IBM Spectrum Protect Plus
Version 10.1.0

Installation and User's Guide

IBM Spectrum Protect Plus
Version 10.1.0

Installation and User's Guide

Note:
Before you use this information and the product it supports, read the information in "Notices" at the end of this publication.

This edition applies to version 10, release 1, modification 0 of IBM Spectrum Protect Plus (product number 5737-F11) and to all subsequent releases and modifications until otherwise indicated in new editions.

Table of Contents

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. It can unlock your valuable data for emerging use cases. It 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, then select **Help**.

Getting Started

For IBM Spectrum Protect Plus system requirements, see System Requirements on page **8**.

For IBM Spectrum Protect Plus installation procedures, see Install IBM Spectrum Protect Plus as a VMware Virtual Appliance on page **25** and Install IBM Spectrum Protect Plus as a Hyper-V Virtual Appliance on page **28**.

To install additional virtual or physical vSnap backup destinations, see Install vSnap Server on page **38**.

To configure VADP Proxies, which enable load sharing and load balancing for jobs in Linux environments, see VADP Proxy on page **93**.

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 VMs, Unprotected VMs, Failed Jobs, and Running Jobs. Additional widgets include:

The **Backup Storage Utilization** 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.

The **Backup Storage Summary** 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.

The **Protection by Policy** widget displays the total number of protected VMs 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.

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

RELATED TOPICS:

- System Requirements on page **8**
- IBM Spectrum Protect Plus Overview on page **5**
- Install IBM Spectrum Protect Plus as a VMware Virtual Appliance on page **25**
- Install IBM Spectrum Protect Plus as a Hyper-V Virtual Appliance on page **28**
- Start IBM Spectrum Protect Plus on page **31**
- Operations Overview on page **51**
- System Overview on page **90**
- Reports Overview on page **80**
- Add a Backup Storage Provider on page **45**

Installation and Setup

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

System Requirements

Ensure that you have the required system configuration and browser to deploy and run IBM Spectrum Protect Plus.

Virtual Machine Installation

IBM Spectrum Protect Plus is installed as a virtual appliance. Before deploying to the host, ensure you have the following:

- The correct VMware or Microsoft Hyper-V template
- vSphere 5.5, 6.0, or 6.5 or Microsoft Hyper-V Server 2016

  Note: For later versions of vSphere, the vSphere Web Client may be required to deploy IBM Spectrum Protect Plus appliances.
- Network information and VMware host information
- Either an available static IP address to use or access to DHCP

For initial deployment, configure your virtual appliance to meet the following recommended minimum requirements:

- 64-bit dual core machine
- 16 GB memory

The IBM Spectrum Protect Plus appliance has five virtual disks that total 370 GB of storage.

Use an NTP server to synchronize the time zones across IBM Spectrum Protect Plus resources in your environment, such as the IBM Spectrum Protect Plus appliance, storage arrays, hypervisors and application servers . 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 the following VMware knowledge base article: Time in virtual machine drifts due to hardware timer drift.

Browser Support

Run IBM Spectrum Protect Plus from a computer that has access to the installed virtual appliance.

IBM Spectrum Protect Plus was tested and certified against the following web browsers. Note that newer versions may be supported.

- Firefox 55.0.3
- Google Chrome 60.0.3112
- Microsoft Edge 40.15063

If your resolution is below 1024 x 768, some items may not fit on the window. Pop-up windows must be enabled in your browser to access the Help system and some IBM Spectrum Protect Plus operations.

IBM Storage Requirements

- IBM Spectrum Protect Version 8.1.0 and later

Hyper-V Requirements

- Microsoft Hyper-V Server 2016
- 150 GB+ of drive space if Disk Type is set to *Fixed Size* during the installation procedure
- 16 GB memory

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 registering the Hyper-V server in IBM Spectrum Protect Plus, the server must be added to the /etc/hosts file on the IBM Spectrum Protect Plus appliance via command line. 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.

VMware Requirements

- vSphere 5.5 and later
- vSphere 6.0 and later
- vSphere 6.5 and later

Ensure the latest version of VMware Tools is installed in your environment. IBM Spectrum Protect Plus was tested against VMware Tools 9.10.0.

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.

vSnap Requirements

A vSnap server serves 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 desired.

vSnap Server Virtual Machine Installation Requirements

Before deploying to the host, ensure you have the following:

- The correct VMware or Microsoft Hyper-V template
- vSphere 5.5, 6.0, or 6.5 or Microsoft Hyper-V Server 2016

Note: For later versions of vSphere, the vSphere Web Client may be required to deploy IBM Spectrum Protect Plus appliances.

- Network information and VMware host information
- Either an available static IP address to use or access to DHCP

For initial deployment, configure your virtual appliance to meet the following recommended minimum requirements:

- 64-bit dual core machine
- 16 GB memory

Note: Memory should be adjusted based on backup capacity for more efficient deduplication. General Rule of thumb is 1GB for every 1TB of backup data.

The vSnap appliance has two virtual disks that total 150 GB storage

vSnap Server Physical Installation Requirements

For initial deployment, configure your physical server to meet the following recommended minimum requirements:

- CentOS Linux7.3.1611(x86_64) or CentOSLinux7.4.1708(x86_64)
- 64-bit quad core machine
- 32 GB memory
- 8GB free space in root partition

Note: Memory should be adjusted based on backup capacity for more efficient deduplication. General Rule of thumb is 1GB for every 1TB of backup data.

Optionally, an SSD improves backup and restore performance.

- To improve backup performance, configure the pool to use one or more log devices backed by SSD. Specify at least two log devices to create a mirrored log for better redundancy.
- To improve restore performance, configure the pool to use a cache device backed by SSD

VADP Proxy Requirements

In IBM Spectrum Protect Plus, running virtual machine backup jobs through VADP can be taxing on system resources. By creating VADP backup job proxies, you enable load sharing and load balancing for your IBM Spectrum Protect Plus backup jobs. If proxies exist, the entire processing load is shifted off the IBM Spectrum Protect Plus appliance and onto the proxies.

This feature has been tested only for SUSE Linux Enterprise Server and Red Hat environments. It is supported only in 64-bit quad core configurations with a minimum kernel of 2.6.32.

A minimum of 8 GB of RAM is required (16 GB recommended), along with 60 GB of disk space.

Each proxy must have a fully qualified domain name.

Port 8080 on the VADP proxy server must be open when the proxy server firewall is enabled. If the port is not open, VADP Backups will run on local vmdkbackup instead of the VADP proxy server.

Ports

The following ports are used by IBM Spectrum Protect Plus and associated services. Note that ports marked as Open use a secure connection (https/ssl).

Ports

	Port	Service	Comment	Firewall
IBM Spectrum Protect Plus	22	OpenSSH 5.3 (protocol 2.0)	Used for troubleshooting IBM Spectrum Protect Plus.	Open
	443	User interface and Zuul reverse proxy	A microservice running a Zuul reverse-proxy listens on 443.	Open
	5432	PostgreSQL	SQL RDBMS - Supports job management and some security related data and transactions.	Blocked
	5671	RabbitMQ	Message framework used to manage messages produced and consumed by the VADP proxy and VMware job management workers. Also facilitates job log management.	Open
	5672	RabbitMQ	Message framework used to manage messages produced and consumed within the IBM Spectrum Protect Plus appliance.	Blocked
	8082	Virgo	Modular Java application server. Serves core functions for IBM Spectrum Protect Plus including the REST APIs.	Blocked
	8083	NodeJs	JavaScript server. Provides higher level APIs to the user interface leveraging the REST APIs running in Virgo.	Blocked
	8090	Administrative Console Framework (ACF)	Extensible framework for system administration functions. Supports plugins that perform operations such as system updates and catalog backup/restore.	Open
	8092	ACF Plugin EMI	Supports system update, certificate and license management.	Blocked
	8093	ACF Plugin Catalog Backup/Recovery	Performs backup and restore of the IBM Spectrum Protect Plus catalog data.	Blocked
	8761	Discovery Server	Automatically discovers VADP proxies and is used by IBM Spectrum Protect	Open

	Port	Service	Comment	Firewall
			Plus VM backup operations.	
	27017	MongoDB	Persists configuration related documents for IBM Spectrum Protect Plus.	Blocked
	27018	MongoDB2	Persists recovery meta data documents for IBM Spectrum Protect Plus.	Blocked
Guest Apps	5985	Windows Remote Management (WinRM)	Service that runs on a Windows server which is used for application protection operations initiated by IBM Spectrum Protect Plus and targeted to IBM Spectrum Protect Plus application plugins running within the Windows servers.	Open
vSnap	111	NFS	Used for NFS data transfer to/from vSnap.	Open
	2049	NFS	Used for NFS data transfer to/from vSnap.	Open
	3260	iSCSI	Used for iSCSI data transfer to/from vSnap.	Open
	8900	vSnap	OVA/Installer version of the intelligent storage framework used as a target for data protection operations.	Open
	20048	NFS	Used for NFS data transfer to/from vSnap.	Open
VADP Proxy	8080	VADP Proxy	Virtual machine data protection proxy.	Open

Use the following diagram as guidance for understanding the communication paths managed by IBM Spectrum Protect Plus. It can be leveraged to provide assistance for troubleshooting and network configuration for deployment scenarios.

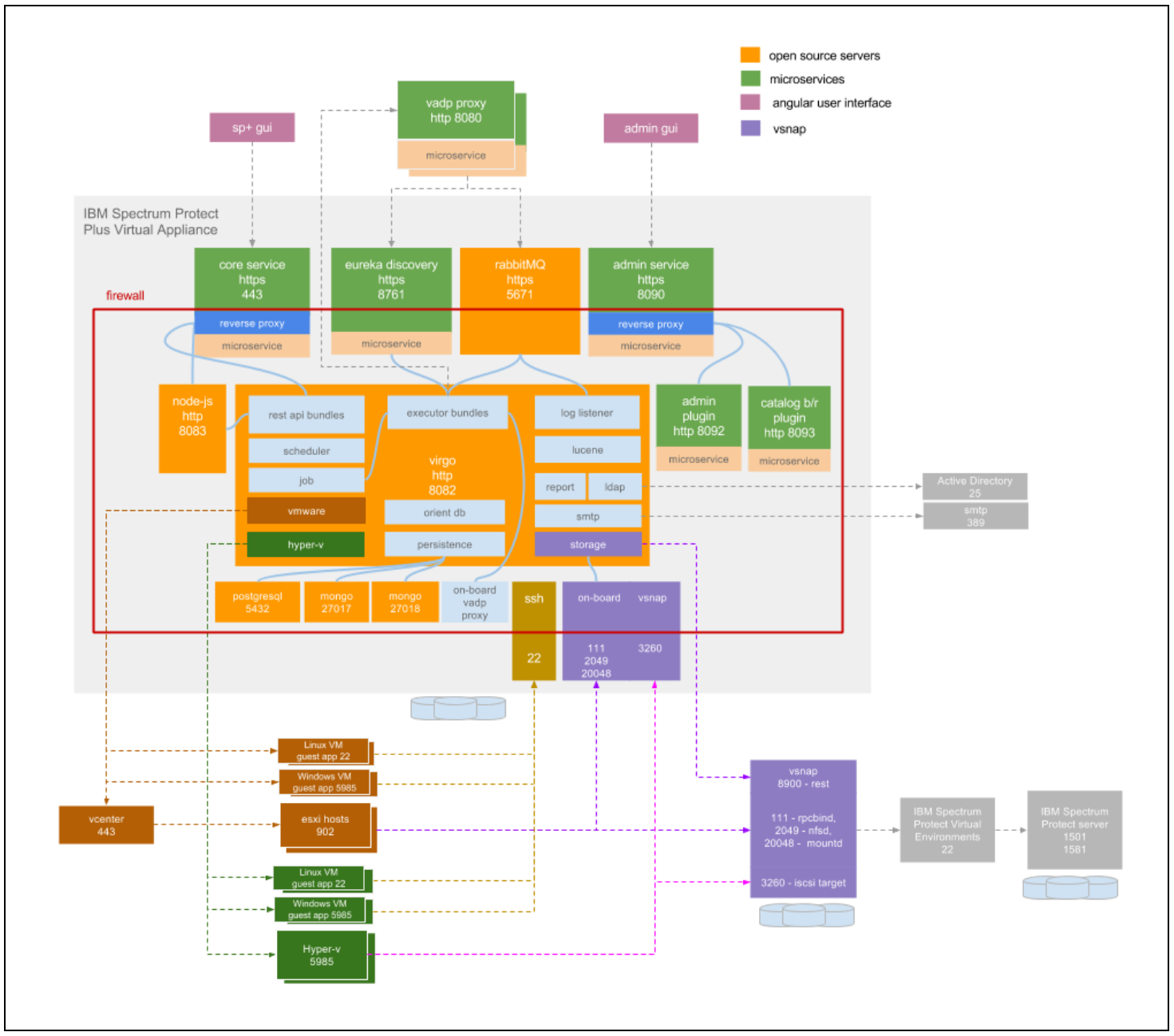
The **labeled resources** within the gray background represent the core services of the IBM Spectrum Protect Plus virtual appliance. The **curved lines** represent implicit communications.

The **colors** of the various modules represent different types of services as defined by the key in the upper right.

The **red rectangle** represents the network firewall. Services that appear on the red rectangle are indicative of the ports that are open on the firewall.

Dashed arrows represent communication among resources and services. The arrow flows TOWARD the listening port. The **port numbers** that need to be open are indicated by the LISTENING port.

For example, the vSnap service near the bottom of the diagram is represented as being external to the IBM Spectrum Protect Plus virtual appliance. It is listening on port 8900 as well as other ports. As represented by the dashed line, a component within the virtual appliance establishes a communication path by way of a connection to the vSnap service at port 8900.



RELATED TOPICS:

- File Indexing and Restore Requirements on page **21**
- Install IBM Spectrum Protect Plus as a VMware Virtual Appliance on page **25**
- Install IBM Spectrum Protect Plus as a Hyper-V Virtual Appliance on page **28**

Virtual Machine Privileges

The following vCenter permissions are required for Backup and Restore operations if a virtual machine is configured as a provider in IBM Spectrum Protect Plus with credentials lower than an administrator.

vCenter Permissions for Backup and Restore Operations

Datacenter

- Create datacenter
- Reconfigure datacenter

Datastore

- Allocate space
- Browse datastore
- Configure datastore
- Low level file operations
- Remove file
- Update virtual machine files

Datastore Cluster

- Configure a datastore cluster

Distributed switch

- Create
- Delete
- Host operation
- Modify
- Move
- Network I/O Control operation
- Policy operation
- Port configuration option
- Port setting operation
- VSPAN operation

ESX Agent Manager

- Config
- Modify
- View

Extension

- Register extension

Folder

- Create folder
- Delete folder
- Move folder
- Rename folder

Global

- Cancel task
- Diagnostics (used for troubleshooting, not required for operations)
- Disable methods
- Enable methods
- Licenses
- Log event
- Manage custom attributes
- Set custom attribute
- Settings

Host

- Configuration
- Advanced settings
- Storage partition configuration

Network

- Assign network
- Configure
- Move network
- Remove

Resource

- Apply recommendation
- Assign a vApp to resource pool
- Assign virtual machine to resource pool
- Create resource pool
- Migrate powered off VM
- Migrate powered on VM
- Modify resource pool
- Move resource pool
- Query vMotion
- Remove resource pool
- Rename resource pool

Sessions

- View and stop sessions

Storage views

- Configure service
- View

Tasks

- Create task
- Update task

Virtual Machine > Configuration

- Add existing disk
- Add new disk
- Add or remove device
- Advanced
- Change CPU count
- Change resource
- Configure managedBy
- Disk change tracking
- Disk lease
- Display connection settings
- Extend virtual disk

- Host USB device
- Memory
- Modify device settings
- Query Fault Tolerance compatibility
- Query unowned files
- Raw device
- Reload from path
- Remove disk (detach and remove virtual disk)
- Rename
- Reset guest information
- Set annotation
- Settings
- Swapfile placement
- Unlock virtual machine
- Upgrade virtual machine compatibility

Virtual Machine > Guest Operations

- Guest Operation Modifications
- Guest Operation Program Execution
- Guest Operation Queries

Virtual Machine > Interaction

- Answer question
- Backup operation on virtual machine
- Configure CD media
- Configure floppy media
- Console interaction
- Create screenshot
- Defragment all disks
- Device connection
- Disable Fault Tolerance
- Enable Fault Tolerance
- Guest operating system management by VIX API
- Inject USB HID scan codes

- Perform wipe or shrink operations
- Power Off
- Power On
- Record session on VM
- Replay session on VM
- Reset
- Resume Fault Tolerance
- Suspend
- Suspend Fault Tolerance
- Test failover
- Test restart Secondary VM
- Turn Off Fault Tolerance
- Turn On Fault Tolerance
- VMware Tools install

Virtual Machine > Inventory

- Create from existing
- Create new
- Move
- Register
- Remove
- Unregister

Virtual Machine > Provisioning

- Allow disk access
- Allow read-only disk access
- Allow virtual machine download
- Allow virtual machine files upload
- Clone template
- Clone virtual machine
- Create template from virtual machine
- Customize
- Deploy template
- Mark as template

- Mark as virtual machine
- Modify customization specification
- Promote disks
- Read customization specifications

Virtual Machine > Service configuration

- Allow notifications
- Allow polling of global event notifications
- Manage service configurations
- Modify service configurations
- Query service configurations
- Read service configurations

Virtual Machine > Snapshot management

- Create snapshot
- Remove snapshot
- Rename snapshot
- Revert to snapshot

Virtual Machine > vSphere Replication

- Configure replication
- Manage replication
- Monitor replication

vApp

- Add VM (to vApp)
- Assign resource pool to vApp
- Assign vApp (to another vApp)
- Clone
- Create
- Delete
- Export
- Import
- Move
- Power Off

- Power On
- Rename
- Suspend
- Unregister
- View OVF Environment
- vApp application configuration
- vApp instance configuration
- vApp managedBy configuration
- vApp resource configuration

In the All Privileges section located below the permissions selection window, ensure **Propagate to children** is selected.

File Indexing and Restore Requirements

Review the following requirements for indexing and restoring files through IBM Spectrum Protect Plus.

General Requirements for VMware

In the virtual machine settings under Advanced Configuration, the *disk.enableUUID* setting must be present and set to true.

Windows Requirements

- Supported operating systems: Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016
- Supported file systems: NTFS, ReFS, CsvFS

IBM Spectrum Protect Plus supports only the operating systems available to your hypervisors. Review your hypervisor's documentation for information about supported operating systems.

File indexing and restore operations support SCSI disks in a Hyper-V environment. IDE disks are not supported. Note that Generation 1 virtual machines require IDE boot disks, however if additional SCSI disks are available, file indexing and restore operations will be supported on those disks.

Windows Remote Shell (WinRM) must be enabled. By default, WinRM is not enabled in a Windows Server 2008 R2 or Windows 10 Server environments. To ensure services are able to receive connections, perform the following procedure: Run `winrm quickconfig`, then select `Yes` to make changes. This adds a listener for port 5985. To ensure the listener is available, enter the following command: `winrm e winrm/config/listener`.

Note: IBM Spectrum Protect Plus can protect and restore virtual machines with other file systems, but only the file systems listed above are eligible for file indexing and restore.

When file indexing is performed in a Windows environment, the following directories on the resource are skipped: /Drivers, /Program Files, /Program Files (x86), /Windows, and /winnt. Files within these directories are not added to the IBM Spectrum Protect Plus Inventory and are not available for file recovery.

Ensure the latest version of VMware Tools is installed on VMware virtual machines, and Hyper-V Integration Services is installed on your Hyper-V virtual machines.

Space Requirements

The C drive must have sufficient temporary space to save the file indexing results.

Connectivity Requirements

- The hostname of the IBM Spectrum Protect Plus appliance should be resolvable from the Windows virtual machine. If the hostname of the IBM Spectrum Protect Plus appliance is not resolvable, add the IP address of the appliance in the *ecxAddress* field in the IBM Spectrum Protect Plus configuration file, which can be found in the following location on the appliance:

  /opt/virgo/repository/ecx-usr/com.catalogic.ecx.deploy.vmware.ecxvmdeployer.json

- The IP address of the virtual machine selected for indexing must be visible to the vSphere client or Hyper-V Manager.
- The Windows virtual machine selected for indexing must allow outgoing connections to port 22 (ssh) on the IBM Spectrum Protect Plus appliance.
- All firewalls must be configured to allow IBM Spectrum Protect Plus to connect to the server through WinRM.

Authentication and Privilege Requirements

The credentials specified for the virtual machine must include a user with the following privileges:

- The user identity must have 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.
- 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. Note that credentials must be established for the associated virtual machine through the Guest OS Username and Guest OS Password option within the associated backup job definition.
- The system login credential must have the permissions of the local administrator.

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. Note that Kerberos does not allow local user accounts to be used and is only suitable for environments in which all machines are on a single domain.
- 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 5 minutes. Note that the default Windows NTLM protocol is not time dependent.

Linux Requirements

- Supported operating systems: Red Hat Enterprise Linux 6.4+, CentOS 6.4+, Red Hat Enterprise Linux 7.0+, CentOS 7.0+, SUSE Linux Enterprise Server 12.0+
- Supported file systems: ext2, ext3, ext4, XFS.

IBM Spectrum Protect Plus supports only the operating systems available to your hypervisors. Review your hypervisor's documentation for information about supported operating systems.

Note: IBM Spectrum Protect Plus can protect and restore virtual machines with other file systems, but only the file systems listed above are eligible for file indexing and restore.

When file indexing is performed in a Linux environment, the following directories on the resource are skipped: /tmp, /usr/bin, /Drivers, /bin, and /sbin. Files within these directories are not added to the IBM Spectrum Protect Plus Inventory and are not available for file recovery.

Software Requirements

- Python version 2.6.x or 2.7.x must be installed.
- When file systems are indexed, temporary metadata files are generated under the /tmp directory and then deleted as soon as the indexing is complete. The amount of free space required for the metadata depends on the total number of files present on the system. Ensure that there is approximately 350 MB of free space per 1 million files.
- Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 6.x only: Ensure the *util-linux-ng package* is up-to-date by running `yum update util-linux-ng`. Depending on your version or distribution, the package may be named *util-linux*.
- If data resides on LVM volumes, ensure the LVM version is 2.02.118 or later. Run `lvm version` to check the version and run `yum update lvm2` to update the package if necessary.
- If data resides on LVM volumes, the *lvm2-lvmetad* service must be disabled as it can interfere with IBM Spectrum Protect Plus's ability to mount and resignature 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`

  For a discussion of the lvmetad service, see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Logical_Volume_Manager_Administration/metadatadaemon.html.
- 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.

Connectivity Requirements

The SSH service must be running on port 22 on the server, and any firewalls must be configured to allow IBM Spectrum Protect Plus to connect to the server through SSH. The SFTP subsystem for SSH must also be enabled. For SFTP configuration information, see https://en.wikibooks.org/wiki/OpenSSH/Cookbook/File_Transfer_with_SFTP.

Authentication and Privilege Requirements

The credentials specified for the virtual machine must specify a user that has the following sudo privileges:

- The *sudoers* configuration must allow the user to run commands without a password.
- The !*requiretty* setting must be set.

The recommended approach is to create a dedicated IBM Spectrum Protect Plus Agent user with the following privileges. Sample configuration:

- Create user: `useradd -m sppagent`
- Set a password: `passwd sppagent`
- Place the following lines at the end of your sudoers configuration file, typically */etc/sudoers*. If your existing sudoers file is configured to import configurations from another directory (for example, /etc/sudoers.d), you can also place the lines in a new file in that directory:
  - `Defaults:sppagent !requiretty`
  - `sppagent ALL=(root) NOPASSWD:ALL`

RELATED TOPICS:

- Restore a File on page **76**
- System Requirements on page **8**

Install IBM Spectrum Protect Plus as a VMware Virtual Appliance

To install IBM Spectrum Protect Plus, deploy an OVF template. This 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.

It is recommended to work with your network administrator when configuring network properties.

This topic is for VMware environments. For Hyper-V installation instructions, see Install IBM Spectrum Protect Plus as a Hyper-V Virtual Appliance on page **28**.

BEFORE YOU BEGIN:

- Review IBM Spectrum Protect Plus system requirements. See System Requirements on page **8**.
- Before deployment, run MD5 Checksum on the downloaded OVA file. Ensure the generated checksum matches the one provided in the MD5 Checksum file, which is part of the software download.
- You may need to configure an IP address pool 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), network prefix, gateway, DNS search string, and a DNS server IP address.
- To use DHCP instead of a static IP address with network access to a properly configured DHCP server, leave all fields blank when prompted to enter network properties. If you don't have access to a DHCP server and wish to use a static IP address, assign a static IP with the NetworkManager Text User Interface (nmtui). See To assign a static IP with NetworkManager Text User Interface (nmtui) on page **26**.
- To change the IP address allocation type after IBM Spectrum Protect Plus deploys, redeploy the virtual machine.
- For later versions of vSphere, the vSphere Web Client may be required to deploy IBM Spectrum Protect Plus appliances.
- Note that IBM Spectrum Protect Plus has not been tested for IPv6 environments.

To install IBM Spectrum Protect Plus as a virtual appliance:

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 IBM Spectrum Protect Plus OVA template 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's default 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 wish to use a static IP address, assign a static IP with the NetworkManager Text User Interface (nmtui). See To assign a static IP with NetworkManager Text User Interface (nmtui) on page **26**.

   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 between 1 and 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. This can be done from vSphere Client.

    Note: The virtual machine must remain powered on for the IBM Spectrum Protect Plus application to be accessible.
12. Make a note of the IP address of the newly created virtual machine. This is needed 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.

    Note: You must allow several minutes for IBM Spectrum Protect Plus to initialize completely.

To assign a static IP with NetworkManager Text User Interface (nmtui)

A network administrator can assign static IP addresses with the NetworkManager Text User Interface (nmtui), which is a CentOS tool used to configure networking options. Sudo privileges are required to run nmtui.

1. Ensure the newly imported IBM Spectrum Protect Plus virtual machine is powered on. From a CentOS command line, enter `nmtui` to open the NetworkManager Text User Interface. Navigate the interface with arrow keys and press Enter to make a selection.
2. From the main menu, select **Edit a connection**.
3. Select the network connection, then select **Edit**.
4. On the Edit Connection screen, enter an available static IP address that is not already in use.
5. Select **OK** to save the static IP configuration.

Upload the Product Key

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

1. Save the product key to a computer with Internet access. Make a note of the location on your computer.
2. From a supported browser, enter the following URL to access the Administrative Console of the virtual machine where IBM Spectrum Protect Plus is deployed:

   https://<HOSTNAME>:8090/

   where *<HOSTNAME>* is the IP address of the virtual machine where the application is deployed.
3. In the login window, select **System** from the **Authentication Type** drop-down menu. Enter your password to access the Administrative Console. The default password is **sppadLG235**.
4. Click **Manage your licenses**. Click **Choose File**, then browse for the product key on your computer, then click **Upload new license**.
5. Click **Logout**.

NEXT STEPS:

- Reboot the newly create virtual appliance if you are using a static IP address instead of DHCP.
- Start IBM Spectrum Protect Plus and begin using it from any supported web browser. See Start IBM Spectrum Protect Plus on page **31**.

RELATED TOPICS:

- Start IBM Spectrum Protect Plus on page **31**

Install IBM Spectrum Protect Plus as a Hyper-V Virtual Appliance

To install the IBM Spectrum Protect Plus application in a Hyper-V environment, you will import a Hyper-V template. This 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.

This topic is for Hyper-V environments. For VMware installation instructions, see Install IBM Spectrum Protect Plus as a VMware Virtual Appliance on page **25**.

BEFORE YOU BEGIN:

- Review IBM Spectrum Protect Plus system requirements. See System Requirements on page **8**.
- 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 with the NetworkManager Text User Interface (nmtui), which is a CentOS tool used to configure networking options. See To assign a static IP with NetworkManager Text User Interface (nmtui) on page **29**.
- 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.

To install IBM Spectrum Protect Plus as a Hyper-V virtual appliance:

1. Locate the IBM Spectrum Protect Plus installer file at IBM Passport Advantage. The installer file is named SPP-{release}.
2. Copy the installation file to your Hyper-V server.
3. Launch the installer and complete the installation steps.
4. Once complete, close the installer.
5. Open Hyper-V Manager and select the required server.
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 you designated during the installation and select the Virtual Machines folder.
8. Click **Next**. The Select Virtual Machine dialog opens.

9. Select **SPP-{release}**, then click **Next**. The Choose Import Type dialog opens.
10. Choose the following import type: **Register the virtual machine in place**. Click **Next**.
11. If the Connect Network dialog opens, specify the virtual switch to use, then click **Next**. The Completing Import dialog opens.
12. Review the description, then click **Finish** to complete the import process and close the Import Virtual Machine wizard. The virtual machine is imported.
13. Right-click the newly deployed VM, then click **Settings...**
14. Under the section named IDE Controller 0, select **Hard Drive**.
15. Click **Edit**, then click **Next**.
16. In the Choose Action screen, choose **Convert** then click **Next**.
17. For the Disk Format, choose **VHDX**.
18. For the Disk Type, choose **Fixed Size**.
19. For the Configure Disk option, give the disk a new name and optionally, a new location.
20. Review the description, then click **Finish** to complete the conversion.
21. Once the conversion completes, click **Browse**, then locate and select the newly created VHDX.
22. Repeat steps 15 through 21 for each disk under the SCSI Controller section.
23. Power on the virtual machine from the Hyper-V Manager.
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 using NetworkManager Text User Interface, see the following section.

To assign a static IP with NetworkManager Text User Interface (nmtui)

A network administrator can assign static IP addresses with the NetworkManager Text User Interface (nmtui), which is a CentOS tool used to configure networking options.

1. Ensure the newly imported IBM Spectrum Protect Plus virtual machine is powered on. Log in to the IBM Spectrum Protect Plus virtual machine's console as the root user. The initial root password is **sppDP758**.
2. From a CentOS command line, enter `nmtui` to open the NetworkManager Text User Interface. Navigate the interface with arrow keys and press Enter to make a selection.
3. From the main menu, select **Edit a connection**.
4. Select the network connection, then select **Edit**.
5. On the Edit Connection screen, enter your static IP configuration.
6. Select **OK** to save the static IP configuration.

Upload the Product Key

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

1. Save the product key to a computer with Internet access. Make a note of the location on your computer.
2. From a supported browser, enter the following URL to access the Administrative Console of the virtual machine where IBM Spectrum Protect Plus is deployed:

   https://<HOSTNAME>:8090/

   where *<HOSTNAME>* is the IP address of the virtual machine where the application is deployed.
3. In the login window, select **System** from the **Authentication Type** drop-down menu. Enter your password to access the Administrative Console. The default password is **sppadLG235**.
4. Click **Manage your licenses**. Click **Choose File**, then browse for the product key on your computer, then click **Upload new license**.
5. Click **Logout**.

Note: 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.

NEXT STEPS:

- Start IBM Spectrum Protect Plus and begin using it from any supported web browser. See Start IBM Spectrum Protect Plus on page **31**.

RELATED TOPICS:

- Start IBM Spectrum Protect Plus on page **31**

Start IBM Spectrum Protect Plus

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

BEFORE YOU BEGIN:

- IBM Spectrum Protect Plus must be installed prior to starting the application. See Install IBM Spectrum Protect Plus as a VMware Virtual Appliance on page **25** or Install IBM Spectrum Protect Plus as a Hyper-V Virtual Appliance on page **28**.
- The System Administrator must provide you with the IP address for the virtual appliance and the IBM Spectrum Protect Plus user name and password.

To start IBM Spectrum Protect Plus:

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

   https://<HOSTNAME>

   where *<HOSTNAME>* 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 Install vSnap Server on page **38**.

RELATED TOPICS:

- Install IBM Spectrum Protect Plus as a VMware Virtual Appliance on page **25**
- Install IBM Spectrum Protect Plus as a Hyper-V Virtual Appliance on page **28**
- System Requirements on page **8**
- Account on page **96**

Configure 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.

To create an SLA Policy:

1. From the navigation menu, click **SLA Policy**.
2. Click **Add** . The New SLA Policy pane opens.
3. In the **Name** field, enter a name that will provide a meaningful description of the SLA Policy.
4. In the Backup Target 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 copies. In the **Every** field, set the backup frequency and interval.
5. In the **Target Site** field, select a primary or secondary vSnap 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 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.

   Note: Microsoft Hyper-V is not currently supported for offloading.
7. 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.

NEXT STEPS:

- Assign user permissions to the SLA policy. See User Access on page **98**.
- Create a Backup job definition that utilizes an SLA Policy.

RELATED TOPICS:

- Offloading to IBM Spectrum Protect by Using IBM Spectrum Protect Plus on page **34**
- Create a VMware Backup Job Definition on page **56**
- Create a Hyper-V Backup Job Definition on page **70**

Offloading to IBM Spectrum Protect by Using IBM Spectrum Protect Plus

IBM Spectrum Protect 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.

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

BEFORE YOU BEGIN:

- Review the IBM Spectrum Protect for Virtual Environments vmname restrictions: https://www.ibm.com/support/knowledgecenter/SSERB6_8.1.0/ve.user/r_ve_vmcli_backup.html.
- Review unsupported characters in VM or datacenter names: https://www.ibm.com/support/knowledgecenter/SSERB6_8.1.0/ve.user/r_ve_gui_troubleshoot.html.
- 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.

CONSIDERATIONS:

- 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 IBM 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 backup and offloading of virtual machine templates, you must specify VMENABLETEMPLATEBACKUPS in the data mover options file. Note that a backup of a templates can only be performed as a Full type backup. For more information about configuring your environment for backing up virtual machine templates, see https://www.ibm.com/support/knowledgecenter/en/SSEQVQ_8.1.2/client/r_opt_vmenabletemplatebkup.html.
- 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.

RELATED TOPICS:

- VMware Overview on page **53**
- Configure SLA Policies on page **32**

vSnap Installation and Setup

The topics in the following section cover installing, configuring, and administrating vSnap servers.

Install vSnap Server

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 v-Snap server might be sufficient.

In larger backup enterprise environments, additional vSnap servers might be desired. 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

vSnap servers can be deployed through the following formats:

- IBM Spectrum Protect Plus default installation, which includes a pre-registered vSnap server with the name *localhost*. Before the storage can be used, additional software components will be initialized and a storage pool will be created. Refer to Initial Configuration on page **41** for next steps.
- Physical vSnap server, installed on a physical machine
- Virtual vSnap server, installed in a VMware or Hyper-V environment

BEFORE YOU BEGIN:

- Review vSnap requirements. See System Requirements on page **8**.

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`.

To install a vSnap Server in a Physical environment.:

1. Install CentOS Linux 7.3.1611 (x86_64) or CentOS Linux 7.4.1708 (x86_64). The "Minimal Install" configuration is sufficient, but you can also install additional packages including a graphical user interface if desired. The root partition must have at least 8GB of free space after installation.
2. Edit the file `/etc/selinux/config`, change the `SELINUX` setting to *permissive*, then reboot the system for the changes to take effect.

3. Download the vSnap installation package, which is a self-extracting archive named vsnap-dist-<version>.run.
4. Make the file executable through the following command: `chmod +x vsnap-dist-<version>.run`, then execute it. The vSnap packages are installed, plus all of its dependencies.
5. Refer to Initial Configuration on page **41** for next steps.

To install a virtual vSnap server in a VMware environment:

1. Locate the vSnap OVA file at IBM Passport Advantage.
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 vSnap OVA template 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 machine's default 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 wish to use a static IP address, assign a static IP with the NetworkManager Text User Interface (nmtui). For information about using nmtui, see Install IBM Spectrum Protect Plus as a VMware Virtual Appliance on page **25**.

   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 between 1 and 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. This can be done from vSphere Client.

    Note: The virtual machine must remain powered on for the vSnap server to be accessible.
13. Make a note of the IP address of the newly created virtual machine. This is needed 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.
14. Refer to Initial Configuration on page **41** for next steps.

To install 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.

Note: 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 rebooted.

1. Locate the vSnap installer file at IBM Passport Advantage.
2. Copy the installation file to your Hyper-V server.
3. Launch 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** and 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**. If the Connect Network dialog opens, specify the virtual switch to use, then click **Next**. The Completing Import dialog opens.
10. Review the description, then click **Finish** to complete the import and close the Import Virtual Machine wizard. The virtual machine is imported.
11. Right-click the newly deployed VM, then click **Settings...**
12. Under the section named IDE Controller 0, select **Hard Drive**.
13. Click **Edit**, then click **Next**.

14. In the Choose Action screen, choose **Convert** then click **Next**.
15. For the Disk Format, choose **VHDX**.
16. For the Disk Type, choose **Fixed Size**.
17. For the Configure Disk option, give the disk a new name and optionally, a new location.
18. Review the description, then click **Finish** to complete the conversion.
19. Once the conversion completes, click **Browse**, then locate and select the newly created VHDX.
20. Repeat steps 13 through 19 for each disk under the SCSI Controller section.
21. Power on the virtual machine from the Hyper-V Manager. If prompted, select the option where the kernel boots in rescue mode.
22. 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.
23. Refer to Initial Configuration on page **41** for next steps.

    Note: 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.

To assign a static IP with NetworkManager Text User Interface (nmtui)

A network administrator can assign static IP addresses with the NetworkManager Text User Interface (nmtui), which is a CentOS tool used to configure networking options.

1. Ensure the newly imported vSnap server is powered on. Log in to the vSnap server console as the root user. The initial root password is **sppDP758**.
2. From a CentOS command line, enter `nmtui` to open the NetworkManager Text User Interface. Navigate the interface with arrow keys and press Enter to make a selection.
3. From the main menu, select **Edit a connection**.
4. Select the network connection, then select **Edit**.
5. On the Edit Connection screen, enter your static IP configuration.
6. Select **OK** to save the static IP configuration.

Initial Configuration

Before using a new installation of vSnap, you must perform the following initial configuration tasks:

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

Register the vSnap server as a backup storage target

Note: If deploying an IBM Spectrum Protect Plus appliance, a vSnap installation is present on the same appliance, and the following section can be skipped. The default, or on-board, vSnap is registered in IBM Spectrum Protect Plus with the name *localhost* when the appliance is deployed.

1. Log in to the vSnap server console as the root user and run `vsnap user create`. The initial root password is **sppDP758**.
2. Enter a username 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. See Add a Backup Storage Provider on page **45**.

System and Storage Initialization

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 needs to be run only on new installations.

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 100GB unused virtual disk which is used to create the pool. Refer to vSnap Server Administration Reference on page **47** for details on how to expand and administer the pool.

If no unused disks are found, the initialization process completes without creating a pool. Refer to vSnap Server Administration Reference on page **47** for details on how to create and administer a pool.

Simple Initialization

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

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 them into IBM Spectrum Protect Plus as described in Register the vSnap server as a backup storage target on page **41**, then from the **Actions** menu, select **Initialize** for each server. The initialization process runs in the background and requires no further user interaction. Note that the process may take 5 to 10 minutes to complete.

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.

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 `vsnap system init --skip_pool`. The command requires no further interaction and performs all initialization tasks except for the creation of a storage pool. Note that the process may take 5 to 10 minutes to complete.
3. Refer to vSnap Server Administration Reference on page **47** for details on how to create and administer a pool.

To update your vSnap server:

The default, or on-board, vSnap server is updated along with the IBM Spectrum Protect Plus appliance. To update additional vSnap servers that are installed on either virtual or physical appliances, perform the following procedure.

Download the self-extracting archive *snap-dist-version.run* file from the FixCentral Online Web site to a temporary location on the vSnap server. For information about the file and how to obtain it from Fix Central, see technote 404421.

If a vSnap server update is not required for a patch, an update file is not provided with the patch.

1. Ensure there are no active jobs utilizing the vSnap server to be updated. Once associated jobs complete or are in an idle state, navigate to the Systems > Job Monitoring page in IBM Spectrum Protect Plus, then select **Hold Schedule** from the **Actions** list for each job.
2. Download the latest vSnap installation package, which is a self-extracting archive named vsnap-dist-<version>.run, to a temporary location on the vSnap server.
3. On the vSnap server, open a terminal.
4. From the directory where the file was downloaded, make the file executable through the following command: `chmod +x vsnap-dist-<version>.run`.
5. From the directory where the file was downloaded, execute the installer through the following command: `./vsnap-dist-<version>.run`.The vSnap packages are installed, plus all of its dependencies.
6. On the Job Monitoring page in IBM Spectrum Protect Plus, select **Release Schedule** from the **Actions** list for the jobs that are associated with the vSnap server.

NEXT STEPS:

- Configure advanced vSnap features such as network configuration or storage pool management. See vSnap Server Administration Reference on page **47**.
- Start IBM Spectrum Protect Plus and begin using it from any supported web browser. See Start IBM Spectrum Protect Plus on page **31**.
- Register the newly added vSnap server in IBM Spectrum Protect Plus. See Add a Backup Storage Provider on page **45**.

RELATED TOPICS:

- Add a Backup Storage Provider on page **45**
- vSnap Server Administration Reference on page **47**

Add a Backup Storage Provider

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 registered so IBM Spectrum Protect Plus recognizes it.

BEFORE YOU BEGIN:

- Configure a vSnap server. See vSnap Server Administration Reference on page **47**.

To register Backup Storage:

1. From the navigation menu, click **Backup Storage**.
2. Click **Add** . The Storage Properties pane opens.
3. Populate 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 include Primary and Secondary. If more than one Primary or Secondary Backup Storage is available to IBM Spectrum Protect Plus, the Backup Storage with the largest amount of available storage will be 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 may take 5 to 10 minutes to complete.

To expand 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. Once complete, perform the following procedure.

Note: Pool expansion must be performed by adding new, unused disks to the pool. Expanding existing disks that are already part of the pool is not supported.

1. From the navigation menu, click **Backup Storage**.
2. From the **Actions** menu associated with an existing vSnap server you wish to expand, select **Rescan**.
3. Click the **Manage** icon associated with the vSnap server you wish to expand, then expand the **Add New Disks vSnap Storage** section. The Manage vSnap Server section displays.
4. Add and save the newly added disks. The vSnap pool expands by the size of the added disks.

RELATED TOPICS:

- Install vSnap Server on page **38**
- vSnap Server Administration Reference on page **47**
- Create a VMware Backup Job Definition on page **56**
- Create a Hyper-V Backup Job Definition on page **70**

vSnap Server Administration Reference

General vSnap Administration

Once vSnap 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 defined in IBM Spectrum Protect Plus.

However, you may still need to configure and administer certain aspects of vSnap, such as network configuration or storage pool management. The vSnap command-line interface is the primary means of administering vSnap. In addition, some of the most common operations can also be performed from the IBM Spectrum Protect Plus user interface.

Managing vSnap Using a Command Line Interface

Run the `vsnap` command to access the command line interface. The command can be invoked as the root user or any other OS user that has vSnap admin privileges. Use the `vsnap user create` command to create additional OS 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 **47** and Network Management on page **49** 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 IBM Spectrum Protect Plus User Interface

Log in to the IBM Spectrum Protect Plus user interface and from the navigation menu select **Backup Storage**. Click the **Manage** icon next to a vSnap server to manage it. Refer to Storage Management on page **47** and Network Management on page **49** for details.

Storage Management

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.

If vSnap was deployed as part of a virtual appliance, it already contains a 100GB 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.

Once you have added disks to a vSnap server, you can rescan to detect newly attached disks.

- To rescan using the IBM Spectrum Protect Plus user interface: From the navigation menu select **Backup Storage**, then click the **Actions** menu next to the relevant vSnap server and select **Rescan**.
- To rescan using the vSnap command line interface: Run `vsnap disk rescan`.

Run the command `vsnap disk show` to list all disks discovered on the 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 may 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's 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 performed the Simple initialization procedure described in Install vSnap Server on page **38**, a storage pool was already created automatically.

To create a storage pool manually, use the `vsnap pool create` command. Before running, ensure one or more unused disks are available as described in Managing Disks on page **47**. For information about available options, pass the `--help` flag to any command or subcommand to view usage help.

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 using the `vsnap pool update` command.

Your choice of pool type specified during creation 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.
- **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 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 one or more unused disks are available as described in Managing Disks on page **47**.

To expand a storage pool from the IBM Spectrum Protect Plus user interface, from the navigation menu select **Backup Storage**. Click the **Manage** icon next to a vSnap server to manage it, then expand the tab titled Add New Disks. 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.

To expand a storage pool from the command line interface, use the `vsnap pool expand` command. For information about available options, pass the `--help` flag to any command or subcommand to view usage help.

Network Management

Showing Network Interface Information

Run the `vsnap network show` command to list network interfaces and the services associated with each.

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

- **mgmt** - Used for management traffic between IBM Spectrum Protect Plus and vSnap.
- **nfs** - Used for data traffic when backing up data using NFS (currently used for VMware backups).
- **smb** - Used for data traffic when backing up data using SMB/CIFS (currently not used, reserved for future use.)
- **iscsi** - Used for data traffic when backing up data using iSCSI (currently used for Hyper-V backups).

Modifying Services Associated with Network Interfaces

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

Specify the following options:

--id <TEXT> - Enter the ID of the interface to update (required).

--services <TEXT> - Specify "all" or a comma-separated list of services to enable on the interface. The following are valid services: mgmt, nfs, smb, and iscsi (required).

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

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

RELATED TOPICS:

- Install vSnap Server on page **38**
- Add a Backup Storage Provider on page **45**

Operations

The topics in the following section cover backing up and restoring resources.

Operations Overview

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 hypervisor(s) that contain the components to be backed up. VMware vCenters and Microsoft Hyper-V servers are both supported hypervisors.
- The vSnap Storage Appliance(s) 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's 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.

RELATED TOPICS:

- VMware Overview on page **53**
- Hyper-V Overview on page **67**
- Restore a File on page **76**

VMware

The topics in the following section cover backing up and restoring VMware resources.

VMware Overview

In order 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.

RELATED TOPICS:

- Add a VMware Provider on page **54**
- Create a VMware Backup Job Definition on page **56**
- Create a VMware Restore Job Definition on page **59**

Add 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.

To register a VMware provider:

1. From the navigation menu, expand **Hypervisor**, then **VMware**. Click **Backup**.
2. Click **Manage vCenter**.
3. Click **Add** . The vCenter Properties pane opens.
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 username and password for the provider.

   Username

   Enter your username 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 VM's 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 operational recoveries, and one on the Spectrum Protect 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 vStorage Backup Server's operating system type. 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.

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.

NEXT STEPS:

- Assign user permissions to the hypervisor. See User Access on page **98**.

RELATED TOPICS:

- Create a VMware Backup Job Definition on page **56**
- Create a VMware Restore Job Definition on page **59**

Create a VMware Backup Job Definition

Back up VMware data including virtual machines, datastores, folders, vApps, and datacenters with snapshots using a VMware Backup job definition.

BEFORE YOU BEGIN:

- Register the providers you wish to back up. See Add a VMware Provider on page **54**.
- Configure an SLA Policy. See Configure SLA Policies on page **32**.
- 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 **User Access** feature. Roles and associated permissions are assigned during user account creation. See User Access on page **98** and Account on page **96**.

CONSIDERATIONS:

- 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.

To create a VMware Backup job definition:

1. From the navigation menu, expand Hypervisor, then VMware. Click **Backup**.
2. To see all vCenters, click **All**. if desired, filter your selections using the filter boxes and drop-down menus next to All. For example, click **VM not in Policy** to display all virtual machines that are not associated with an SLA Policy. Select one or more resources to back up.
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 Monitoring 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 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 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/ecxdeployer/<Latest-Date>/<Latest-Entry>/<VM name>.

VM Snapshot retry attempts

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

VADP Proxy

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

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 the

virtual machine can be accessed from the IBM Spectrum Protect Plus appliance either through DNS or host-name.

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 Jobs Monitoring pane.

NEXT STEPS:

- If in a Linux environment, consider creating VADP proxies to enable load sharing. See VADP Proxy on page **93**.
- Create a VMware Restore job definition. See Create a VMware Restore Job Definition on page **59**.

RELATED TOPICS:

- Create a VMware Restore Job Definition on page **59**
- Add a VMware Provider on page **54**

Create a VMware Restore Job Definition

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

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, copied, or put immediately into production use as needed.

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

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 Create a Fenced Network Through a VMware Restore Job on page **63**.

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 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.

BEFORE YOU BEGIN:

- Create and run a VMware Backup job. See Create a VMware Backup Job Definition on page **56**.
- 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 **User Access** feature. Roles and associated permissions are assigned during user account creation. See User Access on page **98** and Account on page **96**.

CONSIDERATIONS:

- When selecting virtual machines for recovery, recovery points offloaded to IBM Spectrum Protect storage cannot be recovered in Test Mode.
- 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.
- Recovery points that were offloaded to IBM Spectrum Protect storage cannot be used to recover VMDKs.
- 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.

To create a VMware Restore job definition:

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. To run the job now using default options, click **Restore**. To schedule the job to run using default options, click **Manage Job(s)** 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.

   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.

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 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 reconfiguration 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.

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.

   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 TOPICS:

- Create a Fenced Network Through a VMware Restore Job on page **63**
- Create a VMware Backup Job Definition on page **56**
- Add a VMware Provider on page **54**

Create 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 used for production. Fenced networking can be used with with jobs running in Test Mode and Production Mode.

Running a VMware Restore job in **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. Virtual machines created through Test mode are also given unique names and identifiers to avoid conflicts within your production environment.

Production Mode enables disaster recovery at the local site from primary storage or a remote disaster recovery site, replacing original machine images with recovered 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.

The following procedure describes how to create a fenced network through VMware Restore jobs.

BEFORE YOU BEGIN:

- Create and run a VMware Backup job. See Create a VMware Backup Job Definition on page **56**.

CONSIDERATIONS:

- When selecting virtual machines for recovery, recovery points offloaded to IBM Spectrum Protect storage cannot be recovered in Test Mode.
- Recovery points that were offloaded to IBM Spectrum Protect storage cannot be used to recover VMDKs.

To create a fenced network through a VMware Restore job:

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**. 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:

   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 will be retained.

   Use original IP configuration – For Test, during a restore, the destination virtual machine receives a new MAC address. The source IP address is retained

   Add mappings for subnets and IP addresses for VM guest OS on destination – the destination virtual machine can reconfigured with a new IP.

   To change the IP of the target machine, create a new mapping configuration: select Add mappings, enter an IP range 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. If a virtual machine is DHCP only, then IP reconfiguration is skipped for that virtual machine.

   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. To run the job now, click **Restore**. To schedule the job click **Manage Job(s)** and define a trigger for the job definition.
9. 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:

   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 TOPICS:

- Create a VMware Backup Job Definition on page **56**
- Add a VMware Provider on page **54**

Hyper-V

The topics in the following section cover backing up and restoring Hyper-V resources.

Hyper-V Overview

In order 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.

RELATED TOPICS:

- Add a Hyper-V Provider on page **68**
- Create a Hyper-V Backup Job Definition on page **70**
- Create a Hyper-V Restore Job Definition on page **73**

Add 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.

CONSIDERATIONS:

- Before registering the Hyper-V server in IBM Spectrum Protect Plus, the server must be added to the /etc/hosts file on the IBM Spectrum Protect Plus appliance via command line. 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.
- Run the following command through a command prompt with "run as administrator" enabled:

  ```
  winrm s winrm/config/service @{AllowUnencrypted="true"}
  ```
- Verify that the *AllowUnencrypted* option is set to *true* through the following command:

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

To register a Hyper-V provider:

1. From the navigation menu, expand **Hypervisor**, then **Hyper-V**. Click **Backup**.
2. Click **Manage Hyper-V Server**.
3. Click **Add** . The Server Properties pane opens.
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 username and password for the provider.

   Username

   Enter your username 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.

5. 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.

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.

NEXT STEPS:

- Assign user permissions to the hypervisor. See User Access on page **98**.

RELATED TOPICS:

- Create a Hyper-V Backup Job Definition on page **70**
- Create a Hyper-V Restore Job Definition on page **73**

Create a Hyper-V Backup Job Definition

BEFORE YOU BEGIN:

- Register the providers you wish to back up. See Add a Hyper-V Provider on page **68**.
- Configure an SLA Policy. See Configure SLA Policies on page **32**.
- Hyper-V Backup and Restore jobs require the installation of the latest Hyper-V integration services. For Microsoft Windows environments, see 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 perform backup and restore operations, roles must be assigned to the user. Grant users access to hypervisors and backup and restore operations through the **User Access** feature. Roles and associated permissions are assigned during user account creation. See User Access on page **98** and Account on page **96**.

To create a Hyper-V Backup job definition:

1. From the navigation menu, expand Hypervisor, then Hyper-V. Click **Backup**.
2. To see all Hyper-V resources, click **All**. if desired, filter your selections using the filter boxes and drop-down menus next to All. click **VM not in Policy** to display all virtual machines that are not associated with an SLA Policy. Select one or more resources to back up.
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 Monitoring 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 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/ecxdeployer/<Latest-Date>/<Latest-Entry>/<VM name>.

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 the virtual machine can be accessed from the IBM Spectrum Protect Plus appliance either through DNS or host-name.

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. 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 Jobs Monitoring pane.

RELATED TOPICS:

- Create a Hyper-V Restore Job Definition on page **73**
- Add a Hyper-V Provider on page **68**

Create a Hyper-V Restore Job Definition

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

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, copied, or put immediately into production use as needed.

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

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 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 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.

BEFORE YOU BEGIN:

- Create and run a Hyper-V Backup job. See Create a Hyper-V Backup Job Definition on page **70**.
- Hyper-V Backup and Restore jobs require the installation of the latest Hyper-V integration services. For Microsoft Windows environments, see 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 **User Access** feature. Roles and associated permissions

are assigned during user account creation. See User Access on page **98** and Account on page **96**.

CONSIDERATIONS:

- 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.

To create a Hyper-V Restore job definition:

1. From the navigation menu, expand Hypervisor, then Hyper-V. Click **Restore**.
2. In the Restore pane, review the available recovery points of your Hyper-V 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. To run the job now using default options, click **Restore**. To schedule the job to run using default options, click **Manage Job(s)** 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.

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 TOPICS:

- Create a Hyper-V Backup Job Definition on page **70**
- Add a Hyper-V Provider on page **68**

Restore 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:

- Review the File Indexing and Restore Requirements. See File Indexing and Restore Requirements on page **21**.
- 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 host-name. 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 indexing 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 Protect storage.
- 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.
- Use an NTP server to synchronize the time zones across IBM Spectrum Protect Plus resources in your environment, such as the IBM Spectrum Protect Plus appliance, storage arrays, hypervisors and application servers . 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 the following VMware knowledge base article: Time in virtual machine drifts due to hardware timer drift.

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 IBM Spectrum Protect Plus's ability to mount and resignature 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.

To restore a file:

1. From the navigation menu, click **File Restore**.
2. Search for a file to restore. Use filters to fine-tune your selection across specific virtual machines. See Search Guidelines on page **77**.
3. To restore the file using default options, click **Restore**. The file is restored to its original location.
4. To edit options before restoring the file, click **Options**. Set the file restore options.

   Overwrite existing files/folder

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

   Destination

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

Search Guidelines

- Enter a character string to find objects with a name that exactly matches the character string. Searching for the term **string.txt** will return the exact match, **string.txt**.
- Apply wildcards as needed.
- Regular Expression search entries are supported. For more information see https://docs.microsoft.com/en-us/sql/relational-databases/scripting/search-text-with-regular-expressions.

A wildcard is a character that you can substitute for zero or more unspecified characters when searching text. Position wildcards at the beginning, middle, or end of a string, and combine them within a string.

- Match a character string with an asterisk, which represents a variable string of zero or more characters:

  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

- Match a single character 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

You can use multiple asterisk wildcards in a single text string, though this might considerably slow down a large search.

The search functionality supports special characters, which must be escaped with a \ before the character. The following special characters are supported: + - & | ! ( ) { } [ ] ^ " ~ * ? : \

To search for a file named **string[2].txt**, enter the following: **string\[2\].txt**.

RELATED TOPICS:

- File Indexing and Restore Requirements on page **21**
- Create a VMware Backup Job Definition on page **56**
- Create a VMware Restore Job Definition on page **59**

Report

The topics in the following section cover running and customizing reports, as well as individual report details.

Reports Overview

IBM Spectrum Protect Plus provides a number of predefined reports, which you can tailor to meet your specific reporting requirements. Reports are based on the data collected by the most recently run Inventory job, and you can generate reports after all cataloging jobs and subsequent database condense jobs complete. Click Report from the navigation menu to display the Report pane. You can run reports with predefined default parameters or run and save customized reports driven by custom parameters.

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

RELATED TOPICS:

- Run, Save, and Schedule a Report on page **81**
- User Access on page **98**
- Backup Storage Utilization Reports on page **83**
- Protection Reports on page **84**
- System Reports on page **86**
- VM Environment Reports on page **87**

Run, Save, and Schedule a Report

Perform the following steps to run any report from the Report pane. You can run reports with predefined default parameters or run customized reports driven by custom parameters.

BEFORE YOU BEGIN:

- Before an IBM Spectrum Protect Plus user can view and run reports, roles must be assigned to the user. Roles and associated permissions are assigned during user account creation. See User Access on page **98** and Account on page **96**.
- From the Report pane, expand a report type, then select a report. Click **User Access**, select a user, then click **Add**. The user is granted access to the report based on the roles and associated permissions assigned to the user.

To run a report:

1. From the navigation menu, click **Report**.
2. From the Report pane, expand a report type, then select a report to run.
3. To run the report using default parameters, click **Run**. The report runs and displays on the Report pane.
4. To edit parameters before running the report, click **Options** . Parameters are unique to each report. Set the report parameters, then click **Run**.

Perform the following steps to create a report with customized parameters. Select a predefined report, set custom parameters, and save the report with a customized name to run on demand or create a schedule to run the report as defined by the parameters of the schedule.

To save a customized report:

1. From the navigation menu, click **Report**.
2. From the Report pane, expand a report type, then select a report to save.
3. Click **Options** to edit the report parameters.
4. Enter a **Name** and a **Description** for the customized report, then set the associated report parameters.
5. Click **Save**. The customized reports display nested under the source report on the Report pane.

Perform the following steps to schedule a report to run at a determined interval and time.

To schedule a report:

1. From the navigation menu, click **Report**.
2. From the Report pane, expand a report type, then select a report to schedule.

3. Click **Options** to edit the report parameters.
4. Enter a **Name** and a **Description** for the report, then set the associated report parameters.
5. Click **Schedule Report** to expand the schedule editor. Define a trigger for the report.
6. Enter an e-mail address to receive the scheduled report in the e-mail field, then click **Add a recipient**.
7. Click **Schedule**.

RELATED TOPICS:

- Reports Overview on page **80**
- Backup Storage Utilization Reports on page **83**
- Protection Reports on page **84**
- System Reports on page **86**
- VM Environment Reports on page **87**

Backup Storage Utilization Reports

Backup Storage Utilization reports display the storage utilization and status of your backup storage, such as vSnap servers.

BEFORE YOU BEGIN:

- Before an IBM Spectrum Protect Plus user can run specific reports, permissions must be assigned to the user. From the Report pane, expand a report type, then select a report. Click **Manage Permissions** to assign permissions to the report. For more information about assigning permissions to a report, see User Access on page **98**.

To view Backup Storage Utilization reports, click **Report** from the navigation menu, then expand the Backup Storage Utilization heading 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, as well as a detailed view of the individual virtual machines 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 protected on each vSnap server, enable the **Show VMs protected per vSnap Storage** parameter. This area of the report displays the virtual machines names, associated hypervisor, location, and the number of available recovery points on the vSnap server.

RELATED TOPICS:

- Run, Save, and Schedule a Report on page **81**
- Reports Overview on page **80**

Protection Reports

Protection reports display the protection status of your resources, and help ensure your data is protected through user-defined recovery point objective parameters.

BEFORE YOU BEGIN:

- Before an IBM Spectrum Protect Plus user can run specific reports, permissions must be assigned to the user. From the Report pane, expand a report type, then select a report. Click Manage Permissions to assign permissions to the report. For more information about assigning permissions to a report, see User Access on page **98**.

To view Protection reports, click **Report** from the navigation menu, then expand the Protection heading 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. The report can be tailored to show unprotected virtual machines, which will display the total number of virtual machines added to the IBM Spectrum Protect Plus inventory before running backup jobs.

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, as well as 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 their names and location.

VM Backup History Report

Run the VM Backup History report to review the protection history of specific virtual machines. Note that to run the report at least one virtual machine must be specified in the VMs option. The VMs option supports multiple virtual machine entries separated by commas.

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 the Detail View of the report, 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 number of virtual machines in compliance, not in compliance, and 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.

RELATED TOPICS:

- Run, Save, and Schedule a Report on page **81**
- Reports Overview on page **80**

System Reports

System reports offer an in-depth view of the status of your IBM Spectrum Protect Plus configuration, including storage system information, jobs, and their status.

BEFORE YOU BEGIN:

- Before an IBM Spectrum Protect Plus user can run specific reports, permissions must be assigned to the user. From the Report pane, expand a report type, then select a report. Click **Manage Permissions** to assign permissions to the report. For more information about assigning permissions to a report, see User Access on page **98**.

To view System reports, click **Report** from the navigation menu, then expand the System heading in the Report pane. The following reports are available:

Configuration Report

Review the configuration of the Hypervisor providers and Backup Storage available to IBM Spectrum Protect Plus.

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, its type, associated site, and the SSL connection status.

Job Report

Review the available jobs in your IBM Spectrum Protect Plus 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, as well as display jobs that have been successfully run over a period of time. The Summary View lists jobs by type along with the number of times a job session was run, completed, or failed. Job sessions listed as Other are jobs that have been aborted, partially run, are currently running, skipped, or stopped.

In the Detail View of the report, 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.

RELATED TOPICS:

- Run, Save, and Schedule a Report on page **81**
- Reports Overview on page **80**

VM Environment Reports

VM Environment reports display the storage utilization and status of your virtual machines and datastores.

BEFORE YOU BEGIN:

- Before an IBM Spectrum Protect Plus user can run specific reports, permissions must be assigned to the user. From the Report pane, expand a report type, then select a report. Click **Manage Permissions** to assign permissions to the report. For more information about assigning permissions to a report, see User Access on page **98**.

To view VM Environment reports, click **Report** from the navigation menu, then expand the VM Environment heading 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 datastores orphaned state displays 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 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 their 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, as well as 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 allocated for virtual disk files.

RELATED TOPICS:

- Run, Save, and Schedule a Report on page **81**
- Reports Overview on page **80**

System

The topics in the following section cover creating and configuring accounts, viewing scheduled jobs and audit logs, and monitoring the status of your VADP proxies.

System Overview

Configure and monitor your IBM Spectrum Protect Plus environment through the System menu. Create and configure accounts, view scheduled jobs and audit logs, and monitor the status of your VADP proxies.

RELATED TOPICS:

- Job Monitoring on page **91**
- Audit Logs on page **92**
- VADP Proxy on page **93**
- Account on page **96**
- LDAP / SMTP on page **101**

Job Monitoring

From the Job Monitoring pane you can run a job session on demand, pause or cancel a running job, and hold all future scheduled instances of a job from running until you are ready for the job to proceed.

To start a job session:

1. From the navigation menu, expand **System**, then click **Job Monitoring**.
2. Click the **Actions** drop-down menu associated with the job, then select **Start**. The job session runs.
3. Click **Expand** next to the running job session to view the job session details. Details include duration, start and end time, and total number of protected and failed VMs.

To hold and release a job's schedule:

1. From the navigation menu, expand **System**, then click **Job Monitoring**.
2. Click the **Actions** drop-down menu associated with the job, then select **Hold Schedule**. All future scheduled instance of the job will not run until released.
3. To release the reschedule, click the **Actions** drop-down menu associated with the job, then select **Release Schedule**.

Audit Logs

Audit logs can be viewed through the System menu. The Audit Log window displays a log of actions performed in IBM Spectrum Protect Plus, along with the user performing the action and a description of the action. Audit logs are searchable by user.

To collect audit logs from the Support menu:

1. From the navigation menu, expand **System**, then click **Audit Log**.
2. The Audit Log window displays a log of actions performed in IBM Spectrum Protect Plus, along with the user performing the action and a description of the action.
3. To search for the actions of a specific IBM Spectrum Protect Plus user, search for the user name in the Search User field.

VADP Proxy

In IBM Spectrum Protect Plus, running VMware Backup jobs through VADP can be taxing on your system resources. By creating VMware Backup job proxies, you enable load sharing and load balancing for those jobs in Linux environments.

Note that the first time a given job is run, the proxies do not take effect because VM clone technology is used. But the second and subsequent times the job is run, change block tracking technology is used and the proxies are employed.

If proxies exist, the entire processing load is shifted off the IBM Spectrum Protect Plus host machine and onto the proxies, else the entire load stays on the IBM Spectrum Protect Plus host. Within a Backup job, the processing load for any single VM is shifted to a single proxy machine; multiple VMs are shifted to multiple proxies if available.

If a proxy server goes down or is otherwise disabled before the start of the job, the other proxies (or if there are no other proxies, the IBM Spectrum Protect Plus host) take over and the job completes. If a proxy server becomes disabled during the running of a job, there is a possibility that the job will fail.

BEFORE YOU BEGIN:

- Determine how many proxies to create; the more proxies, the faster the jobs run. Each proxy is used merely to process data, and the results are returned through the host IBM Spectrum Protect Plus server. The only impact seen by the user is the improvement in performance when running the job.

To view proxy server connections:

1. From the navigation menu, expand **System**, then click **VADP Proxy**.
2. The VADP Proxy window displays each proxy server. Click **Expand**  next to the Service Type name to view detailed information about the proxy server.

Review the following for more information about creating VADP proxies.

System Requirements:

This feature has been tested only for SUSE Linux Enterprise Server and Red Hat environments. It is supported only in 64-bit quad core configurations with a minimum kernel of 2.6.32.

A minimum of 8 GB of RAM is required (16 GB recommended), along with 60 GB of disk space.

Each proxy must have a fully qualified domain name.

Port 8080 on the VADP proxy server must be open when the proxy server firewall is enabled. If the port is not open, VADP Backups will run on local vmdkbackup instead of the VADP proxy server.

Installer Notes:

The IBM Spectrum Protect Plus version of the VADP Proxy installer includes Virtual Disk Development Kit (VDDK) version 5.5.5. This version of the VADP proxy installer provides the following functionality:

- External VADP Proxy support with vSphere 6.5
- External VADP Proxy support for Hot Add operations, which provides higher performance for VADP Backups.

To create a proxy:

For each proxy:

1. Power up a physical or virtual Linux machine that meets the system requirements defined above, and is on the same network as the host IBM Spectrum Protect Plus machine.
2. Copy the VADP Proxy installation program to the local proxy machine.
3. Log in to the proxy machine as root, or as a user capable of running “sudo” commands. The initial root password is **sppDP758**.
4. On the proxy machine, open a terminal. Enter the following command to install the proxy server software:

   ```
   ./vmdkbackup-x.x-installer.bin
   ```

   The Setup wizard opens.

   Note: Alternatively you can run the installer using command line protocol by entering the following command: `./vmdkbackup-x.x-installer.bin --mode text`
5. Follow the steps in the Setup wizard to configure your proxy server and connect to the IBM Spectrum Protect Plus host.
   a. When prompted for the installation directory, select **/opt/IBM/SPP**.
   b. When prompted for the IBM Spectrum Protect Plus Discovery Server IP, enter the IP Address of the IBM Spectrum Protect Plus host.
6. Click **Finish** when the Setup wizard indicates it has completed. After installation, note that your new installation directory includes a subdirectory called `/log`, which is the job log location.

   After successful installation, the service **`ecxvadp`** is started on the proxy machine. A log file **`ecxvadp.log`** is generated in /opt/IBM/SPP/logs directory.

Repeat the previous steps for each proxy you want to create.

NEXT STEPS:

- Run the VMware Backup job. The use of the proxies are indicated in the job log by a log message similar to the following:


```
Run remote vmdkbackup of MicroService: http://<proxy
node name>, IP:<proxy IP address>
```

- Uninstall the proxies when you cease running the VMware Backup jobs. To uninstall a proxy, on your host machine, run the following command from the uninstall subdirectory of the installation directory (default installation directory is /opt/IBM/SPP):

  ```
  ./uninstall_vmdkbackup
  ```

  The installation directory is removed.

RELATED TOPICS:

- Create a VMware Backup Job Definition on page **56**

Account

To enable a user to log on to IBM Spectrum Protect Plus and use its functions, an administrator must first add the user to IBM Spectrum Protect Plus. From the Account pane, add new users, delete existing users, change user passwords, and assign user roles.

Role-based access control allows you to set the resources and permissions available to IBM Spectrum Protect Plus accounts. Through role-based access control, administrators can tailor IBM Spectrum Protect Plus for individual users, giving them access to the features and providers they need. Roles contain pre-defined sets of permissions, and are assigned during user account creation. Users are then associated with hypervisors, SLA policies, and reports through the **User Access** option, which is available throughout the IBM Spectrum Protect Plus interface. Resources and providers assigned to users through permissions will be available upon their next log in.

The following roles are available:

Administrator - The Administrator role provides access to all resources and privileges, which is comparable to the native administrator, or Super User role. No additional resource-specific privileges need to be granted for an Administrator. An Administrator can create new users, as well as edit, delete, and change the passwords of other users, with the exception of the Super User. The Administrator role can only be assigned to native users.

VM Administrator - The VM Administrator role allows a user to register and modify hypervisor resources and modify hypervisor resources delegated by an Administrator, as well as associate hypervisors to assigned SLA policies, perform backup and restore operations, and run and schedule reports delegated by an Administrator. Access to resources available to a VM Administrator must be manually applied by an Administrator through the User Access option on associated resource screens.

BEFORE YOU BEGIN:

- Before importing an LDAP group, register an LDAP provider in IBM Spectrum Protect Plus. See LDAP / SMTP on page **101**.

To add a native user:

1. From the navigation menu, expand **System**, then click **Account**.
2. Click **Add** . The Account Properties pane displays.
3. From the **Type** drop-down select **Native User**.
4. Populate the **Name**, **Password**, and **Confirm Password** fields.
5. In the **User Roles** section, assign a role to the user. For information about assigning roles and associated resources, see User Access on page **98**.
6. Click **Save**. The new user appears in the Account list.

To import an LDAP group:

1. From the navigation menu, expand **System**, then click **Account**.
2. Click **Add** . The Account Properties pane displays.
3. From the **Type** drop-down select **LDAP Group**.
4. From the **Group** field select an LDAP group to import
5. In the **User Roles** section, assign a role to the group. The Administrator role cannot be assigned to LDAP groups. For information about assigning roles and associated resources, see User Access on page **98**.
6. Click **Save**. The LDAP group appears in the Accounts list, and associated LDAP users can log in to IBM Spectrum Protect Plus.

To edit a native user's username and password:

All users can change their own usernames and passwords. An Administrator can change the usernames and passwords of other users, with the exception of the Super User.

1. From the navigation menu, expand **System**, then click **Account**.
2. Click the **Edit** icon associated with the account to change the username or the **Edit Password** icon to reset the password.
3. Click **Save**.

To delete a native user:

An Administrator can delete other users, with the exception of the Super User.

1. From the navigation menu, expand **System**, then click **Account**.
2. Click the **Delete** icon associated with the account. A confirmation dialog box displays.
3. Confirm the deletion. The user is deleted.

RELATED TOPICS:

- User Access on page **98**
- LDAP / SMTP on page **101**
- Start IBM Spectrum Protect Plus on page **31**

User Access

Role-based access control allows you to set the resources and permissions available to IBM Spectrum Protect Plus accounts. Through role-based access control, administrators can tailor IBM Spectrum Protect Plus for individual users, giving them access to the features and providers they need. Roles contain pre-defined sets of permissions, and are assigned during user account creation. Users are then associated with hypervisors, SLA policies, and reports through the **User Access** option, which is available throughout the IBM Spectrum Protect Plus interface. Resources and providers assigned to users through permissions will be available upon their next log in.

The following roles are available:

Administrator - The Administrator role provides access to all resources and privileges, which is comparable to the native administrator, or Super User role. No additional resource-specific privileges need to be granted for an Administrator. An Administrator can create new users, as well as edit, delete, and change the passwords of other users, with the exception of the Super User. The Administrator role can only be assigned to native users.

VM Administrator - The VM Administrator role allows a user to register and modify hypervisor resources and modify hypervisor resources delegated by an Administrator, as well as associate hypervisors to assigned SLA policies, perform backup and restore operations, and run and schedule reports delegated by an Administrator. Access to resources available to a VM Administrator must be manually applied by an Administrator through the User Access option on associated resource screens.

To assign Administrator privileges:

A native administrator (the account used to log in to IBM Spectrum Protect Plus for the first time) or a user with Administrator privileges can assign Administrator privileges to a new user. The Administrator role can only be assigned to native users.

1. From the navigation menu, expand **System**, then click **Account**.
2. Click **Add** . The Account Properties pane displays.
3. Select **Native User** as the user Type, then create the user's name and password.
4. In the User Roles section, select **Administrator**, then click **Save**. The user is created and now has access to all resources and privileges in IBM Spectrum Protect Plus.

To assign VM Administrator privileges:

A native administrator (the account used to log in to IBM Spectrum Protect Plus for the first time) or a user with Administrator privileges can assign privileges to a new user.

1. From the navigation menu, expand **System**, then click **Account**.
2. Click **Add** . The Account Properties pane displays.
3. Select the user Type. If assigning privileges to a Native User, create the user's name and password. If assigning privileges to an LDAP Group, select the LDAP group.

4. In the User Roles section, select **VM Administrator**, then click **Save**. The user is created with the assigned role. Access to resources available to the role must be manually applied by an Administrator through the User Access option on associated resource screens.

To grant users access to hypervisors:

Access to hypervisors must be manually applied through the User Access option on associated resource screens. A native administrator (the account used to log in to IBM Spectrum Protect Plus for the first time) or a user with Administrator privileges can assign the necessary resources.

1. From the navigation menu, expand **Hypervisor**, then **VMware** or **Hyper-V**. Click **Backup**.
2. From the Backup pane, select a hypervisor, then click **User Access**. The Add User pane opens.
3. Click **Add** .
4. Select a user from the Add User section. Click **Add**.

Upon next login, the user will have access to the assigned hypervisor resources.

To grant users access to SLA Policies:

Access to SLA Policies must be manually applied through the **User** icon associated with an SLA Policy. A native administrator (the account used to log in to IBM Spectrum Protect Plus for the first time) or a user with Administrator privileges can assign the necessary resources.

1. From the navigation menu, click **SLA Policy**.
2. From the SLA Policy pane, click the **User** icon associated with an SLA Policy. The Add User pane opens.
3. Click **Add** .
4. Select a user from the Add User section. Click **Add**.

Upon next login, the user will have access to the assigned SLA Policy.

To grant users access to reports:

Access to reports must be manually applied through the User Access option on associated resource screens. A native administrator (the account used to log in to IBM Spectrum Protect Plus for the first time) or a user with Administrator privileges can assign the necessary resources.

1. From the navigation menu, click **Report**.
2. From the Report pane, select a report, then click **User Access**. The Add User pane opens.
3. Click **Add** .
4. Select a user from the Account column, then select roles to apply to the user from the Roles column.
5. Click **Add**. The permissions are assigned to the user.

Upon next login, the user will have access to the assigned report.

RELATED TOPICS:

- Account on page **96**
- LDAP / SMTP on page **101**
- Start IBM Spectrum Protect Plus on page **31**

LDAP / SMTP

System Administrators can add LDAP and SMTP providers to IBM Spectrum Protect Plus through the LDAP / SMTP pane. Adding an LDAP provider enables LDAP users to be provisioned and access IBM Spectrum Protect Plus using LDAP usernames and passwords. Adding an SMTP server enables email communications to be sent from IBM Spectrum Protect Plus. Note that only one SMTP server can be associated with IBM Spectrum Protect Plus.

To register an LDAP provider:

1. From the navigation menu, expand **System**, then click **LDAP / SMTP**.
2. From the LDAP table, click **Add** . The LDAP Settings pane displays.
3. Populate the fields:

Host Address

The IP address or resolvable logical node 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 to establish a secure connection to the LDAP server.

Username

The Bind Distinguished Name used for authenticating the connection to the LDAP server. IBM Spectrum Protect Plus supports simple bind.

Password

The password 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 under the Base DN that match certain criteria. An example of a valid default user filter is **cn={0}**.

To enable authentication using the sAMAccountName Windows user naming attribute, set the User Filter to **samaccountname={0}**.

To enable authentication using an e-mail address associated with LDAP, set the User Filter to **mail={0}**.

Note that this entry also controls the type of user name that appears in 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. Specify the path where group records can be found if the group is at a different level than the user path.

4. Click **Save**. IBM Spectrum Protect Plus first confirms a network connection and then adds the provider to the database.

   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 register an SMTP provider:

1. From the navigation menu, expand **System**, then click **LDAP / SMTP**.
2. From the SMTP table, click **Add** . The SMTP Settings pane displays.
3. Populate the fields:

   Host Address

   A resolvable IP address or a resolvable path and machine name.

   Port

   The communications port of the provider you are adding. The typical default port is 25 for non SSL connections or 443 for SSL connections.

   Username

   The name used to access the provider.

   Password

   The password associated with the username.

   Timeout

   Set the email timeout value in milliseconds.

   From Address

   Set the address to be 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 first confirms a network connection and then adds the provider to the database.

   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.

RELATED TOPICS:

- Account on page **96**

Maintenance

The topics in the following section cover maintenance information including logging on to the virtual appliance and collecting logs for troubleshooting.

Maintenance Overview

In most cases, IBM Spectrum Protect Plus is installed on a virtual appliance. The virtual appliance contains the application and the Inventory.

System Administrators can perform maintenance tasks on the IBM Spectrum Protect Plus application. Note that 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. Maintenance tasks are performed in vSphere Client, through the IBM Spectrum Protect Plus command-line, or through a web-base management console.

Maintenance tasks include collecting logs, updating the application, and reviewing the configuration of the virtual appliance.

Note: Customers of IBM Spectrum Protect Plus are not encouraged to update any of the underlying components of IBM Spectrum Protect Plus themselves. Customers should not update the operating system, ZFS, or any other infrastructure component outside of the IBM Spectrum Protect Plus update packages. Infrastructure updates are managed by IBM's update facilities. The Administrator Console serves as the primary means for updatingIBM Spectrum Protect Plus features and underlying infrastructure components including the operating system and filesystem. ZFS update packages are also provided for vSnap standalone instances.

RELATED TOPICS:

- Manage the Administrative Console on page **106**
- Maintenance Job on page **112**
- Log On to the Virtual Appliance on page **113**
- Collect Logs for Troubleshooting on page **114**
- Backup and Restore the Catalog on page **115**
- Data Disk Expansion on page **116**

Manage 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.

To manage the Administrative Console:

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 **System** from the **Authentication Type** drop-down menu. Enter your password to access the Administration Console. The default password is **sppadLG235**.
3. Review the available options for the virtual appliance.

RELATED TOPICS:

- Update IBM Spectrum Protect Plus on page **108**
- Upload an SSL Certificate on page **107**
- Backup and Restore the Catalog on page **115**

Upload an SSL Certificate

To establish secure connections in IBM Spectrum Protect Plus, you must upload an SSL certificate through the web-based management console of the virtual machine where IBM Spectrum Protect Plus is deployed, for example, HTTPS or LDAP certificates. If uploading an LDAP SSL certificate, ensure an LDAP server is running and reachable by IBM Spectrum Protect Plus.

To upload a certificate:

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. See Related Topics.
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 **System** from the **Authentication Type** drop-down menu. Enter your password to access the Administration Console. The default password is **sppadLG235**.
5. Click **Manage your certificates**. Click **Browse**, browse for the certificate file on your computer, then click **Upload SSL Certificate**.
6. Reboot the virtual machine where the application is deployed.

RELATED TOPICS:

- Microsoft Knowledge Base Article 179380: How to Remove, Import, and Export Digital Certificates
- Firefox Knowledge Base Article: Advanced settings for accessibility, browsing, system defaults, network, updates, and encryption
- Google Chrome Knowledge Base Article: Advanced security settings

Update IBM Spectrum Protect Plus

The process of applying software patches is called software update or the update process. Use the software update process to upgrade your IBM Spectrum Protect Plus software with the latest features and enhancements. It is strongly recommended that you run the most current release of IBM Spectrum Protect Plus to take advantage of the latest functionality including operating system and application support. Software patches and updates are delivered as ISO files and installed through the Administrative Console.

The default, or on-board, vSnap server is updated along with the IBM Spectrum Protect Plus appliance. To update additional vSnap servers that are installed on either virtual or physical appliances, see the procedure below.

To update your VADP proxy to the latest version, you must first uninstall the current VADP proxy installation, then install the updated version. See the procedure below.

BEFORE YOU BEGIN:

- The ISO file updates the default, or on-board, vSnap Server and VADP functionality. You must update additional vSnap servers or VADP proxies separately.
- The ISO file and the vSnap server and VADP proxy update files are available from the Fix Central Online Web site. For information about available update files and how to obtain them from Fix Central, see technote 404421.
- A patch might not require updates for all IBM Spectrum Protect Plus components. The update files that are available in each patch might vary.
- Note that 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, perform a virtual machine snapshot rollback to return to a previous version of IBM Spectrum Protect Plus.
- Customers of IBM Spectrum Protect Plus are not encouraged to update any of the underlying components of IBM Spectrum Protect Plus themselves. Customers should not update the operating system or any other infrastructure component outside of the IBM Spectrum Protect Plus update packages. Infrastructure updates are managed by IBM's update facilities. The Administrator Console serves as the primary means for updating IBM Spectrum Protect Plus features and underlying infrastructure components including the operating system and filesystem.

To update your IBM Spectrum Protect Plus appliance:

Download the *spp_10.1.0_patch.iso* file from the Fix Central Online Web site to a directory on the computer that is running the browser for the Administrative Console. For information about the file and how to obtain it from Fix Central, see technote 404421.

1. From a machine with internet access, download the necessary update file. IBM Spectrum Protect Plus updates are delivered as ISO files.
2. 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.
3. In the login window, select **System** from the **Authentication Type** drop-down menu. Enter your password to access the Administration Console. The default password is **sppadLG235**.
4. Click **Manage updates**.
5. Click **Browse** to browse for the *spp_10.1.0_patch.iso* file to upload to the appliance, then click **Upload Update Image**. The update process begins once the update image has been uploaded to the appliance.
6. After the update completes, 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 may be stored in your browser's cache. Clear your browser's cache before logging in to an updated version of IBM Spectrum Protect Plus to ensure you are viewing the latest content changes.

To update your vSnap server:

The default, or on-board, vSnap server is updated along with the IBM Spectrum Protect Plus appliance. To update additional vSnap servers that are installed on either virtual or physical appliances, perform the following procedure.

Download the self-extracting archive *snap-dist-version.run* file from the FixCentral Online Web site to a temporary location on the vSnap server. For information about the file and how to obtain it from Fix Central, see technote 404421.

If a vSnap server update is not required for a patch, an update file is not provided with the patch.

1. Ensure there are no active jobs utilizing the vSnap server to be updated. Once associated jobs complete or are in an idle state, navigate to the Systems > Job Monitoring page in IBM Spectrum Protect Plus, then select **Hold Schedule** from the **Actions** list for each job.
2. Download the latest vSnap installation package, which is a self-extracting archive named vsnap-dist-<version>.run, to a temporary location on the vSnap server.
3. On the vSnap server, open a terminal.
4. From the directory where the file was downloaded, make the file executable through the following command: `chmod +x vsnap-dist-<version>.run`.
5. From the directory where the file was downloaded, execute the installer through the following command: `./vsnap-dist-<version>.run`.The vSnap packages are installed, plus all of its dependencies.

6. On the Job Monitoring page in IBM Spectrum Protect Plus, select **Release Schedule** from the **Actions** list for the jobs that are associated with the vSnap server.

To update a VADP proxy:

The default, or on-board, VADP functionality is updated along with the IBM Spectrum Protect Plus appliance. To update additional external VADP proxies, perform the following procedure.

Download the *vmdkbackup-version-installer.bin* file from the Fix Central Online Web site to a temporary location on the proxy server. For information about the file and how to obtain it from Fix Central, see technote 404421.

If a VADP proxy update is not required for a patch, an update file is not provided with the patch.

To update a VADP proxy to the latest version, you must uninstall the current VADP proxy first, then install the updated version.

1. Ensure there are no active jobs utilizing the VADP proxy to be updated. Once associated jobs complete or are in an idle state, click the Actions drop-down menu associated with the jobs on the Job Monitoring page, then select **Hold Schedule**.
2. Log in to the proxy machine as root, or as a user capable of running “sudo” commands. The initial root password is **sppDP758**.
3. Stop the VADP proxy service, *ecxvadp*, on the proxy machine through the following command: `systemctl stop ecxvadp`.
4. Uninstall the VADP proxy. On your IBM Spectrum Protect Plus host machine, run the following command (this example assumes the installation directory is /opt/IBM/SPP): `/opt/IBM/SPP/uninstall/uninstall_vmdkbackup`.
5. Copy the updated VADP Proxy installation program to a temporary location on the local proxy machine.
6. On the proxy machine, open a terminal.
7. From the directory where the file was downloaded, enter the following command to install the proxy server software:

   ```
   ./vmdkbackup-x.x-installer.bin
   ```

   The Setup wizard opens.

   Note: Alternatively you can run the installer using command line protocol by entering the following command from the directory where the file was downloaded: `./vmdkbackup-x.x-installer.bin --mode text`

8. Follow the steps in the Setup wizard to configure your proxy server and connect to the IBM Spectrum Protect Plus host.
   a. When prompted for the installation directory, select **/opt/IBM/SPP**.
   b. When prompted for the IBM Spectrum Protect Plus Discovery Server IP, enter the IP Address of the IBM Spectrum Protect Plus host.

9. Click **Finish** when the Setup wizard indicates it has completed.
10. On the Job Monitoring page in IBM Spectrum Protect Plus, select **Release Schedule** from the **Actions** list for the jobs that are utilizing the VADP proxy.

RELATED TOPICS:

- Install IBM Spectrum Protect Plus as a VMware Virtual Appliance on page **25**
- Install IBM Spectrum Protect Plus as a Hyper-V Virtual Appliance on page **28**
- Manage the Administrative Console on page **106**

Maintenance Job

The Maintenance job removes resources and associated objects created by IBM Spectrum Protect Plus when a job 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 associated with deleted jobs. By default, the Maintenance job runs once a day. The job cannot be deleted.

The Maintenance job only performs cleanup operations once a job in a pending state is deleted. All logs 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 deleting a pending job, all associated copy data, including recovery points, are deleted. The Maintenance job removes all VM Copies and Primary copies associated with deleted VMware Backup and Restore jobs. Once the Maintenance job completes, data that was copied as part of the backup job cannot be recovered. Any data related to the deleted job will not be recoverable.

RELATED TOPICS:

- Operations Overview on page **51**
- Maintenance Overview on page **105**

Log On to the Virtual Appliance

Log on to the IBM Spectrum Protect Plus virtual appliance through vSphere Client to access the command prompt.

To access the virtual appliance command prompt in a VMware environment:

1. In vSphere Client, select the virtual machine where IBM Spectrum Protect Plus is deployed.
2. In 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**.

To log off, enter **`exit`**.

To access the virtual appliance command prompt in a Hyper-V environment:

1. In Hyper-V Manager, select the virtual machine where IBM Spectrum Protect Plus is deployed.
2. Right-click the virtual machine, then select **Connect**.
3. Select **Login**, and enter your user name and password. The default user name is **administrator** and the default password is **sppadLG235**.

To log off, enter **`exit`**.

Collect Logs for Troubleshooting

For troubleshooting the IBM Spectrum Protect Plus application, IBM Spectrum Protect Plus can generate an archive of logs containing various files.

BEFORE YOU BEGIN:

- Contact Technical Support to determine if they need a log collection file for troubleshooting.

To collect logs for troubleshooting:

1. Click the **User** icon, then select **Download Logs**.
2. Select a location to save the zip file.

   Note: The following logs are added to the zip file and saved to your local machine: mongo, rabbitmq, and virgo.

NEXT STEPS:

- Contact Technical Support to inform them that you have created a log collection file for troubleshooting. Send the zipped log collection file to Technical Support.

RELATED TOPICS:

- Manage the Administrative Console on page **106**

Backup and Restore the Catalog

The Catalog Manager provides IBM Spectrum Protect Plus administrators with the ability to backup and restore the IBM Spectrum Protect Plus Catalog. The Catalog Manager is available through the Administrative Console, which is available at https://<HOSTNAME>:8090/, where <HOSTNAME> is the IP address of the virtual machine where IBM Spectrum Protect Plus is deployed.

BEFORE YOU BEGIN:

- Install IBM Spectrum Protect Plus. This creates a virtual machine containing the application. See Install IBM Spectrum Protect Plus as a VMware Virtual Appliance on page **25**.

To manage your IBM Spectrum Protect Plus catalog through the Catalog Manager:

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 **System** from the **Authentication Type** drop-down menu. Enter your password to access the Administration Console. The default password is **sppadLG235**.
3. Click **Get Started**. Click **Menu**, then select **Catalog Manager**.
4. Select **Backup Catalog** or **Restore Catalog**.

- **Backup Catalog**: In the **Directory** field, enter the backup destination on the IBM Spectrum Protect Plus host. Ensure the destination volume exists and that there is enough room on the destination volume for the Catalog backup. Click **Backup** to begin the Catalog backup.

  Backup Catalog considerations: IBM Spectrum Protect Plus will be stopped while the Catalog is being backed up. The IBM Spectrum Protect Plus user interface will not be accessible, and all running jobs will be aborted.

- **Restore Catalog**: From the list provided, determine the Restore Point associated with the Catalog Backup you want to recover. Click **Restore** to begin the Catalog restore.

  Restore Catalog considerations: IBM Spectrum Protect Plus will be stopped while the Catalog is being restore. The IBM Spectrum Protect Plus user interface will not be accessible, and all running jobs will be aborted. All IBM Spectrum Protect Plus snapshots created after the Catalog backup was run will be lost.

RELATED TOPICS:

- Manage the Administrative Console on page **106**

Data Disk Expansion

This document describes how to add new virtual disks (hard disks) on your IBM Spectrum Protect Plus virtual machine through vCenter. By default, when you deploy the IBM Spectrum Protect Plus virtual appliance you have the option to deploy all virtual disks to one datastore that you specify at the time of deployment. These instructions will guide you through adding a new disk within the virtual machine and to configure it as an LVM. You can then mount it as a new volume or attach this new disk to the existing volumes within the virtual appliance.

In order to run the commands below you need to SSH into the IBM Spectrum Protect Plus appliance's command prompt as the root account. The default initial password is "sppDP758" and you will be prompted to change the password at the first login.

Review the disk partitions using the `fdisk -l` command, then review the physical volumes and the volume groups on the IBM Spectrum Protect Plus virtual appliance using the `pvdisplay` and `vgdisplay` commands respectively.

Add a disk to the IBM Spectrum Protect Plus virtual machine:

1. From the vCenter client, edit the settings of the IBM Spectrum Protect Plus virtual machine.
2. On the Hardware tab, click **Add...**
3. Select **Create a new virtual disk**.
4. Select the required Disk Size. In the Location section, select either:

   Store with the virtual machine to use the current datastore, or

   Specify a datastore or datastore cluster, then click **Browse...** to select the new datstores where you want the virtual disk to reside.
5. Leave the default values in the Advanced Options tab.
6. Review and save your changes.
7. Click the **Edit Settings** option for the virtual machine to view the new hard disk.
8. Add the new SCSI device without rebooting the virtual machine. This can be performed by going back to the console of the IBM Spectrum Protect Plus virtual machine and running the following command: `echo "- - -" > /sys/class/scsi_host/host<#>/scan`, where # is the latest host number.

Add the storage capacity from the new disk to an existing IBM Spectrum Protect Plus volume:

This section will guide you through adding storage capacity from the new disk to an existing IBM Spectrum Protect Plus volume. For users that are simply adding an additional volume to their appliance, this section does not need to be completed. First, set up the filesystem for the new disk to be LVM type.

1. Follow the commands below on the console. The commands set up a partition for the new disk and set the partition to be of type Linux LVM. The output of fdisk shows you the same.

```
[root@localhost ~]# fdisk /dev/sdd
```



```
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): n (add a new partition)

Command action

e extended

p primary partition (1-4)
```

---

p [Selects the primary partition]

```
Partition number (1-4): 1
```

```
First cylinder (1-2610, default 1): (Leave blank)

Using default value 1
```

```
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610): (Leave
blank)

Using default value 2610
```

```
Command (m for help): t (change a partition's system id)

Selected partition 1
```

```
Hex code (type L to list codes): 8e

Changed system type of partition 1 to 8e (Linux LVM)
```



```
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. Review the changes to the disk through the `fdisk -1` command.
3. Review the current list of Physical Volumes (PV) through the `pvdisplay` command.
4. Create a new Physical Volume (PV) through the following command: `pvcreate /dev/sdd1`
5. You can view the newly created PV from /dev/sdd1 through the `pvdisplay` command.
6. Review the Volume Group (VG) through the `vgdisplay` command.
7. Add the new Physical Volume (PV) to the Volume Group (VG) to increase its space through the following command: `vgextend data_vg /dev/sdd1`
8. Through the `vgdisplay` command, you can see that after the Volume Group (VG) data_vg is extended, there is now free space available for logical volumes (or /data volume) to use.
9. Review the Logical Volume (LV) /data through the `lvdisplay` command. The usage of the /data volume displays.
10. Add space to the Logical Volume (LV) /data through the `lvextend` command by adding the additional space to the total volume capacity. 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, reduce the amount of space to add by 1 GB, then add it to the overall volume capacity. It should read 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.
```


11. After running the above, the size of the /data volume displays as the following:

```
[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
```


The data disks have quotas in place to ensure disks are not filled to capacity. When a data disk is expanded, set a new disk quota hard limit, which is generally 90% of the total capacity. Through the `edquota -u mongod` command, change the values under “blocks hard” to your desired quota.

RELATED TOPICS:

- Log On to the Virtual Appliance on page **113**
- Manage the Administrative Console on page **106**

Acronyms

A

AD

Active Directory

API

Application Programming Interface

B

B

Bytes

C

CBT

Changed Block Tracking

CIDR

Classless Inter-Domain Routing

CIFS

Common Internet File System

CPU

Central Processing Unit

CSV

Comma-Separated Values

CsvFS

Clustered Shared Volume File System

D

DHCP

Dynamic Host Configuration Protocol

DN

Distinguished Name

DNS

Domain Name Server

E

EULA

End User License Agreement

F

FCM

FlashCopy Manager

FQDN

Fully Qualified Domain Name

G

GB

Gigabytes

GUI

Graphical User Interface

H

HTTP

Hypertext Transfer Protocol

I

IP

Internet Protocol

IDE

Integrated Development Environment

iSCSI

Internet Small Computer System Interface

K

KB

Kilobytes

KDC

Key Distribution Center

L

LDAP

Lightweight Directory Access Protocol

LUN

Logical Unit Number

LVM

Logical Volume Manager

M

MB

Megabytes

N

NFS

Network File System

NMTUI

NetworkManager Text User Interface

NTFS

New Technology File System

NTLM

NT LAN Manager

NTP

Network Time Protocol

O

OSSV

Open Systems SnapVault

OS

Operating System

OVA

Open Virtual Appliance

OVF

Open Virtualization Format

P

PDF

Portable Document Format

R

RAID

Redundant Array of Independent Disks

RAM

Random Access Memory

RBAC

Role-based access control

RDBMS

Relational Database Management System

RDM

Raw Device Mapping

RDN

Relative Distinguished Name

ReFS

Resilient File System

REST

Representational State Transfer

S

SAN

Storage Area Network

SCSI

Small Computer System Interface

SFTP

Secure File Transfer Protocol

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SQL

Structured Query Language

SSD

Solid State Drive

SSH

Secure Shell

SSL

Secure Sockets Layer

SVC

SAN Volume Controller

SVM

Storage Virtual Machine

T

TB

Terabytes

U

UI

User Interface

URL

Uniform Resource Locator

UUID

Universally Unique Identifier

V

VADP

VMware vStorage API for Data Protection

VASA

vSphere API for Storage Awareness

VDDK

Virtual Disk Development Kit

VHDX

Hyper-V virtual hard disk

VM

Virtual Machine

VMCLI

VMware vSphere Power Command Line Interface

VMDK

Virtual Machine Disk

VMFS

Virtual Machine File System

VVOL

Virtual Volume

W

WinRM

Windows Remote Management

X

XFS

X File System

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.

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.

SoftLayer® is a registered trademark of SoftLayer, Inc., an IBM Company.

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.

Product Number: 5737-F11

Printed in USA