interact with SLA Policies, which allow users to create customized templates for Backup jobs. |
| User | Create, view, edit, delete | Used to interact with users, which associated a resource group with a role, and provides access to the IBM Spectrum Protect Plus user interface. |

### Editing a user role

An administrator can edit a role to change the resources and permissions that are assigned to the role. Updated role settings take affect when user accounts that are associated with the role log in to IBM Spectrum Protect Plus.

#### Before you begin

Note the following considerations before editing a role:

- If a user is logged in when their permissions or access rights are changed, the user must log out and log in again for the updated permissions to take affect.
- An administrator can edit any role that is not designated as **Cannot be modified**.

#### Procedure

An administrator can edit any user role that is not designated as **Cannot be modified**.

Complete the following steps to edit a user role:

1. From the navigation menu, expand **Access**, and then click **Role**.
2. Click the edit icon for the role. The **Modify Role** pane displays.
3. Revise the name of the role and selected permissions.
4. Click **Update role**.

### Deleting a user role

An administrator can delete a user role that is not designated as **Cannot be modified**.

#### Procedure

Complete the following steps to delete a user role:

1. From the navigation menu, expand **Access**, and then click **Role**.
2. Click the delete icon that is associated with the role, and then click **Yes**.

## Managing user accounts

Before a user can log on to IBM Spectrum Protect Plus and use the available functions, an administrator must add the user account to IBM Spectrum Protect Plus.

An administrator can also modify and delete user accounts.

## Creating a user account for an individual user

An administrator can add an account for an individual user in IBM Spectrum Protect Plus. If you are upgrading from a previous version of IBM Spectrum Protect Plus, permissions assigned to users in the previous version must be reassigned in IBM Spectrum Protect Plus 10.1.1.

### Before you begin

If you want to use custom roles and resource groups, create them before you create a user. See "Creating a resource group" on page 106 and "Creating a user role" on page 110.

### Procedure

Complete the following steps to create an account for an individual user:

1. From the navigation menu, expand **Access**, and then click **User**.
2. Click **Add user**. The **Add User** pane displays.
3. Click **What type of user/group are you wanting to add?** > **Individual new user**.
4. Enter a name and password for the user.
5. In the **Assign Role** section, select one or more roles for the user.
6. In the **Permission Groups** section, review the permissions and resources that are available to the user, and then click **Continue**.
7. In the **Add Users - Assign Resources** section, assign one or more resource groups to the user, and then click **Add resources**.

   The resource groups are added to the **Selected Resources** section.
8. Click **Create user**.

### Results

The new user displays in the **USER** table. Select a user from the table to view available roles, permissions, and resource groups.

## Creating a user account for an LDAP group

An administrator can add a user account for an LDAP group to IBM Spectrum Protect Plus.

### Before you begin

Review the following procedures before you create a user account for an LDAP group:

- Register an LDAP provider in IBM Spectrum Protect Plus. See "Registering LDAP providers in IBM Spectrum Protect Plus" on page 88.
- If you want to use custom roles and resource groups, create them before you create a user. See "Creating a resource group" on page 106 and "Creating a user role" on page 110.

### Procedure

Complete the following steps to create a user account for an LDAP group:

1. From the navigation menu, expand **Access**, and then click **User**.
2. Click **Add user**. The **Add User** pane displays.
3. Click **What type of user/group are you wanting to add?** > **LDAP Group**.
4. Select an LDAP group.
5. In the **Assign Role** section, select one or more roles for the user.
6. In the **Permission Groups** section, review the permissions and resources that are available to the user, and then click **Continue**.
7. In the **Add Users - Assign Resources** section, assign one or more resource groups to the user, and then click **Add resources**.

The resource groups are added to the **Selected Resources** section.

8. Click **Create user**.

**Results**

The new user displays in the **USER** table. Select a user from the table to view available roles, permissions, and resource groups.

## Editing a user account

An administrator can edit the user name, password, associated resource groups, and roles for a user account, with the exception of users who are assigned to the SUPERUSER role. If a user is a member of the SUPERUSER role, the administrator can change only the password for the user.

**Before you begin**

If a user is logged in when their permissions or access rights are changed, the user must log out and log in again for the updated permissions to take affect.

**Procedure**

Complete the following steps to edit the credentials of a user account:

1. From the navigation menu, expand **Access**, and then click **User**.
2. Select one or more users. If you select multiple users with different roles, you can modify only their resources and not their roles.
3. Click the options icon ⋯ to view available options. The options that are shown depend on the selected user or users.

   **Modify settings**
   Edit the user name and password, associated roles, and resource groups.

   **Modify resources**
   Edit the associated resource groups.
4. Modify the settings for the user, and then click **Update user** or **Assign resources**.

## Deleting a user account

An administrator can delete any user account, with the exception of users who are assigned to the SUPERUSER role.

**Procedure**

Complete the following steps to delete a user account:

1. From the navigation menu, expand **Access**, and then click **User**.
2. Select a user.
3. Click the options icon ⋯, and then click **Delete user**.

# Search guidelines

Use filters to search for an entity such as a file or a restore point.

You can enter a character string to find objects with a name that exactly matches the character string. For example, searching for the term `string.txt` returns the exact match, `string.txt`.

Regular expression search entries are also supported. For more information, see https://docs.microsoft.com/en-us/sql/relational-databases/scripting/search-text-with-regular-expressions.

You can also include the following special characters in the search. These characters must be escaped with a \ before the character:

```
+ - & | ! ( ) { } [ ] ^ " ~ * ? : \
```

For example, to search for the file `string[2].txt`, enter the `string\[2\].txt`.

### Searching with wildcards

You can position wildcards at the beginning, middle, or end of a string, and combine them within a string.

**Match a character string with an asterisk**

The following examples show search text with an asterisk:

- `string*` searches for terms like string, strings, or stringency
- `str*ing` searches for terms like string, straying, or straightening
- `*string` searches for terms like string or shoestring

You can use multiple asterisk wildcards in a single text string, but multiple wildcards might considerably slow down a large search.

**Match a single character with a question mark:**

The following examples show search text with a question mark:

- `string?` searches for terms like strings, stringy, or string1
- `st??ring` searches for terms like starring or steering
- `???string` searches for terms like hamstring or bowstring

# 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.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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.

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.

To view glossaries for other IBM products, see IBM Terminology.

# Index

## W