IBM Tivoli Storage Manager for Virtual Environments
Version 7.1.6

# *Data Protection for VMware Installation Guide*

IBM Tivoli Storage Manager for Virtual Environments
Version 7.1.6

# *Data Protection for VMware Installation Guide*

**Note:**

Before you use this information and the product it supports, read the information in “Notices” on page 133.

**Sixth edition (June 2016)**

This edition applies to version 7, release 1, modification 6 of IBM Tivoli Storage Manager for Virtual Environments (product number 5725-A44) and to all subsequent releases and modifications until otherwise indicated in new editions.

# Contents

# About this publication

IBM® Tivoli® Storage Manager 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 Tivoli Storage Manager for Virtual Environments with the Tivoli Storage Manager backup-archive client. In addition, protection of vApps and Organization VDCs in a vCloud Director environment is also available.

## Who should read this publication

This publication is intended for users and administrators who want to install and configure IBM Tivoli Storage Manager for Virtual Environments.

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

## Publications

The Tivoli Storage Manager product family includes IBM Tivoli Storage FlashCopy® Manager, IBM Tivoli Storage Manager for Space Management, IBM Tivoli Storage Manager for Databases, and several other storage management products from IBM.

To view IBM product documentation, see IBM Knowledge Center.

# What's new in Version 7.1.6

Data Protection for VMwareVersion 7.1.6 introduces new features and updates.

For a list of new features and updates in this release and previous Version 7 releases, see Data Protection for VMware updates.

New and changed information in this product documentation is indicated by a vertical bar (|) to the left of the change.

# Chapter 1. Installing and upgrading Data Protection for VMware

Installation of Data Protection for VMware includes planning, installation, and initial configuration.

## Installable components

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

Depending on the operating system environment, the following Data Protection for VMware features are available for installation:

**Restriction:** Each installation package presents you with a user licensing file (EULA). If you do not accept the file, the installation process stops.

*Table 1. Available Data Protection for VMware features by operating system*

| Component | Linux | Windows |
|---|---|---|
| **Tivoli Storage Manager recovery agent**<br>This component provides virtual mount and instant restore capabilities. | √ | √ |
| **Recovery agent command-line interface**<br>The command-line interface used for mount operations. | | √ |
| **Documents**<br>Documents include the readme and notices files. | √ | √ |
| **Data Protection for VMware enablement file**<br>This component enables Tivoli Storage Manager to run the following backup types:<br>• Periodic incremental VM backup.<br>• Full VM incremental-forever backup.<br>• Incremental-forever-incremental VM backup.<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 features by operating system (continued)

| Component | Linux | Windows |
|---|---|---|
| **Data Protection for VMware vSphere GUI**<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 three views:<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>`https://guihost.mycompany.com:9081/TsmVMwareUI/`<br>• A plug-in view that integrates with the VMware vSphere Client. This plug-in is accessed as a vCenter Server extension in the Solutions and Applications panel of your vCenter Server System. The panels and functionality of this view are the same as offered in the browser view.<br>**Tip:** The plug-in view is not supported in a VMware vSphere 6 environment.<br>• The IBM Data Protection extension view in the VMware vSphere Web Client. This panels in this view are uniquely designed to integrate within the web client, but data and commands for this view are obtained from the same GUI web server as the other views. The IBM Data Protection extension provides a subset of the functions that are available in the web browser and plug-in views and some additional functions. Configuration and advanced reporting functions are not offered in this view.<br>You can specify one or more views during installation. | √ | √ |
| **Data Protection for VMware vCloud GUI**<br>When you run the Tivoli Storage Manager for Virtual Environments installation wizard, you must select one of the following environment protection options: **vSphere Protection** or **vCloud Protection**. If you select **vCloud Protection**, the Data Protection for VMware vCloud GUI is installed.<br>This component is a web-based GUI that protects and manages vApps. It also organizes vDCs in a vCloud Director environment. This component also includes the Data Protection for VMware command-line interface. | √ | √ |
| **File restore GUI**<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. | [1] | √ |

*Table 1. Available Data Protection for VMware features by operating system (continued)*

| Component | Linux | Windows |
|---|---|---|
| **Data mover**<br>The Tivoli Storage Manager backup-archive client moves data for Data Protection for VMware. This functionality is referred to as the data mover. The data mover moves data from the virtual environment to the Tivoli Storage Manager 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. | √ | √ |

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.

Data Protection for VMware offloads the backup workload from VMs to a vStorage backup server. To accomplish this task, the backup-archive client V7.1.6 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 a Tivoli Storage Manager server.
- Initiate a full recovery of your VMs from a Tivoli Storage Manager 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.

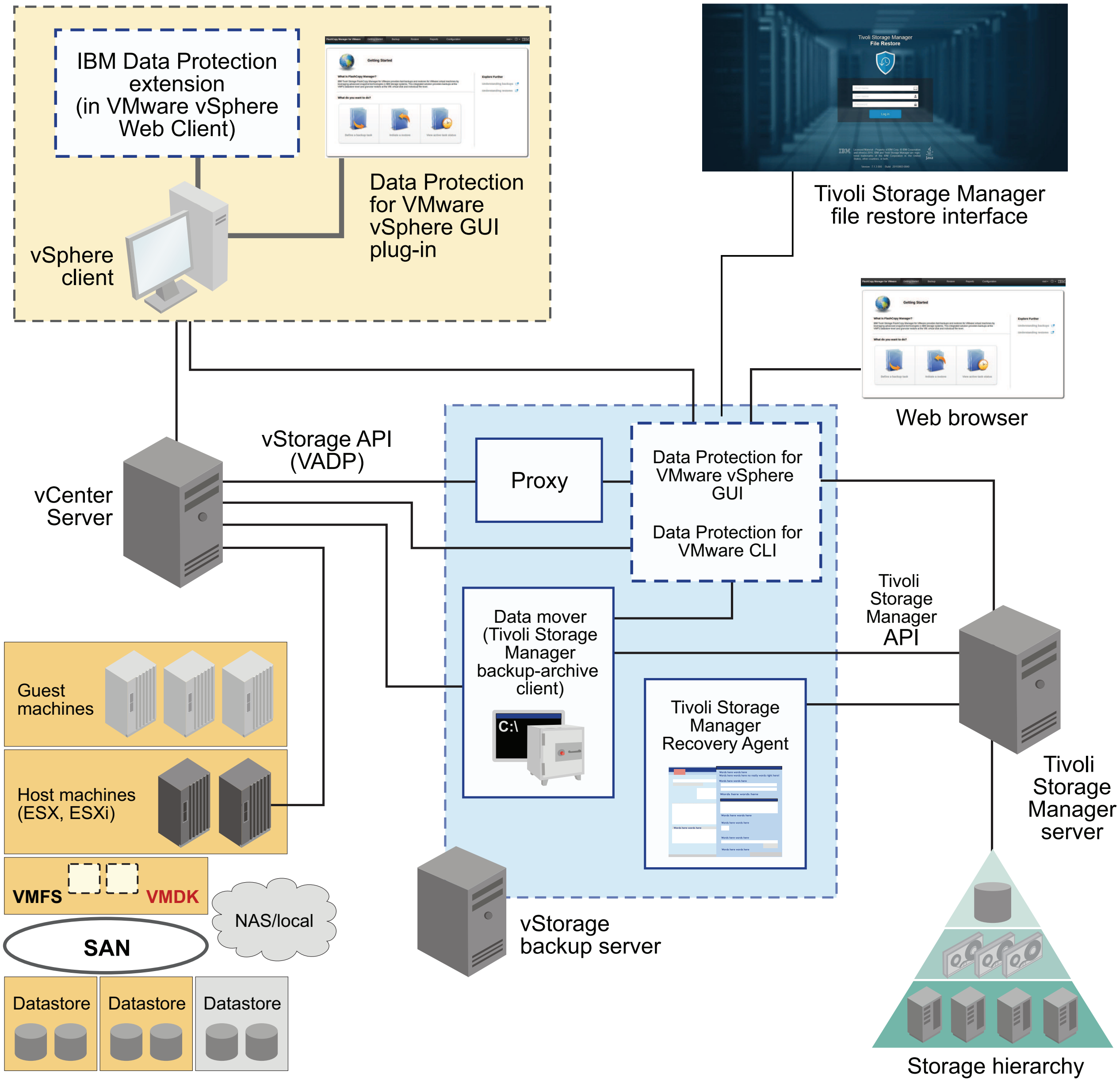
IBM Data Protection extension (in VMware vSphere Web Client)
Data Protection for VMware vSphere GUI plug-in
vSphere client
Tivoli Storage Manager file restore interface
Web browser
vStorage API (VADP)
vCenter Server
Proxy
Data Protection for VMware vSphere GUI
Data Protection for VMware CLI
Tivoli Storage Manager API
Data mover (Tivoli Storage Manager backup-archive client)
C:\
Tivoli Storage Manager Recovery Agent
Tivoli Storage Manager server
Guest machines
Host machines (ESX, ESXi)
VMFS
VMDK
NAS/local
SAN
Datastore
Datastore
Datastore
vStorage backup server
Storage hierarchy

*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
- Tivoli Storage Manager 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. Each plug-in can then manage a subset of the total number of datacenters that are defined on the vCenter Server. For each plug-in that is registered to the vCenter Server, one Data Protection for VMware package must be installed on a separate host.

To update the managed datacenters, go to **Configuration** > **Edit Configuration**. In the Plug-in Domain page, reduce the list of datacenters that are managed by the plug-in. Managing a subset of all available datacenters reduces the query and processing time that is required by the plug-in to complete operations.

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 plug-in that integrates with the VMware vSphere Client. This plug-in is accessed as a vCenter Server extension in the Solutions and Applications panel of your vCenter Server system.
- 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 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 plug-in and web browser GUI.

You can specify one or more access methods during installation.

Windows The default installation directory is C:\IBM\tivoli\tsm\tdpvmware\webserver.

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

## Data Protection for VMware vCloud GUI

The Data Protection for VMware vCloud GUI (vCloud GUI) component is a graphical user interface that protects vApps and organization vDCs in a vCloud Director environment.

### Overview

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

- Initiate or schedule incremental forever backups of specific vApps, or vApps that are contained in an organization vDC to the Tivoli Storage Manager server storage.
- Restore single or multiple vApps.
- Generate reports to display progress information about tasks and space-usage information about backups.
- Display information about the progress of tasks, the most recent events that completed, the backup status of vApps, and space usage. This information can help you troubleshoot errors that occurred in backup processing.

**Tip:** Information about how to complete tasks with the vCloud 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.

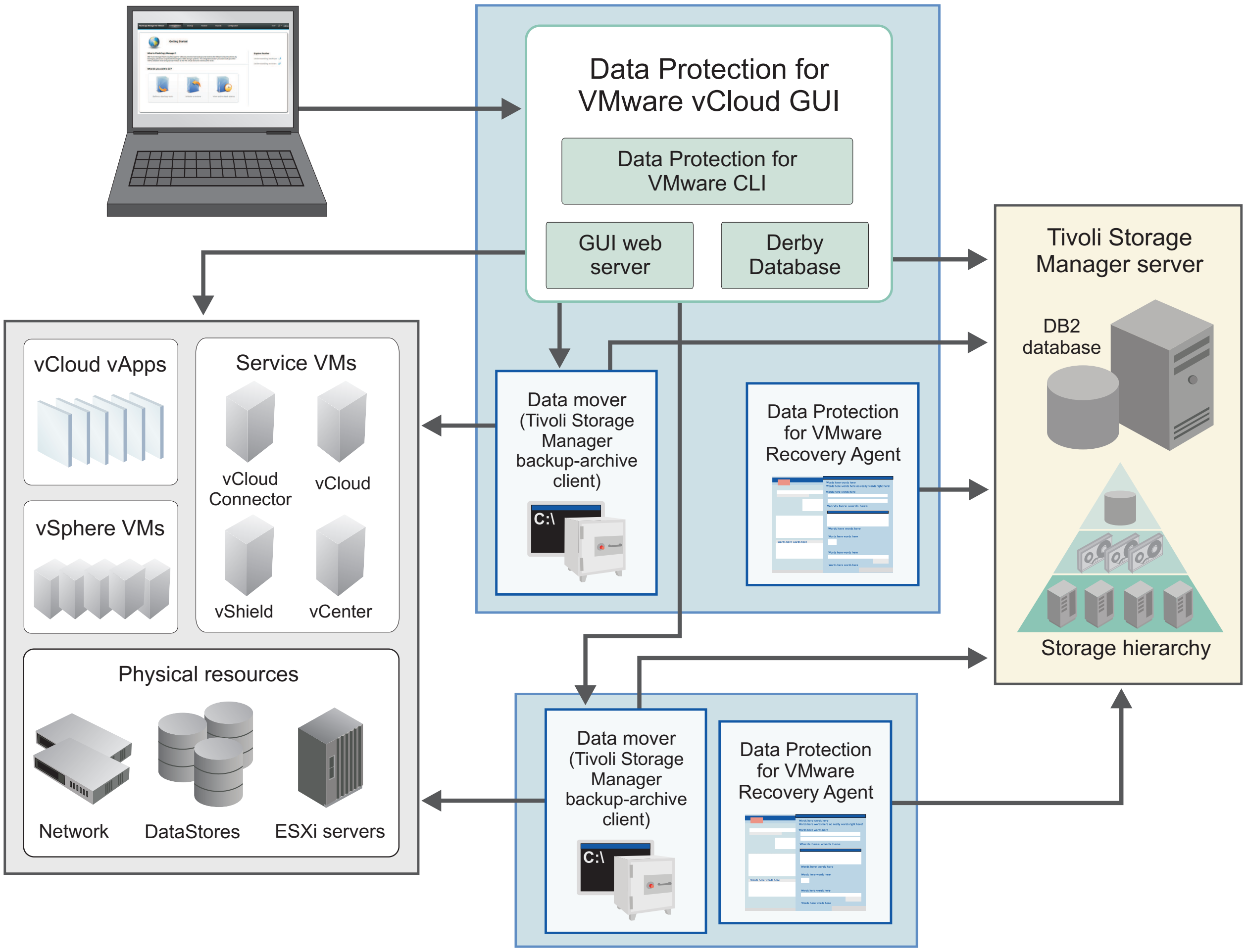
Data Protection for VMware vCloud GUI
Data Protection for VMware CLI
GUI web server
Derby Database
Tivoli Storage Manager server
DB2 database
Storage hierarchy
vCloud vApps
Service VMs
vCloud Connector
vCloud
vSphere VMs
vShield
vCenter
Data mover (Tivoli Storage Manager backup-archive client)
C:\
Data Protection for VMware Recovery Agent
Physical resources
Network
DataStores
ESXi servers
Data mover (Tivoli Storage Manager backup-archive client)
C:\
Data Protection for VMware Recovery Agent

*Figure 2. Data Protection for VMware system components in a VMware vCloud Director user environment*

## Accessing the vCloud GUI

The vCloud GUI is accessed through a web browser by using the following URL:

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

where:

- *hostname* is the name of the system where the Data Protection for VMware vCloud GUI is installed
- *port* is the port number where the vCloud GUI is accessible through. The default port number is 9081.

Windows The default installation directory is `C:\IBM\tivoli\tsm\tdpvmware\webserver`.

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

## Tivoli Storage Manager recovery agent

Use the recovery agent service to mount any snapshot volume from the Tivoli Storage Manager server.

### Overview

You can view snapshots locally, with read-only access, on the client system, or use an iSCSI protocol to access a snapshot from a remote system.

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.

**Important:** When you install the recovery agent for the instant restore function, you must also select the device driver for installation. It is not selected by default. Choosing this option requires a system reboot.

The device driver is not required for application 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.
- Mount a snapshot as a virtual device.
- Provide a list of virtual devices.
- Remove a virtual device.

### Requirements

Windows On Windows systems, you can install the recovery agent GUI, command-line interface, and device driver.

Linux On Linux systems, you can install the recovery agent GUI and device driver. The command-line interface is not available.

### Accessing the recovery agent

Windows You can access the recovery agent from the **Start** menu: **Start** > **Tivoli Storage Manager** > **Tivoli Storage Manager for Virtual Environments** > **Tivoli Storage Manager recovery agent**

Windows Alternatively, you can access the GUI and command-line interface from a command prompt:

```
install_dir\TSM\recoveryagent\mount\RecoveryAgent.exe -notservice
install_dir\TSM\recoveryagent\shell\RecoveryAgentShell.exe
```

where *install_dir* is the installation directory. The default is `C:\Program Files\Tivoli`. On Windows 64-bit systems, use `Program Files (x86)`.

Linux To start the recovery agent, issue the following commands from a command line as `root` user:

```
cd /opt/tivoli/tsm/tdpvmware/mount
./TDPVMwareMountRestore.sh
```

## IBM Data Protection extension

The IBM Data Protection extension is a VMware vSphere Web Client extension that provides a view of the Data Protection for VMware vSphere GUI.

### Overview

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

### Requirement

To install the IBM Data Protection extension, you must select the following options when you run the Tivoli Storage Manager for Virtual Environments installation wizard.

- On the Environment Protection page of the installation wizard, click **vSphere protection**.
- On the GUI information for vSphere protection page, select **Enable access to the GUI by a web browser** and **Register as an Extension in vSphere Web Client**.

### Accessing the data protection extension

You can access the extension from the vSphere Web Client.

## 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 a Tivoli Storage Manager server.
- Initiate a full recovery of your VMs, VM files, or VM Disks (VMDKs) from a Tivoli Storage Manager 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.

## Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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

The data mover is a specific backup-archive client node that "moves" data from one system to another.

### Overview

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

For more information about the data mover, including information about environments with multiple data movers, see How Tivoli Storage Manager nodes are used in a virtual environment.

### Accessing the data mover configuration files

You can configure the data mover from the Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI.

Windows The default installation directory is `C:\Program Files\Tivoli\TSM\baclient`.

Linux The default installation directory is `/opt/tivoli/tsm/client/ba/bin`.

## 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 ESX or ESXi-based host to a vStorage Backup server.

Data Protection for VMware works with the backup-archive client (installed on the vStorage Backup server) to complete full and incremental backups of VMs. The client node that is installed on the vStorage Backup server is called the data mover node. This node "moves" the data to the Tivoli Storage Manager 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. In addition, protection of vApps and organization vDCs in a vCloud Director environment is also available.

**Tip:** The backup-archive client 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 (backup-archive client).

### 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>• Installing Data Protection for VMware by using the installation wizard<br>• “Installing the Data Protection for VMware components in silent mode” on page 29<br>Upgrade Data Protection for VMware:<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 page 57<br>If you are planning to upgrade Data Protection for VMware, depending on the components that are installed, more configuration tasks might be required. See Configure Data Protection for VMware 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 Tivoli Storage Manager Wiki:
Step by Step Guide To vStorage Backup Server (Proxy) Sizing
This publication is available in the Tivoli Storage Manager 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 24
- "Installing the Data Protection for VMware components in silent mode" on page 29

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 (backup-archive client) on the same system. | Windows You can use the Suite Installer in GUI or silent mode to install both software. **Restriction:** On Windows 32-bit systems, the only the recovery agent GUI and command line are available to install.<br>Linux You can use the Data Protection for VMware and data mover stand-alone installers to install both software in GUI or silent mode. |

*Table 3. Installation scenarios (continued)*

| Scenario Number | Description | Tasks that you must complete |
|---|---|---|
| 2 | Use this scenario for a new installation where you want to install only Data Protection for VMware. | Windows You can complete a custom installation by using the Suite Installer or you can use the stand-alone installer to install Data Protection for VMware in GUI or silent mode.<br>**Restriction:** On Windows 32-bit systems, the only the recovery agent GUI and command line are available to install.<br>Linux You must use the Data Protection for VMware stand-alone installer in GUI or silent mode to install Data Protection for VMware. |
| 3 | Use this scenario when you want to install only the data mover (backup-archive client) on a system. | Windows You can complete a custom installation by using the Suite Installer or you can use the stand-alone installer to install the data mover in GUI or silent mode.<br>**Restriction:** The data mover is not available on Windows 32-bit systems.<br>Linux You must use the data mover stand-alone installer in GUI or silent mode to install the data mover.<br>**Tip:** You can install the data mover on a different system than the system with Data Protection for VMware to free up resources. |

# System requirements

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

## Software requirements

*Table 4. Software requirements for Data Protection for VMware.*

| Component | Minimal requirement | Preferred |
|---|---|---|
| Operating system | **Important:** Details of the software and operating system requirements can change over time. For current software requirements, see technote 1505139. | |
| Communication protocol | | |
| Device drivers | | |
| Other software | | |

## 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 Tivoli Storage Manager 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 5. Hardware requirements for Data Protection for VMware.*

| Component | Minimal requirement | Preferred |
|---|---|---|
| System | IntelPentium D 3 GHz Dual Core processor or compatible | Not applicable |
| Memory | 2 GB RAM, 2 GB virtual address space | Not applicable |
| Available hard disk | 200 MB for 'Documents and Settings' folder | 2 GB |
| NIC Card | 1 NIC - 100 Mbps | 1 NIC - 1 Gbps |

A Windows proxy host is required for Tivoli Storage Manager recovery agent on Linux. This Windows proxy host must have the Tivoli Storage Manager recovery agent installed.

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

- For incremental forever 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, see Vmmaxvirtualdisks.
- For periodic full backup mode, each individual VMDK involved in a backup operation cannot exceed 2 TB. If a VMDK exceeds 2 TB, the backup operation fails.

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

## File restore prerequisites

Before you restore files with the Tivoli Storage Manager 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:

- Linux Windows VMware Tools must be installed on the virtual machine.
- Linux Windows The virtual machine must be running during the file restore operation.

- Windows The virtual machine must belong to the same Windows domain as the data mover system.
- 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.
- 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 backup-archive client 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 Tivoli Storage Manager 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.

Linux Windows 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:

- Windows Windows domain administrator credentials are required to access the network share. An administrator enters these 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 Tivoli Storage Manager 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 Tivoli Storage Manager file restore interface.

### Tape media prerequisites

File restore from tape media is supported. However, recovery of individual files generates random read request patterns. As a result, processing might be slow when a sequential-access device (such as tape media) is used. File restore from disk storage is the preferred method.

Consider moving target virtual machine backup data from tape media to disk storage before you attempt a file restore operation. You can do move data with the Tivoli Storage Manager server **MOVE NODEDATA** command. You can also run traditional full VM backups regularly.

## Required installation permissions

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

### About this task

*Table 6. Users permissions required to install and configure Data Protection for VMware*

| **System** | **Required permission** |
|---|---|
| Windows | Administrator |
| Linux | Root |
| vCenter Server | Administrator privileges<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. |
| Tivoli Storage Manager server<br>**Restriction:** The server must be started. | Administrative access<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
- Tivoli Storage Manager 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 7. 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) |
| 443 | Data Protection for VMware vSphere GUI Server | vCenter Server |
| 443<br>This setting is required only when the data mover is a Linux system. | Windows mount proxy | vCenter Server |
| 902<br>443 | vCenter Server | ESXi hosts |
| 902<br>443 | vStorage Backup Server (proxy) | ESXi hosts (all protected hosts) |
| 1500 (`tcpport`) | vStorage Backup Server (proxy) | Tivoli Storage Manager server |

*Table 7. Required communication ports (continued).* 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) |
|---|---|---|
| 1500 (**tcpadminport**) | Data Protection for VMware vSphere GUI Server<br>• 1500 (**tcpadminport**) is non-SSL communication<br>• For SSL communication, **tcpadminport** is the only port that supports SSL communication with the Tivoli Storage Manager server. The correct port number to use for the SSL protocol is typically the value that is specified by the **ssltcpadminport** option in the Tivoli Storage Manager 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. | Tivoli Storage Manager server |
| 1527<br>Internal Derby database | | |
| 1501<br>1581 (**httpport**) | Tivoli Storage Manager server | vStorage Backup Server<br>• Backup-archive client scheduler<br>• Web client<br>• Client Acceptor Daemon |
| 1581 (**httpport**)<br>1582, 1583 (**webports**) | Data Protection for VMware vSphere GUI server | vStorage Backup Server |
| 9080 | vSphere Client | Data Protection for VMware vSphere GUI Server (HTTP port for access to vCenter as plug-in) |
| 9081<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>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 |

*Table 7. Required communication ports (continued).* 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) |
|---|---|---|
| 3260<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 |
| 135 | Windows mount proxy | VMware virtual machine that contains the files to be restored with the Tivoli Storage Manager file restore interface |

## 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 install the vSphere Client plug-in or IBM Data Protection extension view for the Data Protection for VMware vSphere GUI

To install the vSphere Client plug-in or IBM Data Protection extension view for the Data Protection for VMware vSphere GUI, the vSphere user requires the **Extension** > **Register extension, Unregister extension, Update extension** privileges. From the VMware vSphere client, you can create a role and add to the role the extension set of associated privileges. You must then assign this role to the vCenter object in the VMware vCenter Server hierarchy for the user ID that you plan to use during the installation process. You must enter this user ID when prompted for the vCenter user name on the following pages of the Tivoli Storage Manager for Virtual Environments installation wizard:

- vSphere Client plug-in: Plug-in Registration vCenter page
- IBM Data Protection extension: Data Protection for VMware vSphere GUI information page

**Tip:** Alternatively, rather than creating a specific role for the installation, you can enter the administrator user name when prompted for the vCenter user name.

### vCenter Server privileges required to protect VMware datacenters with the web-browser or vSphere Client plug-in view for the Data Protection for VMware vSphere GUI

The vCenter Server user ID that signs on to the browser or plug-in views 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. You must assign this role to a user ID for a specified vCenter Server or datacenter. 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 and plug-in view GUIs 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 Tivoli Storage Manager backup-archive client 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 technote 7047438.

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 theIBM Data Protection extension view for the Data Protection for VMware vSphere GUI

The IBM Data Protection extension 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 Data Protection extension:

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

Custom privileges that are required for the IBM Data Protection extension 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 Data Protection extension content. Only users with these custom privileges on the required VMware object can access the IBM Data Protection extension content. One IBM Data Protection extension 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 Data Protection extension. 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 Data Protection extension 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 Data Protection extension in the vSphere web client to manage virtual machines in their respective datacenters only.

## Issues related to insufficient permissions

When the web browser or vSphere Client plug-in view 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 Data Protection extension 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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
```

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 GUI registration keys

Depending on the options that 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
- Data Protection for VMware vSphere GUI accessed as a plug-in from either of the vSphere GUIs
- IBM Data Protection extension in the vSphere Web Client GUI

The Data Protection for VMware vSphere GUI plug-in registration key is `com.ibm.tsm.tdpvmware@hostname`. This key is registered when you select the **Register GUI as vCenter plug-in** check box during the installation. A separate key is registered for each web GUI host. When multiple web GUI hosts exist, then multiple instances of the Data Protection for VMware vSphere GUI plug-in are registered.

IBM Data Protection extension 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 Data Protection extension 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.

## 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:

- Tivoli Storage Manager recovery agent
- Recovery agent command-line interface
- Documentation (readme file and notices file)
- Data Protection for VMware enablement file
- Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI
- Data mover feature (backup-archive client), which includes the following items:
  - Backup-archive client GUI
  - Backup-archive web client
  - Client API (64-bit) runtime files
  - Administrative client command line
  - VMware vStorage API runtime files

**Restriction:** You can install only the data mover feature and Data Protection for VMware vSphere or vCloud GUI on 64-bit systems, not 32-bit systems.

**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 a DVD or an IBM download site such as IBM Passport Advantage®.

Linux

### Before you begin

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, or you can access the files from the product DVD:
   - 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 Tivoli Storage Manager 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 128 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, for example, `7.1.6.000-TIV-TSM4VE-LinuxX64.bin`.

   d. Windows Extract the package by double-clicking the *package_name*, where *package_name* is the name of the downloaded file, for example, `7.1.6.000-TIV-TSM4VE-Windows.bin`.

## 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 the Data Protection for VMware and the data mover (backup-archive client). Optionally, you can use the Data Protection for VMware stand-alone installer or the data mover stand-alone installer.

Linux You can install Data Protection for VMware by using the Data Protection for VMware stand-alone installer. Similarly, you can use the data mover stand-alone installer to install 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 5.x (or later) with administrator privilege access.
- Network connectivity to a Tivoli Storage Manager 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 13
  - "Required installation permissions" on page 16
  - "Required communication ports" on page 17

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**
With advanced installations, you can select the components and features that you want to install.

**Restriction:** The following components and features are only available to install on Windows 64-bit systems:

- Data mover (backup-archive client)
- Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI

**Environment Protection**
During the installation, you must choose one of the following environments to protect your data:

**Protect data in a vSphere environment**
With the Data Protection for VMware vSphere GUI, you can back up, restore, and manage VMs in a VMware vCenter environment.

**Protect data in a vCloud Directory environment**
With the Data Protection for VMware vCloud GUI, you can back up, restore, and manage vApps and organization virtual data centers.

### About this task

You can use the Suite Installer to install both Data Protection for VMware and the data mover feature. The `spinstall.exe` file for the Suite Installer is located at the root of the installation package that is on DVD or in the installation folder.

Alternatively, you can use the separate stand-alone installers to install Data Protection for VMware and the data mover feature separately. The `spinstall.exe` file for Data Protection for VMware is in the `tsm4ve` directory in the installation package. The `spinstall.exe` file for the data mover feature is in the `client` directory in 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 or the data mover feature, 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. When you install the recovery agent for instant restore, you must also select the device driver for installation. It is not selected by default. Choosing this option requires a system reboot.

### What to do next

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

- "Accessing the Data Protection for VMware vSphere GUI" on page 41
- "Accessing the Data Protection for VMware vCloud GUI" on page 42

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 13
  - "Required installation permissions" on page 16
  - "Required communication ports" on page 17

### Procedure

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

1. From the root of the DVD or 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 87.

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 a Linux system" on page 55.

You can install the data mover feature (backup-archive client) on the same system as Data Protection for VMware or install it on a separate system. To install the data mover feature, see "Installing the data mover feature on Linux systems."

## Installing the data mover feature on Linux systems

Install the data mover feature (backup-archive client) on Linux systems by using the InstallAnywhere mode.

### Before you begin

### Procedure

To install the data mover feature, complete the following steps:

1. Open a command line and change directories to `CD/Linux/DataMover`.
2. If the Tivoli Storage Manager API is not already installed on the system, complete the following steps from a command line:
   a. Install the 64-bit GSKit packages:

      ```
      rpm -U gskcrypt64-version.linux.x86_64.rpm gskssl64-version.linux.x86_64.rpm
      ```

      where *version* represent the GSKIT version in the file name on the installation media. For example, in the `gskcrypt64-8.0.50.35.linux.x86_64.rpm` and `gskssl64-8.0.50.35.linux.x86_64.rpm` files, the *version* is `8.0.50.35`.

   b. Install the 64-bit Tivoli Storage Manager API:

      ```
      rpm -ivh TIVsm-API64.x86_64.rpm
      ```

   c. Optional: Install the Common Inventory Technology package that is used by the API to supports processor value unit (PVU) calculations. This package depends on the API so it must be installed after the API package is installed.

      ```
      rpm -ivh TIVsm-APIcit.x86_64.rpm
      ```

3. Install the backup-archive client, command-line client, administrative client, web client, and the documentation:

   ```
   rpm -ivh TIVsm-BA.x86_64.rpm
   ```

4. Optional: Install the Common Inventory Technology package the client uses to send PVU metrics to the server. This package depends on the client package so it must be installed after the client package is installed.

   ```
   rpm -ivh TIVsm-msg.language_ID.x86_64.rpm
   ```

### Results

If you receive any warnings or errors, check the log files for more information. See "Log file activity" on page 87.

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 a Linux system" on page 55.

## 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 the Data Protection for VMware and the data mover (backup-archive client). Optionally, you can use the Data Protection for VMware stand-alone installer or the data mover stand-alone installer.

Linux You can install Data Protection for VMware by using the Data Protection for VMware stand-alone installer. Similarly, you can use the data mover stand-alone installer to install the data mover.

### Installing Data Protection for VMware in silent mode on Windows systems by using the Suite Installer

Use the Suite Installer to install all of the components for Data Protection for VMware in silent mode.

### About this task

Use the Suite Installer to install all of the components and features from one package.

**Restriction:** On Windows 32-bit systems, you can install only the recovery agent GUI and command-line interface.

### Installing Data Protection for VMware on Windows 32-bit systems by using the Suite Installer in silent mode:

Install the recovery agent GUI and command-line interface silently on a Windows 32-bit operating system.

#### About this task

**Restriction:** All features are installed to their default location. To locate the default installation directories for the components, see the subtopics in "Installable components" on page 1.

#### Procedure

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

1. Open a command prompt and enter the following command:

   ```
   spinstall.exe /silent SETUP_SUPPORT_DIR="directory to setup.iss file"
   ```

   For example, if the `setup.iss` file is in the `C:\install\test` directory, enter the following command:

   ```
   spinstall.exe /silent SETUP_SUPPORT_DIR="C:\install\test"
   ```

   The default location of the `setup.iss` file is `C:\TSM4VE_WIN\tsm4ve\X86`.
2. Restart the system.

   **Note:** The following message displays 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?
   ```

   You must register the Virtual Volume Driver to proceed with the recovery agent operations.

**Related tasks**:

"Uninstalling Data Protection for VMware for a Windows 32-bit system in silent mode" on page 53

### Installing Data Protection for VMware on Windows 64-bit systems by using the Suite Installer in silent mode:

Install all Data Protection for VMware components and the data mover feature (backup-archive client) 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 13
- "Required installation permissions" on page 16
- "Required communication ports" on page 17

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

*Table 8. Data Protection for VMware silent installation parameters*

| Parameter | Description | Default value |
|---|---|---|
| **ISFeatureInstall** | Specify one or both of the following options:<br>**TSM4VE** Install all Data Protection for VMware features except the recovery agent device driver.<br>**Client** Install all data mover features. | TSM4VE,Client |
| **ComponentsToInstallVe** | Specify the Data Protection for VMware features to install. Use the features that are described in Table 9 on page 32 | None |
| **ComponentsToInstallBa** | Specify the data move features to install. Use the features that are described in Table 10 on page 33 | None |
| **GUI_MODE** | To protect data in a vSphere environment, specify **GUI_MODE=vcenter**.<br>This parameter installs the Data Protection for VMware vSphere GUI. This GUI integrates the product with the VMware vSphere client to back up, restore, and manage VMs in a VMware vCenter environment. Includes the Data Protection for VMware command-line interface. You can install only one Data Protection for VMware vSphere GUI on a machine. As a result, multiple Data Protection for VMware vSphere GUIs are not allowed on the same machine. vcenter is the default value when **GUI_MODE** is specified.<br>To protect data in a vCloud environment, specify **GUI_MODE=vcloud**.<br>This parameter installs the Data Protection for VMware vCloud GUI. This GUI integrates the product with the vCloud Director environment to back up, restore, and manage vApps and organization vDCs. Includes the Data Protection for VMware command-line interface. | vcenter |
| **VCENTER_HOSTNAME** | The vCenter Server fully qualified domain name or IP address. This feature is required when **GUI_MODE=vcenter** is specified. | None |
| **VCENTER_USERNAME** | The vCenter user ID. This user ID must be a VMware administrator that has permission to register and unregister extensions. This feature is required when **GUI_MODE=vcenter** is specified. | None |
| **VCENTER_PASSWORD** | The vCenter password. This feature is required when **GUI_MODE=vcenter** is specified. | None |

Table 8. Data Protection for VMware silent installation parameters (continued)

| Parameter | Description | Default value |
|---|---|---|
| **VCLOUD_HOSTNAME** | The vCloud server address or name. This feature is required when **GUI_MODE=vcloud** is specified. | None |
| **VCLOUD_USERNAME** | The vCloud user ID. This feature is required when **GUI_MODE=vcloud** is specified. | None |
| **VCLOUD_PASSWORD** | The vCloud password. This feature is required when **GUI_MODE=vcloud** is specified. | None |
| **DIRECT_START** | (vSphere only) To access the Data Protection for VMware vSphere GUI in a web browser, specify **DIRECT_START=1**.<br>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=0**. | 1<br>**Important:** After installation completes, the **DIRECT_START** value cannot be changed except by reinstalling the product. |
| **REGISTER_PLUGIN** | (vSphere only) To access the Data Protection for VMware vSphere GUI as an extension in the Solutions and Applications panel of your vCenter Server System, specify **REGISTER_PLUGIN=1**.<br>This plug-in access method is the same method as provided in prior versions of Tivoli Storage Manager for Virtual Environments.If you do not want to access the Data Protection for VMware vSphere GUI as an extension, specify **REGISTER_PLUGIN=0**. | 0 |
| **REGISTER_EXTENSION** | (vSphere only) To access the Data Protection for VMware vSphere GUI as an extension in the vSphere Web Client, specify **REGISTER_EXTENSION=1**. | 0 |
| **DB_PORT** | The TCP/IP port number for the Derby database. | 1527 |
| **WC_DEFAULTHOST** | The HTTP protocol for the GUI web server. | 9080 |
| **WEBSERVER_SECUREPORT** | The HTTPS protocol for the GUI web server. | 9081 |

Table 9. Data Protection for VMware silent installation features

| Feature | Description | Installed by default? |
|---|---|---|
| mount | Tivoli Storage Manager recovery agent<br>Provides virtual mount capabilities. | Yes |
| mountdriver | Recovery agent device driver<br>Required for instant restore operations. | No |
| shell | Recovery agent command-line interface<br>Command-line interface that is used for mount operations (RecoveryAgentShell.exe). | Yes |

*Table 9. Data Protection for VMware silent installation features (continued)*

| Feature | Description | Installed by default? |
|---|---|---|
| LAP | Data Protection for VMware license | Yes |
| TSMLicence | Data Protection for VMware enablement file<br>Enables Tivoli Storage Manager to run the following backup types:<br>• Periodic incremental VM backup<br>• Full VM incremental-forever backup<br>• Incremental-forever-incremental VM backup<br>If you offload backup workloads, this file must be installed on the vStorage Backup Server. | Yes |
| documents | Readme file | Yes |
| gui | Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI | No |

Use the following data mover parameters with the silent installation features:

*Table 10. Data mover silent installation parameters*

| Parameter | Description | Default value |
|---|---|---|
| **BackupArchiveGUI** | Tivoli Storage Manager backup-archive client GUI | None |
| **BackupArchiveWeb** | Tivoli Storage Manager backup-archive web client | None |
| **Api64Runtime** | Tivoli Storage Manager API runtimes | None |
| **AdministrativeCmd** | Tivoli Storage Manager Administrative command line | None |

### About this task

**Restriction:** All features are installed to their default location. To locate the default installation directories for the components, see the subtopics in “Installable components” on page 1.

### Procedure

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

1. Open a command prompt and go to the location of the `spinstall.exe` file for the component that you want to install.
2. Specify which features to install.
   The following example installs the Tivoli Storage Manager recovery agent, device driver, and recovery agent command-line interface:

   ```
   spinstall.exe ISFeatureInstall=TSM4VE ComponentsToInstallVe=mount,mountdriver,shell
   REBOOT=ReallySuppress SUITE_MODE=1 /silent
   ```

The following example installs a subset of Data Protection for VMware and data mover features:

```
spinstall.exe ISFeatureInstall=Client,TSM4VE /silent
ComponentsToInstallBa=BackupArchiveGUI,BackupArchiveWeb,Api64Runtime
ComponentsToInstallVe=LAP,TSMLicence,documents,gui  SUITE_MODE=1 REBOOT=ReallySuppress
GUI_MODE=vcenter VCENTER_HOSTNAME=host_name
VCENTER_USERNAME=user_name VCENTER_PASSWORD=password
REGISTER_PLUGIN=1 DIRECT_START=1
```

The following example installs all Data Protection for VMware and data mover features:

```
spinstall.exe /silent SUITE_MODE=1 REBOOT=ReallySuppress
GUI_MODE=vcenter VCENTER_HOSTNAME=host_name VCENTER_USERNAME=user_name
VCENTER_PASSWORD=password REGISTER_PLUGIN=1 DIRECT_START=1
```

3. Optional: When the device driver is installed, you must restart the system.

   **Note:** The following message displays 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?
   ```

   You must register the Virtual Volume Driver to proceed with the recovery agent operations.

**Related tasks**:

"Uninstalling Data Protection for VMware for Windows 64-bit system in silent mode" on page 54

## Installing the Data Protection for VMware components in silent mode by using the stand-alone installer

Use the stand-alone installer to install the Data Protection for VMware and data mover feature (backup-archive client) components in silent mode.

### About this task

Use the stand-alone installer to install the Data Protection for VMware and data mover features separates.

Windows If you do not want to install Data Protection for VMware and the data mover feature on the same system, you can use the stand-alone installers. You can install multiple data movers on different systems and you can use the stand-alone installer for the data mover to do so.

**Restriction:** On Windows 32-bit systems, you can install only the recovery agent GUI and command-line interface.

### Installing Data Protection for VMware on Windows 32-bit systems in silent mode:

You can silently install the recovery agent GUI and the recovery agent command-line interface on a Windows 32-bit operating system.

#### Before you begin

Data Protection for VMware provides the following silent installation features for Windows 32-bit operating systems:

*Table 11. Data Protection for VMware silent installation features*

| **Feature** | **Description** | **Installed by default?** |
|---|---|---|
| Mount | Tivoli Storage Manager recovery agent<br>Provides virtual mount capabilities. | Yes |
| Mountdriver | Recovery agent device driver<br>Required for instant restore operations. | No |
| Shell | Recovery agent command-line interface<br>Command-line interface that is used for mount operations (`RecoveryAgentShell.exe`). | Yes |
| XpressUtilsShortCut | Shortcut to the Recovery Agent utility folder | Yes |
| LAP | Data Protection for VMware license | Yes |
| TSMLicence | Data Protection for VMware enablement file<br>Enables Tivoli Storage Manager to run the following backup types:<br>• Periodic incremental VM backup<br>• Full VM incremental-forever backup<br>• Incremental-forever-incremental VM backup<br>If you offload backup workloads, this file must be installed on the vStorage Backup Server. | Yes |
| Documents | Readme file, notices file | Yes |

**Restriction:** You cannot install the data mover (backup-archive client) on a Windows 32-bit system.

#### Procedure

To install Data Protection for VMware, complete the following steps from the directory where you extracted the files or from the product DVD:

1. Change directories to the `tsm4ve\X86` directory.
2. Open the `setup.iss` file in a text editor:
   - For a default installation, complete the following tasks:

    a. In the SERVER_IP= string, specify the host name or IP address of the Windows system where the recovery agent is to be installed.
    b. Save and close the setup.iss file.
    c. From a command prompt window, enter the following command:

       ```
       spinstall.exe /s /f1"path\setup.iss"
       ```

       where *path* is the absolute path to the setup.iss file.
- For a custom installation, complete these tasks:
    a. In the SERVER_IP= string, specify the host name or IP address of the Windows system where the recovery agent is to be installed.
    b. Specify the features that you want to install.
    c. Save and close the setup.iss file.
    d. From a command prompt window, enter the following command:

       ```
       spinstall.exe /s /f1"path\setup.iss"
       ```

       where *path* is the absolute path to the setup.iss file.

3. Restart the system.
4. Optional: To use the updated setup.iss file to silently install Data Protection for VMware on another system, complete the following tasks:
    a. During initial installation, enter the following command to record the setup.iss file in the location specified after the f1 parameter:

       ```
       spinstall.exe /r /f1"path\setup.iss"
       ```

       where *path* is the absolute path to the setup.iss file.
    b. After installation completes successfully, copy the updated setup.iss file to the system where you want to silently install Data Protection for VMware.
    c. On this system where the updated setup.iss file was copied, complete Step 1 and Step 2 in this procedure.
    d. From a command prompt window, enter the following command:

       ```
       spinstall.exe /s /f1"path\setup.iss"
       ```

       where *path* is the absolute path to the setup.iss file.
    e. Restart the 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:
  - "System requirements" on page 13
  - "Required installation permissions" on page 16
  - "Required communication ports" on page 17

**About this task**

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

*Table 12. Data Protection for VMware silent installation features*

| Feature | Description | Installed by default? |
|---|---|---|
| Docs | Readme file | Yes |
| RecoveryAgent | Tivoli Storage Manager recovery agent<br>Provides virtual mount capabilities. | Yes |
| MountDriver | Recovery agent device driver<br>Required for instant restore operations. | No |
| TDPVMwareEnableFile | Data Protection for VMware enablement file<br>Enables Tivoli Storage Manager to run the following backup types:<br>• Periodic incremental VM backup<br>• Full VM incremental-forever backup<br>• Incremental-forever-incremental VM backup<br>If you offload backup workloads, this file must be installed on the vStorage Backup Server. | Yes |
| TDPVMwareGUI | Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI | No |

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

*Table 13. Data Protection for VMware silent installation parameters for the* `installer.properties` *file*

| Parameter | Description | Default value |
|---|---|---|
| **PRODUCT_PROTECT _TYPE** | To protect data in a vSphere environment, specify **PRODUCT_PROTECT_TYPE=VSPHERE**. This parameter installs the Data Protection for VMware vSphere GUI. This GUI integrates the product with the VMware vSphere client to back up, restore, and manage VMs in a VMware vCenter environment. Includes the Data Protection for VMware command-line interface. You can install only one Data Protection for VMware vSphere GUI on a machine. As a result, multiple Data Protection for VMware vSphere GUIs are not allowed on the same machine.<br>To protect data in a vCloud environment, specify **PRODUCT_PROTECT_TYPE=VCLOUD**. This parameter installs the Data Protection for VMware vCloud GUI. This GUI integrates the product with the vCloud Director environment to back up, restore, and manage vApps and organization vDCs. Includes the Data Protection for VMware command-line interface. | VSPHERE |
| **VCENTER_HOSTNAME** | The vCenter Server fully qualified domain name or IP address. This parameter is required when **PRODUCT_PROTECT_TYPE=VSPHERE** is specified. | None |
| **VCENTER_USERNAME** | The vCenter user ID. This user ID must be a VMware administrator that has permission to register and unregister extensions. This parameter is required when **PRODUCT_PROTECT_TYPE=VSPHERE** is specified. | None |
| **VCENTER_PASSWORD** | The vCenter password. This parameter is required when **PRODUCT_PROTECT_TYPE=VSPHERE** is specified. | None |
| **VCLOUD_HOSTNAME** | The vCloud Server address or name. This parameter is required when **PRODUCT_PROTECT_TYPE=VCLOUD** is specified. | None |
| **VCLOUD_USERNAME** | The vCloud user ID. This parameter is required when **PRODUCT_PROTECT_TYPE=VCLOUD** is specified. | None |
| **VCLOUD_PASSWORD** | The vCloud password. This parameter is required when **PRODUCT_PROTECT_TYPE=VCLOUD** is specified. | None |

Table 13. Data Protection for VMware silent installation parameters for the `installer.properties` file (continued)

| Parameter | Description | Default value |
|---|---|---|
| **DIRECT_START** | (vSphere only) 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<br>**Important:** After installation completes, the **DIRECT_START** value cannot be changed except by reinstalling the product. |
| **USERNAME** | User name. A profile for this user name is created in /home/<username>/tdpvmware/config. | tdpvmware |
| **REGISTER_PLUGIN** | (vSphere only) To access the Data Protection for VMware vSphere GUI as an extension in the Solutions and Applications panel of your vCenter Server System, specify **REGISTER_PLUGIN=YES**.<br>This plug-in access method is the same method as provided in prior versions of Tivoli Storage Manager for Virtual Environments.If you do not want to access the Data Protection for VMware vSphere GUI as an extension, specify **REGISTER_PLUGIN=No**. | NO |
| **REGISTER_EXTENSION** | (vSphere only) To access the Data Protection for VMware vSphere GUI as an extension in the vSphere Web Client, specify **REGISTER_EXTENSION=1**. | 0 |
| **VMCLI_DB_PORT** | The TCP/IP port number for the Derby Database. | 1527 |
| **WC_defaulthost** | The HTTP protocol for the GUI web server. | 9080 |
| **WebServer_Https** | The HTTPS protocol for the GUI web server. | 9081 |
| **Keystore_Password** | The keystore password for the GUI web server. The password must be a minimum of six valid characters (a-z A-Z 0-9). | None |
| **SSL_Certificate** | The installation process generates a self-signed SSL certificate. Enter the number of years to keep this SSL certificate active. | 10 |

## Procedure

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

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

   ```
   #LICENSE_ACCEPTED=TRUE
   ```

   As a result, the entry must be exactly as shown in the following example:

```
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,RecoveryAgent,TDPVMwareEnableFile,TDPVMwareGUI
           ```
        3) Specify the `installer.properties` parameters as described in Table 13 on page 38.

     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 14. Data Protection for VMware configuration worksheet*

| Item | Your value | Notes |
|---|---|---|
| **Tivoli Storage Manager server information** | | |
| Tivoli Storage Manager server address | | |
| Tivoli Storage Manager server port | | |
| Tivoli Storage Manager server admin ID/password | | |
| Tivoli Storage Manager 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 | | |

*Table 14. Data Protection for VMware configuration worksheet (continued)*

| Item | Your value | Notes |
|---|---|---|
| Datacenter node names/passwords<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>For example: *nodePrefix_datacenterName* |
| Data mover node names/passwords on the vStorage backup server<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>For example: *datacenterNodename*_DM |
| Data mover node names/passwords on remote servers<br>**Remember:** You can create multiple data mover nodes that are not on the vStorage backup server. | | |
| Mount proxy node<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 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.

### Accessing the Data Protection for VMware vCloud GUI

Use the Data Protection for VMware vCloud GUI to back up, restore, and manage vApps and organization virtual data centers.

#### 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

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

   `https://hostname:port/TsmVMwareUI`

   - *hostname* is the name of the system where the Data Protection for VMware vCloud GUI is installed
   - *port* is the port number where the vCloud GUI is accessible through. The default port number is 9081.
2. Log in by using your vCloud Directory user ID and password.

# Upgrading Data Protection for VMware

You can upgrade Data Protection for VMware from a previous version of the software. Upgrading Data Protection for VMware also requires upgrading other components.

If you are installing Data Protection for VMware Version 7.1.6 on a system that contains IBM Tivoli Storage FlashCopy Manager for VMware Version 3.x, you must also upgrade Tivoli Storage FlashCopy Manager for VMware to Version 4.1.6. Data Protection for VMware Version 7.1.6 is not compatible with Tivoli Storage FlashCopy Manager for VMware Version 3.x.

See the Tivoli Storage FlashCopy Manager for VMware Installation and User's Guide when working with that product.

For compatibility with earlier versions, see technote 1648031.

## Upgrading Data Protection for VMware

This procedure documents how to upgrade to Data Protection for VMware V7.1.6.

#### Before you begin

**Important:** This upgrade procedure applies to a system that does not have Tivoli Storage FlashCopy Manager 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 Tivoli Storage Manager for Virtual Environments was installed to a non-default location, the upgrade process installs Tivoli Storage Manager for Virtual Environments V7.1.6 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.
- Linux Windows The upgrade process does not install new components.

  For example, if your previous version has only the Tivoli Storage Manager recovery agent GUI installed, the upgrade procedure does not install the Tivoli Storage Manager recovery agent command-line interface. In such a scenario, you must run the installation program again and then select the missing component to install.
- Linux The Tivoli Storage Manager recovery agent on Linux version must be the same version as the Tivoli Storage Manager recovery agent on the Windows proxy. Therefore, if you upgrade Tivoli Storage Manager recovery agent on Linux, you must also upgrade the Tivoli Storage Manager 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 Tivoli Storage Manager recovery agent GUI or command-line interface (**`mount del`** command) to unmount volumes.
3. If the system you are upgrading to has both the Data Protection for VMware vSphere GUI and Tivoli Storage Manager backup-archive client installed, install the backup-archive client V7.1.6. Follow the instructions in "Installing the Data Protection for VMware components on Windows systems" on page 25 or "Installing Data Protection for VMware on Linux systems" on page 26.

   **Note:** Linux If the backup-archive client V6.x is installed, you must uninstall it before you install V7.1.6. Follow the instructions in Uninstalling the Tivoli Storage Manager Linux x86_64 client
4. Either download the code package or insert the Data Protection for VMware product DVD into the DVD drive.
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.

   A message displays this text: `The Existing Data Protection for VMware is going to be upgraded.`

   If you confirm the upgrade, the installer updates the files. You can install only one Data Protection for VMware vSphere GUI on a machine. As a result, multiple Data Protection for VMware vSphere GUIs are not allowed on the same machine.

## Upgrading Data Protection for VMware from Tivoli Storage FlashCopy Manager for VMware

This procedure documents how to upgrade to Data Protection for VMware V7.1.6 when Tivoli Storage FlashCopy Manager for VMware is also installed.

### Before you begin

**Important:** This upgrade procedure applies to a Linux system that does not have Data Protection for VMware installed.

### About this task

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.
- The values in the profile (`vmcliprofile`) are used for the Data Protection for VMware command-line interface.

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

### Procedure

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

1. Either download the code package or insert the Data Protection for VMware product DVD into the DVD drive.
2. Start the installation program by running install-Linux.bin for your platform. The default installation path is `/opt/tivoli/tsm/tdpvmware`.
3. Choose the language to be used for the installation process and click **OK**.
4. The Welcome page opens. Click **Next**.
5. The Software License Agreement page opens. Read the terms of the license agreement. Select **I accept the terms in the license agreement** and click **Next**. If you do not accept the terms of the license agreement, the installation ends.
6. The Choose Installation Folder page opens prompting you to specify where to install the software. You can accept the default location shown in the **Destination Folder** field, type the location name, or click **Browse** to go to the location. Click **Next**.
7. Select **Complete** or **Custom**:
   - Select **Complete** to install all of the components.
   - Select **Custom** to specify only those components you want to install. At the prompt, enter the number that corresponds to the component. If multiple components, separate each number with a comma.

   After completing your selection, click **Next** to continue.
8. The Pre-Installation Summary panel opens. This panel contains a list of the settings you provided. Review the settings and click **Install** to begin installing the files.
   - When the Data Protection for VMware V7.1.6 installation is successful, the following message is displayed:

```
The installation process completed successfully. If you are upgrading, you must
upgrade all components from the Data Protection for VMware, FlashCopy Manager for
VMware, and Tivoli Storage Manager Backup-Archive Client (data mover) packages
because of component dependencies.
```

- When Data Protection for VMware V7.1.6 does not install successfully, follow the instructions provided in the installation dialog. You can also check the log file to determine what must be done to resolve the issue. See "Log file activity" on page 87 for the location of various log files.

## Upgrading Data Protection for VMware from Tivoli Storage FlashCopy Manager for VMware and Data Protection for VMware

This procedure documents how to upgrade to Data Protection for VMware V7.1.6 from Data Protection for VMware V6.x when Tivoli Storage FlashCopy Manager for VMware V3.x is also installed.

### Before you begin

**Important:** This upgrade procedure applies to a Linux system that has both Data Protection for VMware V6.x and Tivoli Storage FlashCopy Manager for VMware V3.x 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.
- The values in the profile (`vmcliprofile`) are used for the Data Protection for VMware command-line interface.

**Restriction:**

- 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.
- 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. If the system you are upgrading to has both the Data Protection for VMware vSphere GUI V6.x and backup-archive client V6.x installed, complete the following tasks:
   a. Uninstall the backup-archive client V6.x. Follow the instructions in Uninstalling the Tivoli Storage Manager Linux x86_64 client.

   b. Install the backup-archive client V7.1.6. Follow the instructions in "Installing Data Protection for VMware on Linux systems" on page 26.

2. Either download the code package or insert the Data Protection for VMware product DVD into the DVD drive.
3. Start the installation program by running install-Linux.bin for your platform. The default installation path is `/opt/tivoli/tsm/tdpvmware`.
4. Choose the language to be used for the installation process and click **OK**.
5. The Welcome page opens. Click **Next**.
6. The Software License Agreement page opens. Read the terms of the license agreement. Select **I accept the terms in the license agreement** and click **Next**. If you do not accept the terms of the license agreement, the installation ends.
7. The Choose Installation Folder page opens prompting you to specify where to install the software. You can accept the default location shown in the **Destination Folder** field, type the location name, or click **Browse** to go to the location. Click **Next**.
8. Select **Complete** or **Custom**:
   - Select **Complete** to install all of the components.
   - Select **Custom** to specify only those components you want to install. At the prompt, enter the number that corresponds to the component. If multiple components, separate each number with a comma.

   After completing your selection, click **Next** to continue.
9. The Pre-Installation Summary panel opens. This panel contains a list of the settings you provided. Review the settings and click **Install** to begin installing the files.
   - When the Data Protection for VMware V7.1.6 installation is successful, the following message is displayed:

     ```
     The installation process completed successfully. If you are upgrading, you must
     upgrade all components from the Data Protection for VMware, FlashCopy Manager for
     VMware, and Tivoli Storage Manager Backup-Archive Client (data mover) packages
     because of component dependencies.
     ```

     – If you are using Tivoli Storage FlashCopy Manager for VMware V3.x, you must upgrade to V4.1.6 as described in Upgrading Tivoli Storage FlashCopy Manager for VMware.

     – If you are using Tivoli Storage Manager backup-archive client V6.x or earlier, you must upgrade to V7.1.6 as described in Upgrading the Tivoli Storage Manager backup-archive client.

     – Data Protection for VMware offloads the backup workload from VMs to a vStorage Backup Server. To accomplish this task, the backup-archive client must be installed on the vStorage Backup Server. During configuration, the backup-archive client is registered as a data mover node. This node runs the operation and "moves" the data from the vStorage Backup Server to the Tivoli Storage Manager server. You must upgrade all data mover nodes to the backup-archive clientV7.1.6 level as described in "Upgrading the data mover nodes on the vStorage Backup Server" on page 49.
   - When Data Protection for VMware V7.1.6 does not install successfully, follow the instructions provided in the installation dialog. You can also check the log file to determine what must be done to resolve the issue. See "Log file activity" on page 87 for the location of various log files.

## Upgrading Data Protection for VMware on a Windows 32-bit system in silent mode

You can silently upgrade Data Protection for VMware on a supported 32-bit operating system

### 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 Tivoli Storage Manager recovery agent GUI or command-line interface (**mount del** command) to unmount volumes.
3. Unmount any mounted virtual volumes. You can use the Tivoli Storage Manager recovery agent GUI or command-line interface (**mount del** command) to unmount volumes.
4. Either download the code package or insert the Data Protection for VMware DVD into the DVD drive.
5. In the Data Protection for VMware folder, go to the X86 folder.
6. In a text editor, open the upgrade.iss file.
7. Edit the upgrade.iss file:
   a. Locate the line that starts with the following string: szDir=
   b. **Optional:** If you are not using the default installation path, edit this line to refer to the installation path that you are using.
   c. Save and close the upgrade.iss file.
8. From a command prompt window, enter the following command:
   ```
   spinstall.exe /s /f1"<path_to_the_upgrade.iss_file>"
   ```
9. Restart the system.

## 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 V7.1.6 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 Tivoli Storage Manager recovery agent GUI or command-line interface (**mount del** command) to unmount volumes.

3. Unmount any mounted virtual volumes. You can use the Tivoli Storage Manager recovery agent GUI or command-line interface (**mount del** command) to unmount volumes.
4. Either download the code package or insert the Data Protection for VMware product DVD into the DVD drive.
5. In the folder for Data Protection for VMware, either go to the X64 folder.
6. From a command prompt window, enter the following command:

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

## 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 15. Data Protection for VMware silent installation upgrade parameters*

| Parameter | Description | Default value |
|---|---|---|
| **DVCENTER_HOSTNAME** | The vCenter Server fully qualified domain name or IP address. | None |
| **DVCENTER_USERNAME** | The vCenter user ID. This user ID must be a VMware administrator that has permission to register and unregister extensions. | None |
| **DVCENTER_PASSWORD** | The vCenter password. | None |
| **DDIRECT_START** | To access the Data Protection for VMware vSphere GUI in a web browser, specify **DDIRECT_START=YES**.<br>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 **DDIRECT_START=NO**. | YES<br>**Important:** After upgrade completes, the **DDIRECT_START** value cannot be changed except by reinstalling the product. |
| **DREGISTER_PLUGIN** | To access the Data Protection for VMware vSphere GUI as an extension in the Solutions and Applications panel of your vCenter Server System, specify **DREGISTER_PLUGIN=YES**.<br>This plug-in access method is the same method as provided in prior versions of Tivoli Storage Manager for Virtual Environments.If you do not want to access the Data Protection for VMware vSphere GUI as an extension, specify **DREGISTER_PLUGIN=No**. | NO |
| **DREGISTER_EXTENSION** | To access the Data Protection for VMware vSphere GUI as an extension in the vSphere Web Client, specify **DREGISTER_EXTENSION=1**. | 0 |

### 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 Tivoli Storage Manager recovery agent GUI is closed.
3. Either download the code package, or insert the Data Protection for VMware product DVD into the DVD drive.
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=hostname -DVCENTER_USERNAME=username
   -DVCENTER_PASSWORD=password -DREGISTER_PLUGIN=yes
   -DDIRECT_START=yes -DREGISTER_EXTENSION=yes
   ```

## Upgrading the data mover nodes on the vStorage Backup Server

If you offloaded backup workloads to a vStorage Backup Server using Data Protection for VMware, you must upgrade all data mover nodes to the 7.1.6 level.

### Before you begin

Data Protection for VMware works with Tivoli Storage Manager backup-archive client (installed on the vStorage Backup server) to complete full, incremental, and incremental forever snapshots of VMs. The client node on the vStorage Backup server is called the data mover node. This node "moves" the data to the Tivoli Storage Manager server for storage, and VM image-level restore at a later time.

**Important:** Data Protection for VMware stores sensitive information locally on the data mover, and the data mover might also have direct access to VM storage. Access to the data mover must be protected. Allow only trusted users access to the data mover system.

Tivoli Storage Manager backup-archive client is a separately licensed product that contains its own user interfaces and documentation. You must be familiar with the product to create a comprehensive plan to protect your VMs with Data Protection for VMware. Follow the instructions in Upgrading the Tivoli Storage Manager backup-archive client.

### Procedure

1. Upgrade each vStorage Backup Server in your Data Protection for VMware environment with Tivoli Storage Manager backup-archive client V7.1.6.
2. When upgrading the Tivoli Storage Manager backup-archive client, upgrade the VMware vStorage API runtime files:
   a. During the upgrade process, select setup type **Custom**.
   b. Select **VMware vStorage API runtime files**.
3. Upgrade each vStorage Backup Server in your Data Protection for VMware environment with Data Protection for VMware V7.1.6:
   a. Detailed instructions are provided in “Upgrading Data Protection for VMware” on page 42.

b. When upgrading the vStorage Backup Server, the only Data Protection for VMware component required for the data mover node is the Data Protection for VMware Enablement File. This file enables the data mover node to perform the backup VM incremental function.

# 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 Data Protection extension, do not unregister the web client extension.
- When the Data Protection for VMware vSphere GUI plug-in is uninstalled, the IBM Data Protection extension is also uninstalled. The IBM Data Protection extension cannot be uninstalled by itself.
- When you uninstall the IBM Data Protection extension 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.
- The Data Protection for VMware Enablement File is not removed after the product is uninstalled.

### About this task

Configuration and property files are located in the `C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\config` directory after the uninstall completes.

### Procedure

1. Stop any Data Protection for VMware components that are running.
2. Unmount any mounted virtual volumes. You can use the Tivoli Storage Manager recovery agent GUI or command-line interface (**`mount del`** command) to unmount volumes.
3. Click **Start** > **Control Panel** > **Programs and Features** > **Uninstall a program**.
   - If you installed Data Protection for VMware with the Suite Installer, select `Data Protection for VMware suite` and click **Uninstall**.
   - If you installed Data Protection for VMware with the stand-alone installer, select `IBM Tivoli Storage Manager for Virtual Environments` and click **Uninstall**.

   This action uninstalls the Windows Data Protection for VMware program. It also removes services that are associated with the Recovery Agent, web server, and Data Protection for VMware command-line interface. However, this action does not remove log files, backup-archive client (data mover and mount proxy) services, or other items that were created when you configured or used Data Protection for VMware. Leaving these artifacts on disk is not a problem if you want to reinstall Data Protection for VMware in the future. However, if you want to more thoroughly remove Data Protection for VMware and related files and settings, go to Step 4.

4. Remove the following Data Protection for VMware files and directories from the file system. Open an Administrator command prompt and complete the following steps:
   a. Go to the `C:\Program Files\Tivoli\TSM\` directory. For example:
      ```
      cd /d "C:\Program Files\Tivoli\TSM\"
      ```
      Issue the following commands:
      ```
      rd /s RecoveryAgent
      ```
      ```
      rd /s TDPVMware
      ```
   b. Go to the `C:\Program Files (x86)\Common Files\Tivoli\` directory. For example:
      ```
      cd /d "C:\Program Files (x86)\Common Files\Tivoli\"
      ```
      **Note:** The following command deletes all configuration and property files that were saved after uninstallation.
      Issue the following command:
      ```
      rd /s TDPVMware
      ```
   c. Go to the `C:\ProgramData` directory. For example:
      ```
      cd /d "C:\ProgramData"
      ```
      Issue the following commands:
      ```
      del installed.txt
      ```
      ```
      del TDPVMwareInstallation.log
      ```
   d. Go to the `C:\ProgramData\Tivoli\TSM` directory. For example:
      ```
      cd /d "C:\ProgramData\Tivoli\TSM"
      ```
      Remove the following files if they are on your system:
      ```
      del vmFileLevelRestoreDataSet.xml
      del vmFileLevelRestoreDataSet.xml.bak
      del vmFileLevelRestoreDataSet.xml.lock
      ```
      Issue the following command:
      ```
      rd /s RecoveryAgent
      ```

## What to do next

Uninstall the data mover on Windows.

**Related tasks**:

"Uninstalling the data mover on Windows" on page 52

# Uninstalling the data mover on Windows

Uninstall backup-archive client components (data mover) and remove files and directories from a Windows system.

## Before you begin

Uninstall Data Protection for VMware before you proceed with this task.

## Procedure

1. Stop any backup-archive client components that are running.
2. Delete any existing virtual machine backups by issuing the backup-archive client **`delete backup`** command. For example, to delete the active backup of a virtual machine that is named vm1, issue the following command:

   ```
   delete backup -objtype=vm vm1
   ```

   To delete one or more backup versions of a virtual machine that is named vm_test., issue the following command:

   ```
   delete backup -objtype=vm -inactive vm_test
   ```

3. Enter the following commands. You can use the **`dsmcutil list`** command to display any backup-archive client services that are installed.
   a. `cd /d "c:\program files\tivoli\tsm\baclient"`

      If necessary, replace `c:\program files\tivoli` with the correct installation folder.

   b. `dsmcutil remove /name:"TSM Remote Client Agent"`

      **Important:** Ensure that you remove the `TSM Remote Client Agent` in Step 3b before you remove the `TSM Client Acceptor` in Step 3c. Otherwise, the `TSM Client Acceptor` (Step 3c) cannot be removed.

   c. `dsmcutil remove /name:"TSM Client Acceptor"`
4. Click **Start** > **Control Panel** > **Programs and Features** > **Uninstall a program**. Uninstall the following Tivoli Storage Manager backup-archive client items if they are listed:

   ```
   IBM® Tivoli Storage Manager client
   IBM Tivoli Storage Manager Client - Chinese(PRC)
   IBM Tivoli Storage Manager Client - Chinese(Taiwan)
   IBM Tivoli Storage Manager Client - French
   IBM Tivoli Storage Manager Client - German
   IBM Tivoli Storage Manager Client - Italian
   IBM Tivoli Storage Manager Client - Japanese
   IBM Tivoli Storage Manager Client - Korean
   IBM Tivoli Storage Manager Client - Portuguese(Brazil)
   IBM Tivoli Storage Manager Client - Spanish
   ```

   This action uninstalls the Windows client program. It does not remove any services, log files, or other items that were created when you configured or used the client. Leaving these artifacts on disk is not a problem if you want to reinstall the client in the future. However, if you want to more thoroughly remove the client and related files and settings, see the following IBM developerWorks article: How to completely remove the Backup-Archive client from Microsoft Windows.

**Related tasks**:

"Uninstalling Data Protection for VMware on Windows" on page 50

## Uninstalling Data Protection for VMware with the Windows Installer

Uninstall Data Protection for VMware from a Microsoft Windows Server Core with the Microsoft Windows Installer Tool.

### About this task

Configuration and property files are located in the `C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\config` directory after the uninstall completes.

### Procedure

1. Stop any Data Protection for VMware components that are running.
2. Unmount any mounted virtual volumes. You can use the Tivoli Storage Manager recovery agent GUI or command-line interface (**`mount del`** command) to unmount volumes.
3. Initiate the Windows Installer (MSI) with either of the following methods:
   - To initiate the MSI with the Suite installer in GUI mode, complete the following steps:
     a. Locate the Data Protection for VMware **`UninstallString`** in the `Wow6432Node` registry path. For example:

        ```
        [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\
        Uninstall\{4D11E402-4480-4A4D-B6E5-B98A7E5FA97F}]
        ```

     b. Run the following command:

        ```
        C:\"C:\Program Files (x86)\InstallShield Installation Information\
        {4D11E402-4480-4A4D-B6E5-B98A7E5FA97F}\spinstall.exe" -remove -runfromtemp
        ```

   - To initiate the MSI directly, complete the following steps:

     Uninstall Tivoli Storage Manager for Virtual Environments:

     a. Obtain the product code from the `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall` registry key.
        1) Issue **CTRL + F** to search for the `Tivoli Storage Manager for Virtual Environments` text string.
        2) The product code is viewable when the text string is located.

     b. Issue **`msiexec.exe /uninstall`** *{PRODUCTCODE}*. For example:

        ```
        C:\Program Files (x86)>Msiexec.exe /uninstall {9ED81E7A-E410-4A39-990D-3256DDDCFCD5}
        ```

## Uninstalling Data Protection for VMware for a Windows 32-bit system in silent mode

You can silently uninstall Data Protection for VMware on a Windows 32-bit operating system.

### About this task

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

### Procedure

1. Stop any Data Protection for VMware components that are running.
2. Unmount any mounted virtual volumes. You can use the Tivoli Storage Manager recovery agent GUI or command-line interface (**`mount del`** command) to unmount volumes.

3. From a command prompt window, use the **cd** command to change to one of the following folders:
   - To uninstall Data Protection for VMware with an `uninstall.iss` file, go to the `X64` folder.
   - To uninstall Data Protection for VMware with Suite installer, go to one of the following folders:
     - If you downloaded the product image from Passport Advantage, go to `<extract folder>TSM4VE_WIN`.
     - If you inserted the product DVD into the DVD drive, go to `<DVD>\`.
4. Enter one of the following commands:
   - To uninstall Data Protection for VMware with an `uninstall.iss` file, enter the following command:

     ```
     spinstall.exe /s /f1"
     <full absolute path_to_the_uninstall.iss_file and uninstall.iss>"
     ```

     **Note:** The command must be entered on one line. This example shows two lines to accommodate page formatting.
   - To uninstall Data Protection for VMware with Suite installer, enter the following command:

     ```
     spinstall.exe /silent /remove
     ```
5. Restart the system after uninstallation completes.

## Uninstalling Data Protection for VMware for Windows 64-bit system in silent mode

You can silently uninstall Data Protection for VMware on a Windows 64-bit operating system.

### About this task

Configuration and property files are located in the `C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\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 Tivoli Storage Manager recovery agent GUI or command-line interface (**mount del** command) to unmount volumes.
3. From a command prompt window, use the **cd** command to change to one of the following folders:
   - To customize the uninstall operation, go to the `X64` folder.
   - To uninstall Data Protection for VMware with Suite installer, go to one of the following folders:
     - If you downloaded the product image from Passport Advantage, go to `<extract folder>TSM4VE_WIN`.
     - If you inserted the product DVD into the DVD drive, go to `<DVD>\`.
4. In the command prompt window, run the following command:
   - For a custom uninstall operation, select from the following commands:

- Enter this command to uninstall Data Protection for VMware and unregister the Data Protection for VMware vSphere GUI:

  ```
  spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
  VCENTER_HOSTNAME=<vCenter hostname or IP>
  VCENTER_USERNAME=<vCenter user name>
  VCENTER_PASSWORD=<vCenter password>"
  ```

- To uninstall Data Protection for VMware and skip Data Protection for VMware vSphere GUI unregistration, enter this command:

  ```
  spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
  IGNORE_VCENTER_UNREGISTER=1"
  ```

- Enter this command to uninstall Data Protection for VMware and unregister the Data Protection for VMware vCloud GUI:

  ```
  spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
  VCLOUD_HOSTNAME=<vCloud Server IP address or name>"
  ```

- To uninstall Data Protection for VMware and skip Data Protection for VMware vCloud GUI unregistration, enter this command:

  ```
  spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
  IGNORE_VCLOUD_UNREGISTER=1"
  ```

- To uninstall all features with Suite installer, enter the following command:

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

5. Restart the system after uninstallation completes.

## Uninstalling Data Protection for VMware a Linux system

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

### 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 56.

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 or vCloud connection information. This information is needed to uninstall the Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud 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 or Data Protection for VMware vCloud GUI, remove its package from the Package Manager database with this command:

   ```
   rpm -e TIVsm-TDPVMwarePlugin
   ```
2. Remove the Tivoli Storage Manager API with this command:

   ```
   rpm -e TIVsm-API64
   ```
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
      TDPVMwareMount
      JavaHelp
      TDPVMwareEnableFile
      ```
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. Attempt to install the product again as described in "Installing Data Protection for VMware on Linux systems" on page 26.

# Chapter 2. Configuring Data Protection for VMware

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

## Configuring a new installation with the wizard

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

### Before you begin

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

- vStorage Backup Server
- Tivoli Storage Manager 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/`
   - In a vSphere environment, log in with the vCenter user name and password.
   - In a vCloud environment, log in with the vCloud user name and password. This user name must be the name of a vCloud system administrator.
2. In the Getting Started window, go to the Configuration window and click **Run Configuration Wizard**.
3. 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.
4. 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.

## 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 Tivoli Storage Manager 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/
   ```
   - In a vSphere environment, log in with the vCenter user name and password.
   - In a vCloud environment, log in with the vCloud user name and password. This user name must be the name of a vCloud system administrator.
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.

## Enabling the environment for file restore operations

Windows

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 File restore prerequisites.

### 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 TSM 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 the Windows domain administrator credentials. Otherwise, clear the check box and do not enter any credentials.

           **Tip:** A file restore operation uses the domain administrator 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 the Windows domain administrator credentials. Otherwise, clear the check box and do not enter any credentials.

      **Tip:** A file restore operation uses the domain administrator 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 Tivoli Storage Manager file restore interface.

## Setting up file restore operations on Linux

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 or in combination with Tivoli Storage FlashCopy Manager for VMware, 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 Tivoli Storage Manager 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.

## Modifying options for file restore operations

Windows

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\tivoli\tsm\tdpvmware\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 62 to determine which options to modify.
3. Save your changes and close the `frConfig.props` file.

### Results

Modified options are applied to the Tivoli Storage Manager 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 Tivoli Storage Manager file restore interface.

**`false`**

File owners cannot restore their files with the Tivoli Storage Manager file restore interface. This value is the default.

**`true`**

File owners can restore their files with the Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Install_Directory\IBM\tivoli\tsm\tdpvmware\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" 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 `Install_Directory/IBM/tivoli/tsm/tdpvmware/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 backup management tags to virtual machines 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.
- A data mover and the Data Protection for VMware vSphere GUI must be installed on the same server. The data mover node must be configured so that the vCenter server credentials are saved by running the configuration wizard to save the data mover node password. Other data movers can be installed elsewhere.
- Linux On Linux operating systems, the Data Protection for VMware vSphere GUI must be installed by using the default user name (`tdpvmware`).
- Linux

  For Linux data mover nodes, the default password file (`/etc/adsm/TSM.PWD`) must be used.

### About this task

You can use backup management tags to change backup policy, such as excluding virtual machines from scheduled backups or changing the retention policy of virtual machine backups. These backup management tags are presented as settings that can be changed in the IBM Data Protection extension.

### Procedure

Use one of the following methods:

- To configure a new data mover for tagging support on Windows by using the Data Protection for VMware vSphere GUI, complete the following steps:
  1. On the Windows 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:

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

     Log on with the vCenter user ID and password.
  2. Go to the **Configuration** tab, and select the **Edit TSM Configuration** action.
  3. Go to the Data Mover Nodes page of the configuration notebook.
  4. Complete the steps to add a data mover node.
     a. For the data mover node that you want to set up tagging support for, select **Create Services**, then select **Tag Based Node**.
     b. Click **OK** to save your changes.
- To configure a new or existing Linux or existing Windows data mover node for tagging support, add the `vmtagdatamover yes` option in the client options file (`dsm.sys` for Linux and `dsm.opt` for Windows).

### Results

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

**Related information**:

`Vmtagdatamover`

## 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 Tivoli Storage Manager 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 VMware ESXi and vCenter Server 5 Documentation.

- 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
   Tivoli Storage Manager 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 V7.1.6 and Tivoli Storage Manager backup-archive client V7.1.6 are 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 V7.1.6 and the Tivoli Storage Manager backup-archive client V7.1.6 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 backup-archive client.
   Follow the instructions in Configuring the backup-archive client.
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:

      ```
      VMISCSIServeraddress=<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** > **Tivoli Storage Manager** > **Tivoli Storage Manager for Virtual Environments** > **Tivoli Storage Manager 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 16. iSCSI network settings*

| Virtual Machine Network | iSCSI Network |
|---|---|
| **Standard Switch**: *vSwitch0* | **Standard Switch**: *vSwitch1* |

*Table 16. iSCSI network settings (continued)*

| Virtual Machine Network | iSCSI Network |
|---|---|
| **Virtual Machine Port Group**: *VM Network* | **VMkernel Port**: *VMkernel iSCSI*<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.

## Setting up communication with Transport Layer Security

The Data Protection for VMware vSphere GUI uses the Transport Layer Security (TLS) protocol to communicate with its web GUI client and the Tivoli Storage Manager server.

### About this task

The Data Protection for VMware vSphere GUI always uses the HTTPS protocol to communicate with web browsers. In other words, TLS is always enabled. During the installation of Data Protection for VMware, a self-signed digital certificate is generated and is then used for web browser sessions.

If you want to use a certificate that is signed by a third party (known as a certificate authority), follow the steps described in “Using a third-party certificate.”

TLS communication with the Tivoli Storage Manager server is optional and is not enabled by default. To enable it, follow the steps described in “Enabling secure communication with the Tivoli Storage Manager server” on page 74.

## Using a third-party certificate

To use a certificate that is signed by a third party (also known as a certificate authority), 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:\IBM\tivoli\tsm\tdpvmware\webserver\jre\jre\bin` 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 certifiate 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\tivoli\tsm\tdpvmware\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\tivoli\tsm\tdpvmware\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\tivoli\tsm\tdpvmware\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 90

## 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\tivoli\tsm\tdpvmware\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 70.

**-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\tivoli\tsm\tdpvmware\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 generated the certificate signing request (CSR).

   **-file** *signedcert.pem*
   The signed certificate file received from the CA.

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

8. Delete the existing certificate that contains the `vekey` alias:

   ```
   keytool -delete -alias vekey -keystore key.jks -storepass password
   ```

   Where `-storepass` *password* is the password for the keystore.

9. Rename the signed certificate to `vekey`:

   ```
   keytool -changealias -alias mykey -destalias vekey -keystore
   key.jks -storepass password
   ```

   Where:

   **-alias** *mykey*
   The alias of the signed certificate.

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

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

**Related reference**:
"Starting and running services for Data Protection for VMware" on page 90

## Enabling secure communication with the Tivoli Storage Manager server

If the Tivoli Storage Manager server is configured to use the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol, you can enable the Data Protection for VMware vSphere GUI to communicate with the server over the SSL or TLS protocol.

### Before you begin

If the server is using a self-signed certificate, you must obtain a copy of that certificate from the server administrator.

If the server is using a third-party certificate, you must obtain the certificate authority (CA) root certificate.

### About this task

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:\IBM\tivoli\tsm\tdpvmware\webserver\jre\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 64-bit: `C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\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 **Run Configuration Wizard** and go to the Server Credentials page.
   - If you are modifying an existing configuration, click **Edit Configuration** and go to the Server Credentials page.

4. Enter the port number in the **Tivoli Storage Manager Admin Port** field.

   The port number to use is typically the value specified by the `SSLTCPPort` option in the server options file (`dsmserv.opt`). However, if the `ADMINONCLIENT NO` statement is specified in the `dsmserv.opt` file, then the correct port number to use for the SSL protocol is the value specified by the `SSLTCPADMINPort` option.
5. Select **Use SSL communications on the Admin Port**.
6. If you want to use this setting for future GUI sessions, select **Save the Admin ID, password, and port setting**.
7. Click **OK** to apply the changes.

## 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 install the vSphere Client plug-in or IBM Data Protection extension view for the Data Protection for VMware vSphere GUI

To install the vSphere Client plug-in or IBM Data Protection extension view for the Data Protection for VMware vSphere GUI, the vSphere user requires the **Extension** > **Register extension, Unregister extension, Update extension** privileges. From the VMware vSphere client, you can create a role and add to the role the extension set of associated privileges. You must then assign this role to the vCenter object in the VMware vCenter Server hierarchy for the user ID that you plan to use during the installation process. You must enter this user ID when prompted for the vCenter user name on the following pages of the Tivoli Storage Manager for Virtual Environments installation wizard:

- vSphere Client plug-in: Plug-in Registration vCenter page
- IBM Data Protection extension: Data Protection for VMware vSphere GUI information page

**Tip:** Alternatively, rather than creating a specific role for the installation, you can enter the administrator user name when prompted for the vCenter user name.

### vCenter Server privileges required to protect VMware datacenters with the web-browser or vSphere Client plug-in view for the Data Protection for VMware vSphere GUI

The vCenter Server user ID that signs on to the browser or plug-in views 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. You must assign this role to a user ID for a specified vCenter Server or datacenter. 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 and plug-in view GUIs 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 Tivoli Storage Manager backup-archive client 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 technote 7047438.

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 theIBM Data Protection extension view for the Data Protection for VMware vSphere GUI

The IBM Data Protection extension 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 Data Protection extension:

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

Custom privileges that are required for the IBM Data Protection extension 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 Data Protection extension content. Only users with these custom privileges on the required VMware object can access the IBM Data Protection extension content. One IBM Data Protection extension 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 Data Protection extension. 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 Data Protection extension 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 Data Protection extension in the vSphere web client to manage virtual machines in their respective datacenters only.

## Issues related to insufficient permissions

When the web browser or vSphere Client plug-in view 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 Data Protection extension 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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
```

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 Tivoli Storage Manager administrator ID.

When a node is registered on the Tivoli Storage Manager server, the server automatically creates an administrator ID with client owner authority for the node. The server also assigns a privilege class to that administrator ID. This privilege class is a level of authority that determines which tasks the administrator ID can run. As a result, the tasks you run with the Data Protection for VMware vSphere GUI are based on the privilege class that is assigned to the administrator ID that you specify.

When the administrator ID does not have unrestricted policy domain privileges, you cannot register new nodes or set their proxy relationship on the Tivoli Storage Manager server. If you do not enter an administrator ID, a macro script is created so you can run on the Tivoli Storage Manager server.

A Tivoli Storage Manager 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 17. Available functions based on Tivoli Storage Manager 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 |
| **Tivoli Storage Manager 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 |

*Table 17. Available functions based on Tivoli Storage Manager Administrator ID privilege requirements (continued)*

| | **Operator** | **Operator with Reporting** | **Restricted Administrator** | **Administrator** |
|---|---|---|---|---|
| Datacenter Occupancy | No | Yes | Yes | Yes |
| | | **Configuration tab** | | |
| Node Registration (Configuration Status -> **Run Configuration Wizard**) | No | No | No[2] | Yes |
| Change Tivoli Storage Manager Admin ID Credentials (Configuration Status -> **Edit Configuration**) | Yes | Yes | Yes | Yes |
| 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. When both Data Protection for VMware and Tivoli Storage FlashCopy Manager for VMware are installed, an offloaded backup schedule is supported.
2. You cannot register the node because an unrestricted domain policy is required.
3. You can add or remove VMware datacenters and register datacenter nodes.

To view the Tivoli Storage Manager 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 Tivoli Storage Manager Server Credentials page.

**Important:**

- If the Tivoli Storage Manager administrator ID authority level changes on the Tivoli Storage Manager 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
- Data Protection for VMware vSphere GUI accessed as a plug-in from either of the vSphere GUIs
- IBM Data Protection extension in the vSphere Web Client GUI

The Data Protection for VMware vSphere GUI plug-in registration key is `com.ibm.tsm.tdpvmware@hostname`. This key is registered when you select the **Register GUI as vCenter plug-in** check box during the installation. A separate key is registered for each web GUI host. When multiple web GUI hosts exist, then multiple instances of the Data Protection for VMware vSphere GUI plug-in are registered.

IBM Data Protection extension 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 Data Protection extension 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 Tivoli Storage Manager recovery agent GUI

Instructions about how to set up the Tivoli Storage Manager 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 Tivoli Storage Manager recovery agent GUI.

**Important:** Information about how to complete tasks with the Tivoli Storage Manager 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. Linux Log on to the Linux system with root user authority. Tivoli Storage Manager recovery agent must be installed on this Linux system.
   a. Start the Tivoli Storage Manager recovery agent by clicking the Tivoli Storage Manager recovery agent GUI icon or running the `TDPVMwareMountRestore.sh` script from the shell prompt.
   b. Enter the login ID for the Windows system where both the Tivoli Storage Manager recovery agent command-line interface and Secure Shell (SSH) are installed. Make sure that this login ID uses a host name convention that is defined in the SSH `known_hosts` file. This Windows system uses SSH to communicate with the Tivoli Storage Manager recovery agent on your Linux system.
   c. Enter the host name or IP address of the Windows system where both the Tivoli Storage Manager recovery agent command-line interface and Secure Shell (SSH) are installed.
2. Windows Log on to the system where you want to restore files. Tivoli Storage Manager recovery agent must be installed on the system.
3. Click **Select TSM server** in the Tivoli Storage Manager recovery agent GUI to connect to a Tivoli Storage Manager server. Windows When the Tivoli Storage Manager 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 Tivoli Storage Manager server are populated in the Tivoli Storage Manager 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 Tivoli Storage Manager recovery agent uses that node to authenticate when started.The Tivoli Storage Manager recovery agent remembers the last node name that connected to the Tivoli Storage Manager server. If **Use Password access generate** is selected for this node (the last node name to connect), the Tivoli Storage Manager recovery agent uses these credentials to connect to the Tivoli Storage Manager server on startup. If no previous connection to the Tivoli Storage Manager server was done, and only one data mover node and one data center node are configured with the wizard, the Tivoli Storage Manager recovery agent uses these credentials to connect to the Tivoli Storage Manager server on startup.

   Linux Windows Specify the following options:

   **Server address**
   Enter the IP address or host name of the Tivoli Storage Manager.

   **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 Tivoli Storage Manager 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 Tivoli Storage Manager information dialog.

When you use this method, the Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager information dialog.

**Use Password access generate**

When this option is selected and the password field is empty, the Tivoli Storage Manager 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 Tivoli Storage Manager 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.

Tivoli Storage Manager recovery agent queries the specified server for a list of protected VMs, and shows the list.

4. Set the following mount, backup, and restore options by clicking **Settings**:

**Virtual Volume write cache**

The Tivoli Storage Manager recovery agent that is running on the Windows backup proxy host saves data changes that are created during Linux 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 on Linux 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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**.

5. Verify that each Tivoli Storage Manager server node (that was specified with the `Asnodename` and `Fromnode` options) allows backups to be deleted. The Tivoli Storage Manager 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 Tivoli Storage Manager 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.

6. When you use the Tivoli Storage Manager 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.

## 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 vCloud GUI accessed in a web browser
- Data Protection for VMware vSphere GUI accessed in a web browser
- Data Protection for VMware vSphere GUI accessed as a plug-in from either of the vSphere GUIs
- IBM Data Protection extension in the vSphere Web Client GUI
- Tivoli Storage FlashCopy Manager for VMware 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, the VMware vCloud Director, and the Tivoli Storage Manager server.

Specify the same locale settings among the systems that run the Data Protection for VMware GUI, the VMware vSphere Client, the VMware vCloud Director, and the Tivoli Storage Manager 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.

### Tivoli Storage Manager file restore interface

The interface content and message prompt language is determined by the language setting of the web browser that accesses the Tivoli Storage Manager file restore interface.

For error messages that are logged to the `fr_api.log` file, the Tivoli Storage Manager 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 Tivoli Storage Manager 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.

## Tivoli Storage Manager recovery agent log files

The Tivoli Storage Manager 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 or Data Protection for VMware vCloud GUI places log files in this directory:

Windows `C:\IBM\tivoli\tsm\tdpvmware\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 (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/logs`
When you are collecting log files, make sure to include all subdirectories in your compressed file.

## Tivoli Storage Manager file restore interface log files

The Tivoli Storage Manager 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\tivoli\tsm\tdpvmware\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 Tivoli Storage Manager 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>'2015-03-11 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>'2015-03-11 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, Tivoli Storage Manager recovery agent is started under the Local System Account.

### Tivoli Storage Manager recovery agent services on Microsoft Windows

When you start the Tivoli Storage Manager recovery agent from the Windows Start menu, the service is automatically stopped. When the Tivoli Storage Manager 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** > **Tivoli Storage Manager** > **Data Protection for VMware** > **Tivoli Storage Manager 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:

- A Tivoli Storage Manager 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
  - Tivoli Storage Manager server
  - vCenter Server

## Procedure

1. Log on to the Tivoli Storage Manager server and complete the tasks described in “Setting up the Tivoli Storage Manager nodes in a vSphere environment” on page 92.
2. Log on to the vStorage Backup Server and complete the tasks described in “Setting up the data mover nodes in a vSphere environment” on page 93.
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 101.
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 Tivoli Storage Manager nodes in a vSphere environment

This procedure describes how to manually register nodes to the Tivoli Storage Manager server and grant proxy authority for these nodes in a vSphere environment.

### Before you begin

**Important:** This manual task is not available for vCloud Director environments. You must use the Data Protection for VMware vCloud GUI to register nodes.

### About this task

All steps in this procedure are completed on the Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager nodes, the next manual configuration task is to set up the data mover nodes as described in “Setting up the data mover nodes in a vSphere environment.”

## Setting up the data mover nodes in a vSphere environment

If you offload backup workloads to a vStorage backup server in a vSphere environment, set up the data mover nodes to run the operation and move the data to the Tivoli Storage Manager server.

### Before you begin

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. The minimum set of required options is provided in Step 2.

A 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. Consider the following conditions for restore configurations:

**The data mover node is on a Windows Server 2008 or Windows Server 2008 R2 system:**

If you plan to use the SAN to restore data, you must set the Windows SAN policy to OnlineAll. Run diskpart.exe and type the following commands to turn off automatic drive letter assignment and set the SAN policy to **OnlineAll**:

```
diskpart
  automount disable
  automount scrub
  san policy OnlineAll
  exit
```

**The backup-archive client is installed in a virtual machine on a Windows Server 2008 or Windows Server 2008 R2 system:**

If you plan to use the `hotadd` transport to restore data from dynamically added disks, the SAN policy on that system must also be set to `OnlineAll`.

Whether the client uses the SAN or `hotadd` transport, the Windows SAN policy must be set to `OnlineAll`. If the SAN policy is not set to `OnlineAll`, restore operations fail, and the following message is returned:

```
ANS9365E VMware vStoragee API error.
TSM function name: vddksdk Write
TSM file : vmvddkdsk.cpp (2271)
API return code : 1
API error message : Unknown error
ANS0361I DIAG: ANS1111I VmRestoreExtent(): VixDiskLib_Write
FAILURE startSector=512 sectorSize=512 byteOffset=262144,
rc=-1
```

**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.

## About this task

**Tip:** All steps in this procedure are completed on the vStorage Backup Server.

## Procedure

1. Update the backup-archive client options file with these settings:
   - 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**
   Specify the name of a previously defined data mover node. Tivoli Storage Manager schedules are associated with the data mover node.

   **PASSWORDACCESS**
   Specify GENERATE so that the password is generated automatically (instead of a user prompt).

   **VMCHOST**
   Specify the host name of the vCenter (or ESX server) where the off-host backup commands are directed.

   **VMBACKUPTYPE**
   Specify FULLVM. This setting designates that a full VM backup is run. This value is necessary to run full VM and full VM incremental backups.

   **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 Tivoli Storage Manager server.

**TCPPORT**
Specify the TCP/IP port address for the Tivoli Storage Manager server.

**COMMMETHOD**
Specify the communication method to be used by the Tivoli Storage Manager server. For data mover nodes, you must specify TCP/IP as the communication method. If another method is specified, operations fail.

**HTTPPORT**
This option specifies a TCP/IP port address and is required only when more than one client acceptor service is used. For example, if two data mover nodes (and two client acceptor services) are used, then the option file for each data mover node must specify a different `HTTPPORT` value.

An example dsm.dm.opt file with these settings 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
```

For instant access, instant restore, or mount (file restore) operations, make sure to add `VMISCSISERVERADDRESS` to the backup-archive client 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.

2. 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>
   ```

3. Start a backup-archive client 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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:

   a. Verify the connection to the Tivoli Storage Manager 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.

b. Verify you can back up a VM by issuing this command:

```
dsmc backup vm vm1
```

In Steps 3b and 3d, `vm1` is the name of the VM.

c. Verify that the backup completed successfully by issuing this command:

```
dsmc query vm "*"
```

d. Verify that the VM can be restored by issuing this command:

```
dsmc restore vm vm1 -vmname=vm1-restore
```

4. Set up the client acceptor service and backup-archive scheduler service by completing the following tasks:
   - Windows This procedure uses the Tivoli Storage Manager 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 Tivoli Storage Manager Client Service Configuration Utility (**`dsmcutil`**) for this task, make sure to also install the remote client agent service.

     Start the Tivoli Storage Manager 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 and proceed to Step b.

       **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**.
   - Linux For the backup-archive client on Linux, complete the following steps:

     a. Specify the following options in the `dsm.sys` file, in the stanza for the data mover 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.

- (Optional) If you want to direct schedule and error information to log files other than the default files, specify the `schedlogname` and `errorlogname` options with the fully qualified path and file name in which to store log information. For example:

  ```
  schedlogname /vmsched/dsmsched_dm.log
  errorlogname /vmsched/dsmerror_dm.log
  ```

b. Start the client acceptor service:

   The installation program creates a startup script for the client acceptor (`dsmcad`) in `/etc/init.d`. The client acceptor must be started before it can manage scheduler tasks, or manage the web client. As root, complete the following steps:

   1) Configure the client acceptor service and backup-archive scheduler service to act as a vStorage Backup Server. You must set the `LD_LIBRARY_PATH` environment variable to the client installation directory and the Java shared library `libjvm.so`. The path to `libjvm.so` is also used for tagging support when you enable the `vmtagdatamover` client option on the data mover.

      Ensure that Java software is installed and the `JAVA_HOME` environment variable is exported correctly.

      The following paths are typical examples of the path to `libjvm.so`:

      - For IBM Java: `$JAVA_HOME/jre/bin/classic/libjvm.so`
      - For Oracle Java: `$JAVA_HOME/jre/lib/amd64/server/libjvm.so`

      You must set the `LD_LIBRARY_PATH` environment variable in the `/etc/init.d/dsmcad` file. For example:

      - For IBM Java, set the following environment variable:

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

      - For Oracle Java, set the following environment variable:

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

   2) Start the client acceptor by issuing the following command:

      ```
      service dsmcad start
      ```

      To enable the client acceptor to start automatically after a system restart, add the service as follows, at a shell prompt:

      ```
      # chkconfig --add dsmcad
      ```

      **Tip:** If you want to run the **`dsmc`** command directly from the Linux command-line, you must also apply the `LD_LIBRARY_PATH` environment variable to the command shell.

5. 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
      ```

   **Tip:** When the IP address changes on the system where the Data Protection for VMware vSphere GUI is installed, you must complete the following:

   a. Set up the client acceptor again (Step 3) 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.

### What to do next

After successfully setting up the data mover nodes, the next manual configuration task is to configure the VMCLI profile as described in "Configuring the Data Protection for VMware command-line interface in a vSphere environment" on page 101.

## Setting up the data mover nodes in a vCloud environment

If you offload backup workloads to a vStorage backup server, set up the data mover nodes to run the operation and move the data to the Tivoli Storage Manager server.

### Before you begin

In a standard Data Protection for VMware vCloud GUI 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 provider vDC 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. The minimum set of required options is provided in Step 2.All steps in this procedure are completed by using the Tivoli Storage Manager backup-archive client that is installed on the vStorage backup server.

### About this task

This task sets up the data mover nodes by updating the backup-archive client options and verifying connectivity to the Tivoli Storage Manager server.

### Procedure

1. Update the backup-archive client options file with these settings:
   - 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**
   Specify the name of a previously defined data mover node. Tivoli Storage Manager schedules are associated with the data mover node.

   **PASSWORDACCESS**
   Specify GENERATE so that the password is generated automatically (instead of a user prompt).

   **VCDHOST**
   Specify the host name of the VMware vCloud Director server that manages vApps that you want to protect.

   **VMCHOST**
   Specify the host name of the VMware VirtualCenter or ESX server that you want to back up, restore, or query.

   **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 Tivoli Storage Manager server.

**TCPPORT**

Specify the TCP/IP port address for the Tivoli Storage Manager server.

**COMMMETHOD**

Specify the communication method to be used by the Tivoli Storage Manager server. For data mover 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 required only when more than one client acceptor service is used. For example, if two data mover nodes (and two client acceptor services) are used, then the option file for each data mover node must specify a different `HTTPPORT` value.

An example dsm.dm.opt file with these settings is provided here:

```
NODename DM_MYDMNODE
PASSWORDAccess generate
VCDHost vcloud1.example.com
VMCHost vcenter1.example.com
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort 1500
COMMMethod tcpip
HTTPPORT 1583
```

2. Issue this command to set the vCloud Director user and password for the data mover node:

   ```
   dsmc set password -type=vcd vcloud1.example.com <vcloud_administrator1> <vcloud_password1>
   ```

3. Issue this command to set the vCenter user and password for the data mover node:

   ```
   dsmc set password -type=vm vcenter1.example.com <vcenter_administrator1> <vcenter_password1>
   ```

4. Start a backup-archive client command-line session with the `-asnodename` and `-optfile` command-line parameters:

   ```
   dsmc -asnodename=PVDC_vcloud1 -optfile=dsm_MYDM.opt
   ```

   Make sure that after your initial sign-on, you are not prompted for your password.

   **Attention:** To prevent the Tivoli Storage Manager 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 Tivoli Storage Manager server for schedules associated with `nodename` (data mover node), not `asnodename` (provider vDC 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:

   a. Verify the connection to the Tivoli Storage Manager 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.

   b. Verify you can back up a vApp by issuing this command:

```
dsmc backup vapp org=organization_name,orgvdc=org_vdc_name1,vapp=vapp1
```

In Steps 3b and 3d, vapp1 is the name of the vApp.

c. Verify that the backup completed successfully by issuing this command:

```
dsmc query vapp "*"
```

d. Verify that the vApp can be restored by issuing this command:

```
dsmc restore vapp org=organization_name,orgvdc=org_vdc_name1,vapp=vapp1
-vappname=vapp1-restore
```

5. Set up the client acceptor service and backup-archive scheduler service by completing these tasks:
   - Windows This procedure uses the Tivoli Storage Manager 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 Tivoli Storage Manager Client Service Configuration Utility (**dsmcutil**) for this task, make sure to also install the remote client agent service. Start the Tivoli Storage Manager 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 and proceed to Step b.

       **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**.
   - Linux For the backup-archive client on Linux, complete the following steps:
     a. Specify the following options in the `dsm.sys` file, in the stanza for the data mover 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.
        - (Optional) If you want to direct schedule and error information to log files other than the default files, specify the `schedlogname` and `errorlogname` options with the fully qualified path and file name in which to store log information. For example:

```
schedlogname /vmsched/dsmsched_dm.log
errorlogname /vmsched/dsmerror_dm.log
```

b. Start the client acceptor service:

The installation program creates a startup script for the client acceptor (dsmcad) in /etc/init.d. The client acceptor must be started before it can manage scheduler tasks, or manage the web client. As root, complete the following steps:

1) Configure the client acceptor service and backup-archive scheduler service to act as a vStorage Backup Server. You must set the LD_LIBRARY_PATH environment variable to the client installation directory and the Java shared library libjvm.so.

Ensure that Java software is installed and the JAVA_HOME environment variable is exported correctly.

The following paths are typical examples of the path to libjvm.so:

- For IBM Java: $JAVA_HOME/jre/bin/classic/libjvm.so
- For Oracle Java: $JAVA_HOME/jre/lib/amd64/server/libjvm.so

You must set the LD_LIBRARY_PATH environment variable in the /etc/init.d/dsmcad file. For example:

- For IBM Java, set the following environment variable:

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

- For Oracle Java, set the following environment variable:

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

2) Start the client acceptor by issuing the following command:

```
service dsmcad start
```

To enable the client acceptor to start automatically after a system restart, add the service as follows, at a shell prompt:

```
# chkconfig --add dsmcad
```

**Tip:** If you want to run the **dsmc** command directly from the Linux command-line, you must also apply the LD_LIBRARY_PATH environment variable to the command shell.

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
```

## 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 (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\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 Tivoli Storage Manager server and the agent node (`MY_VMCLINODE`).

   **Restriction:** The VMCLI node does not support the SSL protocol or LDAP authentication when communicating with the Tivoli Storage Manager 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 Tivoli Storage Manager server.

   **VE_TSM_SERVER_PORT**

   Specify the port name to use for the Tivoli Storage Manager 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 Tivoli Storage Manager 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.
- Linux Windows 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 Tivoli Storage Manager 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

Linux Windows After successfully completing the three manual configuration tasks described in this section:

1. “Setting up the Tivoli Storage Manager nodes in a vSphere environment” on page 92
2. “Setting up the data mover nodes in a vSphere environment” on page 93

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 Tivoli Storage Manager server.

1. Register the following nodes to the Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 backup-archive client 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 To configure the Client Acceptor Service and Backup-Archive 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
   ```
8. 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
```

9. Verify that the Tivoli Storage Manager 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.

10. 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 (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\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 Tivoli Storage Manager node configuration:

```
vmcli -f inquire_config -t TSM
```

## Tape configuration guidelines

Review these guidelines before attempting backup or restore operations to tape storage.

### Preparing for backup to tape

Linux Windows Before attempting a backup to tape, these parameters must be set on the Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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.

## Preparing for restore from tape

**File restore from physical tape**

File restore from a mounted snapshot volume on tape is supported with the following limitations:

- To mount a snapshot volume on physical tape, the recovery agent mount must be operating in Tape Mode. In this mode, only one VM snapshot volume can be mounted at a time from the recovery agent. The limit is one disk when mounting an iSCSI target or one volume when creating a virtual volume from a selected partition. You can have multiple Tivoli Storage Manager tape storage pool volume mounts for different VM snapshots. Create this scenario by installing the recovery agent on multiple physical systems or on multiple VM guests. Enable Tape Mode by selecting Storage Type=Tape in the recovery agent GUI Settings menu.
- While recovery agent mount does not prevent an attempt to mount a snapshot on physical tape, performance can vary significantly and might be severely affected. The recovery agent mount does not control the way data is accessed on tape. Data access patterns can be random and cause extensive challenges associated with tape positioning operations. For Linux VMs, Tape Mode is only supported when directly using the iSCSI initiator. Tape Mode is not supported from the Linux recovery agent user interface.

While a limited number of files can be recovered from a mounted volume snapshot on physical tape, consider running a full VM restore from physical tape if you must recover a large quantity of data or many files.

Typically the performance associated with a file restore from a VTL is quicker than physical tape. But, performance delays can be encountered. For example, mount might require a virtual tape volume that is in use by another restore operation. Tape volumes in a VTL cannot be shared. In this case, mount processing is delayed until the restore operation with the virtual tape volume completes.

When a mount or instant restore operation requires the same tape storage simultaneously in use by a backup operation, the backup operation becomes interrupted.

**Instant restore from physical tape**

The Tivoli Storage Manager recovery agent instant restore operation is not supported for snapshot volumes on physical tape.

The failure behavior for instant restore depends on the mode of operation:

- Tape mode: Instant restore fails when the restore operation is selected.
- Non-tape mode: Instant restore fails when an attempt is made to access data on a tape volume.

This failure can occur when the user interface tries to show partition information or when the operation is restoring data. The latter condition occurs only if disk to tape migration is being used, and part of the snapshot data (the partition information) is on disk and some of the actual snapshot data is on tape.

If you try to run instant restore in Tape Mode, the following message is shown:

```
Instant Restore is not supported in Tape Mode.
```

If you try to run instant restore while not in Tape Mode, and the data is on tape, the following message is shown:

```
An error occured while reading snapshot data from server. See log for details.
```

## Manually configuring an iSCSI device on a Linux system

Linux

This procedure describes how to configure a Linux system that is used during an iSCSI mount operation. The VM snapshot is mounted from Tivoli Storage Manager server storage.

### Before you begin

During an iSCSI mount, an iSCSI target is created on the Tivoli Storage Manager recovery agent system. Microsoft iSCSI Initiator is not required on the Tivoli Storage Manager 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 Tivoli Storage Manager recovery agent (or iSCSI target) is installed:
   a. Start the Tivoli Storage Manager recovery agent. Complete the `Select TSM 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
      Tivoli Storage Manager 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

Windows

This procedure describes how to configure a Windows system that is used during an iSCSI mount operation. The snapshot is mounted from Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager recovery agent (or iSCSI target) is installed:
   a. Start the Tivoli Storage Manager recovery agent GUI. Complete the Select TSM 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 Tivoli Storage Manager 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 Tivoli Storage Manager 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 Tivoli Storage Manager recovery agent GUI and clicking **Dismount**.

## Manually configuring the mount proxy nodes on a Linux system

Linux

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 backup-archive client that is installed on the backup server.

### About this task

This task sets up the mount proxy nodes by updating the backup-archive client options and verifying connectivity to the Tivoli Storage Manager 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. Tivoli Storage Manager 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 Tivoli Storage Manager server.

**TCPPORT**
Specify the TCP/IP port address for the Tivoli Storage Manager server.

**COMMMETHOD**
Specify the communication method to be used by the Tivoli Storage Manager 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 backup-archive client 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 Tivoli Storage Manager scheduler from failing, make sure that the `asnodename` option is not set in the `dsm.sys` file stanza (Linux). The scheduler queries the Tivoli Storage Manager 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 Tivoli Storage Manager 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 Backup-Archive 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
       ```
   - To configure the Client Acceptor Service and Backup-Archive Scheduler Service to act as a backup server, set the following environment variable in the /etc/init.d/dsmcad file:
     ```
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
     ```
   - 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:
     ```
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
     ```
     ```
     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
      ```

## Manually configuring the mount proxy nodes on a remote Windows system

Windows

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:
   - Tivoli Storage Manager recovery agent
   - Tivoli Storage Manager backup-archive client

   Access both products on the Tivoli Storage Manager for Virtual Environments product DVD or 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 25
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.
   d. In the Primary Node column of the table, go to the Windows mount proxy node with the pending location and click **View Settings**.
   e. Copy the sample `dsm.opt` file content that is shown in the **Mount Proxy Settings** dialog.
   f. 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 backup-archive client 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→ Tivoli Storage Manager → 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 Tivoli Storage Manager 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 Backup-Archive Scheduler Service by completing these steps:
   This step uses the Tivoli Storage Manager 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 Tivoli Storage Manager Client Service Configuration Utility (`dsmcutil`) for this task, make sure to also install the Remote Client Agent Service.
Start the Tivoli Storage Manager 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
```

## 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 or Data Protection for VMware vCloud GUI.

The Data Protection for VMware installation process requires that a user specifies a vCenter or vCloud 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\tivoli\tsm\tdpvmware\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 modify whether to use the GUI for vSphere protection or vCloud protection, specify one of the following values in the **<mode></mode>** parameter:

- *vcenter* The GUI is used for vSphere protection. For example:

  ```
  <mode>vcenter</mode>
  ```

- *vcloud* The GUI is used for vCloud protection. For example:

  ```
  <mode>vcloud</mode>
  ```

To modify the vCloud Director server IP address, make sure **<mode>vcloud</mode>** is set, then specify the IP address in the **<vcloud_url></vcloud_url>** parameter. For example:

```
<vcloud_url>https://vclouddir.myco.com</vcloud_url>
```

The https:// value is required at the beginning of the vCloud Director server IP address.

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 vCloud protection and web browser access is enabled for the GUI:

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
 <VMCLIPath>C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts\
</VMCLIPath>
 <interruptDelay>900000</interruptDelay>
 <mode>vcloud</mode>
 <vcloud_url>https://vclouddir.myco.com</vcloud_url>
 <vcenter_url></vcenter_url>
 <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

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 (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts\
</VMCLIPath>
 <interruptDelay>900000</interruptDelay>
 <mode>vcenter</mode>
 <vcloud_url></vcloud_url>
 <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
 <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

# Appendix B. Migrating to an incremental forever 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 periodic 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 periodic 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 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 backup strategy.

To migrate existing Data Protection for VMware schedules to an incremental forever 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 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 Tivoli Storage Manager Backup-Archive Client 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 backups:

Complete the following backup policy tasks on the Tivoli Storage Manager 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 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 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 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 full and incremental backups are taken (as part of the 6.2 and 6.3 periodic 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 full and incremental backups.

   The `verexists` parameter specifies the maximum number of VM backup versions to retain on the server. If an incremental forever 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 full backup of each ESX host with data mover node `dm1`.

- The `bup_esxcluster_incr` schedule runs a daily 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 periodic full or incremental backups) to update. In this procedure, the periodic full `bup_esxcluster_full` schedule is used.

d. Right-click the schedule and select **Properties**.

e. Go to the Schedule page and specify **Incremental forever** from the **Backup strategy** drop-down list.

f. Click **OK** to save your update.

g. Locate the backup schedule used for incremental backups. Right-click the schedule and select **Delete**. Since the periodic full `bup_esxcluster_full` schedule was updated to incremental forever, this incremental schedule is no longer needed.

3. Now that you have an incremental forever 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 Tivoli Storage Manager 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 backup strategy.

**Restrictions**: After migrating schedules from periodic full backup types to incremental forever backup types, be aware of the following restrictions:

- Changing migrated schedules back to periodic full backup types per VM (file space) is not supported.
- Using an earlier version of the Tivoli Storage Manager backup-archive client on a migrated file space is not supported.
- When a file space contains one (or more) incremental forever backups, a periodic 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 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 backup is scheduled (Monday through Saturday).

The number of backups taken for a four week period is 28:

- Four full backups (one weekly full backup multiplied by four weeks)
- 24 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 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 full and incremental backups, the `verexists=28` value preserves all 28 backups.

# Appendix C. Integrating with Tivoli Storage FlashCopy Manager for VMware

Integration allows offload backups of the Tivoli Storage FlashCopy® Manager hardware snapshots to a Tivoli® Storage Manager server for long-term retention.

The benefits of integrating Tivoli Storage FlashCopy Manager for VMware with Data Protection for VMware are as follows:

- In addition to the hardware snapshots that are retained on disk, backup versions of virtual machines are retained on the Tivoli Storage Manager server based on Storage Management policies that are set up by the Tivoli Storage Manager administrator.
- The data movement to Tivoli Storage Manager can be offloaded using a vStorage backup server to minimize the load on the resources available to the virtual machines in the vCenter server. The vStorage backup server can be a physical or virtual machine.

## Comparing solutions

Compare the key features for each Tivoli Storage Manager for Virtual Environments and Tivoli Storage FlashCopy Manager for VMware solution to determine which configuration best meets your data protection requirements.

| | **Tivoli Storage Manager for Virtual Environments only** | **Tivoli Storage FlashCopy Manager for VMware only** | **Tivoli Storage Manager for Virtual Environments integrated with Tivoli Storage FlashCopy Manager for VMware** |
|---|---|---|---|
| **Backup objective** | | | |
| Back up an entire virtual machine to Tivoli Storage Manager storage. | ✓ | | |
| Back up an entire virtual machine to hardware storage. | | ✓ | |
| Back up only the virtual machine data that changed since the last full backup completed. | ✓ | | |
| Back up one or more VMware datastores to hardware storage. | | ✓ | |
| Offload backup on hardware storage to Tivoli Storage Manager storage. | | | ✓ |
| **Restore objective** | | | |
| Restore an entire virtual machine to the state it existed in when originally backed up. | ✓ | ✓ | ✓ |
| Restore the content of a single virtual machine volume for immediate use. | ✓ | ✓ | ✓ |
| Restore one or more VMware datastores. | | ✓ | |
| Restore individual files. | ✓ [1] | ✓ [2] | |

| | **Tivoli Storage Manager for Virtual Environments only** | **Tivoli Storage FlashCopy Manager for VMware only** | **Tivoli Storage Manager for Virtual Environments integrated with Tivoli Storage FlashCopy Manager for VMware** |
|---|---|---|---|
| Restore one or more virtual disks. | | ✓ | |

Notes:

1. Use the Tivoli Storage Manager file restore interface to restore files with a web-based interface.
2. Individual files that you want to restore are located in virtual disks that are part of a virtual machine backup. For individual file restore operations from a Tivoli Storage FlashCopy Manager for VMware backup, you must attach the virtual disks to the ESXi host where the target virtual machine is running, and use the tools within the guest virtual machine to mount the virtual disks and copy the individual files to the target virtual machine.

# Roadmap for implementing an integration solution

Plan for an integration solution that includes both Tivoli Storage Manager for Virtual Environments and Tivoli Storage FlashCopy Manager for VMware in the VMware vSphere environment.

## About this task

This method requires these programs to be installed and configured:

- Tivoli Storage FlashCopy Manager for VMware is installed and configured on a physical server running RedHat or SUSE Linux, or in a virtual machine, in one of the ESXi hosts in the VMware datacenter, with a guest operating system of RedHat or SUSE Linux. If Tivoli Storage FlashCopy Manager for VMware is installed on a virtual machine, this virtual machine must not be part of any backup process.
- Tivoli Storage Manager for Virtual Environments is installed and configured on the same system as Tivoli Storage FlashCopy Manager for VMware.

## Procedure

To integrate Tivoli Storage Manager for Virtual Environments with Tivoli Storage FlashCopy Manager for VMware, complete the following tasks:

1. Install Tivoli Storage Manager for Virtual Environments and the data mover feature V7.1.6. Follow the instructions in “Installing Data Protection for VMware on Linux systems” on page 26.
2. Configure Tivoli Storage Manager for Virtual Environments V7.1.6. Follow the instructions in Chapter 2, “Configuring Data Protection for VMware,” on page 57.
3. Install Tivoli Storage FlashCopy Manager for VMware V4.1.6. Follow the instructions in Installing by using the installation wizard
4. Configure Tivoli Storage FlashCopy Manager for VMware V4.1.6. Follow the instructions in Configuring Tivoli Storage FlashCopy Manager for VMware

## What to do next

The following scenarios provide insight into possible integration uses:

- To minimize the impact of the offload backup operation to the production ESXi host, specify an auxiliary ESXi host for Tivoli Storage FlashCopy Manager for VMware. In this scenario, the hardware snapshots are mounted and attached to the auxiliary ESXi host. As a result, the Tivoli Storage Manager for Virtual Environments offload backup operation is processed from the auxiliary ESXi host.
- When you implement backups for disaster recovery scenarios, consider storing the offloaded backups in a different physical location than the original data. For example, offload the backups to a Tivoli Storage Manager server that is in a different location than the storage device subsystem.

# Appendix D. Accessibility features for the Tivoli Storage Manager product family

Accessibility features help users who have a disability, such as restricted mobility or limited vision to use information technology products successfully.

## Accessibility features

The IBM Tivoli Storage Manager family of products includes the following accessibility features:

- Keyboard-only operation using standard operating-system conventions
- Interfaces that support assistive technology such as screen readers

The command-line interfaces of all products in the product family are accessible.

Tivoli Storage Manager Operations Center provides the following additional accessibility features when you use it with a Mozilla Firefox browser on a Microsoft Windows system:

- Screen magnifiers and content zooming
- High contrast mode

The Operations Center and the Tivoli Storage Manager server can be installed in console mode, which is accessible.

The Operations Center help system is enabled for accessibility. For more information, click the question mark icon on the help system menu bar.

## Vendor software

The Tivoli Storage Manager 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 the accessibility information about its products.

## IBM and accessibility

See the IBM Human Ability and Accessibility Center (http://www.ibm.com/able) for information about the commitment that IBM has to accessibility.

# Notices

This information was developed for products and services offered in the U.S.A.

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*
*United States of America*

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*

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** 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 states 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 want 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 Corporation*
*2Z4A/101*
*11400 Burnet Road*
*Austin, TX 78758*
*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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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:

```
Portions of this code are derived from IBM® Corp. Sample Programs.
© Copyright IBM® Corp. _enter the year or years_. All rights reserved.
```

## 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.

## 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 Tivoli Storage Manager family of products.

See Tivoli Storage Manager glossary.

To view glossaries for other IBM products, see IBM Terminology.

# Index

Product Number: 5725-A44

Printed in USA