IBM Spectrum Protect for Virtual
Environments
Version 8.1.10

*Data Protection for VMware Installation
Guide*

IBM

**Note:**

Before you use this information and the product it supports, read the information in "Notices" on page 111.

# Contents

# About this publication

IBM Spectrum Protect for Virtual Environments provides off-host block-level incremental backup and file recovery and instant restore from a full-VM backup for Windows and Linux guest machines. Block level incremental backups are available when you use IBM Spectrum Protect for Virtual Environments with the IBM Spectrum® Protect data mover.

## Who should read this publication

This publication is intended for users and administrators who want to install and configure IBM Spectrum Protect for Virtual Environments.

Overview information, user tasks, backup and restore scenarios, command reference, and error messages are documented in the *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware User's Guide.*

## Publications

The IBM Spectrum Protect product family includes IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases, and several other storage management products from IBM®.

To view IBM product documentation, see IBM Knowledge Center.

# What's new in Version 8.1.10

IBM Spectrum Protect for Virtual Environments Version 8.1.10 introduces updates addressing defects and APARs.

For a list of new features and updates in this release and previous Version 8 releases, see Data Protection for VMware updates.

If changes were made in the documentation, they are indicated by a vertical bar (|) in the margin.

**viii** IBM Spectrum Protect for Virtual Environments: Data Protection for VMware Installation Guide

# Chapter 1. Installing and upgrading Data Protection for VMware

Installation of IBM Spectrum Protect for Virtual Environments includes planning, installation, and initial configuration.

## Installable components

Data Protection for VMware includes several components that you can install to protect your virtual environment.

The availability of components depends on the operating system environment. To determine which components are available in your environment, review the table.

On Windows and Linux, all install locations are to fixed locations. The Windows locations are listed in the table below. For Linux: Spectrum Protect for VE component is installed at `/opt/tivoli/tsm/tdpvmware`. The Linux Spectrum Protect backup-archive API and client are installed by the VE installer in their fixed locations: `/opt/tivoli/tsm/client/api` and `/opt/tivoli/tsm/client/ba`.

Each installation package presents you with an End User Licensing Agreement. If you do not accept the license agreement, the installation process stops.

| Table 1. Available Data Protection for VMware components by operating system | | |
|---|---|---|
| **Component** | **Linux®** | **Windows** |
| **IBM Spectrum Protect recovery agent**<br><br>This component provides virtual mount and instant restore capabilities.<br><br>Fixed installation location on Windows: `C:\Program Files\Tivoli\TSM\RecoveryAgent` | | √ |
| **Recovery agent command-line interface**<br><br>The command-line interface is used for mount operations.<br><br>Fixed installation location on Windows: `C:\Program Files\IBM\SpectrumProtect\Framework` | | √ |
| **Documents**<br><br>Documents include the readme and notices files. | √ | √ |
| **Data Protection for VMware enablement file**<br><br>This component enables IBM Spectrum Protect Data Protection for VMware to run the following backup types:<br><br>• Incremental-forever incremental backup<br>• Incremental-forever full backup<br><br>This component is required for application protection. If you offload backup workloads, this file must be installed on the vStorage Backup Server. | √ | √ |

| Table 1. Available Data Protection for VMware components by operating system (continued) | | |
|---|---|---|
| **Component** | **Linux®** | **Windows** |
| **Data Protection for VMware vSphere GUI**<br><br>This component is a graphical user interface (GUI) that accesses VM data on the VMware vCenter Server. The content of the GUI is available in these views:<br><br>• A web browser view. This view is accessed in a supported web browser by using the URL for the GUI web server host. For example:<br><br>   `https://guihost.mycompany.com:9081/TsmVMwareUI/`<br><br>• The IBM Spectrum Protect vSphere Client plug-in view. This view is accessed in the VMware vSphere Web Client. The panels in this view are uniquely designed to integrate within the vSphere web client, but data and commands for this view are obtained from the same GUI web server as the other views. The IBM Spectrum Protect vSphere Client plug-in provides a subset of the functions that are available in the web browser view and some additional functions. | √ | √ |
| **File restore GUI**<br><br>This component is a web-based GUI that enables you to restore files from a VMware virtual machine backup without administrator assistance. The GUI is installed automatically when the Data Protection for VMware GUI is installed. It is enabled through the configuration wizard. | √ | √ |
| **Data mover**<br><br>The IBM Spectrum Protect Data Protection for VMware data mover is the component that moves data for Data Protection for VMware. The data mover moves data from the virtual environment to an IBM Spectrum Protect backup server. When you install the data mover on a server, the server can be used as a vStorage backup server. You can install the data mover on the same system as Data Protection for VMware or on another server.<br><br>Fixed installation location on Windows: `C:\Program Files\Tivoli\TSM\baclient` | √ | √ |

On Windows, the JVM is installed at: `C:\Program Files\Common Files\Tivoli\TSM\jvmNNNNNN` where NNNNNN is the JVM version number (for example JVM80516). The web server is installed at `C:\IBM\SpectrumProtect\webserver`.

From Data Protection for VMware V8.1.8 and upwards, the location of Framework and DP for VMware components of the TSM4VE package can no longer be changed. The default location is `C:\Program Files\IBM\SpectrumProtect`.

• Framework - `C:\Program Files\IBM\SpectrumProtect\Framework`: FLR, Derby, vmcli, and tsmcli files.
• DP for VMware - `C:\Program Files\IBM\SpectrumProtect\DPVMware`: vmgui files.

1. Although the file restore interface component must be installed and enabled on a Windows system, you can use this interface to restore files on both Windows and Linux guest virtual machines.
2. When you install Data Protection for VMware, the data mover is included in the installation.

Data Protection for VMware offloads the backup workload from VMs to a vStorage backup server. To accomplish this task, the data mover must be installed on the vStorage Backup Server.

## Data Protection for VMware vSphere GUI

The Data Protection for VMware vSphere GUI (vSphere GUI) component is a graphical user interface that accesses VM data on the VMware vCenter Server.

### Overview

The Data Protection for VMware vSphere GUI is the primary interface from which to complete the following tasks:

- Initiate or schedule backups of your VMs to an IBM Spectrum Protect server.
- Initiate a full recovery of your VMs from an IBM Spectrum Protect server.
- Issue reports about the progress of your tasks, the most recent events that completed, backup status, and space usage. This information can help you troubleshoot errors that occurred in backup processing.

**Tip:** Information about how to complete tasks with the vSphere GUI is provided in the online help that is installed with the GUI. Click **Learn More** in any of the GUI windows to open the online help for task assistance.
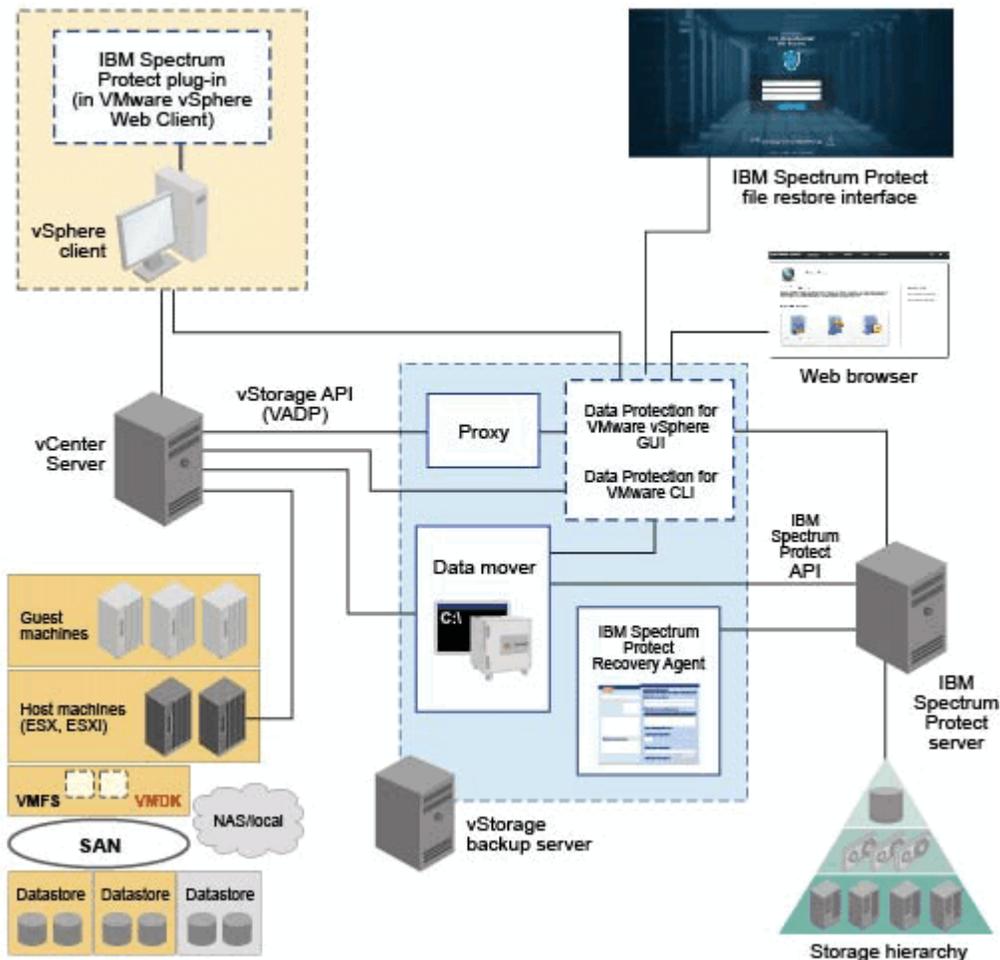


*Figure 1. Data Protection for VMware system components in a VMware vSphere user environment*

### Requirements

The Data Protection for VMware vSphere GUI can be installed on any system that meets the operating system prerequisites. The vSphere GUI resource requirements are minimal as it does not process I/O data transfers.

**Tip:** Installing the vSphere GUI on the vStorage Backup Server is the most common configuration.

The vSphere GUI must have network connectivity to the following systems:

- vStorage Backup Server
- IBM Spectrum Protect server
- vCenter Server

In addition, ports for the Derby database (default 1527) and GUI web server (default 9081) must be available.

### Configuration

You can register multiple vSphere GUIs to a single vCenter Server. This scenario reduces the number of datacenters (and their VM guest backups) that are managed by a single VMware vSphere GUI. A vCenter Server can then manage a subset of the total number of datacenters that are defined on the vCenter Server.

To update the managed datacenters, go to **Configuration** > **Edit Configuration**.

When you register multiple vSphere GUIs to a single vCenter Server, the following guidelines apply:

- Each datacenter can be managed by only one installed vSphere GUI.
- A unique VMCLI node name is required for each installed vSphere GUI.
- Using unique data mover node names for each installed vSphere GUI simplifies managing the nodes.

### Accessing the vSphere GUI

The vSphere GUI is accessed by the following methods:

- A stand-alone web browser GUI. This GUI is accessed through a URL bookmark to the GUI web server, for example:

```
https://hostname:port/TsmVMwareUI/
```

where:

- *hostname* is the name of the system where the Data Protection for VMware vSphere GUI is installed
- *port* is the port number where the vSphere GUI is accessible through. The default port number is9080. For secure ports, the default is 9081.
- A vSphere Web Client extension that connects to a GUI web server to access virtual machines in IBM storage (referred to as the data protection extension). The content is a subset of what is provided in the web browser GUI.

You can specify one or more access methods during installation.

**Windows** The default installation directory is `C:\IBM\SpectrumProtect\webserver`.

**Linux** The default installation directory is `/opt/tivoli/tsm/tdpvmware/common/webserver`.

## IBM Spectrum Protect recovery agent

Use the recovery agent service to mount any snapshot volume from the IBM Spectrum Protect server.

### Overview

You can use the iSCSI protocol to access a snapshot from a remote system.

If you need to view the snapshot locally with read-only access on the client system, use Data Protection for VMware V8.1.4 or earlier versions.

In addition, the recovery agent provides both the instant restore function and protection for in-guest applications. Instant restore enables the volume that is in use to remain available while the restore operation proceeds in the background. Application protection enables applications that are installed in a guest virtual machine, such as Microsoft Exchange Server and Microsoft SQL Server, to be available for backup and restore protection.

The recovery agent can complete the following tasks from a remote system:

• Gather information about the data that can be restored, for example:

   – Backed-up VMs.

   – Snapshots available for a backed-up virtual machine.

   – Partitions available in a specific snapshot.

For detailed information about commands, parameters, and return codes, see the command reference section in the *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware User's Guide*.

### Requirements

**Windows** On Windows systems, the recovery agent GUI and command-line interface are installed as part of a full installation of Data Protection for VMware or an advanced installation of the data mover.

### Accessing the recovery agent

**Windows** You can access the recovery agent from the **Start** menu: **Start** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect recovery agent**

## IBM Spectrum Protect vSphere Client plug-in

The IBM Spectrum Protect vSphere Client plug-in is a VMware vSphere Web Client extension that provides a view of the Data Protection for VMware vSphere GUI.

### Overview

The IBM Spectrum Protect vSphere Client plug-in provides a subset of the functions that are available in the browser view for the Data Protection for VMware vSphere GUI and some additional functions.

### Requirement

To install the IBM Spectrum Protect vSphere Client plug-in, you must select the following options when you run the IBM Spectrum Protect for Virtual Environments configuration wizard:

• On the **vCenter Settings** page of the configuration wizard, select **Update Registration** to register the plug-in with the associated vCenter.

• Enter the GUI host address, vCenter User and password.

   **Note:** The default domain is based on the local domain address, and may not be externally accessible. If external access is required, specify a GUI host address that can be resolved by DNS, or an IP address.

Upon completion of the wizard, the plug-in will be registered with the vCenter.

### Accessing the data protection plug-in
You can access the plug-in from the vSphere Web Client:

1. Log in to the vSphere Web Client using vCenter credentials. The data protection plugin-in is located under the main menu, **IBM Spectrum Protect**.

2. Selecting this menu item will take you to the main area of the IBM Spectrum Protect extension. The **Monitor** and **Configure** sections associated with particular items in the vCenter inventory will also have IBM Spectrum Protect for Virtual Environments functionality.

## Data Protection for VMware command-line interface

The Data Protection for VMware CLI is a full-function command-line interface that is installed with the Data Protection for VMware vSphere GUI.

### Overview

You can use the Data Protection for VMware CLI to complete the following tasks:

- Initiate or schedule backups of your VMs to an IBM Spectrum Protect server.
- Initiate a full recovery of your VMs, VM files, or VM Disks (VMDKs) from an IBM Spectrum Protect server.
- View configuration information about the backup database and environment.

Although the Data Protection for VMware vSphere GUI is the primary task interface, the Data Protection for VMware CLI provides a useful secondary interface.

For example, the Data Protection for VMware CLI can be used to implement a scheduling mechanism that is different from the one that is implemented by the Data Protection for VMware vSphere GUI. Also, the Data Protection for VMware CLI is useful when you evaluate automation results with scripts.

### Accessing the Data Protection for VMware command-line interface

You can access the Data Protection for VMware CLI from a command line.

For detailed information about the available commands, see the command reference section in the *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware User's Guide*

## IBM Spectrum Protect file restore interface

You can restore individual files from a VMware virtual machine backup.

### Overview

The file restore interface is a web-based interface where you can restore individual files from a VM backup. The advantage of this interface is that file, software, and platform owners can restore their own files without prior knowledge of IBM Spectrum Protect backup and restore operations.

The file restore interface feature is installed when you select the option to protect your data in a vSphere environment. In the Data Protection for VMware configuration wizard, you must enable the file restore feature for the interface to be available.

### Accessing the IBM Spectrum Protect file restore interface

To access the file restore interface, open a web browser and enter the URL provided by your administrator. For example:

```
https://hostname:9081/FileRestoreUI
```

where *hostname* is the host name of the system where the Data Protection for VMware vSphere GUI is installed.

## Data mover feature

A data mover is a software component of Data Protection for VMware that moves data to and from the IBM Spectrum Protect server.

### Overview

In the typical VMware environment, the data mover is used to save virtual machine backups to a datacenter node.

When you install Data Protection for VMware, the data mover is included in the installation. The data mover is installed on the same system as the Data Protection for VMware vSphere GUI and other Data Protection for VMware components.

You can also install data movers on remote systems independently of the other Data Protection for VMware components to redistribute the backup workload among multiple systems.

Snapshot differential backup operations are not supported in the VMware environment. You cannot run snapshot differential backup operations of a file system that resides on a NetApp filer on a host where the Data Protection for VMware data mover is also installed.

**Setting up data movers**

For information about planning for, installing, and configuring data movers, review the following list:

| Action | Description |
| --- | --- |
| Determine the number of data movers that are required to protect your vSphere environment. | Multiple data mover nodes might be required to protect your vSphere environment. |
| | To determine the number of data mover nodes that are required, see technote 2007197. This technote also includes considerations for using virtual or physical machines for data mover nodes and for data mover locality. |
| Install Data Protection for VMware. | To install Data Protection for VMware, run the Data Protection for VMware installer and select **Typical Installation** for Windows operating systems or **Complete** for Linux operating systems. This installation option installs all Data Protection for VMware components, including the data mover. |
| | For information about how to run the Data Protection for VMware installer, see "Installing the Data Protection for VMware components" on page 18. |
| Define the data movers for your environment. | When the Data Protection for VMware installation wizard completes, the Data Protection for VMware vSphere GUI configuration wizard opens to enable you to set up communication with the IBM Spectrum Protect server. |
| | On the **Data Mover Nodes** page of the configuration wizard, define the information for the local data mover and any remote data movers that you will install on separate systems. |
| | If you install on a Windows operating system and select **Create Services** when you define the data mover, the configuration information for the data mover is saved in a options file in the following location: |
| | `C:\Program Files\Tivoli\TSM\baclient\` |
| | In addition, the services that are required by the data mover are configured. |
| | If you install the data mover on a Linux operating system, or install on a Windows operating system, but do not select **Create Services** during configuration, you must complete the steps in "Setting up data mover nodes with the vSphere plug-in GUI" on page 77 to create the options file and configure the required services. |

| Action | Description |
|---|---|
| Install and configure additional data movers on remote systems, if required. | To install a data mover on a remote system, run the Data Protection for VMware installer and take one of the following actions:<br><br>On Windows operating systems, select **Advanced Installation** > **Install the data mover feature only** in the configuration wizard.<br><br>On Linux operating systems, select **Custom** from the **Install Set** list in the configuration wizard. Ensure that **Data Protection for VMware data mover** is selected. This option is selected by default.<br><br>When the installation is complete, to set up data movers on remote systems, follow the instructions in "Setting up data mover nodes with the vSphere plug-in GUI" on page 77. |

## Planning to install Data Protection for VMware

Data Protection for VMware eliminates the impact of running backups on a VM by offloading backup workloads from a VMware ESXi-based host to a vStorage Backup server.

Data Protection for VMware works with the integrated data mover to complete incremental-forever full, and incremental-forever incremental backups of VMs. The data mover node "moves" the data to the IBM Spectrum Protect server for storage, and for VM image-level restore at a later time. Instant restore is available at the disk volume level and full VM level.

**Tip:** The data mover is a separately licensed component that contains its own user interfaces and documentation. Familiarity with this product and its documentation is necessary in order to adequately integrate a comprehensive plan for protecting your VMs with Data Protection for VMware. Data Protection for VMware for Windows 64-bit includes the data mover feature.

### Installation roadmap

The following table identifies the steps to complete a successful installation process.

| | Table 2. Installation tasks for new or existing Data Protection for VMware customers | |
|---|---|---|
| **Step** | **Task** | **Get started here** |
| 1 | Check system requirements. | Make sure the system on which Data Protection for VMware is to be installed meets the system requirements. |
| 2 | Check user permission requirements. | Avoid potential installation errors or delays by using the required user permission levels. |
| 3 | Check availability of required communication ports. | Prevent installation failure or delays by opening the required communication ports before you attempt to install Data Protection for VMware. |
| 4 | Install Data Protection for VMware:<br><br>• Installing Data Protection for VMware by using the installation wizard<br>• "Installing the Data Protection for VMware components in silent mode" on page 22<br><br>Upgrade Data Protection for VMware:<br><br>    Upgrade Data Protection for VMware | Each installation package presents you with a user licensing file (EULA). If you do not accept the file, the installation ends. |

| Table 2. Installation tasks for new or existing Data Protection for VMware customers (continued) | | |
|---|---|---|
| **Step** | **Task** | **Get started here** |
| 5 | "Configuring a new installation with the wizard on Windows" on page 35<br><br>If you are planning to upgrade Data Protection for VMware, depending on the components that are installed, more configuration tasks might be required.<br><br>See the configuration topics in the *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware User's Guide* for more details. | Use the configuration wizard for an initial configuration. Depending on the features that are installed, more configuration tasks might be required as described in this section. |

**Tip:** To assist with planning the quantity of proxy hosts that are required for your specific Data Protection for VMware backup environment, the following publication is available on the IBM Spectrum Protect Wiki: Step by Step Guide To vStorage Backup Server (Proxy) Sizing
This publication is available in the IBM Spectrum Protect for Virtual Environments product section.

## Installation scenarios

Before you install Data Protection for VMware, choose the scenario that best meets the needs of your business.

You can install Data Protection for VMware and the data mover by using the GUI or in silent mode:

- "Installing the Data Protection for VMware components by using the installation wizard" on page 19
- "Installing the Data Protection for VMware components in silent mode" on page 22

For a list of features and components that are available by platform, see "Installable components" on page 1.

| Table 3. Installation scenarios | | |
|---|---|---|
| **Scenario Number** | **Description** | **Tasks that you must complete** |
| 1 | Use this scenario for a new installation where you want to install Data Protection for VMware and the data mover on the same system. | **Windows** You can use the Suite Installer in GUI or silent mode.<br>**Linux** You can use InstallAnywhere in GUI or silent mode. |
| 2 | Use this scenario when you want to install a data mover (mount proxy), recovery agent, and required support packages on this system.. | **Windows** You can complete an advanced installation using the Suite Installer.<br>**Linux** The data mover feature is now installed with Data Protection for VMware. |

## System requirements

To implement Data Protection for VMware components, your system must meet appropriate system requirements.

### Software requirements

Details of the software and operating system requirements can change over time. For current software requirements, see technote 1505139.

**Hardware requirements**

Hardware requirements vary and depend on the following items:

- Number of protected servers
- Number of protected volumes
- Data set sizes
- LAN and SAN connectivity

    **Note:** The recovery agent component does not support operations in a LAN-free environment.

The following table describes the hardware requirements that are needed to install Data Protection for VMware.

| Table 4. Hardware requirements for Data Protection for VMware. | | |
|---|---|---|
| **Component** | **Minimal requirement** | **Preferred** |
| System | IntelPentium D Dual Core processor or compatible | Not applicable |
| Memory | 4 GB RAM, 4 GB virtual address space | Not applicable |
| Available hard disk | 4.4 GB | 9.0 GB |
| Network | 1 GbE | 10 GbE |

**Note:** Depending on the number of parallel processes, back ups of virtual machines takes a significant amount of memory.

The memory requirements can be expanded regarding the **dsmc backup vm** command and can be calculated by the following formula:

**Required memory = (DiskSize / MBLKSize) * ReadBufferSize * VMMAXPARALLEL**

where:

- **DiskSize** is the size of the guest disk currently being processed;
- **MBLKSize** is the size of a megablock. It is equal to 128 MB for disks under 2 TB, and equal to 1 GB for disks larger than 2 TB;
- **ReadBufferSize** is the size of the IBM Spectrum Protect internal buffer that is used to accommodate the MBLK information. The buffer size is equal to 256 KB;
- **VMMAXPARALLEL** is the maximum number of virtual machines that can be backed up at any one time by a single backup operation process.

For example, to back up 10 guests, each with 40 GB disks and run with VMMAXPARALLEL 2 in a single backup operation process, would require:

- **DiskSize** = 40 GB = 41943040 KB;
- **MBLKSize** = 128 MB = 131072 KB;
- **ReadBufferSize** = 256 KB;
- **VMMAXPARALLEL** = 2.

**Required memory = (41943040 / 131072) * 256kB * 2 = 163840KB = 160MB**.

**Note:** To back up the same number of guests with 'VMMAXPARALLEL 2' in five parallel backup operation processes, would require (at the maximum) five times more memory than the previous example, or 800 MB.

**Restriction:** The following restrictions apply to VMware VMDKs that are involved in a backup operation:

- For incremental-forever incremental backup mode, each individual VMDK involved in a backup operation cannot exceed 8 TB. If a VMDK exceeds 8 TB, the backup operation fails. To increase the size

of the VMDK to be larger than the default 2 TB, specify the maximum size with the `vmmaxvirtualdisks` option. For more information, search for `vmmaxvirtualdisks` on the IBM Knowledge Center.

To prevent a failure during either backup mode, you can skip processing the VMDK by specifying `vmskipmaxvirtualdisks yes` in the data mover options file. For more information, see Vmskipmaxvirtualdisks.

### File restore prerequisites
Before you restore files with the IBM Spectrum Protect Data Protection for VMware file restore interface, ensure that your environment meets the minimum prerequisites.

To enable the file restore feature, Data Protection for VMware must be installed on a Windows system.

### VMware virtual machine prerequisites

The following prerequisites apply to the VMware virtual machine that contains the files to be restored:

- **Windows** | **Linux** VMware Tools must be installed on the virtual machine.
- **Windows** | **Linux** The virtual machine must be running during the file restore operation.
- **Windows** The data mover system must either belong to the same windows domain or be in a domain with a trust relationship with the virtual machine that contains the files to be restored.
- **Windows** When a virtual machine is deleted from a Windows domain and then restored later, the virtual machine must rejoin the domain to ensure the domain trust relationship. Do not attempt a file restore from the virtual machine until the domain trust relationship is restored.
- **Windows** If the user does not own the file to be restored, the Microsoft Windows `Restore Files and Directories` privilege must be assigned to the user for that virtual machine.
- For further information on Microsoft Windows domain account prerequisites required to use the Data Protection for VMware file restore interface, see technote 1998066.
- **Linux** Local user authentication is required for the virtual machine. Authentication is not available through Windows domain, Lightweight Directory Access Protocol (LDAP), Kerberos, or other network authentication methods.
- **Linux** On a Red Hat Enterprise Linux 6 operating system, the `ChallengeResponseAuthentication` option in the sshd daemon configuration file (`/etc/ssh/sshd_config`) must specify YES or be commented out. For example, either of the following statements are valid:

```
ChallengeResponseAuthentication yes
```

```
#ChallengeResponseAuthentication no
```

Restart the sshd daemon after you modify this option.

### Data mover prerequisites

The data mover system represents a specific data mover that "moves data" from one system to another.

**Windows** The data mover system must belong to the same Windows domain as the virtual machine that contains the files to be restored.

### Mount proxy prerequisites

The mount proxy system represents the Linux or Windows proxy system that accesses the mounted virtual machine disks through an iSCSI connection. This system enables the file systems on the mounted virtual machine disks to be accessible as restore points to the file restore interface.

**Linux** Linux operating systems provide a daemon that activates Logical Volume Manager (LVM) volume groups as these groups become available to the system. Set this daemon on the Linux mount

proxy system so that LVM volume groups are not activated as they become available to the system. For detailed information about how to set this daemon, see the appropriate Linux documentation.

**Windows** | **Linux** The Windows mount proxy system and Linux mount proxy system must be on the same subnet.

**Microsoft Windows domain account prerequisites**

The following prerequisites apply to Windows domain accounts. The first requirement is to establish a Windows domain user account with local administrative authority over all VMs:

- To perform the necessary tasks to enable file recovery to a virtual machine guest, you need a user account that belongs to a Windows domain and is a local administrator on the mount proxy system . An administrator with this account enters the account credentials in the Data Protection for VMware vSphere GUI configuration wizard or notebook to enable the environment for file restore operations.
- To create a user account with sufficient privileges to use the file restore interface, you can use the Windows Group Policy object to centrally manage a single domain user, allow it to access multiple machines with local administrator credentials, and optionally restrict undesirable actions.

The following steps illustrate how this user account can be created. Complete these steps on a domain controller by using the Active Directory Users and Computers MMC snap-in:

1. Select **Action->New->Groups** and create a new security group named **FR Admins**. The group scope should be set to `Global`.
2. Create a new domain user account with the user name `fradmin1` and add it to the **FR Admins** security group. You can also add other domain user accounts to the group.
3. To provide more control over the set of computers that `fradmin1` can access, create a new organizational unit
4. From the domain object, select **New->Organizational Unit**, name it as `FR Computers`
5. Populate the `FR Computers` organizational unit with a number of machines. .

Complete the following steps on the domain controller from the Group Policy MMC snap-in:

1. Create a new Group Policy object named `FR Admin GPO`, which will add the administrators in the **FR Admins** group to the local administrator group of the computers associated with the organizational unit to which the Group Policy object is applied.
2. In the Group Policy object, add the account to both the local administrator group and optionally to remote desktop users.
3. Select the `FR Computers` organizational unit and add the newly created Group Policy object.

   **Note:** The Group Policy object could have been associated with the domain itself, but then `fradmin1` would be in the local administrator group of all computers in the domain. Using an explicit organization unit provides additional control.
4. Optionally: use Group Policy Management to restrict undesirable actions on the local machine such as `Deny log on locally` and `Deny log on through Terminal Services`.
5. On the File Restore page of the Data Protection for VMware vSphere GUI configuration wizard or notebook, update the settings to use the `domain\fradmin1` account that was created in the steps above.
6. Restart the mount proxy client access daemon (CAD) service.

When you have set up an account with suitable privileges:

- **Windows** Enter your credentials in the Data Protection for VMware vSphere GUI configuration wizard or notebook to enable the environment for file restore operations.
- **Windows** A file owner accesses the remote virtual machine (that contains the files to be restored) with Windows domain user credentials. These credentials are entered in the file restore interface during login. Domain user credentials verify that the file owner has permission to log in to the remote virtual

machine and restore files into the remote virtual machine. These credentials do not require any special permissions.

- **Windows** If a file owner uses a Windows domain user account that limits access to specific computers (instead of access to all computers within the domain), ensure that the mount proxy system is included in the list of computers that are accessible to this domain user account. Otherwise, the file owner is unable to log in to the file restore interface.

**Tape media prerequisites**

File restore from tape media is not supported. File restore from disk storage is the preferred method.

**Required installation permissions**
Before you begin installation, ensure that your user ID contains the required permission level.

**About this task**

| Table 5. Users permissions required to install and configure Data Protection for VMware | |
|---|---|
| **System** | **Required permission** |
| Windows | Administrator |
| Linux | Root |
| vCenter Server | Administrator privileges<br><br>The vCenter Server role requires the following privileges: **Extension** > **Register extension, Unregister extension, Update extension** This new role must be applied to the vCenter object in the VMware vCenter Server hierarchy for the user ID that is specified during installation. |
| IBM Spectrum Protect server<br><br>**Restriction:** The server must be started. | Administrative access<br><br>(**System** or **Unrestricted Policy Domain** privilege) |

**Required communication ports**
View a list of communication ports that are required to be open in the firewall when you install Data Protection for VMware.

The ports that are identified in the table reflect a typical installation. A typical installation consists of the following components on the same Windows system:

- Data Protection for VMware GUI server
- vStorage backup server (data mover)
- Windows mount proxy
- IBM Spectrum Protect file restore interface

If a non-typical installation is used, more ports might be required.

**Restriction:** The Windows mount proxy and Linux mount proxy must be on the same subnet.

| Table 6. Required communication ports. This table identifies the ports that are accessed by Data Protection for VMware. | | |
|---|---|---|
| **TCP Port** | **Initiator: Out-Bound (From Host)** | **Target: In-Bound (To Host)** |
| 443 | vStorage Backup Server | vCenter Server (secure HTTP) |

| TCP Port | Initiator: Out-Bound (From Host) | Target: In-Bound (To Host) |
|---|---|---|
| 443 | Data Protection for VMware vSphere GUI Server | vCenter Server |
| 443<br><br>This setting is required only when the data mover is a Linux system. | Windows mount proxy | vCenter Server |
| 443 | vStorage Backup Server | Platform Services Controller |
| 443 | Data Protection for VMware vSphere GUI Server | Platform Services Controller |
| 443 | Windows mount proxy | Platform Services Controller |
| 902<br><br>443 | vCenter Server | ESXi hosts |
| 902<br><br>443 | vStorage Backup Server (proxy) | ESXi hosts (all protected hosts) |
| 1500<br>(**tcpport**) | vStorage Backup Server (proxy) | IBM Spectrum Protect server |
| 1500<br>(**tcpadminport**) | Data Protection for VMware vSphere GUI Server<br><br>• 1500 (**tcpadminport**) is non-SSL communication<br>• For SSL communication, **tcpadminport** is the only port that supports SSL communication with the IBM Spectrum Protect server. The correct port number to use for the SSL protocol is typically the value that is specified by the **ssltcpadminport** option in the IBM Spectrum Protect server dsmserv.opt file. However, if **adminonclient no** is specified in the dsmserv.opt file, then the correct port number to use for the SSL protocol is the value that is specified by the **ssltcpadminport** option. The **ssltcpadminport** option does not have a default value. Therefore, the value must be specified by the user. | IBM Spectrum Protect server |
| 1527<br>Internal Derby database | | |

*Table 6. Required communication ports.* This table identifies the ports that are accessed by Data Protection for VMware. *(continued)*

| TCP Port | Initiator: Out-Bound (From Host) | Target: In-Bound (To Host) |
|---|---|---|
| 1501<br><br>1581<br><br>(**httpport**) | IBM Spectrum Protect server | vStorage Backup Server<br>• Data mover scheduler<br>• Web client<br>• Client Acceptor Daemon |
| 1581<br><br>(**httpport**)<br><br>1582, 1583<br><br>(**webports**) | Data Protection for VMware vSphere GUI server | vStorage Backup Server |
| 9081<br><br>GUI web server (HTTPS protocol) | vSphere Client | Data Protection for VMware vSphere GUI Server (secure HTTPS port for access to vCenter through web browser) |
| 22<br><br>SSH default port for the recovery agent | Recovery agent | Data Protection for VMware Windows "mount" host<br>• SSH for Linux recovery agent |
| 3260 | Linux Data Protection for VMware file restore | Data Protection for VMware Windows "mount" host<br>• iSCSI |
| 3260<br><br>iSCSI default port for the recovery agent | Windows target with Dynamic disk for file restore | Data Protection for VMware Windows "mount" host<br>• iSCSI |
| 5985 | File restore GUI operations | Windows Remote Management |
| 135 | Windows mount proxy | VMware virtual machine that contains the files to be restored with the IBM Spectrum Protect file restore interface |

*Table 6. Required communication ports.* This table identifies the ports that are accessed by Data Protection for VMware. *(continued)*

**VMware vCenter Server user privilege requirements**
Certain VMware vCenter Server privileges are required to run Data Protection for VMware operations.

**vCenter Server privileges required to protect VMware datacenters with the web-browser view for the Data Protection for VMware vSphere GUI**

The vCenter Server user ID that signs on to the browser view for the Data Protection for VMware vSphere GUI must have sufficient VMware privileges to view content for a datacenter that is managed by the GUI.

For example, a VMware vSphere environment contains five datacenters. A user, "jenn", has sufficient privileges for only two of those datacenters. As a result, only those two datacenters where sufficient privileges exist are visible to "jenn" in the views. The other three datacenters (where "jenn" does not have privileges) are not visible to the user "jenn".

The VMware vCenter Server defines a set of privileges collectively as a role. A role is applied to an object for a specified user or group to create a privilege. From the VMware vSphere web client, you must create a role with a set of privileges. To create a vCenter Server role for backup and restore operations, use the VMware vSphere Client **Add a Role** function.

If you want to propagate the privileges to all datacenters within the vCenter, specify the vCenter Server and select the `propagate to children` check box. Otherwise, you can limit the permissions if you assign the role to the required datacenters only with the `propagate to children` check box selected. Enforcement for the browser GUI is at the datacenter level.

The following example shows how to control access to datacenters for two VMware user groups. First, create a role that contains all of the privileges defined in technote 7047438. The set of privileges in this example are identified by the role named "TDPVMwareManage". Group 1 requires access to manage virtual machines for the `Primary1_DC` and `Primary2_DC` datacenters. Group 2 requires access to manage virtual machines for the `Secondary1_DC` and `Secondary2_DC` datacenters.

For Group 1, assign the "TDPVMwareManage" role to the `Primary1_DC` and `Primary2_DC` datacenters. For Group 2, assign the "TDPVMwareManage" role to the `Secondary1_DC` and `Secondary2_DC` datacenters.

The users in each VMware user group can use the Data Protection for VMware GUI to manage virtual machines in their respective datacenters only.

**Tip:** When you create a role, consider adding extra privileges to the role that you might need later to complete other tasks on objects.

**vCenter Server privileges required to use the data mover**

The IBM Spectrum Protect data mover that is installed on the vStorage Backup server (the data mover node) requires the VMCUser and VMCPw options. The VMCUser option specifies the user ID of the vCenter or ESX server that you want to back up, restore, or query. The required privileges that are assigned to this user ID (VMCUser) ensure that the client can run operations on the virtual machine and the VMware environment. This user ID must have the VMware privileges that are described in the above technote.

To create a vCenter Server role for backup and restore operations, use the VMware vSphere Client **Add a Role** function. You must select the `propagate to children` option when you add privileges for this user ID (VMCUser). In addition, consider adding other privileges to this role for tasks other than backup and restore. For the VMCUser option, enforcement is at the top-level object.

**vCenter Server privileges required to protect VMware datacenters with the IBM Spectrum Protect vSphere Client plug-in view for the Data Protection for VMware vSphere GUI**

The IBM Spectrum Protect vSphere Client plug-in requires a set of privileges that are separate from the privileges that are required to sign in to the GUI.

During the installation the following custom privileges are created for the IBM Spectrum Protect vSphere Client plug-in:

- **Datacenter** > **IBM Data Protection**
- **Global** > **Configure IBM Data Protection**

Custom privileges that are required for the IBM Spectrum Protect vSphere Client plug-in are registered as a separate extension. The privileges extension key is `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

These privileges allow the VMware administrator to enable and disable access to IBM Spectrum Protect vSphere Client plug-in content. Only users with these custom privileges on the required VMware object can access the IBM Spectrum Protect vSphere Client plug-in content. One IBM Spectrum Protect vSphere Client plug-in is registered for each vCenter Server and is shared by all GUI hosts that are configured to support the vCenter Server.

From the VMware vSphere web client, you must create a role for users who can complete data protection functions for virtual machines by using the IBM Spectrum Protect vSphere Client plug-in. For this role, in

addition to the standard virtual machine administrator role privileges required by the web client, you must specify the **Datacenter** > **IBM Data Protection** privilege. For each datacenter, assign this role for each user or user group where you want to grant permission for the user to manage virtual machines.

The **Global** > **IBM Data Protection** privilege is required for the user at the vCenter level. This privilege allows the user to manage, edit, or clear the connection between the vCenter Server and the Data Protection for VMware vSphere GUI web server. Assign this privilege to administrators that are familiar with the Data Protection for VMware vSphere GUI that protects their respective vCenter Server. Manage your IBM Spectrum Protect vSphere Client plug-in connections on the extension **Connections** page.

The following example shows how to control access to datacenters for two user groups. Group 1 requires access to manage virtual machines for the `NewYork _DC` and `Boston_DC` datacenters. Group 2 requires access to manage virtual machines for the `LosAngeles_DC` and `SanFranciso_DC` datacenters.

From the VMware vSphere client, create for example the "IBMDataProtectManage" role, assign the standard virtual machine administrator role privileges and also the **Datacenter** > **IBM Data Protection** privilege.

For Group 1, assign the "IBMDataProtectManage" role to the `NewYork _DC` and `Boston_DC` datacenters. For Group 2, assign the "IBMDataProtectManage" role to the `LosAngeles_DC` and `SanFranciso_DC` datacenters.

The users in each group can use the IBM Spectrum Protect vSphere Client plug-in in the vSphere web client to manage virtual machines in their respective datacenters only.

**Issues related to insufficient permissions**

When the web browser user does not have sufficient permissions for any datacenter, access to the view is blocked. Instead, the error message GVM2013E is issued to advise that the user is not authorized to access any managed datacenters due to insufficient permissions. Other new messages are also available that inform users of issues that result from insufficient permissions. To resolve any permissions-related issues, make sure that the user role is set up as described in the previous sections. The user role must have all privileges that are identified in the Required privileges vCenter Server user ID and data mover table, and these privileges must be applied at the datacenter level with the `propagate to children` check box.

When the IBM Spectrum Protect vSphere Client plug-in user does not have sufficient permissions for a datacenter, the data protection functions for that datacenter and its content are made unavailable in the extension.

When the IBM Spectrum Protect user ID (specified by the `VMCUser` option) contains insufficient permissions for a backup and restore operation, the following message is shown:

```
ANS9365E VMware vStorage API error.
"Permission to perform this operation was denied."
```

When the IBM Spectrum Protect user ID contains insufficient permissions to view a machine, the following messages are shown:

```
Backup VM command started.  Total number of virtual machines to process: 1
ANS4155E Virtual Machine 'tango' could not be found on VMware server.
ANS4148E Full VM backup of Virtual Machine 'foxtrot' failed with RC 4390
```

For further information on the use of privileges, see the note on **vCenter Server privileges required for the Data Protection for VMware vSphere GUI and data mover**.

To retrieve log information through the VMware Virtual Center Server for permission problems, complete these steps:

1. In **vCenter Server Settings**, select **Logging Options** and set "**vCenter Logging** to **Trivia (Trivia)**.
2. Re-create the permission error.
3. Reset **vCenter Logging** to its previous value prevent recording excessive log information.

4. In **System Logs**, look for the most current vCenter Server log (`vpxd-wxyz.log`) and search for the string `NoPermission`. For example:

```
[2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
Throw: vim.fault.NoPermission
```

This log message indicates that the user ID did not contain sufficient permissions to create a snapshot (`createSnapshot`).

# Installing the Data Protection for VMware components

You can install all or some of the components that are available in the Data Protection for VMware package for your operating system.

**About this task**

Using the Data Protection for VMware installer, you can install the following components:

- IBM Spectrum Protect recovery agent
- <span style="background:#b5006e;color:white"> Windows </span>Recovery agent command-line interface
- <span style="background:#b5006e;color:white"> Windows </span>Documentation (readme file and notices file)
- Data Protection for VMware enablement file
- Data Protection for VMware vSphere GUI
- Data mover feature, which includes the following items:
  - Data mover GUI
  - Data mover web client
  - Client API (64-bit) runtime files
  - Administrative client command line
  - VMware vStorage API runtime files

You can choose a full installation or use the Advanced Installation option when you want to install a data mover (mount proxy), recovery agent, and required support packages.

**Tip:** You can create multiple data movers on the same system as the Data Protection for VMware software, or you can create data movers on remote systems. This configuration increases the resources available for use by Data Protection for VMware. The systems with the data mover installed are called vStorage backup servers.

## Obtaining the Data Protection for VMware installation package

You can obtain the Data Protection for VMware installation package from an IBM download site such as IBM Passport Advantage®.

**Before you begin**

<span style="background:#b5006e;color:white"> Linux </span>

If you plan to download the files, set the system user limit for maximum file size to unlimited to ensure that the files can be downloaded correctly:

1. To query the maximum file size value, issue the following command:

```
ulimit -Hf
```

2. If the system user limit for maximum file size is not set to unlimited, change it to unlimited by following the instructions in the documentation for your operating system.

**Procedure**

1. Download the appropriate package file from one of the following websites:

   - For a first-time installation or a new release go to Passport Advantage at: http://www.ibm.com/software/lotus/passportadvantage/. Passport Advantage is the only site that you can download a licensed package file from.
   - For the latest information, updates, and maintenance fixes, go to the IBM Spectrum Protect support site: http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.

2. If you downloaded the package from an IBM download site, complete the following steps:

   a. Download the package file to the directory of your choice. The path must contain no more than 40 characters. Be sure to extract the installation files to an empty directory. Do not extract to a directory that contains previously extracted files, or any other files.

   b. **Linux** Ensure that executable permission is set for the package. If necessary, change the file permissions by issuing the following command:

   ```
   chmod a+x package_name.bin
   ```

   c. **Linux** Extract the package by issuing the following command:

   ```
   ./package_name.bin
   ```

   where *package_name* is the name of the downloaded file.

   d. **Windows** Extract the package by double-clicking the *package_name*, where *package_name* is the name of the downloaded file.

## Installing the Data Protection for VMware components by using the installation wizard

You can install the Data Protection for VMware components by using the installation wizard.

**About this task**

**Windows** You can use the Suite Installer to install both Data Protection for VMware and the data mover.

**Linux** You can use the stand-alone installer to install both Data Protection for VMware and the data mover.

**Installing the Data Protection for VMware components on Windows systems**
Install Data Protection for VMware components and features by using the installation wizard.

**Before you begin**

Before you install the Data Protection for VMware components, ensure that you meet the following requirements:

- A user ID with administrator privilege access.
- Network connectivity to a VMware vCenter Server 6.x (or later) with administrator privilege access.
- Network connectivity to an IBM Spectrum Protect server with administrator access (**System** or **Unrestricted Policy Domain** privilege). This server must be available and running.
- Ensure that you reviewed the following requirements:
  - "System requirements" on page 9
  - "Required installation permissions" on page 13
  - "Required communication ports" on page 13

Before you install Data Protection for VMware, you must be aware of the following options:

**Installation Type**

> **Typical Installation**
>> With typical installations, all of the Data Protection for VMware components and features are installed.

> **Advanced Installation**
>> The Advanced Installation panel provides the option to install an individual data mover. The process will install a data mover (mount proxy), recovery agent, and required support packages on the system. Use this install option to add individual data movers. This option also installs application protection agents to enable recovery of individual databases. After installation, you can use the IBM Spectrum Protect GUI to configure the data mover and services via a VMware vSphere plugin.

**About this task**

You can use the Suite Installer to install Data Protection for VMware. The `spinstall.exe` file for the Suite Installer is located at the root of the installation package.

For a list of components and features that you can install, see "Installable components" on page 1.

**Procedure**

To install Data Protection for VMware, complete the following steps from the location of the `spinstall.exe` file for the component that you chose to install:

1. Double-click the `spinstall.exe` file.
2. Follow the wizard instructions to install the selected components.

**What to do next**

To access the Data Protection for VMware vSphere GUI, see the following:

- "Accessing the Data Protection for VMware vSphere GUI" on page 25

The configuration wizard is automatically displayed the first time that you start the GUI.

**Installing Data Protection for VMware on Linux systems**
Install Data Protection for VMware on Linux systems by using the InstallAnywhere mode.

**Before you begin**

Before you install Data Protection for VMware, ensure that you meet the following requirements:

- Ensure that the user ID has the required permission level and that the required communication ports are open before you proceed.
- The installation process creates user `tdpvmware`. You must issue all **vmcli** commands as user `tdpvmware`, and with root user ID.
- X Window Server is required when you install in console mode.
- Ensure that you reviewed the following requirements:

  - "System requirements" on page 9
  - "Required installation permissions" on page 13
  - "Required communication ports" on page 13

**Procedure**

To install Data Protection for VMware, complete the following steps:

1. From the root of the installation folder, change directories to `CD/Linux/DataProtectionForVMware`.
2. From a command line, enter the following command:

```
./install-Linux.bin
```

**Results**

If you receive any warnings or errors, check the log files for more information. See "Log file activity" on page 72.

If you are unable to install Data Protection for VMware because of a failure, see the "Manually removing Data Protection for VMware" procedure in "Uninstalling Data Protection for VMware on a Linux system" on page 31.

**Performing a clean installation of Data Protection for VMware on Linux**
If a Linux installation is interrupted, you can usually restart it. However, if the installation fails to restart, a clean installation is required.

**About this task**
Before starting a clean installation, ensure that product is removed. Perform following steps to ensure a clean environment:

**Procedure**

1. If the Data Protection for VMware vSphere GUI is installed, complete these tasks:
   a) Stop the Data Protection for VMware command-line interface by issuing this command:
      `/etc/init.d/vmcli stop`
   b) Stop the Data Protection for VMware GUI Web Server by issuing this command:
      `/etc/init.d/webserver stop`
   c) Remove the `.rpm` package by issuing this command:
      `rpm -e TIVsm-TDPVMwarePlugin`
2. Remove the Deployment Engine product entries:
   a) Issue the following command to list all Deployment Engine entries:
      `/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
   b) Issue the following command to remove all Deployment Engine entries:
      `/usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>`
   c) Remove the `/var/ibm/common` directory.
   d) Remove the `/usr/ibm/common` directory.
   e) Clean up the `/tmp` directory by removing the `acu_de.log` file, if it exists.
   f) Remove the `/tmp` directory that contains the ID of the user that installed the Deployment Engine.
   g) Remove all Deployment Engine entries from the `/etc/inittab` system file. The entries are delimited by `#Begin AC Solution Install block` and `#End AC Solution Install block`. Remove all text between those delimiters, and remove the delimiting text itself.
   h) Remove all Deployment Engine references from the `/etc/services` system file.
3. Remove all Data Protection for VMware files from the failed installation:
   a) Remove files in the `<USER_INSTALL_DIR>`, which is the path where the failed installation was attempted. For example: `/opt/tivoli/tsm/TDPVMware/`
   b) Remove any desktop shortcuts.
4. Back up the global registry file (`/var/.com.zerog.registry.xml`). After backing up this file, remove all tags that reference Data Protection for VMware.
5. Remove log files under root that contain the TDPVMware string.
   For example:
   `IA-TDPVMware-00.log` or `IA-TDPVMware_Uninstall-00.log`.
6. Remove the user that ran the Data Protection for VMware command-line interface.
   a) Issue the following command:

```
userdel -r tdpvmware
```

b) Issue the following command:

```
groupdel tdpvmware
```

**Tip:** In some versions of Linux, the **userdel** command also removes the group when no other associated user exists. As a result, ignore any command-related fail message.

**Results**
After you complete these steps, start the clean installation.

## Installing the Data Protection for VMware components in silent mode

You can install Data Protection for VMware in the background. During this silent installation, no messages are displayed.

**About this task**

**Windows** You can use the Suite Installer to install both Data Protection for VMware and the data mover.

**Linux** You can use the stand-alone installer to install both Data Protection for VMware and the data mover.

**Installing Data Protection for VMware on Windows systems in silent mode**
Install all Data Protection for VMware components and the data mover feature by using the Suite Installer in silent mode.

**Before you begin**
Before you install Data Protection for VMware and the data mover feature, ensure that your system meets the requirements in the following sections:

- "System requirements" on page 9
- "Required installation permissions" on page 13
- "Required communication ports" on page 13

**About this task**

**Restriction:** On Windows, some default install locations are fixed. To locate the installation directories for the components, see the section "Installable components" on page 1.

**Procedure**

To install Data Protection for VMware, complete the following steps:

1. From a command prompt, issue the following command:

```
cd extract_folder\TSMVMWARE_WIN
```

2. Enter the following command:

```
spinstall.exe /silent
```

The following message is displayed the first time that you mount a volume:

```
The Virtual Volume Driver is not yet registered. Recovery Agent can register
the driver now. During registration, a Microsoft Windows Logo warning may be displayed.
Accept this warning to allow the registration to complete.
Do you want to register the Virtual Volume Driver now?
```

To proceed, enter **Yes** to register the Virtual Volume Driver.

**Related tasks**

You can silently uninstall Data Protection for VMware on a Windows operating system.

**Installing Data Protection for VMware on Linux systems in silent mode**
You can customize which Data Protection for VMware features to silently install on a Linux operating system.

**Before you begin**

Before you install Data Protection for VMware, ensure that you meet the following requirements:

- Ensure that the user ID has the required permission level and that the required communication ports are open before you proceed.
- The installation process creates user `tdpvmware`. You must issue all **vmcli** commands as user `tdpvmware`, and with root user ID.
- X Window Server is required when you install in console mode.
- Ensure that you reviewed the following requirements:

  -
  -
  -

**About this task**

**Restriction:** On Linux, all install locations are fixed. To locate the installation directories for the components, see the section .

Data Protection for VMware provides the following silent installation features for Linux operating systems:

*Table 7. Data Protection for VMware silent installation features*

| Feature | Description | Installed by default? |
|---|---|---|
| Docs | Readme file | Yes |
| TDPVMwareDM | Installation of this feature includes the enablement file.<br><br>Enables IBM Spectrum Protect to run the following backup types:<br><br>• Periodic incremental VM backup<br><br>• Full VM incremental-forever backup<br><br>• Incremental-forever-incremental VM backup<br><br>If you offload backup workloads, this file must be installed on the vStorage Backup Server. | Yes |
| TDPVMwareGUI | Data Protection for VMware vSphere GUI.<br><br>**Note:** Also includes enablement file installation. | No |

**Procedure**

To install Data Protection for VMware, complete the following steps from the directory where you extracted the installation package:

1. Open the *path*`../Linux/DataProtectionForVMware/installer.properties` file and uncomment the following entry to accept the license (where *path* is the installation folder):

```
LICENSE_ACCEPTED=TRUE
```

2. Choose one of the following methods to install the Data Protection for VMware components:

- For a default installation, open the `CD/Linux/DataProtectionForVMware` folder and enter the following command:

  ```
  ./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true
  ```

- For a custom installation, complete the following steps:

  a. Edit the `installer.properties` file with the appropriate values:

     1) Specify **INSTALL_MODE=Custom**. Ensure the number sign (#) is removed from this statement.

     2) Specify the features to install with the **CHOSEN_INSTALL_FEATURE_LIST** option. For example, all features are installed with the following value:

        ```
        CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI
        ```

  b. From the `CD/Linux/DataProtectionForVMware` folder, issue the following command:

     ```
     ./install-Linux.bin -i silent -f installer.properties
     ```

## Taking the first steps after you install Data Protection for VMware

After you install Data Protection for VMware, prepare for the configuration. Using the configuration wizard is the preferred method of configuring Data Protection for VMware.

**Configuration worksheet**
Use this worksheet to record information that you need when you configure and administer Data Protection for VMware. The worksheet is intended to help you remember the values that you specified after the configuration.

| Table 8. Data Protection for VMware configuration worksheet | | |
|---|---|---|
| **Item** | **Your value** | **Notes** |
| **IBM Spectrum Protect server information** | | |
| IBM Spectrum Protect server address | | |
| IBM Spectrum Protect server port | | |
| IBM Spectrum Protect server admin ID/ password | | |
| IBM Spectrum Protect server admin port | | |
| **Node definition options** | | |
| Prefix to add to nodes | | |
| Policy domain to use when you register new nodes | | |
| vCenter node name/password | | |
| VMCLI node name/password | | |
| Datacenter node names/passwords<br><br>**Remember:** You can create multiple datacenter nodes. | | The data center node name consists of the specified prefix, followed by an underscore character, followed by the datacenter name.<br><br>For example:<br>*nodePrefix_datacenterName* |

| Table 8. Data Protection for VMware configuration worksheet (continued) | | |
|---|---|---|
| **Item** | **Your value** | **Notes** |
| Data mover node names/passwords on the vStorage backup server<br><br>**Remember:** You can create multiple data mover nodes. | | The data mover node consists of the datacenter node name, followed by an underscore character, followed by DM.<br><br>For example: *datacenterNodename*_DM |
| Data mover node names/passwords on remote servers<br><br>**Remember:** You can create multiple data mover nodes that are not on the vStorage backup server. | | |
| Mount proxy node<br><br>The mount proxy node is used when you restore data. | Windows:<br>Linux: | |

### Accessing the Data Protection for VMware vSphere GUI
Use the Data Protection for VMware vSphere GUI to back up, restore, and manage virtual machines in a VMware vCenter environment.

#### Before you begin

Before you can access the Data Protection for VMware vSphere GUI, during the installation, you must have selected the option to protect your data in a vSphere environment.

#### Procedure

- If you selected the **Enable access to the GUI by a web browser** option during the installation, you can access the Data Protection for VMware vSphere GUI from the browser:

  1. Open a web browser and enter the following URL:

     ```
     https://hostname:port/TsmVMwareUI
     ```

     where:

     - *hostname* is the name of the system where the Data Protection for VMware vSphere GUI is installed
     - *port* is the port number where the vSphere GUI is accessible through. The default port number is 9080. For secure ports, the default is 9081.

  2. Log in by using your vCenter user ID and password.

- If you did not select the **Enable access to the GUI by a web browser** option during the installation, you can start the Data Protection for VMware vSphere GUI by completing the following steps:

  1. Open the VMware vSphere Client and log on with the vCenter user ID and password.

  2. In the **Solutions and Applications** panel of the vSphere Client, click the Data Protection for VMware vSphere GUI icon.

## Upgrading Data Protection for VMware

You can upgrade Data Protection for VMware from a previous version of the software.

For compatibility with earlier versions, see technote 1993819.

**Upgrading from version 7.1.8:** If a message is shown during the upgrade process asking if you want to overwrite the existing `jextract` file, select **Yes to All**.

## Upgrading Data Protection for VMware

This procedure documents how to upgrade to Data Protection for VMware V8.1.10.

**Before you begin**

**Important:** This upgrade procedure applies to a system that does not have IBM Spectrum Protect Snapshot for VMware installed.

You must have administrator privileges to upgrade Data Protection for VMware.

Updates to the existing Data Protection for VMware vSphere GUI are processed in the following manner:

- Parameter files are backed up before the Data Protection for VMware vSphere GUI upgrade process begins.
- The same Derby Database Port and WebSphere® Application Server Default Base Port numbers are used.
- `Linux` The values in the profile (`vmcliprofile`) are used for the Data Protection for VMware command-line interface.

**Restriction:**

- `Windows` When IBM Spectrum Protect for Virtual Environments was installed to a non-default location, the upgrade process installs IBM Spectrum Protect for Virtual Environments V8.1.10 features to the default installation directory. You cannot upgrade to a non-default location. See the subtopics in "Installable components" on page 1 for the default installation directories for each feature.
- `Windows` `Linux` The upgrade process does not install new components.

  For example, if your previous version has only the recovery agent GUI installed, the upgrade procedure does not install the recovery agent command-line interface. In such a scenario, you must run the installation program again and then select the missing component to install.
- `Windows` `Linux` The v Center needs access to the domain name of the GUI host.

  The domain name of the GUI host used in upgrade must be reachable by the vCenter in order to upgrade the Data Protection vSphere plug-in. If the domain name is not reachable, then re-registering the plug-in will be necessary post-upgrade.
- `Linux` The recovery agent on Linux version must be the same version as the recovery agent on the Windows proxy. Therefore, if you upgrade recovery agent on Linux, you must also upgrade the recovery agent version on the Windows proxy.

**Procedure**

To upgrade Data Protection for VMware, complete the following steps:

1. Stop any Data Protection for VMware components and services that are running.
2. Unmount any mounted virtual volumes.

   You can use the recovery agent GUI or command-line interface (**mount del** command) to unmount volumes.
3. Follow the instructions in "Installing the Data Protection for VMware components on Windows systems" on page 19.

   **Note:** `Linux` If the data mover V6.x is installed, you must uninstall it before you install V8.1.10. Follow the instructions in the topic Uninstalling the IBM Spectrum Protect Linux x86_64 client.
4. Download the code package.
5. From the folder where you saved the code package start the upgrade process:

   a) `Windows`
      Run the `spinstall.exe` file.

   b) `Linux`
      Run the `install-Linux.bin` file.

You can install only one Data Protection for VMware vSphere GUI on a machine. As a result, more than one Data Protection for VMware vSphere GUI is not allowed on the same machine.

## Upgrading Data Protection for VMware on a Windows 64-bit system in silent mode

You can silently upgrade Data Protection for VMware on a supported 64-bit operating system.

**Before you begin**

When Data Protection for VMware V6.x was installed to a non-default location, the silent upgrade process installs Data Protection for VMware V8.1.10 features to the default installation directory. You cannot silently upgrade to a non-default location. See the subtopics in "Installable components" on page 1 section for the default installation directories for each feature.

**Procedure**

To upgrade Data Protection for VMware, complete the following steps:

1. Stop any Data Protection for VMware components that are running.
2. Unmount any mounted virtual volumes.

   You can use the recovery agent GUI or command-line interface (**mount del** command) to unmount volumes.

3. Unmount any mounted virtual volumes.

   You can use the recovery agent GUI or command-line interface (**mount del** command) to unmount volumes.

4. Download the code package.
5. Navigate to the folder for Data Protection for VMware.
6. From the command prompt window, enter the following command:

   ```
   spinstall.exe /silent REGISTER_EXTENSION=1 VCENTER_HOSTNAME=<hostname>
   VCENTER_USERNAME=<username> VCENTER_PASSWORD=<pass> /debuglog<file_path>
   ```

## Upgrading Data Protection for VMware on a Linux system in silent mode

You can silently upgrade Data Protection for VMware on a supported Linux operating system.

**About this task**

Use the following Data Protection for VMware parameters with the silent installation feature:

Table 9. Data Protection for VMware silent installation upgrade parameters

| Parameter | Description | Default value |
|---|---|---|
| **VCENTER_HOSTNAME** | The vCenter Server fully qualified domain name or IP address. | None |
| **VCENTER_USERNAME** | The vCenter user ID. This user ID must be a VMware administrator that has permission to register and unregister extensions. | None |
| **VCENTER_PASSWORD** | The vCenter password. | None |
| **DIRECT_START** | To access the Data Protection for VMware vSphere GUI in a web browser, specify **DIRECT_START=YES**. The Data Protection for VMware vSphere GUI is accessed through a URL bookmark to the GUI web server. If you do not want to access the Data Protection for VMware vSphere GUI in a web browser, specify **DIRECT_START=NO**. | YES **Important:** After upgrade completes, the **DIRECT_START** value cannot be changed except by reinstalling the product. |

**Procedure**

To upgrade Data Protection for VMware, complete the following steps:

1. Make sure that there are no active backup, restore, or mount sessions.
2. Make sure that any existing Data Protection for VMware vSphere GUI or recovery agent GUI is closed.
3. Download the code package.
4. From the Data Protection for VMware folder, go to the Linux folder.
5. From a command prompt window, enter the `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` command with the preferred parameters.
   For example: `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true -DVCENTER_HOSTNAME=9.11.90.86 -DVCENTER_USERNAME=administrator@vsphere.local -DVCENTER_PASSWORD=**** -DREGISTER_EXTENSION=yes -DDIRECT_START=yes`

## Upgrading Data Protection for VMware in a vCenter Server Linked Mode environment

All Data Protection for VMware GUI hosts must be updated in a timely manner to enable Data Protection for VMware components to support current VMware Linked Mode features.

**About this task**

**Note:** This information is specific to Versions 6.0, 6.5 & 6.7 of the vSphere application run on a VMware vCenter.

VMware vCenter Server Linked Mode is a tool that provides an overview of management zones so that servers can support greater numbers of virtual machines. The IBM Spectrum Protect Data Protection for VMware plug-in is compatible with VMware running in Linked Mode. See the VMware documentation at vCenter Enhanced Linked Mode for more information on this VMware feature

When vCenters are in Linked Mode, there is a single view of all vCenters through the vSphere UI. The same UI is visible by logging in to any of the vCenters that are linked together. As a result, the IBM Spectrum Protect Data Protection plug-in is displayed on all vCenters, even if it has only been installed and configured on a single vCenter.

While the plug-in is visible to every vCenter, the functionality of the plug-in is only available to each vCenter that has an IBM Spectrum Protect Data Protection for VMware GUI host associated with it.

When upgrading a vCenter Server Linked Mode environment, take into account the following issues:

- When you use vCenters in linked mode, the first vCenter upgraded will result in the newer level plug-in being visible to all linked vCenters. The IBM Spectrum Protect Data Protection for VMware plug-in has been developed to be compatible with a single lower level release GUI host. For example, a Data Protection for VMware V8.1.6 plug-in is still compatible with a Data Protection for VMware V8.1.4 GUI host.
- While the lower level GUI host will still work with a newer plug-in, the functions introduced in the newer release will not work. You must update all GUI hosts in a timely manner to allow full functionality of the newer plug-in.

**Example**

Prior to upgrading to Version 8.1.6, vCenter1 and vCenter2 are in linked mode. They each have an IBM Data Protection for VMware GUI Host. The plug-in within vSphere and the GUI hosts are at Version 8.1.4.

vCenter1 is now upgraded to V8.1.6. The plug-in and GUI host1 are now at V8.1.6. A user who logs in to the vSphere for vCenter2 will see the V8.1.6 plug-in, not the V8.1.4 plug-in. The user can then navigate to **IBM Spectrum Protect -> Configure -> Connections** and see that vCenter1 has a GUI host at V8.1.6, but the vCenter2 GUI host is still at V8.1.4.

The Spectrum Protect plug-in still functions for vCenter2 in the same way as it did in V8.1.4. The difference is that any new features for V8.1.6 can not be used on vCenter2, only vCenter1, until a V8.1.6 upgrade to vCenter2's GUI host has been completed.

# Uninstalling Data Protection for VMware

The process for uninstalling Data Protection for VMware is the same for a new installation and for an upgraded version.

## Uninstalling Data Protection for VMware on Windows

Uninstall Data Protection for VMware components and remove files and directories from a Windows system.

**Before you begin**

To ensure a successful uninstall, use the following guidance:

- If other Data Protection for VMware web GUI hosts use the IBM Spectrum Protect vSphere Client plug-in, do not unregister the web client extension.

**About this task**

Configuration and property files are located in the `C:\Program Files\IBM\SpectrumProtect \Framework\VEGUI\config` directory after the uninstall completes.

**Procedure**

1. Stop any Data Protection for VMware components that are running.
2. Unmount any mounted virtual volumes.
3. Delete any existing virtual machine backups using the data mover `delete backup` command.
4. Remove any installed data mover services using the `dsmcutil remove` command.

   For a list of services go to `C:\Program Files\Tivoli\TSM\baclient\` and run the command `dsmcutil list`.

   Remove services with commands similar to the following, adapting the quoted name to the listed service:

   ```
     dsmcutil remove /name:"TSM Remote Client Agent"
    dsmcutil remove /name:"TSM Client Acceptor"
   ```

5. Click **Start** > **Control Panel** > **Programs and Features** > **Uninstall a program**. Uninstall the following programs:

   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware Suite
   - IBM Spectrum Protect for Virtual Environments Data Protection for VMware License
   - IBM Spectrum Protect JVM

6. Remove the following Data Protection for VMware files and directories from the file system, if they are present.

   For IBM Spectrum Protect for Virtual Environments V8.1.6 and higher, delete:

   ```
    C:\IBM\SpectrumProtect
    C:\Program Files\IBM\SpectrumProtect
    C:\ProgramData\Tivoli\TSM
    C:\ProgramData\config
    C:\IBM\SpectrumProtect
    C:\Program Files\IBM\SpectrumProtect
   ```

   You can also remove:

   ```
    C:\Program Files\Tivoli\TSM
   ```

   if the remaining log files and configuration files are no longer needed. If you wish to keep those files they are located in `C:\Program Files\Tivoli\TSM\baclient`.

For IBM Spectrum Protect for Virtual Environments V8.1.4 and prior, delete:

```
C:\IBM\tivoli
C:\Program Files (x86)\Common Files\Tivoli\TDPVMware
C:\Program Files\Common Files\Tivoli
C:\ProgramData\Tivoli\TSM
C:\ProgramData\config
```

You can also remove:

```
C:\Program Files\Tivoli\TSM
```

if the remaining log files and configuration files are no longer needed. If you wish to keep those files they are located in `C:\Program Files\Tivoli\TSM\baclient`.

**What to do next**

Check that all components have been removed from the system.

## Uninstalling Data Protection for VMware for Windows in silent mode

You can silently uninstall Data Protection for VMware on a Windows operating system.

**About this task**

Configuration and property files are located in the `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config` directory after the uninstall completes.

**Procedure**

To uninstall Data Protection for VMware, complete the following steps:

1. Stop any Data Protection for VMware components that are running.
2. Unmount any mounted virtual volumes.

   You can use the recovery agent GUI or command-line interface (**mount del** command) to unmount volumes.
3. In a command prompt window:

   • Unregister the Data Protection for VMware vSphere GUI plug-in and uninstall the Data Protection for VMware component:

      a. Go to the following directory on the installer:

      ```
      TSMVMWARE_WIN\DPVMware
      ```

      b. Enter the following command:

      ```
      spinstall.exe /s /v"/qn REBOOT=ReallySuppress
      ```

      ```
      REMOVE=ALL UNREGISTER_EXTENSION=1
      ```

      ```
      VCENTER_HOSTNAME=<vCenter hostname or IP>
      ```

      ```
      VCENTER_USERNAME=<vCenter user name>
      ```

      ```
      VCENTER_PASSWORD=<vCenter password>"
      ```

   • Uninstall all features with Suite installer:

      a. Go to the following directory on the installer:

      ```
      TSMVMWARE_WIN
      ```

      b. Enter the following command:

```
spinstall.exe /silent /remove
```

> **Note:** With a complete uninstall, you must unregister the Data Protection for VMware vSphere GUI as outlined above.

4. Restart the system after uninstallation completes.

## Uninstalling Data Protection for VMware on a Linux system

Uninstall Data Protection for VMware and remove files and directories on a supported Linux operating system.

### Before you begin

To ensure a successful uninstall, use the following guidance:

- Remove nodes from IBM Spectrum Protect Server. You must do this prior to the uninstall of the Data Protection for VMware product:

  1. Run the dsmadmc from `/opt/tivoli/tsm/client/ba/bin/dsmadmc`.
  2. You may need to use the del command to delete file space for nodes: `del file` *nodename* `*`
  3. Use the q command to query for nodes: `q filespace` *nodename* `*`
  4. Use the rem command to remove nodes: `rem node` *nodename*

- Stop dsmcad services created for Data Movers. Use the instructions in the technical note [http://www-01.ibm.com/support/docview.wss?uid=swg21358414](http://www-01.ibm.com/support/docview.wss?uid=swg21358414)

  1. Use the ps command to check if the dsmcad service is running: `ps -ef|grep dsmcad`
  2. Use the kill command to halt the dsmcad service: `kill -9` *dsmcad-processID*

- You must clean up files related to the creation of a Data Mover services. Go to the installation directory and issue the following command:

```
/opt/tivoli/tsm/client/ba/bin/dsmutillnx cleanupDmFiles 1
```

  Press Enter to select the node name and press Press Enter to delete.

  You can find the node names in `dsm.sys`

- When you uninstall the IBM Spectrum Protect vSphere Client plug-in from a VMware vSphere 5.5 environment, only its associated privilege labels and descriptions are removed. The actual privileges remain installed. This issue is a known VMware limitation. For more information, see the following VMware Knowledge Base article: [http://kb.vmware.com/kb/2004601](http://kb.vmware.com/kb/2004601).

- The Data Protection for VMware Enablement File is not removed after the product is uninstalled.

### About this task

When you uninstall Data Protection for VMware on a Linux system, by default, the type of uninstallation is the same process as the type of original installation. To use a different uninstallation process, specify the correct parameter. For example, if you used a silent installation process, you can use the installation wizard to uninstall by specifying the `-i swing` parameter. Run the uninstallation process as the root user. The root user profile must be sourced. If you use the su command to switch to root, use the `su -` command to source the root profile.

When the uninstall process begins removing program files, canceling the uninstall process does not return the system to a clean state. This situation might cause the reinstallation attempt to fail. As a result, clean the system by completing the tasks that are described in "Manually removing Data Protection for VMware from a Linux system" on page 32.

To uninstall Data Protection for VMware, complete the following steps:

**Procedure**

1. Change to the directory for the uninstallation program. The following path is the default location to the uninstallation program: `/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/`

2. Depending on the type of installation, use one of the following methods to uninstall Data Protection for VMware:

   **Note:** The commands in this procedure must be entered on one line. These examples show two lines to accommodate page formatting.

   • To use the installation wizard to uninstall Data Protection for VMware, enter this command:

   ```
   ./Uninstall_Tivoli_Data_Protection_for_VMware –i swing
   ```

   • To use the console to uninstall Data Protection for VMware, enter this command:

   ```
   ./Uninstall_Tivoli_Data_Protection_for_VMware -i console
   ```

   • To silently uninstall Data Protection for VMware, enter this command:

   ```
   ./Uninstall_Tivoli_Data_Protection_for_VMware -i silent
   -f uninstall.properties
   ```

   The `uninstall.properties` file contains the vCenter connection information. This information is needed to uninstall the Data Protection for VMware vSphere GUI.

**Manually removing Data Protection for VMware from a Linux system**

**About this task**

When Data Protection for VMware cannot be uninstalled by using the standard uninstallation procedure, you must manually remove Data Protection for VMware from the system as described in these steps. Complete this process as the root user.

**Procedure**

1. If you installed the Data Protection for VMware vSphere GUI, remove its package from the Package Manager database with this command:

   ```
   rpm -e TIVsm-TDPVMwarePlugin
   ```

2. Remove the IBM Spectrum Protect API with this command:

   ```
   rpm -e TIVsm-API64
   gskssl64.linux.x86_64.rpm
   skcrypt64.linux.x86_64
   TIVsm-TDPVMwarePlugin.x86_64.rpm
   TIVsm-DPAPI.x86_64.rpm
   ```

3. Remove the product entries from the Deployment Engine:

   a) Issue this command to view a list of all entries:

   ```
   /usr/ibm/common/acsi/bin/de_lsrootiu.sh
   ```

   b) Issue this command to remove the installed unit entries that are related to Data Protection for VMware:

   ```
   /usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>
   ```

   Ensure that these unit entries are removed:

   ```
   FBJRE
   TDPVMwareGUI
   JavaHelp
   TDPVMwareDM
   ```

After the uninstaller completes, remove the following directories, if present:

- `/opt/tivoli/tsm/client`
- `/opt/tivoli/tsm/tdpvmware`

Remove the user `tdpvmware` and associated directories:

- `userdel tdpvmware`
- `/home/tdpvmware`
- `/etc/adsm`

4. Back up the global registry file (`/var/.com.zerog.registry.xml`).

   After the file is backed up, remove all tags that are related to Data Protection for VMware.

5. Remove all files in the installation directory (`/opt/tivoli/tsm/tdpvmware`). Also, remove any shortcuts that are on the desktop.

6. Back up the log files that are in the `/root` directory that contain TDPVMware in the file name. For example, `IA-TDPVMware-00.log` or `IA-TDPVMware_Uninstall-00.log`.

   Remove these log files after they are backed up. By removing them, you can view any error that is issued if the installation process fails again.

7. You can now install the product again as described in "Installing Data Protection for VMware on Linux systems" on page 20.

# Modifying an existing installation of Data Protection for VMware

This section provides instructions for modifying packages and features in an existing Data Protection for VMware installation.

Using the Suite Installer, you can change which underlying packages are installed on the system. To modify any of the individual package features, you can use the Windows **Programs and Features** Control Panel.

## Modifying packages in an existing installation of Data Protection for VMware

You can use the Suite Installer to make changes to the packages in an existing installation of Data Protection for VMware.

**Before you begin**
Ensure that you have the source media to hand before using the Suite Installer. The `spinstall.exe` executable file for the Suite Installer is located at the root of the installation package.

**About this task**

Use the Suite Installer to modify which packages are installed in an existing installation of Data Protection for VMware. You can choose to add or remove:

- Data Mover
- Data Protection for VMware

Complete the following steps:

**Procedure**

1. Double-click the `spinstall.exe` file to run the Suite Installer package.
2. Use the package check-boxes on the **Custom Setup** panel to determine the packages you need to install.
3. Select the packages required for this installation.

# Modifying features in an existing installation of Data Protection for VMware

You can use the Windows Programs and Features Control Panel to make changes to the features in an existing installation of Data Protection for VMware.

**Before you begin**
Ensure that you have the source media to hand before modifying the installation package.

**About this task**

Use Windows to modify which individual package features are available in an existing installation of Data Protection for VMware. You can choose to modify the features of:

- Data Mover
- Data Protection for VMware

Complete the following steps:

**Procedure**

1. In the **Programs and Features** section of the Windows **Control Panel**, right-click on the IBM Spectrum Protect for Virtual Environments: Data Protection for VMware application.
2. Click **Modify** to update the currently installed features of the package.
3. Select the features required for this installation.

# Chapter 2. Configuring Data Protection for VMware

This section provides instructions for configuring Data Protection for VMware and starting related services.

**Tip:** After you install Data Protection for VMware, the IBM License Metric Tool counts the data mover only if it is connected to an IBM Spectrum Protect server and is used for data operations. Subsequently, that data mover is always included in license calculations. Data movers that are not connected to a server and are not used for data operations are excluded from license calculations.

## Configuring a new installation with the wizard on Windows

Use the configuration wizard for the initial configuration or to complete minor changes on Windows.

### Before you begin

For systems using a Linux-only environment, consult Configuring a new installation with the wizard on Linux.

The system where Data Protection for VMware is installed must have network connectivity to the following servers:

- Remote Data Mover
- IBM Spectrum Protect server
- vCenter Server

### About this task
To configure the Data Protection for VMware environment, complete these steps:

### Procedure

1. Open a web browser and enter the GUI web server address.
   For example:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

2. Log in with the vCenter user name and password.
3. In the **Getting Started** window, go to the **Configuration** window and click **Run Configuration Wizard**.
4. Follow the instructions in each page of the wizard until the **Summary** window displays. Review the settings and click **Finish** to complete the configuration and exit the wizard.

   **Tip:** Information about each configuration page is provided in the online help that is installed with the GUI. Click **Learn More** in any of the GUI windows to open the online help for task assistance. See the *Running the configuration wizard* topic.
5. Verify that the data mover nodes are configured properly:
   a) Click the **Configuration** tab to view the **Configuration Status** page.
   b) In the **Configuration Status** page, select a data mover node to view its status information in the **Status Details** pane.

      When a node displays a warning or error, click that node and use the information in the **Status Details** pane to resolve the issue. Then, select the node and click **Validate Selected Node** to verify whether the issue is resolved. Click **Refresh** to retest all nodes.

### Results

**Fast path:** After you successfully complete this wizard task, no additional configuration tasks are required to back up your VM data.

# Configuring a new installation with the wizard on Linux

Use the configuration wizard for the initial configuration or to complete minor changes on Linux.

**Before you begin**
The system where Data Protection for VMware is installed must have network connectivity to the following servers:

- Remote Data Mover
- IBM Spectrum Protect server
- vCenter Server

**About this task**
To configure the Data Protection for VMware environment on Linux, complete these steps:

**Procedure**

1. Run the installer on the Linux host.
2. Select options 2 and 3 (**Data Mover** and **GUI**).
3. After the install completes, run the configuration wizard at this location:

   ```
   https://localhost:9081/TsmVMwareUI
   ```

   For ease of setup, only define one Data Mover on the GUI host. This Data Mover must be configured manually before you can use the Web Client plug-in GUI to add or configure more data movers.

   **Note:** If you are performing an upgrade, and you had a working Data Mover instance prior to the upgrade, simply restart the services. You can now use the Web Client plug-in for future operations.
4. While completing the panels on the wizard collect the following information:

   - Node names and passwords for the data mover and mount proxy pair registered.
   - dsm.sys content for each Data Mover and Mount Proxy created.
5. Once the configuration wizard is completed, manually set up the Data Mover that will run on the GUI host.

   For this step, and for steps 6 and 7, review the information on manual setup on Linux, in the topic Manually setting up the data mover nodes in a vSphere environment .
6. When the Data Mover instance is running, manually set up the Linux mount proxy instance that will run on the GUI host.
7. When the Linux mount proxy instance is running, manually set up the Windows mount proxy instance on a Windows host.
8. You can now use the Web Client plug-in for future operations. The legacy GUI interface can be used when you want to change or update the default Spectrum Protect server information.

**Results**

**Fast path:** After you successfully complete this wizard task, no additional configuration tasks are required to back up your VM data.

# Configuring a multiserver environment

You can now view all of your backups, schedules and restore operations across multiple backup servers from a single vSphere plug-in.

**Monitor your entire data protection environment across multiple backup servers from a single view**

After you install IBM Spectrum Protect, you can configure an initial backup server using the setup wizard. This server is designated as the default backup server, since it runs as a web application on the GUI host.

Additional backup servers can then be added or removed using the plug-in. The default backup server must not be removed from the plug-in. You can then assign multiple IBM Spectrum Protect backup servers to support datacenters on a vCenter. Each datacenter can be associated with one backup server out of a pool of Spectrum Protect servers. All the backup servers can be managed from a single vSphere plug-in or Data Protection for VMware GUI host.

## Configuring a default backup server

After you install IBM Spectrum Protect Data Protection for VMware, you can set up an initial default backup server by using the configuration wizard.

**Procedure**

1. When the installation wizard completes processing, select the **Launch Data Protection for VMware Configuration Wizard** check box, and click **Finish**.

   The wizard is launched in a web browser at the following URL: `https://localhost:9081/TsmVMwareUI/`.

2. Authenticate to Data Protection for VMware by specifying vCenter administrator credentials.

3. On the VMware vSphere vCenter tab, update the plug-in registration details. Ensure that the GUI host address is a valid address that can be pinged from the vCenter.

4. On the **Server Credentials** tab, enter details for the default backup server. The default backup server will be used for the Web GUI where the configuration wizard is located (`https://localhost:9081/TsmVMwareUI/`).

5. Choose the prefix and policy domain. The best practice is to choose a different prefix for each backup server.

6. Accept the default values or modify the names on the **vCenter Node** and **VMCLI Node** tabs.

7. In the **GUI Domain** pane, add to the **Managed Datacenters** column only the datacenters that the default server will be backing up. Omit any datacenters that an additional backup server will manage.

8. Accept the defaults or modify the names on the **Data Mover Nodes** and **Mount Proxy Node** tabs. Where applicable, take note of the data mover node and mount proxy node passwords for any later manual configuration steps.

9. You can optionally elect to set up file restore at this stage.

10. Review the **Summary** page, and then click **Finish** to complete the configuration process.

11. Optionally, verify the configuration by logging on to the vSphere Client. You can navigate directly to the client, or click the **Open vSphere Web Client** button on the configuration screen.

## Configuring additional backup servers

You can use the IBM Spectrum Protect vSphere plug-in to configure additional backup servers.

**Before you begin**

**Note:** When you configure additional backup servers with the vSphere plug-in, you must use a server that supports the SSL protocol.

**Procedure**

1. After the initial configuration is completed in the Web GUI host, log in to the plug-in and navigate to IBM Spectrum Protect Configuration.

2. Click **Configure -> Connections** to set up the connection between the plug-in and the GUI host.

3. Edit the connection to point to the GUI host.

   After a successful connection, click the **Backup Servers** tab. You might have to refresh the table to see the backup server information. After a refresh, the default server that is configured in the Web GUI host is displayed.

4. To create an additional backup server, click the **+** (add server) button. Enter information for the second server.

5. You might be prompted to accept digital certificates if this is the first time you are accessing the API and server. The first certificate verifies the connection to the REST API of the Web GUI host. The second certificate verifies the new backup server itself. You must accept both certificates in order to proceed.

6. Select a policy domain from a drop-down list and a prefix. The best practice is to choose a different prefix for each backup server.

7. On the summary screen, review your choices and click **Finish** to add the backup server.

8. Add a datacenter by clicking **Add Datacenter Association** in the **Results** pane.

9. Under **Datacenter Management**, review the list of all datacenters in a particular vCenter. Select the datacenter that is to be associated with a backup server. Click **Create association** to associate a backup server with a datacenter.

10. Click **Create Association**, and enter the details for the server that must be associated with that datacenter.

11. Add a data mover for the datacenter. Each datacenter requires its own data mover. However, the same installation of a data mover can be used for multiple datacenters. Select **Add Data Mover** to go directly to the data mover pane.

12. Click **Add Data Mover** on the **Data Movers** tab. The data mover host can be on the GUI host machine. Another option is to install the data mover separately.

13. After the first data mover is added to a datacenter, a schedule is automatically created.

14. Click **Configure -> Schedules**. Refresh the schedules table to see the new schedule.

    The additional backup server is now configured to be used by Data Protection for VMware.

## Creating schedules with additional backup servers

After you set up the default backup server, use the IBM Spectrum Protect vSphere plug-in to configure additional backup servers.

**Before you begin**

The initial default schedule has no object. A schedule must have a tagged object to start backups.

**About this task**

After you configure one or more backup servers, you can create a default schedule. This schedule can be used to define additional backup servers. If additional schedules are required, follow the instructions in Creating a schedule that is compatible with tagging.

Each schedule is associated with a particular datacenter. Each schedule can have one or more data movers.

**Procedure**

1. To add an object for the schedule to back up, go to the datacenter associated with that schedule. Select an object at the datacenter level or lower, right click on the object and click **IBM Spectrum Protect -> Configure Data Protection**.

2. In the **Configure Backup Policies** pane, select the new schedule to start backing up that object.

3. After the object has been associated, verify the following items:

   • Verify that the object shows the correct information when you click **Configure -> IBM Spectrum Protect** screen.

   • Verify that the schedule now has the object selected listed when you click **Menu -> IBM Spectrum Protect -> Configure -> Schedules**.

   • After the schedule runs, go to the object and click **Monitor -> IBM Spectrum Protect**.

   **Hint:** Optionally, to update the start time for the schedule from the command line, take the following actions:

a. Go to the dsmadmc location: `C:/Program Files/Tivoli/TSM/baclient`

b. At the prompt, find the `dsm*opt` file for the data mover associated with that server. (`dir * opt`)

c. Issue the command dsmadmc - `optfile=dsm.datamovername.opt`

d. Type the following command to start the schedule in 10 minutes:

   `update schedule policyDomain scheduleName StartTIME=NOW+00:10`

## Running ad hoc backups

When configuration is completed for multiple IBM Spectrum Protect backup servers, you can run ad hoc backups.

**Procedure**

1. Select the datacenter that is associated with a particular server you want to test backups on. Go to an object within that datacenter, right-click the object and click **Backup**.
2. Select the desired options and click **Start** to begin the backup.
3. Optionally, monitor progress in the vSphere **Recent Tasks** table.
4. Optionally, after the backup is completed, you can check the status by selecting the object backup, then click **Monitor -> IBM Spectrum Protect**.

## Running ad hoc restore operations

After a virtual machine (VM) has been backed up to an IBM Spectrum Protect server, you can run ad hoc restore operations.

**Procedure**

1. Determine which VMs have backups by selecting the datacenter and choosing **Monitor -> IBM Spectrum Protect**.

   A table with a list of all VMs and their backup status is displayed.
2. Select a VM that has a backup in the inventory, and right-click **IBM Spectrum Protect -> Restore**.
3. Select the restore point and specify any additional options.
4. When the restore wizard is completed, click **Finish**.
5. Optionally, monitor restore progress by using the **Recent Tasks** view in vSphere.
6. Optionally, verify the status of the restore operation in the inventory.

# Using the notebook to edit an existing installation

Use the Edit Configuration notebook to edit existing configuration settings.

**Before you begin**
The Edit Configuration notebook provides the following tasks for an existing configuration:

- Set or change the IBM Spectrum Protect Administrator ID.
- Reset the password and unlock the VMCLI node.
- (vSphere environment) Add or remove VMware data centers to your Data Protection for VMware vSphere GUI domain.
- Add or remove mount proxy nodes. Modify a password for an existing mount proxy node.
- Add or remove data mover nodes. Modify a password for an existing data mover node.
- Enable file restore.
- Enable tagging support for a data mover node.

**About this task**
To edit an existing configuration, complete these steps:

**Procedure**

1. Open a web browser and enter the GUI web server address.
   For example:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   Log in with the vCenter user name and password.

2. In the **Getting Started** window, go to the **Configuration** window and click **Edit Configuration**.

3. Go to the page relevant for your edit task and follow the instructions. You must click **OK** to save your changes before you proceed to another **Configuration Settings** page. Otherwise, your changes do not take effect.

   **Important:** Information about each configuration page is provided in the online help that is installed with the GUI. Click **Learn More** in any of the GUI windows to open the online help for task assistance. See the *Editing an existing configuration* topic.

**Results**

The updated settings are displayed in the **Configuration** window.

## Windows Enabling the environment for file restore operations

When the file restore feature is enabled by an administrator, file owners can restore files without assistance.

**Before you begin**

If you did not verify that all prerequisites are met, review the topic on file restore prerequisites in the *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware User's Guide.*

**About this task**

Complete these steps on the system where the Data Protection for VMware vSphere GUI is installed.

**Procedure**

1. Start the Data Protection for VMware vSphere GUI by opening a web browser and entering the GUI web server address.
   For example:

   ```
   https://<GUI web server address>:9081/TsmVMwareUI/
   ```

   Log on with the vCenter user ID and password.

2. From the **Getting Started** window, click **Configuration** and select one of the following tasks in the **Tasks** list:

   - If you are configuring a new environment, complete the following steps:

     a. Select **Run Client Configuration Wizard**.

     b. Follow the instructions on each page of the wizard. Use the following guidance to complete the **File Restore** page:

        1) Select the **Enable File Restore** option.

        2) Enter the administrator contact information that is shown in the file restore interface. If you do not want to provide contact information, clear the check box.

        3) If the environment contains backups of Windows virtual machines, enter Windows domain user credentials. Otherwise, clear the check box and do not enter any credentials.

           **Tip:** A file restore operation uses Windows domain user credentials to access network shares on the remote virtual machine. An operation fails when the environment contains backups of

Windows virtual machines and no credentials, or the incorrect credentials, are entered. Therefore, clear this check box only when there are no Windows virtual machine backups.

   4) Click the file restore interface URL to verify that the interface is accessible.

      **Remember:** Keep a record of the file restore interface URL. The owner of the guest virtual machine accesses the file restore interface through this URL.

   5) Click **OK** to save your changes.

- If you are updating an existing environment, complete the following steps:

   a. Select **Edit TSM Configuration**.

   b. On the **File Restore** page, use the following guidance:

      1) Select the **Enable File Restore** option.

      2) Enter the administrator contact information that is shown in the file restore interface. If you do not want to provide contact information, clear the check box.

      3) If the environment contains backups of Windows virtual machines, enter Windows domain user credentials. Otherwise, clear the check box and do not enter any credentials.

         **Tip:** A file restore operation uses Windows domain user credentials to access network shares on the remote virtual machine. An operation fails when the environment contains backups of Windows virtual machines and no credentials, or the incorrect credentials, are entered. Therefore, clear this check box only when there are no Windows virtual machine backups.

      4) Click the file restore interface URL to verify that the interface is accessible.

         **Remember:** Keep a record of the file restore interface URL. The owner of the guest virtual machine accesses the file restore interface through this URL.

      5) Click **OK** to save your changes.

**Results**

The environment is enabled for file restore operations. File owners can restore their files by using the URL to access the IBM Spectrum Protect file restore interface.

## `Linux` Setting up file restore operations on Linux

To enable the file restore feature when Data Protection for VMware is installed on a Linux system, an additional Data Protection for VMware environment must be set up on a Windows system.

**About this task**

When you run Data Protection for VMware in a Linux environment, the file restore feature must be installed on a Windows system to enable the file restore feature.

**Procedure**

1. Set up a separate Windows server that is used for the file restore feature.
2. Install Data Protection for VMware on the Windows system. Accept the default values during the installation.
3. When you configure Data Protection for VMware on the Windows system, use the following node names:
   a) Create a vCenter node named VCENTER_FR.
   b) Create a VMCLI node named VMCLI_FR.
   c) Reuse the datacenter node name from the Linux environment.
      For example: DATACENTER.
   d) Do not create a data mover node. A data mover node is not required for the file restore feature in this scenario.

e) Create the following new pair of mount proxy nodes named REMOTE_FR_MP_WIN and REMOTE_FR_MP_LNX.

4. On the **File Restore** page in the configuration wizard, select the `Enable File Restore` option.

5. To access the file restore interface, open a web browser and enter the URL provided by your administrator.
   For example:

   ```
   https:\\hostname:9081\FileRestoreUI
   ```

   where `hostname` is the host name of the Windows system where Data Protection for VMware is installed.

### Results

The following example shows the proxy node relationships on the IBM Spectrum Protect server:

```
tsm: SERVER>q proxy

Target Node        Agent Node
---------------    ---------------------------------------------
VCENTER            VMCLI DATACENTER
VCENTER_FR         VMCLI_FR DATACENTER
DATACENTER         VMCLI VMCLI_FR
                    DATAMOVER1
                    REMOTE_MP_WIN REMOTE_MP_LNX
                    REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX
```

The additional nodes that are created to enable the file restore feature have the _FR suffix.

## <span style="color:purple">Windows</span> Modifying options for file restore operations

To allow administrators to configure and control restore processing for file restore operations, modify the options in the `frConfig.props` file.

### About this task
Complete these steps on the system where the Data Protection for VMware vSphere GUI is installed.

### Procedure

1. Go to the directory where the `frConfig.props` file is located.
   For example, open a command prompt and issue the following command:

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI
   ```

2. Open the `frConfig.props` file with a text editor in administrator mode and modify the options as needed.
   Use the information in "File restore options" on page 42 to determine which options to modify.

3. Save your changes and close the `frConfig.props` file.

### Results
Modified options are applied to the IBM Spectrum Protect file restore interface.

## File restore options

The `frConfig.props` options control configuration, support, and restore processing for file restore operations.

**enable_contact_info=false | true**
> Specify whether to provide administrator contact information that file owners can use to obtain support.

> **false**
>> File owners do not receive administrator contact information. This value is the default.

**true**
> File owners receive administrator contact information.

If you specify **enable_contact_info=true**, you must provide information in the **contact_info** option.

**enable_filerestore=false | true**
> Specify whether file owners can restore their files from a virtual machine with the IBM Spectrum Protect file restore interface.

> **false**
> > File owners cannot restore their files with the IBM Spectrum Protect file restore interface. This value is the default.

> **true**
> > File owners can restore their files with the IBM Spectrum Protect file restore interface.

**maximum_mount_points=*num_mount_points***
> Specify the maximum number of simultaneous recovery points that are available to the user account. The minimum value is 1 recovery point. The maximum value is 256 mount points. The default value is 2 mount points.

> **Tip:** To prevent a virtual machine from being mounted multiple times for simultaneous restore operations, set this option with a low value.

**mount_session_timeout_minutes=*num_mins***
> Specify the amount of time, in minutes, that a restore and the mounted recovery point can be idle before the session is canceled. A cancellation unmounts the recovery point. The maximum value is 8 hours (480 minutes). The default value is 30 minutes.

> **Tip:** To prevent the session from being canceled unexpectedly, increase the number of minutes.

**restore_info_duration_hours=*num_hrs***
> Specify the amount of time, in hours, that information about recent restore activity is retained in the IBM Spectrum Protect file restore interface. Use the restore activity window to view error information and recently completed tasks. This information provides a way to locate recently restored files. The maximum value is 14 days (336 hours). The default value is one week (168 hours).

**contact_info=*administrator information***
> Provide administrator contact information that file owners can use to obtain support. Contact information displays in the IBM Spectrum Protect file restore interface in the following locations:

> - Login window
> - The **About** pane in the help menu
> - The support information link in interface messages

You can overwrite the following options with the Data Protection for VMware vSphere GUI configuration wizard or notebook:

- **enable_contact_info**
- **enable_filerestore**
- **contact_info**

## Configuring log activity for file restore operations

To allow administrators to configure and control how content is formatted and logged for file restore operations, modify the options in the `FRLog.config` file.

**Before you begin**

The `FRLog.config` file is generated the first time that the IBM Spectrum Protect file restore interface is accessed.

**About this task**
Complete these steps on the system where the Data Protection for VMware vSphere GUI is installed.

**Procedure**

1. Go to the directory where the `FRLog.config` file is located.
   Open a command prompt and issue the following command:

   ```
   cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI\
   ```

2. Open the `FRLog.config` file with a text editor in administrator mode and modify the options as needed.

   Use the information in "File restore log activity options" on page 44 to determine which options to modify.

3. Save your changes and close the `FRLog.config` file.

4. Restart the GUI web server:

   a) Click **Start** > **Control Panel** > **Administrative Tools** > **Services**.

   b) Right-click **Data Protection for VMware Web Server Service** and click **Restart**.

**Results**
Settings are applied to the content and format of logging information for file restore operations.

## File restore log activity options

The `FRLog.config` options control the content and format of logging information for file restore operations.

The following options log information for file restore tasks in the `fr_gui.log` file:

**MAX_LOG_FILES=*number***
   Specify the maximum number of `fr_gui.log` files to retain. The default value is 8.

**MAX_LOG_FILE_SIZE=*number***
   Specify the maximum size of the `fr_gui.log` file in KBs. The default value is 8192 KB.

The following options log information for file restore services in the `fr_api.log` file. These services are internal API services that are related to file restore activity:

**API_MAX_LOG_FILES=*number***
   Specify the maximum number of `fr_api.log` files to retain. The default value is 8.

**API_MAX_LOG_FILE_SIZE=*number***
   Specify the maximum size of the `fr_api.log` file in KBs. The default value is 8192 KB.

**API_LOG_FILE_NAME=*API_log_file_name***
   Specify the name of the API log file. The default value is `fr_api.log`.

**API_LOG_FILE_LOCATION=*API_log_file_name***
   Specify the location of the API log file. The location must be specified with a forward slash (/). The default location is `C:/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs`.

**FR.API.LOG=ON | OFF**
   Specify whether to enable logging for file restore services.

   - To enable logging for file restore services, specify ON. The default value is ON.
   - To disable logging for file restore services, specify OFF.

To troubleshoot problems that you might encounter during file restore operations, see Trace options for file restore. Trace options are also specified in the `FRLog.config` file.

# Configuring a data mover node for tagging support

When tagging support is enabled on a data mover node, administrators can apply data protection tags to inventory objects in the VMware vCenter.

**Before you begin**

Ensure that the following requirements are met:

- VMware vCenter Server must be at Version 6.0 Update 1 or later.
- In order for the Data Protection for VMware vSphere GUI to function correctly with tagging support, ensure that the following requirements are met during the installation of the GUI:

  – At least one data mover and the Data Protection for VMware vSphere GUI must be installed on the same server. This data mover node must be configured so that the vCenter server credentials are saved. You can save the credentials by running the configuration wizard to save the data mover node password, or by using the **dsmc set password** command on the data mover command line.

  If you use other data movers, running on virtual machines or physical machines as additional data movers, you can install them on other servers. For tagging support, all these data movers must also be configured with the VMTAGDATAMOVER YES option. These additional data movers do not require the Data Protection for VMware vSphere GUI to be installed on the same server in order for them to work correctly as tag-based data movers.

  – **Linux**

  For Linux data movers, ensure that you specify the data mover installation directory and the JavaTM shared library `libjvm.so` in the LD_LIBRARY_PATH environment variable. The path to `libjvm.so` is used for tagging support when you enable the `vmtagdatamover` option on the data mover. Starting with 8.1.8, a new script (`spve.sh`) has been added to `/etc/profile.d`. This will correctly set the LD_LIBRARY path for the following applications: dsmc, dsmcad and dsmj. This should cover the `libjvm.so` as well. If you see errors with LD_LIBRARY_PATH, follow the manual instructions:

  1. For IBM Java:

     ```
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic
     ```

     For Oracle Java:

     ```
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server
     ```

  2. To configure the Client Acceptor Service and Data Mover Scheduler Service to act as a vStorage Backup Server, set the following environment variable in the `/etc/init.d/dsmcad` file:

     ```
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
     ```

  **Note:** On Linux operating systems, the Data Protection for VMware vSphere GUI must be installed by using the default user name (`tdpvmware`).

  – On UNIX and Linux clients, the existing passwords in the TSM.PWD files are migrated to the new password store in the same location. For root users, the default location for the password store is `/etc/adsm`. For non-root users, the location of the password store is specified by the `passworddir` option.

  The TSM.PWD file is deleted after the migration.

**Note:** For further information on the use of privileges required for working with tagging, see Installing the Data Protection for VMware components

**About this task**

You can use data protection tags to configure the backup policy of virtual machines in VMware inventory objects. These data protection tags are presented as settings that can be changed in the IBM Spectrum Protect vSphere Client plug-in.

**Procedure**

- Use one of the following methods:

| Option | Description |
|---|---|
| **To configure a data mover node using the vSphere plug-in GUI** | 1. From the vSphere plug-in, select IBM Spectrum Protect .<br><br>2. In the **Configure** tab, select **Data Movers**.<br><br>3. In the **Add Data Mover** panel, select a datacenter from the drop-down menu.<br><br>4. Accept defaults, or edit settings for **Data mover name**, **Data mover host name**, **vCenter User** and **vCenter password**.<br><br>5. Click **Add** when settings are complete.<br><br>For further details, see the topic, Setting up data mover nodes with the vSphere plug-in GUI in the Data Protection for VMware vSphere GUI Installation Guide. |
| **To configure a *new* data mover for tagging support on Windows or Linux by using the Data Protection for VMware vSphere GUI** | 1. On the system where the Data Protection for VMware vSphere GUI is installed, start the GUI by opening a web browser and entering the GUI web server address. For example:<br><br>```<br>https://<GUI web server address>:<br>9081/TsmVMwareUI/<br>```<br><br>2. Log on with the vCenter user ID and password.<br><br>3. Go to the **Configuration** tab, and select the **Edit IBM Spectrum Protect Configuration** action.<br><br>4. Go to the **Data Mover Nodes** page of the configuration notebook.<br><br>5. Add a data mover node by completing the following steps:<br><br>  a. For the data mover node that you want to set up tagging support for, select **Create Services**. By default, **Tag Based Node** is selected to enable the data mover node for tagging support<br><br>  b. To designate the tag-based node as a default data mover node, select **Default Data Mover**. A default data mover node backs up any new VMs that are added to any container in the datacenter, if the container is already in a protection set. The default data mover also backs up any VMs in the protection set that are not assigned the `Data Mover` tag.<br><br>  **Tip:** For Linux systems, if you select a new data mover node as the default tagging node, then remove the `vmtagdefaultdatamover` line from any other data mover options file that is associated with that datacenter.<br><br>  c. Click **OK** to save your changes.<br><br>  The `vmtagdatamover` and `vmtagdefaultdatamover` (if set) options are added to the data mover options file (`dsm.opt`). |
| **To configure an *existing* Windows data mover node for tagging support when the node is on a the same server as the Data Protection for VMware vSphere GUI** | 1. Complete steps 1-3 in the preceding instructions for configuring a new data mover node for tagging support.<br><br>2. On the **Data Mover Nodes** page, select **Tag Based Node** for the node that you want to enable tagging support for.<br><br>3. **Optional:** To designate the tag-based node as a default data mover node, select **Default Data Mover**. |

| Option | Description |
|---|---|
| **To configure an** *existing* **Linux data mover node for tagging support or an existing Windows data mover node that is on a different server than the Data Protection for VMware vSphere GUI** | 1. Add the `vmtagdatamover yes` option in the data mover options file (`dsm.sys` for Linux and `dsm.opt` for Windows).<br><br>2. **Optional:** To designate the tag-based node as a default data mover node, add the `vmtagdefaultdatamover yes` or `vmtagdefaultdatamover` *dm_name* option to the data mover options file.<br><br>**Tip:** For Linux systems, if you select a new data mover node as the default tagging node, then remove the `vmtagdefaultdatamover` line from any other data mover options file that is associated with that datacenter. |

**Results**

After the data mover node is enabled for tagging support, the data mover queries the VMware inventory for tagging information when it runs a backup. The data mover then backs up the virtual machines according to the data protection tags that are set. If the data mover node is not configured for tagging support, any data protection tags are ignored during a backup operation.

**Related information**

Vmtagdatamover
Vmtagdefaultdatamover
Configuring backup policies

# Configuring your environment for full virtual machine instant restore operations

Set up a dedicated iSCSI network for full virtual machine instant restore and instant access operations.

**Before you begin**

Use the appropriate VMware documentation (ESXi or vSphere) to determine the specific steps to follow for configuring the iSCSI virtual switch and virtual machine network. Although general guidelines are provided, specific documentation and explanations for how you add virtual networks and virtual switches are outside of the scope of the product documentation. At the time of publication, the VMware vSphere ESXi and vCenter 5.5 documentation is available at VMware ESXi and vCenter Server 5 Documentation. The "Networking" topics contain the information for adding and configuring virtual switches and virtual networks.

**Important:** These configuration settings are provided to assist with setting up the VMware environment for efficient full virtual machine instant restore and instant access operations. However, since these settings apply to VMware configuration tasks and VMware user interfaces, you must refer to your appropriate VMware documentation for detailed, step-by-step instructions.

**About this task**

This procedure requires an iSCSI adapter on each ESXi host that is used for instant restore operations. Use the appropriate VMware documentation to set up the adapter. At the time of publication, the following procedures are available at this VMware vSphere resource.

- To set up a software iSCSI adapter, follow the instructions in the VMware "Configure Software iSCSI Adapters" procedure.
- To set up a hardware iSCSI adapter, follow the instructions in the VMware "Setting Up Independent Hardware iSCSI Adapters" procedure.

# 1. Configuring the iSCSI software on the ESXi host

**Procedure**

This task sets up the iSCSI software for a basic configuration.

1. Log in to the ESXi host to be used for instant restore operations.
2. Follow the instructions in this VMware Knowledge Base article until the iSCSI adapter is enabled:
   http://kb.vmware.com/kb/1008083
   IBM Spectrum Protect automatically discovers the iSCSI target server.
3. Verify that the IP address of the iSCSI adapter (on the ESXi host) is the same subnet address that is used by the data mover.
4. Verify that the Storage vMotion license is enabled on the ESXi host.

**What to do next**
After the iSCSI software is set up on the ESXi host, install and configure applications on the data mover system.

# 2. Installing and configuring applications on the data mover

**Before you begin**
If the Recovery Agent and IBM Spectrum Protect data mover are already installed and configured on the data mover system, begin at Step 3.

**Procedure**

This task sets up the data mover system with the applications and settings for instant restore operations.

1. Install the Recovery Agent and the IBM Spectrum Protect data mover on the data mover system.

   In Step 4 of the Installing Data Protection for VMware procedure, select the **Install a complete data mover for in-guest application protection** installation type.
2. Configure the data mover.

   Follow the instructions in the topic "Configuring the Data Mover" in the Client documentation.
3. Set the iSCSI server IP address:

   a) Go to the `C:\Program Files\Tivoli\TSM\baclient\dsm.opt` file and specify the following parameter:

   ```
   VMISCSISer veraddress=<IP address of the network card on the data mover
   system that exposes the iSCSI targets.>
   ```

   If your data mover system has more than one network card, make sure that you specify the correct network card for the iSCSI network.

**What to do next**
After the data mover system is set up, establish a connection between the Recovery Agent CLI and the Recovery Agent GUI.

# 3. Setting the Recovery Agent connection

**Before you begin**
The Recovery Agent command-line interface (CLI) V7.1.x can be viewed as a command-line API to the Recovery Agent GUI. You can use the Recovery Agent CLI to communicate with the Recovery Agent GUI.

**Procedure**

This task establishes a connection between the Recovery Agent CLI and the Recovery Agent GUI.

1. Start the Recovery Agent CLI on the data mover system.

From the **Windows Start** menu, click **Programs** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect Recovery Agent**.

2. In the command prompt window, enter the following command:

```
RecoveryAgentShell.exe -c set_connection mount_computer <IP address
of the network card on the data mover system that exposes the iSCSI targets.>
```

This command establishes a connection between the Recovery Agent CLI and the Recovery Agent GUI.

**What to do next**
After you establish a connection, configure a dedicated iSCSI network.

## 4. Configuring a dedicated iSCSI network for the ESXi host and data mover

**Before you begin**
Review these guidelines before you proceed with this task:

- Use a dedicated iSCSI network for instant restore operations.
- Each ESXi host that is used for instant restore operations must have a second physical network card available. This second network card is bound to the software iSCSI adapter of the respective ESXi host.
- The data mover system that runs in a virtual machine must have a second network card available. This second network card is bound to the software iSCSI adapter of the ESXi host.
- Each ESXi host that is used for instant restore operations must have a secondary VMware datastore available. This temporary datastore contains the configuration information and data of the virtual machine that is created during the operation.

**Procedure**

This task sets up a dedicated iSCSI network for the ESXi host and for the data mover that runs in a virtual machine.

1. Log in to the ESXi host to be used for instant restore operations.
2. Set up the virtual switch for the iSCSI network.

    These steps use *vSwitch1* for the virtual switch.

    a) Select **VMkernel Network Adapter** for the `Connection Type`.

    The iSCSI network requires this connection type.

    b) Select **Create a vSphere standard switch** for the `VMkernel Network Access`.

    c) Select **Network Label** for the `VMkernel Connection Settings`.

    Specify a label that indicates that *vSwitch1* and this network are for your iSCSI traffic.
    For example: *VMkernel iSCSI*.

    d) Specify an IP address and subnet mask for *vSwitch1* in `VMkernel IP Connection Settings`.

    Do not change the `Subnet Mask` or `VMkernel Default Gateway` values.

    e) Specify the kernel port for the iSCSI network to operate.

3. Set up the virtual switch for the virtual machine network.

    These steps use *vSwitch0* for the virtual switch.

    a) Select **Virtual Machine** for the `Connection Type`.

    b) Select **Create a vSphere standard switch** for the `VMkernel Network Access`.

    c) Go to the **Port Group Properties** tab and select **Network Label**.

    Specify the same label that you specified for *vSwitch1* virtual machine network.
    For example: *VMkernel iSCSI*.

4. Bind the newly created iSCSI adapter with the `VMkernel Network Adapter`.

Follow the instructions in the VMware "Bind iSCSI Adapters with VMkernel Adapters" procedure. At the time of publication, this procedure was available at VMware ESXi and vCenter Server 5 Documentation.

**Tip:** If a timeout occurs when iSCSI devices are scanned, reduce the number of iSCSI devices that are connected to the ESXi host. Then, scan the iSCSI devices again.

5. Verify that the iSCSI adapter binding properties are correct.

   a) Go to the **Hardware** > **Storage Adapters** in the VMware vSphere Client.

   b) Right-click the iSCSI adapter and select **iSCSI Initiator Properties**. Make sure that the following binding properties exist:

| Table 10. iSCSI network settings | |
|---|---|
| **Virtual Machine Network** | **iSCSI Network** |
| `Standard Switch`: *vSwitch0* | `Standard Switch`: *vSwitch1* |
| `Virtual Machine Port Group`: *VM Network* | `VMkernel Port`: *VMkernel iSCSI*<br><br>**Tip:** *VMkernel iSCSI* is bound to **`VMkernel Adapter`**: *vmk1*, which is on **`Physical Network Adapter`**: *vmnic1*. |
| `Physical Adapter`: *vmnic0* | `VMkernel Network Adapter`: *vmk1* |
| | `Physical Network Adapter`: *vmnic1* |
| | Virtual Network Adapter **`IP address`**: 192.168.42.x (subnet for the iSCSI network) |

**Results**
A dedicated iSCSI network is ready for full VM instant restore and instant access operations.

# Configuring security settings for Data Protection for VMware

The Data Protection for VMware data movers, vmcli command-line interface, and Data Protection for VMware vSphere GUI components require configuration to enable secure connection with the IBM Spectrum Protect server.

## Configuring security settings to connect data mover and VMCLI nodes to the IBM Spectrum Protect server

There are several configuration options that pertain to the Data Protection for VMware security settings for data mover and VMCLI nodes when connecting to the IBM Spectrum Protect server V7.1.8 or V8.1.2 or later. Accepting the default values for those options transparently configures these components for enhanced security, and is recommended for most use cases.

### Configuring by using the default security settings (fast path)
Fast path details the configuration options that impact the security of the data mover and VMCLI node connection to the server and the behavior for various use cases when default values are accepted. The fast path scenario minimizes the steps in the configuration process at endpoints.

This scenario automatically obtains certificates from the server when the node connects the first time, assuming that the IBM Spectrum Protect server **SESSIONSECURITY** parameter is set to **TRANSITIONAL**, which is the default value at first connection. You can follow this scenario whether you first upgrade the IBM Spectrum Protect server to V7.1.8 and later V7 levels, or V8.1.2 and later V8 levels, and then upgrade Data Protection for VMware to these levels, or vice versa.

**Attention:** This scenario cannot be used if the IBM Spectrum Protect server is configured for LDAP authentication. If LDAP is used, you can manually import the certificates necessary by using the

dsmcert utility. For more information, see "Configuring without automatic certificate distribution" on page 52.

**Data mover node options that affect session security**

The following dsmc options specify security settings for the data mover node. For more information about these options, see Client options reference.

- SSLREQUIRED. The default value `Default` enables existing session-security connections to servers earlier than V7.1.8 or V8.1.2, and automatically configures the Data Protection for VMware data mover to securely connect to a V7.1.8 or V8.1.2 or later server by using TLS for authentication.
- SSLACCEPTCERTFROMSERV. The default value Yes enables the data mover to automatically accept a self-signed public certificate from the server, and to automatically configure the data mover to use that certificate when the data mover connects to a V7.1.8 or V8.1.2 or later server.
- SSL. The default value No indicates that encryption is not used when data is transferred between the data mover and a server earlier than V7.1.8 or V8.1.2. When the data mover connects to a V7.1.8 or V8.1.2 or later server, the default value No indicates that object data is not encrypted. All other information is encrypted, when the data mover communicates with the server. The value Yes indicates that TLS is used to encrypt all information, including object data, when the data mover communicates with the server.
- SSLFIPSMODE. The default value No indicates that a Federal Information Processing Standards (FIPS) certified TLS library is not required.

In addition, the following options apply only when the data mover uses TLS connection to a server earlier than V7.1.8 or V8.1.2. They are ignored when the data mover connects to a later server.

- SSLDISABLELEGACYTLS. A value of No indicates that the data mover does not require TLS 1.2 for SSL sessions. It allows connection at TLS 1.1 and lower SSL protocols. When the data mover communicates with an IBM Spectrum Protect server that is V7.1.7 or V8.1.1 or earlier, No is the default.
- LANFREESSL. The default value No indicates that the data mover does not use TLS when communicating with the Storage Agent when LAN-free data transfer is configured.
- REPLSSLPORT. Specifies the TCP/IP port address that is enabled for TLS when the data mover communicates with the replication target server.

**VMCLI node options that affect session security**

The following parameters specify the security settings for the VMCLI node. For more information about these options, see Profile parameters.

- VE_TSM_SSL. The default value NO indicates that encryption is not used when data is transferred between the data mover and a server earlier than V7.1.8 or V8.1.2. Set this value to YES if you want to use TLS is to encrypt all information when connecting to a server earlier than V7.1.8.
- VE_TSM_SSLACCEPTCERTFROMSERV. The default value YES enables the interface to automatically accept a self-signed public certificate from the server, and to automatically configure the interface to use that certificate when the data mover connects to a V7.1.8 or V8.1.2 or later server.
- VE_TSM_SSLREQUIRED. The default value DEFAULT enables existing session-security connections to servers earlier than V7.1.8 or V8.1.2, and automatically configures the interface to securely connect to a V7.1.8 or V8.1.2 or later server by using TLS for authentication.

**Uses cases for default security settings**

- First, the server is upgraded to V7.1.8 or V8.1.2 or later. Then, Data Protection for VMware is upgraded. The existing data mover and VMCLI nodes *are not* using SSL communications:
  - No changes are required to the security options for the data mover and VMCLI nodes.
  - The configuration is automatically updated to use TLS when the nodes authenticate with the server.
- First, the server is upgraded to V7.1.8 or V8.1.2 or later. Then, Data Protection for VMware is upgraded. The existing data mover and VMCLI nodes *are* using SSL communications:

- No changes are required to the security options for the data mover and VMCLI nodes.

- SSL communication with existing server public certificate continues to be used.

- SSL communication is automatically enhanced to use the TLS level that is required by the server.

- First, Data Protection for VMware is upgraded to V7.1.8 or V8.1.2 or later. Then, the server is upgraded later. The existing data mover and VMCLI nodes *are not* using SSL communications:

   - No changes are required to the security options for the data mover and VMCLI nodes.

   - Existing authentication protocol continues to be used to servers at levels earlier than V7.1.8 or V8.1.2.

   - The configuration is automatically updated to use TLS when the nodes authenticate with the server after the server is updated to V7.1.8 or V8.1.2 or later.

- First, Data Protection for VMware is upgraded to V7.1.8 or V8.1.2 or later. Then, the server is upgraded later. The existing data mover and VMCLI nodes *are* using SSL communications:

   - No changes are required to the security options for the data mover and VMCLI nodes.

   - SSL communication with existing server public certificate continues to be used with servers at levels earlier than V7.1.8 or V8.1.2.

   - SSL communication is automatically enhanced to use the TLS level that is required by the server after the server is updated to V7.1.8 or V8.1.2 or later.

- First, Data Protection for VMware is upgraded to V7.1.8 or V8.1.2 or later. Then, the data mover and VMCLI nodes connect to multiple servers. The servers are upgraded at different times:

   - No changes are required to the security options for the data mover and VMCLI nodes.

   - The data mover and VMCLI nodes use existing authentication and session security protocol to servers at versions earlier than V7.1.8 or V8.1.2, and automatically upgrade to use TLS authentication when initially connecting to a server at V7.1.8 or V8.1.2 or later. Session security is managed per server.

- New client installation, server is at V7.1.8 or V8.1.2 or later:

   - Configure Data Protection for VMware according to a new installation.

   - Default values for the security options automatically configure the data mover and VMCLI nodes for TLS-encrypted session authentication.

   - Set the SSL parameter to the Yes value if encryption of all data transfers between the client and the server is required.

- New client installation, server is at a version earlier than V7.1.8 or V8.1.2:

   - Configure the client according to a new client installation.

   - Accept the default values for client session-security parameters if SSL encryption of all data transfers is not required.

     - Non-SSL authentication protocol is used until the server is upgraded to V7.1.8 or V8.1.2 or later.

   - Set the SSL parameter to the Yes value if encryption of all data transfers between the data mover and the server is required, and proceed with the manual configuration for SSL.

     - See Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer for configuration instructions.

     - SSL communication is automatically enhanced to use the TLS level that is required by the server after the server is updated to V7.1.8 or V8.1.2 or later.

**Configuring without automatic certificate distribution**

This scenario details the configuration options that impact the security of the data mover and VMCLI nodes when automatic distribution of certificates from the server is not acceptable. For example, automatic distribution of certificates from the server is not acceptable if the server is configured to use LDAP authentication or it is necessary that certificates are signed by a certificate authority (CA).

**Options that affect session security**

The options for security settings are the same as those described in "Configuring by using the default security settings (fast path)" on page 50, with the exception that you must set the SSLACCEPTCERTFROMSERV option to No to ensure that the data mover node does not automatically accept a self-signed public certificate from the server when the node first connects to a V7.1.8 or V8.1.2 or later server.

**Uses cases for configuring data mover nodes without automatic certificate distribution**

If automatic certificate distribution is not possible or wanted, use the dsmcert utility to import the certificate. Obtain the necessary certificate from the IBM Spectrum Protect server or from a CA. The CA can be from a company such as VeriSign or Thawte, or an internal CA that is maintained within your company.

If the data mover and VMCLI nodes are on the same machine, only one certificate is required. If the nodes are on separate machines, a certificate is required one each machine.

- First, the server is upgraded to V7.1.8 or V8.1.2. Then, Data Protection for VMware is upgraded. The existing data mover nodes *are not* using SSL communications:
  - Set the SSLACCEPTCERTFROMSERV option with the value No.
  - Obtain the necessary certificate from the IBM Spectrum Protect server or from a CA and use the dsmcert utility to import the certificate. See Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer for configuration instructions.
- First, the server is upgraded to V7.1.8 or V8.1.2. Then, Data Protection for VMware is upgraded. The existing data mover nodes *are* using SSL communications:
  - No changes are required to the security options for the data mover nodes. If the nodes already have a server certificate for SSL communication, the SSLACCEPTCERTFROMSERV option does not apply.
  - SSL communication with existing server public certificate continues to be used.
  - SSL communication is automatically enhanced to use the TLS level that is required by the server.
- First, Data Protection for VMware is upgraded to V7.1.8 or V8.1.2. Then, the server is upgraded later. The existing data mover nodes *are not* using SSL communications:
  - Set the SSLACCEPTCERTFROMSERV option with the value No.
  - Existing authentication protocol continues to be used to servers at levels earlier than V7.1.8 or V8.1.2.
  - Before the data mover nodes connect to a V7.1.8 or V8.1.2 or later server:
    - Obtain the necessary certificate from the IBM Spectrum Protect server or from a CA and use the dsmcert utility to import the certificate. See Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer for configuration instructions.
- First, Data Protection for VMware is upgraded to V7.1.8 or V8.1.2. Then, the server is upgraded later. The existing data mover nodes *are* using SSL communications
  - No changes are required to the security options for the data mover nodes. If the nodes already have a server certificate for SSL communication, the SSLACCEPTCERTFROMSERV option does not apply.
  - SSL communication with existing server public certificate continues to be used with servers at levels earlier than V7.1.8 or V8.1.2.
  - SSL communication is automatically enhanced to use the TLS level that is required by the server after the server is updated to V7.1.8 or V8.1.2 or later.
- First, Data Protection for VMware is upgraded to V7.1.8 or V8.1.2. Then, the data mover nodes connect to multiple servers. The servers are upgraded at different times:
  - Set the SSLACCEPTCERTFROMSERV option with the value No.
  - Existing authentication protocol continues to be used to servers at levels earlier than V7.1.8 or V8.1.2.

- – Before the data mover nodes connect to a V7.1.8 or V8.1.2 later server, or when SSL communication is required at any server level:

    - Obtain the necessary certificate from the IBM Spectrum Protect server or from a CA and use the dsmcert utility to import the certificate. See Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer for configuration instructions.

- – The data mover nodes use existing authentication and session security protocol to servers at versions earlier than V7.1.8 or V8.1.2, and automatically upgrade to use TLS authentication when initially connecting to a server at V7.1.8 or V8.1.2 or later. Session security is managed per server.

- New Data Protection for VMware installation, server is at V7.1.8 or V8.1.2 or later:

    - – Configure Data Protection for VMware according to a new installation.

    - – Set the SSLACCEPTCERTFROMSERV option with the value No.

    - – Obtain the necessary certificate from the IBM Spectrum Protect server or from a CA and use the dsmcert utility to import the certificate. See Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer for configuration instructions.

    - – Set the SSL parameter to the Yes value if encryption of all data transfers between the data mover and the server is required.

- New Data Protection for VMware installation, server is at a version earlier than V7.1.8 or V8.1.2, SSL-encrypted sessions *are* required:

    - – Configure Data Protection for VMware according to a new installation.

    - – Set the SSL parameter to the Yes value.

    - – Obtain the necessary certificate from the IBM Spectrum Protect server or from a CA and use the dsmcert utility to import the certificate. See Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer for configuration instructions.

- New Data Protection for VMware installation, server is at a version earlier than V7.1.8 or V8.1.2, SSL-encrypted sessions *are not* required:

    - – Configure Data Protection for VMware according to a new installation.

    - – Set the SSLACCEPTCERTFROMSERV option with the value No.

        - Non-SSL authentication protocol is used until the server is upgraded to V7.1.8 or V8.1.2 later.

    - – Before the data mover nodes connect to a V7.1.8 or V8.1.2 or later server:

        - Obtain the necessary certificate from the IBM Spectrum Protect server or from a CA and use the dsmcert utility to import the certificate. See Configuring Tivoli Storage Manager client/server communication with Secure Sockets Layer for configuration instructions.

### Configuring Data Protection for VMware vSphere GUI communication using the Transport Layer Security

The Data Protection for VMware vSphere GUI uses the Transport Layer Security (TLS) protocol to provide secure communication with web browsers; the VMware vCenter Server; and, optionally, the IBM Spectrum Protect server.

**About this task**

For communication with web browsers and the VMware VCenter Server, the TLS protocol is always enabled. During the installation of Data Protection for VMware, a self-signed TLS digital certificate is generated and is then used for connection.

You can also use a certificate that is signed by a certificate authority (CA) to communicate with web browsers. Data Protection for VMware To use a certificate from a CA, see Using a third-party certificate for web browser sessions.

For communication with the IBM Spectrum Protect server, the use of the TLS protocol depends on the version of the server.

**If you are using IBM Spectrum Protect server V7.1.7 or V8.1.1 or earlier**
> The use of the TLS protocol to communicate with the server is optional. You can manually enable the Data Protection for VMware vSphere GUI to communicate with the server over the TLS protocol by creating or updating the truststore and importing a certificate as described in "Enabling secure communication with the IBM Spectrum Protect server" on page 55

**If you are using IBM Spectrum Protect server V7.1.8 or V8.1.2 later**
> The TLS protocol is required. In most cases, the truststore is created automatically on first use by using the default security settings that are described in "Configuring by using the default security settings (fast path)" on page 50. However, in some scenarios, you might be required to manually create the truststore. .
>
> **Important:** The fast path scenario automatically obtains certificates when the Data Protection for VMware vSphere GUI communicates with the sever for the first time, assuming that the IBM Spectrum Protect server **SESSIONSECURITY** parameter is set to **TRANSITIONAL**, which is the default value at first connection. After the GUI connects to the server, **SESSIONSECURITY** parameter is set to **STRICT**. Because the GUI uses the server administrator ID to connect to the server, if another entity has used that ID to connect, an error messages will display in the GUI when trying to connect to the server. To resolve this issue, set the **SESSIONSECURITY** parameter to back to **TRANSITIONAL**.

**Enabling secure communication with the IBM Spectrum Protect server**
If you are using IBM Spectrum Protect server V7.1.7 or earlier or V8.1.2 or earlier, connection to the server by using the TLS protocol is optional and if you want to enable the Data Protection for VMware vSphere GUI communicate with the server by using the protocol, you must enable the communication manually.

**Before you begin**
Obtain a copy of the certificate from the server administrator.

**About this task**

If you are using server V7.1.8 or V8.1.2 or later, the TLS protocol is required and a truststore with a certificate is created automatically on first use by using default security settings that are described in "Configuring by using the default security settings (fast path)" on page 50. However, in some scenarios, you might be required to manually create the truststore and configure the Data Protection for VMware vSphere GUI as described in this topic.

The following procedure uses the Java™ key and certificate management tool **keytool**.

On Linux operating systems, the tool is in the `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/` directory.

On Microsoft Windows operating systems, the tool is in the `C:\Program Files\Common Files \Tivoli\TSM\jvm80516\jre\bin` directory.

You might need to specify the full path when you run the **keytool** command.

**Procedure**

1. From the command line, change the directory to the truststore location:

    - On Linux: `/opt/tivoli/tsm/tdpvmware/common/scripts/`

    - On Windows: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\`

2. Create the truststore and import the certificate with the following command:

    ```
    keytool -importcert -alias my-cert -file cert.pem -keystore
    tsm-ve-truststore.jks -storepass password
    ```

    Where:

    **-alias *my-cert***
        The unique alias that identifies the certificate in the truststore.

**-file** *cert.pem*
> The file that contains the server self-signed certificate or the CA root certificate.

**-storepass** *password*
> The keystore password. Ensure that you remember this password for future use.

3. Start the Data Protection for VMware vSphere GUI and go to the **Configuration** window.

   - If you are creating an initial configuration, click **Tasks** > **Run IBM Spectrum Protect Configuration Wizard** and go to the **Server Credentials** page.

   - If you are modifying an existing configuration, click **Tasks** > **Edit IBM Spectrum Protect Configuration** and go to the **Server Credentials** page.

4. Enter the port number in the **IBM Spectrum Protect Admin Port** field. This is the server port that allows administrative connections using SSL or TLS.

5. Select **Use encrypted communications on the admin port**.

6. If you want to use this setting for future GUI sessions, select **Save the administrator ID, password, and port settings**.

7. Click **OK** to apply the changes.

**Using a certificate from a certificate authority**
To use a certificate that is signed by a certificate authority (CA), you must complete multiple steps.

**About this task**

The following procedures use the standard key and certificate management tool called **keytool**.

On Linux operating systems, it is located in the `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/` directory.

On Microsoft Windows operating systems, it is located in the `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre` directory.

You might need to specify the full path when running **keytool** from the command line.

**Procedure**

1. Obtain access to the keystore.
2. Create a certificate signing request (CSR).
3. Send the certificate signing request to the certificate authority for signing.
4. Receive the signed certificate into the Data Protection for VMware vSphere GUI.

*Obtaining access to the keystore*
Certificates are stored in a Java keystore. The keystore contents are protected with a password. To manipulate the certificates in the keystore, you must obtain access to the keystore.

**About this task**

The default self-signed certificate and keystore password are generated automatically during installation, so you are unlikely to know the initial password.

Complete the following procedure to replace the original keystore with a new keystore and a new self-signed certificate. The new keystore is protected by a password of your choice.

If you already know the keystore password, skip this procedure.

**Procedure**

1. Stop the Data Protection for VMware vSphere GUI service.
2. From the command line, change the directory to the keystore location.

- On Linux: /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/
resources/security/
- On Windows: C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources
\security\

3. Make a backup copy of the keystore file (key.jks) by renaming it or moving it to a different location.

4. Create a new keystore and a new self-signed certificate by issuing the following command:

```
keytool -genkeypair -alias vekey -dname
CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM -keyalg RSA
-sigalg SHA256withRSA -keysize 2048 -validity days -keystore
key.jks -storepass password -keypass password
```

Where:

**-dname CN=*fqdn*,OU=Tivoli_Storage_Manager_for_VMware,O=IBM**
*fqdn* is the DNS name or fully qualified domain name of the computer on which the Data Protection for VMware vSphere GUI is installed.

**-validity *days***
The certificate validity period.

**-storepass *password***
The keystore password. Ensure that you remember this password for future use.

**-keypass *password***
The private key password for the certificate. This password must match the keystore password.

5. Encode the keystore password by using the **securityUtility** tool. Issue the following command.

- On Linux: /opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility
encode
- On Windows: C:\IBM\SpectrumProtect\webserver\bin\securityUtility.bat encode

Enter your keystore password when prompted and then save the output (for example, copy it to the clipboard).

6. Open the bootstrap.properties file in an editor and set the veProfile.keystore.pswd property to the encoded value from the previous step.

The bootstrap.properties file is in the following location:

- On Linux: /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/
- On Windows: C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\

7. Start the Data Protection for VMware vSphere GUI service.

**Related reference**
"Starting and running services for Data Protection for VMware" on page 74
By default, when you start the Windows operating system, recovery agent is started under the Local System Account.

### *Creating a certificate signing request*
After you obtained access to the keystore, you must create a certificate signing request (CSR).

**Procedure**

Complete the following steps to create a CSR:

1. From the command line, change the directory to the keystore location.

- On Linux: /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/
resources/security/
- On Windows: C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources
\security\

2. Create a new certificate by issuing the following command:

```
keytool -genkeypair -alias mykey -dname
CN=fqdn,OU=unit,O=organization -keyalg RSA -sigalg SHA256withRSA
-keysize 2048 -validity days -keystore key.jks -storepass
password -keypass password
```

Where:

**-alias** *mykey*
> *mykey* is the unique alias that identifies the certificate in the keystore. It is renamed when the signed certificate is received.

**-dname CN=*fqdn*,OU=*unit*,O=*organization***
> *fqdn* is the DNS name or fully qualified domain name of the computer on which the Data Protection for VMware vSphere GUI is installed.
>
> *Unit* and *organization* are the organization information that is required by your policies or by the certificate authority.

**-validity *days***
> The certificate validity period.

**-storepass *password***
> The keystore password. If you do not know or forgot the keystore password, see "Obtaining access to the keystore" on page 56.

**-keypass *password***
> The private key password for the certificate. This password must match the keystore password.

3. Create a CSR by issuing the following command:

```
keytool -certreq -alias mykey -file certreq.pem -keystore key.jks
```

Where:

**-alias *mykey***
> The certificate alias from the previous step.

**-file *certreq.pem***
> The file to store the certificate signing request.

### *Sending the certificate signing request to the certificate authority*
After you create the certificate request (`certreq.pem`), you must send it to the certificate authority for signing. Follow the specific instructions from the certificate authority.

### *Receiving the signed certificate*
After you get the signed certificate from the certificate authority (CA), you must receive the certificate in the keystore.

**Procedure**

To receive the signed certificate, complete the following steps:

1. From the command line, change the directory to the keystore location.

   - On Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - On Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`

2. Copy the files that you received from the CA to this location. These files include the CA root certificate, intermediate CA certificates (if any), and the signed certificate for the Data Protection for VMware vSphere GUI.

3. Stop the Data Protection for VMware vSphere GUI service.

4. Make a backup copy of the keystore file (`key.jks`) by copying it to a different name or location.

5. Import the intermediate CA certificates, if any, with the following command. When you are prompted to trust the certificates, answer *yes*. Repeat this step for multiple intermediate CAs as needed.

```
keytool -importcert -alias ca-intermediate -file intermediate.pem
-keystore key.jks -storepass password
```

Where:

**-alias *ca-intermediate***
The unique alias that identifies the certificate in the keystore. Each intermediate certificate must have a unique alias.

**-file *intermediate.pem***
The intermediate certificate file that is obtained from the CA.

**-storepass *password***
The keystore password.

6. Import the CA root certificate by issuing the following command. When you are prompted to trust this certificate, answer *yes*.

```
keytool -importcert -alias ca-root -file root.pem -keystore
key.jks -storepass password
```

Where:

**-alias *ca-root***
The unique alias that identifies the certificate in the keystore.

**-file *root.pem***
The root certificate file obtained from the CA.

**-storepass *password***
The keystore password.

7. Import the signed certificate by issuing the following command:

```
keytool -importcert -alias mykey -file signedcert.pem -keystore
key.jks -storepass password
```

Where:

**-alias *mykey***
The alias for the signed certificate. The alias must be the same one that was used when you created the keystore. For further detail on creating a new keystore and a new self-signed certificate , see Obtaining access to the keystore.

**-file *signedcert.pem***
The signed certificate file received from the CA.

**-storepass *password***
The keystore password.

8. Start the Data Protection for VMware vSphere GUI service.

**Related reference**
"Starting and running services for Data Protection for VMware" on page 74
By default, when you start the Windows operating system, recovery agent is started under the Local System Account.

## VMware vCenter Server user privilege requirements

Certain VMware vCenter Server privileges are required to run Data Protection for VMware operations.

**vCenter Server privileges required to protect VMware datacenters with the web-browser view for the Data Protection for VMware vSphere GUI**

The vCenter Server user ID that signs on to the browser view for the Data Protection for VMware vSphere GUI must have sufficient VMware privileges to view content for a datacenter that is managed by the GUI.

For example, a VMware vSphere environment contains five datacenters. A user, "jenn", has sufficient privileges for only two of those datacenters. As a result, only those two datacenters where sufficient

privileges exist are visible to "jenn" in the views. The other three datacenters (where "jenn" does not have privileges) are not visible to the user "jenn".

The VMware vCenter Server defines a set of privileges collectively as a role. A role is applied to an object for a specified user or group to create a privilege. From the VMware vSphere web client, you must create a role with a set of privileges. To create a vCenter Server role for backup and restore operations, use the VMware vSphere Client **Add a Role** function.

If you want to propagate the privileges to all datacenters within the vCenter, specify the vCenter Server and select the `propagate to children` check box. Otherwise, you can limit the permissions if you assign the role to the required datacenters only with the `propagate to children` check box selected. Enforcement for the browser GUI is at the datacenter level.

The following example shows how to control access to datacenters for two VMware user groups. First, create a role that contains all of the privileges defined in technote 7047438. The set of privileges in this example are identified by the role named "TDPVMwareManage". Group 1 requires access to manage virtual machines for the `Primary1_DC` and `Primary2_DC` datacenters. Group 2 requires access to manage virtual machines for the `Secondary1_DC` and `Secondary2_DC` datacenters.

For Group 1, assign the "TDPVMwareManage" role to the `Primary1_DC` and `Primary2_DC` datacenters. For Group 2, assign the "TDPVMwareManage" role to the `Secondary1_DC` and `Secondary2_DC` datacenters.

The users in each VMware user group can use the Data Protection for VMware GUI to manage virtual machines in their respective datacenters only.

**Tip:** When you create a role, consider adding extra privileges to the role that you might need later to complete other tasks on objects.

**vCenter Server privileges required to use the data mover**

The IBM Spectrum Protect data mover that is installed on the vStorage Backup server (the data mover node) requires the VMCUser and VMCPw options. The VMCUser option specifies the user ID of the vCenter or ESX server that you want to back up, restore, or query. The required privileges that are assigned to this user ID (VMCUser) ensure that the client can run operations on the virtual machine and the VMware environment. This user ID must have the VMware privileges that are described in the above technote.

To create a vCenter Server role for backup and restore operations, use the VMware vSphere Client **Add a Role** function. You must select the `propagate to children` option when you add privileges for this user ID (VMCUser). In addition, consider adding other privileges to this role for tasks other than backup and restore. For the VMCUser option, enforcement is at the top-level object.

**vCenter Server privileges required to protect VMware datacenters with the IBM Spectrum Protect vSphere Client plug-in view for the Data Protection for VMware vSphere GUI**

The IBM Spectrum Protect vSphere Client plug-in requires a set of privileges that are separate from the privileges that are required to sign in to the GUI.

During the installation the following custom privileges are created for the IBM Spectrum Protect vSphere Client plug-in:

- **Datacenter** > **IBM Data Protection**
- **Global** > **Configure IBM Data Protection**

Custom privileges that are required for the IBM Spectrum Protect vSphere Client plug-in are registered as a separate extension. The privileges extension key is `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

These privileges allow the VMware administrator to enable and disable access to IBM Spectrum Protect vSphere Client plug-in content. Only users with these custom privileges on the required VMware object can access the IBM Spectrum Protect vSphere Client plug-in content. One IBM Spectrum Protect vSphere Client plug-in is registered for each vCenter Server and is shared by all GUI hosts that are configured to support the vCenter Server.

From the VMware vSphere web client, you must create a role for users who can complete data protection functions for virtual machines by using the IBM Spectrum Protect vSphere Client plug-in. For this role, in addition to the standard virtual machine administrator role privileges required by the web client, you must specify the **Datacenter** > **IBM Data Protection** privilege. For each datacenter, assign this role for each user or user group where you want to grant permission for the user to manage virtual machines.

The **Global** > **IBM Data Protection** privilege is required for the user at the vCenter level. This privilege allows the user to manage, edit, or clear the connection between the vCenter Server and the Data Protection for VMware vSphere GUI web server. Assign this privilege to administrators that are familiar with the Data Protection for VMware vSphere GUI that protects their respective vCenter Server. Manage your IBM Spectrum Protect vSphere Client plug-in connections on the extension **Connections** page.

The following example shows how to control access to datacenters for two user groups. Group 1 requires access to manage virtual machines for the `NewYork _DC` and `Boston_DC` datacenters. Group 2 requires access to manage virtual machines for the `LosAngeles_DC` and `SanFranciso_DC` datacenters.

From the VMware vSphere client, create for example the "IBMDataProtectManage" role, assign the standard virtual machine administrator role privileges and also the **Datacenter** > **IBM Data Protection** privilege.

For Group 1, assign the "IBMDataProtectManage" role to the `NewYork _DC` and `Boston_DC` datacenters. For Group 2, assign the "IBMDataProtectManage" role to the `LosAngeles_DC` and `SanFranciso_DC` datacenters.

The users in each group can use the IBM Spectrum Protect vSphere Client plug-in in the vSphere web client to manage virtual machines in their respective datacenters only.

### Issues related to insufficient permissions

When the web browser user does not have sufficient permissions for any datacenter, access to the view is blocked. Instead, the error message GVM2013E is issued to advise that the user is not authorized to access any managed datacenters due to insufficient permissions. Other new messages are also available that inform users of issues that result from insufficient permissions. To resolve any permissions-related issues, make sure that the user role is set up as described in the previous sections. The user role must have all privileges that are identified in the Required privileges vCenter Server user ID and data mover table, and these privileges must be applied at the datacenter level with the `propagate to children` check box.

When the IBM Spectrum Protect vSphere Client plug-in user does not have sufficient permissions for a datacenter, the data protection functions for that datacenter and its content are made unavailable in the extension.

When the IBM Spectrum Protect user ID (specified by the VMCUser option) contains insufficient permissions for a backup and restore operation, the following message is shown:

```
ANS9365E VMware vStorage API error.
"Permission to perform this operation was denied."
```

When the IBM Spectrum Protect user ID contains insufficient permissions to view a machine, the following messages are shown:

```
Backup VM command started.  Total number of virtual machines to process: 1
ANS4155E Virtual Machine 'tango' could not be found on VMware server.
ANS4148E Full VM backup of Virtual Machine 'foxtrot' failed with RC 4390
```

For further information on the use of privileges, see the note on **vCenter Server privileges required for the Data Protection for VMware vSphere GUI and data mover**.

To retrieve log information through the VMware Virtual Center Server for permission problems, complete these steps:

1. In **vCenter Server Settings**, select **Logging Options** and set "**vCenter Logging** to **Trivia (Trivia)**.
2. Re-create the permission error.
3. Reset **vCenter Logging** to its previous value prevent recording excessive log information.

4. In **System Logs**, look for the most current vCenter Server log (`vpxd-wxyz.log`) and search for the string `NoPermission`. For example:

```
[2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
Throw: vim.fault.NoPermission
```

This log message indicates that the user ID did not contain sufficient permissions to create a snapshot (`createSnapshot`).

# Data Protection for VMware vSphere GUI user roles

The availability of Data Protection for VMware vSphere GUI functions is based on the authority level that is assigned to your IBM Spectrum Protect administrator ID.

The administrator ID must match the node name. In earlier product releases, the **REGISTER NODE** command automatically created an administrative user ID whose name matched the node name. Beginning with IBM Spectrum Protect V8.1, the **REGISTER NODE** command does not automatically create an administrative user ID that matches the node name.

When registering a new node, the IBM Spectrum Protect server administrator must specify the `userid` parameter with the **REGISTER NODE** server command:

```
REGISTER NODE node_name password userid=user_id
```

Where the node name and the administrative user ID must be the same. For example:

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

By default, the node has client owner authority.

The tasks that you can run with the Data Protection for VMware vSphere GUI are based on the privilege class that is assigned to the administrator ID.

When the administrator ID does not have unrestricted policy domain privileges, you cannot register new nodes or set their proxy relationship on the IBM Spectrum Protect server. If you do not enter an administrator ID, a macro script is created so you can run on the IBM Spectrum Protect server.

An IBM Spectrum Protect administrator ID is requested when configuring the Data Protection for VMware vSphere GUI. This table lists the functions that are available based on the privilege class assigned to that ID:

- A Yes value indicates available function for the user role.
- A No value indicates function that is not available for the user role.

To view your current Data Protection for VMware vSphere GUI role, hover the cursor over your user ID in the navigation bar.

*Table 11. Available functions based on IBM Spectrum Protect Administrator ID privilege requirements*

|  | **Operator** | **Operator with Reporting** | **Restricted Administrator** | **Administrator** |
|---|---|---|---|---|
| *Summary* | Run now backup and restore | Operator plus reporting | Operator plus reporting and schedule operations for listed policy domains | All roles, including initial configuration |

| | **Operator** | **Operator with Reporting** | **Restricted Administrator** | **Administrator** |
|---|---|---|---|---|
| **IBM Spectrum Protect Admin ID Privilege Class** | None | One of the following privilege classes:<br>• Storage<br>• Operator<br>• Analyst | Policy (Restricted) or one of the following privilege classes:<br>• Storage<br>• Operator<br>• Analyst | Policy (Unrestricted) or System |
| **Backup tab** | | | | |
| Manage **Run now** backup tasks | Yes | Yes | Yes | Yes |
| Manage **Scheduled** backup tasks | No[1] | No[1] | Yes, within policy domains | Yes |
| View **Run now** backup tasks | Yes | Yes | Yes | Yes |
| View **Scheduled** backup tasks | No | Yes | Yes | Yes |
| Delete a **Scheduled** backup task | No | No | Yes within policy domains | Yes |
| **Restore tab** | | | | |
| Run a **Restore** task | Yes | Yes | Yes | Yes |
| **Reports tab** | | | | |
| Events | No | Yes | Yes | Yes |
| Recent Tasks | Yes | Yes | Yes | Yes |
| Backup Status | No | Yes | Yes | Yes |
| Application Protection | No | Yes | Yes | Yes |
| Datacenter Occupancy | No | Yes | Yes | Yes |
| **Configuration tab** | | | | |
| Node Registration (**Configuration Status** -> **Run Configuration Wizard**) | No | No | No[2] | Yes |
| Change IBM Spectrum Protect Admin ID Credentials (**Configuration Status** -> **Edit Configuration**) | Yes | Yes | Yes | Yes |

| | Operator | Operator with Reporting | Restricted Administrator | Administrator |
|---|---|---|---|---|
| Change VMCLI Node Password (**Configuration Status** -> **Edit Configuration**) | No | No | Yes | Yes |
| Change GUI Domains (**Configuration Status** -> **Edit Configuration**) | Yes[3] | Yes[3] | Yes[3] | Yes |
| Change Data Mover Nodes (**Configuration Status** -> **Edit Configuration**) | No | No | No[2] | Yes |
| Change Mount Proxy Nodes (**Configuration Status** -> **Edit Configuration**) | No | No | No[2] | Yes |

1. You cannot register the node because an unrestricted domain policy is required.
2. You can add or remove VMware datacenters and register datacenter nodes.

To view the IBM Spectrum Protect administrator ID authority level and corresponding Data Protection for VMware vSphere GUI role:

1. Go to the **Configuration** window.
2. Click **Edit Configuration**.
3. The relevant information is shown on the **Spectrum Protect Server Credentials** page.

**Important:**

- If the IBM Spectrum Protect administrator ID authority level changes on the IBM Spectrum Protect server, the Data Protection for VMware vSphere GUI must be restarted to reflect this change.
- When changing the **User Role**, you must click **OK** to save your changes before going to another **Configuration Settings** page or attempting another configuration change. Otherwise your **User Role** changes do not take effect.

## Data Protection for VMware GUI registration keys

Depending on the options you select during installation, you can access the Data Protection for VMware GUI by using different methods. Registration keys are created for the Data Protection for VMware GUIs.

The phrase "Data Protection for VMware GUI" applies to the following GUIs:

- Data Protection for VMware vSphere GUI accessed in a web browser
- IBM Spectrum Protect vSphere Client plug-in in the vSphere Web Client GUI

IBM Spectrum Protect vSphere Client plug-in registration key is `com.ibm.tsm.tdpvmware.IBMDataProtection`. This key is registered when you select the **Register the vSphere Web Client extension** check box during the installation. A single instance of the IBM Spectrum Protect vSphere Client plug-in is registered per vCenter server.

A registration key is not created for the Data Protection for VMware vSphere GUI that is accessed in a web browser.

To view the registration keys, log in to the VMware Managed Object Browser (MOB). After you log in to the MOB, go to **Content→Extension Manager** to view the registration keys.

# Configuring the recovery agent GUI

Instructions about how to set up the recovery agent GUI for mount, file restore, or instant restore operations is provided.

**Before you begin**
These configuration tasks must be completed before you attempt an operation in the recovery agent GUI.

**Important:** Information about how to complete tasks with the recovery agent GUI is provided in the online help that is installed with the GUI. Click **Help** in any of the GUI windows to open the online help for task assistance.

**Procedure**

1. Log on to the system where you want to restore files. recovery agent must be installed on the system.
2. Click **Select TSM server** in the recovery agent GUI to connect to an IBM Spectrum Protect server.

   When the recovery agent is installed on the same system as the Data Protection for VMware vSphere GUI, and the applications were successfully configured with the Data Protection for VMware vSphere GUI configuration wizard, the following conditions exist:

   - The data mover node and IBM Spectrum Protect server are populated in the recovery agent **TSM Server** field.
   - The following fields are populated in the **TSM Server information** panel:
     - **Authentication node** contains a list of available data mover nodes.
     - **Target node** contains a list of data center nodes that are available for the selected data mover node.

   When only one data mover node was defined locally with the configuration wizard, the recovery agent uses that node to authenticate when started.

   The recovery agent remembers the last node name that connected to the IBM Spectrum Protect server. If **Use Password access generate** is selected for this node (the last node name to connect), the recovery agent uses these credentials to connect to the IBM Spectrum Protect server on startup. If no previous connection to the IBM Spectrum Protect server was done, and only one data mover node and one data center node are configured with the wizard, the recovery agent uses these credentials to connect to the IBM Spectrum Protect server on startup.

   Specify the following options:

   **Server address**
       Enter the IP address or host name of the IBM Spectrum Protect.

   **Server port**
       Enter the port number that is used for TCP/IP communication with the server. The default port number is 1500.

   Node access method:

   **Asnodename**
       Select this option to use a proxy node to access the VM backups that are in the target node. The proxy node is a node that is granted "proxy" authority to perform operations on behalf of the target node.

       Typically, the IBM Spectrum Protect administrator uses the `grant proxynode` command to create the proxy relationship between two existing nodes.

       If you select this option, complete the following steps:

       a. Enter the name of the target node (the node where the VM backups are located) in the **Target Node** field.

b. Enter the name of the proxy node in the **Authentication node** field.

c. Enter the password for the proxy node in the **Password** field.

d. Click **OK** to save these settings and exit the IBM Spectrum Protect information dialog.

When you use this method, the recovery agent user knows only the proxy node password, and the target node password is protected.

**Fromnode**

Select this option to use a node with access limited only to the snapshot data of specific VMs in the target node.

Typically, this node is given access from the target node that owns the VM backups by using the `set access` command:

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

For example, this command gives the node named `myMountNode` the authority to restore files from the VM named `myTestVM`:

```
set access backup -TYPE=VM myTestVM myMountNode
```

If you select this option, complete the following steps:

a. Enter the name of the target node (the node where the VM backups are located) in the **Target Node** field.

b. Enter the name of the node that is given limited access in the **Authentication node** field.

c. Enter the password for the node that is given limited access in the **Password** field.

d. Click **OK** to save these settings and exit the IBM Spectrum Protect information dialog.

When you use this method, you can see a complete list of backed-up VMs. However, you can restore only those VM backups to which the node was granted access. In addition, the snapshot data is not protected from expiration on the server. As a result, instant restore is not supported in this method.

**Direct**

Select this option to authenticate directly to the target node (the node where the VM backups are located).

If you select this option, complete the following steps:

a. Enter the name of the target node (the node where the VM backups are located) in the **Authentication node** field.

b. Enter the password for the target node in the **Password** field.

c. Click **OK** to save these settings and exit the IBM Spectrum Protect information dialog.

**Use Password access generate**

When this option is selected and the password field is empty, the recovery agent authenticates with an existing password that is stored in the registry. If not selected, you must manually enter the password.

To use this option, you must first manually set an initial password for the node to which the option applies. You must specify the initial password when you connect to the IBM Spectrum Protect node for the first time by entering the password in the **Password** field and selecting the **Use Password access generate** check box.

However, when you use the local data mover node as the **Authentication node**, the password might already be stored in the registry. As a result, select the **Use Password access generate** check box and do not enter a password.

recovery agent queries the specified server for a list of protected VMs, and shows the list.

3. Set the following mount, backup, and restore options by clicking **Settings**:

**Virtual Volume write cache**
The recovery agent that is running on the Windows backup proxy host saves data changes that are created during instant restore and mount. These changes are saved on a virtual volume in the write cache. By default, the write cache is enabled and specifies the `C:\ProgramData\Tivoli\TSM\TDPVMware\mount\` path and the maximum cache size is 90% of the available space for the selected folder. To prevent the system volume from becoming full, change the write cache to a path on a volume other than the system volume.

**Folder for temporary files**
Specify the path where data changes are saved. The write cache must be on a local drive and cannot be set to a path on a shared folder. If the write cache is disabled or full, attempting to start an instant restore or mount session fails.

**Cache size**
Specify the size of the write cache. The maximum allowed cache size is 90% of the available space for the selected folder.

**Restriction:** To prevent any interruption during restore processing, exclude the write cache path from all antivirus software protection settings.

**Data Access**
Specify the type of data to be accessed. If you are using an offline device (such as tape or virtual tape library), you must specify the applicable data type.

**Storage type**
Specify one of the following storage devices from which to mount the snapshot:

**Disk/File**
The snapshot is mounted from a disk or file. This device is the default.

**Tape**
The snapshot is mounted from a tape storage pool. When this option is selected, it is not possible to mount multiple snapshots or run an instant restore operation.

**VTL**
The snapshot is mounted from an offline virtual tape library. Concurrent mount sessions on the same virtual tape library are supported.

**Note:** When the storage type is changed, you must restart the service for the changes to take effect.

**Disable expiration protection**
During a mount operation, the snapshot on the IBM Spectrum Protect server is locked to prevent it from expiring during the operation. Expiration might occur because another snapshot is added to the mounted snapshot sequence. This value specifies whether to disable expiration protection during the mount operation.

- To protect the snapshot from expiration, do not select this option. The snapshot on the IBM Spectrum Protect server is locked and the snapshot is protected from expiration during the mount operation.

- To disable expiration protection, select this option. This option is selected by default. The snapshot on the IBM Spectrum Protect server is not locked and the snapshot is not protected from expiration during the mount operation. As a result, the snapshot might expire during the mount operation. This expiration can produce unexpected results and negatively impact the mount point. For example, the mount point can become unusable or contain errors. However, expiration does not affect the current active copy. The active copy cannot expire during an operation.

  When the snapshot is on a target replication server, the snapshot cannot be locked because it is in read-only mode. A lock attempt by the server causes the mount operation to fail. To avoid the lock attempt and prevent such a failure, disable expiration protection by selecting this option.

**Read Ahead size (in 16-KB blocks)**

Specify the number of extra data blocks that are retrieved from the storage device after a read request is sent to a single block. The default values are as follows:

- Disk or file: 64
- Tape: 1024
- VTL: 64

The maximum value for any device is 1024.

**Read Ahead cache size (in blocks)**

Specify the size of the cache where the extra data blocks are stored. The default values are as follows:

- Disk or file: 10000
- Tape: 75000
- VTL: 10000

Since each snapshot has its own cache, make sure to plan how many snapshots are mounted or restored simultaneously. The cumulative cache size cannot exceed 75000 blocks.

**Driver timeout (seconds)**

This value specifies the amount of time to process data requests from the file system driver. If processing is not completed in time, the request is canceled and an error is returned to the file system driver. Consider increasing this value when you experience timeouts. For example, timeouts might occur when the network is slow, the storage device is busy, or multiple mount or instant restore sessions are being processed. The default values are as follows:

- Disk or file: 60
- Tape: 180
- VTL: 60

Click **OK** to save your changes and exit the **Settings**.

4. Verify that each IBM Spectrum Protect server node (that was specified with the `Asnodename` and `Fromnode` options) allows backups to be deleted.

   The recovery agent creates unused temporary objects during operations. The `BACKDELete=Yes` server option allows these objects to be removed so that they do not accumulate in the node.

   a) Log on to the IBM Spectrum Protect server and start an administrative client session in command-line mode:

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

   b) Enter this command:

   ```
   Query Node <nodename> Format=Detailed
   ```

   Make sure the command output for each node includes the following statement:

   ```
   Backup Delete Allowed?: Yes
   ```

   If this statement is not included, update each node with this command:

   ```
   UPDate Node <nodename> BACKDELete=Yes
   ```

   Run the `Query Node` command again for each node to verify that each node allows backups to be deleted.

5. When you use the Recover Agent in an iSCSI network, and the Recovery Agent does not use a data mover, go to the `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf file` and specify the `[IMOUNT]` tag and **Target IP** parameter:

```
[IMOUNT config]
Target IP=<IP address of the network card on the system
that exposes the iSCSI targets.>
```

For example:

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

After you add or change the Target IP parameter, restart the Recovery Agent GUI or Recovery Agent CLI.

## Enabling secure communication from the recovery agent to the IBM Spectrum Protect server

If the IBM Spectrum Protect server is configured to use the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol, you can enable the recovery agent to communicate with the server by using the protocol.

### Before you begin

Consider the following requirements before you begin configuration for secure communication to the server:

- Each server that is enabled for SSL must have a unique certificate. The certificate can be one of the following types:
  - A certificate that is self-signed by the server.
  - A certificate that is issued by a third-party certificate authority (CA) certificate. The CA certificate can be from a company such as Symantec or Thawte, or an internal certifcate that is maintained within your company.
- For performance reasons, use SSL or TLS only for sessions where security is required. Consider adding more processor resources on the server system to manage the increased requirements.
- For a client to connect to a server that is using TLS Version 1.2, the certificate signature algorithm must be Secure Hash Algorithm 1 (SHA-1) or later. If you are using a self-signed certificate to a server that is using TSL V1.2, you must use the `cert256.arm` certificate. Your IBM Spectrum Protect administrator might need to change the default certificate on the server.
- To disable security protocols that are less secure than TLS 1.2, add the **SSLDISABLELEGACYtls yes** option to the `C:\windows\system32\fb.opt` or `C:\Windows\SysWOW64\fb.opt` file. TLS 1.2 or later helps to prevent attacks by malicious programs.

### Enabling secure communication by using an IBM Spectrum Protect server self-signed certificate

If the IBM Spectrum Protect server is using a self-signed certificate, you must obtain a copy of that certificate from the server administrator and configure the recovery agent to communicate with the server by using the SSL or TLS protocol.

### About this task

Each server generates its own certificate. Version 6.3 and later servers generate files that are named `cert256.arm` if the server is using TLS 1.2 or later or `cert.arm` if the server is using an earlier version of SSL or TLS. Server versions earlier than V6.3 generate files that are named `cert.arm` regardless of the protocol. You must choose the certificate that is set as the default on the server.

The certificate file is stored on the server workstation in the server instance directory. For example, `C:\IBM\tivoli\tsm\server\bin\cert256.arm`. If the certificate file does not exist, the certificate file is created when you restart the server with these options set.

**Procedure**

To enable SSL or TLS communication from the recovery agent to the server by using a self-signed certificate:

1. Append the GSKit binary path and library path to the PATH environment variable on the client.

   For example:

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
        C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. If you are configuring SSL or TLS on the client for the first time, you must create the client local key database dsmcert.kdb.

   From the C:\Windows\SysWOW64 directory, run the **gsk8capicmd_64** command as shown in the following example:

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   The password that you provide is used to encrypt the key database. The password is automatically stored encrypted in the stash file (dsmcert.sth). The stash file is used by the client to retrieve the key database password.

3. Obtain the server self-signed certificate.

4. Import the certificate in to the dsmcert.kdb database. You must import the certificate for each client in to the dsmcert.kdb.

   From the C:\Windows\SysWOW64 directory, run the **gsk8capicmd_64** command as shown in the following example:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Server server_name self-signed
   key"
   -file path_to_certificate -format ascii -trust enable
   ```

   Multiple server certificates can be added to the dsmcert.kdb database so that the client can connect to different servers. Different certificates must have different labels. Use meaningful names for the labels.

   **Important:** For a disaster recovery of the server, if the certificate has been lost, the server automatically generates a new certificate. Each client must then import the new certificate.

5. After the server certificate is added to the dsmcert.kdb database, add the `ssl yes` option to the C:\Windows\SysWOW64\fb.opt file and update the value of the `tcpport` option.

   **Important:**

   The server is normally set up for SSL and TLS connections on a different port than non-SSL and TLS connections. Do not specify a non-SSL or TLS port number for the `tcpport` value. If the value of `tcpport` is incorrect, the recovery agent cannot connect to the server.

   You cannot connect to a non-SSL or TLS port with a recovery agent that is enabled for SSL or TLS or connect a SSL or TLS port to a recovery agent that is not enabled for SSL or TLS.

6. Set the correct SSL or TLS ports in the following recovery agent configuration files:

   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

**Enabling secure communication by using a third-party certificate**
If the IBM Spectrum Protect server is using a third-party certificate authority (CA), you must obtain the CA root certificate.

**About this task**

If the certificate was issued by a CA such as Symantec or Thawte, the client is ready for SSL or TLS and you can skip the following configuration steps. For a list of preinstalled CA root certificates, search for **Certificate Authorities root certificates** on the IBM Knowledge Center.

If the certificate was not issued by a preinstalled root certificate or is an internal CA certificate that is maintained within your company, you must configure the recovery agent to communicate with the server by using the SSL or TLS protocol.

**Procedure**

To enable SSL or TLS communication from the recovery agent to the server by using a CA certificate:

1. Append the GSKit binary path and library path to the PATH environment variable.

   For example:

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. If you are configuring SSL or TLS on the client for the first time, you must create the client local key database dsmcert.kdb.

   For clients, from the C:\Windows\SysWOW64 directory, run the **gsk8capicmd_64** command as shown in the following example:

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   The password that you provide is used to encrypt the key database. The password is automatically stored encrypted in the stash file (dsmcert.sth). The stash file is used by the client to retrieve the key database password.

3. Obtain the CA certificate.

4. Import the certificate in to the dsmcert.kdb database. You must import the certificate for each client in to the dsmcert.kdb.

   For clients, from the C:\Windows\SysWOW64 directory, run the **gsk8capicmd_64** command as shown in the following example:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "XYZ Certificate Authority"
   -file path_to_CA_root_certificate -format ascii -trust enable
   ```

   Multiple server certificates can be added to the dsmcert.kdb database so that the client can connect to different servers. Different certificates must have different labels. Use meaningful names for the labels.

   **Important:** For a disaster recovery of the server, if the certificate has been lost, the server automatically generates a new certificate. Each client must import the new certificate.

5. After the server certificate is added to the dsmcert.kdb database, add the `ssl yes` option to the C:\Windows\SysWOW64\fb.opt file and update the value of the `tcpport` option.

   **Important:**

   The server is normally set up for SSL and TLS connections on a different port than non-SSL and TLS connections. Do not specify a non-SSL or TLS port number for the `tcpport` value. If the value of `tcpport` is incorrect, the recovery agent cannot connect to the server.

   You cannot connect to a non-SSL or TLS port with a recovery agent that is enabled for SSL or TLS or connect a SSL or TLS port to a recovery agent that is not enabled for SSL or TLS.

6. Set the correct SSL or TLS ports in the following recovery agent configuration files:

   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

# Locale settings

Locale settings identify the language that is used for interfaces, messages, and online help.

**Data Protection for VMware GUIs**

The phrase "Data Protection for VMware GUI" applies to the following GUIs:

- Data Protection for VMware vSphere GUI accessed in a web browser
- IBM Spectrum Protect vSphere Client plug-in in the vSphere Web Client GUI

The Data Protection for VMware GUIs do not support running in an environment that contains inconsistent locale settings among the processors that run the Data Protection for VMware GUI, the VMware vSphere Client, and the IBM Spectrum Protect server.

Specify the same locale settings among the systems that run the Data Protection for VMware GUI, the VMware vSphere Client, and the IBM Spectrum Protect server.

When a Data Protection for VMware GUI help page is accessed through the "Learn more" link for the first time, the help displays in the language that is specified by the locale setting of the system that runs the Data Protection for VMware GUI. The help does not display in the language that is specified by the locale of the VMware vSphere Client the first time the help is accessed. In this situation, after the Data Protection for VMware GUI help page displays, click at least two links within the help, then close the help. The next time that the help is started from the "Learn more" link, it displays in the language that is specified by the locale setting of the VMware vSphere Client.

### IBM Spectrum Protect file restore interface

The interface content and message prompt language is determined by the language setting of the web browser that accesses the IBM Spectrum Protect file restore interface.

For error messages that are logged to the `fr_api.log` file, the IBM Spectrum Protect file restore interface uses the language that is specified by the locale setting of the system that runs the Data Protection for VMware vSphere GUI.

# Log file activity

Data Protection for VMware creates and modifies several log files during installation, back up, mount, and restore operations.

Data Protection for VMware log files are plain text files that use an `.sf` file extension.

**Windows** Logs are placed in the following directory:
`%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware`
The directories contain a subdirectory for each Data Protection for VMware component. For example, the recovery agent subdirectory is `\mount`, and the Recovery Agent command-line interface subdirectory is `\shell`.
You can search for log files from the **Windows** > **Start** menu, by selecting **Control Panel** > **Search** and entering `*.log`.

**Linux** Logs are placed in both of the following paths:
`<user.home>/tivoli/tsm/ve/mount/log`
`/opt/tivoli/tsm/TDPVMware/mount/engine/var`
You can search for log files by entering this command:

```
find /opt/tivoli/ -name "*.log"
```

**Important:** Existing log files are overwritten every time an installation is started. If you encounter an installation issue and must reinstall the product, retrieve the existing `TDPVMwareInstallation.log` file from the `%allusersprofile%` directory before you try the installation again.

**Note:** While the Data Protection for VMware service is running, several log files are held in an open state. As a result, some file managers do not display the current state of these files, and might report a file size of zero. Selecting or opening one of these files forces the file manager to update the file's details.

### recovery agent log files
The recovery agent log file is TDP_FOR_VMWARE_MOUNT*nnn*.sf. The log file with the most recent data is stored in the log file with the *040* number (TDP_FOR_VMWARE_MOUNT040.sf). When a log file reaches the maximum size limit, a new log file is created. The log file name is the same except that the log file

number decrements by one. Specifically, the data in the log file with the *040* number is copied to a log file with the *039* number. The log file with the *040* number contains the newest log file data. When *040* again reaches maximum file size, the *039* file contents move to *038* and the *040* information goes to *039* again.

**Data Protection for VMware GUI log files**

The Data Protection for VMware vSphere GUI places log files in this directory:

`Windows` `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs`

`Linux` `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

When you are collecting log files, make sure to include all subdirectories in your compressed file.

**Data Protection for VMware command-line interface log files**

The Data Protection for VMware command-line interface places log files in this directory:

`Windows` `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\logs`

`Linux` `/opt/tivoli/tsm/tdpvmware/common/logs`

When you are collecting log files, make sure to include all subdirectories in your compressed file.

**IBM Spectrum Protect file restore interface log files**

The IBM Spectrum Protect file restore interface logs error messages to the `fr_api.log`, `fr_gui.log`, and `messages.log` files. These files are in the following default directory:

`Windows` `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs`

`Linux` `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

You can change the name and location of the `fr_api.log` file by setting the API_LOG_FILE_NAME and API_LOG_FILE_LOCATION options in the file restore log activity file (`FRLog.config`).

File restore operations are also logged by the IBM Spectrum Protect server. You can search these messages with a server administrative command-line client.

- To start an administrative client session in command-line mode, enter this command on your workstation:

```
dsmadmc -id=admin -password=admin -dataonly=yes
```

By entering the **DSMADMC** command with the **-ID** and **-PASSWORD** options as shown, you are not prompted for a user ID and password.

- To search the SQL summary extended table to view results about file restore operations, issue the **select** command from the administrative command-line client:

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
```

You can narrow the search by including one or more of the following criteria in the select statement:

- * ENTITY='*DATA_MOVER_NODE_NAME*'
- * AS_ENTITY='*DATA_CENTER_NODE_NAME*'
- * SUB_ENTITY='*VM_HOST_NAME*'
- * START_TIME='*yyyy-MM-dd HH:mm:ss*'

For example:

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'
and START_TIME>'2017-03-11 17:30:00'
```

The START_TIME criteria supports queries with the following signs: equal (=), less than (<), or greater than (>).

- To search the SQL activity log table to view events about file restore operations, issue the **select** command from the administrative command-line client:

```
select * from ACTLOG
```

You can narrow the search by including one or more of the following criteria in the select statement:

- \* NODENAME='*DATA_CENTER_NODE_NAME*'
- \* DATE_TIME='*yyyy-MM-dd HH:mm:ss*'

For example:

```
select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2017-03-11 17:30:00'
```

Specify the *DATA_MOVER_NODE_NAME* and *DATA_CENTER_NODE_NAME* in uppercase characters.

The DATE_TIME criteria supports queries with the following signs: equal (=), less than (<), or greater than (>).

## Starting and running services for Data Protection for VMware

By default, when you start the Windows operating system, recovery agent is started under the Local System Account.

**Running recovery agent services on Microsoft Windows**
When you start the recovery agent from the Windows Start menu, the service is automatically stopped. When the recovery agent, started from the Start menu finishes, the service starts automatically. In addition, for these operating systems, the service does not provide a GUI. In order to use the GUI, go to the Windows Start menu and select **All Programs** > **IBM Spectrum Protect** > **Data Protection for VMware** > **recovery agent**.

**Data Protection for VMware command-line interface**
You can verify that the Data Protection for VMware command-line interface is running by completing the following task:

**Windows** Go to **Start** > **Control Panel** > **Administrative Tools** > **Services** and verify that the status of `Data Protection for VMware command-line interface` is `Started`.

**Linux** Go to the scripts directory (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) and issue this command:

```
./vmclid status
```

- If the daemon is not running, issue this command to manually start the daemon:

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
```

These init scripts can also be used to stop and start the daemon:

```
./vmclid stop
./vmclid start
```

# Appendix A. Advanced configuration tasks

You must manually configure and verify each component using the available application interfaces.

**Before you begin**
Make sure that the following conditions exist before proceeding with this task:

- An IBM Spectrum Protect server must be available to register the nodes.
- The Data Protection for VMware vSphere GUI is installed on a system that meets the operating system prerequisites. It must have network connectivity to the following systems:
  - vStorage Backup Server
  - IBM Spectrum Protect server
  - vCenter Server

**Procedure**

1. Log on to the IBM Spectrum Protect server and complete the tasks described in t_ve_cfg_regtsmnodes.dita.
2. Log on to the vStorage Backup Server and complete the tasks described in "Setting up data mover nodes with the vSphere plug-in GUI" on page 77.
3. Log on to the system where the Data Protection for VMware vSphere GUI is installed and complete the tasks described in "Configuring the Data Protection for VMware command-line interface in a vSphere environment" on page 85.
4. On the system where the Data Protection for VMware vSphere GUI is installed, start the vSphere Client and log on to the vCenter.

   If the vSphere Client is already running, you must stop and restart it.
5. Go to the Home directory in the vSphere Client. Click the Data Protection for VMware vSphere GUI icon in the Solutions and Applications panel.

   **Tip:** If the icon is not shown, then the Data Protection for VMware vSphere GUI was not registered or a connection error occurred.

   a. In the vSphere Client menu, go to **Plug-ins** > **Manage Plug-ins** to start the Plug-in Manager.
   b. If you can locate the Data Protection for VMware vSphere GUI and a connection error occurred, verify connectivity to the machine where the Data Protection for VMware vSphere GUI is installed by issuing the `ping` command.

**Results**
The Data Protection for VMware vSphere GUI is ready for backup and restore operations.

## Setting up the IBM Spectrum Protect nodes in a vSphere environment

This procedure describes how to manually register nodes to the IBM Spectrum Protect server and grant proxy authority for these nodes in a vSphere environment.

**Before you begin**

**Important:**

**About this task**
All steps in this procedure are completed on the IBM Spectrum Protect server.

**Tip:** This task can also be completed by using the Data Protection for VMware vSphere GUI configuration wizard or edit configuration notebook. Start the Data Protection for VMware vSphere GUI by opening a web browser and going to the GUI web server. For example:

```
https://guihost.mycompany.com:9081/TsmVMwareUI/
```

Login by using the vCenter user name and password.

- For an initial configuration, go to **Configuration** > **Run Configuration Wizard**.
- For an existing configuration, go to **Configuration** > **Edit Configuration**.

**Procedure**

1. Log on to the IBM Spectrum Protect server and start an administrative client session in command-line mode:

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

2. Issue the `REGister Node` command to register the following nodes to the IBM Spectrum Protect server:

   a) The node that represents the VMware vCenter (vCenter node):

      ```
      REGister Node MY_VCNODE <password for MY_VCNODE>
      ```

   b) The node that communicates between IBM Spectrum Protect and the Data Protection for VMware vSphere GUI (VMCLI node):

      ```
      REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
      ```

   c) The node that represents the data center and is where the VM data is stored (datacenter node):

      ```
      REGister Node MY_DCNODE <password for MY_DCNODE>
      ```

   d) The node that "moves data" from one system to another (data mover node):

      ```
      REGister Node MY_DMNODE <password for MY_DMNODE>
      ```

   ⚠️ **Attention:** When registering nodes to the IBM Spectrum Protect server, do not use the `userid` parameter.

3. Issue the `GRant PROXynode` command to define proxy relationships for these nodes:

   **Remember:** Target nodes own the data and agent nodes act on behalf of the target nodes. When granted proxy authority to a target node, an agent node can perform backup and restore operations for the target node.

   a) Grant proxy authority to the vCenter node by issuing this command:

      ```
      GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
      ```

      This command grants MY_DCNODE and MY_VMCLINODE the authority to backup and restore VMs on behalf of MY_VCNODE.

   b) Grant proxy authority to the datacenter node by issuing this command:

      ```
      GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
      ```

      This command grants MY_VMCLINODE and MY_DMNODE the authority to backup and restore VMs on behalf of MY_DCNODE.

   c) (Optional) Grant proxy authority to any additional datacenter nodes or data mover nodes in your environment.

   d) Verify the proxy relationships by issuing the IBM Spectrum Protect server `Query PROXynode` command. The expected command output is shown here:

The expected command output is:

```
Target Node       Agent Node
--------------    ------------------------------
MY_VCNODE            MY_DCNODE  MY_VMCLINODE
MY_DCNODE            MY_VMCLINODE  MY_DMNODE
```

**What to do next**

After successfully setting up the IBM Spectrum Protect nodes, the next manual configuration task is to set up the data mover nodes as described in "Setting up data mover nodes with the vSphere plug-in GUI" on page 77.

# Setting up data mover nodes with the vSphere plug-in GUI

If you offload backup workloads to a vStorage backup server in a vSphere environment, you can use the Data Mover wizard to set up a series of data mover nodes to run the operation and move the data to the IBM Spectrum Protect server.

**Before you begin**

Setting up data movers nodes requires configuration changes, starting the necessary services, and verifying the setup.

You can carry out these tasks using the plug-in GUI, which simplifies and speeds up the creation of a series of data mover nodes. Alternatively, you can carry out the work manually, for further information, see "Manually setting up the data mover nodes in a vSphere environment " on page 78.

In a standard Data Protection for VMware environment, a separate `dsm.opt` file (Windows) or `dsm.sys` file stanza (Linux) is used for each data mover node. When multiple data mover nodes on a vStorage Backup Server are used for data deduplication, and these nodes have authority to move data for the same datacenter node, then each `dsm.opt` file or `dsm.sys` file stanza must include a different value for the `dedupcachepath` option.

A physical data mover node typically uses the SAN to back up and restore data. If you configure the data mover node to directly access the storage volumes, turn off automatic drive letter assignment. If you do not turn off letter assignments, the client on the data mover node might corrupt the Raw Data Mapping (RDM) of the virtual disks. If the RDM of the virtual disks is corrupted, backups fail.

**Restriction:** Data Protection for VMware does not support scheduling the vStorage Backup Server (that is used as the data mover) to back up itself. Make sure that the vStorage Backup Server is excluded from its own schedules. Use a different vStorage Backup Server to perform the backup of a VM that contains a vStorage Backup Server.

If you need to carry out any of the above adjustments, consult the topic "Manually setting up the data mover nodes in a vSphere environment."

**About this task**

Use the vSphere plug-in to configure data mover nodes.

**Procedure**

1. From the vSphere plug-in, select IBM Spectrum Protect .
2. In the **Configure** tab, select **Data Movers**.
3. In the **Add Data Mover** panel, select a datacenter from the drop-down menu.
4. Edit, as required, the following fields:

   - **Data mover name**: A node name, already filled with a suggested name based on node prefix, the datacenter node name, data mover name, and an incrementing number.

- **Data mover host name**
- **vCenter User**, already filled in with the name of the user that registered the plug-in.
- **vCenter password**

Click **Add** when settings are complete.

5. The **Results** screen shows:

- The name of the configured data mover.
- The location of the options file. You can configure the data mover by editing this file.
- The location of the log files.
- The default options that were used.

6. You can now test the data mover using the **IBM Spectrum Protect > Configure Data Movers** tab. You can also verify the installation by selecting the data mover, and clicking **Verify**, or by checking the status the next time a data mover is added.

7. You can add the data mover to a schedule using the **IBM Spectrum Protect > Schedules** tab.

# Manually setting up the data mover nodes in a vSphere environment

If you offload backup workloads to a vStorage backup server in a vSphere environment, you can manually set up the data mover nodes to run the operation and move the data to the IBM Spectrum Protect server.

A physical data mover node typically uses the SAN to back up and restore data. If you configure data mover nodes to directly access the storage volumes, turn off automatic drive letter assignment. If you do not turn off letter assignments, the client on the data mover node might corrupt the Raw Data Mapping (RDM) of the virtual disks. If the RDM of the virtual disks is corrupted, backups fail.

**Required services:** The data mover requires the client acceptor service, the remote client agent service, and the data mover scheduler service as described in the following steps. If you remove a data mover from a datacenter, uninstall and delete these services for the data mover.

**Important:** If the data mover is installed on the same Windows system as the Data Protection for VMware vSphere GUI and **Create Services** was selected during the data mover configuration, the following steps are not required.

In a standard Data Protection for VMware environment, a separate `dsm.opt` file (Windows) or `dsm.sys` file stanza (Linux) is used for each data mover node. When multiple data mover nodes on a vStorage Backup Server are used for data deduplication, and these nodes have authority to move data for the same datacenter node, then each `dsm.opt` file or `dsm.sys` file stanza must include a different value for the `dedupcachepath` option. For best results, specify a different `schedlogname` and `errorlogname` option for each `dsm.opt` file or `dsm.sys` file stanza.

**Note:** All steps in these procedure are completed on the vStorage backup server.

A physical data mover node typically uses the SAN to back up and restore data. If you configure the data mover node to directly access the storage volumes, turn off automatic drive letter assignment. If you do not turn off letter assignments, the client on the data mover node might corrupt the Raw Data Mapping (RDM) of the virtual disks. If the RDM of the virtual disks is corrupted, backups fail.

**Restriction:** Data Protection for VMware does not support scheduling the vStorage backup server used as the data mover to back up itself. Make sure that the vStorage backup server is excluded from its own schedules. Use a different vStorage backup server to back up of the vStorage backup server used as the data mover.

## Gathering the information you will need

Data Mover information must be collected from the GUI host configuration wizard at the time of creating the data mover node in the wizard. See the topic for details of the required information. Gather and record the following information before you manually configure a data mover:

- vCenter user name and password

- Data mover node name
- Data mover password
- Data mover sample options

The Data mover name and sample options file can be gathered at a subsequent stage by the following process:

1. Open a web browser and enter the GUI web server address: for example, `https://guihost.mycompany.com:9081/TsmVMwareUI/`
2. Log in with the vCenter user name and password, and ensure that Configuration mode is selected.
3. In the configuration wizard, go to the **Data Mover Nodes** page.
4. Locate the data mover that you want, and click **View**.
5. Copy the sample options from the **View** tab to the options file.
6. Update these options if and as required for your environment

The minimum sets of required options for each platform are provided in these topics:

-
-

## Setting up Windows data mover nodes

You can use the vStorage backup server to set up your Windows data mover nodes.

**Before you begin**
Gather the information described in the conceptual topic, .

**Procedure**

1. Copy the options from the sample `dsm.opt` options file for the data mover to an options file located in `C:\Program Files\Tivoli\TSM\baclient`. Name the options file after the data mover: for example, `dsm.PREFIX_DATACENTER_DM.opt`.

2. You can update these options if and as required for your environment. For a description of the options, see Client options reference.

   For instant access, instant restore, or mount (file restore) operations, add VMISCSISERVERADDRESS to the data mover options file. Specify the iSCSI server IP address of the network card on the vStorage backup server used for the iSCSI data transfer during instant operations. The physical network interface card (NIC) that is bound to the iSCSI device on the ESX host must be on the same subnet as the NIC on the vStorage backup server used for the iSCSI transfer.

3. Issue the following command to set the VMware vCenter user and password for the data mover node:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`

   For information on required administrator rights. see technote 7047438

4. This procedure uses the IBM Spectrum Protect Client GUI Configuration wizard to set up the client acceptor service and scheduler service. By default, the remote client agent service is also set up through the wizard. If you use the IBM Spectrum Protect Client Service Configuration Utility (`dsmcutil`) for this task, you must also install the remote client agent service. Set up the client acceptor service and data mover scheduler service by completing the following tasks:

5. Set up the client acceptor service and data mover scheduler service by completing the following tasks:

   - This procedure uses the IBM Spectrum Protect Client GUI Configuration wizard to set up the client acceptor service and scheduler service. By default, the remote client agent service is also set up through the wizard. If you use the IBM Spectrum Protect Client Service Configuration Utility (**dsmcutil**) for this task, make sure to also install the remote client agent service.

Start the IBM Spectrum Protect Client Configuration wizard from the file menu by going to **Utilities > Setup Wizard**:

– Select **Help me configure the TSM Web Client**. Enter the information as prompted.

    a. In the `When do you want the service to start?` option, select **Automatically when Windows boots**.

    b. In the `Would you like to start the service upon completion of this wizard?` option, select **Yes**.

When the operation completes successfully, return to the wizard welcome page.

**Tip:** When you configure more than one data mover node on the same machine, you must specify a different port value for each client acceptor instance.

– Select `Help me configure the TSM Client Scheduler`. Enter the information as prompted.

    a. When you enter the scheduler name, make sure to select the **Use the Client Acceptor daemon (CAD) to manage the scheduler** option.

    b. In the `When do you want the service to start?` option, select **Automatically when Windows boots**.

    c. In the `Would you like to start the service upon completion of this wizard?` option, select **Yes**.

**Results**

To verify your configuration settings:

1. Start a data mover command-line session with the `-asnodename` and `-optfile` command-line parameters: `dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt`

Make sure that after your initial sign-on, you are not prompted for your password.

> ⚠️ **Attention:** To prevent the IBM Spectrum Protect scheduler from failing, make sure that the asnodename option is not set in the `dsm.opt` file (Windows) or `dsm.sys` file stanza (Linux). The scheduler queries the IBM Spectrum Protect server for schedules associated with nodename (data mover node), not asnodename (datacenter node). If asnodename is set in `dsm.opt` or `dsm.sys`, schedules associated with asnodename (and not nodename) are queried. As a result, scheduling operations fail.

Complete these tasks:

1. Verify the connection to the IBM Spectrum Protect server by issuing this command:

```
dsmc query session
```

This command shows information about your session, including the current node name, when the session was established, server information, and server connection information.

2. Verify you can back up a VM by issuing this command:

```
dsmc backup vm vm1
```

where vm1 is the name of the VM.

3. Verify that the backup completed successfully by issuing this command:

```
dsmc query vm "*"
```

4. Verify that the VM can be restored by issuing this command:

```
dsmc restore vm vm1 -vmname=vm1-restore
```

5. Verify that the client acceptor and agent are set up correctly:

a. In a web browser, enter IBM Spectrum Protect vSphere Client plug-in address. For example:

```
https://guihost.mycompany.com/vsphere-client/
```

b. Log in with the vCenter user name and password.

c. In the vSphere Web Client, click **IBM Spectrum Protect > Configure > Data Movers**.

d. Ensure that **Verified** is shown in the **Status** column for the data mover. If **Failed** is shown, hover over the status to view the failure message.

   **Tip:** When the IP address changes on the system where the Data Protection for VMware vSphere GUI is installed, you must complete the following:

e. Complete the tasks described in Troubleshooting

f. Set up the client acceptor again so that the Data Protection for VMware vSphere GUI becomes enabled for operations. Otherwise, the Plug-in Manager shows the Data Protection for VMware vSphere GUI status as disabled.

**Related tasks**
"Advanced configuration tasks" on page 75
You must manually configure and verify each component using the available application interfaces.

## Setting up Linux data mover nodes

You can use the vStorage backup server to set up your Linux data mover nodes.

**Before you begin**
Gather the information described in the conceptual topic, "Manually setting up the data mover nodes in a vSphere environment " on page 78.

**About this task**

**Procedure**

1. Use the IBM-installed Java version, located at the Linux install location for Java: `export JAVA_HOME=/opt/tivoli/tsm/tdpvmware/common/jre/jre`

2. Set the relevant environment variables.

   a. Ensure that the JAVA_HOME environment variable is exported correctly:

   ```
   JAVA_HOME=<jre-or-jdk-install-dir>
   ```

   b. Ensure that the PATH environment variable is exported correctly:

   ```
   export PATH=$PATH:$JAVA_HOME/jre/bin
   ```

3. Set up the client acceptor service and data mover scheduler service by completing the following tasks:

   - **Configure the data mover on Linux.**

     For the data mover on Linux, use the appropriate approach to configuration for your Linux OS and version: **systemd** or **SysV**. These are described in the following sections.

     **To configure the data mover on Linux using `systemd`, complete the following steps:**

     In this example procedure, PREFIX_DATACENTER_DM is used as a node name.

     a. Copy the following script to `/etc/systemd/system` and name it `dsmcad@PREFIX_DATACENTER_DM.service`

     ```
     #!/bin/bash
     #
     # (C) Copyright IBM Corporation 2018
     #
     # chkconfig: 35 95 5
     # description: IBM Spectrum Protect Client Acceptor Daemon
     ```

```
#
### BEGIN INIT INFO
# Provides: dsmcad
# Required-Start: $local_fs $remote_fs $network $syslog
# Required-Stop:
# Default-Start: 3 5
# Default-Stop: 0 1 2 6
# Short-Description: IBM Spectrum Protect Client Acceptor Daemon
# Description: Start dsmcad to enable scheduler and Web GUI.
### END INIT INFO
# SERVERNAME referenced in dsm.$SERVERNAME.opt and dsm.sys
SERVERNAME=LNX11L_DATACENTER_DM1
DSMCAD_DIR=/opt/tivoli/tsm/client/ba/bin
DSMCAD_BIN=$DSMCAD_DIR/dsmcad
OPTION_FILE=$DSMCAD_DIR/dsm.$SERVERNAME.opt
PID_FILE=/var/run/dsmcad-$SERVERNAME.pid
export JAVA_HOME=/opt/tivoli/tsm/tdpvmware/common/jre/jre
export LD_LIBRARY_PATH=$DSMCAD_DIR:$JAVA_HOME/lib/amd64/classic
export PATH=$JAVA_HOME/bin:$PATH
createPidFile()
{
  pid=`pgrep -f $OPTION_FILE`
  pidarr=($pid)
    if [ -n "${pidarr[1]}" ]
    then
        echo ${pidarr[1]} > $PID_FILE
    else
        echo ${pidarr[0]} > $PID_FILE
    fi
}
removePidFile()
{
  if [ -f $PID_FILE ]
  then
     rm -f $PID_FILE
  fi}
```

Update the script so that the SERVERNAME is set to your node name.

b. You do not need to make any further changes to the script. To ensure the script has 664 permissions, issue the command `chmod 664 dsmcad@.service`

c. Create a text file called `dsm.PREFIX_DATACENTER_DM.opt` in `/opt/tivoli/tsm/client/ba/bin` and add the following setting: `servername PREFIX_DATACENTER_DM`

d. Create `dsm.sys` in `/opt/tivoli/tsm/client/ba/bin` and add the data mover sample options.

For a description of the options, see Options reference.

For instant access, instant restore, or mount (file restore) operations, you must add VMISCSISERVERADDRESS to the data mover options file. Specify the iSCSI server IP address of the network card on the vStorage backup server that is used for the iSCSI data transfer during instant operations. The physical network interface card (NIC) that is bound to the iSCSI device on the ESX host must be on the same subnet as the NIC on the vStorage Backup Server that is used for the iSCSI transfer.

e. After creating the configuration files, store the vCenter credentials so that the data mover / mount proxy can access the vCenter inventory. Go to `/opt/tivoli/tsm/client/ba/bin` and issue the command: `./dsmc set password –type=VM fullyqualifieddomainnameofvcenter vcenteruserid vcenterpassword`

For information on required administrator rights. see technote 7047438

f. To start using the service, issue the following three commands:

– `systemctl daemon-reload`

– `systemctl enable dsmcad@PREFIX_DATACENTER_DM.service`

– `systemctl start dsmcad@PREFIX_DATACENTER_DM.service`

g. Once you have one data mover configured, you can use the Web Client plug-in GUI to add additional data movers or mount proxies.

**Note:** To ensure the service associated with PREFIX_DATACENTER_DM will automatically restart on a system reboot, run the command `systemctl enable dsmcad@PREFIX_DATACENTER_DM.service`

To stop the service, execute the command: `systemctl stop dsmcad@PREFIX_DATACENTER_DM.service`

**Note:** If you uninstall IBM Spectrum Protect, you must halt and remove the associated services:

– Use the above `stop` command to stop the `dsmcad` service.

– Disable the service with the command: `systemctl disable dsmcad@PREFIX_DATACENTER_DM.service`

– Remove the `dsmcad@.service` from the `/etc/systemd/system` directory.

**To configure the data mover on Linux using SysV, complete the following steps:**

In this example procedure, PREFIX_DATACENTER_DM is used as a node name.

a. Copy the provided `rc.dsmcad` script and update the script so that the SERVERNAME is set to your node name: SERVERNAME=PREFIX_DATACENTER_DM

b. Save the file as `/etc/init.d/dsmcad.PREFIX_DATACENTER_DM`

c. Ensure the file has 775 permissions with `chmod 755 dsmcad.PREFIX_DATACENTER_DM`

d. Create a text file called dsm.`PREFIX_DATACENTER_DM.opt` in `/opt/tivoli/tsm/client/ba/bin` and add the following setting: `servername PREFIX_DATACENTER_DM`

e. Create `dsm.sys` in `/opt/tivoli/tsm/client/ba/bin` and add the data mover sample options.

For a description of the options, see Options reference.

For instant access, instant restore, or mount (file restore) operations, you must add VMISCSISERVERADDRESS to the data mover options file. Specify the iSCSI server IP address of the network card on the vStorage backup server that is used for the iSCSI data transfer during instant operations. The physical network interface card (NIC) that is bound to the iSCSI device on the ESX host must be on the same subnet as the NIC on the vStorage Backup Server that is used for the iSCSI transfer.

f. After creating the configuration files, store the vCenter credentials so that the data mover / mount proxy can access the vCenter inventory. Go to `/opt/tivoli/tsm/client/ba/bin` and issue the command: `./dsmc set password –type=VM fullyqualifieddomainnameofvcenter vcenteruserid vcenterpassword`

For information on required administrator rights. see technote 7047438

g. Go to `/opt/tivoli/tsm/client/ba/bin` and execute the command: `./dsmc set password –type=VM fullyqualifieddomainname vcenteruserid vcenterpassword`

h. Depending on your OS, execute the following commands:

– Red Hat: `chkconfig - - add dsmcad.PREFIX_DATACENTER_DM`

– SUSE: `chkconfig - - add dsmcad.PREFIX_DATACENTER_DM`

– Ubuntu: `update-rc.d dsmcad.PREFIX_DATACENTER_DM defaults`

i. Run the command: `service dsmcad.PREFIX_DATACENTER_DM start`

j. Once you have one data mover configured, you can use the Web Client plug-in GUI to add additional data movers or mount proxies.

**Note:** When you run the `chkconfig` command the `dsmcad.PREFIX_DATACENTER_DM` will restart on a system reboot

To start the service: `service dsmcad.PREFIX_DATACENTER_DM start`

To stop the service: `service dsmcad.PREFIX_DATACENTER_DM stop`

**Note:** If you uninstall IBM Spectrum Protect, you must stop the associated services:

- Use the above `stop` command to stop the `dsmcad` service.
- Disable the service with the command: `systemctl disable dsmcad@PREFIX_DATACENTER_DM.service` so that auxiliary files, such as `/var/run/dsmcad.PREFIX_DATACENTER_DM.pid`, are removed.
- On RHEL or SLES, use the command: `chkconfig --del dsmcad.PREFIX_DATACENTER_DM`
- On Ubuntu, use the command: `update-rc.d dsmcad.PREFIX_DATACENTER_DM remove`
- Remove the `dsmcad.*` files from the `/etc/init.d` directory.

**Results**

1. Start a data mover command-line session with the `-asnodename` and `-optfile` command-line parameters: `dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt`

   Make sure that after your initial sign-on, you are not prompted for your password.

   ⚠️ **Attention:** To prevent the IBM Spectrum Protect scheduler from failing, make sure that the `asnodename` option is not set in the `dsm.opt` file (Windows) or `dsm.sys` file stanza (Linux). The scheduler queries the IBM Spectrum Protect server for schedules associated with nodename (data mover node), not `asnodename` (datacenter node). If `asnodename` is set in `dsm.opt` or `dsm.sys`, schedules associated with `asnodename` (and not nodename) are queried. As a result, scheduling operations fail.

Complete these tasks:

1. Verify the connection to the IBM Spectrum Protect server by issuing this command:

   ```
   dsmc query session
   ```

   This command shows information about your session, including the current node name, when the session was established, server information, and server connection information.

2. Verify you can back up a VM by issuing this command:

   ```
   dsmc backup vm vm1
   ```

   where vm1 is the name of the VM.

3. Verify that the backup completed successfully by issuing this command:

   ```
   dsmc query vm "*"
   ```

4. Verify that the VM can be restored by issuing this command:

   ```
   dsmc restore vm vm1 -vmname=vm1-restore
   ```

5. Verify that the client acceptor and agent are set up correctly:

   a. In a web browser, enter IBM Spectrum Protect vSphere Client plug-in address. For example:

   ```
   https://guihost.mycompany.com/vsphere-client/
   ```

   b. Log in with the vCenter user name and password.

   c. In the vSphere Web Client, click **IBM Spectrum Protect > Configure > Data Movers**.

   d. Ensure that **Verified** is shown in the **Status** column for the data mover. If **Failed** is shown, hover over the status to view the failure message.

   **Tip:** When the IP address changes on the system where the Data Protection for VMware vSphere GUI is installed, you must complete the following:

   e. Complete the tasks described in Troubleshooting

f. Set up the client acceptor again so that the Data Protection for VMware vSphere GUI becomes enabled for operations. Otherwise, the Plug-in Manager shows the Data Protection for VMware vSphere GUI status as disabled.

# Configuring the Data Protection for VMware command-line interface in a vSphere environment

Update the Data Protection for VMware command-line interface profile on the system where the Data Protection for VMware vSphere GUI is installed.

**Before you begin**
The profile (`vmcliprofile`) is located in this directory on the system where the Data Protection for VMware vSphere GUI is installed:

`Linux` `/opt/tivoli/tsm/tdpvmware/common/scripts`

`Windows` 64-bit: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts`

**About this task**
All steps in this procedure are completed on the system where the Data Protection for VMware vSphere GUI is installed.

**Tip:** This task can also be completed by using the Data Protection for VMware vSphere GUI configuration wizard or configuration notebook. Go to the Data Protection for VMware vSphere GUI **Configuration** window and click **Run Configuration Wizard** or **Edit Configuration**.

**Procedure**

1. Update the profile with these settings:

   **VE_TSMCLI_NODE_NAME**
   Specify the node that connects the Data Protection for VMware command-line interface to the IBM Spectrum Protect server and the agent node (`MY_VMCLINODE`).

   **Restriction:** The VMCLI node does not support the SSL protocol or LDAP authentication when communicating with the IBM Spectrum Protect server.

   **VE_VCENTER_NODE_NAME**
   Specify the virtual node that represents a vCenter (`MY_VCNODE`).

   **VE_DATACENTER_NAME**
   Specify the virtual node that maps to a data center. The correct syntax is shown here: `datacenter_name::datacenter_node_name`

   - The `datacenter_name` value is case-sensitive.
   - Make sure to set this parameter for each data center in your environment (`MY_DCNODE`).
   - The Data Protection for VMware vSphere GUI does not support data centers with the same name in the vCenter.

   **VE_TSM_SERVER_NAME**
   Specify the hostname or IP of the IBM Spectrum Protect server.

   **VE_TSM_SERVER_PORT**
   Specify the port name to use for the IBM Spectrum Protect server. The default value is 1500.

   An example profile with these settings is provided here:

   ```
   VE_TSMCLI_NODE_NAME     MY_VMCLINODE
   VE_VCENTER_NODE_NAME    MY_VCNODE
   VE_DATACENTER_NAME      MyDatacenter1::MY_DCNODE
   VE_TSM_SERVER_NAME      tsmserver.mycompany.xyz.com
   VE_TSM_SERVER_PORT      1500
   ```

2. Set the VMCLI node password in the `pwd.txt` file.

   This password is for the node that connects the Data Protection for VMware command-line interface to the IBM Spectrum Protect server and the data mover node. It is specified by the VE_TSMCLI_NODE_NAME profile parameter.

   a) Issue the echo command to create a text file that contains the password:

      **Linux** `echo password1 > pwd.txt`

      **Windows** `echo password1> pwd.txt`

      **Windows** A space must not exist between the password (`password1`) and the greater-than sign (`>`).

   b) Issue this vmcli command to set the password for the VMCLI node:

      `vmcli -f set_password -I pwd.txt`

      **Important:**

      - **Linux** You must issue the `vmcli -f set_password` command as tdpvmware user, and not as root.

      - **Windows** **Linux** If you plan to generate application protection reports, you must specify the `-type VMGuest` parameter to identify that the password applies to a VM. For example:

        ```
        vmcli -f set_password -type VMGuest -I password.txt
        ```

3. Verify that the Data Protection for VMware command-line interface is running:

   **Windows** Click **Start** > **Control Panel** > **Administrative Tools** > **Services** and verify that the status of `Data Protection for VMware command-line interface` is `Started`.

   **Linux** Go to the scripts directory (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) and issue this command:

   ```
   ./vmclid status
   ```

   - If the daemon is running, proceed to Step 4.
   - If the daemon is not running, issue this command to manually start the daemon:

     ```
     /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
     ```

     These init scripts can also be used to stop and start the daemon:

     ```
     ./vmclid stop
     ./vmclid start
     ```

4. Issue this vmcli command to verify that the Data Protection for VMware command-line interface recognizes the IBM Spectrum Protect node configuration:

   ```
   vmcli -f inquire_config -t TSM
   ```

5. Validate the nodes to confirm that no configuration errors occurred:

   a) Start the Data Protection for VMware vSphere GUI by clicking the icon in the Solutions and Applications window of the vSphere Client.

   b) Go to the **Configuration** window.

   c) Select a node in the table and click **Validate Selected Node**. Status information is shown in the **Status Details** pane.

**What to do next**

**Windows** **Linux** After successfully completing the three manual configuration tasks described in this section:

1. "Setting up the IBM Spectrum Protect nodes in a vSphere environment" on page 75

2. "Setting up data mover nodes with the vSphere plug-in GUI" on page 77

No additional configuration tasks are required to back up your VM data.

# vSphere environment command-line interface configuration checklist

Use this procedure to configure Data Protection for VMware in a vSphere environment by using a command-line interface only.

**Procedure**

Complete Step 1 and Step 2 on the IBM Spectrum Protect server.

1. Register the following nodes to the IBM Spectrum Protect server:
   a) The node that represents the VMware vCenter (vCenter node):

   ```
   REGister Node MY_VCNODE <password for MY_VCNODE>
   ```

   b) The node that communicates between IBM Spectrum Protect and the Data Protection for VMware vSphere GUI (VMCLI node):

   ```
   REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
   ```

   c) The node that represents the data center and is where the VM data is stored (datacenter node):

   ```
   REGister Node MY_DCNODE <password for MY_DCNODE>
   ```

   d) The node that "moves data" from one system to another (data mover node):

   ```
   REGister Node MY_DMNODE <password for MY_DMNODE>
   ```

2. Define proxy relationships for these nodes:
   a) Grant proxy authority to the vCenter node by issuing this command:

   ```
   GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
   ```

   This command grants `MY_DCNODE` and `MY_VMCLINODE` the authority to back up and restore VMs on behalf of `MY_VCNODE`.

   b) Grant proxy authority to the datacenter node by issuing this command:

   ```
   GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
   ```

   This command grants `MY_VMCLINODE` and `MY_DMNODE` the authority to back up and restore VMs on behalf of `MY_DCNODE`.

   c) (Optional) Grant proxy authority to any additional datacenter nodes or data mover nodes in your environment.

   d) Verify the proxy relationships by issuing the IBM Spectrum Protect server `Query PROXynode` command. The expected command output is shown here:

   ```
   Target Node      Agent Node
   --------------   -----------------------------
   MY_VCNODE              MY_DCNODE  MY_VMCLINODE
   MY_DCNODE          MY_VMCLINODE  MY_DMNODE
   ```

Complete Steps 3 through 9 on the vStorage Backup Server.

3. Set the appropriate values for the following data mover options:

   • **Windows** Specify these options in the `dsm.opt` options file.

   • **Linux** Specify these options in the `dsm.sys` file, in the stanza for the data mover node.

   ```
   NODENAME
   PASSWORDACCESS
   ```

```
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPORT
COMMMETHOD
HTTPPORT
```

**Note:** The HTTPPORT is required only when more than one Client Acceptor Service (CAD) is used. For example, if there are two data mover nodes (and two CAD services), then the option file for each data mover node must specify a different HTTPPORT value.

An example dsm.dm.opt file with these options is provided here:

```
NODename MY_DMNODE
PASSWORDAccess generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType FUllvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort 1500
COMMMethod tcpip
HTTPPORT    1583
```

4. Verify the connection to the IBM Spectrum Protect server by issuing this command:
   `dsmc query session`

5. Issue this command to set the VMware vCenter user and password for the data mover node:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`

6. Set up the following IBM Spectrum Protect services:

   - **Windows**

     a. Install the Scheduler Service:

        ```
        dsmcutil install scheduler /name:"TSM Central Scheduler Service"
        /node:MY_DMNODE    /password:MY_DMNODEPWD /startnow:no /autostart:no
        ```

     b. Install the CAD:

        ```
        dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /cadschedname:"TSM Central Scheduler Service" /startnow:no /autostart:yes
        ```

     c. Install the Remote Client Agent Service:

        ```
        dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /partnername:"TSM CAD - MY_DMNODE" /startnow:no
        ```

   - **Linux** Specify the `managedservices` option in the `dsm.sys` file, in the stanza for the data mover node:

     Make sure to specify the `schedule` and `webclient` parameters:

     ```
     managedservices schedule webclient
     ```

     This setting directs the client acceptor to manage both the Web client and the scheduler.

7. **Linux**

   Start the Client Acceptor Service:

   The installation program creates a startup script for the client acceptor daemon (`dsmcad`) in `/etc/init.d`. The client acceptor daemon must be started before it can manage scheduler tasks, or manage the web client. As root, use the following command to start the daemon:

   ```
   service dsmcad start
   ```

To enable the Client Acceptor Daemon to start automatically after a system restart, add the service as follows, at a shell prompt:

```
# chkconfig --add dsmcad
```

8. Verify that the IBM Spectrum Protect services are set up correctly:

   a) Log on to a remote system.

   b) Use a web browser to connect to the HOST1 system by using this address and port:
      `http://HOST1.xyz.yourcompany.com:1581`

Complete Step 10 on the system where the Data Protection for VMware vSphere GUI is installed.

9. Set the appropriate values for the following options in the Data Protection for VMware command-line interface profile (`vmcliprofile`):

```
VE_TSMCLI_NODE_NAME
VE_VCENTER_NODE_NAME
VE_DATACENTER_NAME
VE_TSM_SERVER_NAME
VE_TSM_SERVER_PORT
```

An example profile with these options is provided here:

```
VE_TSMCLI_NODE_NAME     MY_VMCLINODE
VE_VCENTER_NODE_NAME    MY_VCNODE
VE_DATACENTER_NAME      MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME      tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT      1500
```

The profile is in the following directories:

**Linux** `/opt/tivoli/tsm/tdpvmware/common/scripts`

**Windows** 64-bit: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts`

   a) Set the password for the VMCLI node:

      1) Issue the `echo` command to create a text file that contains the password:

         **Linux** `echo password1 > pwd.txt`

         **Windows** `echo password1> pwd.txt`

      2) Issue this vmcli command to set the password for the VMCLI node:

         **Important:** **Linux** You must issue this command as tdpvmware user, and not as root.

         ```
         vmcli -f set_password -I pwd.txt
         ```

   b) Verify that the Data Protection for VMware command-line interface is running:
      **Windows** Issue this command from a Windows command prompt:
      `net start`
      **Linux** Issue this command:
      `./vmclid status`

   c) Issue this vmcli command to verify that the Data Protection for VMware command-line interface recognizes the IBM Spectrum Protect node configuration:

      ```
      vmcli -f inquire_config -t TSM
      ```

# Tape configuration guidelines

Review these guidelines before attempting backup operations to tape storage.

**Preparing for backup to tape**

`Windows` `Linux` Before attempting a backup to tape, these parameters must be set on the IBM Spectrum Protect server for your tape backups:

1. Define the management class:

   ```
   define mgmtclass <domain name> <policy set name> <mgmtclass name>
   ```

   For example:

   ```
   define mgmtclass tape tape DISK
   ```

2. Define the copy group:

   ```
   define copygroup <domain name> <policy set name> <mgmtclass name>
   destination=<stgpool name>
   ```

   For example:

   ```
   define copygroup tape tape DISK destination=Diskpool
   ```

3. Activate the policy set:

   ```
   activate policyset <domain name> <policy set name>
   ```

   For example:

   ```
   activate policyset tape tape
   ```

When configuring backup to physical tape, there are additional configuration requirements. You must always keep IBM Spectrum Protect metadata (control files) on disk and the actual VM backup data on tape.

- Use the VMMC option to store the VMware backups (and VMware control files) with a management class other than the default management class.
- Use the VMCTLMC option to specify the management class to use specifically for VMware control files during VMware backups. The management class that you specify overrides the default management class. It also overrides the management class specified by the VMMC option. The VMCTLMC management class must specify a disk storage pool, with no migration to tape.
- The VMMC option is always used to control the retention on VM backups. This option applies to both disk and tape configurations. VMCTLMC is not used for the retention of the control files. The control and data files are part of the same grouping and are expired together based on the retention policy of the VMMC option. When both options are set, VMMC is used for data files and VMCTLMC is used for control files.

**Restriction:** Restore operations that use storage agents in LAN-free configurations might restore files from a copy storage pool even though the data might be retrievable from a primary storage pool. This might happen if the restore request is for a specific file, or the restore request is not using the no-query method, and the primary copy of the file is stored in a storage pool that is not accessible through a LAN-free path. This can also affect non-restore situations such as Data Protection for VMware backup operations. In a Data Protection for VMware environment, the preferred storage method for VM control files is disk, such that a mount is not needed to restore the file during the incremental backup process. These VM control files not only need to be placed on disk, but they should not be backed up to a copy storage pool that is available through a LAN-free path. If they are, a tape mount will be used to restore the files during a LAN-free incremental backup from a Data Protection for VMware client.

If the IBM Spectrum Protect server environment uses disk to tape migration, consider the following guidelines before migrating:

- Set the disk storage pool MIGDELAY to a value that supports most mount requests to be satisfied from disk. Typical usage patterns indicate that a high percentage of individual file recoveries occurs within few days. For example, usually 3 - 5 days from the time a file was last modified. Therefore, consider keeping data on disk for this brief period to optimize recovery operations.

  In addition, if client side deduplication is being used with the disk storage pool, set the MIGDELAY option that accommodates frequent full VM backups. Do not migrate data from the deduplicated storage pool to tape until at least two full backups are completed for a VM. When data is moved to tape, it is no longer deduplicated. For example, if full backups are run weekly, consider setting MIGDELAY to a value of at least 10 days. This setting ensures that each full backup identifies and uses duplicate data from the previous backup before being moved to tape.

- Use a device class file storage pool rather than a DISK device class storage pool. A typical value for a volume size, specified by a device class MAXCAPACITY parameter, would be 8 GB to 16 GB. For the associated storage pool, consider applying collocation by file space. Each VM that is backed up is represented as a separate file space in the IBM Spectrum Protect server. Collocating by file space saves the data from multiple incremental backups for a given VM in the same volume (disk file). When migration to tape occurs, collocation by file space locates multiple incremental backups for a given VM together on a physical tape.

Use the **Settings** dialog to set the Tape Mode value.

A backup operation becomes interrupted when a mount or instant restore operation requires the same tape storage simultaneously in use by the backup operation.

## ▄▄ Linux ▄▄ Manually configuring an iSCSI device on a Linux system

This procedure describes how to configure a Linux system that is used during an iSCSI mount operation. The VM snapshot is mounted from IBM Spectrum Protect server storage.

**Before you begin**
During an iSCSI mount, an iSCSI target is created on the Recovery Agent system. Microsoft iSCSI Initiator is not required on the Recovery Agent system.

**Tip:** Open-iSCSI Initiator is provided with Red Hat Enterprise Linux and SUSE Linux Enterprise Server.

Review the following iSCSI requirements before you proceed with this task:

- You can connect to the iSCSI target from any system to create a volume that contains the backup data. You can mount this volume from another system.
- An iSCSI initiator is required on any system that must connect to the iSCSI target.
- An iSCSI initiator must be installed on the system where the data is to be restored.
- If a volume spans several disks, you must mount all the required disks. When mirrored volumes are used, mount only one of the mirrored disks. Mounting one disk prevents a time-consuming synchronization operation.

**About this task**
Complete these steps to configure the Linux system that is used during an iSCSI mount operation:

**Procedure**

1. Record the iSCSI initiator name on the system where data is to be restored.

   The iSCSI initiator name is located in the /etc/iscsi/initiatorname.iscsi file. If the InitiatorName= value is empty, create an initiator name with the following command:

   ```
   twauslbkpoc01:~ # /sbin/iscsi-iname
   ```

   Here is an example initiator name:

```
iqn.2005-03.org.open-iscsi:3f5058b1d0a0
```

2. Add the initiator name to the `/etc/iscsi/initiatorname.iscsi` file.

   a) Edit the `/etc/iscsi/initiatorname.iscsi` file with **vi** command. For example:

   ```
   twauslbkpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
   ```

   b) Update the **InitiatorName=** parameter with the initiator name. For example:

   ```
   InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0
   ```

3. Complete the following steps on the system where the recovery agent (or iSCSI target) is installed:

   a) Start the recovery agent. Complete the `Select IBM Spectrum Protect server` and `Select snapshot` dialogs and click **Mount**.

   b) In the `Choose mount destination` dialog, select `Mount an iSCSI target`.

   c) Create a target name. Make sure that it is unique and that you can identify it from the system that runs the iSCSI initiator. For example:

   ```
   iscsi-mount-tsm4ve
   ```

   d) Enter the iSCSI Initiator name that was recorded in Step 1 and click **OK**.

   e) Verify that the volume you just mounted is displayed in the `Mounted Volumes` field.

4. Locate and start the iSCSI Initiator program on the initiator system that was selected in Step 1:

   a) Verify that the iSCSI service is running by issuing this command:
   Red Hat Enterprise Linux:

   ```
   service iscsi status
   ```

   SUSE Linux Enterprise Server:

   ```
   service open-iscsi status
   ```

   If the service is not running, issuing this command to start the service:
   Red Hat Enterprise Linux:

   ```
   service iscsi start
   ```

   SUSE Linux Enterprise Server:

   ```
   service open-iscsi start
   ```

   b) Connect to the iSCSI target by issuing this command:

   ```
   iscsiadm -m discovery -t sendtargets -p <IP/hostname of
   recovery agent  system> --login
   ```

   c) Verify that a new raw device is available by issuing this command:

   ```
   fdisk -l
   ```

5. Mount the file system:

   For a non-LVM volume, issue the following commands. In this example, the new device is `/dev/sdb1`:

   ```
   mkdir /mountdir
   mount /dev/sdb1 /mountdir
   ```

   For an LVM volume, complete the following tasks on the Linux guest:

   a. Make sure that the `vgimportclone` script is available on the Linux system. This script is not shipped in the base (default) LVM package. As a result, you might need to update the LVM package to a level which provides this script.

b. Issue the **vgimportclone** command and include a new base volume group name (VolGroupSnap01). For example:

```
vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
```

c. Issue the **lvchange** command to mark the logical volume as active. For example:

```
lvchange -a y /dev/VolGroupSnap01/LogVol00
```

d. Issue these commands to mount the volume:

```
mkdir /mountdir
mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
```

6. After the file restore operation completes, issue these commands:

- For a non-LVM volume, issue the following commands:

  a. Unmount the file system:

  ```
  umount /dev/sdb1 /mountdir
  ```

  b. Remove the volume. If the volume is part of a volume group, first remove the volume from the volume group by issuing the following command:

  ```
  vgreduce <your_volume_group> /dev/sdb1
  ```

  Then issue this command to remove the volume:

  ```
  pvremove /dev/sdb1
  ```

  c. Log out of a single target:

  ```
  iscsiadm --mode node --targetname <target_name> --logout
  ```

  d. Log out of all targets:

  ```
  iscsiadm --mode node --logout
  ```

- For an LVM volume, complete the following tasks on the Linux guest:

  a. Unmount the file system:

  ```
  unmount /mountdir
  ```

  b. Remove the logical volume:

  ```
  lvm lvremove LogVol00
  ```

  c. Remove the volume group:

  ```
  lvm vgremove VolGroupSnap01
  ```

  d. Log out of a single target:

  ```
  iscsiadm --mode node --targetname <target_name> --logout
  ```

  e. Log out of all targets:

  ```
  iscsiadm --mode node --logout
  ```

# Manually configuring an iSCSI device on a Windows system

This procedure describes how to configure a Windows system that is used during an iSCSI mount operation. The snapshot is mounted from IBM Spectrum Protect server storage.

**Before you begin**

Review the following iSCSI requirements before you proceed with this task:

- During an iSCSI mount, an iSCSI target is created on the recovery agent system. You can connect to the iSCSI target from any system to create a volume that contains the backup data. Also, you can then mount this volume from another system.
- iSCSI initiator is required on any system that must connect to the iSCSI target.
- Make sure that an iSCSI initiator is installed on the system where the data is to be restored.
- Microsoft iSCSI Initiator is not required on the recovery agent system.

Review the following disk and volume requirements before you proceed with this task:

- If a volume spans several disks, you must mount all the required disks. When mirrored volumes are used, mount only one of the mirrored disks. Mounting one disk prevents a time-consuming synchronization operation.
- If multiple dynamic disks were used on the backup system, these disks are assigned to the same group. As a result, Windows Disk Manager might consider some disks as missing and issue an error message when you mount only one disk. Ignore this message. The data on the backed up disk is still accessible, unless some of the data is on the other disk. This issue can be solved by mounting all the dynamic disks.

**About this task**
Complete these tasks to configure the Windows system that is used during an iSCSI mount operation:

**Procedure**

1. On the recovery agent system, open port 3260 in the LAN firewall and the Windows client firewall.

   Record the iSCSI initiator name on the system where data is to be restored.

   The iSCSI initiator name is shown in the iSCSI initiator configuration window of the Control Panel. For example:

   ```
   iqn.1991-05.com.microsoft:hostname
   ```

2. Complete these tasks on the system where the recovery agent (or iSCSI target) is installed:

   a) Start the recovery agent GUI. Complete the **Select IBM Spectrum Protect server** and **Select snapshot** dialogs and click **Mount**.

   b) In the **Choose mount destination** dialog, select **Mount an iSCSI target**.

   c) Create a target name. Make sure that it is unique and that you can identify it from the system that runs the iSCSI initiator. For example:

   ```
   iscsi-mount-tsm4ve
   ```

   d) Enter the iSCSI Initiator name that was recorded in Step 1 and click **OK**.

   e) Verify that the volume you just mounted is displayed in the **Mounted Volumes** field.

   f) When you use the Recovery Agent in an iSCSI network, and the Recovery Agent does not use a data mover, go to the `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf file` and specify the `[IMOUNT]` tag and **Target IP** parameter:

   ```
   [IMOUNT config]
   Target IP=<IP address of the network card on the system
   that exposes the iSCSI targets.>
   ```

For example:

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

After you add or change the Target IP parameter, restart the Recovery Agent GUI or Recovery Agent CLI.

3. Locate and start the iSCSI Initiator program on the initiator system that was selected in Step 1:

   a) Connect to the iSCSI target:

      1) In the Targets tab, enter the TCP/IP address of the recovery agent (iSCSI target) used in Step 2 in the **Target:** dialog. Click **Quick Connect**.

      2) The **Quick Connect** dialog shows a target that matches the target name that was specified in Step 2c. If it is not already connected, select this target and click **Connect**.

   b) On the initiator system, go to **Control Panel** > **Administrative Tools** > **Computer Management** > **Storage** > **Disk Management**.

      1) If the mounted iSCSI target is listed as **Type=Foreign**, right-click **Foreign Disk** and select **Import Foreign Disks**. The **Foreign Disk Group** is selected. Click **OK**.

      2) The next screen shows the type, condition, and size of the Foreign Disk. Click **OK** and wait for the disk to be imported.

      3) When the disk import completes, press **F5** (refresh). The mounted iSCSI snapshot is visible and contains an assigned drive letter. If drive letters are not automatically assigned, right-click the required partition and select **Change Drive Letters or Paths**. Click **Add** and select a drive letter.

4. Open Windows Explorer (or other utility) and browse the mounted snapshot for a file restore operation.

5. After the file is restored, complete these tasks:

   a) Disconnect each iSCSI target by using the **iSCSI Initiator Properties** dialog.

   b) Dismount the volume from Step 2 by selecting the volume in the recovery agent GUI and clicking **Dismount**.

# Linux Manually configuring the mount proxy nodes on a Linux system

Complete this task to add a mount proxy node to a remote Linux system.

**Before you begin**

In a standard Data Protection for VMware vSphere GUI environment, a separate dsm.sys file stanza is used for each mount proxy node. All steps in this procedure are completed by using the data mover that is installed on the backup server.

**About this task**
This task sets up the mount proxy nodes by updating the data mover options and verifying connectivity to the IBM Spectrum Protect server.

**Procedure**

1. Specify these options in the dsm.sys file, in the stanza for the mount proxy node.

   **NODENAME**
   Specify the name of a previously defined mount proxy node. IBM Spectrum Protect schedules are associated with this node.

**PASSWORDACCESS**

Specify GENERATE so that the password is generated automatically (instead of a user prompt).

**MANAGEDSERVICES**

Specify this option to direct the client acceptor to manage both the Web client and the scheduler (`schedule webclient`).

**TCPSERVERADDRESS**

Specify the TCP/IP address for the IBM Spectrum Protect server.

**TCPPORT**

Specify the TCP/IP port address for the IBM Spectrum Protect server.

**COMMMETHOD**

Specify the communication method to be used by the IBM Spectrum Protect server. For mount proxy nodes, you must specify TCP/IP as the communication method. Operations fail if another method is specified.

**HTTPPORT**

This option specifies a TCP/IP port address and is must be specified only when more than one Client Acceptor Service (CAD) is used. For example, if there are two mount proxy nodes (and two CAD services), then the option file for each mount proxy node must specify a different HTTPPORT value.

**Restriction:** Do not enable the LAN-free option (ENABLELANFREE YES) in the `dsm.sys` file. This option is not supported for mount proxy nodes.

An example dsm.sys file with these settings is provided here:

```
Servername      tsm_server1
        NODename datacenter1_MP_LNX
        PASSWORDAccess generate
        MANAGEDServices schedule webclient
        TCPServeraddress tsmserver.myco.com
        TCPPort 1500
        COMMMethod tcpip
        HTTPPORT     1583
```

2. Issue this command to set the VMware vCenter user and password for the mount proxy node:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`

3. Start a data mover command-line session with the `-asnodename` and `-optfile` command-line parameters:
   `dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys`
   Make sure that after your initial sign-on, you are not prompted for your password.

   ⚠️ **Attention:** To prevent the IBM Spectrum Protect scheduler from failing, make sure that the asnodename option is not set in the `dsm.sys` file stanza (Linux). The scheduler queries the IBM Spectrum Protect server for schedules that are associated with nodename (mount proxy node), not asnodename (datacenter node). If asnodename is set in `dsm.sys`, schedules that are associated with asnodename (and not nodename) are queried. As a result, scheduling operations fail.

4. Verify the connection to the IBM Spectrum Protect server by issuing this command:
   `dsmc query session`

   This command shows information about your session, including the current node name, when the session was established, server information, and server connection information.

5. Set up the Client Acceptor Service (CAD) and Data Mover Scheduler Service by completing these tasks:

   • Specify these options in the `dsm.sys` file, in the stanza for the mount proxy node:

     – Specify the `managedservices` option with these two parameters:

       ```
       managedservices schedule webclient
       ```

       This setting directs the client acceptor to manage both the Web client and the scheduler.

- If you want to direct schedule and error information to log files other than the default files, specify the `schedlogname` and `errorlogname` options. Each option must contain the fully qualified path and file name in which to store log information. For example:

```
schedlogname /vmsched/dsmsched_mp_lnx.log
errorlogname /vmsched/dsmerror_mp_lnx.log
```

- Start the Client Acceptor Service:

  The installation program creates a startup script for the client acceptor daemon (`dsmcad`) in `/etc/init.d`. The client acceptor daemon must be started before it can manage scheduler tasks, or manage the web client. As root, use the following command to start the daemon:

```
service dsmcad start
```

  To enable the Client Acceptor Daemon to start automatically after a system restart, add the service as follows, at a shell prompt:

```
# chkconfig --add dsmcad
```

6. Verify that the client acceptor and agent are set up correctly:

    a. Log on to a remote system.

    b. Use a web browser to connect to the HOST1 system by using this address and port:

```
http://HOST1.xyz.yourcompany.com:1581
```

## Windows Manually configuring the mount proxy nodes on a remote Windows system

Complete this task to add a mount proxy node to a remote Windows system. This task is required when you want to add a second Windows mount proxy node to your environment.

**Before you begin**
Before you proceed with this task, make sure the primary Windows mount proxy node is configured.

**About this task**
Complete these steps on the remote Windows mount proxy system:

**Procedure**

1. Install the following products on the remote Windows mount proxy system:

   - recovery agent
   - IBM Spectrum Protect data mover

   Access both products on the IBM Spectrum Protect for Virtual Environments download image. Step-by-step installation instructions are available in IBM Knowledge Center at "Installing the Data Protection for VMware components on Windows systems" on page 19

2. Retrieve the sample options file content from the Windows mount proxy node that was created and add it to the options file on the remote Windows mount proxy system:

   a) On the primary Windows mount proxy system, go to the **Configuration** window in the Data Protection for VMware vSphere GUI.

   b) Click **Edit TSM Configuration** in the **Tasks** list. The configuration notebook might take a few moments to load.

   c) Go to the **Mount Proxy Node Pairs** page, and click **Add Mount Proxy Pair**.

   d) In the Primary Node column of the table, go to the Windows mount proxy node with the pending location and click **New Settings**.

e) Make a note of the node passwords for both the **Primary Node** and **Linux Partner Node**. You can use this panel to modify or create a suitable password.

f) Copy the sample `dsm.opt` file content that is shown in the **Mount Proxy Settings** dialog.

g) Paste (or add) the sample `dsm.opt` file content to the options file on the remote Windows mount proxy system. Name the options file with a convention that identifies its role as a remote mount proxy node.
For example: `dsm.REMOTE1_MP_WIN.opt`.

**Restriction:** Do not enable the LAN-free option (ENABLELANFREE YES) in the options file. This option is not supported for mount proxy nodes.

3. Issue this data mover command to set the VMware vCenter user and password for the mount proxy node:

**Tip:** To start the dsmc command line, open the **Windows Start** menu and select **Programs→ IBM Spectrum Protect → Backup Client Command Line**.

```
dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
-optfile=dsm.REMOTE1_MP_WIN.opt
```

4. Verify the connection to the IBM Spectrum Protect server by issuing this command:

```
dsmc query session -optfile=dsm.REMOTE1_MP_WIN.opt
```

This command shows information about your session, including the current node name, when the session was established, server information, and server connection information.

5. Set up the Client Acceptor Service (CAD) and Data Mover Scheduler Service by completing these steps:
This step uses the IBM Spectrum Protect Client GUI Configuration wizard to set up the CAD and Scheduler Service. By default, the Remote Client Agent Service is also set up through the wizard. If you use the IBM Spectrum Protect Client Service Configuration Utility (`dsmcutil`) for this task, make sure to also install the Remote Client Agent Service.
Start the IBM Spectrum Protect Client Configuration wizard from the file menu by going to **Utilities >Setup Wizard**:

a) Select `Help me configure the TSM Web Client`. Enter the information as prompted.

   1) In the `When do you want the service to start?` option, select `Automatically when Windows boots`.

   2) In the `Would you like to start the service upon completion of this wizard?` option, select `Yes`.

   When the operation completes successfully, return to the wizard welcome page and proceed to Step b.

   **Tip:** When you configure more than one mount proxy node on the same system, you must specify a different port value for each client acceptor instance.

b) Select `Help me configure the TSM Client Scheduler`. Enter the information as prompted.

   1) When you enter the scheduler name, make sure to select the `Use the Client Acceptor daemon (CAD) to manage the scheduler` option.

   2) In the `When do you want the service to start?` option, select `Automatically when Windows boots`.

   3) In the `Would you like to start the service upon completion of this wizard?` option, select `Yes`.

6. Verify that the client acceptor and agent are set up correctly. Use a web browser to connect to the HOST1 system by using this address and port:

```
http://HOST1.xyz.yourcompany.com:1581
```

# `Windows` `Linux` Manually configuring file restore capabilities on a secondary server on a remote Windows system

You can manually configure file restore capabilities on a secondary server on a remote Windows system. To complete the task, you must ensure that secondary file-restore mount proxy node pairs are deployed to service the secondary IBM Spectrum Protect server. This task can also be implemented in a multiple domain environment.

**Before you begin**

Both the Windows and Linux mount proxy virtual machines must be available and running. Each secondary server requires a secondary mount proxy node pair for file restore operations. Each mount proxy VM must also have its **Microsoft iSCSI Initiator Service** started. For more information, see `Windows` Starting the Microsoft iSCSI Initiator Service and `Linux` Configuration of Mount Proxy Node pair fails with ANS3144W - Linux.

`Windows` Mount proxy VMs must fulfill these prerequisites:

- Meet the minimum hardware requirements as outlined in Hardware and Software Requirements: Data Protection for VMware
- Be members of the same domain as the VM guest to be restored.

    **Note:** In a multiple domain environment, the mount proxy machines must be members of the same domain that the virtual machine users are members of.

**Procedure**

1. Create a mount proxy node pair:

    a) Select the two new mount proxy machines for file restore capabilities. If necessary, install them with IBM Spectrum Protect.

    - `Windows` During the installation process, select > **Installation Type Advanced** > **Data Mover feature only**.
    - `Linux` During the installation process, select **Data Protection for VMware data mover**

    b) `Windows`

    Create the Windows mount proxy:

    1) On the **Data Mover** tab, select **New Data Mover**.
    2) Ensure that the data mover name ends with the string `REMOTE_MP_WIN`.

        **Note:** If the Windows and Linux data mover names do not match, or do not have the correct string ending, the mount proxy node pairs are not created. Instead, they are treated like data movers.

    3) Provide the IP address for the data mover host name on the Windows VM.
    4) Provide the vCenter user name and password.
    5) Click **ADD**.

        **Note:** An unrequired schedule service is also created. This schedule service can be deleted or ignored.

    c) `Linux`

    Create the Linux mount proxy:

    1) On the **Data Mover** tab, select **New Data Mover**.
    2) Ensure that the data mover name is the same as was used for the Windows mount proxy, but ends with the string `REMOTE_MP_LNX`.

        **Note:** If the Windows data mover names do not match, or do not have the correct string ending, the mount proxy node pairs are not created. Instead, they are treated like data movers.

3) Provide the IP address for the data mover host name on the Linux VM.

4) Provide the vCenter user name and password.

5) Click **ADD**.

6) From the command line, run the following command:

```
iscsiadm -m discovery -t sendtargets -p partner mount proxy
```

where *partner mount proxy* is the IP address of the Linux partner mount proxy.

d) After selecting the **Mount Proxy** tab, click **Refresh** to verify that both the Windows and Linux mount proxies are displayed, and are in a verified state.

2. Run a file restore operation on the new mount proxy node pair:

a) On the new Windows mount proxy machine, edit the file restore options file:

```
C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI\frConfig.props
```

For instructions about editing the file restore options file, see .

b) Apply the following changes in the `frConfig.props` file:

```
default_mp_address=LOCALHOST
default_mp_nodename=node_name_of_new_windows_mount_proxy
enable_filerestore=true
```

where *node_name_of_new_windows_mount_proxy* specifies the node name that is associated with the new Windows mount proxy.

c) Restart services on the mount proxy by restarting the IBM Spectrum Protect for Virtual Environments web server.

d) Set the domain user and password for file restore operations by using the option file that is associated with the new Windows mount proxy by entering the following commands in a command prompt:

```
dsmc set password –type=domain cldev1.local\frank secret -
optfile=dsm.node_name_of_new_windows_mount_proxy.opt
```

where *secret* specifies the password and *node_name_of_new_windows_mount_proxy* specifies the node name that is associated with the new Windows mount proxy.

**Note:** In the above command, `clidev1.local\frank` is the user in the domain `clidev1.local`. This user must also be a member of the domain where the Windows mount proxy is being created. For more information, see � Windows ◼ File restore prerequisites.

e) To start the File Restore User Interface for this secondary server, enter the following URL of the Windows mount proxy:

```
https://hostname:9081/FileRestoreUI/
```

where *hostname* specifies the host name of the Windows mount proxy that hosts the File Restore User Interface.

## Manually configuring multiple client acceptor services on a Linux system

Under certain circumstances, it might be beneficial to use multiple dsmcad services on a single Linux client host.

**About this task**
This task sets up multiple dsmcad instances to run and start automatically at system start:

**Procedure**

1. Create two unique node stanzas in the dsm.sys file (by default, this file is in `/opt/tivoli/tsm/client/ba/bin/`):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
   COMMMethod          TCPip
   TCPPort             1500
   TCPServeraddress    localhost
   nodename            node1
   errorlogname        /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
   schedlogname        /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
   managedservices     webclient sched
   httpport            1581
   passwordaccess      generate

SErvername node2
   COMMMethod          TCPip
   TCPPort             1500
   TCPServeraddress    localhost
   nodename            node2
   errorlogname        /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
   schedlogname        /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
   managedservices     webclient sched
   httpport            1582
   passwordaccess      generate
```

   **Tip:** It might be beneficial to include certain includes/exclude options to differentiate these nodes. Otherwise, the same data might be backed up using the two node names.

2. Create two dsm.opt files, one for each node (by default these files are in `/opt/tivoli/tsm/client/ba/bin`):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. Enable `passwordaccess generate` by logging in with the credentials for both nodes:

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. Make two copies of the default `rc.dsmcad` init script (by default, this script is in `/opt/tivoli/tsm/client/ba/bin`):

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. Edit rc.dsmcad-node1:

   a) Change this line for Red Hat Enterprise Linux distributions:

   ```
   daemon $DSMCAD_BIN
   ```

   To this line:

   ```
   daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
   ```

   b) Change this line for SUSE Linux Enterprise Server distributions:

   ```
   startproc $DSMCAD_BIN
   ```

   To this line:

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

6. Edit rc.dsmcad-node2:

   a) Change this line for Red Hat Enterprise Linux distributions:

   ```
   daemon $DSMCAD_BIN
   ```

   To this line:

   ```
   daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
   ```

   b) Change this line for SUSE Linux Enterprise Server distributions:

   ```
   startproc $DSMCAD_BIN
   ```

   To this line:

   ```
   startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
   ```

7. Create new links in /etc/init.d/ to point to the two new rc.dsmcad init scripts. These links allow the Linux init service to start the dsmcad services at system start:

   ```
   # ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
   # ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
   # ls -la dsm*
   lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
   lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
   ```

8. Register the two new rc scripts with **chkconfig**:

   ```
   # chkconfig --add dsmcad-node1
   # chkconfig --add dsmcad-node2
   ```

9. Test the configuration with the **service dsmcad start** command to make sure the scripts load and start without issue:

   ```
   # service dsmcad-node1 start
   Starting dsmcad-node1:                                    [  OK  ]
   # service dsmcad-node2 start
   Starting dsmcad-node2:                                    [  OK  ]
   # ps -ef | grep dsmcad
   root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
   -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
   root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
   -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
   ```

   The command text is placed on two lines in this example to accommodate page formatting.

10. Restart and confirm that the two dsmcad instances started automatically:

    ```
    # ps -ef | grep dsmcad
    root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
    -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
    root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
    -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
    ```

    The command text is placed on two lines in this example to accommodate page formatting.

# Modifying the VMCLI configuration file

The VMCLI configuration file (`vmcliConfiguration.xml`) contains settings for the Data Protection for VMware vSphere GUI.

The Data Protection for VMware installation process requires that a user specifies a vCenter Server IP address and whether to enable access to the GUI by a web browser. However, after installation, the server IP address and GUI access method cannot be modified by the installer.

To update these settings, you can manually edit the VMCLI configuration file (`vmcliConfiguration.xml`). This file is created during installation in the following locations:
On Windows systems:
`C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI`
On Linux systems:
`/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/`

To modify whether to enable access to the GUI by a web browser, enter one of the following values in the **`<enable_direct_start></enable_direct_start>`** parameter:

- *yes* The GUI can be accessed directly by a web browser. For example:

```
<enable_direct_start>yes</enable_direct_start>
```

- *no* The GUI cannot be accessed directly by a web browser. For example:

```
<enable_direct_start>no</enable_direct_start>
```

To use the GUI for vSphere protection, specify the following value in the **`<mode></mode>`** parameter:

- *vcenter* The GUI is used for vSphere protection. For example:

```
<mode>vcenter</mode>
```

To modify the vCenter server IP address, make sure **`<mode>vcenter</mode>`** is set, then specify the IP address in the **`<vcenter_url></vcenter_url>`** parameter. For example:

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

The `https://` value is required at the beginning of the vCenter server IP address. The `/sdk` value is required at the end of the vCenter server IP address.

**Example `vmcliConfiguration.xml` files**

The following `vmcliConfiguration.xml` file is configured for vSphere protection and web browser access is enabled for the GUI:

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
    <VMCLIPath>C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\
</VMCLIPath>
    <interruptDelay>900000</interruptDelay>
    <mode>vcenter</mode>
    <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
    <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

# Appendix B. Migrating to an incremental-forever incremental backup strategy

Use this procedure to migrate existing backup schedules, policies, and data mover nodes for use in an incremental forever backup strategy.

**Before you begin**

You can use the incremental-forever full backup strategy that was implemented in Data Protection for VMware version 6.2 and 6.3. If you want to continue to use the incremental-forever full backup strategy, you do not need to change your policy or schedules. You must ensure that you upgrade only your data mover nodes to version 6.4 (or later), as documented in the following procedure. However, if you want to use the incremental-forever incremental backup strategy, in addition to updating the data mover nodes to version 6.4 (or later), you must also update the schedules and policy for those data mover nodes that move to this incremental-forever incremental backup strategy.

To migrate existing Data Protection for VMware schedules to an incremental-forever incremental backup strategy, you must complete the tasks documented in this procedure.

**Important:**

- Although some tasks are discrete, all applications and components must be upgraded eventually to completely benefit from the incremental-forever incremental strategy. This publication provides all information to guide you through each task.
- There are several methods available to complete the entire migration process. However, the methods documented in this publication are considered efficient methods for typical Data Protection for VMware environments.
- The schedule to be migrated in this procedure is a schedule that was created with the Data Protection for VMware vSphere GUI backup wizard. If the schedule to be migrated was created manually, then the schedule updates identified in this procedure must also be made manually.

**About this task**

**Procedure**

1. Upgrade all vStorage Backup Servers protecting a single vCenter. Make sure that this upgrade is completed at the same time for all data mover nodes.

   - This upgrade requires installing IBM Spectrum Protect Data Mover version 6.4 (or later) on the vStorage Backup Server.
   - As a discrete task, you do not have to complete Step 2 or Step 3 immediately following Step 1. After upgrading the data mover nodes, you can continue to back up VMs in your existing environment. You can complete Step 2 and Step 3 when a more convenient opportunity becomes available.

   **Tip:** If your environment uses multiple vStorage Backup Servers, consider upgrading only one server. Then, verify that your server operates successfully before upgrading the remaining vStorage Backup Servers.

2. Update the backup policy and backup schedules to implement incremental-forever incremental backups:

   Complete the following backup policy tasks on the IBM Spectrum Protect server by issuing commands in the administrative command-line client (`dsmadmc`):

   a. Create a management class for the appropriate domain and policy set for your incremental-forever incremental backups. This example creates management class `mgmt_ifincr28` for domain

domain1 and policy set prodbackups. The management class name is used to describe an incremental-forever incremental backup strategy that retains 28 backup versions:

```
define mgmtclass domain1 prodbackups mgmt_ifincr28
description="Retain 28 backup versions"
```

b. Create a backup copy group for your incremental-forever incremental backups. This example creates a standard backup copy group for domain domain1, policy set prodbackups, and management class mgmt_ifincr28:

```
define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
```

The standard type=backup entries are default values and are not required to be specified. They are included in this example to illustrate that the copy group name is STANDARD and that the type of copy group is backup (instead of archive).

c. Update the backup copy group with the appropriate version, retention, and expiration settings:

**Remember:** In Data Protection for VMware version 6.2 and 6.3, backup version, retention, and expiration is based on a backup-chain granularity level. This method means that even though both incremental-forever full and incremental-forever incremental backups are taken (as part of the 6.2 and 6.3 incremental-forever full backup strategy), version expiration counts only full backups. In Data Protection for VMware version 6.4 (or later), backup version, retention, and expiration is based on a single-backup granularity level. This method means that version expiration counts both incremental-forever full and incremental-forever incremental backups.

The verexists parameter specifies the maximum number of VM backup versions to retain on the server. If an incremental-forever incremental backup operation causes the number to be exceeded, the server expires the oldest backup version that exists in server storage. This example specifies verexists=28. This value means that a maximum of 28 VM backup versions are retained on the server.

The retextra parameter specifies the maximum number of days to retain a VM backup version, after that version becomes inactive. This example specifies retextra=nolimit. This value means that the maximum number of inactive VM backup versions are retained indefinitely. However, when verexists is specified, the nolimit value is superseded by the verexists value. As a result, in this example, a maximum of 28 inactive VM backup versions are retained on the server.

Based on the settings described in this step, the backup copy group is updated as follows:

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28
retextra=nolimit
```

In this example, the existing Data Protection for VMware version 6.3 environment consists of the following hosts and schedules:

- An ESX cluster (esxcluster) that contains two ESX hosts (esxhost1, esxhost2).
- The bup_esxcluster_full schedule runs a weekly incremental-forever full backup of each ESX host with data mover node dm1.
- The bup_esxcluster_incr schedule runs a daily incremental-forever incremental backup of each ESX host with data mover node dm2.

Complete the following backup schedule tasks in the Data Protection for VMware vSphere GUI:

a. Start the Data Protection for VMware vSphere GUI by clicking the icon in the Solutions and Applications window of the vSphere Client.

b. In the **Getting Started** window, click the **Backup** tab to open the **Managing backup schedules** window.

c. Locate the backup schedule (used for incremental-forever full or incremental backups) to update. In this procedure, the incremental-forever full bup_esxcluster_full schedule is used.

d. Right-click the schedule and select **Properties**.

e. Go to the **Schedule** page and specify **Incremental** from the **Backup strategy** drop-down list.

   f. Click **OK** to save your update.

   g. Locate the backup schedule used for incremental-forever incremental backups. Right-click the schedule and select **Delete**. Since the incremental-forever full `bup_esxcluster_full` schedule was updated to incremental-forever incremental, this incremental-forever incremental schedule is no longer needed.

3. Now that you have an incremental-forever incremental backup schedule, you can reduce the number of data mover nodes by consolidating them:

   This example consolidates two data mover nodes into one data mover node.

   a) On the vStorage Backup Server, open a command prompt and go to the directory where the options file for dm1 is located.

   b) Using a text editor (such as Notepad), update this file with the following options:

      1) Specify `vmmaxparallel` to control the number of VMs backed up at one time by dm1:

      ```
      vmmaxparallel=2
      ```

      The default value and minimum value are 1. The maximum value is 50.

      **Tip:** For every data mover node you remove, increase the `vmmaxparallel` value by 1.

      Alternatively, you can specify `vmlimitperhost` to control the number of VMs backed up at one time by dm1 from the same ESX host:

      ```
      vmlimitperhost=1
      ```

      This option is useful when wanting to prevent a host from being overloaded. The default value is 0 (no limit). The minimum value is 1. The maximum value is 50.

   c) Log on the IBM Spectrum Protect server. Use the administrative command-line client (`dsmadmc`) to specify the maximum number of simultaneous VM backup sessions that can connect with the server. For example:

   ```
   maxsessions=4
   ```

   The default value is 25. The minimum value is 2.

4. Verify that the updated data mover nodes are working properly:

   a) Start the Data Protection for VMware vSphere GUI by clicking the icon in the Solutions and Applications window of your vSphere Client.

   b) In the **Getting Started** window, click the **Configuration** tab to view the **Configuration Status** page.

   c) In the **Configuration Status** page, select the vCenter that is protected in Step 1. Click a data mover node to view its status information in the **Status Details** pane.

   When a node displays a warning or error, click that node and use the information in the **Status Details** pane to resolve the issue. Then, select the node and click **Validate Selected Node** to verify whether the issue is resolved. Click Refresh to retest all nodes.

**Results**

Upon successful completion of each task, the environment is ready for use in an incremental-forever incremental backup strategy.

**Restrictions**: After migrating schedules from incremental-forever full backup types to incremental-forever incremental backup types, be aware of the following restrictions:

• Changing migrated schedules back to incremental-forever full backup types per VM (file space) is not supported.

• Using an earlier version of the IBM Spectrum Protect data mover on a migrated file space is not supported.

- When a file space contains one (or more) incremental-forever incremental backups, a incremental-forever full backup is not supported.

**Example of version control with the `verexists` parameter**

In this schedule migration example, Data Protection for VMware version 6.3 uses the following two backup schedules:

- `-mode=full`: A weekly incremental-forever full backup is scheduled (Sundays) and the maximum number of VM backup versions to retain on the server is four (`verexists=4`).
- `-mode=incr`: A weekday incremental-forever incremental backup is scheduled (Monday through Saturday).

The number of backups taken for a four week period is 28:

- Four incremental-forever full backups (one weekly full backup multiplied by four weeks)
- 24 incremental-forever incremental backups (six weekday incremental backups multiplied by four weeks)

Since Data Protection for VMware version 6.3 counts only full backups, the `verexists=4` value preserves all 28 backups.

To provide the same level of protection with Data Protection for VMware version 6.4 (or later) and the incremental-forever incremental backup strategy, create the following schedule:
`-mode=iffull`: A daily incremental-forever full backup is scheduled and the `verexists` parameter is set to 28.
The number of backups taken for a four week period is 28:

- One incremental-forever full backup (initial backup multiplied by one day)
- 27 incremental-forever incremental backups (daily incremental forever backups multiplied by 27 days)

Since Data Protection for VMware version 6.4 (or later) counts both incremental-forever full and incremental-forever incremental backups, the `verexists=28` value preserves all 28 backups.

# Appendix C. Accessibility features for the IBM Spectrum Protect product family

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

**Overview**

The IBM Spectrum Protect family of products includes the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader

The IBM Spectrum Protect family of products uses the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) and Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the product.

The product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described in the Accessibility section of the IBM Knowledge Center help (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

**Keyboard navigation**

This product uses standard navigation keys.

**Interface information**

User interfaces do not have content that flashes 2 - 55 times per second.

Web user interfaces rely on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

Web user interfaces include WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

**Vendor software**

The IBM Spectrum Protect product family includes certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for accessibility information about its products.

**Related accessibility information**

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility (www.ibm.com/able).

# Notices

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

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

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

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


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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

**Trademarks**

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

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

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

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

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

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

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

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

**Terms and conditions for product documentation**

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

**Applicability**

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

**Personal use**

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

**Commercial use**

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

**Rights**

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

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

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

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


**Privacy policy considerations**

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

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

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

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

# Glossary

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

See the IBM Spectrum Protect glossary.

# Index

**IBM**®

Product Number:   5725-X00