Tivoli® Storage Manager for Virtual Environments
Version 6.2

Data Protection for VMware Installation and User's Guide

SC27-2898-00

Tivoli® Storage Manager for Virtual Environments
Version 6.2

Data Protection for VMware Installation and User's Guide

SC27-2898-00

Note:
Before using this information and the product it supports, read the information in “Notices” on page 57.

This edition applies to Version 6.2 of Tivoli Storage Manager for Virtual Environments (product number 5725-A44) and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

Contents

Preface

IBM® Tivoli® Storage Manager for Virtual Environments provides off-host single source block incremental backup and file recovery and instant restore from a full-VM backup for Windows and Linux guest machines. In addition, Data Protection for VMware allows the backup-archive client to perform block level incremental backups.

This publication describes how to install, configure, and use Data Protection for VMware.

Who should read this guide

This guide is intended for anyone who wants to use Tivoli Storage Manager for Virtual Environments.

Publications

Tivoli Storage Manager publications and other related publications are available online.

You can search all publications for Tivoli Storage Manager and download PDFs from the following locations:

Tivoli Storage Manager Information Center
http://publib.boulder.ibm.com/infocenter/tsminfo/v6r2

IBM Publications Center
http://www.ibm.com/shop/publications/order/

You can also order some related publications from the IBM Publications Center Web site. The Web site provides information for ordering publications from countries other than the United States. In the United States, you can order publications by calling 800-879-2755.

Support information

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

Start at the IBM Support Portal: 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.

Getting technical training

Information about Tivoli technical training courses is available online.

Visit the following Web sites for training information:

Tivoli software training and certification
Choose from instructor led, online classroom training, self-paced Web classes, Tivoli certification preparation, and other training options at this site: http://www.ibm.com/software/tivoli/education/

Tivoli Support Technical Exchange
Technical experts share their knowledge and answer your questions in these webcasts: http://www.ibm.com/software/sysmgmt/products/support/supp_tech_exch.html

Searching knowledge bases

If you have a problem with IBM Tivoli Storage Manager, there are several knowledge bases that you can search.

Begin by searching the Tivoli Storage Manager Information Center at http://publib.boulder.ibm.com/infocenter/tsminfo/v6r2. From this Web site, you can search the current Tivoli Storage Manager documentation.

Searching the Internet

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

To search multiple Internet resources, go to the support Web site for Tivoli Storage Manager at http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.

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 Web site, you can search various resources including:
- IBM technotes
- IBM downloads
- IBM Redbooks® publications
- IBM Authorized Program Analysis Reports (APARs)

Select the product and click **Downloads** to search the APAR list.

If you still cannot find a solution to the problem, you can search forums and newsgroups on the Internet for the latest information that might help you find problem resolution.

An independent user discussion list, ADSM-L, is hosted by Marist College. You can subscribe by sending an e-mail to listserv@vm.marist.edu. The body of the message must contain the following text: `SUBSCRIBE ADSM-L` *your_first_name your_family_name*.

To share your experiences and learn from others in the Tivoli Storage Manager user community, go to the Tivoli Storage Manager wiki at http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager.

Using IBM Support Assistant

IBM Support Assistant is a complimentary software product that helps you with problem determination. You can 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.

IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem. For more information, see the IBM Support Assistant Web site at http://www.ibm.com/software/support/isa/.

The product-specific plug-in modules provide you with the following resources:
- Support links
- Education links
- Ability to submit problem management reports

Find add-ons for specific products here: http://www.ibm.com/support/docview.wss?&uid=swg27012689.

Finding product fixes

A product fix to resolve your problem might be available from the IBM Software Support Web site.

You can determine what fixes are available by checking the IBM Software Support Web site at http://www.ibm.com/support/entry/portal/.
- If you previously customized the site based on your product usage:
  1. Click the link for your IBM Tivoli Storage Manager product, or one of the other Tivoli Storage Manager components for which you want to find a fix.
  2. Click **Downloads**, and then click **Fixes by version**.
- If you have not customized the site based on your product usage, click **Downloads** and search for your product.

Receiving notification of product fixes

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

To sign up to receive notifications about IBM products, follow these steps:
1. From the support page at http://www.ibm.com/support/entry/portal/, click **My notifications** in the notifications module.
2. Sign in using your IBM ID and password. If you do not have an ID and password, click **register now** above the IBM ID and password.
3. Click the **Subscribe** tab to select your product family and click **Continue**.
4. Select the type of information that you want to receive, and add your personal preferences. You can specify how you want to be notified, how often, and you can also optionally select a folder for the notifications.
5. Click **Submit**.
6. For notifications for other products, repeat steps 4 and 5.

   Tip: You can also pick a product first, from the main support portal site, and then click in the **Notifications** section to create or update your subscription for that product.

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.

Before you contact IBM Software Support, follow these steps:

1. Set up a subscription and support contract.
2. Determine the business impact of your problem.
3. Describe your problem and gather background information.

Then see "Submitting the problem to IBM Software Support" on page ix for information on contacting IBM Software Support.

Setting up a subscription and support contract

Set up a subscription and support contract. The type of contract that you need depends on the type of product you have.

For IBM distributed software products (including, but not limited to, IBM Tivoli, Lotus®, and Rational® products, as well as IBM DB2® and IBM WebSphere® products that run on Microsoft Windows or UNIX operating systems), enroll in IBM Passport Advantage® in one of the following ways:

- **Online:** Go to the Passport Advantage Web page at http://www.ibm.com/software/lotus/passportadvantage/, click **How to enroll**, and follow the instructions.
- **By Phone:** You can call 1-800-IBMSERV (1-800-426-7378) in the United States, or for the phone 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 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 gather 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 recreated? 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 phone.

Online

Go to the IBM Software Support Web site at 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 phone

For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

Chapter 1. Tivoli Storage Manager for Virtual Environments overview

IBM Tivoli Storage Manager for Virtual Environments enables a backup-archive client to perform block level incremental backups. Data Protection for VMware Recovery Agent can mount snapshots to enable file level restores and can perform instant restores of volumes.

Block level incremental backups

The Windows backup-archive client uses the Change Block Tracking capabilities provided vStorage APIs for Data Protection (VADP). Blocks read from the VMware guest disk snapshot are written to the Tivoli Storage Manager server. The backup-archive client to perform full VM restore and enables the mount and instant restore to be used with data backed up by the client.

File level restore and instant restore use the snapshot data generated by the backup-archive client. The client creates a disk-level snapshot, which is a single snapshot containing a complete disk image. All data is backed up at the disk block level in full and incremental snapshots. The data can then be restored to a disk, or mounted as a virtual volume for an individual file restore.

File level restore

File level restore can be performed in-guest or, off-host, and on supported Windows and Linux machines. You can then use the files located on the virtual device. File restore is done from a backup-archive client full VM backup. The recovery point represented by either a full or incremental backup can be mounted.

Instant restore

With instant restore, you can restore the content of a single partition from a snapshot. Instant restore can be done from a full VM backup. You can use the volume immediately, while the restore process continues in the background.

System components

Tivoli Storage Manager for Virtual Environments consists of the Data Protection for VMware Recovery Agent and the command line.

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.

Command line

You can use the command line, which is installed on Windows only, to perform the following tasks from a remote machine:

- Gather information about available restorable data, including lists of:
  - Backed-up virtual machines
  - 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.

Chapter 2. Planning

Before you install Data Protection for VMware, verify that your system is running a supported operating system, and that you meet all hardware and software requirements.

Data Protection for VMware supports any disk configuration that is supported by the hardware and operating system. The disk configuration includes multipath device drivers.

Operating systems

To implement Data Protection for VMware components, your site must have the appropriate operating system and environment, hardware and software.

- "Operating systems for Data Protection for VMware Recovery Agent"
- "Operating systems for the command line" on page 5

Operating systems for Data Protection for VMware Recovery Agent

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

The following table provides details about operating systems that are supported for Data Protection for VMware Recovery Agent.

Table 1. Operating systems for Data Protection for VMware Recovery Agent

Operating system and supported release	**Support details**
Microsoft Windows 2003, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Storage Server • Storage R2 Server	• Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture • Supports 32-bit and 64-bit processors
Microsoft Windows 2003 64 bit Edition	• Supports the x64 (AMD64 and EM64T) instruction set architecture • Supports 64-bit processors
Microsoft Windows 2008, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Supports the x86 (32 bit), x64 (AMD64 and EM64T) instruction set architecture • Supports 32-bit and 64-bit processors • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/default.aspx?scid=kb;EN-US;970770 . Download the hotfix associated with this knowledge base article.

Table 1. Operating systems for Data Protection for VMware Recovery Agent (continued)

Operating system and supported release	Support details
Microsoft Windows 2008, R2 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Supports the x64 (AMD64 and EM64T) instruction set architecture. • Supports 64-bit processors • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/default.aspx?scid=kb;EN-US;970770 . Download the hotfix associated with this knowledge base article.
Microsoft Windows Vista, Service Pack 1 or later: • Starter • Home Basic • Home Premium • Business • Enterprise • Ultimate	• Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture • Supports 32-bit and 64-bit processors
Microsoft Windows XP Professional Edition, Service Pack 2 or later	• Supports the x86 (32 bit) instruction set architecture • Supports 32-bit processors
Red Hat Enterprise Linux 5.2, 5.3, 5.4 servers	• Supports the x86 (32 bit) instruction set architecture • Supports 32-bit and 64-bit processors • The following kernels are supported: – RedHat-i386: 2.6.18-92.e15.i686 and 2.6.18-92.e15.i686 PAE – RedHat-x86_64: 2.6.18-92.el5-x86_64 • Perl version 5 on Linux systems • **mdadm** tool for managing Linux Software RAID arrays • iSCSI Initiator for Linux package iscsi-initiator-utils-6.2.0.868-0.7.el5 • Secure Shell (SSH) client for Linux
SUSE Linux Enterprise Server 10, Service Pack 2	• Supports the x86 (32 bit) instruction set architecture • Supports 32-bit and 64-bit processors • The following kernels are supported: – SUSE-i386: 2.6.16.60-0.21default, 2.6.16.60-0.21smp, and 2.6.16.60-0.21bigsmp – SUSE-x86_64: 2.6.16.60-0.21default and 2.6.16.60-0.21smp For all kernel versions, auto mount is not supported. • Perl version 5 on Linux systems • **mdadm** tool for managing Linux Software RAID arrays • iSCSI Initiator for Linux • Secure Shell (SSH) client for Linux

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.

Operating systems for the command line

Ensure that you are installing the command line on a supported operating system.

The following table provides details about operating systems that are supported for the command line.

Table 2. Operating systems for the command line

Operating system and supported release	**Support details**
Microsoft Windows 2003, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Storage Server • Storage R2 Server	• Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture • Supports 32-bit and 64-bit processors
Microsoft Windows 2003 64 bit Edition	• Supports the x64 (AMD64 and EM64T) and IA64 (Intel Itanium) instruction set architecture • Supports 64-bit processors
Microsoft Windows 2008, Service Pack 1 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Supports the x86 (32 bit), x64 (AMD64 and EM64T), and IA64 (Intel Itanium) instruction set architecture • Supports 32-bit and 64-bit processors • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/default.aspx?scid=kb;EN-US;970770 . Download the hotfix associated with this knowledge base article.
Microsoft Windows 2008, R2 or later for the following servers: • Standard Server • Enterprise Server • Datacenter Server • Web Server • Storage Server • Small Business Server • Essential Business Server	• Supports the x64 (AMD64 and EM64T) and IA64 (Intel Itanium) instruction set architecture • Supports 64-bit processors • If you use Active Directory with Microsoft Windows 2008, see the Microsoft Knowledge Base article 970770 online at http://support.microsoft.com/default.aspx?scid=kb;EN-US;970770 . Download the hotfix associated with this knowledge base article.

Table 2. Operating systems for the command line (continued)

Operating system and supported release	Support details
Microsoft Windows Vista, Service Pack 1 or later: • Starter • Home Basic • Home Premium • Business • Enterprise • Ultimate	• Supports the x86 (32 bit) and x64 (AMD64 and EM64T) instruction set architecture • Supports 32-bit and 64-bit processors
Microsoft Windows XP Professional Edition, Service Pack 2 or later	• Supports the x86 (32 bit) instruction set architecture • Supports 32-bit processors

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

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

Table 3. Hardware requirements for Data Protection for VMware.

Component	Minimal requirement	Preferred
System	3 GHz Dual Intel Pentium D processor or compatible	
Memory	2 GB RAM, 2 GB virtual address space	
Available hard disk	200 MB for 'Documents and Settings' folder	2 GB
NIC Card	1 NIC - 100 Mbps	1 NIC - 1 Gbps

Software requirements and prerequisites

Before installing Data Protection for VMware Version 6.2, some applications, utilities, and components must be installed or available.

Data Protection for VMware Recovery Agent

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 Data Protection for VMware Recovery Agent operations. 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.

Using the command line to support Mount on a Linux machine

To use the command line client from a system running a supported Linux operating system, complete the following steps:

1. On the Windows system where you have installed or plan to install the command line client, install Cygwin 1.5.25 or later. When you install Cygwin, include the OpenSSH package. To manually install Cygwin, complete the following steps:
    a. Log on to the Windows server using an account with administrator privileges.
    b. Go to the following web site and install Cygwin 1.5.25 or later: http://www.cygwin.com
    c. When completing the installation wizard for Cygwin, there is a **Select Package** page. On this page, clear the **Hide obsolete and administrative packages** check box.
    d. During the installation process for Cygwin, select the following Cygwin packages:

Table 4. Cygwin packages

Category	Package
Net	All default packages. In addition, select the following packages: • **openssh** (contains **ssh.exe**) • **openssl** (contains **ssl.exe**) • **rsync** • **tcp_wrappers**

    e. After finishing the Cygwin installation wizard, add the `Cygwin\bin` directory to the Microsoft Windows `%PATH%` environment variable. The directory must be the first one in the `%PATH%` environment variable.

       Remember: Restart the system so the variable update can take effect.
2. On the system where you have installed or plan to install the command line client, test the Cygwin installation.

   Remember: Before using Cygwin, review the Cygwin documentation for any issues that might affect your environment.
   To test the Cygwin installation, from the Microsoft Windows Start menu, select **Programs** > **Cygnus Solutions** > **Cygwin Bash Shell**. A command prompt window should be displayed. This window is a bash shell.
3. On the system where you have installed or plan to install the command line client with Cygwin, install the SSH daemon service. To install the SSH daemon service, complete the following steps:
    a. Enter the following commands to give read access to the `/etc/passwd` and `/etc/group` files:

```
chmod +r /etc/passwd
chmod +r /etc/group
```

    b. Enter the following command to give read access to the `/var` directory:

```
chmod 755 /var
```

c. From the Cygwin command prompt window, run the following command to create the SSH daemon service:

```
ssh-host-config
```

d. When a query about whether privilege separation should be used is posted in the command prompt window, enter *no*.

e. When a query about whether a new local account named *sshd* should be created is posted in the command prompt window, enter *yes*.

f. When a query about whether *sshd* should be installed as a service is posted in the command prompt window, enter *yes*.

g. When a query asks you to enter the value of **CYGWIN** for the daemon, enter the following text: *ntsec tty*

h. When a query asks if you want to use a different name, enter *no*.

i. When a query asks if you want to create a new privileged user account named *cyg_server*, enter *yes*.

j. When a query asks you to enter a 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.

k. At the prompt, enter the following command:

```
set CYGWIN 'ntsec tty'
```

Also, add CYGWIN as a Microsoft Windows environment variable with the value `ntsec tty`.

4. Configure the authentication key files by logging on to the Linux system where Data Protection for VMware is installed and by completing these tasks:

   a. Issue this command and press **Enter** at all prompt questions:

   ```
   ssh-keygen -t dsa
   ```

   b. Issue these commands:

   ```
   cd .ssh
   scp id_dsa.pub Administrator@windows_machine:/home/Administrator
   ```

   c. Issue these commands from the Cygwin shell on the Windows server:

   ```
   mkdir .ssh
   chmod 700 .ssh
   cd .ssh
   touch authorized_keys
   cat ../id_dsa.pub >> authorized_keys
   rm ../id_dsa.pub
   ```

   d. Configure the SSH server to use the authentication files by editing the SSH service configuration file `c:\cygwin\etc\sshd_config`. Open this file and unmark these entries:

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

   Update the `AuthorizedKeysFile` value to specify `/home/Administrator/.ssh/authorized_keys`.

   e. Issue these commands from the Cygwin shell on the Windows server to restart the sshd service:

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

   f. Verify that the Linux system can communicate with the Windows server system by issuing this command (from the Linux system):

```
ssh Administrator@windows_machine
```

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

```
ssh Administrator@windows_machine
ssh Administrator@windows_machine.xyz.com
```

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 Server.
- Update the known_hosts file with all host name conventions associated with the Windows Server.

Important: You must create authentication key files for each new client system. Therefore, complete Steps 4a through 4f for each client system.

5. Permit any host to connect using SSH to the server by editing the following file: `C:\cygwin\etc\hosts.allow`

   The following line must immediately precede the `ALL : PARANOID : deny` line:

   ```
   sshd: ALL
   ```
6. Log on to the command line (without a password).
7. In the command prompt window, enter the following command:

   ```
   TDPVMwareShell.exe -c command type tag parameter
   ```

In addition to the Cygwin and SSH daemon service, the GNU C libraries, Version 2.3.3-98.38 or later are required.

Virtual environment configurations

Data Protection for VMware provides a variety of configurations for performing file-level restore, instant restore, and disk / block device exposure.

Off-host file-level restore for Windows and for Linux

These configurations do not require Data Protection for VMware Recovery Agent to be installed in each virtual machine guest. Instead, an off-host Windows or Linux instance is responsible for file-level restore of multiple virtual machines. With this configuration, the mount process exposes a virtual volume from a selected disk partition.

The Tivoli Storage Manager node name associated with the Data Protection for VMware Recovery Agent instance requires access to all virtual machines. Issue the following command from the backup-archive client node that owns the virtual machines:

```
set access backup * mountnodename
```

When a snapshot has been mounted to the off-host server, it can then be exported to allow a virtual machine guest user access to the files. This centralized restore process is typically initiated by a VMware administrator, by a Tivoli Storage Manager administrator, or by help desk personnel.

For these configurations, ensure that you compare the specific virtual machine guest operating system requirements with the supported levels of Data Protection for VMware Recovery Agent. If a specific operating system is not supported, determine if the off-host disk / block device exposure configuration could be used. See Figure 7 on page 14.

The data paths for off-host file restores are illustrated in Figure 1 and Figure 2 on page 11

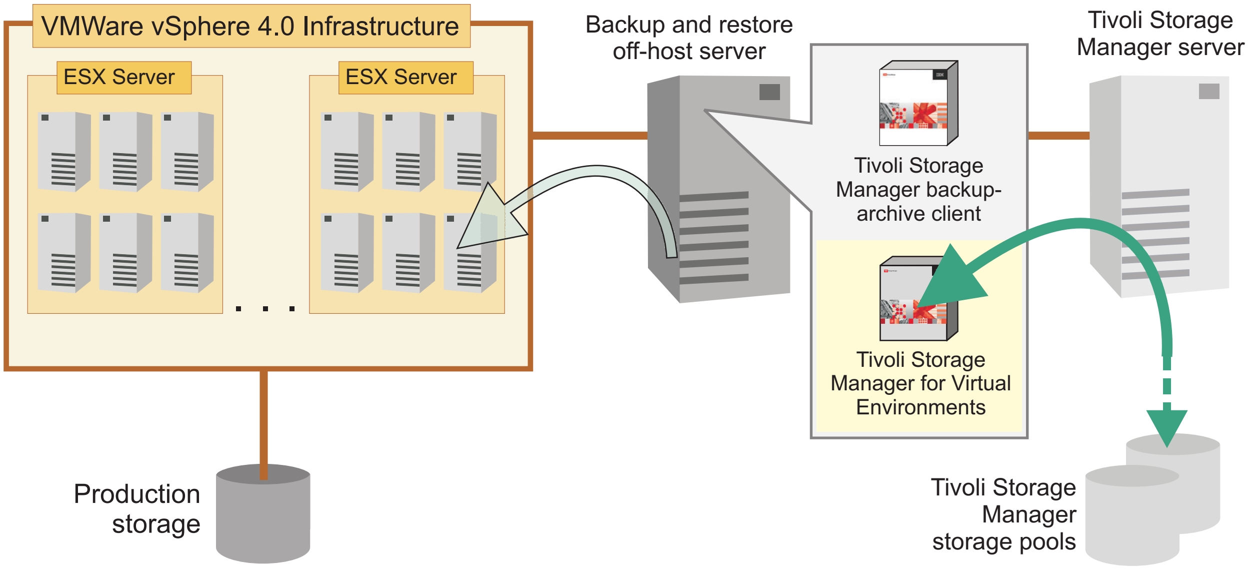
VMWare vSphere 4.0 Infrastructure
ESX Server
ESX Server
. . .
Backup and restore off-host server
Tivoli Storage Manager backup-archive client
Tivoli Storage Manager for Virtual Environments
Tivoli Storage Manager server
Production storage
Tivoli Storage Manager storage pools

Figure 1. Off-host file-level restore for Windows

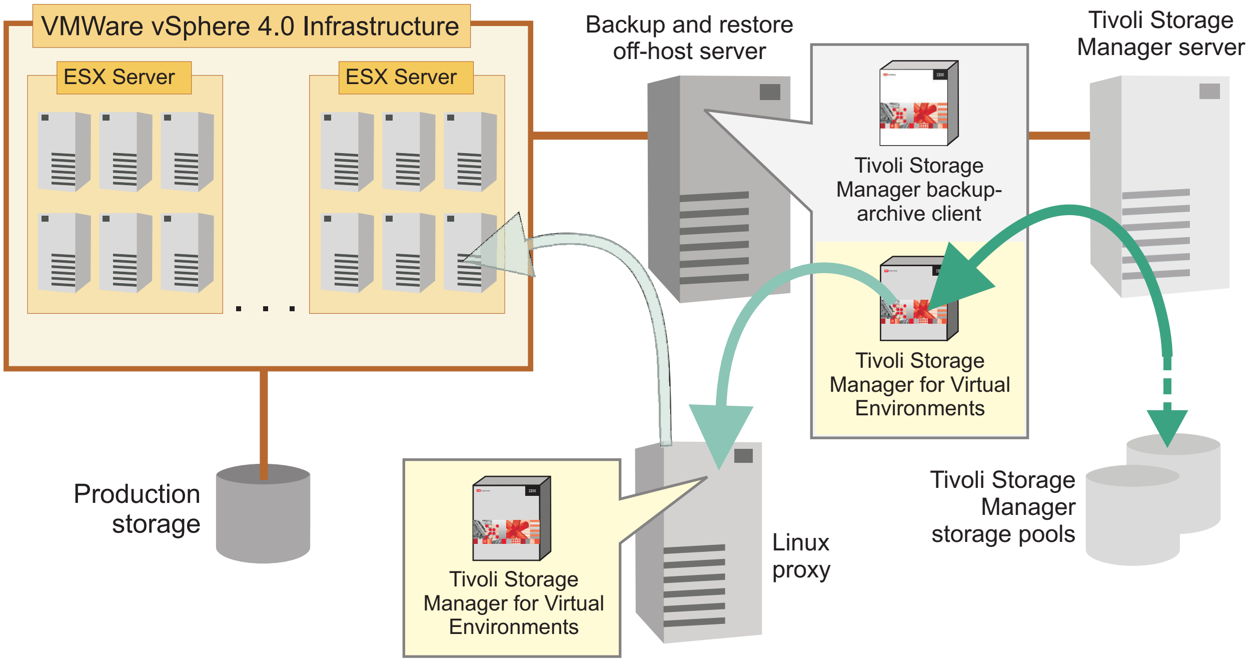
VMWare vSphere 4.0 Infrastructure
ESX Server
ESX Server
Backup and restore off-host server
Tivoli Storage Manager server
Tivoli Storage Manager backup-archive client
Tivoli Storage Manager for Virtual Environments
Production storage
Tivoli Storage Manager for Virtual Environments
Linux proxy
Tivoli Storage Manager storage pools

Figure 2. Off-host file-level restore for Linux

In-guest file-level restore and instant restore for Windows and for Linux

These configurations require Data Protection for VMware Recovery Agent to be installed in each virtual machine guest. The mount and instant restore processes are performed for a virtual volume from a selected disk partition.

The Data Protection for VMware Recovery Agent node name would typically be granted access only to the virtual machine where it is running. To grant access, issue the following command from the backup-archive client node that owns the virtual machines:

```
set access backup "{\\VMFULL-vmdisplayname}\*\*" * mountnodename
```

The restore process is typically begun by a VMware user who logs in to the guest machine of the virtual machine.

For these configurations, be sure to compare the specific virtual machine guest operating system requirements with the supported levels of Data Protection for VMware Recovery Agent. If a specific operating system is not supported, determine if the off-host disk / block device exposure configuration can also be used for file-level recovery. Instant restore can only be used within a virtual machine guest for volumes that are not the operating system volume.

The data paths for in-guest file level restores are illustrated in Figure 3 on page 12 and Figure 4 on page 12. The data path for in-guest instant restore is illustrated in Figure 5 on page 13 and Figure 6 on page 13.

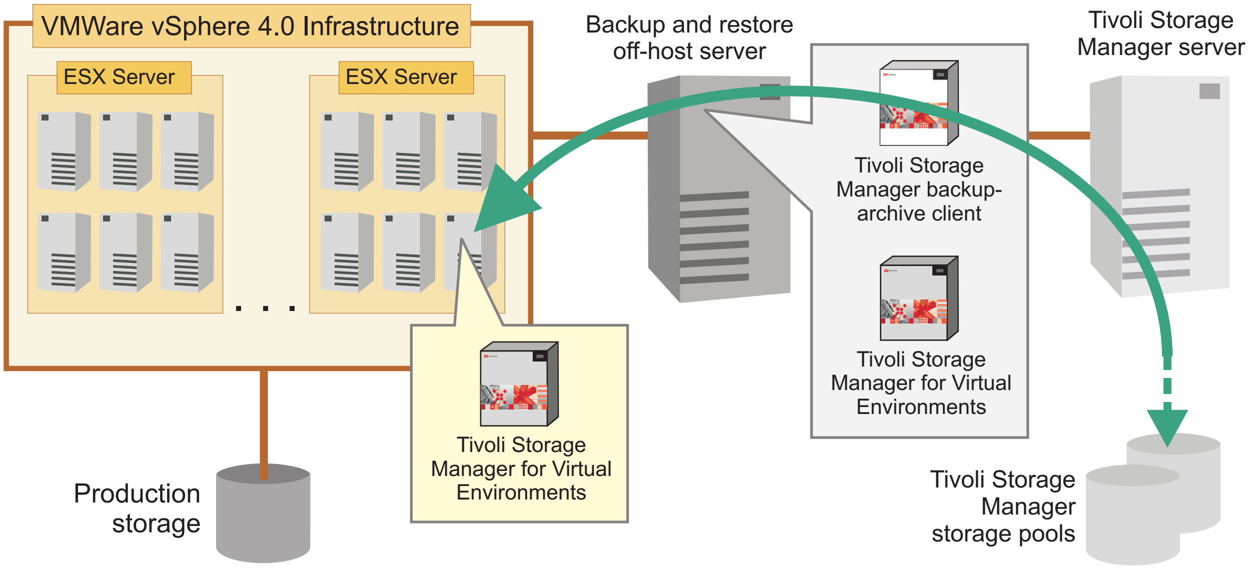
VMWare vSphere 4.0 Infrastructure
ESX Server
ESX Server
. . .
Production storage
Tivoli Storage Manager for Virtual Environments
Backup and restore off-host server
Tivoli Storage Manager backup-archive client
Tivoli Storage Manager for Virtual Environments
Tivoli Storage Manager server
Tivoli Storage Manager storage pools

Figure 3. In-guest file-level restore for Windows

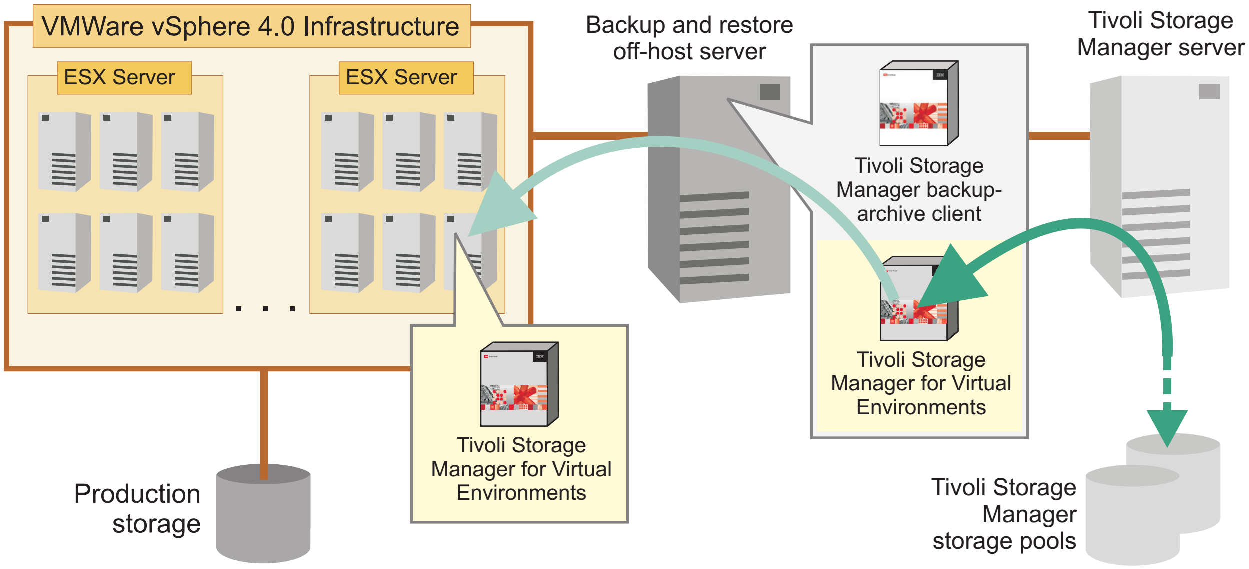
VMWare vSphere 4.0 Infrastructure
ESX Server
ESX Server
. . .
Production storage
Tivoli Storage Manager for Virtual Environments
Backup and restore off-host server
Tivoli Storage Manager backup-archive client
Tivoli Storage Manager for Virtual Environments
Tivoli Storage Manager server
Tivoli Storage Manager storage pools

Figure 4. In-guest file-level restore for Linux

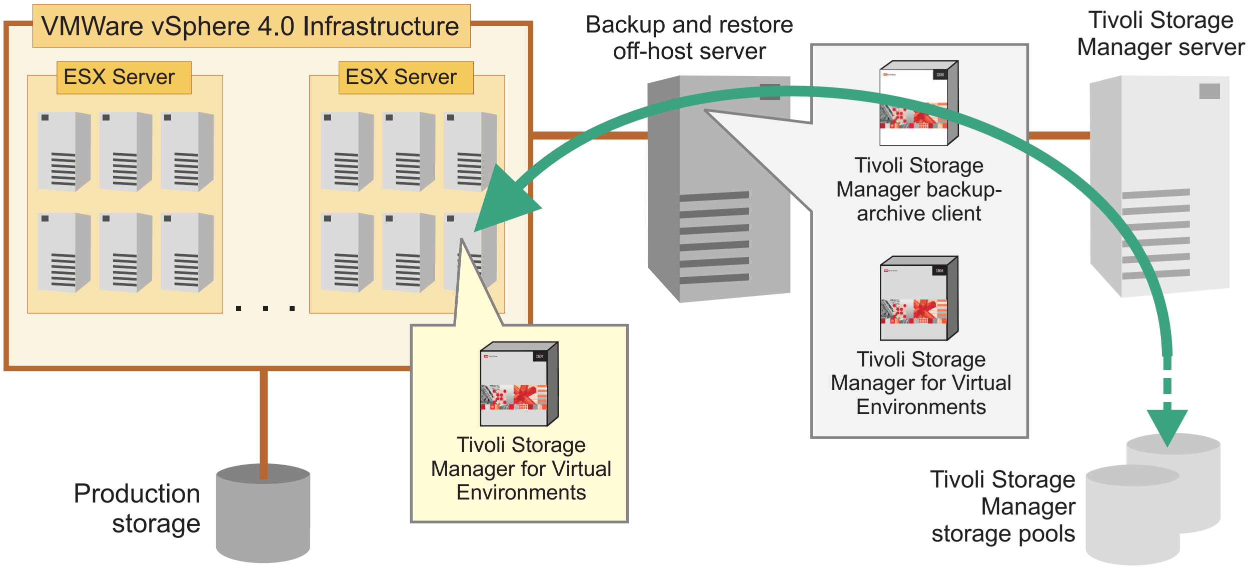
VMWare vSphere 4.0 Infrastructure
ESX Server
ESX Server
Backup and restore off-host server
Tivoli Storage Manager server
Tivoli Storage Manager backup-archive client
Tivoli Storage Manager for Virtual Environments
Tivoli Storage Manager for Virtual Environments
Production storage
Tivoli Storage Manager storage pools

Figure 5. In-guest instant restore for Windows

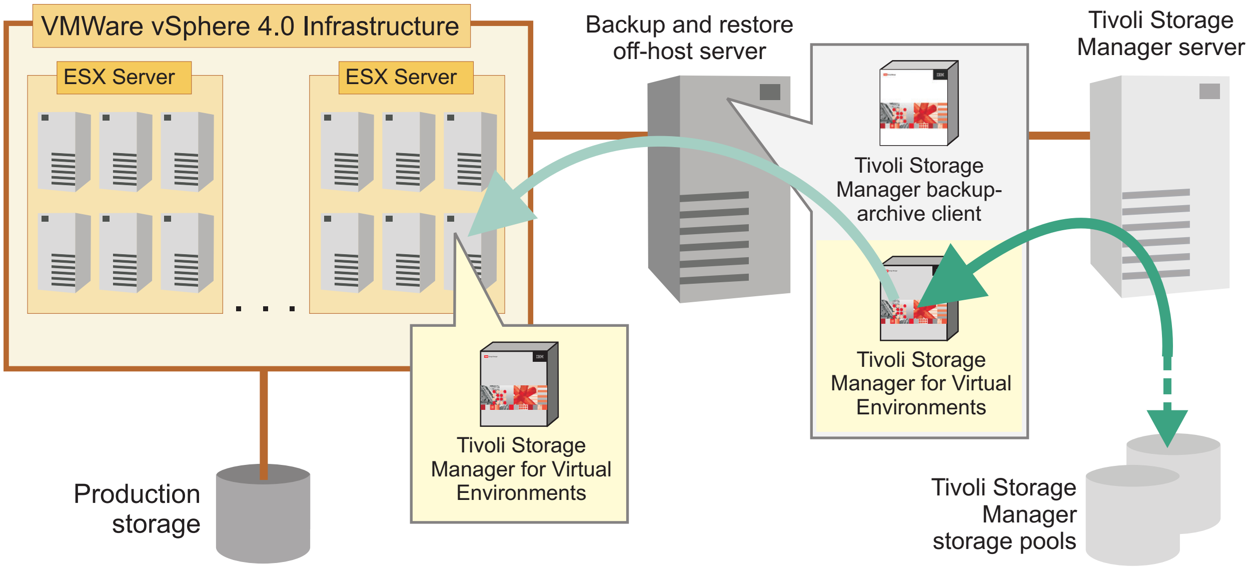
VMWare vSphere 4.0 Infrastructure
ESX Server
ESX Server
Backup and restore off-host server
Tivoli Storage Manager server
Tivoli Storage Manager backup-archive client
Tivoli Storage Manager for Virtual Environments
Tivoli Storage Manager for Virtual Environments
Production storage
Tivoli Storage Manager storage pools

Figure 6. In-guest instant restore for Linux

Off-host iSCSI target

This configuration exposes an iSCSI target from the Windows instance of the off-host Data Protection for VMware Recovery Agent and manually uses an in-guest iSCSI initiator to access the disk snapshot. This configuration requires an iSCSI initiator to be installed within the virtual machine guest. This approach exposes an iSCSI LUN, rather than the off-host file-level restore for Windows and Linux, which expose an individual disk partition.

In this configuration, the mount process specifies the virtual machine guest iSCSI initiator name. After a disk snapshot has been mounted, it can be discovered and logged in to by using the iSCSI initiator in the virtual machine guest. This centralized restore process would typically be initiated by a VMware administrator, Tivoli Storage Manager administrator or help desk personnel.

If you back up a virtual machine that contains GUID Partition Table (GPT) disks and want to mount the volume in the GPT disk, follow this procedure:

1. Mount the GPT disk as an iSCSI target.
2. Use the Microsoft iSCSI Initiator to log onto the target.
3. Open the Windows Disk Management to find the disk and bring it online. You can then view the volume in the GPT disk.

The data path for off-host iSCSI target device exposure is illustrated in Figure 7.

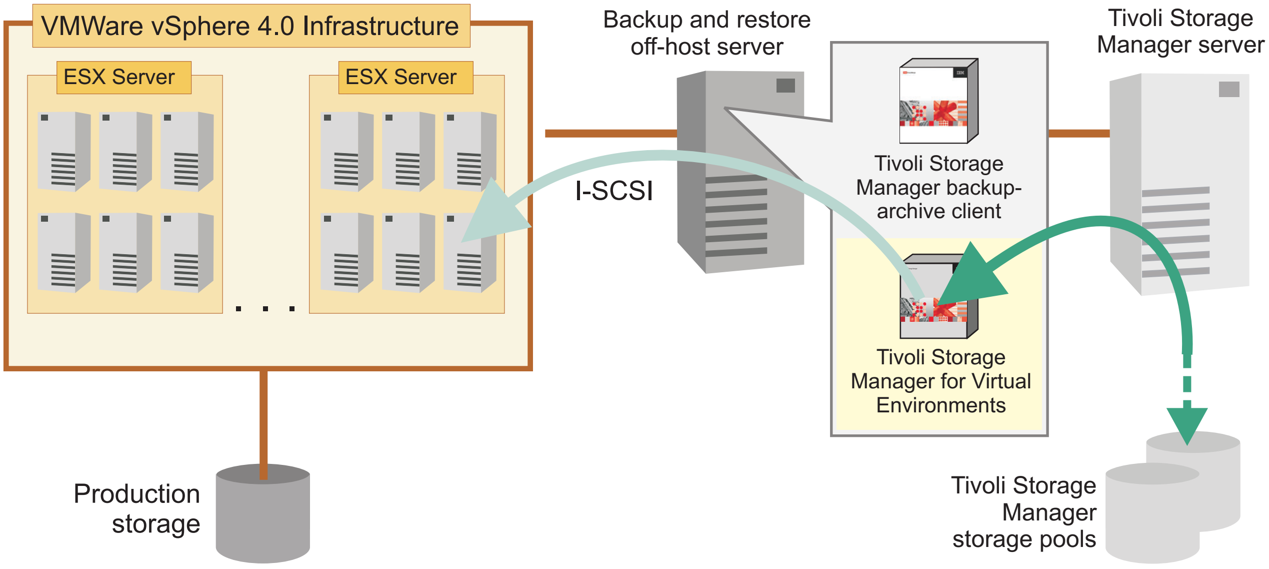
VMWare vSphere 4.0 Infrastructure
ESX Server
ESX Server
. . .
Backup and restore off-host server
I-SCSI
Tivoli Storage Manager backup-archive client
Tivoli Storage Manager for Virtual Environments
Tivoli Storage Manager server
Production storage
Tivoli Storage Manager storage pools

Figure 7. Off-host iSCSI target

Chapter 3. Installing, upgrading, and uninstalling 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 the Chapter 2, "Planning," on page 3 section. Each installation package presents you with an end user licensing file (EULA). If you do not accept the file, the installation stops.

You can install the following components:
- On Windows
  - Data Protection for VMware Recovery Agent
  - Command line
  - Documentation
  - End User Licensing Agreements
  - Data Protection for VMware enablement file
- On Linux
  - Data Protection for VMware Recovery Agent
  - Documentation
  - End User Licensing Agreements

Preparing for installation

Before you begin installation, ensure that certain prerequisites are met.
- Remove any version of IBM Tivoli Storage Manager FastBack on the server. The Data Protection for VMware installation procedure checks for the existence of Tivoli Storage Manager FastBack on the server. If found, the installation fails.
- Windows Run the installation or upgrade process from a Windows logon ID with administrator authority.
- Linux Run the installation 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.
- Linux Ensure that the file `/etc/hosts` contains this text:

  ```
  127.0.0.1 localhost
  ```

Installing Data Protection for VMware

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. Start the installation program.
   - Windows Run setup.exe for your platform.

     The default installation path for Windows is `c:\Program Files\Tivoli\TSM\TDPVMware`.

  - Linux Run install-Linux.bin for your platform. The default installation path for Linux 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 Destination Location page opens prompting you to specify where to install the software. You can accept the default location displayed in the **Destination Folder** field, type the location name, or click **Browse** to navigate to the location. Click **Next**.
7. The Installation Type page opens, prompting you to select either **Custom** or **Complete**. Make your selection and click **Next**.
8. If you selected **Custom**, the Select Feature page opens and presents a list of components. Select the components to be installed and click **Next**.
9. Linux The Pre-Installation Summary panel opens containing a list of the files that you can select. If you click **Install**, the installation proceeds with copying the files.
10. Windows Perform one of the following steps:
    a. If you selected **Custom** or **Complete**, the Define Data Protection for VMware Recovery Agent page opens. Enter the name of the Data Protection for VMware Recovery Agent or a static IP address.
    b. If you selected **Custom** and selected the Data Protection for VMware Recovery Agent, or if you selected **Complete**, a pop-up window notifies you of the Virtual Volume driver installation and asks you to confirm it.
    c. If you selected **Custom** and selected the Data Protection for VMware Recovery Agent, or if you selected **Complete**, a pop-up window asks that you reboot. You can reboot later.

If you restart the installation process after you have completed the initial installation, a Welcome window opens. From this window, there are three options:

- **Modify**: Use this option to select new program features or to delete installed features.
- **Repair**: Use this option to reinstall all program features installed during the previous setup.
- **Remove**: Use this option to uninstall Data Protection for VMware.

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. Open a command prompt window and go to the DVD drive.
3. To start the language pack installation process, enter the following command (where *X* represents the DVD drive letter):
   ```
   X:\LanguagePacks\Windows\setup.exe
   ```
4. Select **setup.exe** and click **OK**.
5. Follow the installation instructions contained in the prompt windows.
6. 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.
3. Run the installation process. For example, type the `./cdrom/TDPVMware/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
- Windows Command line
- Data Protection for VMware documents
- Windows Enablement file

Use the procedure for your operating system:

- "Installing Data Protection for VMware on a Windows 32-bit system in silent mode" on page 18
- "Installing Data Protection for VMware on a Windows 64-bit system in silent mode" on page 18
- "Installing Data Protection for VMware on a Linux system in silent mode" on page 19

If you use the remote desktop to perform a silent install on a Window XP system, the **Mount** icon does not appear in the task bar. To view and use the icon, you must manually restart the machine after installation is complete.

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

You can silently install Data Protection for VMware and the command line on a supported Windows 32-bit operating system:

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. In a text editor, open the `setup.iss` file.
4. Complete the following steps to edit the `setup.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 see the installation path that you are using.
   c. Locate the line that starts with the following string:
      ```
      MOUNT_IP=
      ```
   d. Update the host name or IP address to refer to the Data Protection for VMware server that you have installed and are using.
   e. Save and close the `setup.iss` file.
5. From a command prompt window, enter the following command:
   ```
   setup.exe /s /f1"<path_to_the_setup.iss_file>"
   ```
6. Restart the system.

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

You can silently install Data Protection for VMware and the command line on a supported Windows 64-bit operating system.

To perform a clean installation in the default location, 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 or for Itanium microprocessors, go to the IA64 folder.
3. From a command prompt window, use the **cd** command to change the directory to the installation folder.
4. Enter the following command:
   ```
   setup.exe /s /v"/qn REBOOT=ReallySupress"
   ```
5. Restart the system.

Performing a clean installation in a non-default location

To perform a clean installation in a non-default location, 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 or for Itanium microprocessors, go to the IA64 folder.
3. From a command prompt window, use the **cd** command to change directory to the installation folder.
4. Enter the following command:

   ```
   setup.exe/s /v"/qn REBOOT=ReallySuppress
   INSTALLDIR=\"<your_installation_directory>\""
   ```
5. Restart the system.

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

You can silently install Data Protection for VMware on a supported Linux operating system. This installation does not include the command line or the enablement file.

Tip: Before starting silent installation, update the TDPVMwareInstaller.properties file according to your requirements. Otherwise, only the Data Protection for VMware Recovery Agent is installed (by default).

1. Either download the code package or insert the Data Protection for VMware product DVD into the DVD drive.
2. Open the Linux folder, which is located in the Data Protection for VMware folder and choose one of the following installations:
   a. For the default installation, enter the following command in the command prompt window:

      ```
      ./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true
      ```
   b. For a custom installation, enter the following command into the command prompt window:

      ```
      ./install-Linux.bin -i silent -f <full path to_install.properties file>
      ```

Upgrading Data Protection for VMware

You must have administrator privileges to upgrade your Windows or Linux Data Protection for VMware. An upgrade cannot install new components. For example, if you have installed only Data Protection for VMware Recovery Agent, an upgrade cannot install the command line.

1. Download the code package.
2. 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.
3. A pop-up message displays this text: "The Existing Data Protection for VMware is going to be upgraded."
4. If you confirm the upgrade, the installer updates the 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

1. Either download the code package or insert the Data Protection for VMware DVD into the DVD drive.
2. In the Data Protection for VMware folder, go to the X86 folder.
3. In a text editor, open the `upgrade.iss` file.
4. 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.
5. From a command prompt window, enter the following command:

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

   Note: Specify an absolute path. Using a relative path can cause unpredictable results.
6. 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.

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, either go to the X64 folder, or, for Itanium microprocessors, go to the IA64 folder.
3. From a command prompt window, enter the following command:

   ```
   setup.exe /s /v"/qn REBOOT=ReallySuppress
   INSTALLDIR=\"<path_to_the_install_directory>\""
   ```

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.

1. Either download the code package, or insert the Data Protection for VMware product DVD into the DVD drive.
2. From the folder for Data Protection for VMware go to the Linux folder.
3. From a command prompt window, enter the following command:

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

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.

1. Start the upgrade process:
   - **Windows:** Either run the `setup.exe` file, or select **Add or Remove Programs** from the Windows Control Panel.
   - **Linux:** Run the `install-Linux.bin` file.
2. A screen opens. Select **Modify**, **Repair**, or **Remove**
3. Select **Remove**. Data Protection for VMware is completely uninstalled.

4. 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 for a Windows 32-bit system in silent mode

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

1. In the installation directory for Data Protection for VMware, go to the X86 folder.
2. From a command prompt window, enter the following command:

   ```
   setup.exe /s /f1"
   <full absolute path_to_the_uninstall.iss_file and uninstall.iss>
   ```
3. Restart the system.

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

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

1. In the installation directory for Tivoli Storage Manager FastBack, go to the X64 folder, or, for Itanium microprocessors, go to the IA64 folder.
2. From a command prompt window, enter the following command:

   ```
   setup.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL"
   ```
3. Restart the system.

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, the type of uninstallation depends on the type of installation. For example, if you used a silent install process, you must run a silent uninstall process. 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.

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

     ```
     ./ Uninstall_IBM\ Tivoli\ Storage\ Manager\ for\ Virtual\ Environments\ Data\
      Protection\ for\ VMware –I swing
     ```
   - To use the console to uninstall Data Protection for VMware, enter this command: .

     ```
     / Uninstall_IBM\ Tivoli\ Storage\ Manager\ for\ Virtual\ Environments\ Data\
      Protection\ for\ VMware -i console
     ```
   - To silently uninstall Data Protection for VMware, enter this command

     ```
     ./ Uninstall_IBM\ Tivoli\ Storage\ Manager\ for\ Virtual\ Environments\ Data\
      Protection\ for\ VMware -i silent
     ```

Chapter 4. Starting and configuring Data Protection for VMware

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

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.

Windows 2008 and Vista only: When you start Data Protection for VMware Recovery Agent from the Windows Start menu, the service is automatically stopped. When Data Protection for VMware Recovery Agent, started from the Start menu finishes, the service starts automatically.

Configuration and log files

Configuration files are needed for Data Protection for VMware to run correctly. Do not edit any of the configuration files.

Windows In the Windows operating system, logs are placed as follows:

Windows 2003 and XP: `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\tdpvmware\`

Windows Vista and 2008: `C:\Documents and Settings\All Users\Program Data\Tivoli\TSM\tdpvmware\`

In these paths there are subdirectories with a folder for each Data Protection for VMware service. For example, the subdirectories contain folders labeled `mount` and `shell`.

Linux In the Linux operating system logs are placed in `<user.home>/tivoli/tsm/ve/mount/log`. In addition, logs are placed in `/opt/tivoli/tsm/TDPVMware/mount/engine/var`

The log file with the most recent data is stored in the log file with the *040* number. 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.

Note: Although log files have extensions of "*.sf", they are plain text files.

Chapter 5. Backing up VMware virtual machine data

Windows

You can back up a VMware guest by using a full VMware backup.

The full VM backup method can back up any VMware guests that are supported by VMware. If you have Data Protection for VMware and are using the VStore API backup method, you can recover individual files, have a single source full VM backup, run incremental block level backups, and perform instant restore of volumes. For example:

```
backup vm my_vm -mode=incremental
```

If the VMware client is using Tivoli Storage Manager version 6.2.3 or later, you can use the VStorage API to run a full backup.Data Protection for VMware is not a requirement for this feature. The VStore API offers the following features:

- Backing up VMware guests do not use as a temporary directory. Therefore, the Vstore API does not use as much storage on the off-host backup server.
- If you have Data Protection for VMware, you can restore individual files.
- If you have Data Protection for VMware, you can run incremental backups after running an initial full backup.
- If a backup was created using the Vstore API, you can restore the backup without using the VMware Converter tool.

Scenario: Backing up your virtual machines

Windows

Schedule full and incremental backups to protect your virtual machine. This scenario guides you through the recommended settings for your VMware guests and the Tivoli Storage Manager client to implement VMware backups.

In this scenario, you define a full VMware backup of the guests that runs once a week and a daily incremental backup of the same VMware guests. This configuration ensures that there are frequent backups of the VMware guests and reduces the size of each backup.

Tip: There is no limit to how many full and incremental backups you can take. However, if you do not run a full backup regularly, the size of incremental backups can increase. This scenario ensures that the incremental backups do not get too large.

1. Prepare the off-host server for backups. See "Preparing the environment for VMware backup processing" on page 26.
2. Define a full VM backup for each of the VMware guests. See "Running full virtual machine backups" on page 27.
3. Separate the pool of VMware guests into groups to reduce backup time. The backup time is shorter because each group is backed up by a separate instance on the Tivoli Storage Manager client scheduler, and they are running in parallel on the off-host backup server.
4. Schedule the full VM backup that runs once a week.

5. Configure daily backups using "Running incremental virtual machine backups using the VStore API" on page 28.
6. Schedule the incremental backups to run daily.
7. Specify compression and deduplication to reduce the backup size of the VMware backups using the following steps:
   a. From the VMware guests, open the Tivoli Storage Manager client `dsm.opt` file.
   b. Enable compression by adding the following option to the client `dsm.opt` file: `compression yes`.

      Tip: You can only enable compression if you are using client deduplication and if deduplication has been enabled for the storage pool.
   c. Enable deduplication by adding the following option to the client `dsm.opt` file: `deduplication yes`.

Preparing the environment for VMware backup processing

Windows

Use the following steps to prepare the VMware environment to be backed up.

1. Configure your storage environment so that it can be backed using the following steps:
   a. Configure your storage environment so that the proxy server can access to the storage volumes that are in your ESX server farm.

      Tip: By making the storage volumes visible, the backup uses the SAN transfer path during backup operations.
   b. If you are using network attached storage (NAS) or direct-attach storage, ensure that the backup proxy server is accessing the volumes with a network-based transport.
   c. Optional: If you will be running a direct SAN backup, zone the SAN and configure the disk subsystem host mappings so that all VMware ESX servers and the backup proxy access the same disk volumes.
2. Configure the backup proxy server using the following steps:
   a. The backup proxy server must be a Windows 2003 or Windows 2008 server.
   b. If you are configuring the backup proxy server to directly access the storage volumes, run `diskpart.exe` to disable automatic drive-letter assignment. See the VMware documentation for information about disabling automatic drive-letter assignment.

      Attention: If you do not disable automatic drive-letter assignments, the backup proxy server can corrupt the Raw Device Mapping (RDM) of the virtual disks.
   c. Install the Tivoli Storage Manager client on the backup proxy server. At the custom setup page of the installation wizard, select **VMware Backup Tools**.

      Important: If you are moving the backup data using a LAN-free network, the SAN must have separate connections for tape and disk.
3. Modify the Tivoli Storage Manager server using the following steps:
   a. Access the administrative command line of Tivoli Storage Manager client.
   b. From the Tivoli Storage Manager client of the proxy server, enter the following command to register the node:

```
register node my_server_name my_password
```

Where *my_server_name* is the full computer name of the proxy server and *my_password* is the password to access it.

Tip: You can get the server full computer name by right-clicking on **My Computer**. Click the Computer Name tab and look at the name listed next to **Full computer name**.

Running full virtual machine backups

Windows

A full virtual machine backup is a backup of an entire export of a virtual machine snapshot. It is like a Tivoli Storage Manager image backup.

The off-host VMware virtual machine must be configured as described in "Preparing the environment for VMware backup processing" on page 26.

1. Configure the backup Tivoli Storage Manager client on the off-host backup server using **Client Preferences** editor:
   a. From the welcome page of the Tivoli Storage Manager client, click **Edit** > **Client Preferences**.
   b. Click the notebook tab **VM Backup**.
   c. Select **VMWare Full VM**.
   d. In the **Domain Backup Types** list, select **Domain Full VM**.
   e. In the **Host** field, enter either the host name of the vCenter or the host name of the ESX serverr. Enter the user ID and password information.

      Note: Enter the Virtual Center host name. If you specify the Virtual Center host name, you can back up virtual machines from any of the VMware servers that are managed by the Virtual Center.
   f. In **VM Full Backup Type** section, select **VStorage**.
   g. Click **OK** to save your changes.
2. Verify that your system is configured correctly by running a backup of one of the virtual machines using the following steps:
   a. At the command line of the off-host backup server, enter the command:
      ```
      dsmc backup vm my_vm_name
      ```
      where *my_vm_name* is the name of your virtual machine as seen in the VMware vSphere client.
   b. When the command ends, verify that it completed without errors. The following message indicates that the command completed successfully:
      ```
      Backup VM command complete
      Total number of virtual machines backed up successfully: 1
      virtual machine vmname backed up to nodename NODE
      Total number of virtual machines failed: 0
      Total number of virtual machines processed: 1
      ```
3. Verify that you can restore the virtual machines files using the following steps:
   a. At the command-line interface of the off-host backup server, enter the command:
      ```
      dsmc restore vm my_vm_name -vmbackuptype=fullvm
      ```

   b. If there are any restore processing failures, view the Tivoli Storage Manager error log for more information.

      Tip: The log file is saved to `c:\Program Files\Tivoli\TSM\baclient\dsmerror.log`

Running incremental virtual machine backups using the VStore API

Windows

An incremental backup stores the files that have changed since the last full backup.

Tip: There is no limit to how many full and incremental backups you can take. However, if you do not run a full backup regularly, the size of incremental backups can increase. This scenario ensures that the incremental backups do not get too large.

1. Start the backup of a VM using the following steps:
   a. Open the backup-archive command line.
   b. At the command line, enter the following command:

      ```
      backup vm myVMname -vmbackuptype=fullvm -mode=Incremental
      ```

      where *myVMname* is the name of the virtual machine you are backing up. The backup process starts and displays the progress of the backup. The backup is complete when the following results are displayed:

      ```
      Backup VM command complete
      Total number of virtual machines backed up successfully: 1
        virtual machine myVMname backed up to nodename NODE
      Total number of virtual machines failed: 0
      Total number of virtual machines processed: 1
      ```

2. Verify that you can restore the virtual machines files using the following steps:
   a. At the command-line interface of the off-host backup server, enter the command:

      ```
      dsmc restore vm my_vm_name -RESTORED
      ```

   b. If there are any restore processing failures, view the Tivoli Storage Manager error log for more information.

      Tip: The log file is saved to `c:\Program Files\Tivoli\TSM\baclient\dsmerror.log`

Restoring full VM backups

Windows

You can restore a full VMware backup to recreate all of the files of a VMware guest.

You can restore the backup files directly to the VMware server. The restore procedure is different than using the VMware Consolidated Method tools that required you to restore the files to the off-host backup server and use the VMware converter tool before you could restore it to the VMware server.

1. If the full-VM that you are restoring will replace the existing VMware guest, delete the existing full-VM guest before you restore.

Tip: If you restore the full VM backup to a new VMware guest, you do not need to delete the original.

2. Query the Virtual Machine for full VMware backups using the following steps:
   a. From the off-host backup server, enter the following command:

      ```
      dsmc q vm *
      ```

      The command lists the backups like the following screen:

      ```
        #       Backup Date       Mgmt Class           Type   A/I Virtual Machine
      ---       -----------     ----------           ----   --- ---------------
        1   12/03/2009 03:05:03   DEFAULT              VMFULL  A  vm_guest1
        2   09/02/2010 10:45:09   DEFAULT              VMFULL  A  vm_guest11
        3   09/02/2010 09:34:40   DEFAULT              VMFULL  A  vm_guest12
        4   09/02/2010 10:10:10   DEFAULT              VMFULL  A  vm_guest13
        5   12/04/2009 20:39:35   DEFAULT              VMFULL  A  vm_guest14
        6   09/02/2010 11:15:18   DEFAULT              VMFULL  A  vm_guest15
        7   09/02/2010 02:52:44   DEFAULT              VMFULL  A  vm_guest16
        8   08/05/2010 04:28:03   DEFAULT              VMFULL  A  vm_guest17
        9   08/05/2010 05:20:27   DEFAULT              VMFULL  A  vm_guest18
       10   08/12/2010 04:06:13   DEFAULT              VMFULL  A  vm_guest19
       11   09/02/2010 00:47:01   DEFAULT              VMFULL  A  vm_guest7
       12   09/02/2010 01:59:02   DEFAULT              VMFULL  A  vm_guest8
       13   09/02/2010 05:20:42   DEFAULT              VMFULL  A  vm_guest9
      ANS1900I Return code is 0.
      ANS1901I Highest return code was 0.
      ```

   b. View the output to identify the VMware that you are restoring.
3. Restore the full VMware backup by entering the following command:

   `dsmc RESTORE VM -vmname=my_vmname -datacenter=my_datacenter -host=my_hn -datastore=myPath`See the following parameters to see what you need to substitute for your environment.

   my_vmname
      This is the display name of the virtual machine

   my_datacenter
      This is the name of the MVware datacenter that is defined to the vSphere vCenter.

   my_hn
      This is the ESX host server name that is defined to the vCenter datacenter.

   myPath
      This is the full path location and file name of the volume data and configuration files for the VM backup that you are restoring. You can enter SAN, local storage NAS or iSCSI formatted file paths as defined in vSphere vCenter Datacenter.
4. When the restore is complete, the virtual machine is powered off. Start the virtual machine from the VMware vCenter to use it.

Backup VM

Windows

Use the **backup vm** command to run a full backup of a specified virtual machine.

The **backup vm** command is used to back up VMware virtual machines from the off-host backup of VMware virtual machine data proxy system..

VMware backup

To specify the name of the virtual machine or to list the virtual machine names for a VMware backup, use the domain.vmfull option. If no vmname is specified on the command, use the domain.vmfile or domain.vmfull options.

You can run a full VM backup, that stores a backup copy of complete virtual disk images and configuration information of a virtual machine. Full VM backup enables a complete restore of the complete virtual machine.

You can also specify the -mode option to run an incremental or full backup when you use the full VM backup option. File level VM backup provides individual file restore within the virtual machine and incremental backup, although it does not have an easy full machine recovery procedure.

You might want to use a combination of file level VM backups with periodic full VM backups for optimal results.

Tip: You can only use the compression option with the VSTORE full vm backup if the backup is being saved to a storage pool that has been enabled for deduplication.

Supported Clients

This command is valid for Windows that are configured as an off-host backup of VMware virtual machine data proxy.

Syntax

```
►►──Backup VM──┬────────┬──┬─────────┬──────────────────────────────────────►
               └─VMNAME─┘  └─options─┘

►──┬──────────────────────────────────────────────────┬─────────────────────►
   │                        ┌─-mode=Full────────┐     │
   └─-vmbackuptype=fullvm───┤                   ├─────┘
                            └─-mode=Incremental─┘

►──┬──────────────────────────────┬──┬──────────────────────┬─────────────►◄
   │                 ┌─VCB───┐    │  └─VMMC──{class_name}───┘
   └─-vmfulltype=────┤       ├────┘
                     └─VSTOR─┘
```

Parameters

Table 5. Backup VM command: Related options

Option	Where to use
vmname	Command line
domain.vmfile	Command line or `dsm.opt`
domain.vmfull	Command line or `dsm.opt`
mode	Command line or `dsm.opt`
vmbackdir	Command line or `dsm.opt` This option is only supported if you set `-vmfulltype=VCB`

Table 5. Backup VM command: Related options (continued)

Option	Where to use
vmbacknodelete	Command line or `dsm.opt` This option is only supported if you set `-vmfulltype=VCB`
vmbackuptype	Command line or `dsm.opt`
vmfulltype	Command line or `dsm.opt`. This option only applies if you specify the option `vmbackuptype=fullvm`.
VMMC	Command line or `dsm.opt`. This option only supported if you specify the option `vmbackuptype=fullvm` or `vmfulltype=vstor`.
vmbackvcbtransport	Command line or `dsm.opt`
vmchost	Command line or `dsm.opt`
vmcpw	Command line or `dsm.opt`
vmcuser	Command line or `dsm.opt`

VMware examples

VStore API example commands:

```
dsmc backup vm vm1 -vmbackuptype=file
```

```
dsmc backup vm vm3,vm4 -vmbackuptype=fullvm
```

```
dsmc backup vm vmlocal -vmbackuptype=fullvm
```

To run a file-level virtual machine backup of `vm1.example.com` using the VMware VirtualCenter machine `virtctr.example.com`, see the following example:

```
dsmc backup vm vm1 -vmbackuptype=file -vmchost=virtctr
```

Chapter 6. Restoring virtual machine data

With Data Protection for VMware, you can perform file-level restore and instant restore of virtual machine data.

- "Mounting snapshots"
- "Restoring files and instant restore of volumes" on page 34
  - "Restoring files (Windows)" on page 36
  - "Using instant restore (Windows)" on page 37
  - "File level restore and instant restore (Linux)" on page 38

Mounting snapshots

You can use Data Protection for VMware Recovery Agent to mount a snapshot and use the snapshot to complete data recovery.

Data Protection for VMware Recovery Agent must be installed and operated from a system that is connected to the Tivoli Storage Manager server through a LAN. You can use Data Protection for VMware Recovery Agent from either its graphical user interface or from the command line.

Data Protection for VMware Recovery Agent on Windows

Data Protection for VMware Recovery Agent can be installed and operated from the following Windows operating systems:

Windows 2003 Service Pack 1 or later

- Supports the x86 (32-bit) and x64 (AMD64 and EM64T) instruction set architecture.
- Supports 32-bit and 64-bit processors.

Windows 2003 64-bit Edition

- Supports the x64 (AMD64 and EM64T) instruction set architecture.
- Supports 64-bit processors.

Windows 2008 Service Pack 1 or later

- Supports the x86 (32-bit), x64 (AMD64 and EM64T) instruction set architecture.
- Supports 32-bit and 64-bit processors.

Windows 2008 R2 or later

- Supports the x86 (32-bit) and x64 (AMD64 and EM64T) instruction set architecture.
- Supports 32-bit and 64-bit processors.

Windows XP Professional Edition, Service Pack 2 or later

- Supports the x86 (32 bit) instruction set architecture.
- Supports 32-bit processors.

Windows Vista Service Pack or later

- Supports the x86 (32-bit) and x64 (AMD64 and EM64T) instruction set architecture.

- Supports 32-bit and 64-bit processors.

Note: Data Protection for VMware Recovery Agent can use only snapshots that were created by a Tivoli Storage Manager client V6.2.3 or later.

For systems that run Windows Vista or Windows 2008, Data Protection for VMware Recovery Agent can run in the following two modes:

- When no users are logged in, Data Protection for VMware Recovery Agent runs as a service. The Data Protection for VMware Recovery Agent service enables remote connections through the command line.
- When a user is logged in, Data Protection for VMware Recovery Agent continues to run as a service until you start the Data Protection for VMware Recovery Agent application and use the graphical user interface. When you close the Data Protection for VMware Recovery Agent application and graphical user interface, the Data Protection for VMware Recovery Agent service restarts.

  To start Data Protection for VMware Recovery Agentfrom the Windows Start menu, select **All Programs** > **Tivoli Storage Manager** > **Data Protection for VMware** > **Data Protection for VMware Recovery Agent**.

  You can use only the Data Protection for VMware Recovery Agent application and graphical user interface when running with administrator login credentials. Only one copy of the Data Protection for VMware Recovery Agent application can be active at any time.

Snapshots can be mounted in either read-only or read/write mode. In read/write mode Data Protection for VMware Recovery Agent saves changes to data in RAM.

Note: If the service is restarted, the changes are lost.

Data Protection for VMware Recovery Agent on Linux

Data Protection for VMware Recovery Agent can be installed and operated from any Red Hat Enterprise Linux 5.2, 5.3, 5.4 Server or SuSE Linux Enterprise Server 10 SP2 system. Instructions for using Data Protection for VMware Recovery Agent on Linux are available at “File level restore and instant restore (Linux)” on page 38

Restoring files and instant restore of volumes

With the stored snapshots, you can recover data that is backed up. You can restore files and perform the instant restore of volumes.

Note: Do not attempt to change a Tivoli Storage Manager node password while running a file level restore or an instant restore from snapshots stored in that node. The results are unpredictable.

Restoring files

Administrators can use Data Protection for VMware Recovery Agent for efficient file level restores and to minimize downtime by mounting snapshots to virtual volumes.

The virtual volume can be viewed by using any file manager, for example Windows Explorer. The directories and files in the snapshot can be viewed and managed like any other file. If you edit the files and save your changes, after you unmount the volume, your changes are lost because the changed data is held in memory and never saved to disk. Because the changes are written to memory, Data Protection for VMware Recovery Agent can use a large amount of RAM when working in read/write mode.

You can copy the changed files to another volume before performing an unmount. You can select *read only* as a mounting option.

Data Protection for VMware Recovery Agent mounts snapshots from the Tivoli Storage Manager server.

Data Protection for VMware Recovery Agent can be used for the following tasks:
- Recovering lost or damaged files from a backup
- Mounting a virtual machine guest volume and creating an archive of the virtual machine guest files
- Mounting database applications for batch reports

From the Data Protection for VMware user interface, you must first dismount any snapshots before you click **Remove**. The remove operation fails if there are active mount and restore sessions in the Linux or Windows Mount machines. You cannot remove the connection to server when you are performing a file restore or an instant restore from that server. You must first dismount all virtual devices and stop all instant restore sessions before you disconnect from a server. If you do not do so, the connection is not removed.

To use Data Protection for VMware Recovery Agent for file-level recovery of data that is stored on tape, it is recommended that the data be moved to disk or file storage. From Tivoli Storage Manager, you can use the **QUERY OCCUPANCY** command to see where the data is stored. You can then use the **MOVE NODEDATA** command to move this data back to disk or file storage. For more information about these commands, see the Tivoli Storage Manager Information Center: http://publib.boulder.ibm.com/infocenter/tsminfo/v6r2/index.jsp

Copying files from a mounted snapshot tape storage pool performs more slowly than does a snapshot that is on disk. It might take less time to move the backup data for a virtual machine from tape to disk before performing a file restore. In such cases, you would use the **MOVE NODATA** command with the FILESPACE option. This approach might be better for including file restore if there are many files on a badly fragmented volume.

Instant restore

You can use instant restore to use data on a volume that is being restored, while the restore operation is in progress. For this reason, less downtime is required before a recovered volume can be used.

Instant restore works only with local volumes. Local volumes must have an assigned drive letter.

You can complete an instant restore of a volume in a supported clustered environment. While instant restore process is running, you can access the volume. Other volumes in the cluster should not be affected, and you can work with the cluster, and with that volume, in parallel. During the instant restore, the disk being restored cannot fail over if the node fails.

If a system is shut down while instant restore is in progress, the instant restore automatically continues from the same point when power is restored.

Instant restore destination volumes must be either on basic disks, or simple volumes on dynamic disks. Destination volumes cannot be spanned volumes, mirrored volumes, or RAID-5 volumes. You can use a basic disk as a destination volume and then convert the basic disk to a dynamic disk.

Restoring files (Windows)

You can use Data Protection for VMware Recovery Agent for efficient file level recovery and to minimize downtime by mounting snapshots to virtual volumes. On supported Windows operating systems, file-level recovery is supported from snapshots of NTFS, FAT, or FAT32 volumes.

To run a file level recovery for a Windows system, complete the following steps:

1. Log on to the system where you want to restore files. Data Protection for VMware Recovery Agent must be installed on the system.
2. Start Data Protection for VMware Recovery Agent
   - **For Windows Vista and Windows 2008 only:** Select **All Programs** > **Tivoli Storage Manager** > **Data Protection for VMware** > **Data Protection for VMware Recovery Agent**
   - **For all other supported Windows systems:** From the Microsoft Windows taskbar area, click the Data Protection for VMware Recovery Agent icon.
3. Connect to a Tivoli Storage Manager server by specifying the server address, port, node, and password. If the Tivoli Storage Manager administrator has created a proxy node and has granted it proxy authority to the backup node, this node can be used in an 'asnode' parameter, if you do not want to expose the password of the individual backup node.

   Data Protection for VMware Recovery Agent queries the specified server for a list of protected virtual machines, and displays the list.
4. Select a virtual machine from the list. Data Protection for VMware Recovery Agent queries the server for a list of snapshots available for the specified virtual machine.
5. Select the required snapshot by selecting the date and disk and click **Mount**.
6. In the Mount Destination dialog, check Mount the Following Partition. Data Protection for VMware Recovery Agent displays a list of partitions available on the selected disk. For each partition, its size, label, and file system type are displayed. If the disk is not MBR-based, an error message is displayed. By default, only partitions that can be used for file-level restore are displayed. To display all partitions that existed on the original disk, clear the **Show only mountable partitions** check box, and them take the following steps:
   a. Select the required partition. Partitions formatted using unsupported file systems cannot be selected.
   b. Specify a drive letter or an empty folder as a mount point for the virtual volume.

   Data Protection for VMware Recovery Agent verifies that the data for the selected snapshot available and the target is created.
7. If the device is an iSCSI disk, use the iSCSI initiator to discover and log on to the iSCSI target. You can view and copy files from the target.

Using instant restore (Windows)

With instant restore, you can restore a volume and almost immediately use the restored volume. Less downtime is required before a recovered volume can be used because, you can use data on the disk while the restore is in progress.

Instant restore is available only from VMWare full snapshots of disks of the MBR type. The volume format of volumes on those disks must be NTFS, FAT, or FAT32.

- Restoring a volume involves overwriting data on the existing storage volume. After the restore begins, the current volume contents are permanently erased. Before you start the restore, verify that the correct volume is selected, and that there are no open handles or processes by using that volume.
- The restore operation fails if there are open files or applications that are running on the target restore volume. Selecting **Ignore open handles on the destination volume** causes Data Protection for VMware to ignore the open files and applications that are running on the destination volume. This situation can cause a problem with applications and loss of data in files that are open on the target volume.

To perform an instant restore, complete the following steps:

1. Start Data Protection for VMware Recovery Agent.
   - **For Windows Vista and Windows 2008 only:** Select **All Programs** > **Tivoli Storage Manager** > **Data Protection for VMware** > **Data Protection for VMware Recovery Agent**
   - **For all other supported Windows systems:** From the Microsoft Windows taskbar area, click the Data Protection for VMware Recovery Agent icon.
2. In the Data Protection for VMware Recovery Agent window, select the Tivoli Storage Manager server to use as the source. Data Protection for VMware Recovery Agent queries the Tivoli Storage Manager server for a list of protected virtual machines and displays the list.
3. Select the required snapshot by choosing a date, a time, and a disk and click **Restore**.
4. Data Protection for VMware Recovery Agent displays a list of partitions available on the selected disk. For each partition, its size, label, and file system type are displayed. Select the required partition. By default only partitions that can be restored are displayed. To display all the partitions that are available on one or more disks, clear the **Show only restorable partitions** check box. Select the required partition from the list.

   Note: Drive letters are not displayed.
5. Select the destination partition into which the data is to be restored. Data Protection for VMware Recovery Agent verifies that the data for the selected snapshot is available.
6. Click **Restore**.
7. A confirmation message is displayed. Verify the information and click **Yes**. The restore process begins. In the instant restore section, you can see the status of the restore process. When the status changes to restoring, the volume is available for use.

Use the **Max CPU** slider to adjust the processor usage for the restore process.

To cancel the restore process, select the instant restore session that is in progress and click **Abort**. All data on the target drive is lost. You can click **Abort All** to cancel all processes. If you stop an instant restore without clicking **Abort** or **Abort**

all, the restored volume is displayed as a valid volume, but the data on the volume is invalid. The data is invalid because the data was partially restored, but the restore process did not have time to complete, and the shutdown was abnormal.

If the service is stopped while instant restore is running, the volume appears to be a valid volume. Trying to access the area of the volume that is not yet restored fails, and the data appears corrupted. After the service restarts, the restore process continues, and the data appears valid. If a power failure occurs during instant restore, after the machine boots up, and the volume appears to be unformatted. After the service starts, the instant restore process resumes, and the volume appears valid.

A temporary problem might prevent the session from running. For example, a network problem might cause a temporary loss of access to the Tivoli Storage Manager server. In that case, the instant restore session pauses. To continue to the restore process after the pause, select the appropriate line in the instant restore list and click **Resume**.

You can use instant restore to restore a simple volume on a dynamic disk. This restore might cause the disk status to change to *Online (Errors)* and the status of all volumes on the disk to change to *At Risk*. This change in disk status can occur when network traffic is too heavy for instant restore to operate. In this situation, the volumes are online and mounted. You can return the disk and volume status to normal by going to the Computer Management Console. Right-click the disk; then, click **Reactivate Disk**.

File level restore and instant restore (Linux)

Data Protection for VMware Recovery Agent on Linux is used to restore individual files (file level restore) or volumes (instant restore). Unlike a conventional volume restore, instant restore provides access to volume contents while the restore process is in progress. Less downtime is required before a recovered volume can be used. After you start an instant restore, you can use data on the disk while the restore is in progress.

Configuring Data Protection for VMware Recovery Agent for restore operations (Linux)

Data Protection for VMware Recovery Agent requires specific application settings, environment conditions, and configuration tasks be completed before attempting a restore operation.

These environment requirements must exist before using Data Protection for VMware Recovery Agent on Linux:

- The Tivoli Storage Manager command line must be available on a Windows computer.
- Data Protection for VMware Recovery Agent is available on a Windows system. This system must be accessible from the computer where the command line is installed. Alternatively, Data Protection for VMware Recovery Agent and the command line can be installed on the same computer.
- Data Protection for VMware Recovery Agent must be able to access the IBM Tivoli Storage Manager storage pool. Data Protection for VMware Recovery Agent exposes snapshots as iSCSI targets. Therefore, the snapshots must be accessible to the target Linux machine.

- For the iSCSI to work for Linux mount and restore operations, the iSCSI port must be open on any firewall between the machine running Windows mount, the iSCSI target and the machine performing the restore, the iSCSI initiator. The iSCSI default port is 3260.
- Ensure that your environment consists of all prerequisite applications.
- When performing an instant restore, Data Protection for VMware Recovery Agent saves changes to data on a virtual volume in the write cache. The write cache is enabled by default. The path is `C:\Documents and Settings\All Users\Application Data\Tivoli\TSM\tdpvmware\mount`, and the size is set to a maximum of 90% of the available space. These settings can be configured by clicking settings in the main Data Protection for VMware Recovery Agent window. The write cache must be located on a local drive and cannot be set to a path on a shared folder. You cannot enable or disable the write cache from the UI or form configuration files. You can specify the write cache location in a non-system folder on a local disk.
- In order to prevent the recovery process from mounting the device, stop the cron daemon. For example:

  RedHat
  ```
  /etc/init.d/cron stop
  ```
  SUSE
  ```
  /etc/init.d/cron stop
  ```

  Start the cron daemon when the processing completes.

This task guides you through configuration steps required to use Data Protection for VMware Recovery Agent.

1. Log on to the Linux system with root user authority. Data Protection for VMware Recovery Agent must be installed on this Linux system.
2. Start Data Protection for VMware Recovery Agent by clicking the Data Protection for VMware Recovery Agent icon on the desktop or running a script from the shell prompt. The first time you access Data Protection for VMware Recovery Agent, the Settings dialog displays. You must enter the following configuration information to proceed:
   - Command line
     a. Enter the host name or IP address of the computer where the command line is installed.
     b. Enter the login ID that is used for the Secure Shell (SSH) user.

        Tip: This login ID is for the Windows system where both the command line and SSH are installed. This system uses SSH to communicate with Data Protection for VMware Recovery Agent on the Linux system. Make sure this login ID uses a host name convention defined in the SSH known_hosts file.
   - **Data Protection for VMware Recovery Agent** Enter the host name or IP address of the Windows system where Data Protection for VMware Recovery Agent is installed. Click **OK** to save these values and return to the Data Protection for VMware Recovery Agent window.
3. Use the Select a Tivoli Storage Manager server drop-down menu to identify the server to use as the source. The Tivoli Storage Manager must already be configured and accessible to Data Protection for VMware Recovery Agent.
   - Enter the following information:
     - **Input TSM server address**
       a. Enter the IP address or host name of the Tivoli Storage Manager.

   b. Enter the port number used for TCP/IP communication with the server.
  - **Input TSM server credentials**
    a. Enter the node name used to access the Tivoli Storage Manager server.
    b. Enter the password associated with the node name.
    c. (Optional) Enter the asnodename. This name is like the node name entered previously. However, the asnodename provides proxy authority for your Linux system to back up and restore data to the Tivoli Storage Manager server.
4. Click **OK** to save these values and return to the Data Protection for VMware Recovery Agent window.
5. Click **Refresh** to display the most current data from the Tivoli Storage Manager server.

Data Protection for VMware Recovery Agent is now properly configured and ready for restore operations. Use Data Protection for VMware Recovery Agent to accomplish a file level restore or an instant restore operation.

File-level restore (Linux)

Be aware of these considerations before attempting a file-level restore on Linux:

- The tasks described in "Configuring Data Protection for VMware Recovery Agent for restore operations (Linux)" on page 38 must be completed before attempting a file level restore.
- This procedure assumes that you are logged on to the Linux system with root user authority and the Data Protection for VMware Recovery Agent GUI is available.
- SUSE Linux Enterprise Server 10 requires all iSCSI devices to be unmounted before rebooting or shutting down the system.

This task describes how to use Data Protection for VMware Recovery Agent to restore a snapshot volume (file level) on a Linux system.

1. Identify the Tivoli Storage Manager server where the snapshots are stored. Specify the server address, port, node, and password. Data Protection for VMware Recovery Agent queries the server for a list of protected virtual machines and displays the list.
2. Select a virtual machine from the list. Data Protection for VMware Recovery Agent queries the server for a list of snapshots available for the specified virtual machine.

   Tip: To quickly locate the required virtual machine from the available virtual machine list, type the first few letters of the virtual machine name.
3. Select the required snapshot by selecting the date and disk. Data Protection for VMware Recovery Agent displays a list of partitions available on the selected disk. For each partition, size, label, and file system type are displayed. By default, only mountable partitions are displayed. To display all partitions, clear the **Show only mountable partitions** check box.

   Note: Drive letters are not displayed.
4. Select the required partition.
5. Select the destination partition into which the data is to be restored, and specify the mount point as the target.

Tip: The mount point identifies a volume.

6. Click **OK** to start the file level restore.

After the mount process is completed successfully, a new entry is displayed in the **Mounted Volumes** field. For example:

```
/mnt is mount of [tsm-ba-1@tsm-ve-1]-[vm-1]-[2010-Mar-24
10:10:10]-[Hard Disk 1]-[Partition 0]
```

Instant restore (Linux)

Before attempting an instant restore on Linux review the following information:

- Multiple instant restore sessions to different target disks run in parallel. However, multiple instant restore sessions to different target partitions on the same disk do not run in parallel. As a result, the first instant restore session must complete before the next Instant Restore session begins.
- The tasks described in "Configuring Data Protection for VMware Recovery Agent for restore operations (Linux)" on page 38 must be completed before attempting an instant restore.
- This procedure assumes that you are logged on to the Linux system with root user authority and that the Data Protection for VMware Recovery Agent graphical user interface is available.
- SUSE Linux Enterprise Server 10 requires all iSCSI devices to be unmounted before rebooting or shutting down the system.
- Instant restore to LVM partitions is not supported.

This task guides you through how to use Data Protection for VMware Recovery Agent to restore a snapshot volume (instant restore) on a Linux system.

1. Identify the Tivoli Storage Manager server where the snapshots are stored. Specify the server address, port, node, and password. Data Protection for VMware Recovery Agent queries the server for a list of protected virtual machines and displays the list.
2. Select a virtual machine from the list. Data Protection for VMware Recovery Agent queries the server for a list of snapshots available for the specified virtual machine.

   Tip: To quickly locate the required virtual machine from the available virtual machine list, type the first few letters of the virtual machine name.
3. Select the required snapshot by selecting the date and disk. Data Protection for VMware Recovery Agent displays a list of partitions available on the selected disk. For each partition, its size, label, and file system type is displayed. By default, only restorable partitions are displayed. To display all partitions, clear the **Show only restorable partitions** check box.

   Note: Drive letters are not displayed.
4. Select the required partition.
5. Select the destination partition into which the data is to be restored, by selecting either a mount point or a block device. If you specify both, ensure that the block device is mounted on the specified mount point.
6. Click **OK**. The restore process starts. After a short initialization period, the volume is available for use while the restore process runs in the background and until the volume is completely restored.

Restoring to the same volume again:

If you plan to restore another snapshot into the same target volume, complete one of the following steps:

- Restart the Linux system.
- Manually stop the mirror device and mount the restored volume.

  For example, in the following procedure `sdc1` is the target block device and `md0` is the mirror device:

  1. Issue the command: `umount /dev/md0`.
  2. Issue the command: `mdadm --stop /dev/md0`.
  3. Issue the command: `mount /dev/sdc1 /restoredVolume`.

Checking the file system

After the instant restore completes, you can verify the file system restored volume by using the `fsck` file system utility:

1. Unmount the RAID device by issuing this command: `umount /dev/md0`
2. Type in the `fsck` command to run the file system check.

Chapter 7. Command line interface

The command line lets you access most Data Protection for VMware functions. The command line can be viewed as a command-line API to theData Protection for VMware Recovery Agent. Changes completed with the command line to the Data Protection for VMware Recovery Agent take effect immediately.

You can use the command line to manage only one system running theData Protection for VMware Recovery Agent.

Starting the command line

Before you can start and use the command line from a supported Linux operating system, you need to complete the software prerequisites detailed in “Software requirements and prerequisites” on page 6.

To start the command line, complete the following steps:

1. From the Windows Start menu, select **Programs** > **Tivoli Storage Manager** > **Data Protection for VMware** > **Command Line**.
2. In the command prompt window, enter one of the following commands:
   - To run the command line:

     ```
     TDPVMareShell.exe -c command type tag parameter
     ```

   - Windows To display the help for the command line:

     ```
     TDPVMareShell.exe -h
     ```

   - Linux To display the help for the command line:

     ```
     TDPVMareShell.exe -h dump
     ```

     For example, this command displays detailed help for the mount command line:

     ```
     TDPVMareShell.exe -h mount dump
     ```

Command line overview

When you use the commands, some parameters are not required. See the following sections for details regrading required parameters.

For the parameters that are not required and not entered, default values are used. Parameters with spaces must be enclosed in quotation marks. For example, if you want to use the *Accounting, Daily* parameter, type "Accounting, Daily".

To read a syntax diagram for entering a command, follow the path of the line. Read from left to right, and from top to bottom, and use the following guidelines:

- The `>>-` character sequence indicates the beginning of a syntax diagram.
- The `-->` character sequence at the end of a line indicates that the syntax diagram continues on the next line.
- The `>--` character sequence at the beginning of a line indicates that a syntax diagram continues from the previous line.
- The `--><` character sequence indicates the end of a syntax diagram.

Symbols

Enter these symbols exactly as they are displayed in the syntax diagram:

*	Asterisk
{}	Braces
:	Colon
,	Comma
=	Equal sign
-	Hyphen
()	Parentheses
.	Period
	Space
"	Quotation mark
'	Single quotation mark

Variables

Italicized lowercase items such as *<variable_name>* indicate variables. In this example, you can specify a *<variable_name>* when you enter the **cmd_name** command.

```
►►──-cmd_name──<variable_name>────────────────────────────────────────────►◄
```

Required choices

When two or more items are in a stack and one of them is on the line, you must specify one item. In the following example, you must choose either *A*, *B*, or *C*:

```
►►──-cmd_name──┬─A─┬──────────────────────────────────────────────────────►◄
               ├─B─┤
               └─C─┘
```

Optional choices

When an item is below the line, that item is optional. In the following example, you can select either *A* or nothing at all:

```
►►──-cmd_name──┬───┬──────────────────────────────────────────────────────►◄
               └─A─┘
```

When two or more items are in a stack below the line, all items are optional. In the following example, you can choose either *A*, *B*,*C*, or nothing.

```
►►──-cmd_name──┬───┬──────────────────────────────────────────────────────►◄
               ├─A─┤
               ├─B─┤
               └─C─┘
```

mount

Use the **mount** command to complete various Data Protection for VMware Recovery Agent tasks.

The command line can be used to mount (**mount add**) and unmount (**mount del**) volumes and disks, and to view a list of mounted volumes (**mount view**).To use the **mount** command, Data Protection for VMware Recovery Agent must be running. Use the set_connection command to connect a TDPVMwareShell.exe to the mount application.

Snapshots are mounted or unmounted on the system where Data Protection for VMware Recovery Agent is running.

The **mount** command is supported in command mode. The following command types are available. The appropriate tags and parameters are listed alongside each command type.

add Use this command type to mount a disk or volume of a snapshot to the system where Data Protection for VMware Recovery Agent is running. The following list identifies the tags and parameters for the **add** type:

- **-target** - This tag is required.

  Use this tag to specify the following targets:

  - Windows Virtual volume - only for a partition mount
  - Windows Reparse point - only for a partition mount
  - Windows Linux iSCSI target

  The following examples use the **-target** tag:

  - Windows In the following example *V:* is the virtual volume mount target:

    ```
    -target "V:"
    ```

  - In the following example a reparse point volume mount target is specified:

    ```
    -target "C:\SNOWBIRD@FASTBACK\SnowbirtK\Snowbird\K\\"
    ```

  - Windows Linux In the following example an iSCSI target is specified:

    ```
    -target "ISCSI: target=<target_name> initiator=<initiator_name>"
    ```

- **-rep** - This tag is required.

  Use it to specify the Tivoli Storage Manager server that is storing the VMware snapshots, and the Tivoli Storage Manager node that has access to the VMware backups. For example:

  ```
  tsm: ip=<ip/host_name> port=<port_number>
   node=<node_name pass=<node_password>
  ```

- **-type** - This tag is required. Use it to specify that you want to mount a disk or a partition. The options are:

  -type disk
  -type partition

- **VMname** - This tag is required. Use it to specify the VMware machine name that is source of the snapshot.
- **-disk** - This tag is required. Use it to specify the disk number of the source backed up VMware machine to be mounted.

- **-date** - This tag is required. Use to specify the date of the snapshot that you want to mount. For example :

  ```
  -date "2011-Jan-12 22:42:52 AM"
  ```
- **-PartitionNumber** - This tag is optional. If the -type is partition, enter the partition number to mount.
- **-ro|-fw** - Use this tag to specify whether the mounted volume is read-only (**-ro**) or fake-write (**-fw**).

The following example shows how to specify the **add** type to mount a disk:

```
mount add -rep "tsm: ip=10.10.10.01 port=1500 node=tsm-ba pass=password"
-target "iscsi: target=test1 initiator=initiator_name" -type disk
-vmname VM-03ENT -disk 1 -date "12/9/2010 10:46:57 AM"
```

In this example, a snapshot of VMware named VM-03ent is located on a Tivoli Storage Manager server with IP 10.10.10.01. Disk number 1 of this snapshot is mounted to the system where Data Protection for VMware Recovery Agent is running.

del Use this command type to dismount one or all mounted backups from the system where Data Protection for VMware Recovery Agent is running. The following list identifies the tags and parameters for the **del** type:

- **-target** - This tag is required. Use this tag to specify the target for dismounting. The target for dismounting can be a virtual volume, reparse point, or iSCSI initiator created using the **mount** command. Use *everything* to dismount all mounted backups.
- **-force** - Use this tag to force an unmount. The default option is not to force an unmount if the target is currently in use.

For example, to force an unmount of a snapshot that is currently mounted at the directory, *c:\gever*, use the following command:

```
mount del -target "c:\gever" -force
```

To dismount a snapshot currently mounted as volume *V:*, use the following command:

```
mount del -target V:
```

To dismount a snapshot currently mounted as an iSCSI initiator, use the following command:

```
mount del -target "ISCSI:<target_name>"
```

dump Use this command type to get a list of all the available backups to mount.

- **-rep** - This tag is required. Use this tag to specify the Tivoli Storage Manager server storing the VMware snapshots, and to specify the Tivoli Storage Manager node that has access to the VMware backups. For example:

  ```
  tsm: ip=<IP/host name> port=<PortNumber>
  node=<NodeName> pass=<NodePassword>
  ```
- **-file** - This tag is optional. Use this tag to identify a file name to store the dump text. If this tag is not specified, the dump text is printed only to stdout.

The following examples show how to specify the dump type:

- List all the available backed up virtual machines.

  ```
  mount dump –type TSM –for TSMVE -rep P -request
  ListVM [–file <FileNameAndPath>]
  ```

- List all the available disk snapshots of a VMware.

  ```
  mount dump –type TSM –for TSMVE -rep P -request
  ListSnapshots -VMName P [-file <FileNameAndPath>]
  ```
- List all the available partitions of a disk snapshot.

  ```
  mount dump –type TSM –for TSMVE -rep P -request
  ListPartitions -VMName P -disk P -date P [-file <FileNameAndPath>]
  ```

remove
Use this type to remove the connection to a Tivoli Storage Manager server. There is only one tag for the **remove** type:

-rep - This tag is required. Use this tag to specify the Tivoli Storage Manager server connection to be removed.

In the following example, remove the connection to a Tivoli Storage Manager server (10.10.10.01) using node NodeName:

```
mount remove -rep :tsm: NodeName@10.10.10.01
```

view Use this type to view a list of all mounted snapshots. This type has no tags. The following example uses the **view** type:

```
mount view
```

Mounting a disk

The following syntax diagram is for the command for mounting a disk:

```
►►──TDPVMwareShell.exe -c──mount──add──-rep──"tsm:──ip──=──┬─IP────────┬──────────────►
                                                             └─host_name─┘

►─port──=──portNumber──node──=──nodeName──┬──────────────────────┬────────────────►
                                           └─-as_node──=──nodeName─┘

►─pass──=──NodePassword"──-vmname──vmname──-type──disk────────────────────────────►

►──disk──┬─disk_number──┬──date──date_format──────────────────────────────────────►
         └─vhd_filename─┘

►──target──"ISCSI:──target──=──target_name──initiator──=──initiator_name"──────────►◄
```

Mounting a partition

The following syntax diagram is for the command for mounting a partition:

```
►►──TDPVMwareShell.exe -c──mount──add──-rep "tsm:──ip──=──┬─IP─────────┬──────────────►
                                                            └─ host_name─┘

►─port──=──portNumber──node──=──nodeName──┬──────────────────────┬────────────────►
                                           └─-as_node──=──nodeName─┘

►─pass──=──NodePassword"──-vmname──vmname──-disk──┬─disk_number─┬─────────────────►
                                                   └─vmdk────────┘

►─date──date_format──-type partition──-PartitionNumber──partNum───────────────────►

►──target──┬─volume_letter──────────────────────────────────────────────────┬─────►◄
           └─"ISCSI:──target──=──target_name──initiator──=──initiator_name"─┘
```

del

The **del** command demounts a virtual device.

Use the following format for the **del** command:

```
TDPVMwareShell.exe -c del -target <volume_letter> \ "ISCSI:
target=<target_name>"
```

set_connection

The **set_connection** command sets the shell to work with a specified mount.

Use the following format for the **set_connection** command:

```
TDPVMwareShell.exe -c set_connection Command_Tag <hostname or IP address>
```

The following tag can be used with the **set_connection** command:

mount_computer - Use to set the Data Protection for VMware Recovery Agent connection.

In the following example, the command line is set to work with Data Protection for VMware Recovery Agent on the *ComputerName* host.

```
set_connection mount_computer ComputerName
```

help

The **help** command displays the help for all of the supported shell commands.

Use the following format for the **help** command:

```
TDPVMwareShell.exe -h
```

Command line return codes

Return codes help identify the results of command line operations.

Use these return codes to check the status of your command line operations.

Table 6. command line return codes

Return Code	Value
0	FBC_MSG_MOUNT_SUCCESS
1	FBC_MSG_MOUNT_FAIL
2	FBC_MSG_MOUNT_DRIVER_ERROR
3	FBC_MSG_VOLUME_LETTER_BUSY
4	FBC_MSG_MOUNT_WRONG_PARAMETERS
5	FBC_MSG_MOUNT_ALREADY_MOUNTED
6	FBC_MSG_MOUNT_WRONG_PERMISSIONS
7	FBC_MSG_MOUNT_NETWORK_DRIVE
8	FBC_MSG_MOUNT_LOCKED_BY_SERVER
9	FBC_MSG_CAN_NOT_CHANGE_REPOSITORY
10	FBC_MSG_DISMOUNT_SUCCESS
11	FBC_MSG_DISMOUNT_FAIL

Table 6. command line return codes (continued)

Return Code	Value
12	FBC_MSG_VIEW_SUCCESS
13	FBC_MSG_VIEW_FAIL
14	FBC_MSG_DUMP_SUCCESS
15	FBC_MSG_DUMP_FAIL
16	FBC_MSG_CONNECTION_FAILED
17	FBC_MSG_CONNECTION_TIMEOUT
18	FBC_MSG_MOUNT_FAILED_TO_FIND_REPOSITORY
19	FBC_MSG_MOUNT_JOB_NOT_FOUND
20	FBC_MSG_MOUNT_JOB_FOLDER_NOT_FOUND
21	FBC_MSG_MOUNT_WAIT_FOR_NEXT_DR
22	FBC_MSG_CAN_NOT_REMOVE_REPOSITORY
23	FBC_MSG_REPOSITORY_GOT_MOUNTS
24	FBC_MSG_REMOVE_SUCCESS

Chapter 8. Scenarios

Security Considerations

The Tivoli Storage Manager backup-archive client can back up a number of virtual machines under the same node name. Each virtual machine is a separate file space. The **dsmc set access** command can be used to control which virtual machines can be restored by which Mount or instant restore node name.

Two typical deployments are:

Mount installed on an off-host machine

The Tivoli Storage Manager administrator or help desk operator is responsible for mounting a snapshot and exporting it to the appropriate virtual machine. The **set access** command is issued from the backup-archive client node that owns the virtual machines to authorize the mount node to all virtual machines. For example,

```
set access backup * mountnodename
```

Mount and instant restore installed in-guest

The virtual machine user is responsible for restoring the data. To authorize the mount or instant restore node to a specific virtual machine, issue the **set access** command from the backup-archive client node that owns the virtual machines. For example:

```
set access backup "{\\VMFULL-vmdisplayname}\*\*" * mountnodename
```

The **set access** command does not restrict the ability to see what virtual machines have been backed up. However, it does restrict the ability to restore a virtual machine.

Defining Tivoli Storage Manager nodes

There should be namespace for a Tivoli Storage Manager node map to a VMware datacenter. A Tivoli Storage Manager node has all the virtual machines that are backed up for a given datacenter.

The advantages of this approach are that relocatiing virtual machines through vMotion is handled transparently. In addition, proxy data mover nodes can be defined to handle the work load.

Datacenter node

The virtual node that maps to a datacenter. The datacenter nodes hold the data; there is no data under the vStorage backup agent nodes.

vStorage backup agent

The node that maps to the vStorage backup agent instance that is performing the backup

Data Protection for VMware Recovery Agents

Nodes used to perform mount and instant restore

Node relationships

1. One datacenter virtual node for each VMware datacenter
2. One to *n* datacenter nodes associated with a vCenter node

3. One to *n* datamover nodes associated with a datacenter node
4. Datamover node:
   a. A datamover is normally associated with one datacenter, bit it can be associated with more than one datacenter.
   b. It is best that the datamover node name is different from the datacenter node name. Keeping node names separate makes future adding of data movers simpler. The same node name can be used for the datamover and datacenter.
5. A datacenter node is associated with one vCenter node.
6. IBM Tivoli Storage Manager for Virtual Environments / Tivoli Storage Manager API wrapper node
   a. One IBM Tivoli Storage Manager for Virtual Environments node per vCenter domain
   b. One to *n* datacenter nodes are associated with the IBM Tivoli Storage Manager for Virtual Environments node.

Overview of the node definition process

1. Register a Tivoli Storage Manager client virtual node that represents each VMware datacenter. A datacenter node contains the namespace for all virtual machines backed up for the datacenter.
2. Represent each backup-archive client proxy instance that is used to back up virtual machines.
   a. Register the Tivoli Storage Manager client data mover nodes for each datacenter to be backed up. There must be at least one datamover node per datacenter.
   b. Grant proxy authority to the datamover nodes so that they can back up virtual machines by using the associated datacenter node. For example `asnode=datacenternodename`
3. Register Tivoli Storage Manager client node names used for each system where Mount / instant restore is deployed.
   a. Mount and instant restore node names represent each installed instance of mount and instant restore.
   b. You can set access to allow the mount and instant restore node names access to a specific virtual machine for a guest deployment or to all virtual machines associated with a datacenter, for off-host proxy deployment.

Virtual machine backup examples

The Tivoli Storage Manager V6.2.3 backup-archive client provides a command-line interface and a graphical user interface. You can user either interface to perform vStorage virtual machine backups. You can run both full and incremental backups.

You can use the following client schedule options:

- Specify appropriate virtual machine schedule options.
  - mode=full or incremental. The full backup of a set of virtual machines requires a different schedule than incremental backup of the same set of virtual machines.
  - asnode=datacenternodename

Here are examples of two schedules that perform a weekly full backup and daily incremental backups for two ESX servers. Each dsmc instance processes an ESX server. The virtual node name datacenter1 represents a VMware data center. The options file for vmnode1 contains VMCH esx1, The options file for vmnode2 contains VMCH esx2.

- Schedule a weekly full backup of all virtual machines on ESX host esx1 and esx2. Use vmnode1 and vmnode2 instances and datacenter1 as the virtual node name that maps to data center.

  ```
  define schedule vmdomain vmschedfullesx1 type=client action=backup
  subaction=vm options='-asnodename=datacenter1 –mode=full'
  startdate=mm/dd/yyyy starttime=hh:mm
  perunits=weeks dayofweek=saturday

  define association vmdomain vmschedfullesx1 vmnode1, vmnode2
  ```

- Schedule daily incremental backups of all virtual machines on ESX host esx1 and esx2. Use vmnode1 and vmnode2 instances and datacenter1 Use vmnode1 and vmnode2 instances and datacenter1 as the virtual node name that maps to data center.

  ```
  define schedule vmdomain vmschedincesx1 type=client action=backup
  subaction=vm options='-asnodename=datacenter1 -mode=inc
  startdate=mm/dd/yyyy starttime=hh:mm
  schedstyle=enhanced perunits=weeks dayofweek==sunday, monday,
  tyesday, wednesday, thursday, friday

   define association vmdomain vmschedincesx1 vmnode1, vmnode2
  ```

Appendix. Accessibility features for Tivoli Storage Manager for Virtual Environments

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Tivoli Storage Manager for Virtual Environments:
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices
- User documentation provided in HTML and PDF format. Descriptive text is provided for all documentation images.

The Tivoli Storage Manager Information Center, and its related publications, are accessibility-enabled.

Vendor software

Tivoli Storage Manager for Virtual Environments 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.

Related accessibility information

You can view the publications for Tivoli Storage Manager for Virtual Environments in Adobe Portable Document Format (PDF) using the Adobe Acrobat Reader. You can access these or any of the other documentation PDFs at the IBM Publications Center at http://www.ibm.com/shop/publications/order/.

IBM and accessibility

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

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
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM 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.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs. Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe is either a registered trademark or trademark of Adobe Systems Incorporated in the United States, other countries, or both.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Program Number: 5725-A44

Printed in USA

SC27-2898-00