

IBM Tivoli Storage Manager for Virtual Environments
Version 7.1

*Data Protection for VMware Installation
Guide*



IBM Tivoli Storage Manager for Virtual Environments
Version 7.1

*Data Protection for VMware Installation
Guide*



Note:

Before using this information and the product it supports, read the information in “Notices” on page 107.

First edition (December 2013)

This edition applies to version 7, release 1, modification 0 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.

© Copyright IBM Corporation 2011, 2013.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this publication	v
Who should read this publication	v
Publications	v

New for Tivoli Storage Manager for Virtual Environments Version 7.1 . . . vii

Chapter 1. Preparing to install Data Protection for VMware 1

Installation roadmap	6
Required installation permissions	8
Required communication ports	9
Hardware requirements	11
Environment requirements	12
Supported operating systems	14
Supported operating systems for the Recovery Agent command-line interface	14
Supported operating systems for Data Protection for VMware Recovery Agent GUI	15
Supported operating systems for Data Protection for VMware vSphere GUI	16
Supported operating systems for Data Protection for VMware vCloud GUI	17
Supported operating systems for the data mover	17

Chapter 2. Installing Data Protection for VMware 19

Installing all features on Microsoft Windows 64-bit (Typical Installation)	20
Installing selected features on Microsoft Windows 32-bit or 64-bit (Advanced Installation)	22
Installing selected features on Linux with InstallAnywhere mode	26
Performing a clean installation of Data Protection for VMware on Linux	28
Installing language packs	29
Installing a language pack on Windows	30
Installing a language pack on Linux	30
Installing Data Protection for VMware in silent mode	30
Installing all features on a Windows 32-bit system in silent mode with Suite installer	31
Installing all features on a Windows 64-bit system in silent mode with Suite installer	32
Installing selected Data Protection for VMware features on a Windows 32-bit system in silent mode	33
Installing selected Data Protection for VMware features on a Windows 64-bit system in silent mode	35
Installing selected Data Protection for VMware features on a Linux system in silent mode	39
Uninstalling Data Protection for VMware	42

Uninstalling Data Protection for VMware with the Microsoft Windows Installer Tool	43
Uninstalling Data Protection for VMware for a Windows 32-bit system in silent mode	43
Uninstalling Data Protection for VMware for Windows 64-bit system in silent mode	43
Uninstalling Data Protection for VMware a Linux system	44
Data Protection for VMware log files	46

Chapter 3. Upgrading Data Protection for VMware 49

Upgrading Data Protection for VMware from Version 6.x	49
Upgrading Data Protection for VMware from Tivoli Storage FlashCopy Manager for VMware Version 3.x	51
Upgrading Data Protection for VMware from Tivoli Storage FlashCopy Manager for VMware Version 3.x and Data Protection for VMware Version 6.x	52
Upgrading Data Protection for VMware on a Windows 32-bit system in silent mode	54
Upgrading Data Protection for VMware on a Windows 64-bit system in silent mode	55
Upgrading Data Protection for VMware on a Linux system in silent mode	55
Upgrading the data mover nodes on the vStorage Backup Server	55

Chapter 4. Configuring Data Protection for VMware 57

Creating an initial configuration with the wizard	57
Editing an existing configuration with the notebook	59
Starting and running services for Data Protection for VMware	60
Tape configuration guidelines	61
Configuring systems for iSCSI mount	64
Configuring the Data Protection for VMware Recovery Agent GUI	67
Configuring Cygwin for use when restoring files from a Linux machine	71
Modifying the VMCLI configuration file	75

Appendix A. Advanced configuration tasks 77

Setting up the Tivoli Storage Manager nodes in a vSphere environment	77
Setting up the data mover nodes in a vSphere environment	79
Setting up the data mover nodes in a vCloud environment	83
Configuring the Data Protection for VMware command-line interface in a vSphere environment	87
vSphere environment command-line interface configuration checklist	89

Appendix B. Migrating to an incremental forever backup strategy . . .	93
--	-----------

Appendix C. Integrating Tivoli Storage Manager for Virtual Environments with Tivoli Storage FlashCopy Manager for VMware	97
---	-----------

Appendix D. Tivoli support information	99
Communities and other learning resources	99
Searching knowledge bases.	101
Searching the Internet	101
Using IBM Support Assistant	101
Finding product fixes.	102
Receiving notification of product fixes	102
Contacting IBM Software Support	102
Setting up and managing support contracts	102
Determining the business impact	103
Describing the problem and gathering background information.	103
Submitting the problem to IBM Software Support	103

Appendix E. Accessibility features for the Tivoli Storage Manager product family.	105
--	------------

Notices	107
Trademarks	109
Privacy policy considerations	109

Glossary	111
A	111
B	113
C	114
D	115
E	117
F	118
G	118
H	119
I.	120
J.	120
K	120
L	121
M	122
N	123
O	124
P	124
Q	125
R	126
S	127
T	130
U	130
V	131
W	132

Index	133
------------------------	------------

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 7.1: Data Protection for VMware User's Guide*.

Publications

Publications for the Tivoli Storage Manager family of products are available online. 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 Tivoli.

To search across all publications or to download PDF versions of individual publications, go to the Tivoli Storage Manager information center at <http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1>.

You also can find the Tivoli Storage Manager product family information centers and other information centers that contain official product documentation for current and previous versions of Tivoli products at Tivoli Documentation Central. Tivoli Documentation Central is available at [http://www.ibm.com/developerworks/community/wikis/home/wiki/Tivoli Documentation Central](http://www.ibm.com/developerworks/community/wikis/home/wiki/Tivoli%20Documentation%20Central).

New for Tivoli Storage Manager for Virtual Environments Version 7.1

The Tivoli Storage Manager for Virtual Environments product compliments other Tivoli Storage Manager products.

Simplified installation and configuration

The entire Tivoli Storage Manager for Virtual Environments V7.1 solution is provided on a single DVD. Install and configure both Data Protection for VMware and Tivoli Storage Manager backup-archive client data mover features from a single front end installation GUI for Microsoft Windows. For more information, see Chapter 1, “Preparing to install Data Protection for VMware,” on page 1.

Separate installation and user guides

Tivoli Storage Manager for Virtual Environments V7.1 documentation is provided in the following guides:

- *IBM Tivoli Storage Manager for Virtual Environments Version 7.1: Data Protection for VMware Installation Guide*

Contains software and hardware prerequisites, installation, upgrade, and configuration tasks.

- *IBM Tivoli Storage Manager for Virtual Environments Version 7.1: Data Protection for VMware User's Guide*

Contains overview information, strategy planning, backup and restore scenarios, command-line reference, and error messages.

Chapter 1. Preparing to install Data Protection for VMware

Review prerequisite information before you attempt 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 Tivoli Storage Manager backup-archive client (installed on the vStorage Backup server) to complete full and incremental backups of VMs. The client node installed on the vStorage Backup server is called the Tivoli Storage Manager 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.

The Tivoli Storage Manager 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. Tivoli Storage Manager for Virtual Environments V7.1 for Microsoft Windows 64-bit includes the Tivoli Storage Manager backup-archive client data mover features on the product DVD or download package.

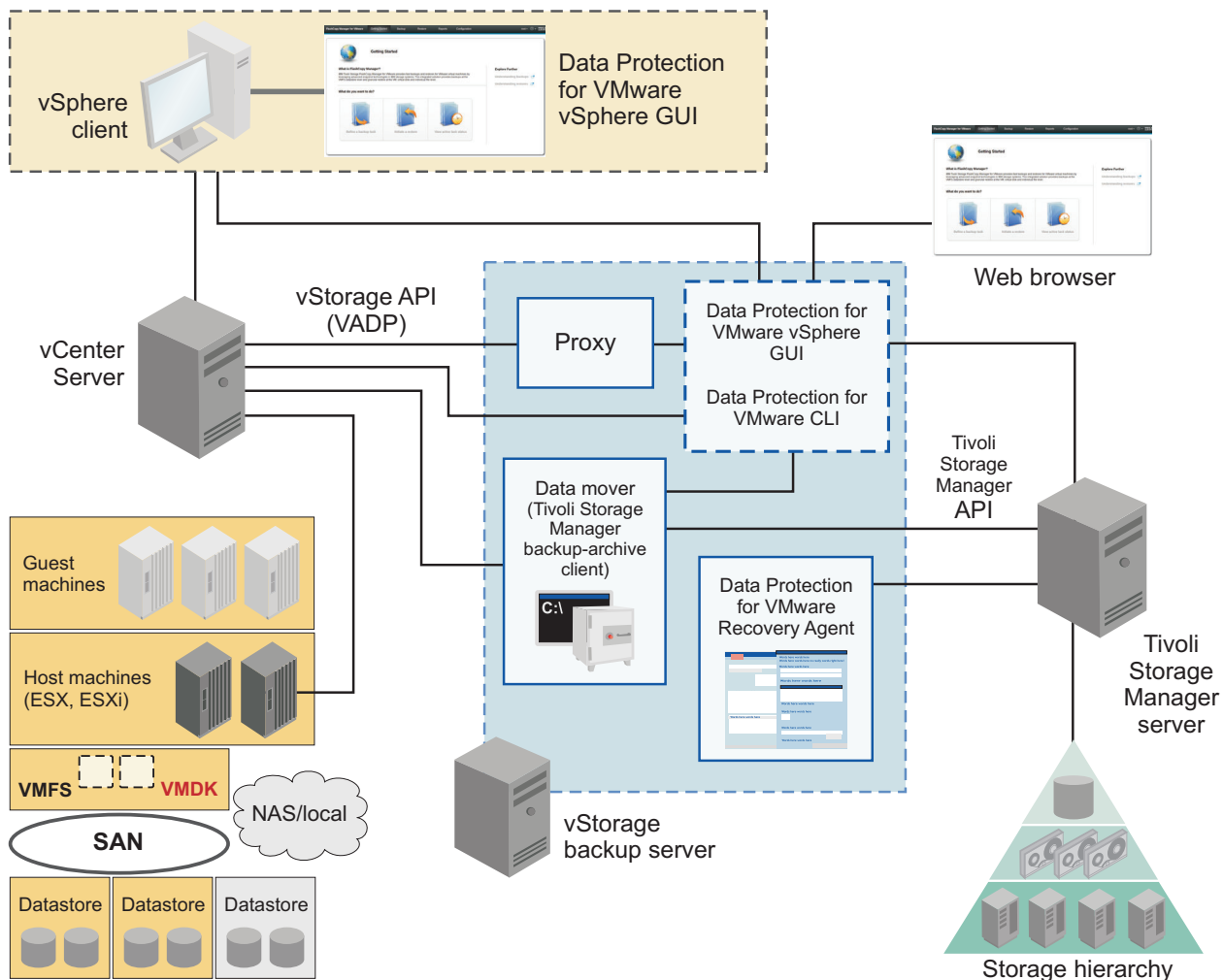


Figure 1. Tivoli Storage Manager for Virtual Environments system components in a VMware vSphere user environment

Data Protection for VMware provides several components to assist with protecting your VMs.

Data Protection for VMware vSphere GUI

This component is a graphical user interface (GUI) that accesses VM data on the VMware vCenter Server. This GUI is provided in two access 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. This access method was also provided in version 6.3 and 6.4.
- A stand-alone web browser GUI. This access method is new in version 7.1. This GUI is accessed through a URL bookmark to the GUI web server. For example:
<https://finapps.mycompany.com:9081/TsmVMwareUI/>

You can specify one or both access methods during installation. In addition to Data Protection for VMware vSphere GUI version 7.1 style updates, the summary tab and VMware inventory tree were removed to provide space for more content.

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

- Initiate a backup of your VMs to a Tivoli Storage Manager server, or schedule a backup for a later time.
- 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 your backups.

Important: Information about how to complete tasks with the Data Protection for VMware 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.

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

You can register multiple Data Protection for VMware 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 Data Protection for 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 Data Protection for VMware vSphere GUIs to a single vCenter Server, the following guidelines apply:

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

The Data Protection for VMware 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 9080, 9081) must be available.

Data Protection for VMware Recovery Agent

This service enables the mounting of any snapshot volume from the Tivoli Storage Manager server. You can view the snapshot locally, with read-only access, on the

client system, or use an iSCSI protocol to access the snapshot from a remote computer. In addition, the Data Protection for VMware Recovery Agent provides the instant restore function. A volume used in instant restore processing remains available while the restore process proceeds in the background. The Data Protection for VMware Recovery Agent is accessed with the Data Protection for VMware Recovery Agent GUI or command-line interface.

The Data Protection for VMware Recovery Agent command-line interface is installed on a Windows system to perform the following tasks from a remote machine:

- Gather information about available restorable data, including lists of:
 - Backed-up VMs
 - Snapshots available for a backed-up machine
 - Partitions available in a specific snapshot
- Mount a snapshot as a virtual device.
- Get a list of virtual devices.
- Remove a virtual device.

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

- Initiate[®] a backup of your VMs to a Tivoli Storage Manager server, or schedule a backup for a later time.
- 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 different from the one implemented by the Data Protection for VMware vSphere GUI. Also, the Data Protection for VMware CLI is useful when evaluating automation results with scripts.

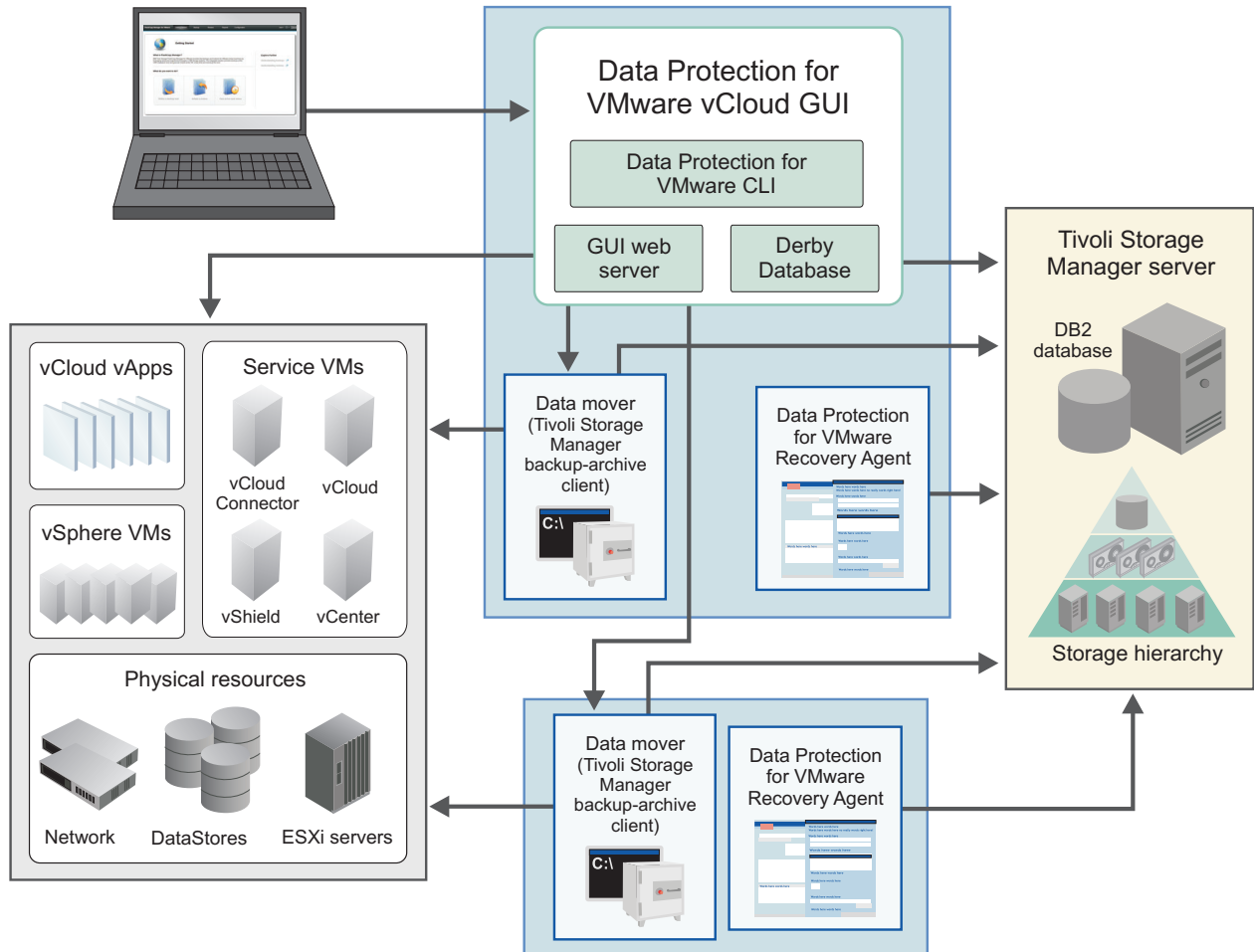


Figure 2. Tivoli Storage Manager for Virtual Environments system components in a VMware vCloud Director user environment

Data Protection for VMware vCloud GUI

This component is a GUI that protects vApps and organization vDCs in a vCloud Director environment. This GUI is accessed through a URL bookmark to the GUI web server. For example:

<https://finapps.mycompany.com:9081/TsmVMwareUI/>

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

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

Important: Information about how to complete tasks with the Data Protection for VMware 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.

Installation roadmap

This list of prerequisites, installation, and configuration tasks guides you through the complete installation process.

Tip: To assist with planning the quantity of proxy hosts required for your specific Tivoli Storage Manager for Virtual Environments 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.

Windows

Install all features on a single Microsoft Windows 64-bit system (Typical Installation)

Table 1. Installation tasks for new Data Protection for VMware customer

Step	Task	Get started here
1	Check operating 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 all features on a single Microsoft Windows 64-bit system	Each installation package presents you with a user licensing file (EULA). If you do not accept the file, the installation ends.
5	Configure Data Protection for VMware	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.

Windows

Install selected features on Microsoft Windows 32-bit or 64-bit (Advanced Installation)

Table 2. Installation tasks for new Data Protection for VMware customer

Step	Task	Get started here
1	Check operating system requirements	Make sure the system on which Data Protection for VMware is to be installed meets the system requirements.

Table 2. Installation tasks for new Data Protection for VMware customer (continued)

Step	Task	Get started here
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 selected features on Microsoft Windows 32-bit or 64-bit	Each installation package presents you with a user licensing file (EULA). If you do not accept the file, the installation ends.
5	Configure Data Protection for VMware	Use the configuration wizard for an initial configuration. Depending on the features that are installed, more configuration tasks might be required as described in Chapter 4, “Configuring Data Protection for VMware,” on page 57.

Linux

Install selected features on Linux with InstallAnywhere mode

Table 3. Installation tasks for new Data Protection for VMware customer

Step	Task	Get started here
1	Check operating 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	Installing selected features on a Linux system with InstallAnywhere mode	Each installation package presents you with a user licensing file (EULA). If you do not accept the file, the installation ends.
5	Configure Data Protection for VMware	Use the configuration wizard for an initial configuration. Depending on the features that are installed, more configuration tasks might be required as described in Chapter 4, “Configuring Data Protection for VMware,” on page 57.

Linux

Windows

Existing Data Protection for VMware customer installation roadmap

Table 4. Installation tasks for existing Data Protection for VMware customer

Step	Task	Get started here
1	Check operating 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	Upgrade 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, such as Tivoli Storage FlashCopy Manager for VMware or Tivoli Storage Manager backup-archive client.
5	Configure Data Protection for VMware	Depending on the components that are installed, more configuration tasks might be required as described in Chapter 4, "Configuring Data Protection for VMware," on page 57.

Required installation permissions

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

Table 5. Users permissions required to install and configure Data Protection for VMware

System	Required permission
Windows	Administrator
Linux	Root
vCenter Server	Administrator privileges
Tivoli Storage Manager server (This server must be available and running.)	Administrative access (System or Unrestricted Policy Domain privilege)

To view more information related to permissions and Data Protection for VMware operations, see this web page:

<http://www.ibm.com/support/docview.wss?uid=swg21497028>.

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.

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

TCP Port	Initiator: Out-Bound (From Host)	Target: In-Bound (To Host)
443	vStorage Backup Server	vCenter Server (secure HTTP)
443	Data Protection for VMware vSphere GUI Server	vCenter Server
902	vCenter Server	ESXi hosts
443		
902	vStorage Backup Server (proxy)	ESXi hosts (all protected hosts)
443		
1500 (tcpport)	vStorage Backup Server (proxy)	Tivoli Storage Manager Server
1500 (tcpadminport)	Data Protection for VMware vSphere GUI Server <ul style="list-style-type: none">1500 (tcpadminport) is non-SSL communicationFor 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
1501 1581 (httpport)	Tivoli Storage Manager server	vStorage Backup Server <ul style="list-style-type: none">backup-archive client schedulerWeb clientClient Acceptor Daemon
1581 (httpport) 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)

Table 6. 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)
9081	vSphere Client	Data Protection for VMware vSphere GUI Server (secure HTTPS port for access to vCenter through web browser)
22	Linux Data Protection for VMware Recovery Agent	Data Protection for VMware Windows "mount" host <ul style="list-style-type: none"> • SSH for Linux Data Protection for VMware Recovery Agent
3260	Linux Data Protection for VMware file-level recovery	Data Protection for VMware Windows "mount" host <ul style="list-style-type: none"> • iSCSI
3260	Windows target with Dynamic disk for file-level recovery	Data Protection for VMware Windows "mount" host <ul style="list-style-type: none"> • iSCSI

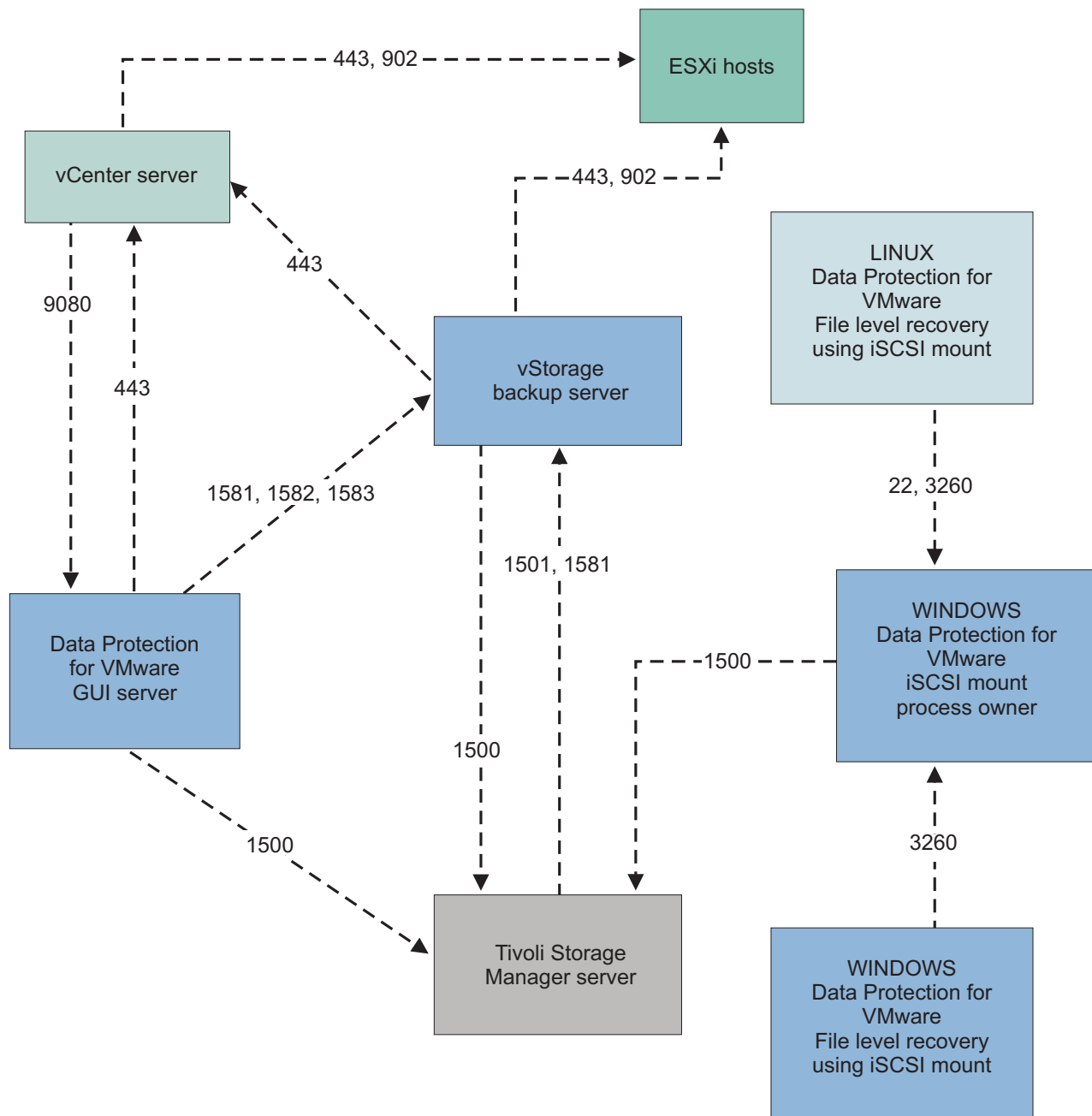


Figure 3. Communication ports diagram.. Communication ports that are accessed by Data Protection for VMware.

Hardware requirements

To implement Data Protection for VMware components, your system must meet appropriate 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 Data Protection for VMware 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 7. 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 Data Protection for VMware Recovery Agent on Linux. This Windows proxy host must have the Data Protection for VMware Recovery Agent installed.

Restriction: 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, you can skip processing the VMDK by specifying the **vmskipmaxvmdks yes** in the Tivoli Storage Manager backup-archive client options file or during the **dsmc** invocation.

Environment requirements

Ensure that the environment meets these requirements before you install Tivoli Storage Manager for Virtual Environments.

Microsoft Windows 32-bit environment requirements

The following environment is required to install Tivoli Storage Manager for Virtual Environments on a Microsoft Windows 32-bit system:

- 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.
- The Oracle Java™ Runtime Environment (JRE) is not part of the setup.exe file, and it is located under the Extra directory. To install the JRE, you must have the product DVD. If you did not install the JRE, you must run the setup.exe from the DVD so that the JRE can be copied to C:\Program Files\Tivoli\TSM\TDPVMware directory. The JRE is installed if you install the Data Protection for VMware Recovery Agent.

The following directories are the default installation locations for these Tivoli Storage Manager for Virtual Environments features:

- Data Protection for VMware Recovery Agent:
C:\Program Files (x86)\Tivoli\TSM\TDPVMware\mount

- Data Protection for VMware Recovery Agent CLI:
C:\Program Files (x86)\Tivoli\TSM\TDPVMware\shell
- Data Protection for VMware vSphere GUI:
C:\IBM\tivoli\tsm\tdpvmware\webserver\
- Data Protection for VMware vCloud GUI:
C:\IBM\tivoli\tsm\tdpvmware\webserver\
- Tivoli Storage Manager backup-archive client:
C:\Program Files (x86)\Tivoli\TSM\baclient\

Microsoft Windows 64-bit environment requirements

The following environment is required to install Tivoli Storage Manager for Virtual Environments on a Microsoft Windows 64-bit system:

- 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.
- The following TCP ports must be open and available:
 - 1527: Internal Derby Database
 - 9080: GUI web server (HTTP protocol)
The Data Protection for VMware vSphere GUI uses this port to access the vCenter as a plug-in extension.
 - 9081: GUI web server (HTTPS protocol)
The Data Protection for VMware vSphere GUI uses this port to access the vCenter through a web browser.
The Data Protection for VMware vCloud GUI uses this port to access the vCloud through a web browser.

The following directories are the default installation locations for these Tivoli Storage Manager for Virtual Environments features:

- Data Protection for VMware Recovery Agent:
C:\Program Files\Tivoli\TSM\TDPVMware\mount
- Data Protection for VMware Recovery Agent CLI:
C:\Program Files\Tivoli\TSM\TDPVMware\shell
- Data Protection for VMware vSphere GUI:
C:\IBM\tivoli\tsm\tdpvmware\webserver\
- Data Protection for VMware vCloud GUI:
C:\IBM\tivoli\tsm\tdpvmware\webserver\
- Tivoli Storage Manager backup-archive client:
C:\Program Files\Tivoli\TSM\baclient\

Linux 64-bit environment requirements

The following environment is required to install Tivoli Storage Manager for Virtual Environments on a Linux 64-bit system:

- Make sure 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.
- The following TCP ports must be open and available:
 - 22: SSH default port for Data Protection for VMware Recovery Agent
 - 3260: iSCSI default port for Data Protection for VMware Recovery Agent
 - 1527: Internal Derby Database
 - 9080: GUI web server (HTTP protocol)
The Data Protection for VMware vSphere GUI uses this port to access the vCenter as a plug-in.
 - 9081: GUI web server (HTTPS protocol)
The Data Protection for VMware vSphere GUI uses this port to access the vCenter through a web browser.
The Data Protection for VMware vCloud GUI uses this port to access the vCloud through a web browser.

The following directories are the default installation locations for these Tivoli Storage Manager for Virtual Environments features:

- Data Protection for VMware Recovery Agent:
/opt/tivoli/tsm/tdpvmware/mount
- Data Protection for VMware Recovery Agent CLI:
/opt/tivoli/tsm/tdpvmware/shell
- Data Protection for VMware vSphere GUI:
/opt/tivoli/tsm/tdpvmware/common/webserver/
- Data Protection for VMware vCloud GUI:
/opt/tivoli/tsm/tdpvmware/common/webserver/
- Tivoli Storage Manager backup-archive client:
/opt/tivoli/tsm/client/ba/bin

Supported operating systems

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

Important: Details of the software and operating system requirements can change over time. For current software requirements, see the *TSM for Virtual Environments - All Requirements Doc* website at <http://www.ibm.com/support/docview.wss?uid=swg21505139>

Supported operating systems for the Recovery Agent command-line interface

Ensure that you are installing the Recovery Agent CLI on a supported operating system.

You can use the following operating systems if your system is 32-bit:

- **Windows** 32-bit Microsoft Windows 2008, Service Pack 1 or later, Standard, Enterprise, Datacenter, Web, Storage, Small Business, and Essential Business editions
- **Windows** 32-bit Microsoft Windows 7, Enterprise, Home Premium, Professional, and Ultimate editions
- **Windows** 32-bit Microsoft Windows 8, Professional and Enterprise editions.

You can use the following operating systems if your system is 64-bit:

- **Windows** 64-bit Microsoft Windows 2008, Service Pack 1 or later, Standard, Enterprise, Datacenter, Web, Storage, Small Business, and Essential Business editions
- **Windows** 64-bit Microsoft Windows 2008, R2, Standard, Enterprise, Datacenter, Web, Storage, Small Business, and Essential Business editions
- **Windows** 64-bit Microsoft Windows 7, Enterprise, Home Premium, Professional, and Ultimate editions
- **Windows** 64-bit Microsoft Windows 8, Professional and Enterprise editions.
- **Windows** 64-bit Microsoft Windows 2012 Server

When issuing commands using the Data Protection for VMware Recovery Agent command-line interface, users can be logged in locally or logged in on a remote machine. The Data Protection for VMware Recovery Agent can be used when it is accessed through a remote desktop when connecting in console mode, by using the administrator switch.

Supported operating systems for Data Protection for VMware Recovery Agent GUI

Ensure that you are installing the Data Protection for VMware Recovery Agent GUI on a supported operating system.

You can use the following operating systems if your system is 32-bit:

- **Windows** 32-bit Microsoft Windows 2008, Service Pack 1 or later, Standard, Enterprise, Web, Storage, Small Business, and Essential Business editions
- **Windows** 32-bit Microsoft Windows 7, all editions
- **Windows** 32-bit Microsoft Windows 8, Professional and Enterprise editions.

You can use the following operating systems if your system is 64-bit:

- **Windows** 64-bit Microsoft Windows 2008, Service Pack 1 or later, Standard, Enterprise, Web, Storage, Small Business, and Essential Business editions
- **Windows** 64-bit Microsoft Windows 2008, R2, Standard, Enterprise, Web, Storage, Small Business, and Essential Business editions
- **Windows** 64-bit Microsoft Windows 7, all editions
- **Windows** 64-bit Microsoft Windows 8, Professional and Enterprise editions.
- **Windows** 64-bit Microsoft Windows 2012 Server
- **Linux** 64-bit Red Hat Enterprise Linux 5 servers, Desktop and Advanced Platform Server
- **Linux** 64-bit Red Hat Enterprise Linux 6, Desktop and Advanced Platform Server
- **Linux** 64-bit SUSE Linux Enterprise Server 11, Desktop, Server

Linux To use the Data Protection for VMware Recovery Agent on Linux, you must install and configure SSH Server on the Windows system where the Data Protection for VMware Recovery Agent command-line interface is installed. For

instructions about how to install and configure SSH Server with Cygwin, see “Configuring Cygwin for use when restoring files from a Linux machine” on page 71.

Data Protection for VMware Recovery Agent uses an internal Tivoli Storage Manager protocol to connect to the server. Port 1500 is the default port that Tivoli Storage Manager uses for Data Protection for VMware Recovery Agent to work. You can customize the port.

Users must be logged in locally in order to run operations from the Data Protection for VMware Recovery Agent GUI.

Note: Windows Support is not provided for applications that use SCSI Pass Through Interface (SPTI) or SCSI Pass Through Direct (SPTD) for performing read and write operations. You cannot use instant restore while applications that use SPTI or SPTD are running. If you try to use instant restore while applications that use SPTI or SPTD are running, it might appear that the instant restore was completed, but the data might be corrupted.

Supported operating systems for Data Protection for VMware vSphere GUI

Ensure that you are installing Data Protection for VMware vSphere GUI on a supported operating system.

You can use the following operating systems if your system is 64-bit:

- Windows 64-bit Microsoft Windows 2008 SP 1, Standard, Enterprise, Datacenter, Web, Storage, Storage R2, Small Business, and Essential Business editions
- Windows 64-bit Microsoft Windows 2008 R2, Standard, Enterprise, Datacenter, Web, Storage, Storage R2, Small Business, and Essential Business editions
- Windows 64-bit Microsoft Windows 7, Enterprise, Professional, Ultimate
- Windows 64-bit Microsoft Windows 8, Professional, Enterprise
- Windows 64-bit Microsoft Windows 2012 Server
- Linux 64-bit Red Hat Enterprise Linux 5 Update2, Desktop and Advanced Platform Server
- Linux 64-bit Red Hat Enterprise Linux 6, Desktop and Advanced Platform Server
- Linux 64-bit SUSE Linux Enterprise Server 11, Desktop, Server

Linux Windows The following versions of VMware vSphere are supported:

- vSphere 5.0
- vSphere 5.1
- vSphere 5.5

The following web browsers are supported:

- Linux Windows Mozilla Firefox 10 Extended Service Release or later
- Linux Windows Google Chrome 12 or later
- Windows Microsoft Internet Explorer 9 and 10

Supported operating systems for Data Protection for VMware vCloud GUI

Ensure that you are installing Data Protection for VMware vCloud GUI on a supported operating system.

You can use the following operating systems if your system is 64-bit:

- **Windows** 64-bit Microsoft Windows 2008 SP 1, Standard, Enterprise, Datacenter, Web, Storage, Storage R2, Small Business, and Essential Business editions
- **Windows** 64-bit Microsoft Windows 2008 R2, Standard, Enterprise, Datacenter, Web, Storage, Storage R2, Small Business, and Essential Business editions
- **Windows** 64-bit Microsoft Windows 7, Enterprise, Professional, Ultimate
- **Windows** 64-bit Microsoft Windows 8
- **Windows** 64-bit Microsoft Windows 2012 Server
- **Linux** 64-bit Red Hat Enterprise Linux 5 Update2, Desktop and Advanced Platform Server
- **Linux** 64-bit Red Hat Enterprise Linux 6, Desktop and Advanced Platform Server
- **Linux** 64-bit SUSE Linux Enterprise Server 11, Desktop, Server

The following web browsers are supported:

- **Linux** **Windows** Mozilla Firefox 10 Extended Service Release or later
- **Linux** **Windows** Google Chrome 12 or later
- **Windows** Microsoft Internet Explorer 9 and 10

Supported operating systems for the data mover

Ensure that you are installing the Tivoli Storage Manager backup-archive client on a supported operating system.

Data Protection for VMware offloads the backup workload from VMs to a vStorage Backup Server. To accomplish this task, the Tivoli Storage Manager 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.

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.

Linux **Windows** The Tivoli Storage Manager backup-archive client is a separately licensed product that contains its own user interfaces and documentation. Familiarity with this product and its documentation is necessary in order to adequately implement a comprehensive plan for protecting your VMs.

Linux **Windows** Tivoli Storage Manager backup-archive client documentation is available in the <http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1>.

Although the Tivoli Storage Manager backup-archive client supports a wide variety of operating systems, only a subset of those operating systems is supported by Data Protection for VMware. The following operating systems are supported for the Tivoli Storage Manager backup-archive client data mover with Data Protection for VMware.

You can use the following operating systems if your system is 64-bit:

- **Windows** 64-bit Microsoft Windows 2008, Standard, Enterprise, Datacenter, Web, Storage, Storage R2, Small Business, and Essential Business editions
- **Windows** 64-bit Microsoft Windows 2008, R2, Standard, Enterprise, Datacenter, Web, Storage, Storage R2, Small Business, and Essential Business editions
- **Windows** 64-bit Microsoft Windows 2012 Server
- **Linux** 64-bit Red Hat Enterprise Linux 5.9 Desktop and Advanced Platform Server
- **Linux** 64-bit Red Hat Enterprise Linux 6.2 and 6.3, Desktop and Advanced Platform Server
- **Linux** 64-bit SUSE Linux Enterprise Server 11.1 and 11.2, Desktop and Server

Important: VM backup and restore operations are not supported on data movers that run on Microsoft Windows 32-bit systems.

Chapter 2. Installing Data Protection for VMware

Before installing or upgrading Data Protection for VMware, verify that your system meets all operating system, hardware, and software requirements.

For the system requirements, see “Supported operating systems” on page 14 for complete details about supported versions.

Important: Each installation package presents you with an user licensing file (EULA). If you do not accept the file, the installation ends.

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

Table 8. Available Data Protection for VMware features by operating system

Component	Linux	Windows
Data Protection for VMware Recovery Agent Provides virtual mount and instant restore capabilities.	√	√
Recovery Agent command-line interface Command-line interface used for mount operations.		√ TDPVMwareShell.exe
Documents Installs the quick start guide, readme file, and notices file.	√	√
Data Protection for VMware Enablement File Enables Tivoli Storage Manager to run the following backup types: <ul style="list-style-type: none">• Periodic incremental VM backup• Full VM incremental-forever backup• Incremental-forever-incremental VM backup It is also required for application protection. If you offload backup workloads, this file must be installed on the vStorage Backup Server.	√	√
Data Protection for VMware vSphere GUI Provides a web-based GUI that is accessible as a plug-in with the VMware vSphere client or directly through a web browser. Use this GUI to back up, restore, and manage VMs in the vCenter. Includes the Data Protection for VMware command-line interface.	√	√ ¹
Data Protection for VMware vCloud GUI Provides a web-based GUI that protects and manages vApps and organization vDCs in a vCloud Director environment. Includes the Data Protection for VMware command-line interface.	√	√ ¹
Data mover The Tivoli Storage Manager backup-archive client installed on the vStorage Backup server.	√	√ ¹

Note: Windows 1. Not available for 32-bit operating systems.

See “Supported operating systems” on page 14 for complete details about supported versions.

Data Protection for VMware offloads the backup workload from VMs to a vStorage Backup Server. To accomplish this task, the Tivoli Storage Manager backup-archive client V7.1 must be installed on the vStorage Backup Server. For prerequisite information, see “Supported operating systems for the data mover” on page 17.

Installing all features on Microsoft Windows 64-bit (Typical Installation)

Install all Tivoli Storage Manager for Virtual Environments and data mover features on a single Windows 64-bit system from the product DVD, or other installation media.

This procedure installs all the features from the following two applications:

Table 9. Available features on Microsoft Windows 64-bit

Tivoli Storage Manager for Virtual Environments features	Tivoli Storage Manager backup-archive client features
-Data Protection for VMware Recovery Agent -Recovery Agent Command-Line Interface -Documentation -Data Protection for VMware Enablement File -Data Protection for VMware vSphere or vCloud GUI	-Backup-Archive Client GUI Files -Backup-Archive Client Web Files -Client API (64-bit) Runtime Files -Administrative Client Command Line Files -VMware vStorage API runtime files

To install Tivoli Storage Manager for Virtual Environments on a Microsoft Windows 64-bit system, complete the following tasks:

1. Either insert the Tivoli Storage Manager for Virtual Environments product DVD into the DVD drive or download the image from IBM Passport Advantage®.
2. To start the installation program, double-click the DVD\x64\setup.exe file. Choose the language for the installation process, then click **Next**.
3. On the Installation Type page, click **Typical Installation**.
The program begins installing the Tivoli Storage Manager backup-archive client data mover and Tivoli Storage Manager for Virtual Environments. This process might take several minutes to complete. When the Welcome to the InstallShield Wizard page displays, click **Next**.
4. On the Software License Agreement page, read the terms of the license agreement. Click **I accept the terms in the license agreement**. If you do not accept the terms of the license agreement, the installation ends. Click **Next**.
5. On the Environment Protection page, select one of the following protection types:
 - To protect data in a vSphere environment, click **vSphere Protection**.
This option 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. It includes the Data Protection for VMware command-line interface. You can install only one

Data Protection for VMware vSphere GUI on a system. As a result, multiple Data Protection for VMware vSphere GUIs are not allowed on the same system.

- To protect data in a vCloud Director environment, click **vCloud Protection**. This option 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 virtual data centers (vDCs). It includes the Data Protection for VMware command-line interface.

After installation completes, the environment protection type cannot be changed except by reinstalling the product. Click **Next** to continue.

6. (vSphere Protection only) On the vSphere Protection GUI Information page, select one or both of the following GUI access methods:
 - To access the GUI as a plug-in extension on the Solutions and Applications panel of your vCenter Server System, click **Register GUI as vCenter Plug-in**.
This plug-in access method is the same method as provided in prior versions of Tivoli Storage Manager for Virtual Environments.
 - To access the GUI in a web browser, click **Enable access to the GUI by a web browser**.

The Data Protection for VMware vSphere GUI is accessed through a URL bookmark to the GUI web server. This access method is new in version 7.1.

After you select the GUI access method, click **Next**.

7. Register the GUI to the appropriate server:
 - If you clicked **vCloud Protection** on the Environment Protection page, specify the vCloud Server IP address or name. Then, click **Next** and proceed to Step 8.
 - If you clicked **vSphere Protection** on the Environment Protection page, complete the following tasks:
 - a. Enter the vCenter Server IP address or name.
 - b. Enter the vCenter user ID. This user ID must be a VMware administrator that has permission to register and unregister extensions.
 - c. Enter the vCenter password.
 - d. Set the communication ports:

To accept the default port values for the internal Derby Database (1527) and GUI web server (HTTP protocol 9080, HTTPS protocol 9081), click **Next** and proceed to Step 8.

To modify the port values, click **Advanced**, and complete the following tasks:

- 1) Enter the TCP/IP port number for the Derby Database, and click **Next**.
- 2) Enter the port for the GUI web server HTTP protocol.
- 3) Enter the port for the GUI web server HTTPS protocol.
- 4) Enter the keystore password for the GUI web server. The password must be a minimum of six valid characters (a-z A-Z 0-9).
- 5) The installation process generates a self-signed SSL certificate. Enter the number of years to keep this SSL certificate active. The default value is 10.

After you set the communication ports, click **Next**.

8. Click **Install** to begin installing Tivoli Storage Manager for Virtual Environments on your system.

Tip: The installation process might take several minutes to complete.

Important: When the Data Protection for VMware Recovery Agent is selected for installation, you are prompted to install the IBM Virtual Volume driver. This driver is required for mount operations. Click **Yes** to install the driver. If you do not install the driver now, you are prompted again to install it when you attempt to mount a volume.

9. After the installation completes, restart your system.
10. After your system restarts, log on and complete the following task for your environment:
 - (vSphere Protection) If you clicked **Enable access to the GUI by a web browser** in Step 6, the Data Protection for VMware vSphere GUI opens in a web browser with the following URL:

`https://<hostname where GUI is installed>:<HTTPS port>/TsmVMwareUI`

Log on to this GUI with the vCenter user ID and password.

If you did not select **Enable access to the GUI by a web browser** in Step 6, start the VMware vSphere Client and log on with the vCenter user ID and password. In the Solutions and Applications panel of the vSphere Client, click the Data Protection for VMware vSphere GUI icon to start the GUI.

- (vCloud Protection) The Data Protection for VMware vCloud GUI opens in a web browser with the following URL:

`https://<hostname where GUI is installed>:<HTTPS port>/TsmVMwareUI`

Log on to this GUI with the vCloud Director user ID and password.

Installing selected features on Microsoft Windows 32-bit or 64-bit (Advanced Installation)

Install only the Tivoli Storage Manager for Virtual Environments and data mover features that you select on a Windows 32-bit or 64-bit system from the product DVD, or other installation media.

During the installation, you select which features to install from the following two applications:

Table 10. Available features on Microsoft Windows 64-bit

Tivoli Storage Manager for Virtual Environments features	Tivoli Storage Manager backup-archive client features
-Data Protection for VMware Recovery Agent -Recovery Agent Command-Line Interface -Documentation -Data Protection for VMware Enablement File -Data Protection for VMware vSphere or vCloud GUI	-Backup-Archive Client GUI Files -Backup-Archive Client Web Files -Client API (64-bit) Runtime Files -Administrative Client Command Line Files -VMware vStorage API runtime files

Table 11. Available features on Microsoft Windows 32-bit

Tivoli Storage Manager for Virtual Environments features (32-bit)
-Data Protection for VMware Recovery Agent -Recovery Agent Command-Line Interface -Documentation -Data Protection for VMware Enablement File

To install Tivoli Storage Manager for Virtual Environments on a Microsoft Windows 32-bit or 64-bit system, complete the following tasks:

1. (32-bit and 64-bit) Either insert the Tivoli Storage Manager for Virtual Environments product DVD into the DVD drive or download the image from IBM Passport Advantage.
2. (32-bit and 64-bit) To start the installation program, double-click the file for your operating system:
 - (32-bit) DVD\x86\setup.exe
 - (64-bit) DVD\x64\setup.exe
 - a. Choose the language for the installation process, then click **Next**.
 - b. On the Welcome page, verify that the requirements are met, then click **Next**.
3. (32-bit and 64-bit) On the Installation Type page, click **Advanced Installation**.

Note:

- (32-bit) The **Typical Installation** type is not available for 32-bit systems.
 - (64-bit) If you want to install all available features, click **Back**, then click **Typical Installation**. Follow the instructions that are provided in “Installing all features on Microsoft Windows 64-bit (Typical Installation)” on page 20.
4. (32-bit and 64-bit) On the Advanced Installation page, complete the following task for your operating system:
 - (32-bit) Click **Install Data Protection for VMware Recovery Agent only** and proceed to Step 8.
 - (64-bit) Click one of the following installation types:

Customized Installation

Select this type if you know which features you want to install. By default, all features are selected.

Install Data Protection for VMware vSphere or vCloud GUI only

Select this type to install the Data Protection for VMware vSphere or vCloud GUI with no other features (such as the data mover).

Since a Data Mover is required for backup and restore operations, it must be installed separately if this type is selected.

Install Data Protection for VMware Instant Restore only

Select this type to install features that run instant restores of full VMs (Recovery Agent CLI), restore files from a VM (Recovery Agent GUI), or restore SQL databases from a VM.

Install the Data Mover only

Select this type to install the Data Mover on this system. If the Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI is also installed on this system, use the GUI configuration wizard to create a data mover node and associated services.

Install Data Protection for VMware Recovery Agent only

Select this type to install the Data Protection for VMware Recovery Agent feature that mounts a database for an in-guest file-level restore from a VM.

5. (64-bit) On the Environment Protection page, select one of the following protection types:

- To protect data in a vSphere environment, click **vSphere Protection**.

This option 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. It includes the Data Protection for VMware command-line interface. You can install only one Data Protection for VMware vSphere GUI on a system. As a result, multiple Data Protection for VMware vSphere GUIs are not allowed on the same system.

- To protect data in a vCloud Director environment, click **vCloud Protection**.

This option 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 virtual data centers (vDCs). It includes the Data Protection for VMware command-line interface.

After installation completes, the environment protection type cannot be changed except by reinstalling the product. Click **Next** to continue.

6. (64-bit) vSphere Protection only: On the vSphere Protection GUI Information page, select one or both of the following GUI access methods:

- To access the GUI as a plug-in extension on the Solutions and Applications panel of your vCenter Server System, click **Register GUI as vCenter Plug-in**.

This plug-in access method is the same method as provided in prior versions of Tivoli Storage Manager for Virtual Environments.

- To access the GUI in a web browser, click **Enable access to the GUI by a web browser**.

The Data Protection for VMware vSphere GUI is accessed through a URL bookmark to the GUI web server. This access method is new in version 7.1.

After you select the access method, click **Next**.

7. (64-bit) Register the GUI to the appropriate server:

- If you clicked **vCloud Protection** on the Environment Protection page, specify the vCloud Server address or name. Then, click **Next** and proceed to Step 8.
- If you clicked **vSphere Protection** on the Environment Protection page, complete the following tasks:
 - a. Enter the vCenter Server IP address or name.
 - b. Enter the vCenter user ID. This user ID must be a VMware administrator that has permission to register and unregister extensions.
 - c. Enter the vCenter password.
 - d. Set the communication ports:

To accept the default port values for the internal Derby Database (1527) and GUI web server (HTTP protocol 9080, HTTPS protocol 9081), click **Next** and proceed to Step 8.

To modify the port values, click **Advanced**, and complete the following tasks:

- 1) Enter the TCP/IP port number for the Derby Database, and click **Next**.
- 2) Enter the port for the GUI web server HTTP protocol.
- 3) Enter the port for the GUI web server HTTPS protocol.
- 4) Enter the keystore password for the GUI web server. The password must be a minimum of six valid characters (a-z A-Z 0-9).
- 5) The installation process generates a self-signed SSL certificate. Enter the number of years to keep this SSL certificate active. The default value is 10.

After you set the communication ports, click **Next**.

8. (32-bit and 64-bit) Click **Install** to begin installing the selected features on your system.

Tip: The installation process might take several minutes to complete.

Important: (32-bit) When the Data Protection for VMware Recovery Agent is selected for installation, you are prompted to install the IBM Virtual Volume driver. This driver is required for mount operations. Click **Yes** to install the driver. If you do not install the driver now, you are prompted again to install it when you attempt to mount a volume.

9. (32-bit and 64-bit) After the installation completes, click **Finish**.

Important: (32-bit and 64-bit) When the Data Protection for VMware Recovery Agent is installed, you must restart your system. After your system restarts, log on to the system and the Data Protection for VMware Recovery Agent is ready for use. The 32-bit installation process is complete.

10. (64-bit) If you installed the Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI, complete one of the following tasks:
 - (vSphere Protection) If you clicked **Enable access to the GUI by a web browser** in Step 6, the Data Protection for VMware vSphere GUI opens in a web browser with the following URL:
`https://<hostname where GUI is installed>:<HTTPS port>/TsmVMwareUI`

 Log on to this GUI with the vCenter user ID and password.
 If you did not select **Enable access to the GUI by a web browser** in Step 6, start the VMware vSphere Client and log on with the vCenter user ID and password. In the Solutions and Applications panel of the vSphere Client, click the Data Protection for VMware vSphere GUI icon to start the GUI.
 - (vCloud Protection) The Data Protection for VMware vCloud GUI opens in a web browser with the following URL:
`https://<hostname where GUI is installed>:<HTTPS port>/TsmVMwareUI`

Log on to this GUI with the vCloud Director user ID and password.

Installing selected features on Linux with InstallAnywhere mode

Install only the Tivoli Storage Manager for Virtual Environments and data mover features that you select on a Linux system from the product DVD, or other installation media.

To install Tivoli Storage Manager for Virtual Environments on a Linux 64-bit system by using the InstallAnywhere mode, complete the following tasks:

1. Either insert the Tivoli Storage Manager for Virtual Environments product DVD into the DVD drive or download the image from IBM Passport Advantage.

2. Change to the directory where the packages are stored on the DVD:

```
cd /CD/Linux/DataProtectionForVMware
```

- a. Start the installation program by issuing the following command:

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

- b. Select the language for the installation process, then click **OK**.
- c. On the Welcome page, review the information, then click **Next**.
- d. Read the license terms on the Software License Agreement page. 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.

Note: The IBM Autonomic Deployment Engine begins installing. This utility is a common technology that is shared by IBM products to manage the lifecycles and relationships of their components that are installed on the machine.

- e. On the Select Installation Directory page, specify where to install Tivoli Storage Manager for Virtual Environments. You can accept the default location that is shown in the **Installation location** field, enter a different location, or click **Choose** to find another location.
 - f. After you enter an installation location, click **Next**.
3. On the Environment Protection page, select one of the following environment protection types:

- To protect data in a vSphere environment, click **vSphere Protection**.

This option 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. It includes the Data Protection for VMware command-line interface. You can install only one Data Protection for VMware vSphere GUI on a system. As a result, multiple Data Protection for VMware vSphere GUIs are not allowed on the same system.

- To protect data in a vCloud Director environment, click **vCloud Protection**.

This option 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 virtual data centers (vDCs). It includes the Data Protection for VMware command-line interface.

After installation completes, the environment protection type cannot be changed except by reinstalling the product. Click **Next** to continue.

4. On the Install Set page, select which Tivoli Storage Manager for Virtual Environments features to install:

- Use the **Custom** install set to specify only those features you want to install.

- Select **Complete** in the **Install Set** list to install all of the features.

After you complete your selection, click **Next**.

5. (vCloud Protection only) On the vCloud Configuration page, specify the vCloud Server IP address or name. Then, click **Next** and proceed to Step 8.
6. (vSphere Protection only) On the vSphere Protection GUI Information page, select one or both of the following GUI access methods:
 - To access the GUI as a plug-in extension on the Solutions and Applications panel of your vCenter Server System, click **Register GUI as vCenter Plug-in**.
This plug-in access method is the same method as provided in prior versions of Tivoli Storage Manager for Virtual Environments.
 - To access the GUI in a web browser, click **Enable access to the GUI by a web browser**.
The Data Protection for VMware vSphere GUI is accessed through a URL bookmark to the GUI web server. This access method is new in version 7.1.

After you select the GUI access method, click **Next**.

7. (vSphere Protection only) On the vSphere Protection GUI Information page, complete the following tasks:
 - a. Enter the vCenter Server IP address or name.
 - b. Enter the vCenter user ID. This user ID must be a VMware administrator that has permission to register and unregister extensions.
 - c. Enter the vCenter password and click **Next**.
8. On the Installation Mode page, set the Tivoli Storage Manager for Virtual Environments user name and communication ports:
 - To accept the default user name (tdpvmware), internal Derby Database port (1527), and GUI web server ports (HTTP protocol 9080, HTTPS protocol 9081), click **Next** and proceed to Step 9.
 - To modify the user name and port values, click **Custom**, then click **Next**. Complete the following tasks:
 - a. Enter a user name. A profile for this user name is created in /home/<username>/tdpvmware/config.
 - b. Enter the TCP/IP port number for the Derby Database, then click **Next**.
 - c. Enter the port for the GUI web server HTTP protocol.
 - d. Enter the port for the GUI web server HTTPS protocol.
 - e. Enter the keystore password for the GUI web server. The password must be a minimum of six valid characters (a-z A-Z 0-9).
 - f. The installation process generates a self-signed SSL certificate. Enter the number of years to keep this SSL certificate active. The default value is 10.

After entering the custom information, click **Next**.

9. On the Preinstallation Summary page, review the list of settings you provided as shown in the page.
 - If your install settings are not correct, click **Previous** to change your settings.
 - If your install settings are correct, click **Install** to begin installing the files.
10. On the Installation Complete page, review the information. Click **Next**, then click **Done** to exit the Tivoli Storage Manager for Virtual Environments installation program.

The following steps install the Tivoli Storage Manager backup-archive client data mover packages:

11. Change to the directory where the Tivoli Storage Manager backup-archive client data mover packages are on the DVD:

```
cd /dvd/Linux/DataMover/baccli
```

- If the Tivoli Storage Manager API is not already installed on the system, proceed to Step 12.
- If the Tivoli Storage Manager API is already installed on the system, proceed to Step 14.

12. Install the 64-bit GSKit packages. In this example, the "8.x.x.x" characters represent the GSKIT version on the DVD:

```
rpm -U gskcrypt64-8.x.x.x.linux.x86_64.rpm gskssl64-8.x.x.x.linux.x86_64.rpm
```

13. Install the 64-bit Tivoli Storage Manager API.

- a. Required: Install the Tivoli Storage Manager API:

```
rpm -ivh TIVsm-API64-7.1.0-73.x86_64.rpm
```

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

```
rpm -ivh TIVsm-APIcit-7.1.0-73.x86_64.rpm
```

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

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

15. Optional: The following packages are available for installation:

- a. Install the Common Inventory Technology package the client uses to send PVU metrics to the server. This package is dependent on the client package so it must be installed after the client package is installed.

```
rpm -ivh TIVsm-BACit.x86_64.rpm
```

- b. The default language that is installed with the backup-archive client is American English. Use the general syntax that is shown in this step to install more languages. Substitute the language identifier that is shown in the following table for the *language_ID* variable in the sample command:

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

If you receive any warnings or errors, check the log files for more information. See "Log file locations on Linux systems" on page 46.

If you are unable to install Tivoli Storage Manager for Virtual Environments successfully, see the "Manually removing Data Protection for VMware" procedure in "Uninstalling Data Protection for VMware a Linux system" on page 44.

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.

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

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 by issuing the following command:
`userdel -r tdpvmware groupdel tdpvmware`

After you complete these steps, start the clean installation.

Installing language packs

Language packs can be installed after Data Protection for VMware is installed. The language packs are available on the product DVD.

Installing a language pack on Windows

You can install a Windows language pack after Data Protection for VMware has been installed. You can install one or more languages from the single package.

Data Protection for VMware supports installation of components on non-English versions of Windows, as well as non-ASCII objects (for example, host names, volume names, user names, passwords, and policies).

To install a language pack on a supported Windows operating system, complete the following steps:

1. Either download the code package or insert the Data Protection for VMware product DVD into the DVD drive.
2. From the Windows Start menu, select **Run** and enter the following command (where X represents the DVD drive letter or installation folder):

```
X:\LanguagePacks\Windows\setup.exe
```

Click **OK**

3. Follow the installation instructions contained in the prompt windows.
4. Click **Finish**.

Installing a language pack on Linux

You can install a Linux language pack after Data Protection for VMware is installed.










To install a language pack on a supported Linux operating system, complete the following steps:

1. Either download the code package or insert the Data Protection for VMware product DVD into the DVD drive.
2. Open a command prompt window and navigate to the /media directory. For example, type the `cd /media` command where /media represents the DVD mount point.
3. Run the installation process. For example, type the `./cdrom/TDPMware/LanguagePacks/Linux/installLP-Linux.bin` command. A Welcome page is displayed.
4. Follow the installation instructions contained in the windows.
5. Click **Finish**.

Installing Data Protection for VMware in silent mode

You can install Data Protection for VMware in the background. During this silent installation, no messages are displayed. After a silent installation completes, you must restart the system.

You can use the silent installation method for the following Data Protection for VMware components:

-   Data Protection for VMware Recovery Agent
-   Data Protection for VMware documents
-   Data Protection for VMware vSphere GUI
-   Data Protection for VMware vCloud GUI
-  Command line

- **Windows** Enablement file

Use the procedure for your operating system:

- “Installing selected Data Protection for VMware features on a Windows 32-bit system in silent mode” on page 33
- “Installing selected Data Protection for VMware features on a Windows 64-bit system in silent mode” on page 35
- “Installing selected Data Protection for VMware features on a Linux system in silent mode” on page 39

The Data Protection for VMware virtual volume kernel driver is not installed during the installation process. The virtual volume kernel driver is installed when Data Protection for VMware Recovery Agent is started for the first time.

Installing all features on a Windows 32-bit system in silent mode with Suite installer

Install the Data Protection for VMware Recovery Agent GUI and the Recovery Agent command-line interface silently on a Windows 32-bit operating system.

Restriction: All features are installed to their default location. You cannot silently install Data Protection for VMware features to a non-default location. See “Microsoft Windows 32-bit environment requirements” on page 12 for a list of default installation directories for each feature.

1. Either insert the Tivoli Storage Manager for Virtual Environments product DVD into the DVD drive or download the image from IBM Passport Advantage.
2. From a command prompt window, use the **cd** command to change 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>\.
3. Enter the following command:

```
setup.exe /silent
```

4. Restart the system after installation completes.

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 Data Protection for VMware Recovery Agent operations.

Related tasks:

“Uninstalling Data Protection for VMware for a Windows 32-bit system in silent mode” on page 43

Installing all features on a Windows 64-bit system in silent mode with Suite installer

Install all Tivoli Storage Manager for Virtual Environments and data mover features silently on a single Windows 64-bit system from the product DVD, or other installation media.

Restriction: All features are installed to their default location. You cannot silently install Tivoli Storage Manager for Virtual Environments and data mover features to a non-default location. See “Microsoft Windows 64-bit environment requirements” on page 13 for a list of default installation directories for each feature.

1. Either insert the Tivoli Storage Manager for Virtual Environments product DVD into the DVD drive or download the image from IBM Passport Advantage.
2. From a command prompt window, use the **cd** command to change 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>\.
3. Enter one of the following commands:

- To protect data in a vSphere environment, enter the following command:

```
setup.exe /silent GUI_MODE=vcenter VCENTER_HOSTNAME=<host_name>  
VCENTER_USERNAME=<user> VCENTER_PASSWORD=<pwd>
```

GUI_MODE

Specify vcenter to install the Data Protection for VMware vSphere GUI.

VCENTER_HOSTNAME

Specify the vCenter Server IP address or name.

VCENTER_USERNAME

Specify the vCenter user ID. This user ID must be a VMware administrator that has permission to register and unregister extensions.

VCENTER_PASSWORD

Specify the vCenter password.

- To protect data in a vCloud Director environment, enter the following command:

```
setup.exe /silent GUI_MODE=vcloud VCLOUD_HOSTNAME=<host_name>  
VCLOUD_USERNAME=<user> VCLOUD_PASSWORD=<pwd>
```

GUI_MODE

Specify vcloud to install the Data Protection for VMware vCloud GUI.

VCLOUD_HOSTNAME

Specify the vCloud Server address or name.

VCLOUD_USERNAME

Specify the vCloud user ID.

VCLOUD_PASSWORD

Specify the vCloud password.

4. Restart the system after installation completes.

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 Data Protection for VMware Recovery Agent operations.

Related tasks:

“Uninstalling Data Protection for VMware for Windows 64-bit system in silent mode” on page 43

Installing selected Data Protection for VMware features on a Windows 32-bit system in silent mode

You can silently install the Data Protection for VMware Recovery Agent GUI and the Recovery Agent command-line interface on a Windows 32-bit operating system.

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

Table 12. Data Protection for VMware silent installation features

Feature	Description	Installed by default?
Mount	Data Protection for VMware Recovery Agent Provides virtual mount and instant restore capabilities.	Yes
Shell	Recovery Agent command-line interface Command-line interface that is used for mount operations. (TDPVMwareShell.exe)	Yes
LAP	Data Protection for VMware License	Yes
TSMLicence	Data Protection for VMware Enablement File Enables Tivoli Storage Manager to run the following backup types: <ul style="list-style-type: none">• Periodic incremental VM backup• Full VM incremental-forever backup• Incremental-forever-incremental VM backup If you offload backup workloads, this file must be installed on the vStorage Backup Server.	Yes
Documents	Readme file, quick start guide	Yes

To install 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. In the folder for Data Protection for VMware, go to the X86 folder.
3. Open the setup.iss file in a text editor:
 - For a default installation, complete these tasks:

- a. In the SERVER_IP= string, specify the host name or IP address of the Microsoft Windows system where the Data Protection for VMware Recovery Agent is to be installed.
- b. Save and close the setup.iss file.
- c. From a command prompt window, enter the following command:

```
setup.exe /s /f1"<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 Microsoft Windows system where the Data Protection for VMware Recovery Agent is to be installed.
 - b. Specify only those features you want to install.
 - c. Save and close the setup.iss file.
 - d. From a command prompt window, enter the following command:

```
setup.exe /s /f1"<absolute_path_to_the_setup.iss_file>"
```

4. Restart the system.

Note: If you installed the Mount feature, 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 Data Protection for VMware Recovery Agent operations.

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

```
setup.exe /r /f1"<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:

```
setup.exe /s /f1"<absolute_path_to_the_setup.iss_file>"
```

- e. Restart the system.

Installing selected Data Protection for VMware features on a Windows 64-bit system in silent mode

You can customize which Data Protection for VMware features to silently install on a Windows 64-bit operating system.

Data Protection for VMware provides the following silent installation features for Windows 64-bit operating systems:

Table 13. Data Protection for VMware silent installation features

Feature	Description	Installed by default?
mount	Data Protection for VMware Recovery Agent Provides virtual mount and instant restore capabilities.	Yes
shell	Recovery Agent command-line interface Command-line interface that is used for mount operations. (TDPVMwareShell.exe)	Yes
LAP	Data Protection for VMware License	Yes
TSMLicence	Data Protection for VMware Enablement File Enables Tivoli Storage Manager to run the following backup types: <ul style="list-style-type: none">• Periodic incremental VM backup• Full VM incremental-forever backup• Incremental-forever-incremental VM backup If you offload backup workloads, this file must be installed on the vStorage Backup Server.	Yes
documents	Readme file, quick start guide	Yes
gui	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 14. Data Protection for VMware silent installation parameters

Parameter	Description	Default value
GUI_MODE	<p>To protect data in a vSphere environment, specify GUI_MODE=vcenter. 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.</p> <p>To protect data in a vCloud environment, specify GUI_MODE=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.</p>	vcenter
VCENTER_HOSTNAME	The vCenter Server IP address or name. 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
VCLLOUD_HOSTNAME	The vCloud Server address or name. This feature is required when GUI_MODE=vcloud is specified.	None
VCLLOUD_USERNAME	The vCloud user ID. This feature is required when GUI_MODE=vcloud is specified.	None
VCLLOUD_PASSWORD	The vCloud password. This feature is required when GUI_MODE=vcloud is specified.	None
DIRECT_START	<p>(vSphere only) To access the Data Protection for VMware vSphere GUI in a web browser, specify DIRECT_START=1. The Data Protection for VMware vSphere GUI is accessed through a URL bookmark to the GUI web server. This access method is new in version 7.1. If you do not want to access the Data Protection for VMware vSphere GUI in a web browser, specify DIRECT_START=0.</p>	<p>1</p> <p>Important: After installation completes, the DIRECT_START value cannot be changed except by reinstalling the product.</p>

Table 14. Data Protection for VMware silent installation parameters (continued)

Parameter	Description	Default value
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 . 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
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
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

Use the following Tivoli Storage Manager backup-archive client data mover parameters with the silent installation features:

Table 15. Tivoli Storage Manager backup-archive client 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

To silently install Data Protection for VMware, follow these steps:

1. Either download the code package or insert the Data Protection for VMware product DVD into the DVD drive.
2. In the folder for Data Protection for VMware, go to the X64 folder.
3. From a command prompt window, use the **cd** command to change the directory to the installation folder.
4. For a default installation, enter the following command:

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

5. For a custom installation, complete the following tasks:

- a. Specify the features to install with the **ADDLOCAL** property. For example, all features are installed with the following value:

```
ADDLOCAL=mount,shell,LAP,TSMLicence,documents,gui
```

You must specify all features on a single line within quotation marks, which are separated by commas, with no spaces before or after the commas.

- b. Specify the feature parameters as described in Table 14 on page 36. The following example installs all features to protect VMs in a vSphere environment:

```
setup.exe /s /v"/qn ADDLOCAL=mount,shell,LAP,documents,TSMLicence,gui  
GUI_MODE=vcenter REGISTER_PLUGIN=1 DIRECT_START=1  
VCENTER_HOSTNAME=9.123.45.678 VCENTER_USERNAME=admin  
VCENTER_PASSWORD=adminpsd DB_PORT=1527 WC_DEFAULTHOST=9080  
WEBSERVER_SECUREPORT=9081 KEYSTORE_PASSWORD=keypass  
SSL_CERTIFICATE=10"
```

Note: If you installed the Mount feature, 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 Data Protection for VMware Recovery Agent operations.

The following example installs all features to protect vApps and organization vDCs in a vCloud Director environment:

```
setup.exe /s /v"/qn ADDLOCAL=mount,shell,LAP,documents,TSMLicence,gui  
GUI_MODE=vcloud VCLLOUD_HOSTNAME=9.123.45.678 VCLLOUD_USERNAME=Administrator  
VCLLOUD_PASSWORD=pass4vclld DB_PORT=1527 WC_DEFAULTHOST=9080  
WEBSERVER_SECUREPORT=9081 KEYSTORE_PASSWORD=keypass  
SSL_CERTIFICATE=10"
```

The following example installs all Tivoli Storage Manager backup-archive client data mover features:

```
setup.exe /s /a /s /v"/qn  
ADDLOCAL=BackupArchiveGUI,BackupArchiveWeb,Api64Runtime,AdministrativeCmd\  
/L1033
```

The /L feature installs the language pack for the preferred language.

Note: The example is shown on separate lines to accommodate page formatting.

6. Restart the system.

Installing selected Data Protection for VMware features on a Linux system in silent mode

You can customize which Data Protection for VMware features to silently install on a Linux operating system.

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

Table 16. Data Protection for VMware silent installation features

Feature	Description	Installed by default?
Docs	Readme file, quick start guide	Yes
TDPVMwareMount	Data Protection for VMware Recovery Agent Provides virtual mount and instant restore capabilities.	Yes
TDPVMwareEnableFile	Data Protection for VMware Enablement File Enables Tivoli Storage Manager to run the following backup types: <ul style="list-style-type: none">• Periodic incremental VM backup• Full VM incremental-forever backup• Incremental-forever-incremental VM backup 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 17. Data Protection for VMware silent installation parameters for the *installer.properties* file

Parameter	Description	Default value
PRODUCT_PROTECT_TYPE	<p>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.</p> <p>To protect data in a vCloud environment, specify PRODUCT_PROTECT_TYPE=VCLLOUD. 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.</p>	VSPHERE
VCENTER_HOSTNAME	The vCenter Server IP address or name. 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
VCLLOUD_HOSTNAME	The vCloud Server address or name. This parameter is required when PRODUCT_PROTECT_TYPE=VCLLOUD is specified.	None
VCLLOUD_USERNAME	The vCloud user ID. This parameter is required when PRODUCT_PROTECT_TYPE=VCLLOUD is specified.	None
VCLLOUD_PASSWORD	The vCloud password. This parameter is required when PRODUCT_PROTECT_TYPE=VCLLOUD is specified.	None

Table 17. 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. This access method is new in version 7.1. If you do not want to access the Data Protection for VMware vSphere GUI in a web browser, specify DIRECT_START=NO .	YES Important: After 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 . 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
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

To silently install 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. Uncomment this entry in the *installer.properties* file to accept the license:

```
#LICENSE_ACCEPTED=TRUE
```

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

```
LICENSE_ACCEPTED=TRUE
```

3. For a default installation, open the Linux folder (which is in the Data Protection for VMware folder) and issue the following command:

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

4. For a custom installation, complete the following tasks:
 - a. Edit the `installer.properties` file with the appropriate values:
 - 1) Specify **INSTALL_MODE=Custom**. Make sure 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,TDPVMwareMount,TDPVMwareEnableFile,TDPVMwareGUI
```
 - 3) Specify the `installer.properties` parameters as described in Table 17 on page 40.
 - b. Open the Linux folder (in the Data Protection for VMware folder) and issue the following command:

```
./install-Linux.bin -i silent -f <full_path_to_properties_file_name>
```

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.

Restriction: You must unmount all virtual volumes before uninstalling Data Protection for VMware Recovery Agent. Otherwise, these mounted virtual volumes cannot be unmounted after Data Protection for VMware Recovery Agent is reinstalled.

1. Start the uninstall process:
 - **Windows** Either run the `setup.exe` file, or select **Add or Remove Programs** from the Windows Control Panel.

This command uninstalls only the Data Protection for VMware features. The Tivoli Storage Manager backup-archive client data mover features must be manually uninstalled as described in the following steps:

 - a. From your Windows Control Panel, go to **Programs and Features**.
 - b. Remove or uninstall the **IBM Tivoli Storage Manager Client** entry.
 - **Linux** Run this command:

```
<installation path>/_uninst/TDPVMware/Uninstall_Tivoli_Data_Protection_for_VMware
```

2. A screen opens. Select **Modify, Repair, or Remove**
3. Select **Remove**. Data Protection for VMware is completely uninstalled.

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

4. **Windows** For a Windows uninstallation of Data Protection for VMware Recovery Agent, you are asked to reboot the computer, in order to complete the uninstallation of Data Protection for VMware Recovery Agent drivers. You can choose to reboot later.

Uninstalling Data Protection for VMware with the Microsoft Windows Installer Tool

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

1. 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}]
```

2. Run the following command:

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

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.

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

1. 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>\`.

2. Enter one of the following commands:

- To uninstall Data Protection for VMware with an `uninstall.iss` file, enter the following command:

```
setup.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:

```
setup.exe /silent /remove
```

3. 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.

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

1. 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>\.
- 2. 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:


```
setup.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:


```
setup.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:


```
setup.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
VCLLOUD_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:


```
setup.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
IGNORE_VCLLOUD_UNREGISTER=1"
```
 - To uninstall all features with Suite installer, enter the following command:


```
setup.exe /silent /remove
```
- 3. 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.

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 described in “Manually removing Data Protection for VMware from a Linux system” on page 45.

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

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

When Data Protection for VMware cannot be uninstalled 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.

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>
```
4. Back up the global registry file (`/var/.com.zerog.registry.xml`). After the file is backed up, remove all tags related to Data Protection for VMware.
5. Remove all files located in the installation directory (`/opt/tivoli/tsm/tdpvmware`). Also remove any shortcuts located on the desktop.
6. Back up the log files located 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 issued if the installation process fails again.
7. Attempt to install the product again as described in “Installing selected features on Linux with InstallAnywhere mode” on page 26.

Data Protection for VMware log files

Data Protection for VMware creates and modifies several log files during installation, backup, mount, and restore operations.

Data Protection for VMware log files are plain text files that use an .sf file extension. For example, the Data Protection for VMware 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.

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 trying the installation again.

Log file locations on Windows operating systems

Logs are placed in the following directories on these Windows operating systems:

%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware

The directories contain a subdirectory for each Data Protection for VMware component. For example, the Data Protection for VMware Recovery Agent subdirectory is \mount, and the Recovery Agent command-line interface subdirectory is \shell.

The Data Protection for VMware command-line interface places log files in this directory:

C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\logs

The Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI places log files in this directory:

C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\logs

When you are collecting log files, make sure to include all subdirectories in your compressed file.

You can search for log files from the Windows Start menu, by selecting **Control Panel > Search** and entering *.log.

Log file locations on Linux systems

Logs are placed in the following paths on Linux systems:

<user.home>/tivoli/tsm/ve/mount/log

/opt/tivoli/tsm/TDPVMware/mount/engine/var

The Data Protection for VMware command-line interface places log files in this path:

/opt/tivoli/tsm/tdpvmware/common/logs

The Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI places log files in this path:

/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

You can search for log files by entering this command:

```
find /opt/tivoli/ -name "*.log"
```

Chapter 3. 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 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. Data Protection for VMware Version 7.1 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.

Table 18. Available Data Protection for VMware upgrade tasks

If your system has the following applications installed:	Then follow this upgrade procedure:
<div>Linux Windows</div> Data Protection for VMware Version 6.x	"Upgrading Data Protection for VMware from Version 6.x"
<div>Linux</div> Tivoli Storage FlashCopy Manager for VMware Version 3.x	"Upgrading Data Protection for VMware from Tivoli Storage FlashCopy Manager for VMware Version 3.x" on page 51
<div>Linux</div> Data Protection for VMware Version 6.x and Tivoli Storage FlashCopy Manager for VMware Version 3.x	"Upgrading Data Protection for VMware from Tivoli Storage FlashCopy Manager for VMware Version 3.x and Data Protection for VMware Version 6.x" on page 52

For compatibility with earlier versions, see the *Compatibility Information: Data Protection for VMware Version 7.1* website at <http://www.ibm.com/support/docview.wss?uid=swg21648031>

Upgrading Data Protection for VMware from Version 6.x

This procedure documents how to upgrade to Data Protection for VMware V 7.1 from V6.x.

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:

- Data Protection for VMware V7.1 installs WebSphere Application Server V8.5. As a result, the previous eWAS folder and daemon are removed during an upgrade. However, the tsmserver.props configuration file remains for the new profile.

- 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 V6.x was installed to a non-default location, the upgrade process installs Tivoli Storage Manager for Virtual Environments V7.1 features to the default installation directory. You cannot upgrade to a non-default location. See “Microsoft Windows 64-bit environment requirements” on page 13 for a list of default installation directories for each feature.
- **Windows** (64-bit) The upgrade process accesses the vCenter server with the existing V6.x port value (HTTP protocol) and the default V7.1 HTTPS protocol value (9081). These port values cannot be modified during the upgrade process.
- **Linux** **Windows** The upgrade process does not install new components. For example, if your previous version has only the Data Protection for VMware Recovery Agent GUI installed, the upgrade procedure does not install the Data Protection for VMware 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 Data Protection for VMware Recovery Agent on Linux version must be the same version as the Data Protection for VMware Recovery Agent on the Windows proxy. Therefore, if you upgrade Data Protection for VMware Recovery Agent on Linux, you must also upgrade the Data Protection for VMware Recovery Agent version on the Windows proxy.

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

1. Verify that there are no active backup, restore, or mount sessions.
2. Verify that any existing Data Protection for VMware vSphere GUI or Data Protection for VMware Recovery Agent GUI is closed.
3. If the system you are upgrading to has both the Data Protection for VMware vSphere GUI V6.x and Tivoli Storage Manager backup-archive client V6.x installed, complete the following tasks:
 - a. Uninstall Tivoli Storage Manager backup-archive client V6.x. Detailed backup-archive client uninstall instructions are described in the Tivoli Storage Manager information center at:
<http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1>
 - b. Install Tivoli Storage Manager backup-archive client V7.1. Detailed backup-archive client install instructions are described in the following procedures:
“Installing all features on Microsoft Windows 64-bit (Typical Installation)” on page 20
“Installing selected features on Linux with InstallAnywhere mode” on page 26
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 setup.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 Version 3.x

This procedure documents how to upgrade to Data Protection for VMware V7.1 when Tivoli Storage FlashCopy Manager for VMware V3.x is also installed.

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

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

- Data Protection for VMware V7.1 installs WebSphere Application Server V8.5. As a result, the previous eWAS folder and daemon are removed during an upgrade. However, the `tsmsrvr.prop` and `vmcliConfiguration.xml` configuration files remain for the new profile.
- 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.

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 listed in Table 8 on page 19.
 - 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 7.1 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 as described in the *IBM Tivoli Storage FlashCopy Manager for VMware Version 4.1: Installation and User's Guide*.
- If you are using Tivoli Storage Manager backup-archive client V6.x or earlier, you must upgrade to V7.1 as described in the *IBM Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide Version 7.1*.
- Data Protection for VMware offloads the backup workload from VMs to a vStorage Backup Server. To accomplish this task, the Tivoli Storage Manager 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 Tivoli Storage Manager backup-archive client V7.1 level as described in "Upgrading the data mover nodes on the vStorage Backup Server" on page 55.
- When Data Protection for VMware V7.1 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 "Data Protection for VMware log files" on page 46 for the location of various log files.

Upgrading Data Protection for VMware from Tivoli Storage FlashCopy Manager for VMware Version 3.x and Data Protection for VMware Version 6.x

This procedure documents how to upgrade to Data Protection for VMware V7.1 from Data Protection for VMware V6.x when Tivoli Storage FlashCopy Manager for VMware V3.x is also installed.

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:

- Data Protection for VMware V7.1 installs WebSphere Application Server V8.5. As a result, the previous eWAS folder and daemon are removed during an upgrade. However, the `tmsserver.prop` and `vmcliConfiguration.xml` configuration files remain for the new profile.

- 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 Data Protection for VMware Recovery Agent GUI installed, the upgrade procedure does not install the Data Protection for VMware 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 Data Protection for VMware Recovery Agent on Linux version must be the same version as the Data Protection for VMware Recovery Agent on the Windows proxy. Therefore, if you upgrade Data Protection for VMware Recovery Agent on Linux, you must also upgrade the Data Protection for VMware Recovery Agent version on the Windows proxy.

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 Tivoli Storage Manager backup-archive client V6.x installed, complete the following tasks:
 - a. Uninstall Tivoli Storage Manager backup-archive client V6.x.
 - b. Install Tivoli Storage Manager backup-archive client V7.1.

Detailed backup-archive client uninstall and install instructions are described in the Tivoli Storage Manager information center at:
<http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1>
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 listed in Table 8 on page 19.
 - 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 7.1 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 as described in the *IBM Tivoli Storage FlashCopy Manager for VMware Version 4.1: Installation and User's Guide*.
- If you are using Tivoli Storage Manager backup-archive client V7.1 or earlier, you must upgrade to V7.1 as described in the *IBM Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide Version 7.1*.
- Data Protection for VMware offloads the backup workload from VMs to a vStorage Backup Server. To accomplish this task, the Tivoli Storage Manager 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 Tivoli Storage Manager backup-archive client V7.1 level as described in "Upgrading the data mover nodes on the vStorage Backup Server" on page 55.
- When Data Protection for VMware V7.1 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 "Data Protection for VMware log files" on page 46 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

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 Data Protection for VMware Recovery Agent GUI is closed.
3. Either download the code package or insert the Data Protection for VMware DVD into the DVD drive.
4. In the Data Protection for VMware folder, go to the X86 folder.
5. In a text editor, open the upgrade.iss file.
6. 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.
7. From a command prompt window, enter the following command:
`setup.exe /s /f1"<path_to_the_upgrade.iss_file>"`
8. 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.

When Tivoli Storage Manager for Virtual Environments V6.x was installed to a non-default location, the silent upgrade process installs Tivoli Storage Manager for Virtual Environments V7.1 features to the default installation directory. You cannot silently upgrade to a non-default location. See “Microsoft Windows 64-bit environment requirements” on page 13 for a list of default installation directories for each feature.

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 Data Protection for VMware 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. In the folder for Data Protection for VMware, either go to the X64 folder.
5. From a command prompt window, enter the following command:
`setup.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.

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 Data Protection for VMware 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 folder for Data Protection for VMware go to the Linux folder.
5. From a command prompt window, enter the following command:
`./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true`

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 Version 6.4, you must upgrade all data mover nodes to the 7.1 level.

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 Tivoli Storage Manager 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. Detailed backup-archive client uninstall and install instructions are described in the Tivoli Storage Manager information center at:
<http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1>

1. If the system you are upgrading to has the Data Protection for VMware vSphere GUI Version 6.x installed, uninstall Tivoli Storage Manager backup-archive client Version 6.x.
2. Upgrade each vStorage Backup Server in your Data Protection for VMware environment with Tivoli Storage Manager backup-archive client Version 7.1.
3. 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**.
4. Upgrade each vStorage Backup Server in your Data Protection for VMware environment with Data Protection for VMware Version 7.1:
 - a. Detailed instructions are provided in Chapter 3, “Upgrading Data Protection for VMware,” on page 49.
 - b. When upgrading the vStorage Backup Server, the only Data Protection for VMware component required for the Tivoli Storage Manager 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.

Chapter 4. Configuring Data Protection for VMware

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

Table 19. Required configuration tasks. Required configuration tasks

To accomplish this objective:	Complete this configuration task:
Bac kup VM data, vApps, or organization VDCs Restore VM data, vApps, or data stores	"Creating an initial configuration with the wizard"
<ul style="list-style-type: none">• Off-host file-level restore• In-guest file-level restore• Instant restore	<ol style="list-style-type: none">1. "Creating an initial configuration with the wizard" ¹2. "Configuring the Data Protection for VMware Recovery Agent GUI" on page 67
Off-host iSCSI target restore	<ol style="list-style-type: none">1. "Creating an initial configuration with the wizard" ¹2. "Configuring the Data Protection for VMware Recovery Agent GUI" on page 673. "Configuring systems for iSCSI mount" on page 644. "Configuring Cygwin for use when restoring files from a Linux machine" on page 71

1. This task is required only when the Tivoli Storage Manager nodes and their proxy relationships are not set up.

Creating an initial configuration with the wizard

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

Fast path:

To access the wizard in the Data Protection for VMware vSphere GUI, start the GUI with either of these methods:

- Click the Data Protection for VMware vSphere GUI icon in the Solutions and Applications window of the vSphere Client.
- Open a supported web browser and go to the GUI web server. For example:
<https://finapps.mycompany.com:9081/TsmVMwareUI/>

Login by using the vCenter user name and password.

To access the wizard in the Data Protection for VMware vCloud GUI, open a supported web browser and go to the GUI web server. For example:

<https://finapps.mycompany.com:9081/TsmVMwareUI/>

Login by using the vCloud user name and password. This user name must be the name of a vCloud system administrator. In the Getting Started window, go to the Configuration window and click **Run Configuration Wizard**.

(vSphere environment) Before you proceed with this configuration task, make sure that the following conditions exist:

- **Windows** On the system where the vSphere Web Client is installed, the C:\ProgramData\VMware\vsphere Web Client\webclient.properties file must contain these flags at the bottom of the file:
allowHttp = true
scriptPlugin.enabled = true

These flags enable the Data Protection for VMware vSphere GUI to be visible in the vSphere Web Client.

- **Linux** **Windows** 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
- **Windows** For vSphere Client 5.0 and 5.1, the Data Protection for VMware vSphere GUI host URL address must be set in your Internet Explorer trusted sites zone. In the Internet Explorer menu bar, go to **Tools > Internet Options > Security > Trusted sites**. Click **Sites** and add the host URL address. Make sure to apply your changes. For example:

Add this website to the zone:http://myvctrmachine.xyzco.com

- **Windows** For vSphere Web Client 5.1, when you are using Internet Explorer on Windows Server 2008 or Windows 2012 Server, Enhanced Security Configuration (IE ESC) must be disabled. Go to the Server Manager and make sure that IE ESC is set to Off.
- **Windows** On Windows Server 2008, if you start the Data Protection for VMware vSphere GUI and then add the address as a trusted site, a JavaScript error denies continued access to the Data Protection for VMware vSphere GUI. To resolve this issue, close and restart the Data Protection for VMware vSphere GUI.

To configure the Data Protection for VMware environment with the wizard, complete these steps:

Note: After an initial installation of the Data Protection for VMware GUI, the configuration wizard starts automatically.

1. In the Getting Started window, go to the Configuration window and click **Run Configuration Wizard**. Review the welcome information and click **Next** to begin the configuration tasks.
2. 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.

When the wizard completes successfully, the following results occur:

- (vSphere environment) The vCenter node, VMCLI node, datacenter nodes, and data mover nodes are registered on the Tivoli Storage Manager server.
 - (vSphere environment) The Data Protection for VMware vSphere GUI domain is set.
 - (vCloud environment) The vCloud Director node, VMCLI node, Provider VDC nodes, Organization VDC nodes, and data mover nodes are registered on the Tivoli Storage Manager server.
 - When the backup-archive client data mover is installed on the same system and the **Create Services** option was selected, the Client Acceptor Service (CAD), backup-archive Scheduler Service, and Remote Client Agent Service are set up and running.
 - The proxy relationships are set correctly for these nodes.
 - The vmcliprofile is updated and set.
 - The local VMCLI password is set.
3. 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. If the issue is not resolved and the data mover nodes must be set up, complete the tasks that are described in “Setting up the data mover nodes in a vSphere environment” on page 79.

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

Important: Information about how to complete tasks with the 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.

Editing an existing configuration with the notebook

Use the Edit Configuration notebook to edit existing configuration settings.

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 data mover nodes.
- Modify a password for an existing data mover node.

To edit an existing configuration, complete these steps:

1. In the Getting Started window, go to the Configuration window and click **Edit Configuration**. (vCloud environment) You can also click the **Tivoli Storage Manager Server** edit icon in the right column.

2. 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.

The updated settings are displayed in the Configuration window.

Starting and running services for Data Protection for VMware

By default, when you start the Windows operating system, Data Protection for VMware Recovery Agent is started under the Local System Account.

Data Protection for VMware Recovery Agent services on Microsoft Windows

When you start the Data Protection for VMware Recovery Agent from the Windows Start menu, the service is automatically stopped. When the Data Protection for VMware 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 > Data Protection for VMware Recovery Agent**.

Data Protection for VMware command-line interface

You can verify that the Data Protection for VMware command-line interface is running by completing the following task:

Windows Go to **Start > Control Panel > Administrative Tools > Services** and verify that the status of Data Protection for VMware command-line interface is **Started**.

Linux Go to the scripts directory (/opt/tivoli/tsm/tdpvmware/common/scripts/) and issue this command:

```
./vmclid status
```

- If the daemon is not running, issue this command to manually start the daemon:
`/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon`

These init scripts can also be used to stop and start the daemon:

```
./vmclid stop  
./vmclid start
```

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, Data Protection for VMware Recovery Agent mount must be operating in Tape Mode. In this mode, only one VM snapshot volume can be mounted at a time from a Data Protection for VMware 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 Data Protection for VMware Recovery Agent on multiple physical systems or on multiple VM guests. Enable Tape Mode by selecting Storage Type=Tape in the Data Protection for VMware Recovery Agent GUI Settings menu.

- While Data Protection for VMware Recovery Agent mount does not prevent an attempt to mount a snapshot on physical tape, performance can vary significantly and might be severely affected. Data Protection for VMware 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 Data Protection for VMware 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 Data Protection for VMware 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 occurred while reading snapshot data from server. See log for details.

Configuring systems for iSCSI mount

This procedure describes how to configure the systems that are used during an iSCSI mount operation. The snapshot is mounted from Tivoli Storage Manager server storage.

Tip: Linux 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:

- During an iSCSI mount, an iSCSI target is created on the Data Protection for VMware Recovery Agent machine, and then connected to the machine where the data is to be restored. You can connect to the iSCSI target from other machines and mount the volume from other machines.
- iSCSI initiator is required on any machine that must connect to the iSCSI target.
- Make sure that an iSCSI initiator is installed on the Windows or Linux machine where the data is to be restored.
- Microsoft iSCSI Initiator is not required on the Data Protection for VMware Recovery Agent machine.

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.

Complete these tasks to configure the systems that are used during an iSCSI mount operation:

1. Windows On the Data Protection for VMware Recovery Agent machine, open port 3260 in the LAN firewall and the Windows client firewall. Record the iSCSI initiator name on the machine where data is to be restored.

Windows The iSCSI initiator name is shown in the iSCSI initiator configuration window of the Control Panel. For example:

iqn.1991-05.com.microsoft:hostname

Linux The iSCSI initiator name is located in the following text file:

/etc/iscsi/initiatorname.iscsi

If the InitiatorName= value is empty, create a unique initiator name with the following command:

```
twaus1bkpoc01:~ # /sbin/iscsi-iname
```

For example:

iqn.2005-03.org.open-iscsi:3f5058b1d0a0

Edit /etc/iscsi/initiatorname.iscsi and insert the InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0 string. For example:

```
twauslbpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
```

2. Linux Windows Complete these tasks on the system where the Data Protection for VMware Recovery Agent (or iSCSI target) is installed:
 - a. Start the Data Protection for VMware 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.
3. Locate and start the iSCSI Initiator program on the initiator system that was selected in Step 1:
 - a. Windows Connect to the iSCSI target:
On Windows Server 2003:
 - 1) In the Discovery tab, click **Add** in the Target Portals dialog. Enter the TCP/IP address of the Data Protection for VMware Recovery Agent (iSCSI target) used in Step 2. Click **OK**.
 - 2) Verify that the iSCSI target is visible in the Targets tab. Click **Refresh** if it is not visible.
 - 3) Select the target and click **Log On** to connect the iSCSI virtual volume.
On Windows 7 and Windows Server 2008:
 - 1) In the Targets tab, enter the TCP/IP address of the Data Protection for VMware 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. Windows 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.
 - a. Linux 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. **Linux** Connect to the iSCSI target by issuing this command:
- ```
iscsiadm -m discovery -t sendtargets -p <IP/hostname of
Data Protection for VMware Recovery Agent machine> --login
```
- c. **Linux** Verify that a new raw device is available by issuing this command:
- ```
fdisk -l
```
- d. **Linux** Mount the file system:

For a non-LVM volume, issue the following commands:

```
mkdir /mountdir  
mount /dev/sdb1 /mountdir
```

In this example, the new device is /dev/sdb1.

For an LVM volume, complete the following tasks:

- 1) Make sure that the **vgimportclone** script is available on the Linux machine. 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.
 - 2) On the Linux guest, issue the **vgimportclone** command and include a new base volume group name (VolGroupSnap01). For example:

```
vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
```
 - 3) On the Linux guest, issue the **lvchange** command to mark the logical volume as active. For example:

```
lvchange -a y /dev/VolGroupSnap01/LogVol100
```
 - 4) On the Linux guest, issue these commands to mount the volume:

```
mkdir /mountdir  
mount -o ro /dev/VolGroupSnap01/LogVol100 /mountdir
```
 - 5) After the restore operation completes, issue these commands to unmount the file system and log out:

Unmount the file system:

```
umount /mountdir
```

Log out of a single target:

```
iscsiadm --mode node --targetname <target_name> --logout
```

Log out of all targets:

```
iscsiadm --mode node --logout
```
4. **Linux** **Windows** Open Windows Explorer (or other utility) and browse the mounted snapshot for a file-level recovery operation.

Configuring the Data Protection for VMware Recovery Agent GUI

Instructions about how to set up the Data Protection for VMware Recovery Agent GUI for mount, file restore, or instant restore operations is provided.

These configuration tasks must be completed before you attempt an operation in the Data Protection for VMware Recovery Agent GUI.

1. **Linux** Log on to the Linux system with root user authority. Data Protection for VMware Recovery Agent must be installed on this Linux system.
 - a. Start the Data Protection for VMware Recovery Agent by clicking the Data Protection for VMware 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 Data Protection for VMware 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 Data Protection for VMware Recovery Agent on your Linux system.
 - c. Enter the host name or IP address of the Windows system where both the Data Protection for VMware Recovery Agent command-line interface and Secure Shell (SSH) are installed.
2. **Windows** Log on to the system where you want to restore files. Data Protection for VMware Recovery Agent must be installed on the system.
3. Click **Select TSM server** in the Data Protection for VMware Recovery Agent GUI to connect to a Tivoli Storage Manager server. **Windows** When the Data Protection for VMware 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 Tivoli Storage Manager data mover node and Tivoli Storage Manager server are populated in the Data Protection for VMware 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 Data Protection for VMware Recovery Agent uses that node to authenticate when started. The Data Protection for VMware 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 Data Protection for VMware 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 Data Protection for VMware 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 Data Protection for VMware 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 Data Protection for VMware 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.

Data Protection for VMware 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 Data Protection for VMware 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.

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 Data Protection for VMware 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:


```
dsmadm -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.

Configuring Cygwin for use when restoring files from a Linux machine

These configuration tasks must be completed before attempting to restore files using the Data Protection for VMware Recovery Agent on a Linux system.

This procedure describes how to set up Cygwin on a Microsoft Windows 32-bit system in order to restore files using a Data Protection for VMware Recovery Agent command-line interface that is installed on a Linux system. These tasks must be completed before attempting to restore any files. Make sure the following prerequisites exist before proceeding:

- **Linux** The SSH daemon service must be installed on the Linux system.
- **Linux** The GNU C library (Version 2.3.3-98.38 or later) must be installed on the Linux system. Access the library at this website: <http://www.gnu.org/software/libc/download.html>
- **Linux** **Windows** The Data Protection for VMware Recovery Agent must be installed on the Linux system and Windows system used in this procedure.
- 1. **Windows** On the Windows system where the Data Protection for VMware Recovery Agent command-line interface is installed, log on using an account with administrator privileges. Install Cygwin by completing the following tasks:
 - a. Download Cygwin 1.7.9-1 (or later) 32-bit for Windows from this website: <http://www.cygwin.com>

Note: Cygwin 64-bit for Windows is not supported for this procedure.

- b. Select these Cygwin packages during the installation process:

Table 20. Cygwin packages

Category	Package
Net	All default packages. In addition, select the following packages: <ul style="list-style-type: none">• openssh (contains ssh.exe)• openssl (contains ssl.exe)• rsync• tcp_wrappers
Editor	vim-common (contains enhanced vi editor)

- c. After the Cygwin installation wizard completes successfully, set the following two Microsoft Windows environment variables. From the Microsoft Windows Start menu, select **Control Panel > System**. In the System Properties page, click the **Advanced** tab, then click **Environment Variables**. The Environment Variables pane opens for you to update.
 - Add the full path of the Cygwin\bin directory to the Microsoft Windows %PATH% system environment variable. The full path must be the first value specified in the %PATH% system environment variable. This example shows the full path statement if Cygwin is installed on your C:\ drive:
c:\cygwin\bin
 - Add CYGWIN as a Microsoft Windows user environment variable with the value ntsec tty.
 - d. After adding these two environment variables, restart the Windows system so that these variable updates are applied.
2. **Windows** After the Windows system restarts, log on using an account with administrator privileges. The Cygwin Terminal must also be run as an administrator. Install the SSH daemon service following these steps:
- a. Issue the getfacl command to verify that the /etc/passwd and /etc/group files possess read, write, and file owner permissions, and that the /var directory possesses read access permission:
getfacl /etc/passwd
getfacl /etc/group
getfacl /var
- If these files do not possess read, write, and file owner permissions, enter the following chmod command to update the owner permissions:
chmod r+u+w /etc/passwd
chmod r+u+w /etc/group
- If the /var directory does not possess read access permission, enter the following chmod command to update the owner permissions:
chmod 755 /var
- b. From the Cygwin command prompt window, run the following command to create the SSH daemon service:
ssh-host-config
- Tip:** The text in the display prompts might be different in a different version of Cygwin.
- c. When a query about whether privilege separation is displayed in the command prompt window, enter *no*.
- Note:** On Windows Server 2008 R2 SP1, enter *yes* when prompted about privilege separation.
- d. When a query about whether a new local account named *sshd* is displayed in the command prompt window, enter *yes*.
 - e. When a query about whether *sshd* is installed as a service is displayed, enter *yes*.
 - f. When a query asks you to enter the value of **CYGWIN** for the daemon, enter the following text: *ntsec tty*
 - g. When a query asks if you want to use a different name, enter *no*.
 - h. When a query asks if you want to create a new privileged user account named *cyg_server*, enter *yes*.

- i. When a query asks you to enter the new user account password, enter a password. You are asked to reenter the password to confirm the entry. The host configuration is complete. A status message is displayed.
- j. At the prompt, set the CYGWIN variable with the following values:
`set CYGWIN 'ntsec tty'`

This variable configures Cygwin global settings and directs the utility to show content to standard input. You can verify that this setting is correct by issuing the `set |grep CYGWIN` command. The expected command output is:
`CYGWIN=' "ntsec tty" '`

3. **Linux** Log on to the Linux system where the Data Protection for VMware Recovery Agent command-line interface is installed. Configure the authentication key files as described in these steps:

- a. Issue this command and press **Enter** at all prompt questions:
`ssh-keygen -t dsa`
- b. Change to the `.ssh` directory and issue the secure copy command (`scp`) to generate the authentication key:
`scp id_dsa.pub <Windows userid>@windows_machine:/home/<Windows userid>`

Important: You must create authentication key files for each new client system. Therefore, complete Steps 3a through 3b for each client system.

4. **Windows** Log on to the Windows system using the same Windows user ID (`<Windows userid>`) that was specified with the secure copy command in Step 3b. Complete these tasks:

- a. Issue these commands from the Cygwin shell:
`mkdir .ssh`
`chmod 700 .ssh`
`cd .ssh`
`touch authorized_keys`
`cat ../id_dsa.pub >> authorized_keys`
`rm ../id_dsa.pub`

The use of `>>` allows more than one authorized key to be set in the file.

- b. Configure the SSH server to use the authentication files by editing the SSH service configuration file `c:\cygwin\etc\sshd_config`:

Tip: Make sure that this file contains write access permission. Use only the `vi` editor or WordPad to edit this file.

- 1) Open the file and unmark these entries:

```
Protocol 2
HostKey /etc/ssh_host_dsa_key
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile
```

- 2) Update the `AuthorizedKeysFile` value to specify `/home/<Windows userid>/.ssh/authorized_keys`. For example:

```
Protocol 2
HostKey /etc/ssh_host_dsa_key
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile /home/<Windows userid>/.ssh/authorized_keys
```

- c. Edit the `C:\cygwin\etc\hosts.allow` file to allow any host to connect to the Windows system using SSH. Specify `sshd: ALL` to immediately precede the `ALL : PARANOID : deny` line. For example:

```
sshd: ALL
ALL : PARANOID : deny
```

- d. Issue these commands from the Cygwin shell on the Windows system to restart the sshd service:

```
net stop sshd
net start sshd
```

5. **Linux** Log on to the Linux system and complete these tasks:

- a. SSH to the Windows system where Cygwin is installed to verify that it can communicate with the Windows system:

```
ssh <Windows userid>@windows_machine
```

SSH attempts to update the known_hosts file for each host name convention specified. For example, although each of these commands identifies the same Windows system, SSH attempts to add an entry to the known_hosts file for each host name:

```
ssh <Windows userid>@windows_machine
ssh <Windows userid>@windows_machine.xyz.com
```

Tip: To prevent possible timeout errors due to authentication failure, implement one (or both) of these recommendations:

- Consistently use the same host name convention when accessing the Windows system.
- Update the known_hosts file with all host name conventions associated with the Windows system.

The first connection prompts you to confirm that the SSH signature should be accepted. After you confirm the signature, exit from this SSH session.

- b. Issue the SSH command again. When the configuration is correct, you are not prompted to confirm the SSH signature. Instead, you are taken to the command shell in the Windows Cygwin environment.
- c. To confirm the environment on the Windows system:
- 1) Change to the folder where TDPVMwareShell.exe is located.
 - 2) Issue this command from the SSH shell you just started:

```
TDPVMwareShell.exe -h
```

This command displays basic help information. The expected command output is:

```
TDPVMware Shell run mode options:

-----
TDPVMwareShell.exe -c      command line.
TPVMwareShell.exe -h      help command.


set_connection  Setting the connection configuration.
mount          Mount command to TDPVMware Mount.


For more information on a specific command, type
TDPVMwareShell.exe -h command-name.
For example: 'TDPVMwareShell.exe -h mount' will print
detailed help on the mount command line.
```

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://vcloudir.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://vcloud.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 A. Advanced configuration tasks

You must manually configure and verify each component using the available application interfaces.

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
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.”
 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 79.
 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 87.
 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.

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.

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

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 clicking the icon in the Solutions and Applications window of the vSphere Client:

- For an initial configuration, go to **Configuration > Run Configuration Wizard**.
 - For an existing configuration, go to **Configuration > Edit Configuration**.
1. Log on to the Tivoli Storage Manager server and start an administrative client session in command-line mode:
`dsmadm -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

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.

In a standard Data Protection for VMware environment, a separate `dsm.opt` file (Windows) or `dsm.sys` file stanza (Linux) is used for each Tivoli Storage Manager data mover node. When multiple data mover nodes on a vStorage Backup Server are used for 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. It is also recommended to 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.

Important:

- The Tivoli Storage Manager Backup-Archive Client (on the vStorage Backup Server) must have the VMware vStorage API runtime files installed and configured. When installing the client, select setup type **Custom**, then select **VMware vStorage API runtime files**.
- The vStorage Backup Server must have the Data Protection for VMware Enablement File installed. When installing Data Protection for VMware, select the **Data Protection for VMware Enablement File** component. This file enables the Tivoli Storage Manager data mover node to perform the backup VM incremental function.

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 vStorage API error.
TSM function name: vddksdk Write
TSM file : vmvddksdk.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.

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

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 Tivoli Storage Manager data mover node.

NODENAME

Specify the name of a previously defined Tivoli Storage Manager 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. 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 (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 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 or instant restore operations, make sure to complete these additional setup tasks:

- a. 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.
- b. Stop the Data Protection for VMware Recovery Agent service.
- c. Add the following statement to the Data Protection for VMware Recovery Agent TDPVMwareMount.conf file:

```
[IMount config]
Target IP=<iSCSI server IP address of the network card
on the data mover machine that is used for the iSCSI
data transfer during instant operations.>
```

The Target IP address must be the same IP address that is specified by the VMISCSISERVERADDRESS option.

- d. Start the Data Protection for VMware Recovery Agent service.

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 (CAD) 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 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**:
 - **Windows** 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.

- **Windows** Select Help me configure the TSM Client Scheduler. Enter the information as prompted.
 - a. When entering 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** Specify these options in the `dsm.sys` file, in the stanza for the Tivoli Storage Manager 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`

- **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
```
- **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:

```
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
```

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.

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 87.

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.

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 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. It is also recommended to 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 using the Tivoli Storage Manager backup-archive client that is installed on the vStorage backup server.

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

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 backup, restore, or query.

MANAGESERVICES

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 (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 settings is provided here:

```
NODename DM_MYDMNODE
PASSWORDAccess generate
VCDHost vcloud1.example.com
VMCHost vcenter1.example.com
MANAGEServices schedule webclient
TCPServeraddress tmsserver.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 (CAD) 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 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**:
 - 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 entering 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** Specify these 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 /vappsched/dsmsched_dm.log
errorlogname /vappsched/dsmerror_dm.log

- **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

- **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:
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

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.

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

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**.

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 Tivoli Storage Manager 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.

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 77
2. "Setting up the data mover nodes in a vSphere environment" on page 79
3. "Configuring the Data Protection for VMware command-line interface in a vSphere environment" on page 87

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.

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 Tivoli Storage Manager data mover node.

NODENAME
PASSWORDACCESS
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPOINT
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  
TCPPOINT 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 Tivoli Storage Manager 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
```

Appendix B. Migrating to an incremental forever backup strategy

Use this procedure to migrate existing backup schedules, policies, and Tivoli Storage Manager data mover nodes for use in an incremental forever backup strategy.

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.
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 7.1 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 (dsmadm):
 - 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. For more details, see “Example of version control with the verexists parameter” on page 96.

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 (`dsmadm`) 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.

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 Tivoli Storage Manager for Virtual Environments 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.

Tivoli Storage FlashCopy Manager for VMware is used to create hardware snapshots of VMs on VMware datastores. When integrated with Data Protection for VMware, you can offload backups of the VMs to a Tivoli Storage Manager server from the Tivoli Storage FlashCopy Manager for VMware hardware snapshots 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 VMs 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 VMs in the vCenter server. The vStorage backup server can be a physical or VM.

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 VM, in one of the ESX or ESXi hosts in the datacenter, with a guest operating system of RedHat or SUSE Linux. If Tivoli Storage FlashCopy Manager for VMware is installed on a VM, this VM must not be part of any backup process.
- Data Protection for VMware is installed and configured on the same system as Tivoli Storage FlashCopy Manager for VMware.

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 V7.1:
See "Installing selected features on Linux with InstallAnywhere mode" on page 26.
2. Install and configure Tivoli Storage Manager backup-archive client V7.1:
See "Install the Tivoli Storage Manager backup-archive client data mover packages".
3. Configure Tivoli Storage Manager for Virtual Environments V7.1:
See Chapter 4, "Configuring Data Protection for VMware," on page 57.
4. Install Tivoli Storage FlashCopy Manager for VMware V4.1:
See the "Installing and upgrading" chapter in *IBM Tivoli Storage FlashCopy Manager for VMware V4.1: Installation and User's Guide* for detailed instructions.
5. Configure Tivoli Storage FlashCopy Manager for VMware V4.1:
See the "Configuring Tivoli Storage FlashCopy Manager for VMware" chapter in *IBM Tivoli Storage FlashCopy Manager for VMware V4.1: Installation and User's Guide* for detailed instructions.

The following scenarios provide insight into possible integration uses:

- To minimize the impact of the offload backup operation to the production ESX host, specify an auxiliary ESX host for Tivoli Storage FlashCopy Manager for VMware. In this scenario, the hardware snapshots are mounted and attached to the auxiliary ESX host. As a result, the Data Protection for VMware offload backup operation is processed from the auxiliary ESX 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. Tivoli support information

You can find support information for Tivoli and other IBM products from various sources.

From the IBM Support Portal at <http://www.ibm.com/support/entry/portal/>, you can select the products that you are interested in and search for a wide variety of relevant information.

Communities and other learning resources

In addition to product documentation, many forms of assistance are available to help you get started as you deploy and use the Tivoli Storage Manager family of products. These resources can also help you to solve problems that you might have.

You can use forums, wikis, and other social media tools to ask questions, talk to experts, and learn from others.

User groups

Tivoli Global Storage Virtual User Group

Access this user group at <http://www.tivoli-ug.org/storage>.

This group makes it possible for individuals from many different industries and types of organizations to share information and work directly with the IBM product experts. Local chapters also exist where members meet in person to share experiences and hear from guest speakers.

ADSM.ORG

Access this mailing list at <http://adsm.org>.

This independently managed Storage Management discussion forum started when Tivoli Storage Manager was known as ADSTAR Distributed Storage Manager (ADSM). The members of this forum have many years of experience with Tivoli Storage Manager in almost every type of IT environment.

To subscribe to the forum, send an email to listserv@vm.marist.edu. The body of the message must contain the following text: `SUBSCRIBE ADSM-L your_first_name your_family_name`.

Tivoli Storage Manager community on Service Management Connect

Access Service Management Connect at <http://www.ibm.com/developerworks/servicemanagement>. In the Storage Management community of Service Management Connect, you can connect with IBM in the following ways:

- Become involved with transparent development, an ongoing, open engagement between users and IBM developers of Tivoli products. You can access early designs, sprint demonstrations, product roadmaps, and prerelease code.
- Connect one-on-one with the experts to collaborate and network about Tivoli and the Tivoli Storage Manager community.
- Read blogs to benefit from the expertise and experience of others.

- Use wikis and forums to collaborate with the broader user community.

Tivoli Storage Manager wiki on developerWorks®

Access this wiki at <https://www.ibm.com/developerworks/servicemanagement/sm/index.html>.

Find the latest best practices, white papers, and links to videos and other resources. When you log on, you can comment on content, or contribute your own content.

Tivoli Support Technical Exchange

Find information about upcoming Tivoli Support Technical Exchange webcasts at http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html. Replays of previous webcasts are also available.

Learn from technical experts who share their knowledge and then answer your questions. The sessions are designed to address specific technical issues and provide in-depth but narrowly focused training.

Other social media sites

LinkedIn

You can join groups on LinkedIn, a social media site for professionals. For example:

- **Tivoli Storage Manager Professionals:** <http://www.linkedin.com/groups/Tivoli-Storage-Manager-Professionals-54572>
- **TSM:** <http://www.linkedin.com/groups?gid=64540>

Twitter

Follow @IBMStorage on Twitter to see the latest news about storage and storage software from IBM.

Tivoli education resources

Use these education resources to help you increase your Tivoli Storage Manager skills:

Tivoli Education and Certification website

View available education at <http://www.ibm.com/software/tivoli/education>.

Use the Search for Training link to find local and online offerings of instructor-led courses for Tivoli Storage Manager.

Education Assistant

Access resources at <http://publib.boulder.ibm.com/infocenter/ieduasst/tivv1r0/index.jsp>.

Scroll to view the list of available training videos. Recorded product demonstrations are also available on a YouTube channel.

Searching knowledge bases

If a problem occurs while you are using one of the Tivoli Storage Manager family of products, you can search several knowledge bases.

Begin by searching the Tivoli Storage Manager Information Center at <http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1>. Within the information center, you can enter words, phrases, or message numbers in the **Search** field to find relevant topics.

Searching the Internet

If you cannot find an answer to your question in the Tivoli Storage Manager information center, search the Internet for the information that might help you resolve the problem.

To search multiple Internet resources, go to the IBM support website at <http://www.ibm.com/support/entry/portal/>. You can search for information without signing in.

Sign in using your IBM ID and password if you want to customize the site based on your product usage and information needs. If you do not already have an IBM ID and password, click **Sign in** at the top of the page and follow the instructions to register.

From the support website, you can search various resources:

- IBM technotes.
- IBM downloads.
- IBM Redbooks® publications.
- IBM Authorized Program Analysis Reports (APARs). Select the product and click **Downloads** to search the APAR list.

Using IBM Support Assistant

IBM Support Assistant is a complimentary software product that can help you with problem determination. It is available for some Tivoli Storage Manager and Tivoli Storage FlashCopy Manager products.

IBM Support Assistant helps you gather support information when you must open a problem management record (PMR), which you can then use to track the problem. The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

You can find more information and download the IBM Support Assistant web page at <http://www.ibm.com/software/support/isa>.

You can also install the stand-alone IBM Support Assistant application on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products that you use. Find add-ons for specific products at <http://www.ibm.com/support/docview.wss?uid=swg27012689>.

Finding product fixes

A product fix to resolve a software problem might be available from the IBM software support website.

Determine what fixes are available by checking the IBM software support website at <http://www.ibm.com/support/entry/portal/>.

If you previously customized the site based on your product usage:

1. Click the link for the product, or a component for which you want to find a fix.
2. Click **Downloads**, and then click **Search for recommended fixes**.

If you have not previously customized the site:

Click **Downloads** and search for the product.

Receiving notification of product fixes

You can receive notifications about fixes, flashes, upgrades, and other news about IBM products.

1. From the support page at <http://www.ibm.com/support/entry/portal/>, click **Sign in** and sign in using your IBM ID and password. If you do not have an ID and password, click **register now** and complete the registration process.
2. Click **Manage all my subscriptions** in the Notifications pane.
3. Click the **Subscribe** tab, and then click **Tivoli**.
4. Select the products for which you want to receive notifications and click **Continue**.
5. Specify your notification preferences and click **Submit**.

Contacting IBM Software Support

You can contact IBM Software Support if you have an active IBM subscription and support contract, and if you are authorized to submit problems to IBM.

1. Ensure that you have completed the following prerequisites:
 - a. Set up a subscription and support contract.
 - b. Determine the business impact of the problem.
 - c. Describe the problem and gather background information.
2. Follow the instructions in “Submitting the problem to IBM Software Support” on page 103.

Setting up and managing support contracts

You can set up and manage your Tivoli support contracts by enrolling in IBM Passport Advantage. The type of support contract that you need depends on the type of product you have.

Enroll in IBM Passport Advantage in one of the following ways:

- **Online:** Go to the Passport Advantage website at <http://www.ibm.com/software/lotus/passportadvantage/>, click **How to enroll**, and follow the instructions.
- **By telephone:** For critical, system-down, or high-severity issues, you can call 1-800-IBMSERV (1-800-426-7378) in the United States. For the telephone number to call in your country, go to the IBM Software Support Handbook web page at <http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html> and click **Contacts**.

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you must understand and assess the business impact of the problem you are reporting.

Severity level	Description
Severity 1	Critical business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	Significant business impact: The program is usable but is severely limited.
Severity 3	Some business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	Minimal business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describing the problem and gathering background information

When explaining a problem to IBM, it is helpful to be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently.

To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be re-created? If so, what steps led to the failure?
- Have any changes been made to the system? For example, hardware, operating system, networking software, and so on.
- Are you using a workaround for this problem? If so, be prepared to explain it when you report the problem.

Submitting the problem to IBM Software Support

You can submit the problem to IBM Software Support online or by telephone.

Online

Go to the IBM Software Support website at [http://www.ibm.com/support/entry/portal/Open_service_request/Software_Software_support_\(general\)](http://www.ibm.com/support/entry/portal/Open_service_request/Software_Software_support_(general)). Sign in to access IBM Service Requests and enter your information into the problem submission tool.

By telephone

For critical, system-down, or severity 1 issues, you can call 1-800-IBMSERV (1-800-426-7378) in the United States. For the telephone number to call in your country, go to the IBM Software Support Handbook web page at <http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html> and click **Contacts**.

Appendix E. 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 Tivoli Storage Manager Information Center is enabled for accessibility. For information center accessibility information, see “Accessibility features in the information center” (http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1/topic/com.ibm.help.ic.doc/iehs36_accessibility.html).

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
Armonk, NY 10504-1785
U.S.A.*

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
U.S.A.*

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 information 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 is for planning purposes only. The information herein is subject to change before the products described become available.

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

COPYRIGHT LICENSE:

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

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.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 <http://www.ibm.com/legal/copytrade.shtml>.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows 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.

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> 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

This glossary provides terms and definitions for Tivoli Storage Manager, Tivoli Storage FlashCopy Manager, and associated products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website at www.ibm.com/software/globalization/terminology.

A

absolute mode

In storage management, a backup copy-group mode that specifies that a file is considered for incremental backup even if the file has not changed since the last backup. See also mode, modified mode.

access control list (ACL)

In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access mode

An attribute of a storage pool or a storage volume that specifies whether the server can write to or read from the storage pool or storage volume.

ACK See acknowledgment.

acknowledgment (ACK)

The transmission of acknowledgment characters as a positive response to a data transmission.

ACL See access control list.

activate

To validate the contents of a policy set and then make it the active policy set.

active-data pool

A named set of storage pool volumes that contain only active versions of client

backup data. See also server storage, storage pool, storage pool volume.

active file system

A file system to which space management has been added. With space management, tasks for an active file system include automatic migration, reconciliation, selective migration, and recall. See also inactive file system.

active policy set

The activated policy set that contains the policy rules currently in use by all client nodes assigned to the policy domain. See also policy domain, policy set.

active version

The most recent backup copy of a file stored. The active version of a file cannot be deleted until a backup process detects that the user has either replaced the file with a newer version or has deleted the file from the file server or workstation. See also backup version, inactive version.

activity log

A log that records normal activity messages that are generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors.

adaptive subfile backup

A type of backup that sends only changed portions of a file to the server, instead of sending the entire file. Adaptive subfile backup reduces network traffic and increases the speed of the backup.

administrative client

A program that runs on a file server, workstation, or mainframe that administrators use to control and monitor the server. See also backup-archive client.

administrative command schedule

A database record that describes the planned processing of an administrative command during a specific time period. See also central scheduler, client schedule, schedule.

administrative privilege class

See privilege class.

administrative session

A period of time during which an administrator user ID communicates with a server to perform administrative tasks. See also client node session, session.

administrator

A person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

agent node

A client node that has been granted proxy authority to perform operations on behalf of another client node, which is the target node.

aggregate

An object, stored in one or more storage pools, consisting of a group of logical files that are packaged together. See also logical file, physical file.

aggregate data transfer rate

A performance statistic that indicates the average number of bytes that were transferred per second while processing a given operation.

application client

A program that is installed on a system to protect an application. The server provides backup services to an application client.

archive

To copy programs, data, or files to another storage media, usually for long-term storage or security. See also retrieve.

archive copy

A file or group of files that was archived to server storage

archive copy group

A policy object containing attributes that control the generation, destination, and expiration of archived files. See also copy group.

archive-retention grace period

The number of days that the storage manager retains an archived file when the server is unable to rebind the file to an appropriate management class. See also bind.

association

The defined relationship between a client

node and a client schedule. An association identifies the name of a schedule, the name of the policy domain to which the schedule belongs, and the name of a client node that performs scheduled operations.

audit To check for logical inconsistencies between information that the server has and the actual condition of the system. The storage manager can audit information about items such as volumes, libraries, and licenses. For example, when a storage manager audits a volume, the server checks for inconsistencies between information about backed-up or archived files that are stored in the database and the actual data that are associated with each backup version or archive copy in server storage.

authentication rule

A specification that another user can use to either restore or retrieve files from storage.

authority

The right to access objects, resources, or functions. See also privilege class.

authorization rule

A specification that permits another user to either restore or retrieve a user's files from storage.

authorized user

A user who has administrative authority for the client on a workstation. This user changes passwords, performs open registrations, and deletes file spaces.

AutoFS

See automounted file system.

automatic detection

A feature that detects, reports, and updates the serial number of a drive or library in the database when the path from the local server is defined.

automatic migration

The process that is used to automatically move files from a local file system to storage, based on options and settings that are chosen by a root user on a workstation. See also demand migration, threshold migration.

automounted file system (AutoFS)

A file system that is managed by an

automounter daemon. The automounter daemon monitors a specified directory path, and automatically mounts the file system to access data.

B

backup-archive client

A program that runs on a workstation or file server and provides a means for users to back up, archive, restore, and retrieve files. See also administrative client.

backup copy group

A policy object containing attributes that control the generation, destination, and expiration of backup versions of files. A backup copy group belongs to a management class. See also copy group.

backup retention grace period

The number of days the storage manager retains a backup version after the server is unable to rebind the file to an appropriate management class.

backup set

A portable, consolidated group of active versions of backup files that are generated for a backup-archive client.

backup set collection

A group of backup sets that are created at the same time and which have the same backup set name, volume names, description, and device classes. The server identifies each backup set in the collection by its node name, backup set name, and file type.

backup version

A file or directory that a client node backed up to storage. More than one backup version can exist in storage, but only one backup version is the active version. See also active version, copy group, inactive version.

bind To associate a file with a management class name. See also archive-retention grace period, management class, rebind.

C

cache To place a duplicate copy of a file on random access media when the server migrates a file to another storage pool in the hierarchy.

cache file

A snapshot of a logical volume created by Logical Volume Snapshot Agent. Blocks are saved immediately before they are modified during the image backup and their logical extents are saved in the cache files.

CAD See client acceptor daemon.

central scheduler

A function that permits an administrator to schedule client operations and administrative commands. The operations can be scheduled to occur periodically or on a specific date. See also administrative command schedule, client schedule.

client A software program or computer that requests services from a server. See also server.

client acceptor

A service that serves the Java applet for the web client to web browsers. On Windows systems, the client acceptor is installed and run as a service. On AIX®, UNIX, and Linux systems, the client acceptor is run as a daemon.

client acceptor daemon (CAD)

See client acceptor.

client domain

The set of drives, file systems, or volumes that the user selects to back up or archive data, using the backup-archive client.

client node

A file server or workstation on which the backup-archive client program has been installed, and which has been registered to the server.

client node session

A session in which a client node communicates with a server to perform backup, restore, archive, retrieve, migrate, or recall requests. See also administrative session.

client option set

A group of options that are defined on

the server and used on client nodes in conjunction with client options files.

client options file

An editable file that identifies the server and communication method, and provides the configuration for backup, archive, hierarchical storage management, and scheduling.

client-polling scheduling mode

A method of operation in which the client queries the server for work. See also server-prompted scheduling mode.

client schedule

A database record that describes the planned processing of a client operation during a specific time period. The client operation can be a backup, archive, restore, or retrieve operation, a client operating system command, or a macro. See also administrative command schedule, central scheduler, schedule.

client/server

Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

client system-options file

A file, used on AIX, UNIX, or Linux system clients, containing a set of processing options that identify the servers to be contacted for services. This file also specifies communication methods and options for backup, archive, hierarchical storage management, and scheduling. See also client user-options file, options file.

client user-options file

A file that contains the set of processing options that the clients on the system use. The set can include options that determine the server that the client contacts, and options that affect backup operations, archive operations, hierarchical storage management operations, and scheduled operations. This file is also called the dsm.opt file. For AIX, UNIX, or Linux systems, see also client system-options file. See also client system-options file, options file.

closed registration

A registration process in which only an administrator can register workstations as client nodes with the server. See also open registration.

collocation

The process of keeping all data belonging to a single-client file space, a single client node, or a group of client nodes on a minimal number of sequential-access volumes within a storage pool.

Collocation can reduce the number of volumes that must be accessed when a large amount of data must be restored.

collocation group

A user-defined group of client nodes whose data is stored on a minimal number of volumes through the process of collocation.

commit point

A point in time when data is considered to be consistent.

communication method

The method by which a client and server exchange information. See also Transmission Control Protocol/Internet Protocol.

communication protocol

A set of defined interfaces that permit computers to communicate with each other.

compression

A function that removes repetitive characters, spaces, strings of characters, or binary data from the data being processed and replaces characters with control characters. Compression reduces the amount of storage space that is required for data.

configuration manager

A server that distributes configuration information, such as policies and schedules, to managed servers according to their profiles. Configuration information can include policy and schedules. See also enterprise configuration, managed server, profile.

conversation

A connection between two programs over a session that allows them to communicate with each other while processing a transaction. See also session.

copy backup

A full backup in which the transaction log files are not deleted so that backup procedures that use incremental or differential backups are not disrupted.

copy group

A policy object containing attributes that control how backup versions or archive copies are generated, where backup versions or archive copies are initially located, and when backup versions or archive copies expire. A copy group belongs to a management class. See also archive copy group, backup copy group, backup version, management class.

copy storage pool

A named set of volumes that contain copies of files that reside in primary storage pools. Copy storage pools are used only to back up the data that is stored in primary storage pools. A copy storage pool cannot be a destination for a backup copy group, an archive copy group, or a management class (for space-managed files). See also destination, primary storage pool, server storage, storage pool, storage pool volume.

D**daemon**

A program that runs unattended to perform continuous or periodic functions, such as network control.

damaged file

A physical file in which read errors have been detected.

database backup series

One full backup of the database, plus up to 32 incremental backups made since that full backup. Each full backup that is run starts a new database backup series. A number identifies each backup series. See also database snapshot, full backup.

database snapshot

A complete backup of the entire database to media that can be taken off-site. When a database snapshot is created, the current database backup series is not interrupted. A database snapshot cannot have incremental database backups associated with it. See also database backup series, full backup.

data center

In a virtualized environment, a container that holds hosts, clusters, networks, and data stores.

data deduplication

A method of reducing storage needs by eliminating redundant data. Only one instance of the data is retained on storage media. Other instances of the same data are replaced with a pointer to the retained instance.

data manager server

A server that collects metadata information for client inventory and manages transactions for the storage agent over the local area network. The data manager server informs the storage agent with applicable library attributes and the target volume identifier.

data mover

A device that moves data on behalf of the server. A network-attached storage (NAS) file server is a data mover.

data storage-management application-programming interface (DSMAPI)

A set of functions and semantics that can monitor events on files, and manage and maintain the data in a file. In an HSM environment, a DSMAPI uses events to notify data management applications about operations on files, stores arbitrary attribute information with a file, supports managed regions in a file, and uses DSMAPI access rights to control access to a file object.

data store

In a virtualized environment, the location where virtual machine data is stored.

deduplication

The process of creating representative records from a set of records that have been identified as representing the same entities.

default management class

A management class that is assigned to a policy set. This class is used to govern backed up or archived files when a file is not explicitly associated with a specific management class through the include-exclude list.

demand migration

The process that is used to respond to an

out-of-space condition on a file system for which hierarchical storage management (HSM) is active. Files are migrated to server storage until space usage drops to the low threshold that was set for the file system. If the high threshold and low threshold are the same, one file is migrated. See also automatic migration, selective migration, threshold migration.

desktop client

The group of backup-archive clients that includes clients on Microsoft Windows, Apple, and Novell NetWare operating systems.

destination

A copy group or management class attribute that specifies the primary storage pool to which a client file will be backed up, archived, or migrated. See also copy storage pool.

device class

A named set of characteristics that are applied to a group of storage devices. Each device class has a unique name and represents a device type of disk, file, optical disk, or tape.

device configuration file

1. For a storage agent, a file that contains the name and password of the storage agent, and information about the server that is managing the SAN-attached libraries and drives that the storage agent uses.
2. For a server, a file that contains information about defined device classes, and, on some servers, defined libraries and drives. The information is a copy of the device configuration information in the database.

disaster recovery manager (DRM)

A function that assists in preparing and using a disaster recovery plan file for the server.

disaster recovery plan

A file that is created by the disaster recover manager (DRM) that contains information about how to recover computer systems if a disaster occurs and scripts that can be run to perform some recovery tasks. The file includes information about the software and

hardware that is used by the server, and the location of recovery media.

domain

A grouping of client nodes with one or more policy sets, which manage data or storage resources for the client nodes. See also policy domain.

DRM See disaster recovery manager.

DSMAPI

See data storage-management application-programming interface.

dynamic serialization

Copy serialization in which a file or folder is backed up or archived on the first attempt regardless of whether it changes during a backup or archive. See also shared dynamic serialization, shared static serialization, static serialization.

E

EA See extended attribute.

EB See exabyte.

EFS See Encrypted File System.

Encrypted File System (EFS)

A file system that uses file system-level encryption.

enterprise configuration

A method of setting up servers so that the administrator can distribute the configuration of one of the servers to the other servers, using server-to-server communication. See also configuration manager, managed server, profile, subscription.

enterprise logging

The process of sending events from a server to a designated event server. The event server routes the events to designated receivers, such as to a user exit. See also event.

error log

A data set or file that is used to record error information about a product or system.

estimated capacity

The available space, in megabytes, of a storage pool.

event An occurrence of significance to a task or system. Events can include completion or

failure of an operation, a user action, or the change in state of a process. See also enterprise logging, receiver.

event record

A database record that describes actual status and results for events.

event server

A server to which other servers can send events for logging. The event server routes the events to any receivers that are enabled for the sending server's events.

exabyte (EB)

For processor, real and virtual storage capacities and channel volume, 2 to the power of 60 or 1 152 921 504 606 846 976 bytes. For disk storage capacity and communications volume, 1 000 000 000 000 000 000 bytes.

exclude

The process of identifying files in an include-exclude list. This process prevents the files from being backed up or migrated whenever a user or schedule enters an incremental or selective backup operation. A file can be excluded from backup, from space management, or from both backup and space management.

exclude-include list

See include-exclude list.

expiration

The process by which files, data sets, or objects are identified for deletion because their expiration date or retention period has passed.

expiring file

A migrated or premigrated file that has been marked for expiration and removal from storage. If a stub file or an original copy of a premigrated file is deleted from a local file system, or if the original copy of a premigrated file is updated, the corresponding migrated or premigrated file is marked for expiration the next time reconciliation is run.

extend

To increase the portion of available space that can be used to store database or recovery log information.

extended attribute (EA)

Names or value pairs that are associated with files or directories. There are three

classes of extended attributes: user attributes, system attributes, and trusted attributes.

external library

A collection of drives that is managed by the media-management system other than the storage management server.

F

file access time

On AIX, UNIX, or Linux systems, the time when the file was last accessed.

file age

For migration prioritization purposes, the number of days since a file was last accessed.

file device type

A device type that specifies the use of sequential access files on disk storage as volumes.

file server

A dedicated computer and its peripheral storage devices that are connected to a local area network that stores programs and files that are shared by users on the network.

file space

A logical space in server storage that contains a group of files that have been backed up or archived by a client node, from a single logical partition, file system, or virtual mount point. Client nodes can restore, retrieve, or delete their file spaces from server storage. In server storage, files belonging to a single file space are not necessarily stored together.

file space ID (FSID)

A unique numeric identifier that the server assigns to a file space when it is stored in server storage.

file state

The space management mode of a file that resides in a file system to which space management has been added. A file can be in one of three states: resident, premigrated, or migrated. See also migrated file, premigrated file, resident file.

file system migrator (FSM)

A kernel extension that intercepts all file system operations and provides any space

management support that is required. If no space management support is required, the operation is passed to the operating system, which performs its normal functions. The file system migrator is mounted over a file system when space management is added to the file system.

file system state

The storage management mode of a file system that resides on a workstation on which the hierarchical storage management (HSM) client is installed. A file system can be in one of these states: native, active, inactive, or global inactive.

frequency

A copy group attribute that specifies the minimum interval, in days, between incremental backups.

FSID See file space ID.

FSM See file system migrator.

full backup

The process of backing up the entire server database. A full backup begins a new database backup series. See also database backup series, database snapshot, incremental backup.

fuzzy backup

A backup version of a file that might not accurately reflect what is currently in the file because the file was backed up at the same time as it was being modified.

fuzzy copy

A backup version or archive copy of a file that might not accurately reflect the original contents of the file because it was backed up or archived the file while the file was being modified.

G

GB See gigabyte.

General Parallel File System (GPFS™)

A high-performance shared-disk file system that can provide data access from nodes in a clustered system environment. See also information lifecycle management.

gigabyte (GB)

For processor storage, real and virtual storage, and channel volume, 10 to the

power of nine or 1,073,741,824 bytes. For disk storage capacity and communications volume, 1,000,000,000 bytes.

global inactive state

The state of all file systems to which space management has been added when space management is globally deactivated for a client node.

Globally Unique Identifier (GUID)

An algorithmically determined number that uniquely identifies an entity within a system. See also Universally Unique Identifier.

GPFS See General Parallel File System.

GPFS node set

A mounted, defined group of GPFS file systems.

group backup

The backup of a group containing a list of files from one or more file space origins.

GUID See Globally Unique Identifier.

H

hierarchical storage management (HSM)

A function that automatically distributes and manages data on disk, tape, or both by regarding devices of these types and potentially others as levels in a storage hierarchy that range from fast, expensive devices to slower, cheaper, and possibly removable devices. The objectives are to minimize access time to data and maximize available media capacity. See also hierarchical storage management client, recall, storage hierarchy.

hierarchical storage management client (HSM client)

A client program that works with the server to provide hierarchical storage management (HSM) for a system. See also hierarchical storage management, management class.

HSM See hierarchical storage management.

HSM client

See hierarchical storage management client.

I

ILM See information lifecycle management.

image A file system or raw logical volume that is backed up as a single object.

image backup
A backup of a full file system or raw logical volume as a single object.

inactive file system
A file system for which space management has been deactivated. See also active file system.

inactive version
A backup version of a file that is either not the most recent backup version, or that is a backup version of a file that no longer exists on the client system. Inactive backup versions are eligible for expiration processing according to the management class assigned to the file. See also active version, backup version.

include-exclude file
A file containing statements to determine the files to back up and the associated management classes to use for backup or archive. See also include-exclude list.

include-exclude list
A list of options that include or exclude selected files for backup. An exclude option identifies files that should not be backed up. An include option identifies files that are exempt from the exclusion rules or assigns a management class to a file or a group of files for backup or archive services. See also include-exclude file.

incremental backup
The process of backing up files or directories, or copying pages in the database, that are new or changed since the last full or incremental backup. See also selective backup.

individual mailbox restore
See mailbox restore.

information lifecycle management (ILM)
A policy-based file-management system for storage pools and file sets. See also General Parallel File System.

inode The internal structure that describes the individual files on AIX, UNIX, or Linux

systems. An inode contains the node, type, owner, and location of a file.

inode number
A number specifying a particular inode file in the file system.

IP address
A unique address for a device or logical unit on a network that uses the Internet Protocol standard.

J

job file
A generated file that contains configuration information for a migration job. The file is XML format and can be created and edited in the hierarchical storage management (HSM) client for Windows client graphical user interface. See also migration job.

journal-based backup
A method for backing up Windows clients and AIX clients that exploits the change notification mechanism in a file to improve incremental backup performance by reducing the need to fully scan the file system.

journal daemon
On AIX, UNIX, or Linux systems, a program that tracks change activity for files residing in file systems.

journal service
In Microsoft Windows, a program that tracks change activity for files residing in file systems.

K

KB See kilobyte.

kilobyte (KB)
For processor storage, real and virtual storage, and channel volume, 2 to the power of 10 or 1,024 bytes. For disk storage capacity and communications volume, 1,000 bytes.

L

LAN See local area network.

LAN-free data movement

The movement of client data between a client system and a storage device on a storage area network (SAN), bypassing the local area network.

LAN-free data transfer

See LAN-free data movement.

leader data

Bytes of data, from the beginning of a migrated file, that are stored in the file's corresponding stub file on the local file system. The amount of leader data that is stored in a stub file depends on the stub size that is specified.

library

1. A repository for demountable recorded media, such as magnetic disks and magnetic tapes.
2. A collection of one or more drives, and possibly robotic devices (depending on the library type), which can be used to access storage volumes.

library client

A server that uses server-to-server communication to access a library that is managed by another storage management server. See also library manager.

library manager

A server that controls device operations when multiple storage management servers share a storage device. See also library client.

local

1. Pertaining to a device, file, or system that is accessed directly from a user system, without the use of a communication line. See also remote.
2. For hierarchical storage management products, pertaining to the destination of migrated files that are being moved. See also remote.

local area network (LAN)

A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

local shadow volume

Data that is stored on shadow volumes localized to a disk storage subsystem.

LOFS See loopback virtual file system.

logical file

A file that is stored in one or more server storage pools, either by itself or as part of an aggregate. See also aggregate, physical file, physical occupancy.

logical occupancy

The space that is used by logical files in a storage pool. This space does not include the unused space created when logical files are deleted from aggregate files, so it might be less than the physical occupancy. See also physical occupancy.

logical unit number (LUN)

In the Small Computer System Interface (SCSI) standard, a unique identifier used to differentiate devices, each of which is a logical unit (LU).

logical volume

A portion of a physical volume that contains a file system.

logical volume backup

A back up of a file system or logical volume as a single object.

Logical Volume Snapshot Agent (LVSA)

Software that can act as the snapshot provider for creating a snapshot of a logical volume during an online image backup.

loopback virtual file system (LOFS)

A file system that is created by mounting a directory over another local directory, also known as mount-over-mount. A LOFS can also be generated using an automounter.

LUN See logical unit number.

LVSA See Logical Volume Snapshot Agent.

M

macro file

A file that contains one or more storage manager administrative commands, which can be run only from an administrative client using the MACRO command. See also Tivoli Storage Manager command script.

mailbox restore

A function that restores Microsoft Exchange Server data (from IBM Data Protection for Microsoft Exchange backups) at the mailbox level or mailbox-item level.

managed object

A definition in the database of a managed server that was distributed to the managed server by a configuration manager. When a managed server subscribes to a profile, all objects that are associated with that profile become managed objects in the database of the managed server.

managed server

A server that receives configuration information from a configuration manager using a subscription to one or more profiles. Configuration information can include definitions of objects such as policy and schedules. See also configuration manager, enterprise configuration, profile, subscription.

management class

A policy object that users can bind to each file to specify how the server manages the file. The management class can contain a backup copy group, an archive copy group, and space management attributes. See also bind, copy group, hierarchical storage management client, policy set, rebind.

maximum transmission unit (MTU)

The largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the maximum transmission unit for Ethernet is 1500 bytes.

MB See megabyte.

media server

In a z/OS® environment, a program that provides access to z/OS disk and tape

storage for Tivoli Storage Manager servers that run on operating systems other than z/OS.

megabyte (MB)

For processor storage, real and virtual storage, and channel volume, 2 to the 20th power or 1,048,576 bytes. For disk storage capacity and communications volume, 1,000,000 bytes.

metadata

Data that describes the characteristics of data; descriptive data.

migrate

To move data to another location, or an application to another computer system.

migrated file

A file that has been copied from a local file system to storage. For HSM clients on UNIX or Linux systems, the file is replaced with a stub file on the local file system. On Windows systems, creation of the stub file is optional. See also file state, premigrated file, resident file, stub file.

migration

The process of moving data from one computer system to another, or an application to another computer system.

migration job

A specification of files to migrate, and actions to perform on the original files after migration. See also job file, threshold migration.

migration threshold

High and low capacities for storage pools or file systems, expressed as percentages, at which migration is set to start and stop.

mirroring

The process of writing the same data to multiple disks at the same time. The mirroring of data protects it against data loss within the database or within the recovery log.

mode

A copy group attribute that specifies whether to back up a file that has not been modified since the last time the file was backed up. See also absolute mode, modified mode.

modified mode

In storage management, a backup copy-group mode that specifies that a file

is considered for incremental backup only if it has changed since the last backup. A file is considered a changed file if the date, size, owner, or permissions of the file have changed. See also absolute mode, mode.

mount limit

The maximum number of volumes that can be simultaneously accessed from the same device class. The mount limit determines the maximum number of mount points. See also mount point.

mount point

A logical drive through which volumes are accessed in a sequential access device class. For removable media device types, such as tape, a mount point is a logical drive associated with a physical drive. For the file device type, a mount point is a logical drive associated with an I/O stream. See also mount limit.

mount retention period

The maximum number of minutes that the server retains a mounted sequential-access media volume that is not being used before it dismounts the sequential-access media volume.

mount wait period

The maximum number of minutes that the server waits for a sequential-access volume mount request to be satisfied before canceling the request.

MTU See maximum transmission unit.

N

Nagle algorithm

An algorithm that reduces congestion of TCP/IP networks by combining smaller packets and sending them together.

named pipe

A type of interprocess communication that permits message data streams to pass between peer processes, such as between a client and a server.

NAS file server

See network-attached storage file server.

NAS file server node

See NAS node.

NAS node

A client node that is a network-attached

storage (NAS) file server. Data for the NAS node is transferred by a NAS file server that is controlled by the network data management protocol (NDMP). A NAS node is also called a NAS file server node.

native file system

A file system that is locally added to the file server and is not added for space management. The hierarchical storage manager (HSM) client does not provide space management services to the file system.

native format

A format of data that is written to a storage pool directly by the server. See also non-native data format.

NDMP

See Network Data Management Protocol.

NetBIOS (Network Basic Input/Output System)

A standard interface to networks and personal computers that is used on local area networks to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not have to handle the details of LAN data link control (DLC) protocols.

network-attached storage file server (NAS file server)

A dedicated storage device with an operating system that is optimized for file-serving functions. A NAS file server can have the characteristics of both a node and a data mover.

Network Basic Input/Output System

See NetBIOS.

Network Data Management Protocol (NDMP)

A protocol that allows a network storage-management application to control the backup and recovery of an NDMP-compliant file server, without installing vendor-acquired software on that file server.

network data-transfer rate

A rate that is calculated by dividing the total number of bytes that are transferred by the data transfer time. For example, this rate can be the time that is spent transferring data over a network.

node A file server or workstation on which the

backup-archive client program has been installed, and which has been registered to the server.

node name

A unique name that is used to identify a workstation, file server, or PC to the server.

node privilege class

A privilege class that gives an administrator the authority to remotely access backup-archive clients for a specific client node or for all clients in a policy domain. See also privilege class.

non-native data format

A format of data that is written to a storage pool that differs from the format that the server uses for operations. See also native format.

O

offline volume backup

A backup in which the volume is locked so that no other system applications can access it during the backup operation.

online volume backup

A backup in which the volume is available to other system applications during the backup operation.

open registration

A registration process in which users can register their workstations as client nodes with the server. See also closed registration.

operator privilege class

A privilege class that gives an administrator the authority to disable or halt the server, enable the server, cancel server processes, and manage removable media. See also privilege class.

options file

A file that contains processing options. See also client system-options file, client user-options file.

originating file system

The file system from which a file was migrated. When a file is recalled, it is returned to its originating file system.

orphaned stub file

A file for which no migrated file can be found on the server that the client node is

contacting for space management services. For example, a stub file can be orphaned when the client system-options file is modified to contact a server that is different than the one to which the file was migrated.

P

packet In data communication, a sequence of binary digits, including data and control signals, that are transmitted and switched as a composite whole.

page A defined unit of space on a storage medium or within a database volume.

partial-file recall mode

A recall mode that causes the hierarchical storage management (HSM) function to read just a portion of a migrated file from storage, as requested by the application accessing the file.

password generation

A process that creates and stores a new password in an encrypted password file when the old password expires. Automatic generation of a password prevents password prompting.

path An object that defines a one-to-one relationship between a source and a destination. Using the path, the source accesses the destination. Data can flow from the source to the destination, and back. An example of a source is a data mover (such as a network-attached storage [NAS] file server), and an example of a destination is a tape drive.

pattern-matching character

See wildcard character.

physical file

A file that is stored in one or more storage pools, consisting of either a single logical file, or a group of logical files that are packaged together as an aggregate. See also aggregate, logical file, physical occupancy.

physical occupancy

The amount of space that is used by physical files in a storage pool. This space includes the unused space that is created when logical files are deleted from aggregates. See also logical file, logical occupancy, physical file.

plug-in

A separately installable software module that adds function to an existing program, application, or interface.

policy domain

A grouping of policy users with one or more policy sets, which manage data or storage resources for the users. The users are client nodes that are associated with the policy domain. See also active policy set, domain.

policy privilege class

A privilege class that gives an administrator the authority to manage policy objects, register client nodes, and schedule client operations for client nodes. Authority can be restricted to certain policy domains. See also privilege class.

policy set

A group of rules in a policy domain. The rules specify how data or storage resources are automatically managed for client nodes in the policy domain. Rules can be contained in management classes. See also active policy set, management class.

premigrated file

A file that has been copied to server storage, but has not been replaced with a stub file on the local file system. An identical copy of the file resides both on the local file system and in server storage. Premigrated files occur on UNIX and Linux file systems to which space management has been added. See also file state, migrated file, resident file.

premigrated files database

A database that contains information about each file that has been premigrated to server storage.

premigration

The process of copying files that are eligible for migration to server storage, but leaving the original file intact on the local file system.

premigration percentage

A space management setting that controls whether the next eligible candidates in a file system are premigrated following threshold or demand migration.

primary storage pool

A named set of volumes that the server uses to store backup versions of files, archive copies of files, and files migrated from client nodes. See also copy storage pool, server storage, storage pool, storage pool volume.

privilege class

A level of authority that is granted to an administrator. The privilege class determines which administrative tasks the administrator can perform. See also authority, node privilege class, operator privilege class, policy privilege class, storage privilege class, system privilege class.

profile

A named group of configuration information that can be distributed from a configuration manager when a managed server subscribes. Configuration information can include registered administrator IDs, policies, client schedules, client option sets, administrative schedules, storage manager command scripts, server definitions, and server group definitions. See also configuration manager, enterprise configuration, managed server.

profile association

On a configuration manager, the defined relationship between a profile and an object such as a policy domain. Profile associations define the configuration information that is distributed to a managed server when it subscribes to the profile.

Q**quota**

1. For HSM on AIX, UNIX, or Linux systems, the limit (in megabytes) on the amount of data that can be migrated and premigrated from a file system to server storage.
2. For HSM on Windows systems, a user-defined limit to the space that is occupied by recalled files.

R

randomization

The process of distributing schedule start times for different clients within a specified percentage of the schedule's startup window.

raw logical volume

A portion of a physical volume that is comprised of unallocated blocks and has no journaled file system (JFS) definition. A logical volume is read/write accessible only through low-level I/O functions.

rebind

To associate all backed-up versions of a file with a new management class name. For example, a file that has an active backup version is rebound when a later version of the file is backed up with a different management class association. See also bind, management class.

recall To copy a migrated file from server storage back to its originating file system using the hierarchical storage management client. See also selective recall.

receiver

A server repository that contains a log of server and client messages as events. For example, a receiver can be a file exit, a user exit, or the server console and activity log. See also event.

reclamation

The process of consolidating the remaining data from many sequential-access volumes onto fewer, new sequential-access volumes.

reclamation threshold

The percentage of space that a sequential-access media volume must have before the server can reclaim the volume. Space becomes reclaimable when files are expired or are deleted.

reconciliation

The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems.

During the reconciliation process, data that is identified as no longer needed is removed.

recovery log

A log of updates that are about to be written to the database. The log can be used to recover from system and media failures. The recovery log consists of the active log (including the log mirror) and archive logs.

register

To define a client node or administrator ID that can access the server.

registry

A repository that contains access and configuration information for users, systems, and software.

remote

For hierarchical storage management products, pertaining to the origin of migrated files that are being moved. See also local.

resident file

On a Windows system, a complete file on a local file system that might also be a migrated file because a migrated copy can exist in server storage. On a UNIX or Linux system, a complete file on a local file system that has not been migrated or premigrated, or that has been recalled from server storage and modified. See also file state.

restore

To copy information from its backup location to the active storage location for use. For example, to copy information from server storage to a client workstation.

retention

The amount of time, in days, that inactive backed-up or archived files are kept in the storage pool before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

retrieve

To copy archived information from the storage pool to the workstation for use. The retrieve operation does not affect the archive version in the storage pool. See also archive.

root user

A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

S

SAN See storage area network.

schedule

A database record that describes client operations or administrative commands to be processed. See also administrative command schedule, client schedule.

scheduling mode

The type of scheduling operation for the server and client node that supports two scheduling modes: client-polling and server-prompted.

scratch volume

A labeled volume that is either blank or contains no valid data, that is not defined, and that is available for use. See also volume.

script A series of commands, combined in a file, that carry out a particular function when the file is run. Scripts are interpreted as they are run. See also Tivoli Storage Manager command script.

Secure Sockets Layer (SSL)

A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective backup

The process of backing up certain files or directories from a client domain. The files that are backed up are those that are not excluded in the include-exclude list. The files must meet the requirement for serialization in the backup copy group of the management class that is assigned to each file. See also incremental backup.

selective migration

The process of copying user-selected files from a local file system to server storage and replacing the files with stub files on the local file system. See also demand migration, threshold migration.

selective recall

The process of copying user-selected files from server storage to a local file system. See also recall, transparent recall.

serialization

The process of handling files that are modified during backup or archive processing. See also shared dynamic serialization, shared static serialization, static serialization.

server A software program or a computer that provides services to other software programs or other computers. See also client.

server options file

A file that contains settings that control various server operations. These settings affect such things as communications, devices, and performance.

server-prompted scheduling mode

A client/server communication technique where the server contacts the client node when tasks must be done. See also client-polling scheduling mode.

server storage

The primary, copy, and active-data storage pools that are used by the server to store user files such as backup versions, archive copies, and files migrated from hierarchical storage management client nodes (space-managed files). See also active-data pool, copy storage pool, primary storage pool, storage pool volume, volume.

session

A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data for the duration of the session. See also administrative session.

session resource usage

The amount of wait time, processor time, and space that is used or retrieved during a client session.

shadow copy

A snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shadow volume

The data stored from a snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shared dynamic serialization

A value for serialization that specifies that a file must not be backed up or archived if it is being modified during the operation. The backup-archive client retries the backup or archive operation a number of times; if the file is being modified during each attempt, the backup-archive client will back up or archive the file on its last try. See also dynamic serialization, serialization, shared static serialization, static serialization.

shared library

A library device that is used by multiple storage manager servers. See also library.

shared static serialization

A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. The client attempts to retry the operation a number of times. If the file is in use during each attempt, the file is not backed up or archived. See also dynamic serialization, serialization, shared dynamic serialization, static serialization.

snapshot

An image backup type that consists of a point-in-time view of a volume.

space-managed file

A file that is migrated from a client node by the hierarchical storage management (HSM) client. The HSM client recalls the file to the client node on demand.

space management

See hierarchical storage management.

space monitor daemon

A daemon that checks space usage on all file systems for which space management is active, and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold.

sparse file

A file that is created with a length greater than the data it contains, leaving empty spaces for the future addition of data.

special file

On AIX, UNIX, or Linux systems, a file that defines devices for the system, or temporary files that are created by processes. There are three basic types of special files: first-in, first-out (FIFO); block; and character.

SSL See Secure Sockets Layer.

stabilized file space

A file space that exists on the server but not on the client.

stanza A group of lines in a file that together have a common function or define a part of the system. Stanzas are usually separated by blank lines or colons, and each stanza has a name.

startup window

A time period during which a schedule must be initiated.

static serialization

A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. If the file is in use during the first attempt, the backup-archive client cannot back up or archive the file. See also dynamic serialization, serialization, shared dynamic serialization, shared static serialization.

storage agent

A program that enables the backup and restoration of client data directly to and from storage attached to a storage area network (SAN).

storage area network (SAN)

A dedicated storage network tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy

A logical order of primary storage pools, as defined by an administrator. The order is typically based on the speed and capacity of the devices that the storage pools use. The storage hierarchy is defined by identifying the next storage pool in a storage pool definition. See also storage pool.

storage pool

A named set of storage volumes that is the destination that is used to store client

data. See also active-data pool, copy storage pool, primary storage pool, storage hierarchy.

storage pool volume

A volume that has been assigned to a storage pool. See also active-data pool, copy storage pool, primary storage pool, server storage, volume.

storage privilege class

A privilege class that gives an administrator the authority to control how storage resources for the server are allocated and used, such as monitoring the database, the recovery log, and server storage. See also privilege class.

stub A shortcut on the Windows file system that is generated by the hierarchical storage management (HSM) client for a migrated file that allows transparent user access. A stub is the sparse file representation of a migrated file, with a reparse point attached.

stub file

A file that replaces the original file on a local file system when the file is migrated to storage. A stub file contains the information that is necessary to recall a migrated file from server storage. It also contains additional information that can be used to eliminate the need to recall a migrated file. See also migrated file, resident file.

stub file size

The size of a file that replaces the original file on a local file system when the file is migrated to server storage. The size that is specified for stub files determines how much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

subscription

In a storage environment, the process of identifying the subscribers to which the profiles are distributed. See also enterprise configuration, managed server.

system privilege class

A privilege class that gives an administrator the authority to issue all server commands. See also privilege class.

T

tape library

A set of equipment and facilities that support an installation's tape environment. The tape library can include tape storage racks, mechanisms for automatic tape mounting, a set of tape drives, and a set of related tape volumes mounted on those drives.

tape volume prefix

The high-level-qualifier of the file name or the data set name in the standard tape label.

target node

A client node for which other client nodes (called agent nodes) have been granted proxy authority. The proxy authority allows the agent nodes to perform operations such as backup and restore on behalf of the target node, which owns the data.

TCA See trusted communications agent.

TCP/IP

See Transmission Control Protocol/Internet Protocol.

threshold migration

The process of moving files from a local file system to server storage based on the high and low thresholds that are defined for the file system. See also automatic migration, demand migration, migration job, selective migration.

throughput

In storage management, the total bytes in the workload, excluding overhead, that are backed up or restored, divided by elapsed time.

timeout

A time interval that is allotted for an event to occur or complete before operation is interrupted.

Tivoli Storage Manager command script

A sequence of Tivoli Storage Manager administrative commands that are stored in the database of the Tivoli Storage Manager server. The script can run from any interface to the server. The script can include substitution for command parameters and conditional logic. See also macro file, script.

tombstone object

A small subset of attributes of a deleted object. The tombstone object is retained for a specified period, and at the end of the specified period, the tombstone object is permanently deleted.

Transmission Control Protocol/Internet Protocol (TCP/IP)

An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types. See also communication method.

transparent recall

The process that is used to automatically recall a migrated file to a workstation or file server when the file is accessed. See also selective recall.

trusted communications agent (TCA)

A program that handles the sign-on password protocol when clients use password generation.

U

UCS-2 A 2-byte (16-bit) encoding scheme based on ISO/IEC specification 10646-1. UCS-2 defines three levels of implementation: Level 1-No combining of encoded elements allowed; Level 2-Combining of encoded elements is allowed only for Thai, Indic, Hebrew, and Arabic; Level 3-Any combination of encoded elements are allowed.

UNC See Universal Naming Convention.

Unicode

A character encoding standard that supports the interchange, processing, and display of text that is written in the common languages around the world, plus many classical and historical texts.

Unicode-enabled file space

Unicode file space names provide support for multilingual workstations without regard for the current locale.

Universally Unique Identifier (UUID)

The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier. See also Globally Unique Identifier.

Universal Naming Convention (UNC)

The server name and network name combined. These names together identify the resource on the domain.

UTF-8 Unicode Transformation Format, 8-bit encoding form, which is designed for ease of use with existing ASCII-based systems. The CCSID value for data in UTF-8 format is 1208. See also UCS-2.

UUID See Universally Unique Identifier.

V**validate**

To check a policy set for conditions that can cause problems if that policy set becomes the active policy set. For example, the validation process checks whether the policy set contains a default management class.

version

A backup copy of a file stored in server storage. The most recent backup copy of a file is the active version. Earlier copies of the same file are inactive versions. The number of versions retained by the server is determined by the copy group attributes in the management class.

virtual file space

A representation of a directory on a network-attached storage (NAS) file system as a path to that directory.

virtual mount point

A directory branch of a file system that is defined as a virtual file system. The virtual file system is backed up to its own file space on the server. The server processes the virtual mount point as a separate file system, but the client operating system does not.

virtual volume

An archive file on a target server that represents a sequential media volume to a source server.

volume

A discrete unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. See also scratch volume, server storage, storage pool, storage pool volume.

volume history file

A file that contains information about volumes that have been used by the server for database backups and for export of administrator, node, policy, or server data. The file also has information about sequential-access storage pool volumes that have been added, reused, or deleted. The information is a copy of volume information that is recorded in the server database.

Volume Shadow Copy Service (VSS)

A set of Microsoft application-programming interfaces (APIs) that are used to create shadow copy backups of volumes, exact copies of files, including all open files, and so on.

VSS See Volume Shadow Copy Service.

VSS Backup

A backup operation that uses Microsoft Volume Shadow Copy Service (VSS) technology. The backup operation produces an online snapshot (point-in-time consistent copy) of Microsoft Exchange data. This copy can be stored on local shadow volumes or on Tivoli Storage Manager server storage.

VSS Fast Restore

An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves the data by using a file-level copy method.

VSS Instant Restore

An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves the data by using a hardware assisted restore method (for example, a FlashCopy operation).

VSS offloaded backup

A backup operation that uses a Microsoft Volume Shadow Copy Service (VSS) hardware provider (installed on an alternate system) to move IBM Data Protection for Microsoft Exchange data to the Tivoli Storage Manager server. This type of backup operation shifts the backup load from the production system to another system.

VSS Restore

A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on Tivoli Storage Manager server storage to their original location.

W**wildcard character**

A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace the wildcard character.

workload partition (WPAR)

A partition within a single operating system instance.

workstation

A terminal or personal computer at which a user can run applications and that is usually connected to a mainframe or a network.

worldwide name (WWN)

A 64-bit, unsigned name identifier that is unique.

WPAR See workload partition.

WWN See worldwide name.

Index

A

- accessibility features 105
- authority
 - see permissions 8

C

- communication ports
 - installation 9
- configuration notebook 59
- configuration wizard 57
- configuring
 - advanced tasks 77
 - Cygwin 71
 - data mover nodes
 - vCloud environment 83
 - vSphere environment 79
 - Data Protection for VMware Recovery Agent GUI 67
 - existing configuration 59
 - initial configuration 57
 - iSCSI mount 64
 - overview 57
 - tape storage 61
 - Tivoli Storage Manager nodes
 - vSphere environment 77
 - VMCLI
 - vSphere environment 87
 - VMCLI configuration file 75
 - vSphere environment
 - command-line checklist 89
- credentials
 - see permissions 8
- customer support
 - contacting 102
- Cygwin
 - configuring 71

D

- data mover
 - nodes
 - configuring in vCloud environment 83
 - configuring in vSphere environment 79
 - operating system requirements 17
 - overview 1
 - upgrading 55
- Data Protection for VMware Recovery Agent GUI
 - configuring 67
 - operating system requirements 15
 - options 67
- Data Protection for VMware vCloud GUI
 - operating system requirements 17
- Data Protection for VMware vSphere GUI
 - operating system requirements 16
- disability 105

E

- environment requirements
 - installation 12

F

- fixes, obtaining 102

G

- glossary 111

H

- hardware requirements 11

I

- IBM Support Assistant 101
- installation
 - communication ports 9
 - environment requirements 12
 - features by operating system 19
 - road map 6
 - user permissions 8
- installation procedure
 - Linux
 - clean 28
 - language pack 30
 - selected features 26
 - silent 39
 - Windows 32-bit
 - language pack 30
 - selected features 22
 - silent 33
 - silent Suite installer 31
 - Windows 64-bit
 - all features 20
 - language pack 30
 - selected features 22
 - silent 35
 - silent Suite installer 32
- integrating
 - with Tivoli Storage FlashCopy Manager for VMware 97
- Internet, searching for problem resolution 101, 102
- iSCSI mount
 - configuring 64

K

- keyboard 105
- knowledge bases, searching 101

L

- language pack
 - installation procedure
 - Linux 30
 - Windows 32-bit 30
 - Windows 64-bit 30
- Linux
 - installation procedure
 - clean 28
 - language pack 30
 - selected features 26
 - silent 39
 - uninstalling
 - silent mode 44
 - typical 42
 - upgrading
 - silent 55

M

- migrating
 - schedules 93

O

- operating system requirements
 - data mover 17
 - Data Protection for VMware Recovery Agent GUI 15
 - Data Protection for VMware vCloud GUI 17
 - Data Protection for VMware vSphere GUI 16
 - Recovery Agent command-line interface 14
- overview
 - Data Protection for VMware command-line interface 1
 - Data Protection for VMware Recovery Agent 1
 - Data Protection for VMware vCloud GUI 1
 - Data Protection for VMware vSphere GUI 1
 - product 1

P

- Passport Advantage 102
- permissions
 - installation 8
- ports
 - installation 9
- problem determination
 - describing problem for IBM Software Support 103
 - determining business impact for IBM Software Support 103

- problem determination (*continued*)
 - submitting a problem to IBM Software 103
- publications
 - download v

R

- Recovery Agent command-line interface
 - operating system requirements 14

S

- services 60
- silent install
 - Linux 39
 - Windows 32-bit
 - silent mode 33
 - silent Suite installer 31
 - Windows 64-bit
 - silent mode 35
 - silent Suite installer 32
- silent uninstall
 - Linux
 - silent mode 44
 - Windows 32-bit
 - silent mode 43
 - Windows 64-bit
 - silent mode 43
- silent upgrade
 - Linux 55
 - Windows 32-bit 54
 - Windows 64-bit 55
- software support
 - describing problem for IBM Software Support 103
 - determining business impact for IBM Software Support 103
 - submitting a problem 103
- Software Support
 - contacting 102
- support contract 102
- support information 99
- support subscription 102

T

- tape storage
 - configuring 61
- Tivoli Storage Manager nodes
 - configuring
 - vSphere environment 77

U

- uninstalling
 - Linux
 - silent mode 44
 - typical 42
 - Windows 32-bit
 - server core 43
 - silent mode 43
 - typical 42
 - Windows 64-bit
 - server core 43

- uninstalling (*continued*)
 - Windows 64-bit (*continued*)
 - silent mode 43
 - typical 42
- upgrading
 - data mover nodes 55
 - from Tivoli Storage FlashCopy Manager for VMware V3.x
 - standard 51
 - from Tivoli Storage FlashCopy Manager for VMware V3.x and Data Protection for VMware V6.x
 - standard 52
 - from V6.x
 - standard 49
 - Linux
 - silent 55
 - overview 49
 - Windows 32-bit
 - silent 54
 - Windows 64-bit
 - silent 55
- user
 - installation permissions 8

V

- VMCLI
 - configuring in vSphere environment 87
- VMCLI configuration file
 - modifying 75
 - vmcliConfiguration.xml 75

W

- Windows 32-bit
 - installation procedure
 - language pack 30
 - selected features 22
 - silent 33
 - silent Suite installer 31
 - uninstalling
 - server core 43
 - silent mode 43
 - typical 42
 - upgrading
 - silent 54
- Windows 64-bit
 - installation procedure
 - all features 20
 - language pack 30
 - selected features 22
 - silent 35
 - silent Suite installer 32
 - uninstalling
 - server core 43
 - silent mode 43
 - typical 42
 - upgrading
 - silent 55



Product Number: 5725-A44

Printed in USA