

IBM Tivoli Storage Manager for Virtual Environments
Version 7.1

*Data Protection for VMware User's
Guide*



IBM Tivoli Storage Manager for Virtual Environments
Version 7.1

*Data Protection for VMware User's
Guide*



Note:

Before using this information and the product it supports, read the information in “Notices” on page 181.

First edition (December 2013)

This edition applies to version 7, release 1, modification 0 of IBM Tivoli Storage Manager for Virtual Environments (product number 5725-A44) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2011, 2013.

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

Contents

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

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

Chapter 1. Tivoli Storage Manager for Virtual Environments overview 1

Documentation resources	6
Backup and restore types	6
How Tivoli Storage Manager nodes are used in a virtual environment	7
Incremental forever backup strategy	11
Periodic full backup strategy	12
Controlling which disks are processed	13
VM templates and vApps in a vSphere environment	13
Automated client failover.	14
Full VM instant restore environment requirements	15
Full VM instant restore iSCSI network requirements	16

Chapter 2. Mount, file-level restore, and instant restore of volumes overview . . 19

Data Protection for VMware Recovery Agent configurations	19
Mounting snapshots overview	24
Mounting snapshot guidelines for Windows systems.	24
Mounting snapshot guidelines for Linux systems	25
File-level restore overview	26
File-level restore guidelines for Windows systems	28
File-level restore guidelines for Linux systems . .	28
Instant restore overview	29
Instant restore guidelines for Windows systems	29
Instant restore guidelines for Linux systems . .	31

Chapter 3. Self-contained application protection overview 33

Application protection for Microsoft Exchange Server and SQL Server.	33
Configuring self-contained application protection. .	35
Verifying that self-contained application protection is working.	35
Application protection for Active Directory domain controllers	36

Chapter 4. Data Protection for VMware command-line interface 39

Backup	40
Restore	43
Inquire_config	47
Inquire_detail.	51

Set_domain	54
Set_mapping	54
Set_option.	56
Set_password.	58
Get_password_info	60
Start_guest_scan.	61
Profile parameters	63

Chapter 5. Recovery Agent command-line interface 71

Starting the Recovery Agent command-line interface	71
Recovery Agent command-line interface overview	71
Mount command	73
Set_connection command.	76
Help command	76
Recovery Agent command-line interface return codes	76

Chapter 6. Backup scenarios 79

vCloud environment backup scenarios	79
vSphere environment backup scenario	80
Incremental forever backup scenario	81
Fine-tuning Tivoli Storage Manager server database scalability	81
Periodic full backup scenario	84
Include scenarios	84
Management class scenarios	86
Controlling disk scenarios	87
Controlling disks used by Tivoli Storage Manager Data Protection applications	91
Cluster and data store backup scenarios.	92
Parallel backup processing	95
Active Directory domain controller protection scenario	97

Chapter 7. Restore scenarios 101

vCloud environment restore scenario	101
vSphere environment restore scenario	102
Full VM instant restore scenarios	102
Full VM instant restore cleanup and repair scenarios	103
Full VM instant restore integrity validation scenarios	105
Full VM recovery with application protection . .	107
Recover a Microsoft Exchange mailbox item from a VM backup	107
Recover individual Microsoft SQL databases from a VM backup	107
Restoring from virtual machine snapshots . .	108
Verifying that the Active Directory Domain Controller replicated successfully	111
Restoring files and instant restore of volumes with the Data Protection for VMware Recovery Agent .	113
Restoring files (Windows)	113
Instant restore of volumes (Windows)	115

Restoring files (Linux)	116
Instant restore of volumes (Linux)	117
Appendix A. Troubleshooting	121
Appendix B. Data Protection for VMware vSphere GUI and Data Protection for VMware vCloud GUI messages	131
Appendix C. Data Protection for VMware Recovery Agent messages	149
Appendix D. Tivoli support information	173
Communities and other learning resources	173
Searching knowledge bases.	175
Searching the Internet	175
Using IBM Support Assistant	175
Finding product fixes.	176
Receiving notification of product fixes	176
Contacting IBM Software Support	176
Setting up and managing support contracts	176
Determining the business impact.	177
Describing the problem and gathering background information.	177
Submitting the problem to IBM Software Support	177
Appendix E. Accessibility features for the Tivoli Storage Manager product family.	179
Notices	181
Trademarks	183

Privacy policy considerations	183
---	-----

Glossary 185

A	185
B	187
C	188
D	189
E	191
F	192
G	192
H	193
I.	194
J.	194
K	194
L	195
M	196
N	197
O	198
P	198
Q	199
R	200
S	201
T	204
U	204
V	205
W	206

Index 207

About this publication

This publication provides overview, planning, and user instructions for Data Protection for VMware.

Who should read this publication

This publication is intended for administrators and users who are responsible for implementing a backup solution with IBM® Tivoli® Storage Manager for Virtual Environments in one of the supported environments.

In this publication, it is assumed that you have an understanding of the following applications:

- Tivoli Storage Manager backup-archive client
- Tivoli Storage Manager server
- VMware vSphere or vCloud Director

Publications

Publications for the Tivoli Storage Manager family of products are available online. The Tivoli Storage Manager product family includes IBM Tivoli Storage FlashCopy® Manager, IBM Tivoli Storage Manager for Space Management, IBM Tivoli Storage Manager for Databases, and several other storage management products from IBM Tivoli.

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

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

New for Tivoli Storage Manager for Virtual Environments Version 7.1

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

The following features are new for Tivoli Storage Manager for Virtual Environments in V7.1:

Protection for vCloud Director objects

Access the vCloud Director environment through a stand-alone web GUI. For overview information, see “Data Protection for VMware vCloud GUI” on page 5.

Protect data in a vSphere environment with a stand-alone web GUI

Access the vCenter Server through a stand-alone web GUI. For overview information, see “Data Protection for VMware vSphere GUI” on page 2.

Recover individual Microsoft SQL databases from a VM backup

Recover Microsoft SQL databases from a VM backup that participates in application protection. For overview information, see “Recover individual Microsoft SQL databases from a VM backup” on page 107.

Instant restore of a full VM

Validate and recover an entire VM for immediate use. For overview information, see “Full VM instant restore” on page 7.

Protection for VM guests that host Microsoft Active Directory domain controller

Protect VMs that host Microsoft Active Directory Domain Controllers in both stand-alone and clustered environments. For overview information, see “Application protection for Active Directory domain controllers” on page 36.

Automated failover for data recovery

When the primary Tivoli Storage Manager server is unavailable, Data Protection for VMware can automatically fail over to the secondary server for data recovery. For more information, see “Automated client failover” on page 14.

Application protection reports

Generate reports about how applications are backed up by multiple Tivoli Storage Manager data protection agents. For more information, see “Start_guest_scan” on page 61.

Data Protection for VMware Recovery Agent messages

A complete list of FBP-prefix error messages are included in this release. See Appendix C, “Data Protection for VMware Recovery Agent messages,” on page 149.

Separate installation and user guides

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

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

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

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

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

Chapter 1. Tivoli Storage Manager for Virtual Environments overview

IBM Tivoli Storage Manager for Virtual Environments (referred to as Data Protection for VMware) provides a comprehensive solution for protecting VMs.

Data Protection for VMware eliminates the impact of running backups on a VM by offloading backup workloads from a VMware ESX or ESXi-based host to a vStorage Backup server. Data Protection for VMware works with the Tivoli Storage Manager backup-archive client (installed on the vStorage Backup server) to complete full and incremental backups of VMs. The client node installed on the vStorage Backup server is called the Tivoli Storage Manager data mover node. This node "moves" the data to the Tivoli Storage Manager server for storage, and for VM image-level restore at a later time. Instant restore is available at the disk volume level and full VM level. In addition, protection of vApps and organization vDCs in a vCloud Director environment is also available.

The Tivoli Storage Manager backup-archive client is a separately licensed component that contains its own user interfaces and documentation. Familiarity with this product and its documentation is necessary in order to adequately integrate a comprehensive plan for protecting your VMs with Data Protection for VMware. Tivoli Storage Manager for Virtual Environments V7.1 for Microsoft Windows 64-bit includes the Tivoli Storage Manager backup-archive client data mover features on the product DVD or download package.

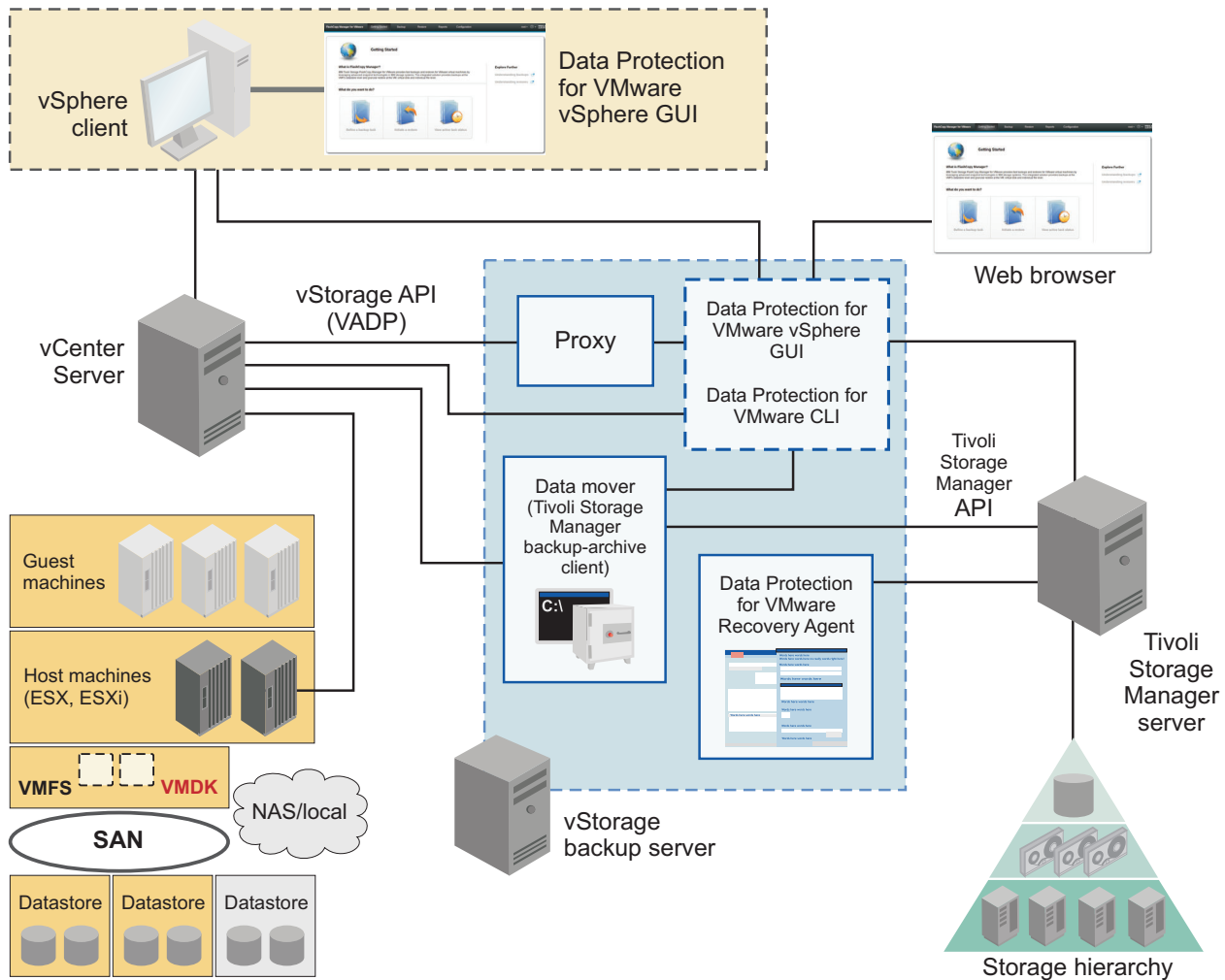


Figure 1. Tivoli Storage Manager for Virtual Environments system components in a VMware vSphere user environment

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

Data Protection for VMware vSphere GUI

This component is a graphical user interface (GUI) that accesses VM data on the VMware vCenter Server. This GUI is provided in two access methods:

- A plug-in that integrates with the VMware vSphere Client. This plug-in is accessed as a vCenter Server extension in the Solutions and Applications panel of your vCenter Server System. This access method was also provided in version 6.3 and 6.4.
- A stand-alone web browser GUI. This access method is new in version 7.1. This GUI is accessed through a URL bookmark to the GUI web server. For example:
<https://finapps.mycompany.com:9081/TsmVMwareUI/>

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

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

- Initiate a backup of your VMs to a Tivoli Storage Manager server, or schedule a backup for a later time.
- Initiate a full recovery of your VMs from a Tivoli Storage Manager server.
- Issue reports about the progress of your tasks, the most recent events that completed, backup status, and space usage. This information can help you troubleshoot your backups.

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

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

You can register multiple Data Protection for VMware vSphere GUIs to a single vCenter Server. This scenario reduces the number of datacenters (and their VM guest backups) that are managed by a single VMware Data Protection for VMware vSphere GUI. Each plug-in can then manage a subset of the total number of datacenters that are defined on the vCenter Server. For each plug-in that is registered to the vCenter Server, one Data Protection for VMware package must be installed on a separate host. To update the managed datacenters, go to **Configuration > Edit Configuration**. In the Plug-in Domain page, reduce the list of datacenters that are managed by the plug-in. Managing a subset of all available datacenters reduces the query and processing time that is required by the plug-in to complete operations.

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

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

The Data Protection for VMware vSphere GUI must have network connectivity to the following systems:

- vStorage Backup Server
- Tivoli Storage Manager server
- vCenter Server

In addition, ports for the Derby Database (default 1527) and GUI web server (default 9080, 9081) must be available.

Data Protection for VMware Recovery Agent

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

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

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

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

For detailed information regarding tasks, scenarios, and guidelines, see “Restoring files and instant restore of volumes with the Data Protection for VMware Recovery Agent” on page 113.

For detailed information regarding commands, parameters, and return codes, see Chapter 5, “Recovery Agent command-line interface,” on page 71.

Data Protection for VMware command-line interface

The Data Protection for VMware CLI is a full-function command-line interface that is installed with the Data Protection for VMware vSphere GUI. You can use the Data Protection for VMware CLI to complete these tasks:

- Initiate[®] a backup of your VMs to a Tivoli Storage Manager server, or schedule a backup for a later time.
- Initiate a full recovery of your VMs, VM files, or VM Disks (VMDKs) from a Tivoli Storage Manager server.
- View configuration information about the backup database and environment.

Although the Data Protection for VMware vSphere GUI is the primary task interface, the Data Protection for VMware CLI provides a useful secondary interface. For example, the Data Protection for VMware CLI can be used to implement a scheduling mechanism different from the one implemented by the Data Protection for VMware vSphere GUI. Also, the Data Protection for VMware CLI is useful when evaluating automation results with scripts.

For detailed information regarding available commands, see Chapter 4, “Data Protection for VMware command-line interface,” on page 39.

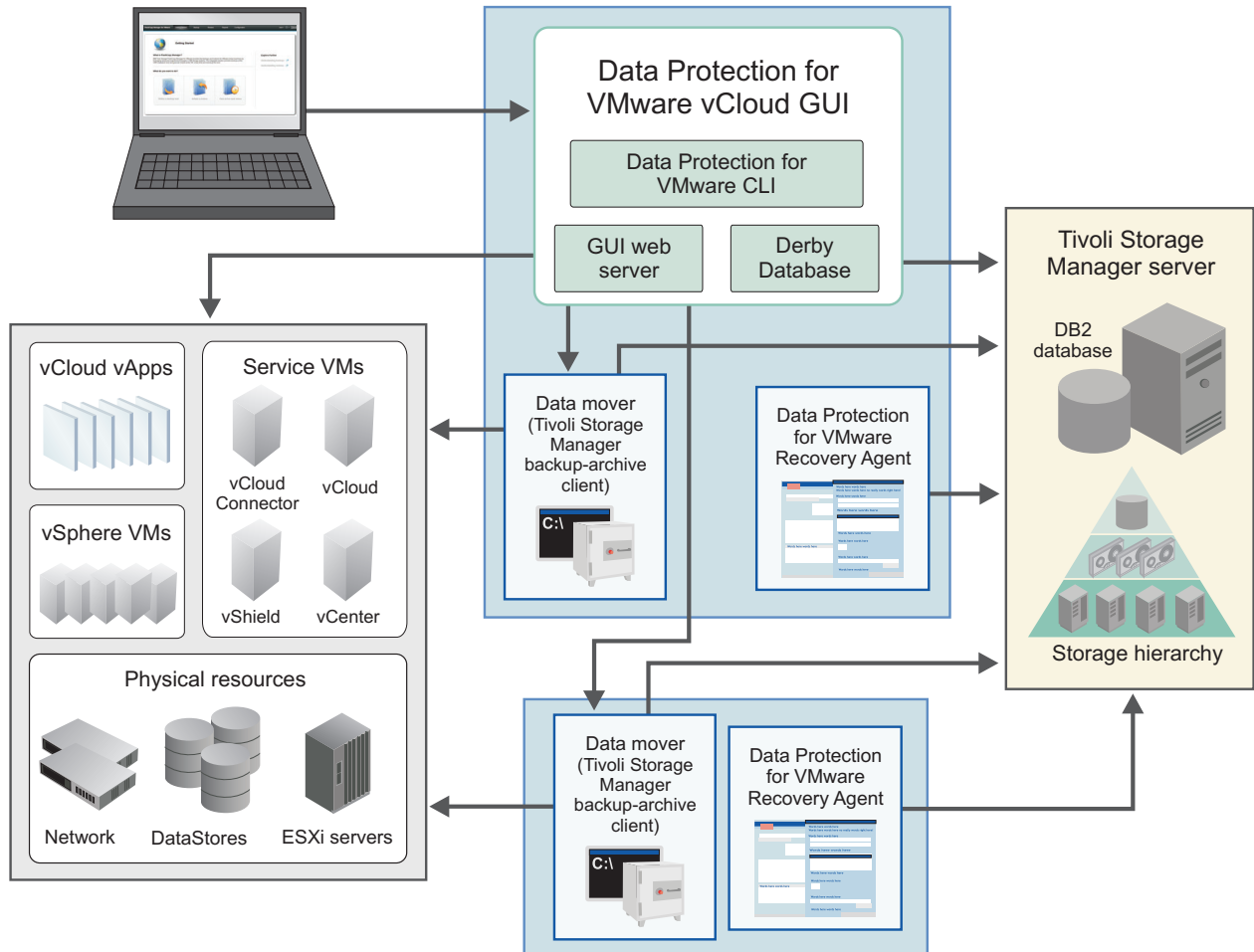


Figure 2. Tivoli Storage Manager for Virtual Environments system components in a VMware vCloud Director user environment

Data Protection for VMware vCloud GUI

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

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

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

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

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

Documentation resources

Data Protection for VMware provides several components to assist with protecting your VMs, vApps, and organization vDCs. As a result, multiple documentation resources are provided to assist with specific tasks.

Table 1. Topics for Tivoli Storage Manager clients, by operating system

Documentation	Contents	Format and location
<i>IBM Tivoli Storage Manager for Virtual Environments Version 7.1: Data Protection for VMware Installation Guide</i>	Software and hardware prerequisites, installation, upgrade, and configuration tasks.	Tivoli Storage Manager V7.1 documentation (XHTML) <i>IBM Tivoli Storage Manager for Virtual Environments 7.1: Data Protection for VMware Installation Guide</i> (PDF)
<i>IBM Tivoli Storage Manager for Virtual Environments Version 7.1: Data Protection for VMware User's Guide</i>	Overview information, strategy planning, back up and restore scenarios, command-line reference, and error messages.	Tivoli Storage Manager V7.1 documentation (XHTML) <i>IBM Tivoli Storage Manager for Virtual Environments 7.1: Data Protection for VMware User's Guide</i> (PDF)
<i>IBM Tivoli Data Protection for VMware Information Center for Version 2.1</i>	Back up and restore tasks related to VM data in a vSphere or vCloud environment.	IBM Eclipse Help System Click Learn More in any of the GUI windows to open for task assistance.
<i>Data Protection for VMware Recovery Agent Version 7.1 GUI Online Help</i>	Mount, file-level restore, and instant restore of volumes overview, configuration, and task information.	Java™ ARchive (JAR) file Click Help in the <i>Data Protection for VMware Recovery Agent Version 7.1 GUI</i> to open for task assistance.

Backup and restore types

Data Protection for VMware provides the following types of backup and restore functions:

Full VM backups

Back up an entire VM in your VMware vCenter to Tivoli Storage Manager storage. This is an entire VM image snapshot, which is a single snapshot that contains all of the VM disks. All data is backed up at the disk block level. The data can then be restored to a disk, or mounted as a virtual volume for an individual file restore. These backups are managed and retained according to storage policies set up by the Tivoli Storage Manager administrator.

Incremental VM backups

Back up only the VM data that has changed since the last full backup completed. All data is backed up at the disk block level. When a full backup has not been issued for the VM, Data Protection for VMware issues a full backup by default.

You can also use Data Protection for VMware to interface with the Windows backup-archive client in order to use the Change Block Tracking capabilities provided by the vStorage APIs for Data Protection (VADP).

File level restore

File level restore can be performed in-guest or off-host on supported Windows and Linux machines. Mount the volumes of the VM backup as a virtual volume. Then, copy the files that you want to restore using tools such as Windows Explorer or system commands. File restore is done from a backup-archive client full or incremental VM backup. The recovery point represented by either a full or incremental backup can be mounted. Although the mounted volume is read only by default, write permissions are also available.

Instant restore

With instant restore, you can restore the content of a single volume from a snapshot. This restore uses the snapshot data that is generated by the backup-archive client. Instant restore can be done from a full or incremental VM backup. You can use the volume immediately, while the restore process continues in the background. Instant restore requires an in-guest installation.

Full VM restore

Restore a full or incremental VM backup. The entire VM is restored to the state it existed in when originally backed up.

Full VM instant restore

Before this version of Data Protection for VMware, instant restore operations include non-operating system volumes that run inside a guest VM only. In addition to this existing restore function, Data Protection for VMware 7.1 provides instant restore for the entire VM. This type of restore is referred to as a full VM instant restore. The restored VM becomes available for instant use, either for validating the backed up VM or for restoring the VM to permanent storage. The restored VM is available for instant use in read/write mode.

How Tivoli Storage Manager nodes are used in a virtual environment

Data Protection for VMware communicates to VMs during backup, restore, and mount operations through Tivoli Storage Manager nodes.

A node represents a system on which the Tivoli Storage Manager backup-archive client, Data Protection for VMware, or other application client is installed. This system is registered to the Tivoli Storage Manager server. Each node has a unique name (node name) that is used to identify the system to the Tivoli Storage Manager server. Communication, storage policy, authority, and access to VM data are defined based on a node.

In a Data Protection for VMware vSphere production environment, the most basic node is the data mover node. This node represents a specific Tivoli Storage Manager backup-archive client (data mover) that "moves data" from one system to another. In a basic vSphere environment, where VMs are backed up by a single client, the VM data is stored directly under the data mover node.

In some scenarios, several data movers are used to back up a complete virtual environment, such as a VMware datacenter. In this scenario, since the backup work is distributed among multiple data movers, the VM data is stored in a shared node (instead of a specific data mover node). This shared node is called the datacenter node. Thus, in this large system vSphere environment, the data mover nodes store VM data into the datacenter node.

Finally, in a large vSphere virtual environment, where multiple data movers and datacenters are operative, a third node is used to communicate among the nodes and Tivoli Storage Manager server. This node is the VMCLI node.

Use the Data Protection for VMware vSphere GUI configuration wizard or configuration notebook to set these nodes in a vSphere environment.

Table 2. Tivoli Storage Manager nodes in a vSphere environment

Node	Description	Example in Figure 9 and Figure 10
vCenter node	The virtual node that represents a vCenter.	VC1
datacenter node	The virtual node that maps to a data center. The datacenter nodes hold the data.	VC1_DC1 VC1_DC2
VMCLI node	The node that connects the Data Protection for VMware command-line interface to the Tivoli Storage Manager server and the Tivoli Storage Manager data mover node. Unlike the Tivoli Storage Manager data mover node, the VMCLI node does not require its own Tivoli Storage Manager client acceptor or scheduler service.	VC1_VCLI1
Tivoli Storage Manager data mover node	The node name for the Tivoli Storage Manager backup-archive client that is installed on the vStorage Backup Server. This node performs the data movement. Each data mover node requires its own Tivoli Storage Manager client acceptor and scheduler service. Important: Data Protection for VMware stores sensitive information locally on the data mover, and the data mover might also have direct access to VM storage. Access to the data mover must be protected. Allow only trusted users access to the data mover system.	VC1_DC1_DM1 VC1_DC2_DM1

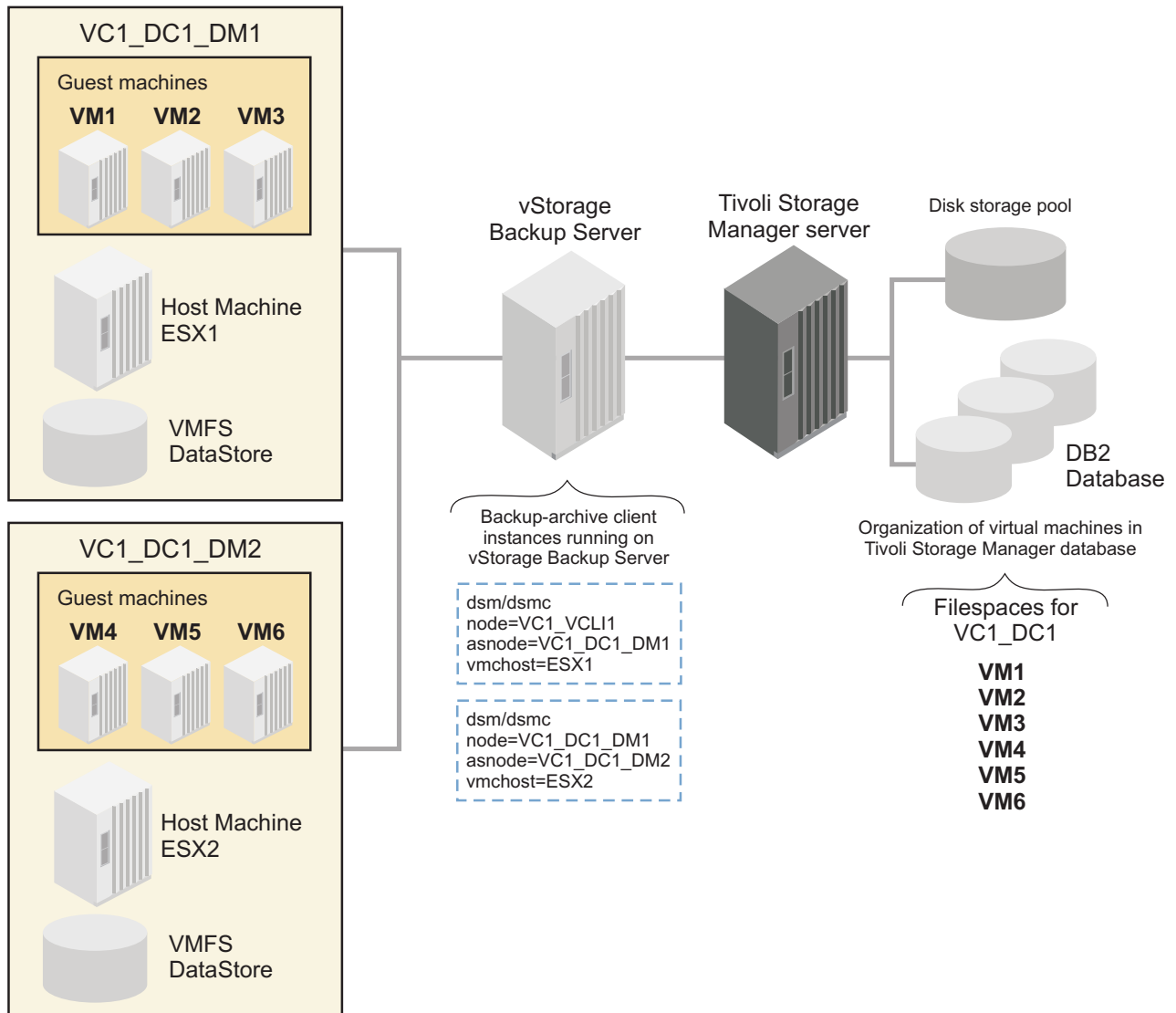


Figure 3. Node relationships and applications in a vSphere production environment that contains one VMware data center and two Tivoli Storage Manager data mover nodes.

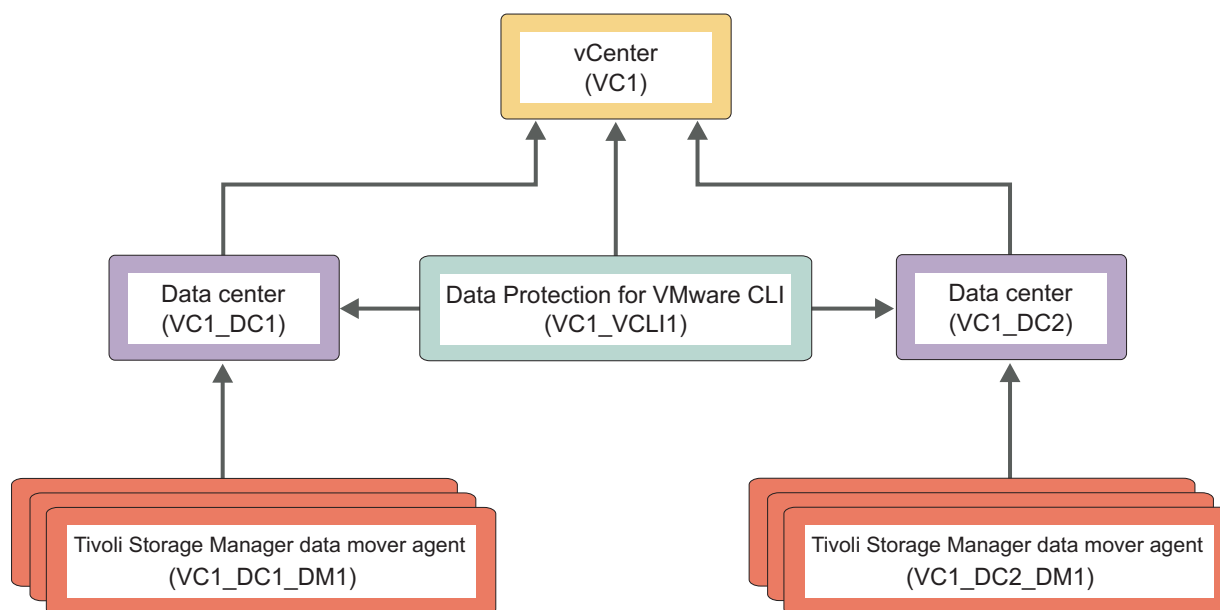


Figure 4. Proxy relationships among the nodes in a vSphere environment that uses two VMware datacenters. The arrows point from the proxy agent node to the proxy target node.

In a Data Protection for VMware vCloud Director production environment, several types of nodes are employed. Some nodes are used to represent vCloud entities and other nodes represent Tivoli Storage Manager entities.

The first node is the vCloud director node, which, as its name implies, represents the vCloud director. This node is the topmost node in the system. Next, vCloud provider virtual data centers (provider vDCs) are represented by corresponding provider vDC nodes. vCloud organization virtual data centers (organization vDCs) are represented by organization vDC nodes. The backup data for vApps (contained in a virtual data center) is stored in the corresponding organization vDC node.

On the Tivoli Storage Manager side, a data mover node represents a specific Tivoli Storage Manager backup-archive client (data mover). This node "moves" data between the vCloud environment and the various data-storing organization vDC nodes. Each data mover node is associated with a single provider virtual data center (provider vDC) node, and moves data only for organization vDCs allocated from its provider. A provider vDC can have one or more data mover nodes that move data for its organization vDCs.

Finally, a central node is used to communicate among the nodes and the Data Protection for VMware vCloud GUI. This node is the VMCLI node.

Use the Data Protection for VMware vCloud GUI configuration wizard or configuration notebook to set these nodes in a vCloud Director environment.

Table 3. Tivoli Storage Manager nodes in a vCloud Director environment

Node	Description	Example
vCloud Director Node	This node represents the vCloud Director and is the top-level node.	This node typically contains the prefix VCD_ in its name.
Provider VDC Node	This node represents a provider vDC in your vCloud environment.	This node typically contains the prefix PVDC_ in its name.

Table 3. Tivoli Storage Manager nodes in a vCloud Director environment (continued)

Node	Description	Example
Organization VDC Node	This node represents an organization vDC in your vCloud environment.	This node holds the data and typically contains the prefix OVDC_ in its name.
Data Mover Node	This node represents a backup-archive client and is associated with a single provider vDC and all of its organization vDCs. It is authorized to do operations for all organization vDCs that belong to the provider vDC.	This node typically contains the prefix DM_ in its name.
VMCLI Node	This node connects the Data Protection for VMware vCloud GUI to the Tivoli Storage Manager server and the other nodes.	This node typically contains the prefix VMCLI_ in its name.

Incremental forever backup strategy

An incremental forever backup strategy minimizes backup windows while providing faster recovery of your data.

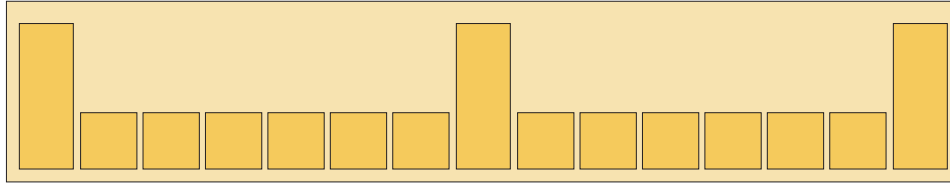
Data Protection for VMware provides a backup strategy called incremental forever. Rather than scheduling weekly (periodic) full backups, this backup solution requires only one initial full backup. Afterward, an ongoing (forever) sequence of incremental backups occurs. The incremental forever backup solution provides these advantages:

- Reduces the amount of data that goes across the network.
- Reduces data growth because all incremental backups contain only the blocks that changed since the previous backup.
- No comparison with the backup target is needed since only changed blocks are identified.
- Minimizes impact to the client system.
- Reduces the length of the backup window.
- No need to schedule an initial full backup as a separate schedule: the first issue of an incremental forever backup automatically defaults to an incremental forever full backup.

In addition, the restore process is optimized, as only the latest versions of blocks that belong to a restored backup are restored. Since the same area on the production disk is recovered only one time, the same block is not written to multiple times as implemented in prior versions of Data Protection for VMware. As a result of these advantages, incremental forever is the preferred backup strategy. However, if your backup solution requires long-term storage or tape retention of your data, consider the tasks described in “Periodic full backup strategy” on page 12.

Periodic full backup strategy

Weekly full backups followed by daily incremental backups



Incremental forever backup strategy

Initial full backup followed by ongoing sequence of incremental backups

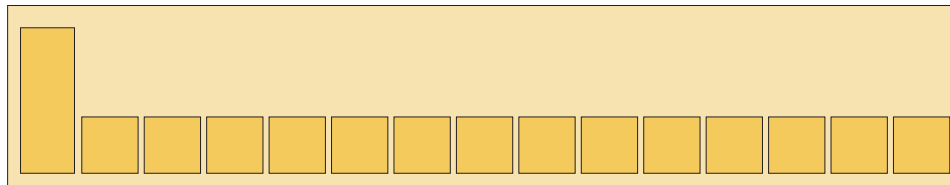


Figure 5. A comparison of both backup strategies

Restriction: Data Protection for VMware support for VM backup and restore operations is limited to VM names and datacenter names that contain only English 7-bit ASCII characters. You cannot use VM names and datacenter names that use other language characters. Additional character restrictions are listed in “Unsupported characters in VM or datacenter name” on page 126.

Periodic full backup strategy

A periodic full backup strategy provides a solution for long term storage or tape retention of your data.

The periodic full backup strategy backs up any VMware guests that are supported by VMware. If you have Data Protection for VMware and are using the VMware vStorage 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:

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

Restriction: Data Protection for VMware support for VM backup and restore operations is limited to VM names and datacenter names that contain English 7-bit ASCII characters only. VM names and datacenter names that use other language characters are not currently supported. Additional character restrictions are listed in “Unsupported characters in VM or datacenter name” on page 126.

Controlling which disks are processed

Set include and exclude statements to control the disks to be processed.

Use Data Protection for VMware in conjunction with the Tivoli Storage Manager backup-archive client to determine which disks in the VM environment are backed up and restored. VM environments typically contain a combination of system, normal, independent, and raw device mapping (RDM) disks. The ability to extend control granularity to specific disks provides benefits in these situations:

- Recover the disk where the operating system is located in order to replace a corrupted system drive.
- Protect disks in VM environments that use Tivoli Storage Manager Data Protection applications as guests that contain large database and log files.
- VM configuration information is lost. The VM configuration information is recovered while the disks remain in place.

In previous versions of Data Protection for VMware, a new VM was required whenever a VM restore was performed. If the VM already existed, the restore failed. With this feature, you can restore selected virtual disks but leave the rest of an existing VM intact.

VM templates and vApps in a vSphere environment

Data Protection for VMware supports backing up and restoring VM templates and vApps.

A VM template is a master image of a VM. The template can include an installed guest operating system and a set of applications.

VM templates can be restored to the original VM template, or to an alternative VM template and data store location. Because Data Protection for VMware marks the VM template as one unit, a single file restore of a VM template is not feasible. A single virtual disk cannot be restored, nor can a single virtual disk backup be attached on an ESX host to a target VM.

VMs that are contained in a vApp can be backed up and restored. A vApp is a logical entity that consists of one or more VMs. By using a vApp, you can specify and include all components of a multitier application. A vApp also includes the operational policies and associated service levels of the application contained in the vApp.

The VMs in the vApp are identified in the Data Protection for VMware vSphere GUI as VMs. While you select the VM to back up, you cannot select a vApp. When you restore the VM, the VM is added to one of the following locations:

- If the vApp is present with the original full inventory path, the VM is restored to that location.
- When the original full inventory path is not present or was changed, the VM is restored to the top-level default location on the target ESX host. No containers are created during the restore operation.

When backing up a VM template, and a full backup does not exist for this VM template, the following occurs:

- If the selected backup type is incremental-forever-incremental, and the VM template contains changes, the backup type changes to incremental-forever-full.

- If the selected backup type is incremental, and the VM template contains changes, the backup type changes to full.
- If the selected backup type is full, and the VM template contains changes, the VM template is backed up.
- If the selected backup type is incremental-forever-full, this type ensures that the VM template is backed up regardless of whether it contains changes.

Automated client failover

If you backed up data to the Tivoli Storage Manager server, Data Protection for VMware can automatically fail over to the secondary server for data recovery when there is an outage on the Tivoli Storage Manager server.

The Tivoli Storage Manager server that the Tivoli Storage Manager data mover node connects to during normal production processes is called the *primary server*. When the primary server and data mover node are set up for node replication, the client data on the primary server can be replicated to another Tivoli Storage Manager server, which is the *secondary server*.

During normal operations, connection information for the secondary server is automatically sent to the data mover node from the primary server during the logon process. The secondary server information is automatically saved to the client options file on the data mover node. No manual intervention is required by you to add the information for the secondary server.

Each time the data mover node logs on to the server, it attempts to contact the primary server. If the primary server is unavailable, the data mover node automatically fails over to the secondary server, according to the secondary server information in the client options file. In failover mode, you can restore any replicated client data. When the primary server is online again, the data mover node automatically fails back to the primary server the next time the data mover node connects to the server.

Requirements: Before the connection information for the secondary server is sent to the client options file, the following processes must occur:

- The primary server, secondary server, and data mover node must be at the V7.1 level.
- The primary and secondary servers must be set up for node replication, and the client node must be configured for node replication on the server.
- You must back up VMware data at least one time to the primary server.
- Client data on the primary server must be replicated to the secondary server at least one time.

Restriction: The following restrictions apply to Data Protection for VMware during failover:

- Any operations that require data to be stored on the Tivoli Storage Manager server, such as backup operations, are not available.
- Schedules are not replicated to the secondary server. Therefore, schedules are not run while the primary server is unavailable.
- Instant restore of virtual machines is not available.
- Validation of virtual machine backups is not available.

- The Data Protection for VMware GUI does not fail over. You must use the backup-archive client on the data mover node to restore data from the secondary server.
- For more information about the failover capabilities of Tivoli Storage Manager components, see Technote 1649484.

For more information about automated client failover with the backup-archive client, see *Automated client failover configuration and use* in the Tivoli Storage Manager information center (http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1/topic/com.ibm.itsm.client.doc/c_cfg_autoclientfailover.html).

Full VM instant restore environment requirements

Windows

Review the applications, systems, and versions that are required for full VM instant restore operations.

The following environment requirements must exist before attempting a full VM instant restore operation:

- Full VM instant restore is supported only for Tivoli Storage Manager backup-archive client 7.1 Windows 64-bit and Windows vStorage Backup servers.
- Instant access and instant restore capability is supported only for VMware VMs that are hosted on VMware ESXi 5.1 servers, or later versions.
- Full VM instant restore is supported only for disks and virtual tape libraries (VTL). Physical tape storage pools are not supported.
- The Data Protection for VMware Recovery Agent 7.1 must be installed on the same system as the Tivoli Storage Manager backup-archive client 7.1 (data mover) system.
- VMs that were backed up with backup-archive client 6.3 (or later) can be restored by using full VM instant restore.
- The data mover system requires the IBM Tivoli Storage Manager for Virtual Environments 7.1 license file.
- iSCSI mount (with the Data Protection for VMware Recovery Agent) is used to expose the VM disks to the ESX as virtual RDMS. Instant access and instant restore operations require an iSCSI software or hardware adapter that is configured on the ESX host that is used for these operations.
- Storage vMotion must be installed and configured on the ESX servers that host the VMs to be used during instant restore operations. Instant access operations (that validate the VM backup data) do not require Storage vMotion.
- Instant access and instant restore operations require vSphere privileges that power on VMs (**Virtualmachine.Interaction.PowerOn**).

Full VM instant restore iSCSI network requirements

If your VMware environment uses a dedicated iSCSI network for full VM instant restore and instant access operations, make sure to use specific configuration settings.

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

ESXi vSwitch network configuration settings

These settings apply to VMware tasks related to adding a VMkernel connection.

Table 4. ESXi vSwitch network configuration settings

Object	Value
Connection Type	VMkernel
VMkernel Network Access	Create a vSphere standard switch
VMkernel Connection Settings	Network Label <i>VMkernel network name</i> Tip: Use a name that reminds you that the VMkernel network is used with iSCSI. For example: VMkernel iSCSI
VMkernel IP Connection Settings	IP Address <i>xyz.xyz.xy.xy</i> Tip: Do not change the Subnet Mask or VMkernel Default Gateway values.

VM network configuration settings

These settings apply to VMware tasks related to adding a VM connection.

Table 5. VM network configuration settings

Object	Value
Connection Type	Virtual Machine
Virtual Machine Network Access	Use the recently created network vSwitch (VMkernel iSCSI)
Virtual Machine Connection Settings	Network Label Tip: Use a name that reminds you that the VM network is used with iSCSI. For example: VM Network iSCSI

iSCSI adapter settings

These actions apply to VMware tasks related to connecting the VMkernel to a network adapter.

Table 6. iSCSI adapter settings

Object	Required Action
Recently created network vSwitch (VMkernel iSCSI)	Must be added to the iSCSI network
vStorage Backup Server (data mover)	If your vStorage Backup Server (data mover) is installed on a VM, a second network card must be added for this VM.

Important: If you experience a timeout when iSCSI devices are rescanned, reduce the number of iSCSI devices that are connected to the ESX host. Then, try the operation again.

Data Protection for VMware Recovery Agent and data mover settings

These settings apply to parameter setting required for the following applications:

- Data Protection for VMware Recovery Agent 7.1
- Tivoli Storage Manager backup-archive client 7.1

Tip: The backup-archive client is also referred to as the data mover and is installed on the system referred to as the vStorage Backup server.

Table 7. Data Protection for VMware Recovery Agent and data mover settings

System	File	Parameter Setting
Windows System where the Data Protection for VMware Recovery Agent installed	TDPVMwareMount.conf Default location: C:\ProgramData\Tivoli\TSM\TDPVMware\mount\	[IMount config] Target IP =IP of the network card on the datamover machine that exposes the iSCSI targets. After you add or change the IP address in the TDPVMwareMount.conf file, restart the Data Protection for VMware Recovery Agent service.
vStorage Backup Server (data mover)	dsm.opt Default location: C:\Program Files\Tivoli\TSM\baclient\	VMISCSIserveraddress = iSCSI server IP is the address of the network card on the datamover machine that exposes the iSCSI targets The VMISCSIserveraddress = IP address must be the same IP address specified in the TDPVMwareMount.conf file.

The Data Protection for VMware Recovery Agent must be configured before you attempt an instant restore operation:

1. Perform the configuration tasks that are described in the Data Protection for VMware Recovery Agent GUI online help. In the Data Protection for VMware Recovery Agent GUI, click **Help**, then click **Configuring the Data Protection for VMware Recovery Agent GUI**.

2. Set the Data Protection for VMware Recovery Agent command-line interface (CLI) on the data mover to work with the local Data Protection for VMware Recovery Agent by issuing the following command:

```
TDPVMwareShell.exe -c set_connection mount_computer <mount_address>
```

The <mount_address> is the IP address of the system where the local Data Protection for VMware Recovery Agent is installed.

Tip: To verify that the Data Protection for VMware Recovery Agent is configured properly, use the Data Protection for VMware Recovery Agent GUI to perform an iSCSI mount and iSCSI dismount operation.

During a VM instant access or VM instant restore operation, each VM disk is mounted as an iSCSI target by the Data Protection for VMware Recovery Agent. For example, an instant access operation for a VM that contains two hard disks uses two iSCSI mount sessions. These sessions are considered concurrent iSCSI mount sessions. The maximum number of concurrent iSCSI mount sessions for the Data Protection for VMware Recovery Agent is 128. Therefore, make sure that the number of concurrent iSCSI mount sessions does not exceed 128 sessions.

Chapter 2. Mount, file-level restore, and instant restore of volumes overview

Overview, planning, and guideline information is provided in this section.

Data Protection for VMware Recovery Agent configurations

The Data Protection for VMware Recovery Agent 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 VM guest. Instead, an off-host Windows or Linux instance is responsible for file-level restore of multiple VMs. With this configuration, the mount process exposes a virtual volume from a selected disk partition. Use the Data Protection for VMware Recovery Agent GUI to accomplish this task.

The Tivoli Storage Manager administrator must register a node that is associated with the Data Protection for VMware Recovery Agent. The Data Protection for VMware Recovery Agent node must be granted proxy authority to access the data node (or nodes) where the snapshots are stored. When a snapshot is mounted to the off-host server, the virtual volume can be network-shared to make it accessible to the VM guest. Or, you can copy the files from the mounted volume to the VM guest by any file-sharing method. This centralized restore process is typically initiated by a VMware administrator, by a Tivoli Storage Manager administrator, or by help desk personnel.

The data paths for off-host file restores are illustrated in Figure 6 and Figure 7 on page 20.

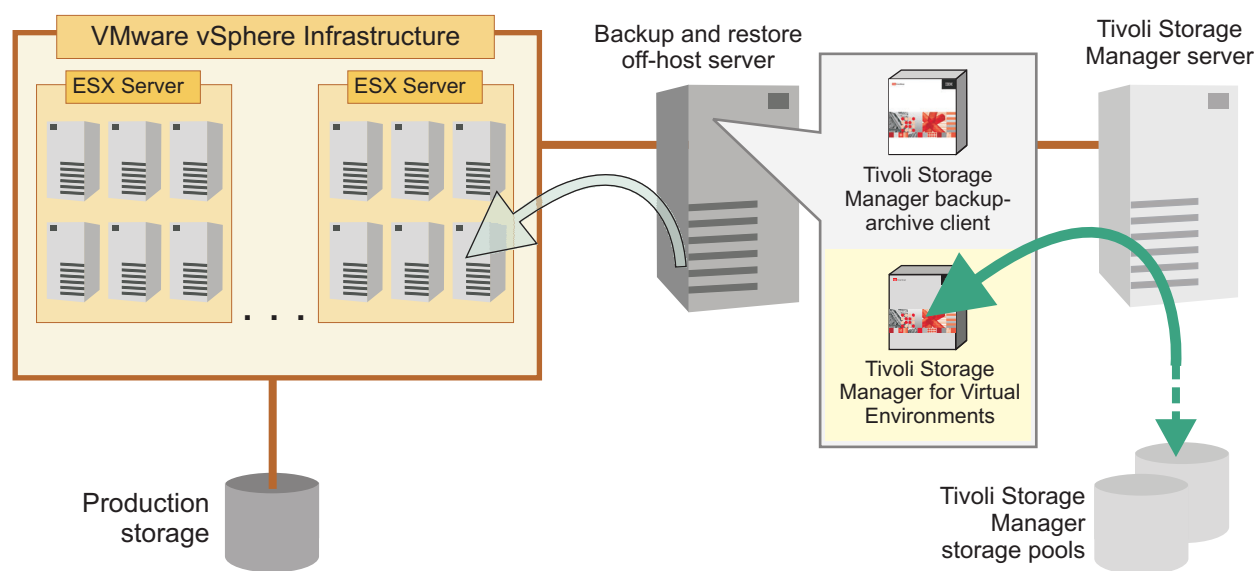


Figure 6. Off-host file-level restore for Windows

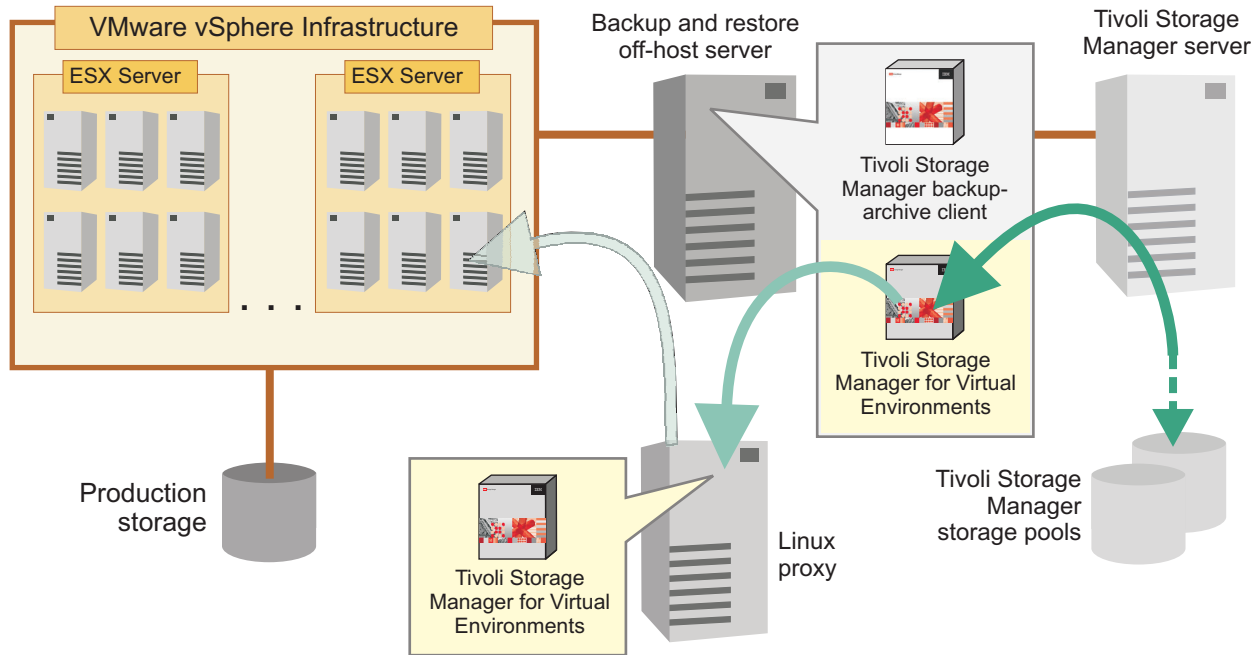


Figure 7. Off-host file-level restore for Linux

- For step by step restore instructions, see “Restoring files and instant restore of volumes with the Data Protection for VMware Recovery Agent” on page 113

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 VM guest. The mount and instant restore processes are performed for a single partition from the backed up disk.

The Data Protection for VMware Recovery Agent node name is typically granted access only to the VM where it is running with the Tivoli Storage Manager backup-archive client **dsmt set access** command. The restore process is typically begun by a VMware user who logs in to the guest machine of the VM.

For these configurations, be sure to compare the specific VM 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 VM guest for volumes that are not the operating system volume. Use the Data Protection for VMware Recovery Agent GUI to accomplish this task.

The data paths for in-guest file level restores are illustrated in Figure 8 on page 21 and Figure 9 on page 21. The data path for in-guest instant restore is illustrated in Figure 10 on page 22 and Figure 11 on page 22.

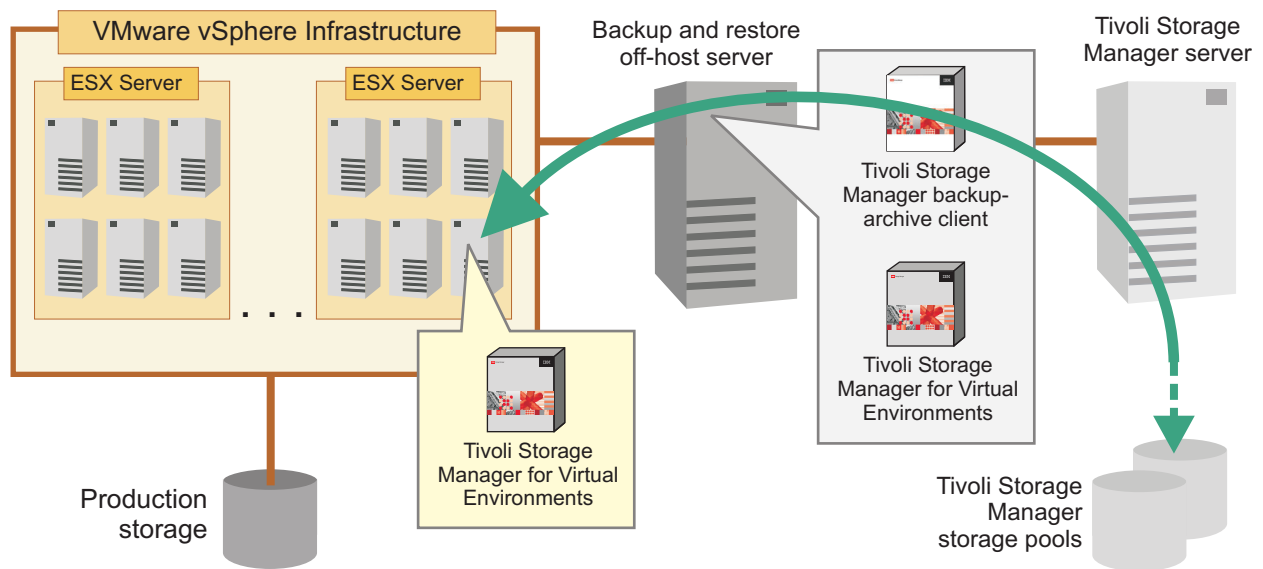


Figure 8. In-guest file-level restore for Windows

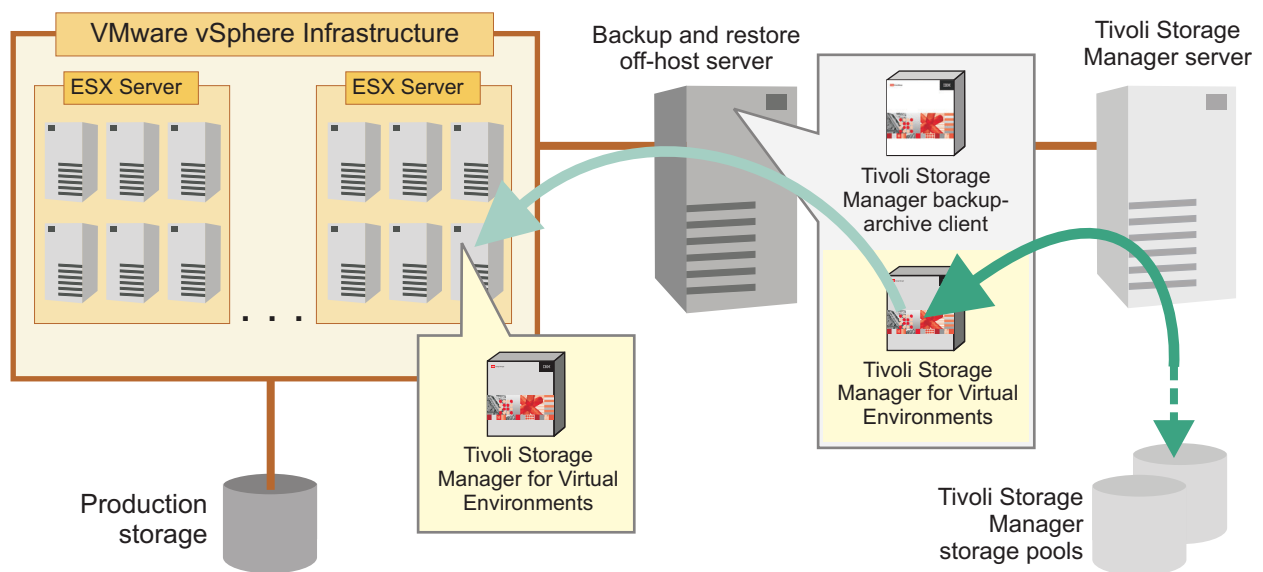


Figure 9. In-guest file-level restore for Linux

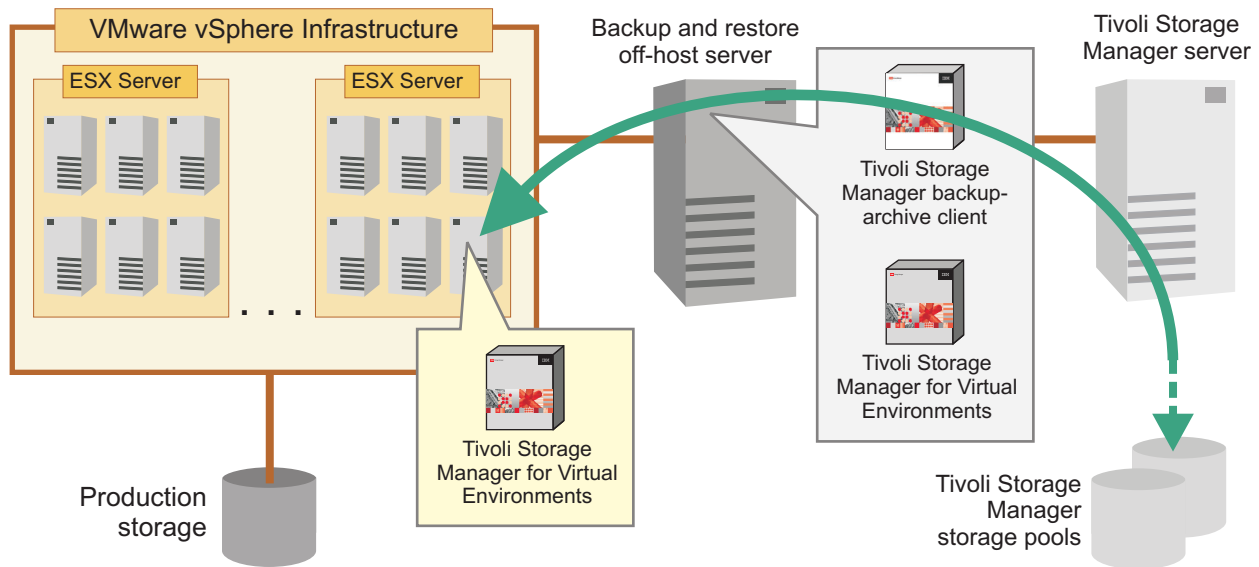


Figure 10. In-guest instant restore for Windows

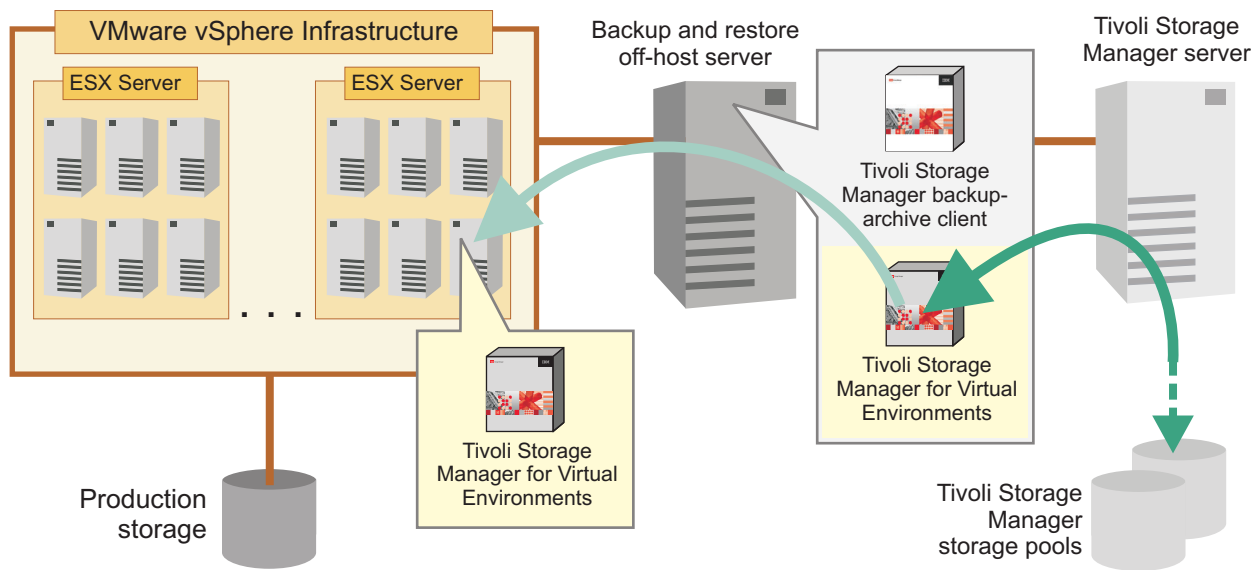


Figure 11. In-guest instant restore for Linux

- For planning information and operating system-based guidelines, see Chapter 2, “Mount, file-level restore, and instant restore of volumes overview,” on page 19.
- For step-by-step restore instructions, see “Restoring files and instant restore of volumes with the Data Protection for VMware Recovery Agent” on page 113.

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 VM guest. This approach exposes an iSCSI

LUN, rather than the off-host file-level restore for Windows and Linux, which exposes an individual disk partition. Use the Data Protection for VMware Recovery Agent GUI to accomplish this task.

In this configuration, the user specifies the VM guest iSCSI initiator name for the system where the iSCSI device is accessed. After a disk snapshot is mounted, it can be discovered and logged in to by using the iSCSI initiator in the VM 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 VM 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 12.

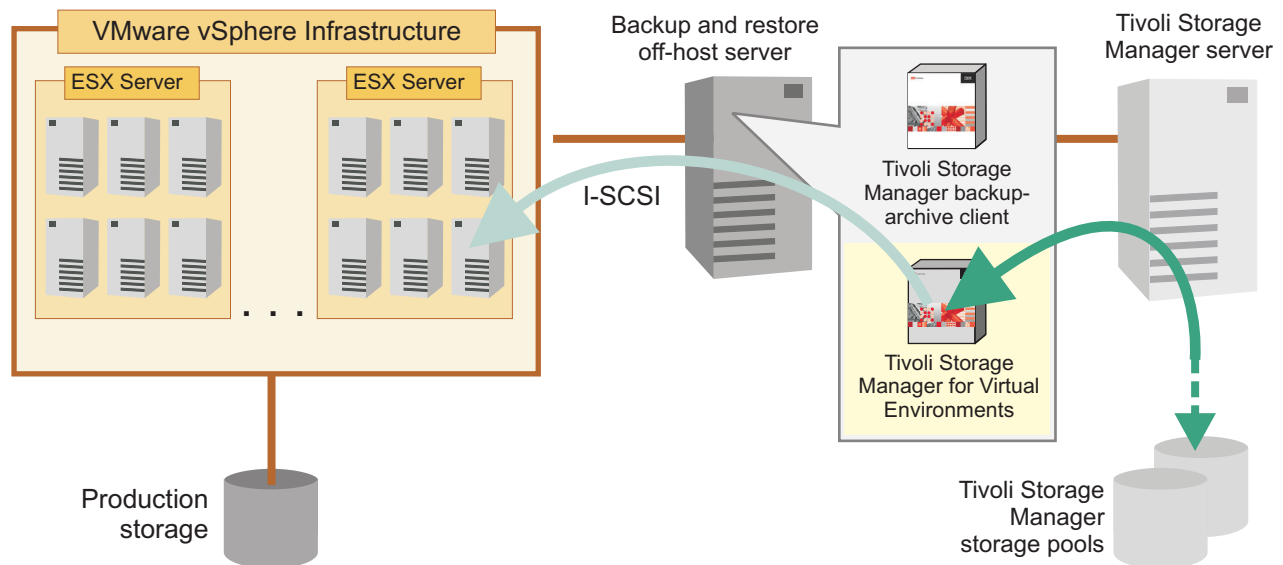


Figure 12. Off-host iSCSI target

- For planning information and operating system-based guidelines, see Chapter 2, “Mount, file-level restore, and instant restore of volumes overview,” on page 19.
- For step by step restore instructions, see “Restoring files and instant restore of volumes with the Data Protection for VMware Recovery Agent” on page 113.
- Before attempting to restore files in an off-host iSCSI target configuration, you must configure Cygwin for use when restoring files from a Linux machine.

Mounting snapshots overview

Linux

Windows

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

Mount snapshots with either the Data Protection for VMware Recovery Agent GUI or with the “Mount command” on page 73. Install and run the Data Protection for VMware Recovery Agent on a system that is connected to the Tivoli Storage Manager server through a LAN. You cannot use the Data Protection for VMware Recovery Agent component operations in a LAN-free path.

Be aware of these three situations when running mount operations:

- When the Data Protection for VMware Recovery Agent is installed on a guest machine, you cannot start an instant restore or a mount operation for any file system or disk while the guest machine is being backed up. You must either wait for the backup to complete, or you must cancel the backup before running an instant restore or a mount operation. These operations are not allowed because the locking mechanism is for a full VM.
- When you browse the snapshot backup inventory, the operating system version of the VM is the version that was specified when the VM was originally created. As a result, Data Protection for VMware Recovery Agent might not reflect the current operating system.
- A volume becomes unstable when a network failure interrupts a mount operation. A message is issued to the event log. When the network connection is reestablished, another message is issued to the event log. These messages are not issued to the Data Protection for VMware Recovery Agent GUI.

A maximum of 20 iSCSI sessions is supported. The same snapshot can be mounted more than one time. If you mount a snapshot from the same tape storage pool by using multiple instances of the Data Protection for VMware Recovery Agent, one of the following actions occurs:

- The second Data Protection for VMware Recovery Agent instance is blocked until the first instance is complete.
- The second Data Protection for VMware Recovery Agent instance might interrupt the activity of the first instance. For example, it might interrupt a file copy process on the first instance.
- The Data Protection for VMware Recovery Agent cannot connect to multiple servers or nodes simultaneously.

As a result, avoid concurrent Data Protection for VMware Recovery Agent sessions on the same tape volume.

Mounting snapshot guidelines for Windows systems

Windows

Information unique to mount operations on a Windows system is provided.

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 memory. If the service is restarted, the changes are lost.

Data Protection for VMware Recovery Agent operates in either of the following two modes for systems that run Windows 7, Windows Vista, or Windows 2008:

No user is logged in

Data Protection for VMware Recovery Agent runs as a service. This service enables remote connections through the Data Protection for VMware command-line interface.

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 and use the GUI. When you close the Data Protection for VMware Recovery Agent and GUI, the service restarts. You can use only the Data Protection for VMware Recovery Agent application and GUI when running with administrator login credentials. Only one copy of the Data Protection for VMware Recovery Agent application can be active at any time.

When mounted volumes exist and you start Mount from the Start menu on Windows 7, Windows 8, Windows Vista, or Windows 2008, this message is displayed:

Some snapshots are currently mounted. If you choose to continue, these snapshots will be dismounted. Note that if a mounted volume is currently being used by an application, the application may become unstable. Continue?

When **Yes** is clicked, the mounted volumes are unmounted, even when they are in use.

Restriction: When exposing snapshots as iSCSI targets, and a snapshot of a dynamic disk is displayed to its original system, the UUIDs become duplicated. Likewise when a snapshot of a GPT disk is displayed to its original system, the GUIDs become duplicated. To avoid this duplication, expose dynamic disks and GPT disks to a system other than the original system. For example, expose these disk types to a proxy system, unless the original disks no longer exist.

Mounting snapshot guidelines for Linux systems

Linux

Information unique to mount operations on a Linux system is provided.

Use either of these methods to mount (and restore) files on Linux:

- Use the Data Protection for VMware Recovery Agent to create an iSCSI target. You can use an iSCSI initiator on the Linux machine to mount the target volume. The Linux machine does not require the Data Protection for VMware Recovery Agent to be installed. iSCSI mount is the preferred method to mount (and restore) files on Linux.
- Install the Data Protection for VMware Recovery Agent command-line interface, Cygwin, and OpenSSH on a Windows system. Use the Data Protection for VMware Recovery Agent GUI on the Linux machine.

Be aware of these requirements when running mount operations:

- The Data Protection for VMware Recovery Agent GUI on Windows must be able to access the IBM Tivoli Storage Manager server. The Data Protection for VMware Recovery Agent GUI on Windows displays snapshots as iSCSI targets. Therefore, the snapshots must be accessible to the target Linux system.

- Linux mount and restore operations require the iSCSI port to be open on any firewall between the Windows mount system, the iSCSI target, and the system that completes the restore (the iSCSI initiator). The iSCSI default port is 3260.

Be aware of these two actions when running mount operations:

- To prevent possible mount errors, disable the FS Automount option for the Tivoli Storage Manager disks. This option is set in the configuration file used for the HAL daemon. If you do not disable the FS Automount option, the unmount operation might fail.
- To prevent the recovery process from mounting the device, stop the cron daemon. For example:

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

Start the cron daemon when the processing completes.

When running a Linux instant restore or mount, Data Protection for VMware Recovery Agent saves changes to data on a virtual volume in the write cache. 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 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 from configuration files. Specify the write cache location in a non-system folder on a local disk to prevent possible errors. For example, Windows 2008 has a different path: C:\ProgramData\Tivoli\TSM\TDPVMWare\mount.

Restriction: These two restrictions affect mount operations:

- To prevent any interruption during restore processing, exclude the write cache path from all antivirus software protection settings.
- When restoring several volumes to several partitions on the same disk, only one volume can be active. The other volumes remain in the DELAYED state. Their progress as shown on the user interface remains at 0% until they move out of the DELAYED state after the active synchronization completes.

File-level restore overview

Linux

Windows

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

Data Protection for VMware Recovery Agent can be used for the following tasks:

- Recovering lost or damaged files from a backup
- Mounting a VM guest volume and creating an archive of the VM guest files
- Mounting database applications for batch reports

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 unmounting the volume.

The default *read only* mount option is the preferred method, unless a mounted volume must be writeable. For example, an archive application might require write access to the archived volume.

The Data Protection for VMware Recovery Agent mounts snapshots from the Tivoli Storage Manager server. In the Data Protection for VMware Recovery Agent GUI, click **Remove** to close an existing connection to a Tivoli Storage Manager server. You must remove any existing connection before you can establish a new connection to a different server or different node. Dismount all volumes 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 a server when you are running 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.

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

Restoring file-level information for a block-level snapshot is a random-access process. As a result, processing might be slow when a sequential-access device (such as a tape) is used. To run a file-level recovery of data that is stored on tape, consider moving the data to disk or file storage first. From a Tivoli Storage Manager server administrative command-line client (dsmadm), issue the **QUERY OCCUPANCY** command to see where the data is stored. Then, issue the **MOVE NODEDATA** command to move the data back to disk or file storage.

For more information about these commands, see the Tivoli Storage Manager Information Center: <http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1>

Mounting a snapshot from the same tape storage pool by two instances of Mount can cause one of these results:

- The second Mount instance is blocked until the first instance is complete.
- Both mounts succeed, but the performance is poor.

When restoring data from a mirrored volume, mount only one of the disks that contains the mirrored volume. Mounting both disks causes Windows to attempt a resynchronization of the disks. However, both disks contain a different timestamp if mounted. As a result, all data is copied from one disk to the other disk. This amount of data cannot be accommodated by the virtual volume. When you must recover data from a volume that spans two disks, and those disks contain a mirrored volume, complete these steps:

1. Mount the two disks.
2. Use the iSCSI initiator to connect to the first disk.
3. Use Windows Disk Manager to import this disk. Ignore any message regarding synchronization.
4. Delete the mirrored partition from the first (or imported) disk.
5. Use the iSCSI initiator to connect to the second disk.
6. Use Windows Disk Manager to import the second disk.

Both volumes are now available.

Restriction: Do not change a Tivoli Storage Manager node password while running a file level restore or an instant restore from snapshots stored in that node.

File-level restore guidelines for Windows systems

Windows

Information unique to file-level restore operations on a Windows system is provided.

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.

In order to recover Microsoft Exchange Server mailbox items, you must use the IBM Tivoli Storage Manager FastBack® for Microsoft Exchange product and documentation. As a result, IBM Tivoli Storage Manager FastBack for Microsoft Exchange must be purchased separately with a valid license. For more information, see the following product website:
<http://www.ibm.com/software/tivoli/products/storage-mgr-fastback-exchange/>

The mount function cannot be used to mount a snapshot of partitions from a dynamic or GPT-based disk as a virtual volume. Only partitions from an MBR-based, basic disk can be mounted as virtual volumes. File-level recovery from GPT, dynamic, or any other non-MBR or non-basic disk is possible by creating a virtual iSCSI target and using an iSCSI initiator to connect it to your system.

Important: The ACL values associated with the folders and files that are restored in a file level recovery operation are not transferred to the recovered files. In order to maintain ACL values, use the XCOPY command when copying files from the target.

File-level restore guidelines for Linux systems

Linux

Information unique to file-level restore operations on a Linux system is provided.

File-level restore is supported from snapshots of disks that use any of the following:

- MBR-style partition tables.
- Partitions formatted using one of these file systems:
 - EXT2
 - EXT3
 - EXT4
 - ReiserFS

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

- If, during a file restore on a Linux machine, the iSCSI target is dismounted, the file level restore fails, and the restored data remains uncompleted.

- The Data Protection for VMware Recovery Agent GUI must be configured before attempting a file level restore. To configure, click **Select TSM server** and **Settings** in the Data Protection for VMware Recovery Agent GUI and enter the required information.
- 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.
- Linux requires all iSCSI devices to be unmounted before rebooting or shutting down the system.
- The Data Protection for VMware Recovery Agent component does not support file level restore operations over a wide area network (WAN).

Instant restore overview

Linux

Windows

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.

Instant restore works only with local volumes. The term "local" is used regarding the Data Protection for VMware Recovery Agent since it must be installed on the guest machine that contains the volume to be restored. Local volumes must have an assigned drive letter. Instant restore cannot be used to restore the system volume.

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 Software RAID 0, RAID 1, and RAID 5 volumes. You can use a basic disk as a destination volume and then convert the basic disk to a dynamic disk. The file system on the destination volume cannot be a FAT file system. If you plan to restore into a FAT volume, you must format it as NTFS before attempting an instant restore.

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 might not be affected, and you can work with the cluster, and with that volume, in parallel. During the instant restore, the disk that is 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 guidelines for Windows systems

Windows

Information unique to instant restore operations on a Windows system is provided.

Instant restore operations on Windows require the Data Protection for VMware Recovery Agent to be installed on the guest machine.

Instant restore is available only from Data Protection for VMware snapshots on a source volume that is on a simple, MBR-based disk. The volume format of

volumes on those disks must be NTFS, FAT, or FAT32. However, instant restore to a destination partition on FAT volumes is not supported. As a result, if you plan to restore to a destination partition that is formatted as FAT, you must format the partition as NTFS before attempting a restore. In addition, when selecting a destination volume for instant restore, make sure that the volume is on a physical disk, and not on a virtual iSCSI disk.

- 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 that are 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.

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 restarts, the volume appears to be unformatted. Do not attempt to format or modify the volume. 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**. During the period when the session is paused, the parts of the volume that are not yet restored are inaccessible.

You can use instant restore to restore into a simple volume that is on a dynamic disk. However, the source volume must be an MBR-based disk. The source volume cannot be a dynamic disk. This restore might cause the disk status to change to *Online (Errors)*. In addition, the status of all volumes on the disk might 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**.

Instant restore guidelines for Linux systems

Linux

Information unique to instant restore operations on a Linux system is provided.

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 Data Protection for VMware Recovery Agent GUI must be configured before attempting an instant restore. To configure, click **Select TSM server** and **Settings** in the Data Protection for VMware Recovery Agent GUI and enter the required information.
- 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 user interface is available.
- SUSE Linux Enterprise Server 11 require all iSCSI devices to be unmounted before rebooting or shutting down the system.
- Instant restore is available for snapshots of disks that use MBR-style partition tables only. The partition used as the source for an instant restore operation must be formatted by using one of the following file systems:
 - EXT2
 - EXT3
 - EXT4
 - ReiserFS
- When selecting a destination volume for instant restore, make sure that the volume resides on a physical disk, and not on a virtual iSCSI disk.
- The Data Protection for VMware Recovery Agent component does not support instant restore operations over a wide area network (WAN).

The instant restore progress can be slow in some situations. This can be due to such things as connectivity issues, very large volumes, restore from tape, or high I/O operations. The recovery process identifies no progress was made on the MDADM device (/dev/md0) for the last 5 minutes and responds to it as a potential problem. As a result, a cleanup is performed, and the restore restarts itself, continuing from the point at which it stopped. The cleanup can cause I/O operations to fail. To fix this problem, you can increase the recovery process period by editing the /etc/crn.d/tsmmount_recover file. Increase the recovery process period to 10 minutes or to 20 minutes if the volume is very large, or the I/O is intense.

Chapter 3. Self-contained application protection overview

Data Protection for VMware protects Microsoft Exchange Server, Microsoft SQL Server, and Active Directory Domain Controllers that run inside VM guests.

Application protection for Microsoft Exchange Server and SQL Server

Data Protection for VMware backs up VM guests that contain Microsoft Exchange Server and Microsoft SQL Server data.

In prior releases, Data Protection for VMware used VMware functions to quiesce applications that run on the VM guest. During backup processing, the application server was not notified that the backup to the Tivoli Storage Manager server completed successfully. As a result, logs were not truncated on the application server.

Data Protection for VMware V7.1 backs up VM guests with both guest level application consistency and log truncation for the following applications:

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012

The SQL Browser service must be running on the guest machine in order for the SQL Server truncated logs function to work. Otherwise, SQL Server logs are not truncated and a warning message is sent to the error log.

Application protection for VM guests is supported on the vStorage Backup server for the following platforms:

-  Microsoft Windows 2008
-  Microsoft Windows 2008 R2
-  Microsoft Windows 2012
-  VMware ESX 5.x (or later)
-  Linux 64-bit platforms
-  VMware ESX 5.x (or later)

You can back up these VM guests with the following interfaces:

- Data Protection for VMware vSphere GUI
- Tivoli Storage Manager backup-archive client command-line interface
- Tivoli Storage Manager backup-archive client Web client
- Tivoli Storage Manager backup-archive client GUI based on Oracle Java

However, to implement this function, you must specify the following Tivoli Storage Manager backup-archive client V7.1 option in the `dsm.opt` file (Windows) or `dsm.sys` file stanza (Linux):

INCLUDE.VMTSMVSS *vmname*

This option notifies VM applications that a backup is about to occur. This notification allows the application to truncate transaction logs and commit transactions so the application can resume from a consistent state when the backup completes. By default, this option is not enabled. You must set this option to enable application protection for a VM.

The *vmname* value specifies the name of the VM that contains the applications to quiesce. Specify one VM per **INCLUDE.VMTSMVSS** statement. To protect all VMs with this option, use an asterisk as a wildcard (**INCLUDE.VMTSMVSS ***). You can also use question marks to match any single character. For example, **INCLUDE.VMTSMVSS vm??** protects all VMs that have names that begin with "vm" and followed by any two characters (vm10, vm15).

If **OPTIONS** **KEEPSQLLOG** is specified in an **INCLUDE.VMTSMVSS** statement, this parameter prevents SQL server logs from being truncated when a data mover node backs up a VM that runs a SQL server. Specifying this parameter allows the SQL server administrator to manually manage (backup and possibly truncate) the SQL server logs, so they can be preserved as needed and be used to restore SQL transactions to a specific checkpoint, after the VM is restored. When this option is specified, the SQL log is not truncated and following message is displayed and logged on the server:

```
ANS4179I IBM Tivoli Storage Manager application protection did not truncate  
Microsoft SQL Server logs on virtual machine vmname
```

Note: Tivoli Storage Manager does not back up the SQL log files. The SQL administrator must back up the log files so they can be applied after the database is restored.

When a backup of a VM guest (with application protection) fails or is stopped, see "Resolving a VM guest (with application protection) backup failure" on page 125 for a solution.

When a backup of a VM guest (with application protection) completes but the event log contains the event ID 8194, VSS error message, see "Event log contains event ID 8194, VSS message" on page 125 for a solution.

Remember: When you use the **EXCLUDE.VMDISK** option to exclude a disk from backup that contains application data, your application is not protected.

For permission required to backup and restore application data for Microsoft Exchange Server, see the following IBM website:

<http://www.ibm.com/support/docview.wss?uid=swg21647986>

For permission required to backup and restore application data for Microsoft SQL Server, see the following IBM website:

<http://www.ibm.com/support/docview.wss?uid=swg21647995>

Configuring self-contained application protection

Linux

Windows

Configuring self-contained application protection requires the Tivoli Storage Manager backup-archive client GUI.

Perform the following steps:

1. In the Tivoli Storage Manager backup-archive client GUI, click **Edit > Client preferences > VM Backup** and specify the VMware Virtual Center or ESX Server host, user, and password information.
2. Click **Apply** and exit the backup-archive client GUI.
3. Add **INCLUDE.VMTSMVSS *vmname*** to either the client options file `dsm.opt` or the client system options file (`dsm.sys`). To prevent SQL server logs from being truncated when a data mover node backs up a VM that runs a SQL server, append this statement to the options file:
`INCLUDE.VMTSMVSS vmname OPTions=KEEPSqllog`
4. On the command line, type **`dsmc set password -type=vmguest vmguestname AdminID AdminPswd`** to store the guest VM password. The guest VM user must have permission to create Volume Shadow Copies and to truncate SQL Server logs.
5. Back up the VM by issuing the **`dsmc backup vm`** command.

Verifying that self-contained application protection is working

Linux

Windows

During backup operations, the command-line interface displays information to help verify that application protection is working.

For example, the following output shows that Tivoli Storage Manager application protection was used to protect Microsoft SQL Server 2008.

```
Starting Full VM backup of VMware Virtual Machine 'wombat'
mode:                               'Periodic Full - Full'
target node name:                    'TSMNODE'
data mover node name:                'TSMNODE'
application protection type:         'TSM VSS'
application(s) protected:            'MS SQL 2008' (database-level recovery)
```

The new database-level recovery field identifies that the VM backup is available for a Microsoft SQL Server database restore.

When application protection is not used or fails because of configuration issues, the application protection type is `VMware`. Your applications are still protected but their logs are not truncated.

```
Starting Full VM backup of VMware Virtual Machine 'wombat'
mode:                               'Periodic Full - Full'
target node name:                    'TSMNODE'
data mover node name:                'TSMNODE'
application protection type:         'VMware'
```

After a backup is completed, you can use the **QUERY VM** command with the `-Detail` option to view the status of application protection for your VM backups. The following is an example of output of the **QUERY VM** command with the `-Detail` option specified.

Query VM wombat -detail

Query Virtual Machine for Full VM backup

#	Backup Date	Mgmt Class	Size	Type	A/I	Virtual Machine
1	08/21/2013 15:07:19	STANDARD	29.14 GB	FULL	A	wombat
The size of this incremental backup: n/a						
The number of incremental backups since last full: n/a						
The amount of extra data: n/a						
The TSM objects fragmentation: n/a						
Backup is represented by: n/a						
Application protection type: TSM VSS						
Application(s) protected: MS SQL 2008 (database-level recovery)						
VMDK[1]Label: Hard disk 1						
VMDK[1]Name: [ess800_dev1] wombat/wombat-000002.vmdk						
VMDK[1]Status: Protected						

Application protection for Active Directory domain controllers

Data Protection for VMware provides back up and restore protection for VMs that host Microsoft Active Directory Domain Controllers in both stand-alone and clustered environments. A clustered environment contains multiple domain controllers that participate in Active Directory. This protection prevents USN rollback.

USN rollback is a condition that results from restoring the Active Directory domain controller in an improper manner. When the domain controller is locally restored, this condition prevents any of its changes from being replicated to other domain controllers. These changes are not replicated because the restored USN is earlier than the USN that is tracked by the other domain controllers. Similar changes on other remote domain controllers are not replicated back to the locally restored domain controller. As a result, the topology remains in an unsynchronized state.

To prevent USN rollbacks, Data Protection for VMware protects guest VMs in a clustered environment where multiple domain controllers participate in Active Directory replication. The backed up VM guest that hosts the Active Directory domain controller is recovered by implementing non-authoritative restore.

Non-authoritative restore recovers the Active Directory (or domain controller) to the version taken at the time of the backup. When the recovered Active Directory (or domain controller) is restored, it is updated with information from the other domain controllers through the existing replication process.

Environment requirements

Data Protection for VMware protects Windows VM guests that host Active Directory Domain Controllers. The following guest versions that host Active Directory Domain Controllers are supported:

-  Microsoft Windows 2008 (32-bit, 64-bit), Microsoft Windows 2008 R2 (64-bit), or Microsoft Windows Server 2012

Important: To protect Active Directory on a VM guest that is running on Microsoft Windows Server 2012, one of the following levels of VMware are required:

- VMware vSphere 5.0 Update 2 (vCenter Server and ESXi must both be at 5.0 Update 2)
- VMware vSphere 5.1 (ESXi 5.0 Update 2 or later)

- **Windows** A current version of VMware Tools must be installed and must be running on the VM guest at the time that it is backed up. This VM guest must be powered on for Data Protection for VMware to detect Active Directory. Otherwise, Active Directory will not be detected and restore protection will be unavailable.
- **Windows** The Data Protection for VMware Enablement File must be installed on the vStorage Backup server for successful restore of VMs that host Active Directory Domain Controllers.

Important:

Application protection for domain controllers is not supported for the following situations:

- Backups that are created by Tivoli Storage FlashCopy Manager for VMware.
- Backups that are created by Data Protection for VMware and Tivoli Storage FlashCopy Manager for VMware.
- A Tivoli Storage Manager data mover that is installed on Linux.
- A file-level restore of Active Directory objects.
- During a full VM instant restore, instant access and instant verification are blocked when the Active Directory domain controller is detected on the VM backup to be restored and the VM guest is on Windows 2008 or Windows 2008 R2.
- Backup and restore of VMs running Active Directory Lightweight Directory Services (AD LDS) is not supported.
- Recovery of expired Active Directory tombstone objects is not supported. To help prevent Active Directory objects from expiring, run backups more frequently than the default tombstone life of 60 days.

Note: When a VM guest contains Active Directory or a domain controller, Windows NT Directory Services (NTDS) must be running for VSS backups and domain controller discovery to function.

Chapter 4. Data Protection for VMware command-line interface

Use the Data Protection for VMware command-line interface to back up, restore, or view configuration information in a vSphere or vCloud environment.

Linux

Windows

The Data Protection for VMware command-line interface provides these commands:

“Backup” on page 40

Initiate full and incremental backups of your VMs.

“Restore” on page 43

Restore backups of your VMs.

“Inquire_config” on page 47

View configuration information about the backup database.

“Inquire_detail” on page 51

View configuration information about the backup environment.

“Set_domain” on page 54

Apply changes to the domain settings.

“Set_mapping” on page 54

Set mapping between the vCloud objects and Tivoli Storage Manager node name.

“Set_option” on page 56

Set a parameter in the vmcliprofile.

“Set_password” on page 58

Set the password for the Data Protection for VMware command-line interface node name.

“Get_password_info” on page 60

View the status of guest credentials that are set for the managed data centers.

“Start_guest_scan” on page 61

Scan guest VMs for application information.

Access the Data Protection for VMware command-line interface in the following directories:

Linux

/opt/tivoli/tsm/tdpvmware/common/scripts

Windows

(32-bit)

C:\Program Files\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts

Windows (64-bit)

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

For Data Protection for VMware command-line interface messages that contain the FMM prefix, message information is available at the following web sites:

Tivoli Storage Manager Information Center

Backup

Use this **vmcli** command to start full and incremental backups of your VMs or VM templates.

Syntax

The **vmcli -f backup** command uses this syntax:

```
vmcli -f backup -t backupType -I backupObjectListFile -d datacenterhostname |  
providerDCnodename -o datamovernodename [--name taskName] [--description  
descriptionInFile.txt] [-s tsmserverhostname] [-n vctrclinodename] [-p tsmserverport]
```

Linux

You must issue the **vmcli -f backup** command as **tdpvmware** user, and not as root.

Parameters

Before you issue a **vmcli -f backup** command, issue the **vmcli -f inquire_config** command to verify that your configuration is correct. Also, use the information from the **vmcli -f inquire_config** command output as a guide for setting your backup parameters.

When a backup operation is running, there is no command or method available to stop the backup, including the Ctrl + C command. You must wait for the operation to complete on its own.

The **vmcli -f backup** command requires that the **VE_VCENTER_NODE_NAME** is set correctly in the **vmcli** profile. You cannot overwrite this parameter with a command-line entry.

The data mover system (the vStorage Backup Server where the Tivoli Storage Manager backup-archive client is installed) must not set the **ASNODENAME** option.

-t backupType

Specify the type of backup to complete. You can choose from one of the following types:

TSM_INCR

Creates an incremental backup of the specified backup object. This parameter is valid only in vSphere mode.

TSM_FULL

Creates a full image backup of the specified backup objects. This parameter is valid only in vSphere mode.

TSM_IFFULL

Creates an incremental forever full backup of the specified backup objects. When **TSM_IFFULL** is specified, template VMs that are

unchanged since the last backup are also included. This parameter is valid in both vSphere and vCloud mode.

TSM_IFINCR

Creates an incremental forever incremental backup of the specified backup object. This type backs up only the changed data since the last backup. This parameter is valid in both vSphere and vCloud mode. This type is the default.

The backup process does not create a snapshot of template VMs in the same manner that a snapshot is created for regular VMs. As a result, VMware VDDK advanced transports (SAN, HotAdd mode), change block tracking (CBT), and incremental backups are not available.

-I *backupObjectListFile*

Specify the file that contains the list of objects to back up. Each line contains one specification for backup.

In vCloud mode, the *backupObjectListFile* uses the following format:

```
vappname:Org=organization,OrgvDC=organization VDC[,vApp=vApp]
```

The org, orgvdc, and vapp keywords must be followed by an equal sign (=) and separated from the next keyword by a comma (,).

In vCloud mode, the *backupObjectListFile* uses the following keywords:

vappname

Specify the name of the vApp to back up. Each line in the *backupObjectListFile* must start with this keyword. You can repeat this keyword for each vApp you want to back up.

org Specify the name of the organization from which the vApps are backed up. This parameter must be specified immediately after the vappname keyword. If you backup vApps from different organizations, create multiple lines.

orgvdc

Specify the name of the organization vDC from which the vApps are backed up. This parameter must be specified as the third parameter of an input line (after the org keyword). If you backup vApps from different organization vDCs, create multiple lines.

vapp Specify the name of the vApp to back up. This parameter must be specified as the fourth parameter of an input line (after the orgvdc keyword). If you backup multiple vApps, create multiple lines. If this parameter is not specified, all vApps from the organization vDC (orgvdc) of the organization (org) are backed up.

In vSphere mode, the *backupObjectListFile* uses the following keyword:

vmname

Specify the name of the VM to back up. You can specify this keyword for each VM you want to back up. For example:

```
vmname:vm1  
vmname:vm2
```

Restrictions:

- Do not specify a VM host name in the *backupObjectListFile*. Data Protection for VMware does not support backing up a VM that is identified by the VM host name.
- When you specify the name of a VM by using the *vmname* keyword in the *backupObjectListFile*, Data Protection for VMware does not differentiate between a colon (:) used as a keyword separator or a colon that is used in the VM name. Therefore, use caution when you specify keyword values. In addition, backing up a VM that contains a comma in its name is not supported.
- Data Protection for VMware support for VM backup operations is limited to VM names and datacenter names that contain English 7-bit ASCII characters only. VM names and datacenter names that use other language characters are not currently supported. More character restrictions are listed in “Unsupported characters in VM or datacenter name” on page 126.
- A VMware vCenter allows the existence of two VMs with the same name. However, Data Protection for VMware does not support backing up two VMs with the same name. To prevent errors or backup failures, do not have two VMs with the same name in a vCenter.

-d *datacenternodename | providervDCnodename | organizationvDCnodename*
 When the **VE_TSM_MODE** parameter specifies VSPHERE, specify the datacenter node name.

When the **VE_TSM_MODE** parameter specifies vCloud, specify the provider vDC node name (backup and restore operations) or the organization vDC node name (query operations).

-o *datamovernodename*
 Specify the Tivoli Storage Manager data mover node name. This name is the node name for the Tivoli Storage Manager backup-archive client that is installed on the vStorage Backup Server. This node performs the data movement.

[--name *taskName*]
 Specify the string that identifies the backup task.

[--description *descriptionInFile.txt*]
 Specify the name of the text file that contains a description of the backup task.

[-s *tmsserverhostname*]
 Specify the host name or IP address of the Tivoli Storage Manager server. If this parameter is not specified, the value in the profile is used.

[-n *vmclinodename*]
 Specify the VMCLI node name. This node connects the Data Protection for VMware command-line interface to the Tivoli Storage Manager server and the Tivoli Storage Manager data mover node. If this parameter is not specified, the value in the profile is used.

[-p *tmsserverport*]
 Specify the port of the Tivoli Storage Manager server.

- If this parameter is not specified in the Data Protection for VMware command-line interface and not specified in the profile, the default port (1500) is used.
- If this parameter is not specified in the Data Protection for VMware command-line interface, but is specified in the profile, the value in the profile is used.

Restore

Use this **vmcli** command to restore backups of your VMs or VM templates.

Syntax

The **vmcli -f restore** command uses this syntax:

```
vmcli -f restore [-c tsm_mode] -I restoreObjectListFile -d datacenternodename -o datamovernodename [-s tsmserverhostname] [-n vmclinodename] [-p tsmserverport] [-vmrestoretype (noninstant | instantrestore | instantaccess | vmcleanup | vmfullcleanup)]
```

Linux

You must issue the **vmcli -f restore** command as **tdpvmware** user, and not as **root**.

Parameters

The **vmcli -f restore** command requires that the **VE_VCENTER_NODE_NAME** is set correctly in the **vmcliprofile**. You cannot overwrite this parameter with a command-line entry.

The data mover system (the vStorage Backup Server where the Tivoli Storage Manager backup-archive client is installed) must not set the **ASNODENAME** option.

-c *tsm_mode*

Specify the mode in which Tivoli Storage Manager restores up the virtual environment. The value is set in the **VE_TSM_MODE** parameter in the **vmcliprofile**. You can choose from one of the following modes:

VSPHERE

Specify this value when Tivoli Storage Manager restores individual VMs from a vCenter.

VCloud

Specify this value when Tivoli Storage Manager restores vApps from a vCloud director.

If the mode is not set in the **vmcliprofile**, the **VSPHERE** mode is used with the **vmcli** command.

-I *restoreObjectListFile*

Specify the file that contains the list of VMs or vApps to restore. Each line can contain only one VM identifier (vSphere mode) or one restore specification for a vApp (vCloud mode).

The *restoreObjectListFile* uses the following keywords:

backupid

Each line must begin with the **backupid**. The syntax is **backupid:your_backup_ID**. Specify the Tivoli Storage Manager Object ID for a specific VM backup (vSphere mode) or vApp backup (vCloud mode). Locate the Object ID by using the **vmcli -f inquire_detail** command. This keyword is required for a restore operation.

vmname

Specify the name of the VM that was originally backed up (vSphere mode). If this keyword is not specified, the name `vmname` is used for the restore.

Restrictions: When you specify a keyword in the *restoreObjectListFile*, Data Protection for VMware does not differentiate between a colon (:) used as a keyword separator or a colon that is used in a keyword value. Therefore, use caution when you specify keyword values. In addition, Data Protection for VMware support for VM restore operations is limited to VM names and VMware datacenter names that contain English 7-bit ASCII characters only. VM names and datacenter names that use other language characters are not currently supported. Additional character restrictions are listed in "Unsupported characters in VM or datacenter name" on page 126.

The restore process does not create a snapshot of template VMs in the same manner that a snapshot is created for regular VMs. As a result, VMware VDDK advanced transports (SAN, HotAdd mode), change block tracking (CBT), and incremental backups are not available.

vmname

(Second entry in vSphere mode) Specify the name that you want the restored VM to be named. Existing VMs are not overwritten. Therefore, either rename the VM (by using this keyword) or delete the original VM before you issue the **vmcli -f restore** command.

vappname

In vCloud mode, specify the restore spec for one vApp. This keyword is specified after the `backupid` keyword. The `vappname` value is comprised of this triplet entry:

org=organization name,orgvdc=organization vDC node name,vapp=vApp name

For example, the following *restoreObjectListFile* entry restores vApp named "vApp1" from organization "Mainz_org" and organization virtual datacenter "MZ_Silver" to a new vApp named "vApp1_restore":

```
vappname "vApp1_restore"  
backupid:47110815 vappname:org=Mainz_org,orgvdc=MZ_Silver,vapp=vApp1  
vappname_new:vApp1_restore
```

org=organization,orgvdc=organization vdc,vapp=name of vApp backup

In vCloud mode, use this triplet to specify the following information:

org The name of the organization to which the vApp belongs.

orgvdc

The name of the organization vDC to which the vApp belongs.

vapp The name of the vApp that was originally backed up.

vappname_new

In vCloud mode, specify the new name for vApp to be restored. Existing vApps are not overwritten. As a result, use the `vappname_new` keyword to rename the restore vApp or delete the original vApp before starting the restore operation. If this keyword is not specified, the `vappname` value is used for the restore.

newdatacentername

When you want the restore destination to be a different datacenter, specify the name of that datacenter with this keyword.

newesxhostname

When you want the restore destination to be a different ESX host, specify the name of that ESX host with this keyword.

newdatastoreurl

Specify the name (not the URL) of the VMware datastore where the VM is to be restored. For example, a datastore name such as `datastore1` is supported. A datastore URL such as `sanfs://vmfs_uuid:4d90pa2d-e9ju45ab-065d-00101a7f1a1d/` is not supported.

vmtempdatastore

When you want to issue an instant restore operation, specify a temporary datastore on the ESX host. This temporary datastore contains the configuration information and data of the VM that is created during the operation.

vmautostartvm

When a VM is created for instant access (**vmrestoretype instantaccess**), specify whether to automatically start the VM:

- YES** The VM created for instant access is automatically started.
- NO** The VM created for instant access is not automatically started. It must be manually started by the user. This value is the default.

vmdiskprovision

Specify the type of provisioning for the VM disk that is restored during an instant restore process (**vmrestoretype instant**):

THICK

The disk is created with thick provisioning. This value is the default.

THIN The disk is created with thin provisioning.

An example *restoreObjectListFile* is provided here:

```
# restore of VM "678912345" named "vmName6" to new vmname "vm6newName" to datacenter
"DataCenter2" to ESX esxhostname:esxHost1Name to new datastore "datastore2"
backupid:678912345 vmname:vmName6::vmname:vm6newName newdatacentername:DataCenter2
newesxhostname:esxHost1Name newdatastoreurl:datastore2 vmtempdatastore:datastore2temp
vmdiskprovision:thin
```

Each restore specification must be on a single line. However, for the sake of page formatting, the restore specification in this example is on multiple lines.

Tip: To make sure that correct information is specified in the *restoreObjectListFile*, you can issue the **inquire_detail** command. "Inquire_detail" on page 51 provides current configuration information about the backup environment.

-d *datacenternodename* | *providervDCnodename*

When the **VE_TSM_MODE** parameter specifies VSPHERE, specify the datacenter node name.

When the **VE_TSM_MODE** parameter specifies VCloud, specify the provider vDC node name.

-o datamovernodename

Specify the Tivoli Storage Manager data mover node name. This is the node name for the Tivoli Storage Manager backup-archive client that is installed on the vStorage Backup Server. This node performs the data movement.

[-s tsmserverhostname]

Specify the host name or IP address of the Tivoli Storage Manager server. If this parameter is not specified, the value in the profile is used.

[-n vmclinodename]

Specify the VMCLI node name. This name is the node that connects the Data Protection for VMware command-line interface to the Tivoli Storage Manager server and the Tivoli Storage Manager data mover node. If this parameter is not specified, the value in the profile is used.

[-p tsmserverport]

Specify the port of the Tivoli Storage Manager server.

- If this parameter is not specified in the Data Protection for VMware command-line interface and not specified in the profile, the default port (1500) is used.
- If this parameter is not specified in the Data Protection for VMware command-line interface but is specified in the profile, the value in the profile is used.

Windows **[-vmrestoretype (noninstant | instantrestore | instantaccess | vmcleanup | vmfullcleanup)]**

In a vSphere environment, specify this option to switch between the following operations: existing restore, instant access, or instant restore. Instant access and instant restore capability is supported only for VMware VMs that are hosted on VMware ESXi 5.1 servers, or later versions. The **vmrestoretype** parameter uses the following keywords:

noninstant

A full VM restore is issued.

instantrestore

The VM is started during the restore process.

instantaccess

The VM might be started but it is not restored.

vmcleanup

Components that are no longer needed are cleaned up.

vmfullcleanup

The VM and all its components are cleaned up, regardless of the current state.

Restriction: When an instant restore or instant access operation that is issued from the Tivoli Storage Manager backup-archive client (dsmc) is followed by an instant restore or instant access operation that is issued from the Data Protection for VMware command-line interface (vmcli) or Data Protection for VMware vSphere GUI, the TDPVMwareMount service must be restarted. This situation applies only when the Data Protection for VMware command-line interface accesses the Tivoli Storage Manager server with a nodename different from the one used by the backup-archive client. This restriction applies to any order of operations between the two products.

Restart the service by going to **Start > Administrative Tools > Computer Management > Services and Applications > Services**. Look for service name Data Protection for VMware Recovery Agent in the Services window. The path to the Services window might vary depending on your operating system.

The service does not have to be restarted when the datacenter name is specified with the `asnodename` option in the `dsm.opt` file.

Inquire_config

Use this **vmcli** command to view configuration information about the Tivoli Storage Manager nodes associated with Data Protection for VMware.

Syntax

The **vmcli -f inquire_config** command uses this syntax:

```
vmcli -f inquire_config [-t backuptype] [-v vcenternodename | vcloudnodename] [-s tmsserverhostname] [-n vctrclinodename] [-p tmsserverport]
```

Linux

You must issue the **vmcli -f inquire_config** command as `tdpvmware` user, and not as `root`.

Parameters

[-t *backuptype*]

Specify the type of backup. You can choose from one of the following types:

TSM Select a backup that was created with Tivoli Storage Manager for Virtual Environments. This type must be specified when in vCloud mode.

FCM Select a backup that was created with IBM Tivoli Storage FlashCopy Manager for VMware.

[-v *vcenternodename* | *vcloudnodename*]

Depending on the backup environment, specify the virtual node that represents either a vCenter or the vCloud Director. If this parameter is not specified in the Data Protection for VMware command-line interface, the value in the profile is used.

[-s *tmsserverhostname*]

Specify the host name or IP address of the Tivoli Storage Manager server. If this parameter is not specified, the value in the profile is used.

[-n *vctrclinodename*]

Specify the VMCLI node name. This name is the node that connects the Data Protection for VMware command-line interface to the Tivoli Storage Manager server and the Tivoli Storage Manager data mover node. If this parameter is not specified, the value in the profile is used.

[-p *tmsserverport*]

Specify the port of the Tivoli Storage Manager server.

- If this parameter is not specified in the Data Protection for VMware command-line interface and not specified in the profile, the default port (1500) is used.

- If this parameter is not specified in the Data Protection for VMware command-line interface but is specified in the profile, the value in the profile is used.

vSphere environment example

The parameter values in this output for the `vmcli -f inquire_config -s TSM` command show that the Data Protection for VMware command-line interface recognizes the Tivoli Storage Manager node configuration. As a result, the configuration is correct:

```
#TASK 858 inquire_config 2011082223402852
#PARAM INSTALLED=FCM
#PARAM INSTALLED=TSM
#RUN 860 2011082223402852
#LANG en_US
#PARAM BACKEND=TSM
#PARAM OPERATION_TYPE 4
#PHASE_COUNT 4
#PHASE PREPARE
#PARAM BACKUP_TYPE=0
#PARAM TSM_SERVER_NAME=TEMPLAR.STORAGE.USCA.IBM.COM
#PARAM TSMCLI_NODE_NAME=DPM02_TSMCLI
#PARAM VCENTER_NODE_NAME=DPM02_VCENTER
#PARAM DATACENTER_NODE_NAME=
#PARAM OFFLOAD_HOST_NAME=
#PARAM TSM_OPTFILE=/tmp/T4VE_DtYWYf
#PARAM INPUT_FILE=
#PARAM TRACEFILE=
#PARAM TRACEFLAGS=
#PHASE INITIALIZE
#PHASE INQUIRE_DATACENTER_NODES
#CHILD datacenternode:DATACENTER1::DPM02_DC1
#PARENT vcenternode:DPM02_VCENTER
#PHASE INQUIRE_PROXY_NODES
#CHILD targetnode:DPM02_DC1
#PARENT peernode:DPM02_DC1_DM
#CHILD hladdress:untoro.storage.usca.ibm.com
#PARENT peernode:DPM02_DC1_DM
#CHILD lladdress:62790
#PARENT peernode:DPM02_DC1_DM
#PARAM STATUS=success
#END RUN 860 20110822234030547
#END TASK 858
#INFO FMM16014I The return code is 0.
#END
```

The `PHASE INQUIRE_DATACENTER_NODES` section shows the mapping of the datacenter name from vSphere to the Tivoli Storage Manager node name for that datacenter. The datacenter name is case sensitive and must be identical to the name shown in vSphere for the mapping to function.

The `PHASE INQUIRE_PROXY_NODES` section shows the data mover nodes with proxy access to each data center node. The format for this proxy relationship is shown in pairs:

```
#CHILD targetnode::<datacenter node name>
#PARENT peernode::<data mover node name>
```

vCloud environment example

The parameter values in this output for the `vmcli -f inquire_config -s TSM` command show that the Data Protection for VMware command-line interface recognizes the Tivoli Storage Manager node configuration. As a result, the configuration is correct:

```
#TASK 3 inquire_config 20130109143746117
#PARAM INSTALLED=TSM
#RUN 2 20130109143746117
#LANG en_US
#PARAM BACKEND=TSM
#PARAM OPERATION_TYPE 4
#PHASE_COUNT 5

#PHASE PREPARE
#PARAM BACKUP_TYPE=0
#PARAM TSM_SERVER_NAME=VM-08R2-TSMDEV2
#PARAM TSM_SERVER_PORT=1500
#PARAM VCLLOUD
#PARAM TSMCLI_NODE_NAME=VMCLI_OFIR
#PARAM VCLLOUD_NODE_NAME=VCD_EUROPE
#PARAM DATACENTER_NODE_NAME=
#PARAM OFFLOAD_HOST_NAME=
#PARAM PASSWORD_TYPE=CLINODE
#PARAM TSM_OPTFILE=C:\Users\qa\AppData\Local\Temp\1\T4VEEF3.tmp
#PARAM INPUT_FILE=
#PARAM TRACEFILE=tsmcli.trace
#PARAM TRACEFLAGS=api api_detail

#PHASE INITIALIZE

#PHASE INQUIRE_PVDC_NODES

#CHILD targetnode:VCD_EUROPE
#PARENT peernode:PVDC_GOLD
#CHILD pvdcname:Gold provider vDC
#PARENT peernode:PVDC_GOLD
#CHILD targetnode:VCD_EUROPE
#PARENT peernode:PVDC_SILVER
#CHILD pvdcname:Silver provider vDC
#PARENT peernode:PVDC_SILVER

#PHASE INQUIRE_OVDC_NODES

#CHILD targetnode:PVDC_GOLD
#PARENT peernode:OVDC_HAIFA
#CHILD orgname:Israel
#PARENT peernode:OVDC_HAIFA
#CHILD orgvdcname:Haifa organization virtual data center
#PARENT peernode:OVDC_HAIFA
#CHILD targetnode:PVDC_SILVER
#PARENT peernode:OVDC_JERUSALEM
#CHILD orgname:Israel
#PARENT peernode:OVDC_JERUSALEM
#CHILD orgvdcname:Jerusalem organization virtual data center
#PARENT peernode:OVDC_JERUSALEM
#CHILD targetnode:PVDC_GOLD
#PARENT peernode:OVDC_MUNICH
#CHILD orgname:Germany
#PARENT peernode:OVDC_MUNICH
#CHILD orgvdcname:Munich organization virtual data center
#PARENT peernode:OVDC_MUNICH
#CHILD targetnode:PVDC_SILVER
#PARENT peernode:OVDC_MAINZ
```

```

#CHILD  orgname:Germany
#PARENT  peernode:OVDC_MAINZ
#CHILD  orgvdcname:Mainz organization virtual data center
#PARENT  peernode:OVDC_MAINZ

#PHASE INQUIRE_DM_NODES

#CHILD  targetnode:PVDC_GOLD
#PARENT  peernode:DM_DM1
#CHILD  targetnode:OVDC_HAIFA
#PARENT  peernode:DM_DM1
#CHILD  targetnode:OVDC_MUNICH
#PARENT  peernode:DM_DM1
#CHILD  hladdress:vm-DM1.com
#PARENT  peernode:DM_DM1
#CHILD  lladdress:49391
#PARENT  peernode:DM_DM1

#CHILD  targetnode:PVDC_GOLD
#PARENT  peernode:DM_DM2
#CHILD  targetnode:OVDC_HAIFA
#PARENT  peernode:DM_DM2
#CHILD  targetnode:OVDC_MUNICH
#PARENT  peernode:DM_DM2
#CHILD  hladdress:vm-DM2.com
#PARENT  peernode:DM_DM2
#CHILD  lladdress:49392
#PARENT  peernode:DM_DM2

#CHILD  targetnode:PVDC_SILVER
#PARENT  peernode:DM_DM3
#CHILD  targetnode:OVDC_JERUSALEM
#PARENT  peernode:DM_DM3
#CHILD  targetnode:OVDC_MAINZ
#PARENT  peernode:DM_DM3
#CHILD  hladdress:vm-DM3.com
#PARENT  peernode:DM_DM3
#CHILD  lladdress:49391
#PARENT  peernode:DM_DM3

#CHILD  targetnode:PVDC_SILVER
#PARENT  peernode:DM_DM4
#CHILD  targetnode:OVDC_JERUSALEM
#PARENT  peernode:DM_DM4
#CHILD  targetnode:OVDC_MAINZ
#PARENT  peernode:DM_DM4
#CHILD  hladdress:vm-DM4.com
#PARENT  peernode:DM_DM4
#CHILD  lladdress:49392
#PARENT  peernode:DM_DM4

#PARAM STATUS=success
#END RUN 2 20130109143749906
#END TASK 3
#INFO FMM16014I The return code is 0.
#END

```

The PHASE INQUIRE_PVDC_NODES section shows the provider VDC nodes with proxy access to each vCloud Director node. The format for this proxy relationship is shown in pairs:

```

#CHILD targetnode::<vCloud Director node name>
#PARENT peernode::<provider VDC name>

```

The PHASE INQUIRE_OVDC_NODES section shows the organization VDC nodes with proxy access to each provider VDC node. The format for this proxy relationship is shown in pairs:

```
#CHILD targetnode::<provider VDC node name>
#PARENT peernode::<organization VDC node name>
```

The PHASE INQUIRE_DM_NODES section shows the data mover nodes with proxy access to each provider VDC node and organization VDC node. The format for this proxy relationship is shown in pairs:

```
#CHILD targetnode::<provider VDC node name> OR <organization VDC node name>
#PARENT peernode::<data mover node name>
```

Inquire_detail

Use this **vmcli** command to view configuration information about the backup environment associated with Data Protection for VMware.

Syntax

The **vmcli -f inquire_detail** command uses this syntax:

```
vmcli -f inquire_detail -d datacenternodename | organizationvDCnodename [-a] [-n vmclinodename] [-o datamovernodename] [-p tmsserverport] [-e vmddetail | vappdetail] [-q dmverify | vmfs | vmsingle | vappfs | vappsingle (-I inputfile)] [-s tmsserverhostname] [-t backupType] [-vmrestoretype (instantrestore | instantaccess | alltype)]
```

Linux

You must issue the **vmcli -f inquire_detail** command as `tdpvmware` user, and not as root.

Parameters

-d *datacenternodename* | *organizationvDCnodename*

When the **VE_TSM_MODE** parameter specifies VSPHERE, specify the datacenter node name.

When the **VE_TSM_MODE** parameter specifies vCloud, specify the organization vDC node name.

[-a]

Specify to show only the active backups on the Tivoli Storage Manager server.

[-n *vmclinodename*]

Specify the VMCLI node name. This name is the node that connects the Data Protection for VMware command-line interface to the Tivoli Storage Manager server and the Tivoli Storage Manager data mover node. If this parameter is not specified, the value in the profile is used.

[-o *datamovernodename*]

Specify the Tivoli Storage Manager data mover node name.

[-p *tmsserverport*]

Specify the port of the Tivoli Storage Manager server.

- If this parameter is not specified in the Data Protection for VMware command-line interface and not specified in the profile, the default port (1500) is used.
- If this parameter is not specified in the Data Protection for VMware command-line interface but is specified in the profile, the value in the profile is used.

[-e vmdetail | vmappdetail]

Specify vmdetail to show more detailed information about the backed up VMs. For example, the parameter shows information about disks that are attached to the VM. This parameter is valid only when the **VE_TSM_MODE** parameter specifies VSPHERE.

Specify vmappdetail to show more detailed information about the backed up vApps. For example, this parameter shows the following information:

- VMs that are attached to the vApp.
- VM name as it appears in both vCloud and vSphere mode.
- Success or fail status for the VM backup.

This parameter is valid only when the **VE_TSM_MODE** parameter specifies vCloud.

[-q dmverify | vmfs | vmsingle | vappfs | vappsingle (-I inputfile)]

dmverify

Specify to query the status of the Tivoli Storage Manager data mover node identified by the **-o** parameter. You must specify the **-d** and **-o** parameters when specifying dmverify.

vmfs Specify to query all VMware Virtual Machine File Systems (VMFS). This parameter shows high level information about all VMs. This parameter is valid only in vSphere mode.

vmsingle

Specify to query individual VMs that are being restored during an instant access or instant restore operation. This parameter is valid only in vSphere mode.

vappfs

Specify to show high level information about all vApps. This parameter is valid only in vCloud mode.

vappsingle

Specify to show information about individual vApps that are identified in the *inputfile*. This parameter is valid only in vCloud mode.

-I inputfile

The *inputfile* value defines the full path and name of the input file. This keyword is valid with the **vmsingle** and **vappsingle** parameters only.

In vSphere mode, specify the name of the VM to query. You can specify this keyword for each VM that you want to query: *vmname:vmname*. For example:

```
vmname:vm1  
vmname:vm2
```

In vCloud mode, specify the name of the VM to query. You can specify this keyword for each VM you want to query: *vappname:vappname*. For example:

```
vappname:vapp1  
vappname:vapp2
```

When the **q** option is not specified, the default value is **vmfs** (in vSphere mode) and **vappfs** (in vCloud mode). When the *inputfile* entry contains spaces, enclose the entry with quotation marks. For example:

-I "/my dir/my file"

[-s *tmsserverhostname*]

Specify the host name or IP address of the Tivoli Storage Manager server. If this parameter is not specified, the value in the profile is used.

[-t *backupType*]

Specify one of the following backup types to query:

ALL Specifies that the **inquire_detail** command is applied to all registered backup types.

FCM Specifies that the **inquire_detail** command is applied to only Tivoli Storage FlashCopy Manager for VMware backups.

Tivoli Storage FlashCopy Manager for VMware is a separately licensed product that contains its own user documentation. Familiarity with this product and its documentation is necessary in order to adequately implement a comprehensive plan for protecting your VMs.

TSM Specifies that the **inquire_detail** command is applied to only Data Protection for VMware backups. This value must be specified when in vCloud mode.

Windows

[-vmrestoretype (*instantrestore* | *instantaccess* | *alltype*)]

Specify this option to query active instant access or restore operations. This option also queries stale or orphan artifacts after a failure. The **vmrestoretype** parameter uses the following keywords:

instantrestore

The query lists VMs that are active in an instant restore operation.

instantaccess

The query lists VMs that are active in an instant access process.

alltype

The query lists VMs that are active in all instant operations.

Restriction: When an instant restore or instant access operation that is issued from the Tivoli Storage Manager backup-archive client (dsmc) is followed by an instant restore or instant access operation that is issued from the Data Protection for VMware command-line interface (vmcli) or Data Protection for VMware vSphere GUI, the TDPVMwareMount service must be restarted. This situation applies only when the Data Protection for VMware command-line interface accesses the Tivoli Storage Manager server with a nodename different from the one used by the backup-archive client. This restriction applies to any order of operations between the two products.

Restart the service by going to **Start > Administrative Tools > Computer Management > Services and Applications > Services**. Look for service name Data Protection for VMware Recovery Agent in the Services window. The path to the Services window might vary depending on your operating system.

The service does not have to be restarted when the datacenter name is specified with the **asnodename** option in the **dsm.opt** file.

Example

In this example, the **vmcli -f inquire_detail** command is issued to query the VM named *antures* for details:

```
vmcli -f inquire_detail -s BORODIN.MAINZ.DE.IBM.COM -p 1505 -n JF_VMCLI_HANNE  
-v CHRISTO.MAINZ.DE.IBM.COM -o JF_MAINZ_DEVELOPMENT_DC_DM -d JF_MAINZ_DEVELOPMENT_DC  
-q vmsingle -I .\inputfile.txt --vmrestoretype (instantrestore | instantaccess)
```

The *inputfile* contains this statement:

```
vmname:antures
```

Set_domain

Use this **vmcli** command to apply changes to the domain settings.

Syntax

The **vmcli -f set_domain** command uses this syntax:

```
vmcli -f set_domain -I domainObjectListFile
```

Linux

You must issue the **vmcli -f set_domain** command as **tdpvmware** user, and not as **root**.

The new domain value is stored in the **vmcli** database.

Parameters

-I domain ObjectListFile

The *domainObjectListFile* has the following requirements:

- The file contains one VMware datacenter identifier per line.
- The valid identifier is the datacenter name.

If no domain is configured, the current instance is used to manage all datacenters that are available in the vCenter. When the **vmcli -f set_domain** command is run without **-I** parameter, the domain configuration is deleted.

An example *domainObjectListFile* is provided here:

```
#datacentername:datacenterName  
datacentername:datacenterXYZ  
datacentername:datacenterA*  
datacentername:datacenterB*  
...
```

Set_mapping

Use this **vmcli** command to set mapping between the vCloud objects and Tivoli Storage Manager node name.

Syntax

The **vmcli -f set_mapping** command uses this syntax:

```
vmcli -f set_mapping -I mappingInputFile [-s tsmserverhostname] [-n vmclinodename]  
[-p tsmserverport]
```

Linux

You must issue the **vmcli -f set_mapping** command as the `tdpvmware` user, and not as root.

To confirm that the mapping is set correctly, issue the **vmcli -f inquire_config** command.

The **vmcli -f set_mapping** command is valid only in a vCloud environment.

Parameters

-I *mappingInputFile*

Specify the following mapping information in this file:

pvdnode: *provider vDC node name*

Specify the provider vDC node name.

pvdname: *provider vDC name*

Specify the provider vDC name. The name is case sensitive.

orgname: *organization name*

Specify the name of the organization. The name is case sensitive.

orgvdcname: *organization vDC*

Specify the name of the organization vDC. The name is case sensitive.

orgvdcnode: *organization vDC node name*

Specify the organization vDC node name. The name is converted to upper case.

The following keywords are required to set the provider vDC name:

- `pvdnode`
- `pvdname`

The following keywords are required to set the organization and organization vDC name:

- `pvdnode`
- `orgname`
- `orgvdcname`
- `orgvdcnode`

When the *mappingInputFile* entry contains more spaces, enclose the entry with quotation marks. For example:

```
-I "/my dir/my input file"
```

[-s *tmsserverhostname*]

Specify the host name or IP address of the Tivoli Storage Manager server. If this parameter is not specified, the value in the profile is used.

[-p *tmsserverport*]

Specify the port of the Tivoli Storage Manager server.

- If this parameter is not specified in the Data Protection for VMware command-line interface and not specified in the profile, the default port (1500) is used.
- If this parameter is not specified in the Data Protection for VMware command-line interface, but is specified in the profile, the value in the profile is used.

[-n *vmclinodename*]

Specify the VMCLI node name. This is the node that connects the Data

Protection for VMware command-line interface to the Tivoli Storage Manager server and the Tivoli Storage Manager data mover node. If this parameter is not specified, the value in the profile is used.

Example

In this example, the `vmcli -f set_mapping` command is issued to set the mapping between the Tivoli Storage Manager node "pvdc_oslo" and the real provider vDC, "Oslo Norway". The *mappingInputFile* contains this entry:

```
pvdcnode:pvdc_oslo
pvdcname:Oslo Norway
```

In this example, the `vmcli -f set_mapping` command is issued to set the mapping for the provider vDC node `pvdc_oslo`, the organization "Production", the organization vDC "Oslo 1", and the organization vDC node "ovdc_oslo1". The *mappingInputFile* contains this entry:

```
pvdcnode:pvdc_oslo
orgname:Production
orgvdcname:Oslo1
orgvdcnode:ovdc_oslo1
```

Related reference:

"`Inquire_config`" on page 47

Set_option

Use this **vmcli** command to set a parameter in the `vmcli` profile.

Syntax

The **vmcli -f set_option** command uses this syntax:

```
vmcli -f set_option [-c tsm_mode] [-m datacentermapping][-n datamovernodename] [-p tsmserverport] [-s tsmserverhostname] [-v vctrnodename]
```

Linux

You must issue the **vmcli -f set_option** command as the `tdpvmware` user, and not as root.

Parameters

-c *tsm_mode*

Specify the mode in which Tivoli Storage Manager backs up the virtual environment. The value is set in the `VE_TSM_MODE` parameter in the `vmcli` profile. You can choose from one of the following modes:

VSPHERE

Specify this value when Tivoli Storage Manager backs up and restores individual VMs from a vCenter.

VCloud

Specify this value when Tivoli Storage Manager backs up and restores vApps from a vCloud director.

If the mode is not set in the `vmcli` profile, the VSPHERE mode is used with the **vmcli** command.

-m *datacentermapping*

Specify the name of the data center that is associated with the datacenter node name (`DC_name::DC_nodename`). The `DC_name` value is case sensitive and must match the name of your datacenter.

[-n *datamovernodename*]

Specify the Tivoli Storage Manager data mover node name. This name is the node name for the Tivoli Storage Manager backup-archive client that is installed on the vStorage Backup Server. This node performs the data movement.

[-p *tmsserverport*]

Specify the port of the Tivoli Storage Manager server.

- If this parameter is not specified in the Data Protection for VMware command-line interface and not specified in the profile, the default port (1500) is used.
- If this parameter is not specified in the Data Protection for VMware command-line interface, but is specified in the profile, the value in the profile is used.

[-s *tmsserverhostname*]

Specify the host name or IP address of the Tivoli Storage Manager server. If this parameter is not specified, the value in the profile is used.

[-v *vcinternodename*]

Specify the vCenter node name. This node is the virtual node that represents a vCenter. If this parameter is not specified in the Data Protection for VMware command-line interface, the value in the profile is used.

Example

In this example, the `vmcli -f set_option` command is issued to set the Tivoli Storage Manager server and its port:

```
vmcli -f set_option -s TEMPLE.MYCOMPANY.XYZ.COM -p 1650
```

The following output is displayed:

```
Setting VE_TSM_SERVER_NAME to: TEMPLE.MYCOMPANY.XYZ.COM
Setting VE_TSM_SERVER_PORT to: 1650
#INFO FMM16014I The return code is 0.
```

In this example, the `vmcli -f set_option` command is issued to set the data center mapping:

```
vmcli -f set_option -m DataCenter2::NANO_DATACENTER123
```

The following mapping is set in the profile:

```
VE_DATACENTER_NAME    DataCenter2::NANO_DATACENTER123
```

Set_password

Use this **vmcli** command to set the password for the guest VM.

Syntax

The **vmcli -f set_password** command uses this syntax:

```
vmcli -f set_password [-type VMGuest] -I passwordfile
```

The **-type VMGuest** parameter is required when you set the password for application protection reporting.

Linux

You must issue the **vmcli -f set_password** command as `tdpvmware` user, and not as `root`.

Linux

Windows

You must issue the **vmcli -f set_password** command before you run a guest scan operation.

Parameters

-type VMGuest

This parameter identifies that the password applies to a VM. This parameter is required when you set the password for application protection reporting.

-I passwordfile

Specify the following information in this file:

datacentername: *data center in vmcliprofile*

Specify the datacenter that contains the VM guests. The datacenter must be defined in the *vmcliprofile*. The password is applied to that datacenter only. For example:

```
datacentername:DataCenter1
```

username: *common VM guest user*

Specify the user name that logs in to the VM guest. For Windows, the *DOMAIN\User* format is allowed for the user name. For example:

```
username:Domain1\Administrator
```

password: *password*

Specify the password to log in to the VM guest.

The settings in the *passwordfile* must be specified on the same line.

Examples

Linux

This example creates (or sets) a common VM guest name and password that is associated with DataCenter3. The *vmcliprofile* contains the following

VE_DATACENTER_NAME settings:

```
VE_DATACENTER_NAME: DataCenter1:TSM_DC1
VE_DATACENTER_NAME: DataCenter2:TSM_DC2
VE_DATACENTER_NAME: DataCenter3:TSM_DC3
VE_DATACENTER_NAME: DataCenter4:TSM_DC4
```

The *passwordfile* contains the following settings. The settings in the *passwordfile* must be specified on the same line:

```
datacentername:DataCenter3 username:tdpvmwareuserY password:tdpvmwareuserYpwd
```

As a result, the **vmcli -f set_password -type VMGuest -I password.txt** sets the password as shown in the command output:

```
Tivoli Storage Manager Command Line Wrapper for Virtual Environments Version: 7.1.0.00
Build Date: Mon Nov 12 20:03:31 2012
Tivoli Storage Manager API Version 71000
Tivoli Storage Manager Command Line Wrapper Compile Version 71000
#PARAM OPERATION_TYPE 8
#PHASE_COUNT 3
#PHASE PREPARE
#PARAM BACKUP_TYPE=0
#PARAM TSM_SERVER_NAME=ORION.FINANCE.MYCOMPANY.COM
#PARAM TSM_SERVER_PORT=1500
#PARAM TSMCLI_NODE_NAME=KA3095_TSMCLI_SLUDGE
#PARAM VCENTER_NODE_NAME=
#PARAM DATACENTER_NODE_NAME=
#PARAM OFFLOAD_HOST_NAME=
#PARAM TSM_OPTFILE=/tmp/T4VE_OD3PZ9
#PARAM INPUT_FILE=/opt/tivoli/tsm/tdpvmware/common/scripts/password.txt
#PARAM TRACEFILE=
#PARAM TRACEFLAGS=
#PHASE INITIALIZE
#PHASE SET_PASSWORD
STATUS=success
#END
```

Windows This example creates (or sets) a common VM guest name and password that is associated with DataCenter1. The *vmcliprofile* contains the following **VE_DATACENTER_NAME** settings:

```
VE_DATACENTER_NAME: DataCenter1:TSM_DC1
VE_DATACENTER_NAME: DataCenter2:TSM_DC2
```

The *passwordfile* contains the following settings. The settings in the *passwordfile* must be specified on the same line:

```
datacentername:DataCenter1 username:Domain1\Administrator password:secret1
```

As a result, the **vmcli -f set_password -type VMGuest -I password.txt** sets the password as shown in the command output:

```
Tivoli Storage Manager Command Line Wrapper for Virtual Environments Version: 7.1.0.00
Build Date: Mon Nov 12 20:03:31 2012
Tivoli Storage Manager API Version 71000
Tivoli Storage Manager Command Line Wrapper Compile Version 71000
#PARAM OPERATION_TYPE 8
#PHASE_COUNT 3
#PHASE PREPARE
#PARAM BACKUP_TYPE=0
#PARAM TSM_SERVER_NAME=ORION.FINANCE.MYCOMPANY.COM
#PARAM TSM_SERVER_PORT=1500
#PARAM TSMCLI_NODE_NAME=KA3095_TSMCLI_SLUDGE
#PARAM VCENTER_NODE_NAME=
#PARAM DATACENTER_NODE_NAME=
#PARAM OFFLOAD_HOST_NAME=
#PARAM TSM_OPTFILE=/tmp/T4VE_OD3PZ9
#PARAM INPUT_FILE=C:\Program Files\Common Files\Tivoli\TDPVMware\VMwarePlugin\
scripts\password.txt
#PARAM TRACEFILE=
#PARAM TRACEFLAGS=
#PHASE INITIALIZE
#PHASE SET_PASSWORD
STATUS=success
#END
```

Windows When you create the password file by using the **echo** command, make sure that a space does not exist between the password (*password1*) and the greater-than sign (>). For example:

```
echo password1> pwd.txt
```

or

```
echo password1>pwd.txt
```

This example sets the password (*password1*) in file *pwd.txt*:

```
vmcli -f set_password -I pwd.txt
```

Linux Create the password file (*pwd.txt*) by specifying the **echo** command:

```
echo password1 > pwd.txt
```

This example sets the password (*password1*) in file *pwd.txt*:

```
vmcli -f set_password -I pwd.txt
```

Linux **Windows** This example sets the password in file *pwd.txt* for domain *mydomain* and user *user1*:

```
set -f set_password -I pwd.txt -pwtype domain -domain mydomain -user user1
```

Get_password_info

Use this **vmcli** command to view the status of guest credentials that are set for the managed datacenters.

Syntax

The **vmcli -f get_password_info** command uses this syntax:

```
vmcli -f get_password_info -type VMGuest
```

Linux

You must issue the **vmcli -f get_password_info** command as *tdpvmware* user, and not as root.

Parameters

-type VMGuest

This required parameter identifies that the password information is returned for a guest VM. The **username** value (shown in the #CHILD statement) of the command output confirms that the password is set for that **username**. The **datacentername** value (shown in the #PARENT statement) of the command output identifies the associated datacenter for which the password is set.

Example

Windows This example shows the status of the managed datacenters that are associated with the VM guest:

```
vmcli -f get_password_info -type VMGuest
#TASK 0 get_password_info 20130129162344670
#RUN 0 20130129162344685
#LANG en_US
#PARAM BACKEND=TSM
```

```
#PARAM OPERATION_TYPE 4
#PHASE PREPARE
#PARAM BACKUP_TYPE=0
#PARAM TSM_SERVER_NAME=
#PARAM TSM_SERVER_PORT=
#PARAM TSMCLI_NODE_NAME=
#PARAM VCENTER_NODE_NAME=
#PARAM DATACENTER_NODE_NAME=
#PARAM OFFLOAD_HOST_NAME=
#PARAM PASSWORD_TYPE=VMGUEST
#PARAM TSM_OPTFILE=C:\Users\ADMINI~1\AppData\Local\Temp\2\T4V3B15.tmp
#PARAM INPUT_FILE=
#PARAM TRACEFILE=
#PARAM TRACEFLAGS=
#CHILD username:<mydomain\myuser>
#PARENT datacentername:DataCenter1
#CHILD username:<mydomain\myuser>
#PARENT datacentername:DataCenter2
#CHILD username:<mydomain\myuser>
#PARENT datacentername:DataCenter3
#PARAM STATUS=success
#END RUN 0 2013012916234513
#END TASK 0
#INFO FMM16014I The return code is 0.
#END
```

Start_guest_scan

Use this **vmcli** command to scan guest VMs for application information.

The **vmcli -f start_guest_scan** command saves VM name, application, and globally unique identifier (GUID) information to the Tivoli Storage Manager server.

You must issue the **vmcli -f set_password** command before you run a guest scan operation.

Syntax

The **vmcli -f start_guest_scan** command uses this syntax:

```
vmcli -f start_guest_scan -dcscan "datacenterNmcliprofile,...," | ALL_DC -o
datamovernodename
```

Required Parameters

-dcscan *datacenterNmcliprofile* | **ALL_DC**

Specify one or more datacenter names that are defined in the *vmcliprofile*. Repeat datacenter names with a comma. Double quotation marks (") must be specified at the beginning and at the end of the datacenter name list. For example:

```
-dcscan "Local DC,svc"
```

To scan all VM guests in all datacenters, specify the **ALL_DC** parameter.

-o *datamovernodename*

Specify the Tivoli Storage Manager data mover node that is configured with proxy authority access to the datacenters specified by **-dcscan**.

During a **vmcli -f start_guest_scan** operation, Data Protection for VMware copies files to a temporary subdirectory in the remote directory (\$TEMP_REMOTE\TSMSCAN) on the guest VM. The remote directory must be unlocked

and not used by another application. Data Protection for VMware determines the location of the remote directory in the following order:

1. If the **TEMP** environment variable is set, **TEMP_REMOTE** is set as the **TEMP** environment variable.
2. If the **TEMP** environment variable is not set, **TEMP_REMOTE** is set as C:\TEMP.

Example

Windows In this example, the *vmcliprofile* contains the following **VE_DATACENTER_NAME** settings:

```
VE_DATACENTER_NAME: DataCenter1:TSM_DC1
VE_DATACENTER_NAME: DataCenter2:TSM_DC2
```

The data mover node, VC1_DC1_DM1, is configured with proxy authority access to DataCenter1 and DataCenter2.

Windows The following command is issued to scan all guest VMs in DataCenter1 and DataCenter2:

```
vmcli -f start_guest_scan -dcscan "DataCenter1,DataCenter2" -o VC1_DC1_DM1
```

The following application information is displayed:

```
Tivoli Storage Manager Command Line Wrapper for Virtual Environments
Version: 7.1.0.00
Build Date: Mon Apr 8 20:03:31 2012
Tivoli Storage Manager API Version 71000
Tivoli Storage Manager Command Line Wrapper Compile Version 71000
#PARAM OPERATION_TYPE 9
#PHASE_COUNT 4
#PHASE PREPARE
#PARAM BACKUP_TYPE=0
#PARAM TSM_SERVER_NAME=OREO.STORE.XYZ.COM
#PARAM TSM_SERVER_PORT=1500
#PARAM TSMCLI_NODE_NAME=VC1_VCLI1
#PARAM VCENTER_NODE_NAME=VC1
#PARAM DATACENTER_NODE_NAME=VC1_DC1
#PARAM OFFLOAD_HOST_NAME=VC1_DC1_DM1
#PARAM PASSWORD_TYPE=CLINODE
#PARAM TSM_OPTFILE=C:\Users\ADMINI~1\AppData\Local\Temp\2\T4V9393.tmp
#PARAM INPUT_FILE=
#PARAM TRACEFILE=c:\amd64_unicode\tsmcli.trace
#PARAM TRACEFLAGS=service,VMVCB,MTSMVSS,verbdetail,C2C
#PHASE INITIALIZE
#CHILD targetnode:VC1_DC1
#PARENT peernode:VC1_DC1_DM1
#CHILD hladdress:9.52.62.65
#PARENT peernode:VC1_DC1_DM1
#CHILD lladdress:50408
#PARENT peernode:VC1_DC1_DM1
#PHASE READ_DATACENTER_GUEST_PASSWORD
#PHASE SCANGUEST
#PARAM STATUS=success

#CHILD scanid: DataCenter1::VC1_DC1.1358316054281
#PARENT datacentername: DataCenter1::VC1_DC1
#PARAM OPERATION_TYPE 9 #PHASE_COUNT 4
#PHASE PREPARE
#PARAM BACKUP_TYPE=0
#PARAM TSM_SERVER_NAME=OREO.STORE.XYZ.COM
#PARAM TSM_SERVER_PORT=1500
#PARAM TSMCLI_NODE_NAME=VC1_VCLI1
#PARAM VCENTER_NODE_NAME=VC1
#PARAM DATACENTER_NODE_NAME=VC1_DC2
```

```
#PARAM OFFLOAD_HOST_NAME=VC1_DC1_DM1
#PARAM PASSWORD_TYPE=CLINODE
#PARAM TSM_OPTFILE=C:\Users\ADMINI~1\AppData\Local\Temp\2\T4V50B.tmp
#PARAM INPUT_FILE= #PARAM TRACEFILE=c:\amd64_unicode\tsmcli.trace
#PARAM TRACEFLAGS=service,VMVCB,MTSMVSS,verbdetail,C2C
#PHASE INITIALIZE #CHILD targetnode:VC1_DC2
#PARENT peernode:VC1_DC1_DM1
#CHILD hladdress:9.52.62.65
#PARENT peernode:J_VC1_DC1_DM1
#CHILD lladdress:50408
#PARENT peernode:VC1_DC1_DM1
#PHASE READ_DATACENTER_GUEST_PASSWORD
#PHASE SCANGUEST
#PARAM STATUS=success
#CHILD scanid: DataCenter2::VC1_DC2.1358316054281
#PARENT datacentername:DataCenter2::VC1_DC2
#INFO FMM16014I The return code is 0.
#END
```

Windows The #PARAM STATUS=success message (in the #PHASE SCANGUEST section) confirms only that the datacenter was successfully submitted for processing by the data mover. The actual scan status for each VM is available only after the data mover completed processing that VM. To view the scan status of an individual VM, see the value in the Scan Status column of the Data Protection for VMware vSphere GUI Application Configuration Status report. To view the overall status of the scan operation, see the **Overall Scan Status** value in the Data Protection for VMware vSphere GUI Report window.

Important: If you receive an error after you run the `vmcli -f start_guest_scan` command, view the contents of the `dsmerror.log` file for more information. The `dsmerror.log` file is on the system that is associated with the Tivoli Storage Manager data mover node defined by the **OFFLOAD_HOST_NAME** parameter in the command output. By default, error log files are in the installation directory: `C:\Program Files\Tivoli\TSM\baclient`

Profile parameters

Use the Data Protection for VMware command-line interface profile to configure settings for backup and restore tasks in your environment.

The profile is located in this directory on the system where the Data Protection for VMware vSphere GUI is installed:

Linux `/home/tdpvmware/tdpvmware/config`

Windows `C:\Program Files\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts`

DERBY_HOME *<path to Derby database>*

This parameter specifies the location of the Derby database that is used by the Data Protection for VMware command-line interface.

Example:

Linux

```
DERBY_HOME /home/tdpvmware/tdpvmware
```

Windows

This parameter is valid in a vSphere or vCloud Director environment.

VE_DATACENTER_NAME <*data_center_name::DATA_CENTER_NODE_NAME*>

Specify the datacenter (data center name) with a value that is case-sensitive and that matches the datacenter name used in the vCenter. Specify the virtual node (DATA_CENTER_NODE_NAME) that maps to the datacenter. If the vCenter manages several datacenters, you can specify this parameter for each datacenter. However, the Data Protection for VMware vSphere GUI does not support datacenters with the same name in the vCenter.

Example:

```
VE_DATACENTER_NAME DataCenter1::Fin_Datacenter1
VE_DATACENTER_NAME DataCenter2::Fin_Datacenter2
```

This parameter is valid only in a vSphere environment.

Restriction: Data Protection for VMware support for VM backup and restore operations is limited to VM names and datacenter names that contain English 7-bit ASCII characters only. VM names and datacenter names that use other language characters are not currently supported. Additional character restrictions are listed in “Unsupported characters in VM or datacenter name” on page 126.

After a datacenter name is created and associated with a Tivoli Storage Manager node, be aware of these restrictions:

- Do not change the datacenter name in the vCenter without also creating a Tivoli Storage Manager node name and associating it with the new datacenter name.
- Do not change the datacenter name and the profile without also changing the Tivoli Storage Manager node name.
- Do not create a datacenter mapping value in the profile with a previously used Tivoli Storage Manager node.

When the datacenter name in the vCenter has changed, you must complete these steps before attempting any operations:

1. Register a datacenter node for the new datacenter name.
2. Grant proxy authority to the new datacenter node to perform tasks on behalf of the vCenter node.
3. Update the profile with the new datacenter mapping.
4. Grant proxy authority to the Tivoli Storage Manager data mover nodes to perform tasks on behalf of the new datacenter node.
5. Remove any entry from the profile that used the previous datacenter node or vCenter node name.

VE_TRACE_FILE <*path and name of trace file*>

Specify the full path and name of the file to be used to contain trace information. Activate tracing only when instructed to do so by IBM Software Support.

This parameter is valid in a vSphere or vCloud Director environment.

VE_TRACE_FLAGS <flags>

Specify one or more trace flags. Multiple trace flags are separated with a space. Activate tracing only when instructed to do so by IBM Software Support.

This parameter is valid in a vSphere or vCloud Director environment.

VE_TSMCLI_NODE_NAME <VMCLI node>

Specify the VMCLI node. This node connects the Data Protection for VMware command-line interface to the Tivoli Storage Manager server and Tivoli Storage Manager data mover node.

Example:

```
VE_TSMCLI_NODE_NAME VC1_VCLI1
```

This parameter is valid in a vSphere or vCloud Director environment.

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

VE_TSM_MODE V CLOUD I V SPHERE

Specify the VMware environment that Data Protection for VMware protects. You can specify one of the following environments:

V CLOUD

Specify this value when Data Protection for VMware protects data in a vCloud Director environment.

V SPHERE

Specify this value when Data Protection for VMware protects data in a vSphere environment.

Example:

```
VE_TSM_MODE V CLOUD
```

This parameter is valid in a vSphere or vCloud Director environment.

VE_TSM_SERVER_NAME <server host name or IP address>

Specify the host name or IP address of the Tivoli Storage Manager server used for backup operations. There is no default value.

Example:

```
VE_TSM_SERVER_NAME tmsserver.xyz.yourcompany.com
```

This parameter is valid in a vSphere or vCloud Director environment.

VE_TSM_SERVER_PORT <port name>

Specify the port name to use for the Tivoli Storage Manager server. The default value is 1500.

Example:

```
VE_TSM_SERVER_PORT 1500
```

This parameter is valid in a vSphere or vCloud Director environment.

VE_VCENTER_NODE_NAME <vCenter node>

Specify the vCenter node. This virtual node represents a vCenter.

Example:

```
VE_VCENTER_NODE_NAME VC1
```

In vCloud mode, the **VE_VCENTER_NODE_NAME** parameter is the top-level node that represents the vCloud.

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_DB_BACKUP *NO AT[day[, day[,.....]]] time T0 backup location*

This parameter controls the backup of the Derby database containing the metadata of the Data Protection for VMware command-line interface. Specify one of these values:

NO This option does not perform a backup of the Derby database.

AT *[day[, day[,.....]]] time_in _24_H*

This option creates a backup on the specified day or days at the specified time, which is triggered by the scheduler. If the day value is not specified, a daily backup is created. Specify one of these values: MON, TUE, WED, THU, FRI, SAT, SUN.

You can separate these values by a comma or a blank space.

AFTER_BACKUP

This option creates a backup of the Derby database after each Data Protection for VMware backup operation.

The default location for the backups of the Derby database is *install_dir/derby_backups*. Specify *T0 path* to set a custom path.

Example:

```
VMCLI_DB_BACKUP AT 00:00
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_DB_BACKUP_VERSIONS *<number>*

Specify the maximum number of backup generations that are maintained for the Derby database, before the oldest version is overwritten by a new version. This parameter applies only to the backups of the Derby database containing metadata. It has no effect on the number of backup generations that are maintained for the backups of a vSphere environment. The default value is 3.

Example:

```
VMCLI_DB_BACKUP_VERSIONS 3
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_DB_HOST *<Derby database local host name>*

Specify the local host name of the Derby database. You can specify the host name (localhost) or the IP address (0.0.0.0).

Example:

```
VMCLI_DB_HOST localhost
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_DB_NAME *<Derby database name>*

Specify the name of the Derby database. The default value is VMCLIDB.

Example:

```
VMCLI_DB_NAME VMCLIDB
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_DB_PORT *<Derby database port number>*

Specify the Derby database port on which the Data Protection for VMware command-line interface starts and connects to the database. The default value is 1527. If this port is in use by another application, specify a different port.

Example:

```
VMCLI_DB_PORT 1527
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_GRACE_PERIOD *<seconds>*

When a backup is no longer available on Tivoli Storage Manager, the backup is marked for deletion as defined by a deletion date. However, before the backup is deleted, a grace period exists. Use this parameter to specify the grace period (length of time) between the deletion date and the date the backup is deleted from the Derby database. The default value is 2592000 seconds (30 days).

Example:

```
VMCLI_GRACE_PERIOD 1296000
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_LOG_DIR *<path of log file>*

Specify the absolute location or the relative location of the installation directory where the Data Protection for VMware command-line interface writes its log files. The default value is logs. If the default value logs is used, then all logs (and trace information) are written to these locations:

```
Linux /opt/tivoli/tsm/tdpvmware/common/logs
```

```
Windows C:\Program Files\Common Files\Tivoli\TDPVMware\logs
```

Example:

```
VMCLI_LOG_DIR logs
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_RECON_INTERVAL_TSM *<seconds>*

This parameter specifies the interval between *reconciliation* operations on the Derby database with Data Protection for VMware. Reconciliation operations delete metadata for backups that are no longer available. This action ensures the Derby database remains synchronized with the Data Protection for VMware repository. The default value is 1200 seconds.

Example:

```
VMCLI_RECON_INTERVAL_TSM 1200
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_RESTORE_TASK_EXPIRATION_TIME <seconds>

Specify the time that a Data Protection for VMware command-line interface restore task is stored in the Derby database. The default value is 2592000 seconds (30 days).

Example:

```
VMCLI_RESTORE_TASK_EXPIRATION_TIME 2592000
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_SCHEDULER_INTERVAL <seconds>

Specify the interval, in seconds, between scheduler checks for scheduled tasks due to begin. The default value is 1 second.

Example:

```
VMCLI_SCHEDULER_INTERVAL 60
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_TASK_EXPIRATION_TIME <seconds>

This parameter specifies the time that a task is stored in the Data Protection for VMware command-line interface Derby database. This parameter applies only to the **inquire_config** command. The default value is 864000 seconds (10 days).

Example:

```
VMCLI_TASK_EXPIRATION_TIME 864000
```

This parameter is valid in a vSphere or vCloud Director environment.

VMCLI_TRACE YES|NO

Specify that tracing files are activated. Activate tracing only when instructed to do so by IBM Software Support.

This parameter is valid in a vSphere or vCloud Director environment.

Example Linux profile in a vSphere environment

Linux

```
VE_TSM_SERVER_NAME      9.11.90.28
VE_TSM_SERVER_PORT      1500
VE_TSMCLI_NODE_NAME     my_vc1_vcli1
VE_VCENTER_NODE_NAME    my_vc1
VE_DATACENTER_NAME      Clovis Lab::MY_VC1_DC1
VMCLI_TASK_EXPIRATION_TIME 864000 # in seconds, defaults to 864000s = 10 days
VMCLI_RESTORE_TASK_EXPIRATION_TIME 2592000 # in seconds, defaults to 2592000s = 30 days
VMCLI_GRACE_PERIOD      2592000 # in seconds, defaults to 2592000s = 30 days
VMCLI_SCHEDULER_INTERVAL 60 # in seconds, defaults to 1s
VMCLI_DB_HOST            localhost
VMCLI_DB_PORT            1527
VMCLI_CACHE_EXPIRATION_TIME 600 # in seconds, defaults to 600s = 10 min
VMCLI_DB_NAME            VMCLIDB
VMCLI_RECON_INTERVAL_FCM 600 # setting in seconds default 600s = 10 min
VMCLI_RECON_INTERVAL_TSM 1200 # setting in seconds default 1200s = 20 min
VMCLI_DB_BACKUP          AT 00:00
VMCLI_DB_BACKUP_VERSIONS 3
VMCLI_LOG_DIR            logs
DERBY_HOME               /home/tdpvmware/tdpvmware
```

Example Windows profile in a vSphere environment

Windows

```
VE_TSM_SERVER_NAME      philadelphia      # -s
VE_TSM_SERVER_PORT      1500          # -p
VE_TSMCLI_NODE_NAME     CLI_WIN8x32      # -n
VE_VCENTER_NODE_NAME    VC_WIN8x32      # -v
VE_DATACENTER_NAME      DC_CVT::DC_Win8x32
VMCLI_TASK_EXPIRATION_TIME 864000 # in seconds, defaults to 864000s = 10 days
VMCLI_RESTORE_TASK_EXPIRATION_TIME 2592000 # in seconds, defaults to 2592000s = 30 days
VMCLI_GRACE_PERIOD      2592000 # in seconds, defaults to 2592000s = 30 days
VMCLI_SCHEDULER_INTERVAL 60 # in seconds, defaults to 1s
VMCLI_DB_HOST           localhost
VMCLI_DB_PORT           1527
VMCLI_CACHE_EXPIRATION_TIME 600 # in seconds, defaults to 600s = 10 min
VMCLI_DB_NAME           VMCLIDB
VMCLI_RECON_INTERVAL_FCM 600 # setting in seconds default 600s = 10 min
VMCLI_RECON_INTERVAL_TSM 1200 # setting in seconds default 1200s = 20 min
VMCLI_DB_BACKUP         AT 00:00
VMCLI_DB_BACKUP_VERSIONS 3
VMCLI_LOG_DIR           logs
DERBY_HOME              C:\Program Files\Common Files\Tivoli\TDPVMware\VMwarePlugin\derby
```

Example Linux profile in a vCloud environment

Linux

```
VE_TSM_SERVER_NAME      fvtseries1lesx6
VE_TSM_SERVER_PORT      1500
VE_TSMCLI_NODE_NAME     VMCLI_LNX_TEST2
VE_VCENTER_NODE_NAME    VCD_LNX_TEST2
VMCLI_TRACE             NO
#VE_TSM_SERVER_NAME     tsmservername      # -s
#VE_TSM_SERVER_PORT     1500          # -p
#VE_TSMCLI_NODE_NAME    tsmclinodename     # -n
#VE_VCENTER_NODE_NAME   vcenternodename     # -v
#VE_TRACE_FILE          tsmcli.trace      # -x tsmcli trace file
#VE_TRACE_FLAGS         api api_detail    # -y trace flags
#VE_DATACENTER_NAME     datacentername::datacenternodename
VMCLI_TASK_EXPIRATION_TIME 864000 # in seconds, defaults to 864000s = 10 days
VMCLI_RESTORE_TASK_EXPIRATION_TIME 2592000 # in seconds, defaults to 2592000s = 30 days
VMCLI_GRACE_PERIOD      2592000 # in seconds, defaults to 2592000s = 30 days
VMCLI_SCHEDULER_INTERVAL 60 # in seconds, defaults to 1s
VMCLI_DB_HOST           localhost
VMCLI_DB_PORT           1527
VMCLI_CACHE_EXPIRATION_TIME 600 # in seconds, defaults to 600s = 10 min
VMCLI_DB_NAME           VMCLIDB
VMCLI_RECON_INTERVAL_FCM 600 # in seconds default 600s = 10 min
VMCLI_RECON_INTERVAL_TSM 1200 # in seconds default 1200s = 20 min
VMCLI_DB_BACKUP         AT 00:00
VMCLI_DB_BACKUP_VERSIONS 3
```

Example Windows profile in a vCloud environment

Windows

```
VE_TSM_SERVER_NAME harding
VE_TSM_SERVER_PORT 1500
VE_TSMCLI_NODE_NAME VMCLI_WINSTR
VE_VCENTER_NODE_NAME VCD_WINSTR
VMCLI_TRACE NO
#VE_TSM_SERVER_NAME tsmservername # -s
#VE_TSM_SERVER_PORT 1500 # -p
#VE_TSMCLI_NODE_NAME tsmclinodename # -n
#VE_VCENTER_NODE_NAME vcenternodename # -v
#VE_TRACE_FILE tsmcli.trace # -x tsmcli trace file
#VE_TRACE_FLAGS api api_detail # -y trace flags
#VE_DATACENTER_NAME datacentername::datacenternodename
VMCLI_TASK_EXPIRATION_TIME 864000 # in seconds, defaults to 864000s = 10 days
VMCLI_RESTORE_TASK_EXPIRATION_TIME 2592000 # in seconds, defaults to 2592000s = 30 days
VMCLI_GRACE_PERIOD 2592000 # in seconds, defaults to 2592000s = 30 days
VMCLI_SCHEDULER_INTERVAL 60 # in seconds, defaults to 1s
VMCLI_DB_HOST localhost
VMCLI_DB_PORT 1527
VMCLI_CACHE_EXPIRATION_TIME 600 # in seconds, defaults to 600s = 10 min
VMCLI_DB_NAME VMCLIDB
VMCLI_RECON_INTERVAL_FCM 600 # in seconds default 600s = 10 min
VMCLI_RECON_INTERVAL_TSM 1200 # in seconds default 1200s = 20 min
VMCLI_DB_BACKUP AT 00:00
VMCLI_DB_BACKUP_VERSIONS 3
VMCLI_LOG_DIR logs
DERBY_HOME C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\derby
VE_TSM_MODE VCLLOUD
VE_DATACENTER_NAME Local DC::WINMA_LOCAL_DC
```

Chapter 5. Recovery Agent command-line interface

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

You can use the Recovery Agent CLI to manage only one system running the Data Protection for VMware Recovery Agent.

Starting the Recovery Agent command-line interface

Before you can start and use the Recovery Agent CLI from a supported Linux operating system, you must configure Cygwin for use when restoring files from a Linux machine.

To start the Recovery Agent CLI, complete the following steps:

1. From the Windows Start menu, click **Programs > Tivoli Storage Manager > Data Protection for VMware > Data Protection for VMware Recovery Agent**.
2. In the command prompt window, enter one of the following commands:

- To run the Recovery Agent CLI:

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

-  To display the help for the Recovery Agent CLI:

```
TDPVMwareShell.exe -h
```

-  To display the help for the Recovery Agent CLI:

```
TDPVMwareShell.exe -h dump
```

-  For example, this command displays detailed help for the mount Recovery Agent CLI:

```
TDPVMwareShell.exe -h mount dump
```

The Recovery Agent CLI on Linux requires a proxy node for the Windows system where the Data Protection for VMware Recovery Agent is running. All Recovery Agent CLI commands should be issued from this Windows system.

Recovery Agent command-line interface overview

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

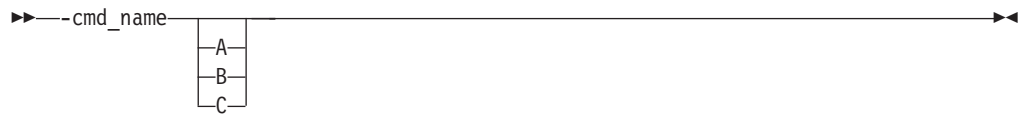
The diagram shows a command line starting with a double arrow pointing to the text `-cmd_name`. A vertical bracket to the right of `-cmd_name` groups three lines of text: `A`, `B`, and `C`. A horizontal line extends from the end of the bracketed group to the right, ending in a double arrow.

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

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.



Mount command

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

The Recovery Agent CLI 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\SnowbirdK\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>
```

You can also specify the `as_node` and `from_node` options. If the password field is empty, the Data Protection for VMware Recovery Agent attempts to use the password for the stored node.

- **-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. The specified value is case-sensitive.
- **-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 it to specify the date of the snapshot that you want to mount. The date format is yyyy-Mmm-dd hh:mm:ss. For example:
 -date "2013-Apr-12 22:42:52 AM"

To view the active (or latest) snapshot, specify `last snapshot`.

- **-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 "2013-Jan-21 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 target created using the **mount** command. Use the *everything* variable 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 target, 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 VMs.

```
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. A connection cannot be removed when it is in use, such as when mounted volumes exist. 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:

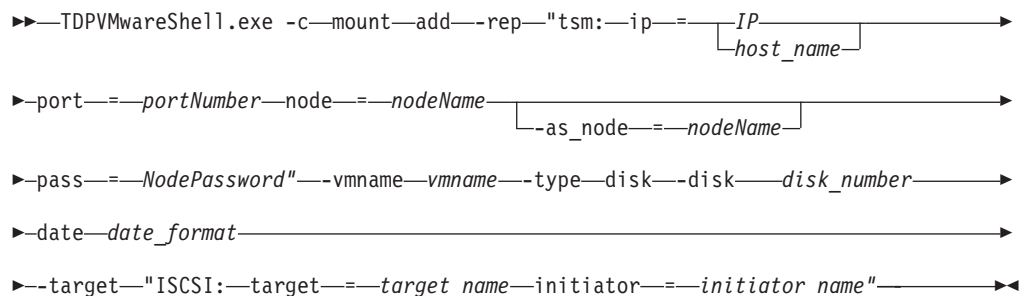
```
mount remove -rep "tsm: NodeName@ip"
```

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
```

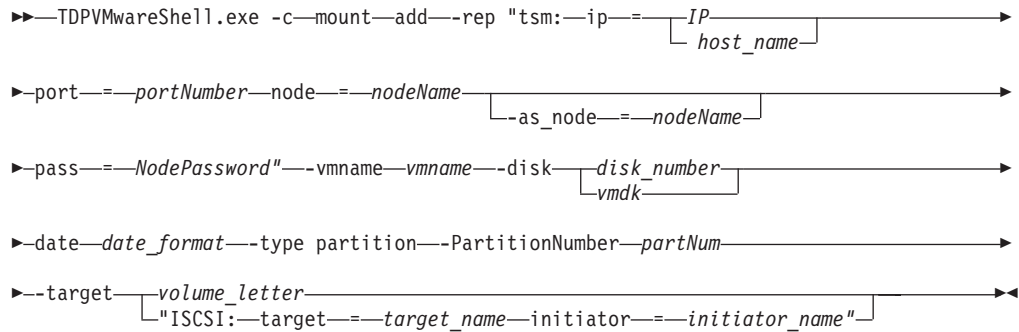
Mounting a disk

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



Mounting a partition

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



Set_connection command

The **set_connection** command sets the Recovery Agent CLI to work with a specified Data Protection for VMware Recovery Agent.

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 Recovery Agent CLI is set to work with Data Protection for VMware Recovery Agent on the *ComputerName* host.

```
set_connection mount_computer ComputerName
```

Help command

The **help** command displays the help for all of the supported Recovery Agent CLI commands.

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

```
TDPVMwareShell.exe -h
```

Recovery Agent command-line interface return codes

Return codes help identify the results of Recovery Agent CLI operations.

Use these return codes to check the status of your Recovery Agent CLI operations.

Table 8. Recovery Agent CLI return codes

Return Code	Value	Description
0	FBC_MSG_MOUNT_SUCCESS	Command submitted successfully to Data Protection for VMware mount.
0	FBC_MSG_DISMOUNT_SUCCESS	Successfully dismounted a snapshot.
0	FBC_MSG_VIEW_SUCCESS	View operation successful.
0	FBC_MSG_DUMP_SUCCESS	Dump operation successful.

Table 8. Recovery Agent CLI return codes (continued)

Return Code	Value	Description
0	FBC_MSG_REMOVE_SUCCESS	Remove operation successful.
1	FBC_MSG_MOUNT_FAIL	Mount failed (See the mount logs for details).
2	FBC_MSG_MOUNT_DRIVER_ERROR	Mount driver error.
3	FBC_MSG_VOLUME_LETTER_BUSY	Volume letter or reparse point is in use.
4	FBC_MSG_MOUNT_WRONG_PARAMETERS	Incorrect parameters assigned to the mount command (See the mount logs for details).
5	FBC_MSG_MOUNT_ALREADY_MOUNTED	Job is already mounted on the requested target.
6	FBC_MSG_MOUNT_WRONG_PERMISSIONS	Insufficient permissions.
7	FBC_MSG_MOUNT_NETWORK_DRIVE	Cannot mount on network mapped volume.
8	FBC_MSG_MOUNT_LOCKED_BY_SERVER	Snapshot locked by the server.
9	FBC_MSG_CAN_NOT_CHANGE_REPOSITORY	Cannot change repository.
11	FBC_MSG_DISMOUNT_FAIL	Failed to dismount a mounted snapshot.
13	FBC_MSG_VIEW_FAIL	Retrieving list of virtual volumes failed.
15	FBC_MSG_DUMP_FAIL	Dump command list creation failed.
16	FBC_MSG_CONNECTION_FAILED	Disconnected from Data Protection for VMware mount.
17	FBC_MSG_CONNECTION_TIMEOUT	Operation timed out.
18	FBC_MSG_MOUNT_FAILED_TO_FIND_REPOSITORY	Failed to find a valid repository with snapshots.
19	FBC_MSG_MOUNT_JOB_NOT_FOUND	Failed to find the requested snapshot.
20	FBC_MSG_MOUNT_JOB_FOLDER_NOT_FOUND	Failed to find the requested snapshot data.
22	FBC_MSG_CAN_NOT_REMOVE_REPOSITORY	Cannot remove selected repository.
23	FBC_MSG_REPOSITORY_GOT_MOUNTS	Repository has mounted snapshots.
38	FBC_MSG_MOUNT_NOT_WRITABLE_VOLUME	The mount volume is not writable
39	FBC_MSG_NO_TSM_REPOSITORY	No Tivoli Storage Manager repository was located.
40	FBC_MSG_MOUNT_NOT_ALLOWED_AS_READONLY	Mounting the iSCSI target as read only is not allowed.
41	FBC_MSG_RESOURCE_BUSY_IN_TAPE_MODE	Data Protection for VMware is running in tape mode - media is busy.

Table 8. Recovery Agent CLI return codes (continued)

Return Code	Value	Description
42	FBC_MSG_DISK_TYPE_NOT_SUPPORTED	Partition operation not supported for this type of disk.
43	FBC_MSG_MOUNT_INITIALIZING	The operation failed, Data Protection for VMware mount is currently initializing. Try again later.
44	FBC_MSG_CANNOT_LOCK_SNAPSHOT	The snapshot cannot be protected against expiration during this operation. Refer to documentation for more details.

Chapter 6. Backup scenarios

Data Protection for VMware backup scenarios are provided in this section.

vCloud environment backup scenarios

These scenarios demonstrate how to back up vApps and organization vDC with the **vmcli -f backup** command.

These vCloud Director objects can also be backed up with the following user interfaces:

Data Protection for VMware vCloud GUI

Information about how to complete backup tasks with the Data Protection for VMware vCloud GUI is provided in the online help that is installed with the GUI. Click **Learn More** in any of the GUI windows to open the online help for task assistance.

Tivoli Storage Manager backup-archive client command-line interface

Information about how to complete backup tasks with the **dsmc Backup VAPP** command is provided in the command-line help that is installed with the product (**dsmc help backup vapp**). Information is also available in the following publications:

- *Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and User's Guide*
- *Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide*

Backup of vApps from a single organization and organization vDC

This scenario creates an incremental forever full backup of all vApps from organization NewYork and organization vDC NY_bronze.

To identify that the backup environment is within vCloud Director, the following **vmcli -f set_option** command is issued:

```
vmcli -f set_option -c vcloud
```

Then, the following **vmcli -f backup** command is issued:

```
vmcli -f backup -t TSM_IFFULL -I vapplistfile
```

The `vapplistfile` contains this statement:

```
vappname:org=NewYork,orgvdc=NY_Bronze
```

Backup of vApps from multiple organizations and organization vDCs

This scenario creates an incremental forever incremental backup of vApp1 and vApp2 from organization Mainz_org and organization vDC MZ_Silver. It also backs up vApp17 from organization Oslo_org and organization vDC OL_silvervDC.

To identify that the backup environment is within vCloud Director, the following **vmcli -f set_option** command is issued:

```
vmcli -f set_option -c vcloud
```

Then, the following **vmcli -f backup** command is issued:

```
vmcli -f backup -t TSM_IFINCR -I vapplistfile
```

The vapplistfile contains this statement:

```
vappname:org=Mainz_org,orgvdc=MZ_Silver,vapp=vApp1  
vappname:org=Mainz_org,orgvdc=MZ_Silver,vapp=vApp2  
vappname:org=Oslo_org,orgvdc=OL_silvervDC,vapp=vApp17
```

This vapplistfile statement can also be specified as follows:

```
vappname:org=Mainz_org,orgvdc=MZ_Silver,vapp=vApp1,vApp2
```

vSphere environment backup scenario

This scenario demonstrates how to back up VMs with the **vmcli -f backup** command.

The VMs can also be backed up with the following user interfaces:

Data Protection for VMware vSphere GUI

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

Tivoli Storage Manager backup-archive client GUI

Information about how to complete backup tasks with the backup-archive client GUI is provided in the online help that is installed with the GUI. Click **Help** in any of the GUI windows to open the online help for task assistance.

Tivoli Storage Manager backup-archive client command-line interface

Information about how to complete backup tasks with the **dsmc Backup VAPP** command is provided in the command-line help that is installed with the product (**dsmc help backup vapp**). Information is also available in the following publications:

- *Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and User's Guide*
- *Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide*

This scenario creates an incremental forever full backup of the following VMs: vm1, vm2, vm3, vm4, and vm5:

```
vmcli -f backup -t TSM_IFFULL -I vmlistfile
```

The vapplistfile contains this statement:

```
vmname:vm1  
vmname:vm2  
vmname:vm3  
vmname:vm4  
vmname:vm5
```

Incremental forever backup scenario

An example of how to define a daily incremental forever incremental backup of the VMs.

Scheduling daily incremental forever backups ensures that there are frequent backups of the VMs and reduces the size of each backup.

1. From the VMware guests, update the Tivoli Storage Manager client backup-archive client options file:

- **Windows** Specify these options in the `dsm.opt` options file.
- **Linux** Specify these options in the `dsm.sys` file, in the stanza for the Tivoli Storage Manager data mover node.

- a. Enable compression by adding the following option: `compression yes`.

Tip: You can only enable compression if you are using client deduplication and if deduplication has been enabled for the storage pool.

- b. Enable deduplication by adding the following option: `deduplication yes`.

- c. Modify the trigger values for megablock refreshes by adding one of the following options:

`mbobjrefreshthresh`

or

`mbpctrefreshthresh`

Ensure that you specify the appropriate values for your environment.

2. Define an incremental forever incremental backup for each of the VMware guests.

The blocks that changed since the previous backup (full or incremental) are now backed up. The most recent incremental is appended to the previous backup. If a full backup does not exist for the VMs, a full backup is performed. Incremental forever incremental backups are run according to schedule repetition.

Related concepts:

“Fine-tuning Tivoli Storage Manager server database scalability”

Fine-tuning Tivoli Storage Manager server database scalability

Use options to adjust scalability within Tivoli Storage Manager for incremental forever backups.

When Tivoli Storage Manager backs up a disk (vmdk), the entire disk is treated as one logical entity. When it is stored on the server, it is partitioned into chunks represented as *megablocks*. These megablocks contain 128 MB of data. When a change occurs on a disk in an area that is represented by a megablock, a Tivoli Storage Manager object is created. This object represents the data for that megablock. For every subsequent incremental backup, if a change is detected, an additional Tivoli Storage Manager object is created on the server. This additional object tracks the changes that point to the original megablock. When a large amount of Tivoli Storage Manager objects exists for the same VM data, excessive demands are placed on the Tivoli Storage Manager server database.

To assist with fine-tuning these Tivoli Storage Manager server scalability conditions, use the `mbobjrefreshthresh` or the `mbpctrefreshthresh` options. These options are set in the Tivoli Storage Manager client backup-archive client `dsm.opt`

file (Windows) or in the appropriate server stanza in the `dsm.sys` file (Linux). However, use only one of these options. Do not use both of these options at the same time.

Occasionally, a megablock is refreshed (backed up) from the production disk. This event causes all the objects that are used in previous backups to eventually be expired. Megablocks are refreshed during incremental backups when these conditions exist:

- The number of Tivoli Storage Manager objects (or megablocks) increase beyond the value specified by the `mbobjrefreshthresh` option.

This `mbobjrefreshthresh` value is a number that defines a threshold. Use this option when estimating Tivoli Storage Manager objects that represent production data for each VM backup. For example, when the number of Tivoli Storage Manager objects exceed this value, the megablock is refreshed. This action means that the entire 128-MB block is copied to the Tivoli Storage Manager server and is represented as a single Tivoli Storage Manager object.

The minimum value is 2 and the maximum value is 8192. The default value is 50.

- The size of the incremental backup of megablock is larger than the value specified by the `mbpctrefreshthresh` option.

The `mbpctrefreshthresh` value is a number (expressed as a percentage) that defines a threshold. That threshold is how much of the current megablock can change before a full refresh is initiated. Use this option when estimating the amount of additional data that is backed up for each VM. For example, when a 128-MB block of a production disk changes more than the percentage specified, the entire 128-MB block is copied to the Tivoli Storage Manager server. The block is represented as a single Tivoli Storage Manager object.

The minimum value is 1 and the maximum value is 99. The default value is 50.

The following table describes how to adjust the `mbobjrefreshthresh` option based on various influences:

Table 9. Issues that influence scalability triggers

Refresh if...	Trigger value is...	# of megablock refreshes becomes...	Extra data	Backup window	# of TSM objects
...number of TSM objects, that represent a megablock	increased	less	less	smaller	more
	decreased	more	more	larger	less

The following table describes how to adjust the `mbpctrefreshthresh` options based on various influences:

Table 10. Issues that influence scalability triggers

Refresh if...	Trigger value is...	# of megablock refreshes becomes...	Extra data	Backup window	# of TSM objects
...size of incremental backup of megablock	increased	less	less	smaller	more
	decreased	more	more	larger	less

Scalability use case scenarios

The scenarios described in this section are based on the following dsmc query vm vmquest1 -ina -detail command-line output:

#	Backup Date	Mgmt Class	Size	Type	A/I	Virtual Machine
1	04/17/2013 02:26:25	MGMT_CLASS	244.14 MB	FULL	I	vmquest1
The size of this incremental backup: n/a						
The number of incremental backups since last full: n/a						
The amount of extra data: n/a						
The TSM objects fragmentation: n/a						
Backup is represented by: n/a						
Application protection type: VMware						
2	04/17/2013 02:27:11	MGMT_CLASS	244.14 MB	INCR	I	vmquest1
The size of this incremental backup: n/a						
The number of incremental backups since last full: n/a						
The amount of extra data: n/a						
The TSM objects fragmentation: n/a						
Backup is represented by: n/a						
Application protection type: VMware						
3	04/17/2013 02:27:52	MGMT_CLASS	244.14 MB	IFFULL	I	vmquest1
The size of this incremental backup: n/a						
The number of incremental backups since last full: 1						
The amount of extra data: 0						
The TSM objects fragmentation: 0						
Backup is represented by: 2212154 TSM objects						
Application protection type: VMware						
4	04/17/2013 02:27:59	MGMT_CLASS	244.14 MB	IFINCR	A	vmquest1
The size of this incremental backup: 0 KB						
The number of incremental backups since last full: 2						
The amount of extra data: 30						
The TSM objects fragmentation: 45						
Backup is represented by: 2212421 TSM objects						
Application protection type: VMware						

All averages are calculated only for backups displayed above.

The average size of incremental backup: 0 KB

The average number of incremental backups since last full: 2

The average overhead of extra data: 30

The average TSM objects fragmentation: 45

The average number of TSM objects per backup: 0 TSM objects

Note: When the dsmc query vm vmquest1 -ina -detail command is issued for periodic full backups, the values related to incremental forever backup statistics display as n/a.

Scenario 1:

When all machines associated with a datacenter node show The average overhead of extra data value as higher than 50, you can increase the mbpctrefreshthresh value. An increased value reduces the amount of extra data that is transferred to the Tivoli Storage Manager server. This adjustment also reduces the size of the backup window. However, be sure to verify The average TSM objects fragmentation value as it might increase.

Scenario 2:

When all machines associated with a datacenter node show The average TSM objects fragmentation value as higher than 50, you can decrease the mbobjrefreshthresh value. A decreased value reduces the number of Tivoli Storage Manager objects for each backup. This adjustment also reduces the load on the Tivoli Storage Manager server database. However, be sure to verify The average

overhead of extra data value as it might increase.

Periodic full backup scenario

This scenario provides an example of how to define a weekly full VM backup and daily full VM incremental backups of the VMs.

This task describes how to schedule 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. Define a full VM backup for each of the VMware guests.
2. 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.
3. Schedule the full VM backup that runs once a week.
4. Configure daily backups.
5. Schedule the incremental backups to run daily.
6. Specify compression and deduplication to reduce the backup size of the VMware backups. From the VMware guests, update the Tivoli Storage Manager client backup-archive client options file:
 - **Windows** Specify these options in the `dsm.opt` options file.
 - **Linux** Specify these options in the `dsm.sys` file, in the stanza for the Tivoli Storage Manager data mover node.
 - a. Enable compression by adding the following option:
compression yes.
 - Tip:** You can only enable compression if you are using client deduplication and if deduplication has been enabled for the storage pool.
 - b. Enable deduplication by adding the following option:
deduplication yes.

Include scenarios

Set include options to specify the VMs or vApps that you want to include for backup services.

The scenarios documented in this section are based on the correct use of the following Tivoli Storage Manager backup-archive client options:

- **include.vm**
- **include.vapp**

Therefore, before implementing an include strategy based on these scenarios, make sure to review these options in the *Tivoli Storage Manager Backup-Archive Client Installation and User's Guide*.

Include scenarios in a vSphere environment

When VMware virtual machine data is backed up, it is bound to a management class that is specified by the **vmmc** option. You can use the **include.vm** option to override the management class that is specified by **vmmc** and bind the backed up data for a virtual machine to a different management class.

The **include.vm** option does not override or affect the management class that is specified by the **vmctlmc** option, which binds backed up VMware control files to a specific management class.

Assume that the following management classes exist and are active on the Tivoli Storage Manager server:

- MCFORTESTVMS
- MCFORPRODVMS
- MCUNIQUEVM

The following **include.vm** statement in the client options file binds all virtual machines that have names that begin with VMTEST to the management class called MCFORTESTVMS:

```
include.vm vmtest* MCFORTESTVMS
```

The following **include.vm** statement in the client options file binds a virtual machine that is named WINDOWS VM1 [PRODUCTION] to the management class called MCFORPRODVMS:

```
include.vm "WINDOWS VM1 ?PRODUCTION?" MCFORPRODVMS
```

The virtual machine name must be enclosed in quotation marks because it contains space characters. Also, the question mark wildcard is used to match the special characters in the virtual machine name.

The following **include.vm** statement in the client options file binds a virtual machine that is named VM1 to a management class that is named MCUNIQUEVM:

```
include.vm VM1 MCUNIQUEVM
```

Include scenarios in a vCloud environment

When you back up a VMware vCloud vApp, the backed up data is bound to a management class that is specified by the **vappmc** option. You can use the **include.vapp** option to override the management class that is specified by **vappmc** and bind the backed up data for a vApp to a different management class.

Assume that the following management classes exist and are active on the Tivoli Storage Manager server:

- MCFORTESTVAPPS
- MCFORPRODVAPPS
- MCUNIQUEVAPP

The following **include.vapp** statement in the client options file binds all vApp backups to the management class called MCFORTESTVAPPS. Wildcards are used in the vApp specification to target all vApps in all organizations and all organization virtual data centers:

```
include.vapp *:::*:* vm vmtest* MCFORTESTVAPPS
```

The following **include.vapp** statement in the client options file binds all vApps in ORG1 and ORG1VDC to the management class called MCFORPRODVAPPS:

```
include.vapp "ORG1::ORGVDC1:*)" MCFORPRODVAPPS
```

The following **include.vapp** statement in the client options file binds a vApp that is named VAPP1 to a management class that is named MCUNIQUEVAPP:

```
include.vapp MY_ORG::MY_VDC::VAPP1 MCUNIQUEVAPP
```

Management class scenarios

Use management classes to determine how to manage your VM and vApp backups on the Tivoli Storage Manager server.

The scenarios documented in this section are based on the correct use of the following Tivoli Storage Manager backup-archive client options:

- **vmmc**
- **vmctlmc**
- **vappmc**

Therefore, before implementing a management class strategy based on these scenarios, make sure to review these options in the *Tivoli Storage Manager Backup-Archive Client Installation and User's Guide*.

Management class scenarios in a vSphere environment

Use the **vmmc** option to store the VMware backups with a management class other than the default management class. The **vmmc** option is only valid when `vmbackuptype=fullvm`.

Task:

- Run a backup of the virtual machine that is named `myVirtualMachine`.
- Save the backup according to the management class `myManagementClass`.

Command line:

```
dsmc backup vm "myVirtualMachine" -vmmc=myManagementClass
```

By default, VMware control files are bound to the default management class. The **vmmc** option can be used to specify a different management class to which VMware data and VMware control files are bound. The **vmctlmc** option overrides the default management class and the **vmmc** option for VMware control files.

Under certain conditions, it might be desirable or necessary to bind VMware control files to a different management class than the VMware data files.

The **vmctlmc** option is required if VMware data files are backed up to tape. VMware control files must be backed up to a disk-based storage pool that does not migrate to tape. The storage pool can be composed of random access volumes and sequential file volumes; the storage pool can also be a deduplicated pool. Use the **vmctlmc** option to specify a management class that stores data in such a storage pool.

Restriction: The management class that is specified by the **vmctlmc** option determines only the destination storage pool for VMware control files. Retention of VMware control files is determined by the **vmmc** option, if specified, or by the default management class. The retention for the VMware control files always matches the retention of the VMware data files.

Options file:

```
vmctlmc diskonlymc
```

Command line:

Does not apply.

Management class scenarios in a vCloud environment

Use the **vappmc** option to store VMware vCloud vApp backups by using a management class other than the default management class. The default management class is defined on the server, for the domain that the node belongs to.

If you set this option in the options file for a data mover node, all vApp back ups that are performed by the data mover are stored as indicated by the specified management class.

mgmtclassname

Specifies a management class that applies to VMware vApp backups. If you do not set this option, the default management class of the node is used.

Tip: The management class that you specify on this option affects the storage of vApp data; the **vmmc** option does not apply to vApp data storage processing. However, the **vmctlmc** option does specify the management class that is used to store control files for both virtual machine backups and vApp backups.

Options file:

Specify a management class to use when the server stores all vApp backups:

```
vappmc MCPRDVAAPS
```

Command line:

```
dsmc backup vapp "org1,vdc1,vapp1" -vappmc=myManagementClass
```

Controlling disk scenarios

Set include and exclude statements to control the disks to be processed.

Important: The scenarios documented in this section are based on the correct use of the following Tivoli Storage Manager backup-archive client options:

- DOMAIN.VMFULL
- EXCLUDE.VMDISK
- INCLUDE.VMDISK

You cannot select disks with the Data Protection for VMware vSphere GUI Schedule a Backup wizard. Therefore, before implementing a disk protection strategy based on these scenarios, make sure to review these options in the *Tivoli Storage Manager Backup-Archive Client Installation and User's Guide*.

Controlling disks with include and exclude statements is provided to accomplish any of the following objectives:

- Do not back up some of the VM virtual disks.
- Do not restore all of the virtual disks from a backup.
- Update an existing VM with some of the data saved from a backup. That is, restoring only a single virtual disk while leaving the other virtual disks intact.

Use this feature to exclude a virtual disk during a backup operation. When the VM is restored, the excluded disk is created on the restored VM. However, no actual disk data is restored. Only the disk definition is restored. Therefore, make sure that the disk is properly formatted before using.

This feature is not provided to reduce backup storage space by occasionally excluding a virtual disk during a backup operation. This feature is provided only for virtual disks that never require backup. For example, those virtual disks that contain data that does not need to be restored, or the data is preserved by another backup mechanism. A virtual disk excluded from the backup operation is considered as deleted from the VM for that backup. If the VM is restored from that backup, the excluded virtual disk is not restored. Only the disk definition is restored.

You can view the disk name and label of the virtual disk by issuing the preview option. For example:

```
dsmc backup vm <vmname> -preview
```

This command does not back up the VM. Rather, it shows information about how the backup operation would proceed if it was started.

The primary method for excluding a virtual disk is to set the EXCLUDE.VMDISK option in the Tivoli Storage Manager backup-archive client dsm.opt options file. For example:

EXCLUDE.VMDISK <vmname> "Hard Disk 3"

Then, issue the backup command:

```
dsmc backup vm <vmname>
```

A secondary method for excluding a virtual disk is to specify the -vmdk option in the backup-archive client command-line interface (without setting the EXCLUDE.VMDISK option). For example:

```
dsmc backup vm "<vmname>:-vmdk=Hard Disk 3"
```

For restore operations, issue the dsmc restore vm command with the -detail option. This option displays the disk name and label from a VM backup. For example:

```
dsmc query vm FinTestUpdate -detail
```

Query Virtual Machine for Full VM backup

#	Backup Date	Mgmt Class	Size	Type	A/I	Virtual Machine
1	08/14/2013 07:56:47	STANDARD	168.94 GB	FULL	A	FinTestUpdate
The size of this incremental backup: n/a						
The number of incremental backups since last full: n/a						
The amount of extra data: n/a						
The TSM objects fragmentation: n/a						
Backup is represented by: n/a						
Application protection type: VMware						
VMDK[1]Label: Hard disk 3						
VMDK[1]Name: [DEVESX02:LocalHD] FinTestUpdate/FinTestUpdate_2-000001.vmdk						
VMDK[1]Status: Skipped: User						
VMDK[2]Label: Hard disk 4						
VMDK[2]Name: [DEVESX02:LocalHD] FinTestUpdate/FinTestUpdate_3.vmdk						
VMDK[2]Status: Skipped: Independent						
VMDK[3]Label: Hard disk 5						

```

VMDK[3]Name:      [DEVESX02:LocalHD] FinTestUpdate/FinTestUpdate_4.vmdk
VMDK[3]Status:    Skipped: Independent
VMDK[4]Label:     Hard disk 1
VMDK[4]Name:      [DEVESX02:LocalHD] FinTestUpdate/FinTestUpdate.vmdk
VMDK[4]Status:    Protected
VMDK[5]Label:     Hard disk 2
VMDK[5]Name:      [DEVESX02:LocalHD] FinTestUpdate/FinTestUpdate_1.vmdk
VMDK[5]Status:    Protected

```

To restore only Hard Disk 1, issue this command:

```
dsmc restore vm "FinTestUpdate:vmdk=Hard Disk 1"
```

When you use selective disk restore, a VM can be updated with only the disks that are specified in the command. In the previous example, if the VM named FinTestUpdate exists, the restore operation restores only disk Hard Disk 1. The other disks remain intact. If the VM named FinTestUpdate does not exist, then a VM is created and only disk Hard Disk 1 is restored. The other disks are created as unformatted disks and contain no data.

Include scenarios (four disks)

In these scenarios, VM vm5_fin_com contains four disks:

```

Hard Disk 1
Hard Disk 2
Hard Disk 3
Hard Disk 4

```

Use the INCLUDE.VMDISK statement to back up disks Hard Disk 1 and Hard Disk 2:

```

INCLUDE.VMDISK vm5_fin_com "Hard Disk 1"
INCLUDE.VMDISK vm5_fin_com "Hard Disk 2"

```

Since an include disk statement is specified, this statement implies that only disks specifically included are backed up. As a result, Hard Disk 3 and Hard Disk 4 are not backed up.

Use the DOMAIN.VMFULL statement to back up disks Hard Disk 1 and Hard Disk 2:

```
DOMAIN.VMFULL "vm5_fin_com:vmdk=Hard Disk 1:vmdk=Hard Disk 2"
```

Hard Disk 3 and Hard Disk 4 are not backed up.

You can include one or more disks with a DOMAIN.VMFULL statement. You can exclude one or more disks with a DOMAIN.VMFULL statement. You can mix include and exclude disks on the same statement. For example, the following statement is valid:

```
domain.vmfull "vm5_fin_com:vmdk=Hard Disk 1:-vmdk=Hard Disk 2:vmdk=Hard Disk 3:vmdk=Hard Disk 4"
```

If an include statement is present, it causes all other disks in the VM to be excluded from a backup operation, unless the other disks are also specified with an include statement. For example, the following statement excludes all hard disks except for Hard Disk 1:

```
domain.vmfull "vm5_fin_com:vmdk=Hard Disk 1"
```

Include scenarios (10 disks)

In these scenarios, VM `vm5_fin_com` contains 10 disks:

Hard Disk 1
Hard Disk 2
Hard Disk 3
Hard Disk 4
Hard Disk 5
Hard Disk 6
Hard Disk 7
Hard Disk 8
Hard Disk 9
Hard Disk 10

When multiple disks exist, include statements can be simpler to use than exclude statements.

Use the `INCLUDE.VMDISK` statement to back up disks Hard Disk 1 and Hard Disk 2:

```
INCLUDE.VMDISK vm5_fin_com "Hard Disk 1"  
INCLUDE.VMDISK vm5_fin_com "Hard Disk 2"
```

The remaining eight hard disks are not backed up.

Use the `DOMAIN.VMFULL` statement to back up disks Hard Disk 1 and Hard Disk 2:

```
DOMAIN.VMFULL "vm5_fin_com:vmdk=Hard Disk 1:vmdk=Hard Disk 2"
```

The remaining eight hard disks are not backed up.

Exclude scenarios (four disks)

In these scenarios, the VM named `vm5_fin_com` contains four disks:

Hard Disk 1
Hard Disk 2
Hard Disk 3
Hard Disk 4

Use the `EXCLUDE.VMDISK` statement to back up disks Hard Disk 1 and Hard Disk 2:

```
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 3"  
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 4"
```

Hard Disk 3 and Hard Disk 4 are not backed up.

Use the `DOMAIN.VMFULL` statement to back up disks Hard Disk 3 and Hard Disk 4:

```
DOMAIN.VMFULL "vm5_fin_com:vmdk=Hard Disk 3:vmdk=Hard Disk 4"
```

Hard Disk 1 and Hard Disk 2 are not backed up.

Exclude scenarios (10 disks)

In these scenarios, the VM named `vm5_fin_com` contains 10 disks:

Hard Disk 1
Hard Disk 2
Hard Disk 3
Hard Disk 4

Hard Disk 5
Hard Disk 6
Hard Disk 7
Hard Disk 8
Hard Disk 9
Hard Disk 10

When multiple disks exist, exclude statements require more information than include statements.

Use the EXCLUDE.VMDISK statement to back up disks Hard Disk 1 and Hard Disk 2, and exclude the remaining eight disks:

```
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 3"  
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 4"  
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 5"  
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 6"  
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 7"  
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 8"  
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 9"  
EXCLUDE.VMDISK vm5_fin_com "Hard Disk 10"
```

Only Hard Disk 1 and Hard Disk 2 are backed up.

Use the DOMAIN.VMFULL statement to back up disks Hard Disk 1 and Hard Disk 2 and exclude the remaining eight disks:

```
DOMAIN.VMFULL "vm5_fin_com:-vmdk=Hard Disk 3:  
-vmdk=Hard Disk 4:-vmdk=Hard Disk 5:-vmdk=Hard Disk 6:  
-vmdk=Hard Disk 7:-vmdk=Hard Disk 8:-vmdk=Hard Disk 9:  
-vmdk=Hard Disk 10"
```

Only Hard Disk 1 and Hard Disk 2 are backed up.

Controlling disks used by Tivoli Storage Manager Data Protection applications

These recommendations provide guidance when you use Data Protection for VMware and Tivoli Storage Manager Data Protection applications to protect your data.

Data Protection for Microsoft Exchange Server is a separately licensed product.

Tivoli Storage Manager provides applications that protect specific database and mail server data. In these environments, the data protection application servers typically run inside a VM. As a result, the Tivoli Storage Manager Data Protection product also runs inside the VM. However, in order to use Data Protection for VMware effectively with the Tivoli Storage Manager data protection applications, you must coordinate the backup and restore capability of each application. This coordination is best accomplished by separating disk usage.

Backup and restore scenario

In this scenario, Data Protection for Microsoft Exchange Server is installed on Disk1 and uses this disk (.vmdk) configuration:

- Disk1: Operating system files
- Disk2: Microsoft Exchange database files
- Disk3: Microsoft Exchange log files
- Disk4: Contains files other than Microsoft Exchange files

1. Use Data Protection for Microsoft Exchange Server to back up Disk2 and Disk3:
`tdpexcc backup * full /backupmethod=vss /backupdestination=tsm`
2. Use Data Protection for VMware to back up Disk1 and Disk4:
`dsmc backup vm "VM2-08R2EX10-1_orig:vmrk=Hard Disk 1:vmrk=Hard Disk 4"`
3. Use Data Protection for VMware to restore the VM named VM2-08R2EX10-1 to a new VM:
`dsmc restore vm VM2-08R2EX10-1_orig -vmname=user_story_Exch
 -datacenter=VC4-VE-2_DATACENTER1 -host=ESX41-VE-2.QA1.COM
 -DATASTORE=ESX41-VE-3`

The following command output is displayed:

```
Restore processing finished.
Session established with server VM-03R2-TSM62-5: Windows
  Server Version 7, Release 1, Level 0.0
  Server date/time: 04/26/2013 12:32:54  Last access: 04/26/2013 11:13:13

Total number of objects restored:          2
Total number of objects failed:           0
Total number of bytes transferred:        42.00 GB
Data transfer time:                       4,708.17 sec
Network data transfer rate:               9,353.97 KB/sec
Aggregate data transfer rate:             9,210.25 KB/sec
Elapsed processing time:                   01:19:41
```

4. Start the vSphere Client and go to **Summary > Edit Settings** to verify that the restored VM contains the same configuration as the source VM. For example, in this scenario, the configuration of the restored VM shows four disks like the original VM. However, only the data for Disk1 and Disk4 are restored. Disk2 and Disk3 must first be formatted for use. Then use Data Protection for Microsoft Exchange to restore Disk2 and Disk3.
5. Start the restored VM:
 - a. Go to **Server Manager > Disk Management**.
 - b. Select Disk2 and Disk3 to complete disk initialization requirements.
 - c. Select partition style MBR and click **OK**.
 - d. Both disks are formatted with the same drive letters as the original VM.
 - e. Use Data Protection for Microsoft Exchange to restore the Exchange data files to Disk2 and Disk3.

Cluster and data store backup scenarios

Backup VMs according to cluster or data store.

Data Protection for VMware domain support includes backing up VMs according to the following criteria:

- Host clusters
- Data Store
- Wildcard character
- ESX or ESXi host
- All VMs within a vCenter
- VMs in folder containers
- VMs defined in a list

These criteria are implemented with the Tivoli Storage Manager backup-archive client `domain.vmfll` option with the following parameters:

vmhostcluster=*hostclustername,hostclustername,...*,

This parameter backs up all VMs that are defined to the vCenter server that is specified by the *vmhost* option. The VMs must also be running on the ESX host cluster that is specified by *hostclustername*. This parameter not available when connecting directly to the ESXi/ESX host.

vmdatastore=*datastorename,datastorename,...*,

This parameter backs up all VMs that are defined to the vCenter or to the ESX server as specified by the *vmhost* option. The VMs must also have their configured default data store location (location of VM configuration files (.vmx)) match the data store name that is specified by *datastorename*.

-vm=*vmname,**,

The *vmname* specifies that the next set of values are VM host names to exclude from the domain. Specifying a wildcard character (*) assists with identifying VMs by their naming convention.

Cluster scenario

In this cluster scenario, the VMware environment consists of more than 3,000 VMs. Host clusters are used to manage the hardware resources. Although most of these clusters contain from 3 to 4 ESXi hosts each, some clusters contain as many as 10 ESXi hosts. However, some ESXi hosts are running from 1 to 3 VMs for larger, mission critical VMs. In order to manage the load, additional VMware hosts are frequently added or removed as needed. Each ESXi host in the cluster manages 10 - 30 VMs. Since the total number of VMs in each cluster ranges from 100 to 200, each host cluster is backed up to a dedicated vStorage Backup Server. Each server uses a dedicated Tivoli Storage Manager data mover node to run the backup operation.

You can select host clusters to back up with the Data Protection for VMware vSphere GUI Schedule a Backup wizard. In the Data Protection for VMware vSphere GUI Getting Started window, click **Define a backup task** to open the Schedule a Backup wizard.

In order to back up all VMs in host cluster TivDev01, the backup schedule contains this statement:

```
domain.vmfull vmhostcluster=TivDev01
```

In order to back up all VMs in host clusters TivDev02 and TivDev03, and exclude VMs from the domain that contain VMTest* in their name, the backup schedule contains this statement:

```
domain.vmfull vmhostcluster=TivDev02,TivDev03;-vm=VMTest*
```

In order to back up all VMs in host clusters TivSVT01, TivSVT02, TivSVT03, and TivSVT04, the backup schedule contains this statement:

```
domain.vmfull vmhostcluster=TivSVT01,TivSVT02,TivSVT03,TivSVT04
```

These domain.vmfull vmhostcluster= statements can be repeated for each host cluster.

Host scenario

The VMware environment is similar to the environment described in the Cluster Scenario. However, this environment contains individual host clusters that contain too many VMs for a single Tivoli Storage Manager data mover node backup

window. A data mover can be assigned for each host or added to an existing data mover that is already processing a host cluster. This type of implementation can also be applied to individual VMs.

These host scenarios plan for a vStorage backup server (data mover) for each host on production systems that contain larger VMs or an increased data change rate.

You can select hosts to back up with the Data Protection for VMware vSphere GUI Schedule a Backup wizard. In the Data Protection for VMware vSphere GUI Getting Started window, click **Define a backup task** to open the Schedule a Backup wizard.

In order to back up all VMs in hosts TivProd01 and mycompany.com, the backup schedule contains this statement:

```
domain.vmfull vmhost=TivProd01,mycompany.com
```

In order to back up all VMs in hosts TivProd02.mycompany.com and TivProd03.mycompany.com, and exclude VMs from the domain that contain MailDept* in their name, the backup schedule contains this statement:

```
domain.vmfull vmhost=TivProd02.mycompany.com,TivProd03.mycompany.com;-vm=MailDept*
```

The largest and most active VMs contain MailDept at the beginning of their name. In this scenario, a separate data mover (Production06) is dedicated to these VMs. The backup schedule contains this statement:

```
domain.vmfull vm=MailDept*
```

This domain.vmfull vm= statement can be repeated for each host.

Wildcard scenario

The *vmname* specified by the VM keyword (vm) and VM exclusion keyword (-vm) supports wildcard characters. Specify an asterisk (*) to match any character. Specify a question mark (?) to match a single character. For example:

```
vm=prod1*,*testvm,*dept*,dept4?prod
```

This command (with wildcards) produces a list that includes only those VMs that match the domain.vmfull filter string with no duplicates. The order of the domain keywords does not affect the results. Exclusion statements are always processed at the end. As a result, the end statements override the inclusion statements.

In these wildcard scenarios, a separate data mover is defined to back up the VMs based on their naming convention. New VMs can be added and included the scheduled backup operation.

Note: The Data Protection for VMware vSphere GUI Schedule a Backup wizard does not support wildcard selection. As a result, you must set the domain.vmfull option in the backup-archive client dsm.opt (Windows) or dsm.sys (Linux) file for the Tivoli Storage Manager data mover node.

This example backs up production VMs that contain MailDept at the beginning of their name:

```
domain.vmfull vm=MailDept*
```

This example backs up training VMs that contain TrainingVM at the beginning of their name:

```
domain.vmfull vm=TrainingVM*
```

This example backs up all VMs that are not used in production or training:

```
domain.vmfull all-vm;-vm=MailDept*,TrainingVM*
```

Parallel backup processing

Back up multiple VMs at the same time with one Tivoli Storage Manager data mover node.

In previous versions of Data Protection for VMware, backups were processed serially: each Tivoli Storage Manager data mover node processed only one VM backup at a time. To back up VMs in parallel, multiple data mover nodes must be created.

Data Protection for VMware 7.1 provides parallel backup processing: a single Tivoli Storage Manager data mover node can back up multiple VMs at the same time. This parallel backup processing is implemented by setting the following Tivoli Storage Manager Backup-Archive 7.1 client options:

vmmaxparallel

This option controls the number of overall VMs that are allowed to be backed up at a single time. This option works in concert with `vmlimitperhost` and `vmlimitperdatastore`. The default value is 1. The maximum value is 50. The minimum value is 1.

vmlimitperhost

This option limits how many VMs are backed up from a single ESX or ESXi host at the same time. The maximum value is 50. The minimum value is 1.

vmlimitperdatastore

This option limits the maximum number of VMs that are backed up at the same time for a single data store. The maximum value is 50. The minimum value is 1. When VMs contain data that is distributed across multiple data stores, the `vmlimitperdatastore` value is applied to each of the distributed data stores. For example, when a VM contains data that is distributed between `datastore_1` and `datastore_2`, the `vmlimitperdatastore` value is applied to both data stores until that VM backup is complete.

These three parallel processing options are only valid in the `dsm.opt` file (Windows) or `dsm.sys` file stanza (Linux) that is defined for each Tivoli Storage Manager data mover node.

Parallel backup scenario

In this scenario, the Data Protection for VMware 6.3 environment contains 2 ESX hosts. Each host contains 6 VM guests that are connected to three data stores. Three scheduled backup operations run every night. Each schedule has its own instance (Tivoli Storage Manager data mover node) that is configured to process one of the three schedules. Each schedule targets VM guests that use the same data store. By using this method, parallel backups are run without causing contention among the three data stores. At any moment, 3 VMs are backed up that do not share a data store.

After installing and configuring Data Protection for VMware 7.1, the following parallel processing options are specified:

```

vmmxparallel 3
vmlimitperdatastore 1
vmlimitperhost 0

```

As a result, only one schedule is required to back up the six VM guests. Three Tivoli Storage Manager sessions start in parallel (`vmmxparallel 3`). The fourth session starts after the three previous sessions complete their backup of the three data stores.

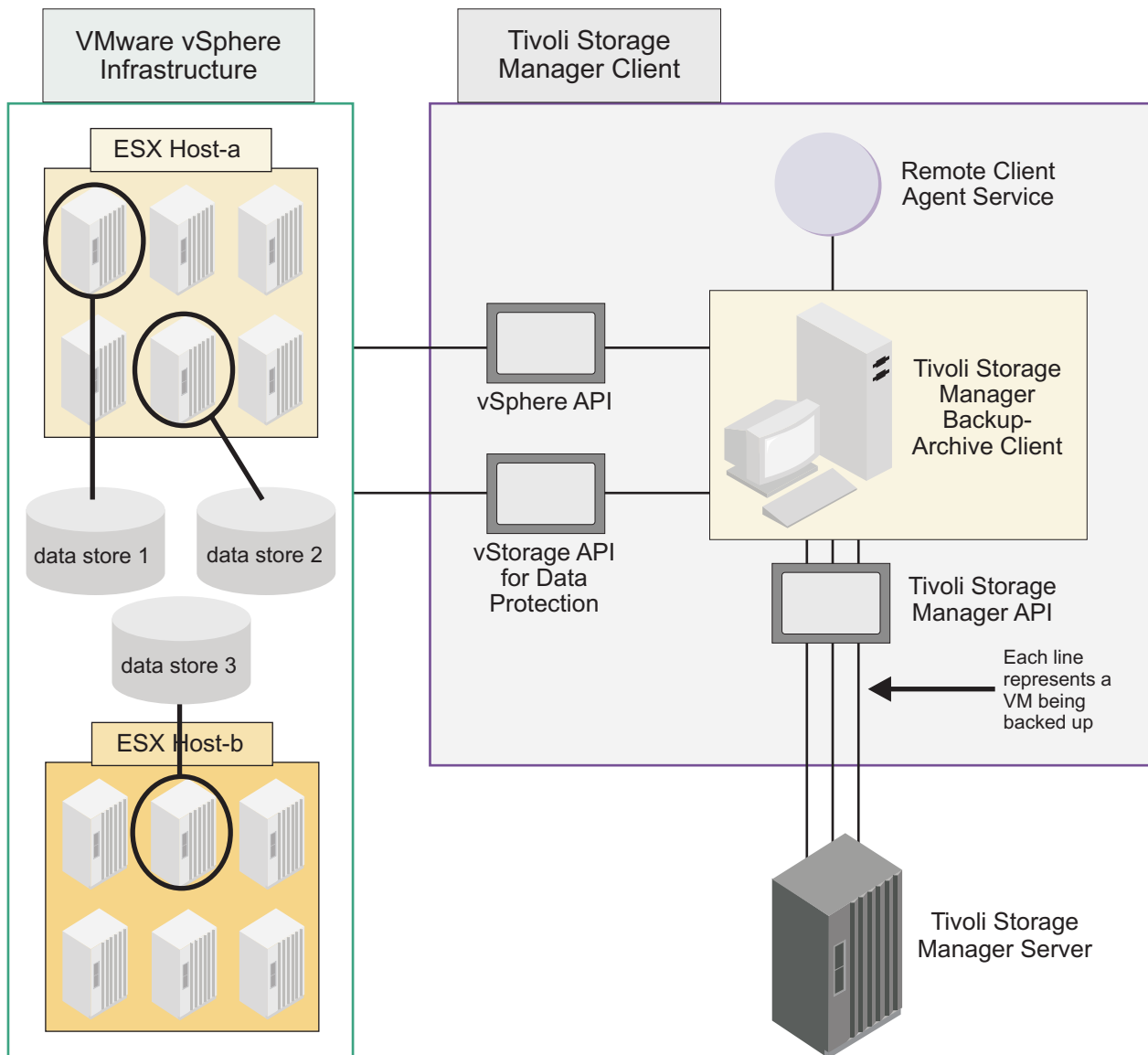


Figure 13. Three VM guests backed up by one instance

Active Directory domain controller protection scenario

The environment in this scenario consists of a data center with five domain controllers. Each domain controller is on a VMware guest. One physical domain controller is also included. The domain controllers are in two geographic locations and replicate with each other using a standard Active Directory replication process.

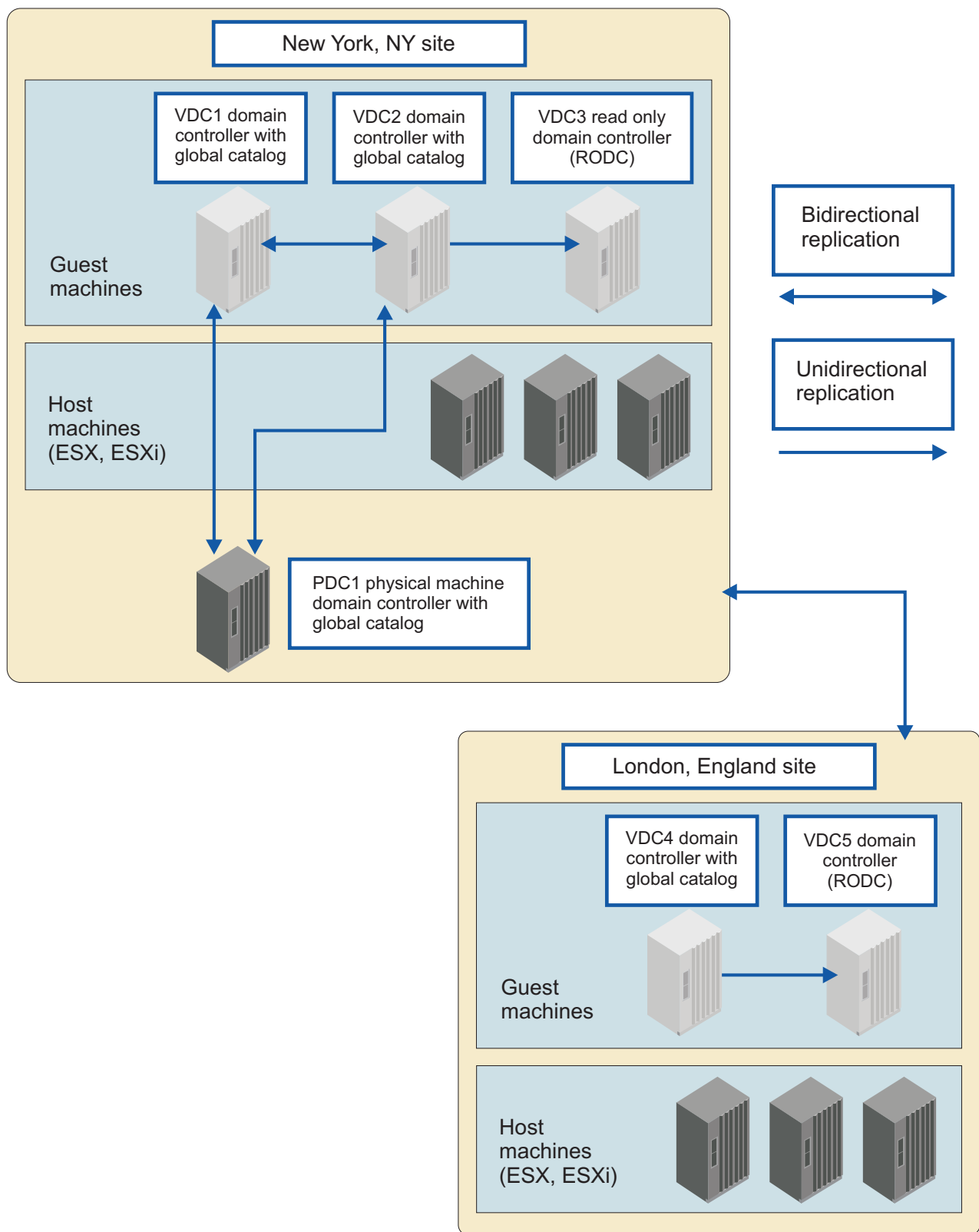


Figure 14. Data Protection for VMware protects the VMware guests that host Active Directory Domain Controllers.

Note: This scenario uses the Tivoli Storage Manager backup-archive client command-line interface to back up and restore the VM guests. The Tivoli Storage Manager backup-archive client GUI can also be used to complete these tasks.

1. VM guests VDC1 and VDC3 are backed up by issuing the following commands on the Tivoli Storage Manager backup-archive client command-line interface:

```
dsmc backup vm vdc1  
dsmc backup vm vdc3
```
2. VDC1 is recovered with non-authoritative restore by issuing the following command:

```
dsmc restore vm vdc1
```
3. After the server restarts, the restored Active Directory domain controller (on VDC1) replicates non-authoritatively with other domain controllers in the network. Make sure to manually reboot the restored VM guest.
4. Verify that the replication completed successfully.

Chapter 7. Restore scenarios

Data Protection for VMware restore scenarios are provided in this section.

vCloud environment restore scenario

This scenario demonstrates how to restore vApps with the **vmcli -f restore** command.

These vCloud Director objects can also be restored with the following user interfaces:

Data Protection for VMware vCloud GUI

Information about how to complete backup tasks with the Data Protection for VMware vCloud GUI is provided in the online help that is installed with the GUI. Click **Learn More** in any of the GUI windows to open the online help for task assistance.

Tivoli Storage Manager backup-archive client command-line interface

Information about how to complete backup tasks with the **dsmc Restore VAPP** command is provided in the command-line help that is installed with the product (**dsmc help restore vapp**). Information is also available in the following publications:

- *Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and User's Guide*
- *Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide*

This scenario restores vApp1 from organization Mainz_org and organization vDC MZ_Silver to a new vApp named vApp1_restore.

To identify that the backup environment is within vCloud Director, the following **vmcli -f set_option** command is issued:

```
vmcli -f set_option -c vcloud
```

Then, the following **vmcli -f restore** command is issued:

```
vmcli -f restore -I vapplistfile
```

The vapplistfile contains this statement:

```
backupid:47110815 vappname:org=Mainz_org,orgvdc=MZ_Silver,vapp=vApp1  
vappname_new:vApp1_restore
```

You can restore a single or multiple vApps. You cannot exclude individual VMs from a vApp restore, nor can you restore a single VM into an existing vApp.

vSphere environment restore scenario

This scenario demonstrates how to restore VMs with the **vmcli -f restore** command.

The VMs can also be restored with the following user interfaces:

Data Protection for VMware vSphere GUI

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

Tivoli Storage Manager backup-archive client GUI

Information about how to complete restore tasks with the backup-archive client GUI is provided in the online help that is installed with the GUI. Click **Help** in any of the GUI windows to open the online help for task assistance.

Tivoli Storage Manager backup-archive client command-line interface

Information about how to complete restore tasks with the **dsmc Restore VM** command is provided in the command-line help that is installed with the product (**dsmc help restore vm**). Information is also available in the following publications:

- *Tivoli Storage Manager for Windows: Backup-Archive Clients Installation and User's Guide*
- *Tivoli Storage Manager for UNIX and Linux: Backup-Archive Clients Installation and User's Guide*

This scenario completes an instant restore of vmName6 to a new VM, data center, ESX host, and data store. During the restore process, the disk is created with thin provisioning.

The following **vmcli -f restore** command is issued:

```
vmcli -f restore -vmrestoretype instantrestore -I vmlistfile
```

The vmpplistfile contains this statement:

```
backupid:678912345 vmname:vmName6::vmname:vm6newName  
newdatacentername:DataCenter2 newesxhostname:esxHost1Name  
newdatastoreurl:datastore2 vmtempdatastore:datastore2temp  
vmdiskprovision:thin
```

Full VM instant restore scenarios

Windows

A backed up VM is restored and available for immediate use.

Instant access and instant restore capability is supported only for VMware VMs that are hosted on VMware ESXi 5.1 servers, or later versions.

This command completes an instant restore of the VM with the name Cologne.

```
dsmc restore vm Cologne -vmrest=INSTANTRestore -vmtempdatastore=Verify_datastore
```

This command completes a regular restore (without starting the VM) when the VM named San_Jose is being restored.

```
dsmc restore vm San_Jose
```

Alternatively, you can also use the following command:

```
dsmc restore vm San_Jose -vmrest=noni
```

In this command, the `-vmtempdatastore` option specifies a temporary data store on the ESX host. The data for the new VM is stored in this temporary data store:

```
dsmc restore vm Haifa -VMRESToretype=INSTANTRestore -vmname=Haifa_verify  
-VMTEMPDatastore=Verify_Datastore
```

The temporary data store is used by Storage vMotion to store the configuration of the restored virtual machine during the instant restore process. The name that you specify must be unique. It cannot match the name of any of the original data stores that were used by the virtual machine when it was backed up, and it cannot be the same as the name specified on the optional `-datastore` option. If the `-datastore` option is omitted, the virtual machine files are restored to the data stores that they used when the virtual machine was backed up.

This command completes an instant restore of the VM with the name Oslo with the `-pick` option to pick a specific backup version.

```
dsmc restore vm Oslo -vmrest=INSTANTRestore -pick -vmtempdatastore=datastore_temp
```

This command queries to find all active and failed instant restore sessions.

```
dsmc query vm * -VMRESToretype=INSTANTRestore
```

This command retrieves the metadata for all instant restore session from the Tivoli Storage Manager server and prints that information as a list.

This command completes a cleanup of the VM and all its components. These components include iSCSI mounts, devices, and temporary data that are identified by the VM name on the ESX host.

```
dsmc restore vm Oslo -VMRESToretype=VMCleanup -vmname=Oslo_Verify
```

This command queries information about the real state of the listed VMs based on information from the vSphere SDK on the ESX host.

```
dsmc query vm * -VMRESToretype=INSTANTRestore -Detail
```

Full VM instant restore cleanup and repair scenarios

When an instant restore operation fails after the VM is powered on, manual cleanup and repair tasks are required.

An instant restore operation that fails with storage vMotion running creates either of the following situations:

- The instant restore operation generates an error message.
- The instant restore operation suspends indefinitely and the VM is not responsive.

To determine the cause of the problem, perform a detailed query of the VM by using the following command:

```
dsmc q vm * -vmrestoretype=instantrestore -detail
```

In the output that is produced by this command, for each VM in the output, look for the line that contains Action Needed. Use the following *Action Needed* paragraphs to recover from failed instant restore operation, depending on the Action Needed status.

Instant access and instant restore capability is supported only for VMware VMs that are hosted on VMware ESXi 5.1 servers, or later versions.

Action Needed: Cleanup

In the output of the query `vm * -vmrestoretype=instantrestore -detail` command, verify that the storage vMotion status is successful (vMotion Status: Successful) and that all VM disks are physical disks (Disk Type: Physical). This status confirms that the VM was restored and cleanup of orphaned components, such as iSCSI mounts, is needed.

This type of failure occurs as a result of either of the following situations:

- The instant restore failed and Storage vMotion is running. VMware vSphere continues the vMotion process.
- Storage vMotion finished successfully, but the automatic cleanup of the iSCSI mounts fails.

To clean up any orphaned components, run the **restore vm** command with the **-VMRESToretype=VMCleanup** parameter. For example:

```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMCleanup
```

Action Needed: Repair

In the output of the query `vm * -vmrestoretype=instantrestore -detail` command, verify that the iSCSI device that is attached to the VM is dead (status is Disk Path: Dead).

This type of failure occurs as a result of one of the following three situations:

- The VM that is used as a data mover or the physical data mover machine failed.
- A network failure occurred between the data mover and the ESX host or the data mover and the Tivoli Storage Manager server.
- The Data Protection for VMware Recovery Agent Service failed.

The iSCSI device must be returned to an active state before any other instant operation is attempted.

To attempt to recover from a data mover failure, complete the following steps:

1. Investigate that cause of the failure and restart the data mover machine if it does not start automatically. This action starts an automatic recovery of the mounted iSCSI disks.
2. In the output of the query `vm * -vmrestoretype=instantrestore -detail` command, verify that the VM disks are active (Disk Path: Active). This status means that the VM was restored and is available for use.
3. Restart storage vMotion in the vSphere client and monitor its progress in the vSphere client status bar.
4. If storage vMotion processing completed successfully, run the **restore vm** command with the **-vmrestoretype=VMCleanup** parameter to clean up the iSCSI disks. For example:

```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMCleanup
```

To attempt recovery after a network failure, complete the following steps:

1. Repair the network issue so that communication between the data mover and the ESX host, and the data mover and the Tivoli Storage Manager server resumes.

2. In the output of the query `vm * -vmrestoretype=instantrestore -detail` command, verify that the VM disks are active (Disk Path: Active). This status means that the VM was restored and is available for use.
3. If the network failure did not cause storage vMotion to time out, no action is required.
4. If the network failure caused storage vMotion to time out, and the error message indicates that the source disk is not responding, restart storage vMotion in the vSphere client. When storage vMotion processing completes, run the **restore vm** command with the **-vmrestoretype=VMCleanup** parameter to clean up the iSCSI disks. For example:

```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMCleanup
```

To attempt recovery after a Data Protection for VMware Recovery Agent service failure, complete the following steps:

1. Investigate that cause of the failure and restart the Data Protection for VMware Recovery Agent service if it does not start automatically. This action starts an automatic recovery of the mounted iSCSI disks.
2. In the output of the query `vm * -vmrestoretype=instantrestore -detail` command, verify that the VM disks are active (Disk Path: Active). This status means that the VM was restored and is available for use.
3. If the Data Protection for VMware Recovery Agent service failure did not cause storage vMotion to time out, no action is required.
4. If the Data Protection for VMware Recovery Agent service failure caused storage vMotion to time out, and the error message indicates that the source disk as not responding, restart storage vMotion in the vSphere client. When storage vMotion processing completes, run the **restore vm** command with the **-vmrestoretype=VMCleanup** parameter to clean up the iSCSI disks. For example:

```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMCleanup
```

Full cleanup

If you are not able to recover from a failure and want to remove the VM and its components, run the **restore vm** with the **-vmrestoretype=VMFULLCleanup** parameter. For example:

```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMFULLCleanup
```

A **VMFULLCleanup** operation forces removal of the VM and all of its components, regardless of the state of the virtual machine. Do not start a full clean up operation while vMotion is still migrating a virtual machine.

Full VM instant restore integrity validation scenarios

Windows

A new VM is built from the requested VM backup and is available for immediate use.

The process that creates a VM for verification is referred to as instant access. The verification itself is done by a specific application that the user must provide and operate. In this scenario, since the VM guest data remains in the Tivoli Storage Manager server repository, no additional storage is required on the primary data store.

Instant access and instant restore capability is supported only for VMware VMs that are hosted on VMware ESXi 5.1 servers, or later versions.

Start an instant access scenario

Start the instant access operation by entering the following Tivoli Storage Manager backup-archive client command and options:

```
dsmc restore vm Haifa -VMRESToretype=instanta -vmname=Haifa_verify
```

This command verifies the VM backup named Haifa without having to restore the VM. Since the original VM exists, the `-vmname` option assigns the new VM name Haifa_verify.

In this command, the `-vmautostart` option specifies that the VM created for verification is powered on automatically:

```
dsmc restore vm Haifa -VMRESToretype=instanta -vmname=Haifa_verify  
-VMAUTOSTARTvm=YES
```

By default, the VM created for verification is not powered on automatically. This default value allows the VM to be reconfigured before startup (if needed).

Specify the `-inactive` and `-pick` options to select the VM backup to validate from a list of all backed up VMs. Or, specify the `-pitdate` and `-pittime` options to select a VM backup by its backup date and time.

All location options (such as `-vmname`, `-datacenter`, `-host`, and `-datastore`) are supported by the `-vmrestoretype=instantaccess` and `-vmrestoretype=instantrestore` options.

This command returns a list of VMs that are running in instant access mode:

```
dsmc query vm * -VMRESToretype=instanta
```

This command starts the cleanup process for a VM backup:

```
dsmc restore vm Haifa -VMRESToretype=VMCleanup -vmname=Haifa_Verify
```

This command completes the instant access session. A cleanup process includes these actions:

- The temporary VM created for verification is deleted on the ESX host.
- The iSCSI mounts are unmounted on the vStorage Backup Server.
- The iSCSI device list is cleaned on the ESX host.
- The temporary data that is generated during verification is deleted by removing the VMware snapshot.

You cannot use the `-VMRESToretype=VMCleanup` option or the `-VMRESToretype=VMFULLCleanup` option to clean up a virtual machine while Storage vMotion is migrating it to a host.

Full VM recovery with application protection

Linux

Windows

Restoring a full VM that was backed up with self-contained application enabled, is the same as restoring a full VM that did not have self-contained application protection enabled. When the VM is powered on after a restore, the applications resume automatically, unless they are configured to be started manually.

Additional files are present on the Windows guest VM after the restore completes. These files are in the %TEMP%\TSM directory (where %TEMP% is the system environment variable for the account that runs the VMware vStorage API runtime files). These files can remain on the guest, or you can delete them. The Tivoli Storage Manager backup-archive client used the files to perform the application protection functions. Since the snapshot was taken when the files were on the guest, the restored guest VM also contains them.

Recover a Microsoft Exchange mailbox item from a VM backup

To recover Microsoft Exchange Server mailbox items from a VM backup, you must use both Data Protection for VMware and the IBM Tivoli Storage Manager FastBack for Microsoft Exchange product and documentation. As a result, IBM Tivoli Storage Manager FastBack for Microsoft Exchange must be purchased separately with a valid license. For more information, see the following product website:

<http://www.ibm.com/software/tivoli/products/storage-mgr-fastback-exchange/>

A mailbox item recovery scenario uses the products in the following order:

1. Access the VM backup by using the Data Protection for VMware Recovery Agent.
2. Recover mailbox items by using FastBack for Microsoft Exchange.

Recover individual Microsoft SQL databases from a VM backup

To recover Microsoft SQL databases from a VM backup, you must use both Data Protection for VMware and the IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server V7.1 product and documentation. As a result, IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server V7.1 must be purchased separately with a valid license. For more information, see the following product website:

<http://www.ibm.com/software/products/us/en/tivostormanafordata/>

A recovery of a Microsoft SQL database from a VM backup scenario requires the following environment:

- Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server V7.1 is installed and configured on a guest VM.
- The Data Protection for VMware Recovery Agent feature is installed on the same guest VM as Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server V7.1. When you install Tivoli Storage Manager for Virtual Environments V7.1, select the Data Protection for VMware Recovery Agent feature.
- The VSS service and SQL Server instance must be online and active. SQL Server databases that do not have an active instance are backed up. However,

information about these databases is not saved to Tivoli Storage Manager. Therefore, these databases are not available for a database-level restore operation. You can restore these databases with a full VM restore operation.

VM backups are identified in the Data Protection for Microsoft SQL Server GUI Recover page with **Backup type VMVSS**.

Restore of individual Microsoft SQL Server databases is available from basic disks with MBR-style partitions within the guest. If Microsoft SQL Server database data or log files are stored on a Windows Dynamic disk, or on a disk with GPT-style partitions, the database is not available at restore time.

Restoring from virtual machine snapshots

You can restore SQL databases from a virtual machine where Tivoli Storage Manager for Virtual Environments, Version 7.1 and later is used to back up the data.

Before restoring SQL databases from virtual machine snapshots, verify that the data was backed up according to the following procedure:

1. Install the Tivoli Storage Manager for Virtual Environments Recovery Agent 7.1 package and the Tivoli Storage Manager Backup-Archive Client 7.1 from the Data Protection for VMware 7.1 package. These software packages are available for download from Passport Advantage.

Install these packages on the guest virtual machine with Data Protection for Microsoft SQL Server.

2. Specify the following Tivoli Storage Manager Backup-Archive Client 7.1 option in the `dsm.opt` file:

INCLUDE.VMTSMVSS *vmname*

When you set this option, virtual machine applications receive a notification when a backup is going to occur. This notification allows the application to truncate transaction logs and commit transactions so the application can resume from a consistent state when the backup completes. By default, this option is not enabled. You must set this option to enable application protection for a virtual machine.

The *vmname* specifies the name of the virtual machine that contains the applications to quiesce. Specify one virtual machine per **INCLUDE.VMTSMVSS** statement. To protect all virtual machines with this option, use an asterisk as a wildcard. For example:

INCLUDE.VMTSMVSS *

You can also use question marks to match any single character. For example:

INCLUDE.VMTSMVSS *vm??*

This type of option setting protects all virtual machines that have names that begin with *vm* and are followed by any two characters. For example, *vm10* and *vm15*.

If the **OPTIONS KEEPSqllog** parameter is specified in an **INCLUDE.VMTSMVSS** statement, this parameter prevents SQL server logs from being truncated when a data mover node backs up a virtual machine that runs a SQL server. Specifying this parameter allows the SQL server administrator to manually manage the SQL server logs. The logs can be preserved as needed and be used to restore SQL transactions to a specific checkpoint, after the virtual machine is restored. When this option is specified, the SQL log is not truncated and following message is displayed and logged on the server:

ANS4179I IBM Tivoli Storage Manager application protection did not truncate Microsoft SQL Server logs on virtual machine *vmname*

Note: Tivoli Storage Manager does not back up the SQL log files. The SQL administrator must back up the log files so they can be applied after the database is restored.

3. Verify that the VSS service and SQL Server instance are online and active. SQL Server databases that do not have an active instance are backed up. However, information about these databases is not saved to Tivoli Storage Manager. Therefore, these databases are not available for a database-level restore operation. You can restore these databases with a full VM restore operation.
4. Use the Tivoli Storage Manager for Virtual Environments software to back up the data. After you back up data, you can use the following procedure to restore the data.
5. Verify that the virtual machine backup contains the necessary database metadata. To do this, enter the following Tivoli Storage Manager Backup-Archive Client command on the data mover:
`dsmc query vm <vmname> -detail`

In the command output, the Application(s) protected: value must specify (database-level recovery). For example:

```
# Backup Date Mgmt Class Size Type A/I Virtual Machine
-----
1 06/07/2012 19:25:58 STANDARD 29.29 GB FULL A wombat
The size of this incremental backup: n/a
The number of incremental backups since last full: n/a
The amount of extra data: n/a
The TSM objects fragmentation: n/a
Backup is represented by: n/a
Application protection type: TSM VSS
Application(s) protected: MS SQL 2008 (database-level recovery)
VMDK[1]Label: Hard disk 1
VMDK[1]Name: [ess800_dev1] wombat/wombat-000002.vmdk
VMDK[1]Status: Protected
```

When you restore data, the data can be restored to basic disks with MBR-style partitions. Because of a SQL Server limitation, you cannot restore a VSS backup to an alternative SQL server instance. VSS backups must be restored to the same SQL server instance where the snapshot was taken.

Also, when restoring an SQL database from a VM backup, if the VM name is changed after the VM backup, the restore is not possible.

To restore SQL databases from a supported virtual machine snapshot, complete the following steps:

1. Log on to the system where you want to restore the SQL database. The Data Protection for VMware Recovery Agent license and Data Protection for Microsoft SQL Server must be installed on the system where you are restoring the data.
2. When Data Protection for Microsoft SQL Server is configured, for the Configuring Recovery Agent rule, verify that the status is *Passed*. If the status is not *Passed*, re-run the configuration wizard. On the TSM Node Names wizard page, enter the data center node name. The data center node is the virtual node that maps to a data center.

3. Use the following procedure to set access to the virtual machine that is backed up in a data center node. To complete the following procedure, use the following reference information:

Table 11. Node names used to set access

Node name	Location	Description	Proxy type
DC_NODE	Data mover	Node for the virtual machine backup	Agent (data owner)
SQL_NODE	In guest virtual machine running Microsoft SQL	Node for Data Protection for Microsoft SQL Server	Agent (data owner)
VSS_NODE	In guest virtual machine running Microsoft SQL	Node for Data Protection for Microsoft SQL Server DSMAGENT	Agent (data worker)

For the Data Protection for Microsoft SQL Server software to restore the data owned by the DC_NODE, the Tivoli Storage Manager administrator gives access to the virtual machine backed up to the VSS_NODE. The Tivoli Storage Manager administrator can use the Tivoli Storage Manager command-line interface to enter the **set access** command while connected to the DC_NODE.

Running the commands from the DC_NODE is ideal because the options file has the necessary settings to communicate with the Tivoli Storage Manager server. The Tivoli Storage Manager administrator credentials can be used if the DC_NODE administrator password is not available.

The **set access** command cannot be run if the ASNODE option is in affect. To issue the **set access** command, use an option file that does not contain ASNODE. The information needed to complete this task is provided in the following procedure.

- a. Copy dsm.opt and dsm.setaccess.opt files.
- b. If running the **set access** command from a node with ASNODE in the options file, complete this step. Edit the dsm.setaccess.opt file. For any line that contains ASNODE, remove the line.
- c. Edit the dsm.setaccess.opt file to set the NODENAME option to the following entry:
DC_NODE NODENAME DC_NODE
- d. Enter the following command:
dsmc set access backup -type=VM traveler VSS_NODE -optfile=dsm.setaccess.opt

You might be prompted to enter the password for the DC_NODE.

For any subsequent **set access**, **query access**, and **delete access** commands, use this same procedure to guide you.

4. From the Data Protection for Microsoft SQL Server Management Console, in the Protect and Recover Data navigation, select a **SQL Server**.
5. Within the **Recover** tab for that SQL server, select **View: Databases** for a list of SQL database backups that are available for restore. SQL databases that were backed up with Tivoli Storage Manager for Virtual Environments software are listed with the VMVSS backup method.
6. Review the restore options by clicking Show Restore Options.
7. Optional: Choose a mode for the current task:
 - **Run Interactively:** Click this item to run the current task interactively. This selection is the default.

- **Run Scheduled:** Click this item to convert the current action into a scheduled task. When you select this item, the schedule wizard begins, complete with the command that is required to complete the task.
8. Click **Restore** in the Actions pane to begin the restore operation.

The restore operation is displayed in the **Task List** pane. Click **Task Details** to view detailed status information about the restore operation.

Verifying that the Active Directory Domain Controller replicated successfully

When a VM guest that contains an Active Directory Domain Controller (AD DC) is restored with Data Protection for VMware, the DC (on that VM) is restored from a backup copy of the AD database.

The original VM must be powered off before the restored VM is started. In addition, the restored VM must be manually rebooted for replication to occur.

The following tasks occur upon a successful Data Protection for VMware restore and subsequent reboot of the VM guest that contains the AD DC:

1. The DC is updated from a backup copy of the AD DC database. A new invocationID is assigned to the Directory Server. This update is indicated by event 1109 in the event log on the VM guest. To verify this update:
 - a. In the Computer Management window on the restored system, go to **System Tools > Event Viewer**.
 - b. When the AD DC restored successfully, the Information type event for the restored DC displays the following message:

ActiveDirectory 1109 Replication

The message in the Event Viewer also confirms a successful restore because of the changed invocationID attribute:

The invocationID attribute for this directory server has been changed.
The highest update sequence number at the time the backup was created is <time>
InvocationID attribute (old value):<Previous InvocationID value>
InvocationID attribute (new value):<New InvocationID value>
Update sequence number:<USN>
The InvocationID is changed when a directory server is restored from backup media or is configured to host a writeable application directory partition.

2. The restored DC replicates itself non-authoritatively with its replication partners in the network. It is updated with the most current domain, schema, configuration, and application partitions:

Note: Data Protection for VMware does not support authoritative restore.

- a. Log in to the VM guest that was restored by using Data Protection for VMware as an Administrator.
- b. Open a Windows command prompt.
- c. Check the status of the last replication that involved the restored DC by issuing the `repadmin /showrepl` command¹. This command shows the replication partners for each directory partition on the DC and the status of the last replication.

1. Repadmin.exe is a Microsoft command-line tool that is installed with Microsoft Active Directory.

If the replication schedule did not start, you can manually start the replication operation. Go to the Active Directory Sites and Services, select the replication partners, and right-click **Replicate Now**.

For detailed information about initiating replication, see the following Microsoft Knowledge Base article:

<http://support.microsoft.com/kb/232072>

When the status is newer than the restore time, this status means that the replication was successful and completed automatically. The following output shows that replication was successful:

```
Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC12012
DSA Options: IS_GC
Site Options: <none>
DSA Object GUID: 8393da24-f18b-453a-b197-b8dc6956d51f
DSA invocationID: 8393da24-f18b-453a-b197-b8dc6956d51f

==== INBOUND NEIGHBORS =====

CN=Configuration,DC=his,DC=local
Default-First-Site-Name\DC22012 via RPC
DSA Object GUID: 790c6f2d-61f1-4704-bdcf-6ef731bcb96e
Last attempt @ 2013-01-25 14:33:10 was successful.
```

When the repadmin /showrepl command displays a successful replication, the AD DC replication is considered successful. No additional tasks are required.

- d. When the repadmin /showrepl command shows that replication was not successful, output similar to the following is shown:

```
Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\DC12012
DSA Options: IS_GC
Site Options: <none>
DSA Object GUID: 8393da24-f18b-453a-b197-b8dc6956d51f
DSA invocationID: 8393da24-f18b-453a-b197-b8dc6956d51f

==== INBOUND NEIGHBORS =====

CN=Schema,CN=Configuration,DC=his,DC=local
Default-First-Site-Name\DC22012 via RPC
DSA Object GUID: 790c6f2d-61f1-4704-bdcf-6ef731bcb96e
Last attempt @ 2013-01-25 14:30:32 failed, result 1908 <0x774>:
Could not find the domain controller for this domain.
1 consecutive failure(s).
Last success @ 2012-12-14 15:01:36.
```

If a replication failure exists or persists, follow the instructions provided in the next section.

Recover from Replication Failures

Use the following methods to investigate the cause of a persistent replication failure:

1. Use the Microsoft Domain Controller Diagnostics tool (dcdiag.exe) to view information about all components, objects, and permissions that are required for successful replication. For example:
 - a. Open a Windows command prompt as an administrator.

- b. Issue the `cdiag /test:replications` command. Use the output information to resolve any issues. If the command fails, investigate the events that are at **Event Viewer > Directory Service > ActiveDirectory_DomainServices**.
2. Use the Microsoft Repadmin.exe command-line tool to view the retired invocationID on a DC. For example:
 - a. Open a Windows command prompt as an administrator.
 - b. Issue the `repadmin /showsig [DC_LIST]` command. This output shows that restore from Tivoli Storage Manager was successful because a retired invocationID exists:

```
C:\Users\Administrator>repadmin /showsig rodc
Default-First-Site-Name\RODC

Current DSA invocationID: ed8ea6b9-d347-4695-b886-b5128be280c4
2c995946-2389-4d98-bc78-3708ba906e01 retired on 2012-12-19 16:56:21
at USN 17703
```

When the output contains the statement No retired signatures, the AD was not restored from Tivoli Storage Manager correctly. As a result, replication cannot be completed because the partner DCs mistake the new invocationID as evidence for a completed replication. For example:

```
C:\Users\Administrator>repadmin /showsig rodc
Default-First-Site-Name\RODC

Current DSA invocationID: ed8ea6b9-d347-4695-b886-b5128be280c4
No retired signatures
```

When the invocationID is retired, the replication can be started. However, this statement does not guarantee success of the replication.

Restoring files and instant restore of volumes with the Data Protection for VMware Recovery Agent

Use the Data Protection for VMware Recovery Agent to perform an instant restore of a volume or to mount a snapshot for a file-level restore.

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.

Before proceeding, make sure you have reviewed the following information:

- “Mounting snapshots overview” on page 24
- “Mounting snapshot guidelines for Windows systems” on page 24
- “File-level restore overview” on page 26
- “File-level restore guidelines for Windows systems” on page 28

In order to recover Microsoft Exchange Server mailbox items, you must use the IBM Tivoli Storage Manager FastBack for Microsoft Exchange product and documentation. As a result, IBM Tivoli Storage Manager FastBack for Microsoft Exchange must be purchased separately with a valid license. For more information, see the following product website:

<http://www.ibm.com/software/tivoli/products/storage-mgr-fastback-exchange/>

Windows 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 the Data Protection for VMware Recovery Agent GUI from the **Start > All Programs** menu or by clicking the Data Protection for VMware Recovery Agent icon in the taskbar.
3. Connect to a Tivoli Storage Manager server by clicking **Select TSM server**. The target node is where the backups are located. You can manage the level of access to the target node data by specifying a different node name in the Node access method section.

A list of VMs with snapshots stored in the specified node displays.

4. Select a VM from the list. A list of snapshots for the selected VM displays.

Tip: You can find your VM quickly by typing the first few letters of the machine name in the edit portion of the list box. The list shows only those machines that match the letters you entered. Machine names are case-sensitive.

A VM might display in the list, but if you select it, the snapshots list might be empty. This situation occurs because of one of the following reasons:

- No snapshots completed successfully for that VM.
 - The **Fromnode** option was used and the specified node is not authorized to restore the selected VM.
5. Select the preferred snapshot date. A list of VM disks that are backed up in the selected snapshot displays. Select a disk and click **Mount**.
 6. In the Select Mount Destination dialog, check **Create virtual volume from selected partition**. A list of partitions available on the selected disk is shown. 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.
 7. Select the required partition. Partitions formatted using unsupported file systems cannot be selected.
 8. Specify a drive letter or an empty folder as a mount point for the virtual volume.
 9. Click **OK** to create a Virtual Volume that can be used to recover the files.
 10. When the Virtual Volume is created, use Windows Explorer to copy the files to your preferred location.

Important: The ACL values associated with the folders and files that are restored in a file level recovery operation are not transferred to the recovered files. In order to maintain ACL values, use the XCOPY command when copying files from the target.

Instant restore of volumes (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.

Before proceeding, make sure you have reviewed the following information:

- “Mounting snapshots overview” on page 24
- “Mounting snapshot guidelines for Windows systems” on page 24
- “Instant restore overview” on page 29
- “Instant restore guidelines for Windows systems” on page 29

The Data Protection for VMware Recovery Agent GUI must be configured before attempting a file-level restore operation. To configure, click **Select TSM server** and **Settings** in the Data Protection for VMware Recovery Agent GUI and enter the required information.

Windows

To perform an instant restore, complete the following steps:

1. On the guest machine, start the Data Protection for VMware Recovery Agent GUI from the **Start > All Programs** menu or by clicking the Data Protection for VMware Recovery Agent icon in the taskbar.
2. In the Data Protection for VMware Recovery Agent window, select the Tivoli Storage Manager server to use as the source by clicking **Select TSM server**. Although the **Select TSM server** list appears to contain multiple servers, this list contains a maximum of one server only. Data Protection for VMware Recovery Agent queries the Tivoli Storage Manager server for a list of protected VMs and displays the list.
3. Select a VM, date, time, and disk, and then 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.
 - If a disk cannot be parsed, an error message is displayed and the **Instant Restore** dialog is closed. For example, this occurs when the disk is dynamic or a GUID partition table (GPT).
5. Select the destination partition into which the data is to be restored. The destination location size must be equal or larger than the source size.
 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**

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, 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**. During the period when the session is paused, the parts of the volume that are not yet restored are inaccessible.

You can use instant restore to restore a simple volume that is located on a dynamic disk. The destination volume can be a dynamic disk; however, the source volume cannot be a dynamic disk. This restore might cause the disk status to change to *Online (Errors)*. In addition, the status of all volumes on the disk might 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**.

Restoring files (Linux)

File-level restore on Linux is available from snapshots of disks.

Before proceeding, make sure you have reviewed the following information:

- “Mounting snapshots overview” on page 24
- “Mounting snapshot guidelines for Linux systems” on page 25
- “File-level restore overview” on page 26
- “File-level restore guidelines for Linux systems” on page 28

Linux 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 by clicking **Select TSM server**. Although the **Select TSM server** list appears to contain multiple servers, this list contains a maximum of one server only. Click **Refresh** after selecting a server.
Data Protection for VMware Recovery Agent queries the server for a list of protected VMs and displays the list.
2. Select a VM from the list. Data Protection for VMware Recovery Agent queries the server for a list of snapshots available for the specified VM. A VM might be displayed in the VMs list, but if you select it, the snapshots list might be empty. This situation might occur for one of the following reasons:
 - No snapshots have yet completed successfully for that VM.
 - The node used for authentication was not granted permission to restore the selected VM.

Tip: To quickly locate the required VM from the available VM list, type the first few letters of the VM 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.

Note: Mount points are not displayed.

4. Click **Mount**.
5. Select the required partition in the Choose mount destination dialog. To display all partitions, clear the **Show only mountable partitions** check box.
6. Specify the path where the virtual volume is mounted in the Use the following mount point field.
7. Click **OK** to complete the mount operation. 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]
```

8. Locate the files you are interested in and restore them from the backup.

Important: The ACL values associated with the folders and files that are restored in a file level restore operation are not transferred to the restored files. In order to maintain ACL values, use the `cp -p` command when copying files.

Instant restore of volumes (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.

Before proceeding, make sure you have reviewed the following information:

- “Mounting snapshots overview” on page 24
- “Mounting snapshot guidelines for Linux systems” on page 25
- “Instant restore overview” on page 29
- “Instant restore guidelines for Linux systems” on page 31

Linux 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 by clicking **Select TSM server**. Click **Refresh** after selecting a server. Data Protection for VMware Recovery Agent queries the server for a list of protected VMs and displays the list.
2. Select a VM from the list. Data Protection for VMware Recovery Agent queries the server for a list of snapshots available for the specified VM.

Tip: To quickly locate the required VM from the available VM list, type the first few letters of the VM name.

3. Select the required snapshot by selecting the date and disk.
4. Click **Restore**.

5. Select the required partition in the Choose instant restore destination dialog. 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: Mount points are not displayed.

6. Specify the destination partition into which the data is to be restored, by specifying a mount point or a block device. If you specify both, make sure the block device is mounted on the specified mount point.
7. 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.

Linux

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 `sdcl` 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/sdcl /restoredVolume`.

Linux

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.

Responding to a timeout during a file level restore or an instant restore (Linux)

During a file level restore or an instant restore, a timeout might occur. If a timeout does occur, the user interface displays a message saying that manual intervention might be needed.

Linux

Follow this procedure if the timeout occurs during a file level restore (Mount operation):

1. Stop the recovery process by commenting out the one line in `/etc/cron.d/tsmmount_recover` Ensure that the recovery process is not running by issuing this command:
`ps -ef | grep tsmRecover`
2. Ensure that the required snapshot is mounted in the Data Protection for VMware Recovery Agent Windows backup server. If the snapshot is not mounted, mount it manually.
3. Ensure that the iSCSI target is connected to the Linux machine by using **iscsiadm -m session**. If the iSCSI target is not connected to the Linux machine, perform a manual login to the target by issuing this command:
`iscsiadm -m discovery -t sendtargets -p <windows_server_ip> --login`

4. Mount the iSCSI device locally by using the Linux **mount** command. For example:

```
mount /dev/sde1 /Mount1
```

Ensure that you use the same mount point as was requested in the user interface. This operation can take long time to complete depending on the consistency of the snapshot.

5. When the mount operation is completed, uncomment the line in `/etc/cron.d/tsmmount_recover`.
6. When you want to unmount, do so first locally by using **umount**. Then use the Linux user interface to unmount the session.

For an instant restore operation the manual intervention is to halt and then retry the restore session.

Appendix A. Troubleshooting

Solutions to Data Protection for VMware vSphere GUI and Data Protection for VMware command-line interface issues are provided.

Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI backup or restore operation fails

Complete these tasks to resolve a backup or restore failure:

1. Log on to the system where the Tivoli Storage Manager backup-archive client is installed.
2. Start a command-line session:
 - **Windows** Open the Windows **Start** menu and select **Programs > Tivoli Storage Manager > Backup Client Command Line**.
 - **Linux** Open a terminal window.
3. If not already there, go to the installation directory:

Windows

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

Linux

```
cd /opt/tivoli/tsm/client/ba/bin
```

By default, error log files are in the installation directory.

4. View these Tivoli Storage Manager backup-archive client log files to see if an error was generated:
 - dsmerror.log: All client messages.
 - dsmwebcl.log: All web client messages.
 - dsmj.log: All client Java GUI messages.

These log files are located in the directory you specify with the DSM_LOG environment variable or in the current working directory.

Tip: You can view error explanations in the Tivoli Storage Manager information center.

5. If neither of these files contain an error, run a backup-archive client backup and restore operation to see if it fails.
6. If the backup-archive client operations complete successfully, run a Data Protection for VMware command-line interface “Backup” on page 40 and “Restore” on page 43 operation. Set the appropriate trace parameters (as described in “Profile parameters” on page 63) so you can view any errors that might be generated.

Data Protection for VMware command-line interface backup fails with scSignOnAsAdmin: Error 53

In this situation, a Data Protection for VMware command-line interface backup operation failed and this error was generated to the backup-archive client dsmerror.log:

```
scSignOnAsAdmin: Error 53 receiving SignOnAsAdminResp verb from server
```

Typically, this error results when the VMCLI node name is different from its administrator name. Tivoli Storage Manager requires these two names to be the same.

Tivoli Storage Manager data mover nodes are not visible during a backup operation

Verify that the correct proxy node authority was granted on the Tivoli Storage Manager server. If the correct authority exists, then the data center mapping specified by the VE_DATACENTER_NAME profile parameter is incorrect. See “Profile parameters” on page 63 for a complete description and correct syntax of the VE_DATACENTER_NAME parameter.

The inquire_detail command failed with Return Code 53

In this situation, the `vmcli -f inquire_detail` command failed and this error was generated to your log file:

```
ANS1033E (RC-53) An invalid TCP/IP address was specified.
```

This error occurs when a node name does not match its administrator name. This issue can happen when you rename a node but do not rename its administrator. The solution is to either rename the administrator to match the new node name or register a new administrator for the new node.

The commands in these examples are issued from the Tivoli Storage Manager Administrative Command Line:

- Rename the administrator at the same time you rename the node:

```
rename node <current_node_name> <new_node_name>
rename admin <current_admin_name> <new_node_name>
```

For example:

```
rename node DC_VC5 DC_WIN2K8_X64
rename admin DC_VC5 DC_WIN2K8_X64
```

As a result, the new administrator name matches the new node name.

- Register the administrator directly after renaming the node:

```
rename node <current_node_name> <new_node_name>
register admin <new_admin_name> <password>
```

For example:

```
rename node DC_VC5 DC_WIN2K8_X64
register admin DC_WIN2K8_X64 DC_WIN2K8_X64PWD
```

As a result, the new administrator name matches the new node name.

Invalid sign on and invalid password errors received

In this situation, Data Protection for VMware command-line interface, Data Protection for VMware vSphere GUI, or Data Protection for VMware vCloud GUI operations failed and your log file contained one (or more) of these errors:

GVM1170E: A VMCLI command failed.

ANR2177I FRSV123015.TSMCLI has 1 invalid sign-on attempts. The limit is 5.

ANR0424W Session 125713 for node FRSV128215.TSMCLI (TSM4VE) refused - invalid password submitted.

This issue can occur when a VMCLI node set password attempt was made by using a password that was previously set.

When the VMCLI node password is set, the password is registered and then automatically changed. As a result, you do not know this changed password. If you must change the VMCLI node password after it is already set, the Tivoli Storage Manager Administrator must use the update node command to reset this node on the Tivoli Storage Manager server. When the node has been reset, set the VMCLI node password again and specify the new password.

The VMCLI node password is set by either of these methods:

- Data Protection for VMware command-line interface: **vmcli -f set_password** command
- Data Protection for VMware vSphere GUI: **Configuration > Tasks > Edit Configuration > VMCLI Node**
- Data Protection for VMware vCloud GUI: **Configuration > Tasks > Edit Configuration > VMCLI Node**

Session timeout

The Tivoli Storage Manager server COMMTIMEOUT option affects the duration of the Data Protection for VMware session. If the processing time of the Data Protection for VMware operation exceeds this value, the server ends the session with Data Protection for VMware. Therefore, if you are sure that no error has occurred during a Data Protection for VMware operation and the COMMTIMEOUT value has been reached, increase the value. Likewise, if an error occurred but Data Protection for VMware did not report the error in a timely manner, then decrease the value for better real-time reporting.

vSphere Client displays a Data Protection for VMware vSphere GUI connection error

In this situation, the Data Protection for VMware vSphere GUI was installed successfully on the vCenter node. However, when viewing the Data Protection for VMware vSphere GUI in the vSphere Client Plug-in Manager (**Menu > Plug-ins > Manage Plug-ins**), the following message is shown:

```

Tivoli Data Protection for VMware
IBM Tivoli Storage Manager 2.1
Disabled
Tivoli Data Protection for VMware Plug-in
The following error occurred while downloading the script plugin from
http://finapps.mycompany.com:9080/TsmVMwareUI/plugin/config.xml:
The request failed because of a connection failure. (Unable to connect
to the remote server)

```

This issue can occur when the web server cannot access ports specified in the bootstrap.properties file. During installation, the web server accesses port 9080. However, when these additional ports cannot be accessed, the vSphere Client cannot connect to the Data Protection for VMware vSphere GUI.

Complete these tasks to resolve this issue:

1. On the system where the Data Protection for VMware vSphere GUI is installed, go to the following directory for your operating system: **Linux**

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

Windows

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

2. Open the bootstrap.properties file to view the eWAS port settings. For example:

```

veProfile.http.port=9080
veProfile.https.port=9081
veProfile.keystore.pswd={xor}KzosK2sp0g==

```

3. Issue the netstat -a command to view all active connections and ports. Compare the results with the port settings in the bootstrap.properties file. If any of the ports (specified in the bootstrap.properties file) are not open, complete either of the following tasks to resolve this connection issue:

- Open the closed ports.
- Update the bootstrap.properties file with ports that are available.

4. Restart the GUI web server:

Windows

- a. Click **Start > Control Panel > Administrative Tools > Services**.
- b. Right-click Data Protection for VMware Web Server Service and click **Restart**.

Linux

Issue the following command as root:

```
[root@bold4win /]# service webserver restart
```

```

Restarting the WebSphere Liberty Profile ...
Stopping server veProfile.
Server veProfile stopped.
Starting server veProfile.
Server veProfile started with process ID 17894.

```

5. Start the Data Protection for VMware vSphere GUI with either of these methods:

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

Login by using the vCenter user name and password.

Resolving a VM guest (with application protection) backup failure

In this situation, a backup (with application protection) of a guest machine is stopped by the user. When the Tivoli Storage Manager backup-archive client backup process (dsmagent or dsmsc) ends in this manner, the cleanup of the application protection does not take place. As a result, the next backup (with application protection) of the same guest machine can be issued only after a 10 minute interval. This interval is the length of time necessary for the process to recognize that the guest machine is not backed up.

To manually clean up application protection without waiting 10 minutes for communication to clear, complete these steps:

1. Log on to the guest machine with the same user ID and password that was entered when issuing the backup operation.
2. Open a command prompt window and issue this command:
`echo %TEMP%`
3. Go to the %TEMP% directory, then change to the Tivoli Storage Manager directory. For example:
`C:\Users\Administrator\AppData\Local\Temp\TSM`
4. Delete the BackupHeartBeat.txt file.
5. Back up the guest machine.

Event log contains event ID 8194, VSS message

After a backup of a VM guest with application protection completes, the event log contains the event ID 8194, VSS error message. This cause of this message is an incorrect security setting in the Volume Shadow Copy Service (VSS) writer or requestor process.

To resolve this error, complete these steps:

1. Log on to the VM guest as an administrator and run the Microsoft dcomcnfg.exe utility in the **Start > Run** dialog:
`dcomcnfg.exe`

Click **OK**.
The dcomcnfg.exe utility is used to modify registry settings.
2. In the Component Services interface, go to **Component Services > Computers**. Right-click **My Computer** and select **Properties**.
3. In the My Computer properties panel, go to **COM Security > Access Permissions: Edit Default**.
4. In the Access Permission panel, add the Network Service account with Local Access permission set to Allow.
5. Apply your changes and close all open Component Services panels.
6. Restart the VM guest.
7. Back up the VM guest and verify that the event ID 8194, VSS error message is not issued to the event log.

Data Protection for VMware installation failure: deployment engine initialization

The Data Protection for VMware installation might be stopped due to a deployment engine initialization failure due to .lock files. If the deployment engine interferes with the Data Protection for VMware installation, the following error message is produced:

```
Deployment Engine failed to initialize.  
The installer will now shutdown. Please check with the log files for a more  
complete description of the failure.  
PRESS ENTER TO CONTINUE:
```

The cause might be deployment engine .lock files that come from a concurrent installation that is running or from an installation that stopped before completing. If another installation is running, wait until that installation finishes before installing Data Protection for VMware. If there are no other installations running and you encounter this problem, delete any .lock files.

Important: Do not delete any .lock files if there are other Data Protection for VMware installations running.

Windows To delete .lock files on Windows, issue the following command:

```
cd C:\Program Files\IBM\Common\acsi\logs  
del .lock*
```

Linux To delete .lock files on Linux, issue the following command:

```
cd /usr/ibm/common/acsi/logs  
rm .lock*
```

After removing these files, restart the installation.

Unsupported characters in VM or datacenter name

Data Protection for VMware does not support backing up VMs or datacenters that contain any of the following characters in their name:

- " Double quotation mark
- ' Single quotation mark
- :
- ;
- *
- ?
- ,
- <
- >
- /
- \
- |

Issues encountered after changing the vCenter

After changing the vCenter in the Data Protection for VMware vSphere GUI, the following two issues might occur:

- A data center associated with the new vCenter does not appear on the Configuration Status page.

To resolve this issue, manually set the domain for the new vCenter. See “Set_domain” on page 54 for details about issuing this command.

- In the Restore tab, an ESX host (associated with a previous data center) displays under a new data center within the new vCenter. This issue is a known limitation. There is currently not a workaround for this issue

Consolidating VM backups

After a VM backup, the VM might contain preexisting snapshots even though no snapshots are present in the Snapshot Manager. For example, the VM hard disk points to snapshot VMDK files (for example *-000001.vmdk) instead of regular VMDK files. Although preexisting snapshots might be intentionally retained, Data Protection for VMware does not provide a mechanism to verify whether the VMDK points to a valid snapshot. When snapshots are not consolidated, and a VM with preexisting snapshot files is backed up, Data Protection for VMware might report an incorrect size for the backup on the Tivoli Storage Manager server. Snapshot consolidation also prevents other VMware related issues. As a result, consolidate your snapshots whenever this situation occurs.

To resolve this potential problem, VMware vSphere Client 5.x (or later) notifies you when a VM requires snapshot consolidation. Details about the consolidate option are provided in the following VMware KB article:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2003638

For vSphere 4.1 (or earlier), no consolidation option is available. However, the equivalent task is to create a snapshot and then complete a Delete All action.

Re-register the Data Protection for VMware vSphere GUI

To use the Data Protection for VMware vSphere GUI as a vSphere Client plug-in, it must be registered to the vCenter. When the IP address changes on the system where the Data Protection for VMware vSphere GUI is installed, you must re-register the Data Protection for VMware vSphere GUI. If you cannot find the Data Protection for VMware vSphere GUI in the plug-in Manager, re-register the Data Protection for VMware vSphere GUI. Use this procedure when the IP address changes or you did not enable GUI access as a plug-in during installation:

1. Log in to the system where the Data Protection for VMware vSphere GUI is installed.
2. Go to the following directory:

Linux /opt/tivoli/tsm/tdpvmware/common/scripts

Windows (64-bit) C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\

3. To register the Data Protection for VMware vSphere GUI, enter the command:

Linux

```
../jre/jre/bin/java -jar reg.jar vCenterServer vCenterUser  
vCenterPassword new_guiHostnameShort new_guiHostnameFull 9080
```

The `new_guiHostnameShort` value is the name that is shown for the Data Protection for VMware vSphere GUI icon in the vCenter.
The `new_guiHostnameFull` value is either the full DNS hostname or the numeric IP address. For example:

```
../jre/jre/bin/java -jar reg.jar vctr.archive.mycompany.com administrator  
pass4admin myguihost myguihost.mydomain.mycompany.com 9080
```

Windows

```
register_vcenter.cmd vCenterServer vCenterUser  
vCenterPassword 9080
```

A `config.xml` file is created.

- Copy the `config.xml` file to the following directory:

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/
veProfile/apps/tsmVmGUI.war/plugin/`

Windows `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\
apps\tsmVmGUI.war\plugin\`

- Restart the GUI web server:

- Linux** Issue the following command as root:

```
[root@bold4win /]# service webserver restart
```

- Windows**

- Click **Start > Control Panel > Administrative Tools > Services**.
- Right-click Data Protection for VMware Web Server Service and click Restart.

- Restart the vSphere Client and confirm that the Data Protection for VMware vSphere GUI is now registered.

An error occurred while making the Web server request (GVM0103E)

In this situation, the Data Protection for VMware vSphere GUI or Data Protection for VMware vCloud GUI shows the following error when you tried to access it:

GVM0103E: An error occurred while making the Web server request. If this error persists, check the network connection with the Web server and verify that the Web server is running.

To prevent this error, make sure that the following conditions exist before you start the GUI:

- Linux** **Windows** The Data Protection for VMware vSphere GUI is installed on a system that meets the operating system prerequisites. It must have network connectivity to the following systems:
 - vStorage Backup Server
 - Tivoli Storage Manager server
 - vCenter Server (Data Protection for VMware vSphere GUI)
 - vCloud Director (Data Protection for VMware vCloud GUI)
- Windows** The Data Protection for VMware vSphere GUI host URL address must be set in your Internet Explorer trusted sites zone. In the Internet Explorer menu bar, go to **Tools > Internet Options > Security > Trusted sites**. Click **Sites** and add the host URL address. Make sure to apply your changes. For example:

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

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

Data Protection for VMware vSphere GUI does not display correctly in the VMware vCenter

In this situation, the Data Protection for VMware vSphere GUI is registered as a vCenter plug-in. However, the Data Protection for VMware vSphere GUI icon does not display in the Solutions and Applications window of the vSphere Client. When you view the Data Protection for VMware vSphere GUI in the vSphere Client Plug-in Manager (**Menu > Plug-ins > Manage Plug-ins**), the following message is shown:

The following error occurred while downloading the script plugin from <http://192.168.66.58:9080/TsmVMwareUI/plugin/config.xml>:
The request failed because of a connection failure.
(Unable to connect to the remote server)

To resolve this error, complete the following steps:

1. Check the network to verify that there is a connection to the web server host.
2. If the URL is incorrect, manually register the Data Protection for VMware vSphere GUI as a plug-in:

- **Windows** (x86) Open a command prompt and go to the following directory:
`C:\Program Files\Common Files\Tivoli\TDPVMware\VMwarePlugin`

Issue the following command:

```
C:\Windows\System32\cmd.exe /c register_vcenter.cmd "vcenter hostname or IP" "vcenter username" "vcenter password" "web server port" "VE proxy machine IP"
```

- **Windows** (x64) Open a command prompt and go to the following directory:
`C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin`

Issue the following command:

```
C:\Windows\System32\cmd.exe /c register_vcenter.cmd "vcenter hostname or IP" "vcenter username" "vcenter password" "web server port" "VE proxy machine IP"
```

Return codes for VM backup operations

The following return codes apply to VM backup operations on Linux or Windows systems:

Table 12. Return codes for VM backup operations

Return Code	Description
0	A command to process one or more VMs completed successfully.

Table 12. Return codes for VM backup operations (continued)

Return Code	Description
8	A command to process multiple VMs succeeded on only some of the VMs that were targeted by the command. Examine the log file to determine the processing status for each of the targeted VMs.
12	A command was issued to process one or more VMs. The command did not complete for any of the VMs that were targeted by the command. Examine the log file to determine possible reasons for the failure.

Appendix B. Data Protection for VMware vSphere GUI and Data Protection for VMware vCloud GUI messages

This information contains explanations and suggested actions for messages issued by the Data Protection for VMware vSphere GUI and Data Protection for VMware vCloud GUI.

For messages shown in the Data Protection for VMware vSphere GUI and Data Protection for VMware vCloud GUI that contain the FMM prefix, message information is available at the following web site:

http://pic.dhe.ibm.com/infocenter/tsminfo/v7r1/topic/com.ibm.itsm.fcm.messages.doc/fcm_common_messages.html

GVM0001E The operation failed with return code
return code

GVM0002E An internal error occurred: *type of error*

GVM0003E A connection with the Tivoli Storage Manager server could not be established.

Explanation: The server might not be running.

Administrator response: Check the network connection with the server machine. Verify that the server is running and try to log in again.

GVM0004W Are you certain that you want to delete this data?

Explanation: You cannot recover the data after it is deleted. Ensure that the data is not needed before you delete it.

Administrator response: Click OK to delete the data or click Cancel to cancel this action.

GVM0005W The connection with the Tivoli Storage Manager server has timed out.

Explanation: Possible causes include a long-running operation, a problem on the server, or a communications problem.

Administrator response: If the operation is long-running, the operation might be complete or it might soon be complete. Before trying the operation again, determine if the expected result occurred. Check the activity log of the Tivoli Manager server for errors related to the operation. Using a SSL port without selecting SSL can cause this error.

GVM0006I A server connection with the name
server name has been successfully created. Click OK to continue.

GVM0007W There is no Tivoli Storage Manager server definition found.

Explanation: A connection for a Tivoli Storage Manager server must be defined before any server operations or queries are performed.

Administrator response: To define a server: Click the Configuration tab. Click the Edit Configuration Settings action link. Click the Tivoli Storage Manager Server Credentials tab.

GVM0008E An error occurred while writing to the server's database file, *tsmsrvr.props*

Explanation: The server definition could not be written to the *tsmsrvr.props* file.

Administrator response: The file must reside in the install directory of Tivoli Data Protection for VMware. Before you try the action again, verify that the file exists and that the file is not write protected.

GVM0011I The VM *VM name* is spanned into multiple datastores. It can only be restored to its original location.

GVM0011W The VM *VM name* exists, are you going to over-write it?

GVM0012W The VM *VM name* is running, make sure the system is powered down, then hit OK to continue.

GVM0020E A connection with the vCenter server could not be established.

Explanation: The server might not be running.

Administrator response: This might indicate a network problem. Ensure that the server is running and the machine is accessible. Try the action again.

GVM0021I A connection with the vCenter server has been established.

GVM0022E The VMCLI inquire configuration command failed, the following messages describe the error.

Explanation: The Derby database might not be running.

Administrator response: Correct the problem. Try the action again.

GVM0023I The VMCLI inquire configuration command completed successfully.

GVM0024E Failed to determine which product or products are installed.

Explanation: See message.

Administrator response: Correct the problem. Try the action again.

GVM0025I Successfully determined which product or products are installed.

GVM0026E Multiple restore points have been selected, but they are not located in the same datacenter.

Explanation: Selecting restore points from different datacenters is not permitted. The restore points must all be located in the same datacenter.

Administrator response: Select the restore points from the same datacenter or select just a single restore point.

GVM0027E Multiple restore points have been selected, but they are not from the same backup.

Explanation: Selecting restore points from different backups is not permitted. The restore points must all be located in the same backup.

Administrator response: For restores from Tivoli Storage FlashCopy Manager for VMware, all restore points must come from the same backup. You cannot restore multiple VMs that come from of different backups.

GVM0028E A key configuration file is missing: vmcliConfiguration.xml.

Explanation: The file vmcliConfiguration.xml is required for the GUI to operate, but has not been found during GUI session startup. This is an unusual problem, it may be due to an install issue or manual editing of the file.

Administrator response: Make sure the file is located in the correct directory, has correct access permissions, and has valid syntax for its content. Retry accessing the GUI.

GVM0029E Invalid mode tag in file vmcliConfiguration.xml.

Explanation: The xml tag mode in file vmcliConfiguration.xml is required for the GUI to operate, but is missing or has an incorrect value. This may be due to an install issue or manual editing of the file.

Administrator response: Make sure the tag is specified with a valid value. Retry accessing the GUI.

GVM0030E Invalid enable_direct_start tag in file vmcliConfiguration.xml.

Explanation: The xml tag enable_direct_start in file vmcliConfiguration.xml is required for the GUI to operate, but is missing or has an incorrect value. This may be due to an install issue or manual editing of the file.

Administrator response: Make sure the tag is specified with a valid value. Retry accessing the GUI.

GVM0031E Invalid URL tag for the specified mode tag in file vmcliConfiguration.xml.

Explanation: In file vmcliConfiguration.xml, the URL tag corresponding to the specified mode tag is required for the GUI to operate, but is missing or has an incorrect value. This may be due to an install issue or manual editing of the file.

Administrator response: Make sure the correct URL tag is specified with a valid value for the specified mode. Retry accessing the GUI.

GVM0032E Invalid VMCLIPath tag in file vmcliConfiguration.xml.

Explanation: The xml tag VMCLIPath in file vmcliConfiguration.xml is required for the GUI to operate, but is missing or has an incorrect value. This may be due to an install issue or manual editing of the file.

Administrator response: Make sure the tag is specified with a valid value. Retry accessing the GUI.

GVM0033E Invalid interruptDelay tag in file vmcliConfiguration.xml.

Explanation: The xml tag interruptDelay in file vmcliConfiguration.xml is required for the GUI to operate, but is missing or has an incorrect value. This may be due to an install issue or manual editing of the file.

Administrator response: Make sure the tag is specified with a valid value. Retry accessing the GUI.

GVM0099E The VM name entered *VM name* conflicts with an existing VM. Please enter a different name.

GVM0100E An error occurred while processing the request to the Web server. If this error persists, check the network connection with the Web server and verify that the Web server is running.Detail: *exception exception message*

GVM0101E A request to the server took too long to complete. If this error persists, check the network connection with the Web server and verify that the Web server is running.

GVM0102E An error occurred while processing the response from the Web server.Detail: *error*

GVM0103E An error occurred while making the Web server request. If this error persists, check the network connection with the Web server and verify that the Web server is running.Error: *message*

GVM0104E No matching device class found. Please return to source page and reselect.

GVM0105E No matching proxy node found. Please return to source page and reselect.

GVM0106E No proxy ESX hosts available.

GVM0107I Password set successfully.

GVM0108E Set password failed.Error: *message*

Explanation: The password may be incorrect or the server is not running.

Administrator response: Verify the password is correct then try the action again. Or check the network connection with the server machine and verify that the

server is running then try the action again.

GVM0109E Get managed domain failed.Error: *message*

GVM0110E Multiple restore points have been selected, but they are not the same backup type.

Explanation: Selecting restore points of different types is not allowed. The restore points must all be located on either a Tivoli Storage Manager server or in the Tivoli FlashCopy Manager repository.

Administrator response: Select the same type of restore points or select just a single restore point.

GVM0111E Backup ID is null.

Explanation: An internal error occurred.

Administrator response: Refresh the table and perform the action again.

GVM0112E Task ID is null.

Explanation: An internal error occurred.

Administrator response: Refresh the table and perform the action again.

GVM0113E Could not open a pop-up window.

Explanation: An internal error occurred.

Administrator response: Try the action again.

GVM0114E Virtual machine name is null.

Explanation: An internal error occurred.

Administrator response: Refresh the table and perform the action again.

GVM0115E Datastore does not exist.

Explanation: An internal error occurred.

Administrator response: Refresh the table and perform the action again.

GVM0116I No selection was made, the whole virtual machine will be attached.

Explanation: No selection was made.

Administrator response: Continue with the action or cancel the action.

GVM0117I Domain set successfully.

GVM0118E Set domain failed.**Error:** *message*

Explanation: The server might not be running. The permissions on the file directory may be incorrect.

Administrator response: Check the network connection with the server machine. Verify that the server is running and try the action again. Check the permissions of the directory indicated in SystemErr.log if error indicates incorrect permissions.

GVM0119E The schedule requires use of the following datacenters that are not in the active domain. Datacenters: *list* **Action:** This schedule may not be updated, instead either update the domain construct to include the datacenters, or create a new schedule without dependence on these datacenters. **Detail:** The schedule definition is as follows: Schedule Summary *summary*

GVM0120E The schedule requires use of the following datacenters that are not known to the system. Datacenters: *list* **Action:** This schedule may not be updated, instead create a new schedule without dependence on these datacenters. **Detail:** The schedule definition is as follows: Schedule Summary: *summary*

GVM0121E The schedule requires use of the following hosts that are not known to the system. Hosts: *list* **Action:** This schedule may not be updated, instead create a new schedule without dependence on these hosts. **Detail:** The schedule definition is as follows: Schedule Summary: *summary*

GVM0122E The schedule requires use of the following datastores that are not known to the system. Datastores: *list* **Action:** This schedule may not be updated, instead create a new schedule without dependence on these datastores. **Detail:** The schedule definition is as follows: Schedule Summary: *summary*

GVM0123E The schedule requires use of the following virtual machines that are not known to the system. Virtual Machines: *list* **Action:** This schedule may not be updated, instead create a new schedule without dependence on these virtual machines. **Detail:** The schedule definition is as follows: Schedule Summary: *summary*

GVM0124I Password set successfully. **Warning:** *message*

Explanation: The password was set successfully with a warning.

Administrator response: Follow the action described in the warning message.

GVM0125E An error occurred while making the Web server request. If this error persists, check the network connection with the Web server and verify that the Web server is running. **Error:** *error*

GVM1100E The following command requires confirmation from the server: *Command*

Explanation: A command was issued, and a reply was expected. Some commands require a confirmation, which you cannot issue through the Tivoli Data Protection for VMware GUI.

Administrator response: Issue the command from the command line.

GVM1101E The following command is unknown to the server: *Command*

Explanation: An unknown command was issued to the server. The command might not be valid on the server version and platform or the command syntax might be incorrect.

Administrator response: Verify that the command is valid for the server version and platform, and verify that the command syntax is correct.

GVM1102E The syntax of the following command is incorrect: *Command*.

Explanation: See message.

Administrator response: Correct the syntax and issue the command from the command line. The activity log of the Tivoli Manager Server shows all the commands issued before and after this command.

GVM1103E An internal server error occurred.

Explanation: See message.

Administrator response: Try the command again. If this does not work, contact customer support. You might be asked to provide tracing information and information about the actions performed before the failure occurred.

GVM1104E The server ran out of memory while processing the request. Close any unnecessary processes on the Tivoli Storage Manager server and try the operation again.

Explanation: See message.

Administrator response: Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1105E The database recovery log is full.

Explanation: See message.

Administrator response: Before trying the action again, extend the recovery log or back up the Tivoli Storage Manager server database. Contact the administrator of the Tivoli Storage Manager server.

GVM1106E The server database is full.

Explanation: See message.

Administrator response: Before trying the action again, extend the server database. Contact the administrator of the Tivoli Storage Manager server.

GVM1107E The server is out of storage space.

Explanation: See message.

Administrator response: Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1108E You are not authorized to perform this action. An administrator with system authority can change your authority level to allow you to perform this action.

GVM1109E The object that you are attempting to access does not exist on the server.

GVM1110E The object that you are attempting to access is currently in use by another session or process. Retry the action at a later time.

GVM1111E The object that you are attempting to remove is referenced by another object defined to the server. Remove the other object before removing this one.

GVM1112E The object that you are attempting to access or remove is not available.

Explanation: See message.

Administrator response: Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1113E The server encountered an I/O error while processing the request. For more information, see the operating system event or error log.

GVM1114E The action failed because the transaction could not be committed.

Explanation: See message.

Administrator response: Retry the action at a later time. Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1115E The action failed because of a resource lock conflict.

Explanation: See message.

Administrator response: Retry the action at a later time. Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1116E The action failed because of a mode conflict.

Explanation: See message.

Administrator response: Retry the action at a later time. Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1117E The action failed because the server could not start a new thread.

Explanation: See message.

Administrator response: Retry the action at a later time. Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1118E The server is not licensed to perform this action. If a license was purchased, use the command line to register the license.

GVM1119E The specified destination is not valid.

Explanation: See message.

Administrator response: Enter a different destination or update the configuration with a valid destination, and try the action again.

GVM1120E The specified input file cannot be opened. Verify the file name and directory permissions, then try the action again.

GVM1121E The specified output file cannot be opened. Verify the file name and directory permissions, then try the action again.

GVM1122E An error occurred while writing to the specified output file.

Explanation: See message.

Administrator response: Check the file system to ensure that there is enough space. Check the operating system event or error log for more information.

GVM1123E The specified administrator is not defined to this server.

Explanation: See message.

Administrator response: Ensure that the administrator name was entered correctly. Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1124E The SQL statement could not be processed.

Explanation: An exception occurred while processing the SQL statement. Possible exceptions include divide-by-zero, math overflow, temporary table storage space unavailable, and data-type errors.

Administrator response: Correct the SQL query and try again.

GVM1125E This operation is not allowed with this object.

Explanation: See message.

Administrator response: Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1126E The table was not found in the server database.

Explanation: See message.

Administrator response: Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1127E The specified file space name is not compatible with the filesystem type.

Explanation: Unicode file space names are incompatible with non-unicode names.

Administrator response: Enter a file space name of the correct type and try the action again.

GVM1128E The specified TCP/IP address is not valid. Verify the TCP/IP address and try the action again.

GVM1129E No objects were found that match the search conditions.

GVM1130E Your administrative ID on this server is locked. An administrator with system authority can unlock your ID.

GVM1131E The connection to the server was lost while performing the action.

Explanation: See message.

Administrator response: This might indicate a network problem. Ensure that the server is running and the machine is accessible. Retry the action.

GVM1132E Your ID or password is not valid for this server.

Explanation: See message.

Administrator response: Launch the Configuration Editor from the Configuration Tab and enter a valid ID or password for your Tivoli Storage Manager Server.

GVM1133E Your password expired on this server.

Explanation: See message.

Administrator response: Launch the Configuration Editor from the Configuration Tab and enter a valid ID or password for your Tivoli Storage Manager Server.

GVM1134E The server cannot accept new sessions. If sessions are disabled for this server, issue the `ENABLE SESSIONS` command from the command line.

GVM1135E A communications failure occurred while processing the request. Retry the action at a later time.

GVM1136E The administrative API encountered an internal error while processing the request.

GVM1137E The administrative API cannot process the command document sent from the server.

Explanation: The XML command document could not be parsed. Either the file could not be read, or the file is corrupted.

Administrator response: Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1138E The following command contains one or more invalid parameters: *command*.

Explanation: The Tivoli Data Protection for VMware GUI tried to run a command, but the call to the API contained one or more invalid parameters.

Administrator response: Check the parameters in the command. If you entered text in a field, you might find the error in the parameters and correct it. Viewing the activity log might help to determine the cause of the problem. Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1139E The administrative API encountered invalid parameters while processing the request.

Explanation: A command was run through the administrative API, but one of the parameters to an API method was invalid.

Administrator response: This is typically an internal error, but it can be caused by unusual parameters. For example, characters such as: < > & can cause the problem. Check the parameters in the command. If you entered text in a field, you might find the error in the parameters and correct it.

GVM1140E The administrator's authority level on this server cannot be determined.

Explanation: See message.

Administrator response: Use a different administrator ID. Before trying the action again, contact the administrator of the Tivoli Storage Manager server.

GVM1141E An object with the name that you specified already exists on the server. Enter a different name.

GVM1142E The version of the server is not supported by the Tivoli Data Protection for VMware GUI.

GVM1143E An internal error has occurred.

Explanation: The operation failed after encountering an internal error.

Administrator response: Retry the operation. If this does not work, contact customer support. You might be asked to provide tracing information and information about the actions performed before the failure occurred.

GVM1144E The operation failed, please go to the log for more details.

GVM1145E Wrong format of the end date and time. Please enter the end date and time format as yyyyMMddHHmmss.

GVM1146E Sorry, the description of the backup task was not created in a file. Please try again.

Explanation: On the general page of the backup wizard, you can describe your backup task in general.

GVM1147E The ESXHOST name you entered is too long. Please change to a shorter one.

GVM1148E Wrong Backup ID. Please try again.

GVM1150E An error occurred when processing the backup object file. Please try again later.

Explanation: When you click submit in the backup wizard, the object list will be stored in a file. When processing this file, an error occurred.

GVM1151E No backup object is selected. You must choose a source node to backup.

Explanation: To initiate a backup task, you have to choose an object on the source page of the backup wizard.

GVM1152E Wrong format of the start date and time. Please enter the start date and time format as yyyyMMddHHmmss.

GVM1153I	Backup task <i>Task Name</i> started, would you like to monitor this task now?
GVM1154I	Delete backup task completed successfully.
GVM1155E	Delete backup task failed, please check log for more detail.
GVM1156I	Restore Task <i>Task ID</i> is started successfully, would you like to monitor this task now?
GVM1157E	Error Or Warning
GVM1158I	Mounted backup Item could not be restored.
GVM1159I	Result of attach is <i>status</i> (Task ID: <i>Task ID</i>), refer to events list to get the details.
GVM1160I	Result of detach is <i>status</i> (Task ID: <i>Task ID</i>), refer to events list to get the details.
GVM1161I	Command successfully submitted to the Tivoli Storage Manager server. Detail: <i>Server Messages</i>
GVM1162E	The command submitted to the Tivoli Storage Manager server failed. Error: <i>Error Code Error Messages</i>
GVM1163E	No Tivoli Storage Manager server connection, please configure the Tivoli Storage Manager server in the configuration panel.
GVM1164E	The selected items can only be under ONE datacenter.
GVM1165E	Authentication failed. Could not connect to vCenter. Make sure you log in using the VMware vSphere client and have a valid session.
GVM1166E	Authentication failed. Please log in using the VMware vSphere client.

GVM1167E	The virtual machine <i>VM name</i> exists. Delete the virtual machine first before restoring it.
GVM1168E	Original virtual machine <i>VM name</i> is running. Close the virtual machine before restoring virtual disks to original location.
GVM1169E	Some of selected virtual disks exist in target virtual machine. Remove those virtual disks from target virtual machine before restoring to it.
GVM1170E	A VMCLI command failed. Error: <i>Error Messages</i>
GVM1171E	A request submitted to the VMware vCenter server failed. Error: <i>Error Messages</i>
GVM1172E	A command submitted to the Tivoli Storage Manager server failed. Error: <i>Error Messages</i>
GVM1173E	Cannot find the file with format 'summary.date.log' in the path: <i>path</i>
GVM1174E	Cannot find the Tivoli FlashCopy Manager installation path using the VMCLI inquire_config command.
GVM1175E	A VMCLI command to get version failed.
GVM1176I	Backup task <i>Task ID</i> started, would you like to monitor this task now?
GVM1177E	The Tivoli Data Protection for VMware Web Server could not be contacted.

Explanation: The Tivoli Data Protection for VMware GUI has attempted to contact its Web Server. The operation was not successful.

Administrator response: Perform one or more of the following steps to try and determine the problem: Verify that the Tivoli Data Protection for VMware Web Server is running. Verify that the Web Server machine is running. Verify that the Web Server machine is accessible over the network. Close the Tivoli Data Protection for VMware GUI. Start the GUI again when the problem is resolved.

GVM1178I Command successfully submitted to the server.

GVM1179E No host is found in datacenter *datacenter name*. Select another datacenter to restore.

GVM1180W The schedule does not contain all the required parameters. It cannot be displayed in the properties notebook.

Explanation: This schedule may have been created or modified outside of the Tivoli Data Protection for VMware GUI.

Administrator response: This schedule must be modified outside the the Tivoli Data Protection for VMware GUI.

GVM1181W One or more VMs exist. Do you want to continue the restore operation and overwrite the existing VMs?

GVM1182E The Administrator Id provided does not have sufficient privileges.

Explanation: The operation you are attempting requires a Tivoli Storage Manager Server Administrator Id to have at least Unrestricted Policy privilege.

Administrator response: Contact your Tivoli Storage Manager Server Administrator to grant you Unrestricted Policy privilege for your Administrative Id. Or, use an alternate Id with such privilege and try again.

GVM1183E The nodename *node name* is already in use. Please choose another nodename.

Explanation: The node name chosen already exists on the server. Choose another name.

Administrator response: Pick another node name to use. If you want to re-use this node, then unselect the 'Register Node' checkbox.

GVM1184E The node name *node name* is not defined on server. Make sure the node name you entered exists on the server.

Explanation: The node name entered does not exist on the server. Since you did not select 'Register Node' checkbox, the node name you enter must have been previously defined and exist on the server.

Administrator response: Check the node name you are supposed to use and enter it again. If you want to register this node, then select the 'Register Node' checkbox.

GVM1185E The passwords in the entry field and the verify field do not match. Please try again.

Explanation: The new passwords entered do not match.

Administrator response: Clear the fields and enter the same password in both password fields.

GVM1186W Please select one or more Datacenters to be managed.

Explanation: At least one Datacenter must be selected.

Administrator response: Add one or more Datacenter(s) into the Managed Datacenters list.

GVM1187W One or more nodes do not have their password set. Make sure all nodes have their password set.

Explanation: If a node has 'Register Node' checkbox set, then that node's password must be set.

Administrator response: Assign a password for nodes that are to be registered.

GVM1188I No datacenter node was found mapped to *datacenter name*. Select a datacenter node from the list to associate with *datacenter name*. Leave the selection empty to have the Configuration Wizard create a new datacenter node for it.

GVM1189I Are you sure you want to proceed without entering a Tivoli Storage Manager Administrative ID? Without Tivoli Storage Manager Administrative access, the Wizard will not validate node names or register nodes. Instead, a macro file will be generated at the end of this Wizard for you to give to your Tivoli Storage Manager Administrator to execute.

GVM1190I This task was skipped because it was not necessary or a pre-requisite task failed.

GVM1191E There was an error writing to script file: *file path*.

Explanation: An error was encountered when trying to write to file at the path indicated.

Administrator response: Try the operation again.

GVM1192I Managed datacenters have changed. Please go to the datamover page to verify or change your current mappings.

GVM1193I No datacenter nodes were found for the vCenter node *vCenter node* and VMCLI node *VMCLI node* configuration. The Wizard will generate a default set of datacenter nodes for you.

GVM1194E The password entered is not acceptable. Choose another password.

Explanation: Tivoli Storage Manager Server could not accept the password chosen. It could be because the password did not meet certain password rule(s).

Administrator response: Try with another password.

GVM1195W Unchecking this checkbox means you are supplying a node name that is already defined on the Tivoli Storage Manager Server AND that it is meant to be used for your configuration. Since this Wizard is proceeding without Administrative access, it cannot verify if the node exists or not. You should only proceed if you understand what you are doing.

Explanation: Since you are using the Configuration Wizard without a Tivoli Storage Manager Administrative ID, you should be very careful. The macro script file generated at the end of running the Configuration Wizard could contain errors because values are not validated.

Administrator response: We strongly recommend you use the Configuration Wizard with a proper Tivoli Storage Manager Administrative ID.

GVM1196W The Tivoli Storage Manager node *TSM node* has already been identified. If you want a different name other than the default name, edit this field again. If you want to use the same DataMover for multiple Datacenters, please use Configuration Settings to do this.

Explanation: The node is already being used in this configuration.

Administrator response: Try using another node name.

GVM1197W The Tivoli Storage Manager node *TSM node* has invalid characters or exceeds 64 characters. Choose a different name and edit this field again.

Explanation: The node name is invalid or longer than 64 characters.

Administrator response: Try using another node name.

GVM1198E The password entered is not acceptable on this Server because it contains invalid characters. The valid characters are: *validCharsString*

Explanation: Tivoli Storage Manager Server could not accept the password chosen because of invalid characters in the password.

Administrator response: Try with another password that only contain valid characters.

GVM1199E The password entered is not acceptable on this Server because of the reason below. Choose another password. Error: *message*

Explanation: Tivoli Storage Manager Server could not accept the password chosen. The reason why this password is not valid is given in the message.

Administrator response: Try with another password that meets the rule(s).

GVM1200E Filter has changed, select Apply filter before continuing.

Explanation: Filter pattern must be applied after it is changed.

Administrator response: Click the Apply filter button.

GVM1201E Select at least one item from a datacenter to continue.

Explanation: A host, host cluster, or VM must be selected to do a backup.

Administrator response: Select an item under a datacenter.

GVM1202E Your selections exceed the 512 character limit allowed for backups, change your selection.

Explanation: The number of characters required to list the selected items exceeds the limit of 512 characters. Also, if hosts have been partially selected, characters are needed to list the VMs that are excluded from the backup.

Administrator response: Create multiple backup tasks, with less selected items per task.

GVM1203I Changing the newly added virtual machines checkbox clears all selections of host clusters, hosts, and virtual machines. Press OK to proceed, or Cancel to leave unchanged.

Explanation: The state of the newly added virtual machines checkbox significantly impacts what is allowed to be selected on the source panel, so selections are cleared when the state changes.

Administrator response: Select OK to proceed, or select Cancel to retain all selections.

GVM1204E Datacenter node *datacenter node name* does not have a TSM node mapped in the vmcli configuration file.

Explanation: The datacenter node must have a corresponding TSM node listed in the configuration file named vmcliprofile.

Administrator response: Correct the problem by going to the Configuration tab in the GUI and selecting Edit Configuration to update the mapping for the datacenter. Also resolve any other configuration errors that are reported on the Configuration tab.

GVM1205E TSM datacenter node *datacenter node name* maps to vCenter datacenter name *datacenter name* in the vmcli configuration file, but *datacenter name* does not exist in the vCenter.

Explanation: The vCenter datacenter name maps to a datacenter node in the vmcli configuration file named vmcliprofile, but the data enter name does not exist in the vCenter.

Administrator response: Correct the problem by going to the Configuration tab in the GUI and selecting Edit Configuration to update the mapping for the datacenter. Also resolve any other configuration errors that are reported on the Configuration tab.

GVM1206E You have selected items from multiple datacenters: *datacenter list*. This is not allowed, all selections must be from one datacenter.

Explanation: A backup task only supports items from one datacenter. If this is an existing task, changes in the vCenter configuration after task creation may have caused this problem.

Administrator response: Check and correct the selections to make sure all selections are under the same datacenter.

GVM1207E The selected items *item list* are not found under datacenter *datacenter name* in the vCenter, please review and de-select them.

Explanation: Items originally selected are no longer found under the datacenter associated with the backup task. This may be caused by changes in the vCenter configuration.

Administrator response: Review if the items are now located under a different datacenter. De-select the not found items, and make new selections under the other datacenter or create a new backup task for these items.

GVM1208I The datacenter in the source page has changed, please reselect the data mover node in the Destination page.

Explanation: When item selection is changed to a different datacenter, the valid datamovers may change. You are required to select the datamover again on the Destination page.

Administrator response: Reselect the datamover node in the Destination Page.

GVM1209I Are you sure you want to use node *datamover node* as a datamover for datacenter *datacenter*?

GVM1210I Are you sure you want to use node *node name* that is already registered on the TSM server as a datamover for datacenter *datacenter*? If so, we will mark the node as such and you will be unable to make any further changes to the node.

GVM1211E The password entered is not acceptable on this Server because it is too short. Passwords must have a least *minPasswordLength* characters.

Explanation: Tivoli Storage Manager Server could not accept the password chosen because it is too short.

Administrator response: Try with another password that is longer than the required minimum length.

GVM1212E Component is downlevel, so its use is disabled in the GUI. You will only be able to use the GUI for *component*.

GVM1213E Mismatching Tivoli Storage Manager Server entries in the current settings is detected. Tivoli Storage Manager Server definition used by the GUI: *server1* Tivoli Storage Manager Server where backups are stored: *server2* Click Reset Server definition to clear the Tivoli Storage Manager definition and enter new credentials. Or click on Reconfigure Environment to launch the Configuration Wizard to reconfigure your Tivoli Data Protection for VMware environment.

Explanation: Tivoli Storage Manager detected mismatching Tivoli Storage Manager Server entries between the vmclprofile and the current GUI's Tivoli Storage Manager Server connection.

Administrator response: Pick one of the two actions available. You may either reset the Tivoli Storage Manager Server definition/credentials OR use the Configuration Wizard to set up a new environment.

GVM1214E The SSL Connection could not be made. The TSM SSL certificate is missing. Check for valid TSM certificate in the *tsm-ve-truststore.jks*

Explanation: Tivoli Storage Manager Server did not accept the SSL connection. SSL keystore is not in the default location or does not contain a TSM certificate.

Administrator response: Check the *tsm-ve-truststore.jks* for a valid certificate, ensure *tsm-ve-truststore.jks* is in the correct default location.

GVM1215E The password entered is not acceptable on this Server because it is too long. Passwords cannot have more than *maxPasswordLength* characters.

Explanation: Tivoli Storage Manager Server could not accept the password chosen because it is too long.

Administrator response: Try with another password that is shorter than the allowed maximum length.

GVM1216E The SSL Connection could not be made. The TSM SSL certificate has expired.

Explanation: Tivoli Storage Manager Server did not accept the SSL connection. The *tsm-ve-truststore.jks* has an expired TSM SSL certificate.

Administrator response: Obtain a new valid TSM SSL certificate from the TSM server and place it in the *tsm-ve-truststore.jks*.

GVM1217E The non-SSL connection could not be made. This Tivoli Storage Manager Admin ID requires a TSM SSL connection.

Explanation: Tivoli Storage Manager Server did not accept the non-SSL connection. The TSM Server requires SSL be used with this Admin ID.

Administrator response: Use SSL with this Admin ID. Ensure that the *tsm-ve-truststore.jks* with a valid TSM server SSL certificate is installed in the default location.

GVM1218E Your selections have caused the backup task definition to require *count* characters, which exceeds the 512 character limit. This can be caused by a long virtual machine exclude list, which is the list of all VMs under host(s) that were not selected. Either select more VMs under selected hosts or de-select the newly added virtual machines checkbox.

Explanation: When the newly added virtual machines checkbox is selected, the resulting backup task must list all unselected VMs for hosts that are partially selected. The backup task definition has a 512 character limit, and the combination of selected items and excluded VMs exceeds this limit.

Administrator response: De-select the newly added virtual machines checkbox or create multiple backup tasks with less selected items per task.

GVM1219E Your selection of virtual machines has caused the backup task definition to require *count* characters, which exceeds the 512 character limit. Either create multiple backup tasks with less virtual machines per task, or select the newly added virtual machines checkbox and choose entire hosts with no more than a few unselected VMs.

Explanation: The backup task definition has a 512 character limit, and the total number of characters for the selected items exceeds this limit.

Administrator response: Create multiple backup tasks with less selected virtual machines per task, or select the newly added virtual machines checkbox and then select hosts instead of individual virtual machines (you can de-select a small number of virtual machines per host if desired.)

GVM1220E There is no data mover node proxy relationship for datacenter node *datacenter node name*. Review the data mover relationships on the Configuration tab or the Tivoli Storage Manager server.

GVM1221E There is no datacenter node defined for datacenter *datacenter name*. Review the node configuration on the Configuration tab.

GVM1222I Node *name name* is currently locked. The Configuration Wizard will attempt to unlock this node if you choose to continue.

GVM1223E A connection with the Tivoli Storage Manager server (*Address:Port*) could not be established. Please verify the server address and *Server or Admin port* are correct.

Explanation: The server might not be running or specified admin port or server port may be incorrect.

Administrator response: Check the network connection with the Tivoli Storage Manager server machine. Verify that the server is running and try to log in again. Also verify server port and admin port information is correct.

GVM1224E The vCenter user name or password is not valid. Please try again.

Explanation: The vCenter user name or password is not valid.

Administrator response: Enter the user name or password again.

GVM1250I A Tivoli Storage Manager Administrative ID and password is currently not set. The absence of this information limits the actions that you can take in the GUI. Click OK to be taken to the configuration settings panel and enter an ID and password. Click Cancel to continue without using an ID and password.

GVM1251W You have chosen an Administrative ID that has less authority than the current ID. Are you sure you want change this ID? Current Tivoli Storage Manager Authority Level: *Current Level* New Tivoli Storage Manager Authority Level: *New Level* Current Role: *Current Role* New Role: *New Role* Click OK to accept these changes, or Cancel to exit without change.

GVM1252I Here are the current and new roles for Tivoli Storage Manager Admin IDs. Review and confirm these changes. Current Tivoli Storage Manager Authority Level: *Current Level* New Tivoli Storage Manager Authority Level: *New Level* Current Role: *Current Role* New Role: *New Role* Click OK to accept these changes, or Cancel to exit without change.

GVM1253I ID has been changed without save. Previous ID will be loaded.

GVM1254I Your current UI role does not allow you to unlock or reset the VMCLI node. In order to make changes, go to the Server Credentials page and enter a TSM Admin ID and password that has the necessary privileges for making VMCLI node updates. Select OK to save these credentials, then re-open the Configuration Settings notebook and you can make VMCLI node updates.

GVM1255I Your current UI role does not allow you visit other panels. Select OK to save these credentials, then re-open the Configuration Settings notebook and you can make other updates.

GVM1256I There are non-English characters contained in one or more datacenters. The domain will be adjusted accordingly.

GVM1257E Datacenter *DataCenter Name* cannot be added to the domain because it contains non-English characters.

Explanation: Datacenters that contain non-English characters are not currently supported. Therefore, they cannot be added to the domain.

Administrator response: Datacenter will not be added to the domain.

GVM1258W Node *Node Name* already exists on the server. Attempt to rename node to *New Node Name*?

Explanation: Node name is already registered on the Tivoli Storage Manager server.

Administrator response: Click Yes to attempt to rename node. Click No to make other changes. Example: unclick register node, rename node manually.

GVM1259W The following virtual machines for host *Host Name* have unsupported characters in their name: *Invalid Virtual Machine Names*. Therefore, these virtual machines are not backed up, regardless of your selections. You must rename these virtual machines to back them up.

Explanation: The following characters are not supported in virtual machine names: ' : ; * ? , < > / \ |

Administrator response: Rename the identified virtual machines to remove unsupported characters from their name.

GVM1260E The following host clusters have unsupported characters in their name: *Invalid Host Clusters*. These host clusters cannot be selected for backup because they contain unsupported characters. Rename these host clusters or remove them from selection.

Explanation: The following characters are not supported in host cluster names: ' : ; * ? , < > / \ |

Administrator response: Rename the identified host clusters to remove unsupported characters from their name. Or, remove them from your backup selection.

GVM1261E Your selections created an empty virtual machine list for backup. This issue might occur because all the selected virtual machines contain unsupported characters in their names. Make sure that you selected virtual machines that do not contain unsupported characters in their names.

Explanation: The following characters are not supported in virtual machine names: ' : ; * ? , < > / \ | . Virtual machine names that contain these characters are automatically removed from the backup task definition. This removal can cause an empty task definition.

Administrator response: Rename the identified virtual machines to remove unsupported characters from their name. Or, select different virtual machines to back up.

GVM1262E The filter pattern cannot be applied because it contains unsupported characters. Change the pattern to remove the unsupported characters, then apply the filter again.

Explanation: The following characters are not supported in filter pattern: ' : ; < > / \ |

Administrator response: Change the filter pattern to remove unsupported characters, then apply the filter again.

GVM1263E A temporary datastore is not available to perform this operation. This temporary datastore is required in addition to the restore destination datastore.

Explanation: A datastore is required for use as a temporary restore destination for this operation. This temporary datastore must be from the same ESX host as the datastore that is used for the actual restore destination. However, the temporary datastore cannot be the same datastore that is used for the actual restore destination.

Administrator response: Add a datastore to the destination ESX host. Then, select this datastore as the temporary restore destination.

GVM1264E There was an error creating opt file: *file name*.

Explanation: An error was encountered when trying to write to file.

Administrator response: Try the operation again.

GVM1265E Creating *service* has failed. No services were created for datamover node *node name*.

Explanation: An error was encountered when trying to create TSM service for datamover node specified.

Administrator response: Check environment and ensure user has proper rights before trying operation again.

GVM1266E Creating firewall for *service* has failed. Please manually add firewall rules for services installed.

Explanation: An error has occurred when attempting to add firewall rule for specified executable.

Administrator response: Check environment and ensure user has proper rights before trying operation again or manually add rule to firewall for TSM CAD, TSM Agent and TSM Scheduler.

GVM1267W Local services were setup successfully but were unable to verify firewall access for these executable files: *agentExe cadExe schedExe* If any problems are experienced related to local services, verify that firewall access is available for these executable files.

Explanation: Microsoft firewall may be disabled or another firewall may be in place.

Administrator response: Check environment and add rules manually if needed for the TSM CAD, TSM Agent, and TSM Scheduler.

GVM1268E Datamover node *node name* was successfully registered on the server, however no services were created.

Explanation: An error has occurred when trying to create services for specified node.

Administrator response: Check environment and ensure user has proper rights before trying operation again.

GVM1269E Reason Code *reason* This error was reported by the TSM data mover. No further description is available. For more information, review the error log *errorLog* on the data mover host machine *hostname* at address '*address*'.

Explanation: The datamover encountered an error with the reported reason code.

Administrator response: Log into the host machine specified and view the error log for more information.

GVM1270W Warning: If this task is canceled, all created data on the virtual machines that are not completely restored is lost and the virtual machines are removed from the ESX host. Are you sure that you want to cancel this task?

Explanation: A cancel task command is submitted. Refresh to see the cancel progress.

Administrator response: Cancel the selected task or allow the task to continue processing.

GVM1271W Scan schedule *schedule name* was successfully defined on the server and associated with node *node name*, however no services were created to run the schedule. Detail: *error*

Explanation: An error was encountered in one of the steps below when trying to create Tivoli Storage Manager services for the VMCLI node. Create the option file for the VMCLI node. Set the password for the VMCLI node to a temporary password for the next step. Run the Tivoli Storage Manager Client Service Configuration Utility to create the services. Run the Tivoli Storage Manager Client Service Configuration Utility to start the CAD service. Reset the VMCLI node password.

Administrator response: Delete the schedule and create the schedule again to automatically configure the services or manually configure the services. Check environment and ensure user has proper rights before trying operation again.

GVM1272W Scan schedule *schedule name* was successfully defined on the server and associated with node *node name*. Tivoli Storage Manager services were created to run the schedule. However, resetting the VMCLI node password failed. Detail: *error*

Explanation: An error was encountered while trying to reset the VMCLI node password.

Administrator response: Use the Configuration Settings to reset the VMCLI node password.

GVM1273W A dismount operation removes the iSCSI disks but does not remove the VM or its data. Before proceeding with dismount, make sure the following conditions exist: -The mounted iSCSI disk is recovered. -Storage vMotion completed migrating the VM to a local datastore. If the recovery operation failed and you want to delete the VM, its data, and dismount any iSCSI targets, click Dismount and Delete. Dismount and Delete is a destructive action and deletes the VM and its data, regardless of the success or failure of the instant restore operation. Based on this information, do you want dismount the VMs that are selected for instant restore?

Explanation: A dismount operation removes the iSCSI disks but does not remove the VM or its data. Before proceeding with dismount, make sure the following conditions exist: The mounted iSCSI disk is recovered, Storage vMotion completed migrating the VM to a local datastore. If the recovery operation failed and you want to delete the VM, its data, and dismount any iSCSI targets, click Dismount and Delete. Dismount and Delete is a destructive action and deletes the VM and its data, regardless of the success or failure of the instant restore operation.

Administrator response: Click 'Dismount' to dismount the virtual machines that are selected for the instant restore operation. Click 'Dismount and Delete' to dismount the virtual machines that are selected for the instant restore operation, remove them from the ESX host, and verify that Storage vMotion is not running.

GVM1274W During a dismount operation, all created data on the virtual machines is lost and the virtual machines are removed from the ESX host. Dismount the selected Instant Access virtual machines?

Explanation: All created data on the virtual machines is lost and the virtual machines are removed from the ESX host.

Administrator response: Click 'Dismount' to dismount (cleanup) the instant access virtual machines.

GVM1275E Selecting multiple virtual machines with different restore types is not allowed.

Explanation: Restoring multiple virtual machines with different restore types is not supported.

Administrator response: Select virtual machines that have the same restore type.

GVM1276I Cleanup Task *Task ID* is started successfully, would you like to monitor this task now?

GVM1277W Are you sure that you want to cancel this task?

Explanation: A cancel task command is submitted. Refresh to see the cancel progress.

Administrator response: Cancel the selected task or allow the task to continue processing.

GVM1278I Your current UI role does not allow you to view backup property notebook.

GVM1279I Your current UI role does not allow you to edit nodes. In order to make changes, open the Configuration Settings notebook and go to the Server Credentials page and enter a TSM Admin ID and password that has the necessary privileges for making node updates.

GVM1280E Reason Code *reason* This error was reported by the TSM data mover. No further description is available. For more information, review the error log 'dsmerror.log' on the data mover host machine.

Explanation: The datamover encountered an error with the reported reason code.

Administrator response: Log into the host machine where datamover resides and view the error log for more information.

GVM1281W Login information for vCenter needed.

Explanation: In order to install new local dm services, vCenter credentials are needed.

Administrator response: Enter vCenter credentials in order to continue.

GVM1282E You do not have the privileges required to access the GUI.

Explanation: In order to access GUI content, the user must have the necessary vSphere privileges.

Administrator response: Add the required privileges for the user.

GVM1283E You do not have the permissions required to access the GUI.

Explanation: In order to access GUI content, the user must have the necessary vSphere permissions.

Administrator response: Add the required permissions for the user.

GVM1500E You have selected organization VDCs from more than one provider VDC. For backup tasks, all selected organization VDCs must belong to the same provider VDC. Change your selections and retry the operation.

GVM1501E The following vcloud resources(vApp, organization, organization vDC) are invalid for selection because they have unsupported characters in their name:
reslist

Explanation: In order to create backup tasks, vcloud resources names must not contain any of the following characters: ' : ; * ? , < > / \ | .

Administrator response: Rename the identified resources to remove unsupported characters from their name. Or, remove them from your backup selection.

GVM1502E You have selected the vApp from a different organization VDC. For restore tasks, all selected vApps must belong to the same organization VDC. Change your selections and retry the operation.

GVM1503E The vApp *vApp name* exists. Choose a different vApp name to be the target of the restore.

GVM2001E Your selection of items to back up has caused the backup task definition to require *count* characters, which exceeds the 512 character limit. Please create multiple backup tasks with less items per task.

Explanation: The backup task definition has a 512 character limit, and the total number of characters for the selected items exceeds this limit.

Administrator response: Create multiple backup tasks with less items per task

GVM2002E The Organization VDC node can not be included because its Provider VDC node is not included. Please select the include checkbox for the Provider VDC node first, and try again.

GVM2004E The nodename *node name* is already in use. Please uncheck the register node checkbox or choose another nodename.

Explanation: The node name chosen already exists on the server. Either choose to not register it or use another name.

Administrator response: Pick another node name to use. If you want to re-use this existing node, then unselect the 'Register Node' checkbox.

GVM2005W Are you certain that you want to remove the data mover node *node name*?

GVM2006W The Tivoli Storage Manager node *TSM node* has already been used. If you want a different name other than the default name, edit this field again.

Explanation: The node is already being used in this configuration.

Administrator response: Try using another node name.

GVM2007E The Organization VDC node can not be registered because its provider VDC is not valid.

GVM2008E The Organization VDC name *OVDC name* is invalid. For information about supported characters, refer to the TSM Administrator's Reference publication section about naming Tivoli Storage Manager objects.

GVM2009I This task was skipped because it was not necessary. No further action is required.

GVM2010W Internet explorer version *version* is not supported, please use a supported version or another browser. You may see visual and functional issues if you continue to use this unsupported browser.

Explanation: Due to differences in Internet Explorer implementation by version number, only specific

versions are supported. The use of a standards-compliant browser such as Mozilla Firefox is recommended. However, if you are accessing the GUI as a plug-in from the vSphere Client, you are limited to using the Internet Explorer browser installed on the system where the vSphere client is installed.

Administrator response: Use a supported version of Internet Explorer or another browser. Supported browser versions are documented in the online help.

GVM2011W The browser *version* is not supported, please use a supported browser. You may see visual and functional issues if you continue to use this unsupported browser.

Explanation: Due to differences in browser implementations, only specific versions are supported.

Administrator response: Use a supported browser. Supported browser versions are documented in the online help.

GVM2012W Targer datastore not found, select a different destination datastore.

GVM4001E This action cannot be performed because there is not a VMCLI node defined. To resolve, use the configuration wizard to define the VMCLI node and complete the other steps in the wizard.

GVM4002E This action cannot be performed because there is not a vCloud Director node defined. To resolve, use the configuration wizard to define the vCloud Director node and complete the other steps in the wizard.

GVM4003E This action cannot be performed because the connection to the TSM Server is not operational. Correct the connection problem, and retry this action.

GVM4004E This task requires use of the provider VDC node *provider VDC node name* from TSM, but this node is not mapped to a known provider VDC in the vCloud Director. This task may not be updated, instead create a new task without dependence on this provider VDC.

GVM4005E The Organization VDCs listed below were selected but are not configured to the TSM server. You must remove these selections in order to execute this action.
org VDC name

GVM4006I

GVM4006I Your current UI role does not allow you
to view node details.

Appendix C. Data Protection for VMware Recovery Agent messages

This information contains explanations and suggested actions for messages issued by the Data Protection for VMware Recovery Agent.

FBP0001E The Recovery Agent is already running.

Explanation: This issue is encountered when multiple users are logged on to the system and attempting to run the Recovery Agent. Only one active Recovery Agent instance is supported.

System action: The Recovery Agent was not started.

User response: To resolve this issue, close the current Recovery Agent instance or start the Recovery Agent on a different system.

FBP0002E The Tivoli Storage Manager server connection cannot be removed.

Explanation: There are currently active instant restore sessions or mounted volumes that require the connection to the Tivoli Storage Manager server. As a result, the existing connection cannot be removed.

System action: The remove connection operation is canceled.

User response: To resolve this issue, wait until the instant restore sessions complete. Or, forcibly end the instant restore sessions or mounted volumes and then disconnect the Tivoli Storage Manager server.

FBP0003E 'Authentication node' and 'Target node' cannot specify the same node.

Explanation: Three node authentication methods are available to access snapshots on the Tivoli Storage Manager server: 'Asnodename' authenticates with a proxy node, 'Fromnode' authenticates with a node that contains limited access, and 'Direct' authenticates directly. When 'Fromnode' or 'Asnodename' are selected, a target node must be specified. The target node is the Tivoli Storage Manager node where the virtual machine backups are located.

System action: The system waits for a user response.

User response: Specify the correct 'Authentication node' and 'Target node'. See information about the node authentication methods in the product documentation.

FBP0004E Recovery Agent failed to mount.

Explanation: The mount operation on the Windows Recovery Agent proxy host failed.

System action: The operation is canceled.

User response: Check the Windows Recovery Agent proxy host logs for information about why the mount operation failed.

FBP0005E RAID mirror status was not obtained.

Explanation: During the instant restore session, the Recovery Agent failed to obtain the status of the mdadm mirror device.

System action: An attempt to recover the instant restore session is being made.

User response: Check the instant restore status in the Recovery Agent GUI and the Recovery Agent engine logs for solutions to this problem.

FBP0006E Incorrect parameters were specified during the Recovery Agent mount operation.

Explanation: The mount operation on the Windows Recovery Agent proxy host failed because incorrect parameters were specified.

System action: The operation is canceled.

User response: Check the Windows Recovery Agent proxy host logs for information about why the mount operation failed.

FBP0007E The selected snapshot is already mounted.

Explanation: The Windows Recovery Agent proxy host identified the selected snapshot as already mounted to the requested target.

System action: None.

User response: The instant restore session or mounted snapshot is available for use.

FBP0010E Failed to dismount.

Explanation: The dismount operation on the Windows Recovery Agent proxy host failed.

System action: The operation is canceled.

User response: Check the Windows Recovery Agent proxy host logs for information about why the dismount operation failed.

FBP0011E The node data was not retrieved.

Explanation: The Windows Recovery Agent proxy host failed to retrieve the node data when querying the Tivoli Storage Manager server.

System action: The operation is canceled.

User response: Check the Windows Recovery Agent proxy host logs for information about why the querying operation failed.

FBP0012E Tivoli Storage Manager server snapshots were not found.

Explanation: The Windows Recovery Agent proxy host failed to expose the snapshots on the specified Tivoli Storage Manager server.

System action: The operation is canceled.

User response: Verify that the correct Tivoli Storage Manager server and node that own the snapshots are specified.

FBP0013E The snapshot was not found. Click 'Refresh'.

Explanation: The selected snapshot was not found on the Tivoli Storage Manager server.

System action: The operation is canceled.

User response: Click Refresh in the Recovery Agent GUI to load the current snapshots on the Tivoli Storage Manager server.

FBP0016E Invalid parameters were specified.

Explanation: The mount operation on the Windows Recovery Agent proxy host failed.

System action: The operation is canceled.

User response: Check the Windows Recovery Agent proxy host logs for information about why the mount operation failed.

FBP0017E The mdadm version is not supported.

Explanation: The installed version of the mdadm utility on the Linux machine is not supported.

System action: The operation is canceled.

User response: Upgrade the mdadm utility on your Recovery Agent Linux machine to a supported version. See which versions are supported in the Tivoli Storage Manager for Virtual Environments All Requirements Document at <http://www.ibm.com/support/docview.wss?uid=swg21505139>.

FBP0018E The mdadm utility was not found.

Explanation: The mdadm utility is not installed on the Linux machine.

System action: The operation is canceled.

User response: Install the mdadm utility on your Recovery Agent Linux machine. See which versions are supported in the Tivoli Storage Manager for Virtual Environments All Requirements Document at <http://www.ibm.com/support/docview.wss?uid=swg21505139>.

FBP0019E The iscsiadm version is not supported.

Explanation: The installed version of the iscsiadm utility (for Recovery Agent on RedHat Linux machines) or open-iscsi (for Recovery Agent on SUSE Linux machines) is not supported.

System action: The operation is canceled.

User response: Upgrade the iscsiadm or open-iscsi utility on your Recovery Agent Linux machine to a supported version. See which versions are supported in the Tivoli Storage Manager for Virtual Environments All Requirements Document at <http://www.ibm.com/support/docview.wss?uid=swg21505139>.

FBP0020E The iscsiadm utility was not found.

Explanation: The iscsiadm utility is not installed on the Linux machine.

System action: The operation is canceled.

User response: Install the iscsiadm utility on your Recovery Agent Linux machine. See which versions are supported in the Tivoli Storage Manager for Virtual Environments All Requirements Document at <http://www.ibm.com/support/docview.wss?uid=swg21505139>.

FBP0021E The lsscsi version is not supported.

Explanation: The installed version of the lsscsi utility is not supported.

System action: The operation is canceled.

User response: Upgrade the lsscsi utility on your Recovery Agent Linux machine to a supported version. See which versions are supported in the Tivoli Storage Manager for Virtual Environments All Requirements Document at <http://www.ibm.com/support/docview.wss?uid=swg21505139>.

FBP0022E The lsscsi utility was not found.

Explanation: The lsscsi utility is not installed on the Linux machine.

System action: The operation is canceled.

User response: Install the lsscsi utility on your Recovery Agent Linux machine. See which versions are supported in the Tivoli Storage Manager for Virtual Environments All Requirements Document at <http://www.ibm.com/support/docview.wss?uid=swg21505139>.

FBP0023E The Secure Shell (SSH) version is not supported.

Explanation: The installed version of the SSH client is not supported.

System action: The operation is canceled.

User response: Upgrade the SSH client on your Recovery Agent Linux machine to a supported version. See which versions are supported in the Tivoli Storage Manager for Virtual Environments All Requirements Document at <http://www.ibm.com/support/docview.wss?uid=swg21505139>.

FBP0024E The Secure Shell (SSH) was not found.

Explanation: The SSH client is not installed on the Linux machine.

System action: The operation is canceled.

User response: Install the SSH client on your Recovery Agent Linux machine. See which versions are supported in the Tivoli Storage Manager for Virtual Environments All Requirements Document at <http://www.ibm.com/support/docview.wss?uid=swg21505139>.

FBP0025E Not all instant restore sessions were stopped.

Explanation: The Recovery Agent was unable to stop all instant restore sessions.

System action: Some of the instant restore sessions are still visible in the Recovery Agent 'Instant Restore' panel.

User response: Try stopping the instant restore sessions one after the other. If the problem persists, check the Linux Recovery Agent engine log file. This file is usually located at `/opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf`. Also check the Windows Recovery Agent proxy host logs for any errors related to this issue.

FBP0026E Failed to read instant restore session.

Explanation: The Recovery Agent was unable to read the instant restore status file.

System action: Information about the instant restore is not available.

User response: Try restarting the instant restore

session. If the problem persists, check the Linux system log (usually located at `/var/log/messages`) for any errors related to this issue.

FBP0027E Mount session already exists.

Explanation: The selected snapshot is already mounted to the requested target.

System action: None.

User response: The instant restore session or mounted snapshot is available for use.

FBP0028E Failed to create the mount sessions directory.

Explanation: The Recovery Agent was unable to create the directory for the mount operation.

System action: The operation is canceled.

User response: Try the mount operation again. If the problem persists, check the Linux system log (usually located at `/var/log/messages`) for any errors related to this issue.

FBP0029E Failed to encrypt node credentials.

Explanation: The Recovery Agent was unable to encrypt the node credentials.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at `/var/log/messages`) for any errors related to this issue.

FBP0030E Failed to decrypt node credentials.

Explanation: The Recovery Agent was unable to decrypt the node credentials.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at `/var/log/messages`) for any errors related to this issue.

FBP0031E Failed to remove mount session.

Explanation: The Recovery agent was unable to delete the mount status file.

System action: The mounted snapshot remain in the Recovery Agent 'Mounted Volumes' panel.

User response: Try unmounting the mounted snapshot again. If the problem persists, check the Linux Recovery Agent engine log file. This file is usually located at `/opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf` for more information. Also check the Linux system log (usually located at `/var/log/messages`) for any errors related to this issue.

FBP0032E Instant restore session already exists.

Explanation: A similar instant restore session already exists or a similar instant restore status file exists.

System action: The new instant restore session is canceled.

User response: Check the Linux Recovery Agent engine log file for more information. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf.

FBP0033E Failed to create the instant restore sessions directory.

Explanation: The Recovery Agent was unable to create the directory for the instant restore operation.

System action: The instant restore operation is canceled.

User response: Try the instant restore operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0034E Failed to remove the instant restore session.

Explanation: The Recovery Agent was unable to delete the instant restore status file.

System action: The instant restore session remains in the Recovery Agent 'Instant Restore' panel.

User response: Try stopping the instant restore session again. If the problem persists, check the Linux Recovery Agent engine log file. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf for more information. Also check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0035E Failed to read from the configuration file that is used for mount and instant restore operations.

Explanation: The Recovery Agent was unable to read the configuration file.

System action: Information about the mount or instant restore is not available.

User response: Try the operation again. If the problem persists check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0036E Failed to write to the configuration file that is used for mount and instant restore operations.

Explanation: The Recovery Agent was unable to write to the configuration file.

System action: Information about the mount or instant restore is not available.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0037E Failed to read from the configuration file section that is used for mount and instant restore operations.

Explanation: The Recovery Agent was unable to read the configuration file.

System action: Information about the mount or instant restore is not available.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0038E Failed to write to the configuration file section that is used for mount and instant restore operations.

Explanation: The Recovery Agent was unable to write to the configuration file.

System action: Information about the mount or instant restore is not available.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0039E Failed to unmount. Device is busy.

Explanation: The Recovery Agent was not able to unmount the file system of the selected mounted snapshot because the file system is in use.

System action: The unmount operation is canceled.

User response: Close any application that might be accessing this volume. Then, try the operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0040E Not all mount sessions were unmounted.

Explanation: The Recovery Agent did not unmount all mounted snapshots.

System action: Some of the mounted snapshots sessions are still visible in the Recovery Agent 'Mounted Volumes' panel.

User response: Try to unmount the mounted snapshots one after the other. If the problem persists check the Linux Recovery Agent engine log file. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf.

FBP0041E Failed to retrieve data from the Recovery Agent CLI.

Explanation: The Recovery Agent was unable to read the Recovery Agent CLI (TDPVMwareShell) output file.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0042E Failed to parse data from the Recovery Agent CLI.

Explanation: The Recovery Agent was unable to parse the data from the Recovery Agent CLI (TDPVMwareShell) output file.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux Recovery Agent engine log file. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf.

FBP0043E Failed to create query for the Recovery Agent CLI.

Explanation: The Recovery Agent was unable to create the Recovery Agent CLI (TDPVMwareShell) output file.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0044E Failed to retrieve mount data from the Recovery Agent CLI.

Explanation: The Recovery Agent was unable to create the Recovery Agent CLI (TDPVMwareShell) output file.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0046E Failed to connect to the Recovery Agent CLI.

Explanation: The Linux Recovery Agent was unable to retrieve the Recovery Agent CLI (TDPVMwareShell)

installation path from the registry on the Windows machine.

System action: The operation is canceled.

User response: Check the connectivity to the Windows machine, verify that the SSH is configured correctly, and that the user defined on Cygwin has administrative privileges. For more information, see the product documentation.

FBP0047E Failed to create the mount directory.

Explanation: The Recovery Agent was unable to locate or create the directory for the mount operation.

System action: The mount operation is canceled.

User response: Try the mount operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0048E Failed to mount the file system of the snapshot.

Explanation: The Recovery Agent succeeded connecting to the mounted snapshot iSCSI device. However, the Recovery Agent was unable to mount the file system of the snapshot.

System action: The mount operation failed. The Recovery Agent automatically attempts to mount the file system every 5 minutes.

User response: Since the mounted snapshot is available as an iSCSI device, attempt to mount the file system of the device. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0049E Failed to set the SSH server address.

Explanation: The Recovery Agent was unable to set the SSH server address. The specified server address might be incorrect.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux Recovery Agent engine log file for more information. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf.

FBP0050E Failed to set SSH user name.

Explanation: The Recovery Agent cannot access the Windows Recovery Agent CLI (TDPVMwareShell) using the defined 'SSH login' user.

System action: The operation is canceled.

User response: Using Secure Shell verify that you can connect to the Windows Recovery Agent CLI machine

using the user defined under 'Settings'>'SSH login'.

FBP0053E Failed to send query to the Recovery Agent CLI.

Explanation: While using SSH, the Recovery Agent failed to send an input command file to the Windows Recovery Agent CLI (TDPVMwareShell). This issue might be caused by an SSH user without read and write privileges on the Windows Recovery Agent CLI machine.

System action: The operation is canceled.

User response: Verify that the SSH user defined under 'Settings'>'SSH login' has read and write privileges on the Windows Recovery Agent CLI machine. Also check the Linux Recovery Agent engine log file for more information. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf.

FBP0056E Failed to locate the block device specified for the mount point.

Explanation: The Recovery Agent failed to locate the block device for the mount point that was specified for the instant restore operation.

System action: The instant restore operation is canceled.

User response: Verify that the mount point specified for the instant restore operation is correct.

FBP0057E Failed to locate the mount point for the specified block device.

Explanation: The Recovery Agent failed to locate the mount point for the specified instant restore block device.

System action: The instant restore operation is canceled.

User response: Verify that the specified block device for the instant restore operation is correct and mounted.

FBP0058E The specified mount point is not mounted on the block device.

Explanation: The specified mount point is not mounted on the specified block device.

System action: The instant restore operation is canceled.

User response: Verify that the specified mount point and block device are correct, and that the mount point is mounted on that block device.

FBP0059E Restore is not allowed to '/' or '/boot'.

Explanation: The Recovery Agent does not support instant restore operations to target devices that are '/' or '/boot' volumes.

System action: The instant restore operation is canceled.

User response: Specify a different target device for the instant restore operation.

FBP0060E Restore is not allowed to RAID devices.

Explanation: The Recovery Agent does not support instant restore operations to RAID devices.

System action: The instant restore operation is canceled.

User response: Specify a different target device for the instant restore operation.

FBP0061E The restore operation failed to start.

Explanation: The Recovery Agent failed to start the instant restore operation.

System action: The instant restore operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux Recovery Agent engine log file for more information. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf.

FBP0062E Failed to get the iSCSI initiator name.

Explanation: No iSCSI initiator was specified.

System action: The operation is canceled.

User response: Verify that the iSCSI initiator name is specified correctly.

FBP0064E Failed to resolve the IP address to a hostname.

Explanation: The Recovery Agent failed to associate a hostname with the specified IP address.

System action: The operation is canceled.

User response: Verify that the IP or hostname are correct. Then, try the operation again. If the problem persists, check the Linux Recovery Agent engine log file for more information. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf.

FBP0065E The iSCSI service was not found.

Explanation: The iSCSI daemon is not installed on the Recovery Agent Linux machine.

System action: The operation is canceled.

User response: Install the required iSCSI daemon on the Recovery Agent Linux machine. See information about related iSCSI tasks in the product documentation.

FBP0066E Failed to start the iSCSI daemon.

Explanation: The Recovery Agent was unable to start the iSCSI daemon.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0067E Failed to discover iSCSI targets.

Explanation: The Recovery Agent was unable to discover the iSCSI targets.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0068E Failed to log in to the iSCSI target.

Explanation: The Recovery Agent was unable to log in to the iSCSI target.

System action: The operation is canceled.

User response: Check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0069E Failed to log out of the iSCSI target.

Explanation: The Recovery Agent was unable to log out of the iSCSI target.

System action: The operation is canceled.

User response: Check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0070E Failed to delete the iSCSI target.

Explanation: The Recovery Agent was unable to delete the iSCSI target.

System action: The operation is canceled.

User response: Check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0071E Failed to identify the block device for the iSCSI target.

Explanation: The Recovery Agent successfully logged in to the iSCSI target; however, the iSCSI block device was not found.

System action: The operation is canceled.

User response: Check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0072E Failed to create the RAID mirror device.

Explanation: The Recovery Agent was unable to create the RAID mirror device using the mdadm utility.

System action: The instant restore operation is canceled.

User response: Check the Linux system log (usually located at /var/log/messages) for any errors related to this issue.

FBP0073E Failed to stop the RAID mirror device.

Explanation: The Recovery Agent uses the mdadm utility to stop the RAID mirror device. However, the Recovery Agent was unable to stop the RAID mirror device.

System action: The instant restore operation is canceled.

User response: Check the Recovery Agent engine log file on the Linux machine for more details about why the device did not stop. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf. Also check the Linux system log (usually located at /var/log/messages).

FBP0074E Failed to add the target block device to the RAID mirror.

Explanation: The Recovery Agent uses the mdadm utility to add the target block device to the RAID mirror. However, the Recovery Agent was unable to add the target block device to the RAID mirror.

System action: The instant restore operation is canceled.

User response: Check the Recovery Agent engine log file on the Linux machine for more details about why the device was unable to add the target block device to the RAID mirror. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf. Also check the Linux system log (usually located at /var/log/messages).

FBP0075E Failed to mark the target block device in RAID mirror as faulty.

Explanation: The Recovery Agent uses the mdadm utility to mark the target block device in the RAID mirror. However, the Recovery Agent was unable to mark the target block device as faulty.

System action: The instant restore session is paused.

User response: Check the Recovery Agent engine log file on the Linux machine for more details about why the device was not marked. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf. Also check the Linux system log (usually located at /var/log/messages).

FBP0076E Failed to remove the target block device from the RAID mirror.

Explanation: The Recovery Agent uses the mdadm utility to remove the target block device from the RAID mirror. However, the Recovery Agent was unable to remove the target block device.

System action: The instant restore operation is canceled.

User response: Check the Recovery Agent engine log file on the Linux machine for more details about why the device was not removed. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf. Also check the Linux system log (usually located at /var/log/messages).

FBP0080E The operation timed-out.

Explanation: The Recovery Agent engine scripts did not reply to the Recovery Agent GUI in a timely manner.

System action: The operation is canceled.

User response: Try the operation again. If the problem persists, check the Recovery Agent engine log file on the Linux machine. This file is usually located at /opt/tivoli/tsm/TDPVMWare/mount/engine/var/TSM4VE_IR_LOG_0040.sf.

FBP0083E The snapshot does not contain a partition with a supported file system.

Explanation: The Recovery Agent successfully parsed the partition structure of the disk. However, the partitions do not use any of these supported file systems: FAT, NTFS, EXT2, EXT3, EXT4, or ReiserFS. As a result, volume-level operations, such as 'Instant Restore' and 'Mount as Virtual Volume', are not supported for this snapshot.

System action: The operation is canceled.

User response: To restore data from the selected snapshot, use the Windows Recovery Agent proxy host

to mount and expose the snapshot. See information about mounting as iSCSI targets in the product documentation.

FBP0084E Failed to retrieve partitions.

Explanation: The Windows Recovery Agent proxy host was unable to retrieve the partition list from the disk snapshot.

System action: The operation is canceled.

User response: Check the Windows Recovery Agent proxy host logs about why the partition list was not retrieved.

FBP0086E Failed to remove the Tivoli Storage Manager server connection.

Explanation: The Windows Recovery Agent proxy host reported that there are active instant restore sessions or mounted volumes that require the connection to the Tivoli Storage Manager server. As a result, the existing connection cannot be removed.

System action: The remove connection operation is canceled.

User response: Check the Windows Recovery Agent proxy host logs about the active instant restore sessions or mounted volumes.

FBP0088E Mount operation failed because the Write cache is either full or configured incorrectly.

Explanation: Mount and instant restore sessions (that run on the Linux machine) access the Virtual Volume write cache on the Windows Recovery Agent proxy host. This proxy host reported that the write cache is unavailable.

System action: The operation is canceled.

User response: Check the log files on the Windows Recovery Agent proxy host for information about why the write cache is unavailable. Verify that the Virtual Volume write cache is configured correctly in the Windows Recovery Agent GUI. See information about setting the Virtual Volume write cache options in the product documentation.

FBP0089E The Recovery Agent GUI storage type option is 'Tape', and the requested media is busy.

Explanation: When the Recovery Agent GUI storage type option specifies 'Tape', only a single snapshot can be mounted.

System action: The operation is canceled.

User response: Dismount the currently mounted

snapshot before you attempt to mount another snapshot.

FBP0090E Operation timed-out. Manual intervention might be required.

Explanation: The Linux Recovery Agent GUI operation timed-out during a mount or instant restore operation.

System action: The operation is canceled.

User response: Follow the "Responding to a timeout during a file level restore or an instant restore (Linux)" procedure documented in the Data Protection for VMware Installation and User's Guide.

FBP0091E The selected disk is not an MBR disk.

Explanation: The Recovery Agent cannot parse the partition structure of the disk, because the disk is not a Basic, MBR-based disk. Volume-level operations, such as 'Instant Restore' and 'Mount as Virtual Volume', are not supported for this snapshot.

System action: Mount and instant restore operations are disabled.

User response: To restore data from the selected snapshot, use the Windows Recovery Agent proxy host to mount and expose the snapshot using 'Mount as iSCSI target' method.

FBP0092E Operation failed. Recovery Agent is initializing.

Explanation: Mount and instant restore operations cannot proceed when the Windows Recovery Agent proxy host is initializing.

System action: The mount or instant restore operation is canceled.

User response: Wait until the Windows Recovery Agent proxy host completes initializing. Then, try the operation again.

FBP0093E The mount point is already in use by another mount session.

Explanation: The mount operation failed because the target mount point is currently in use.

System action: The mount operation is canceled.

User response: Specify a target mount point that is not in use.

FBP0094E The mount point is already in use by another instant restore session.

Explanation: The instant restore operation failed because the target mount point is currently in use.

System action: The instant restore operation is canceled.

User response: Specify a target mount point that is not in use.

FBP1001I The folder: *folder path* does not exist. Do you want to create the folder?

Explanation: The selected folder does not exist. You can create the folder by proceeding with the instructions displayed on the screen.

System action: The system waits for a user response.

User response: Select Yes to create the folder and continue with the operation. Select No to not create the folder and end the current operation.

FBP1003I Specify a folder for the cache files

Explanation: A folder that is used to store the virtual disk and virtual volume cache files was not specified. The cache is used to store write operations to the virtual disk and virtual volume during the mount operation.

System action: The system waits for a user response.

User response: Specify a folder to store the virtual disk and virtual volume cache files.

FBP1005I *mount path* already has a mounted virtual volume. Do you want to dismount the volume before you continue?

Explanation: The selected path already has a mounted virtual volume. This existing mounted virtual volume must be dismounted to continue with the current mount operation.

System action: The system waits for a user response.

User response: Specify Yes to dismount the existing mounted virtual volume and continue with the current mount operation. Specify No to end the current mount operation.

FBP1008I Recovery Agent cannot be started because it is being used by another user

Explanation: The Recovery Agent application is already running on this machine. For example, this situation occurs when the application is started by another user on another session.

System action: The operation is canceled.

User response: Log in to the machine as the user that started the Recovery Agent application.

FBP1009I **Recovery Agent cannot be closed while mounted volumes exist. Do you want to dismount all volumes?**

Explanation: Existing mounted virtual volumes and virtual disks must be dismounted before closing the Recovery Agent application.

System action: The system waits for a user response.

User response: Specify Yes to dismount all the existing mounted virtual volumes and virtual disks and close the Recovery Agent application. Specify No to not dismount all the existing mounted virtual volumes and virtual disks and return to the Recovery Agent application.

FBP1011I **The Virtual Volume Driver was registered successfully**

Explanation: Successful Recovery Agent Virtual Volume Driver registration is required to use the mount function.

System action: Operation completed successfully.

User response: The Recovery Agent application is ready for operations.

FBP1013I **Connection to Tivoli Storage Manager server resumed.**

Explanation: Communication between the Recovery Agent application and the Tivoli Storage Manager server is established.

System action: Operation completed successfully.

User response: The Recovery Agent application is ready for operations.

FBP1014I **You must restart the Recovery Agent application for changes to the Data Access options to take effect.**

Explanation: Recent changes to the Data Access options cannot be implemented until the Recovery Agent application is restarted.

System action: The Recovery Agent application operates with the existing Data Access options setting until it is restarted.

User response: Restart the Recovery Agent application so that changes to the Data Access options are implemented.

FBP1100I **Received CONTINUE from service manager**

Explanation: The Recovery Agent service received a SERVICE_CONTROL_CONTINUE command.

System action: The Recovery Agent service resumes activities. The latest Recovery Agent driver events are

written to the Recovery Agent log file.

User response: The Recovery Agent application is ready for operations.

FBP1101I **Received PAUSE from service manager**

Explanation: The Recovery Agent service received a SERVICE_CONTROL_PAUSE command.

System action: This command has no effect on the Recovery Agent service.

User response: The Recovery Agent application is ready for operations.

FBP1102I **Received a STOP command from the service manager**

Explanation: The Recovery Agent service received a SERVICE_CONTROL_STOP command. This message is issued when the service is stopped from the service manager. Opening the Recovery Agent GUI from the Start menu sends a stop command to the service.

System action: The Recovery Agent service stops.

User response: The Recovery Agent application is ready for operations.

FBP1103I **Service stopped, reporting to service manager**

Explanation: The Recovery Agent service stops. The service can be restarted from the service manager.

System action: The Recovery Agent application stops.

User response: No user action required.

FBP1104I **--- Recovery Agent version string started ---**

Explanation: The Recovery Agent application started. The version string is printed in the message.

System action: Operation completed successfully.

User response: The Recovery Agent application is ready for operations.

FBP1300I **License is OK.**

Explanation: The license file is valid.

System action: Operation completed successfully.

User response: The Recovery Agent application is ready for operations.

FBP1301W **Not for resale license.**

Explanation: The license file is valid.

System action: Operation completed successfully.

User response: The Recovery Agent application is ready for operations.

FBP1302E Error accessing license file.

Explanation: The license file could not be accessed. This situation occurs when the license file cannot be located, it cannot be opened because of permission restrictions, or the file is corrupted.

System action: The Recovery Agent application stops.

User response: Obtain a new license for the Recovery Agent application.

FBP1303E Corrupted license file.

Explanation: The license registration string is not valid.

System action: The Recovery Agent application stops.

User response: Obtain a new license for the Recovery Agent application.

FBP1304E Trial period has expired.

Explanation: The license registration string is not valid.

System action: The Recovery Agent application stops.

User response: Obtain a new license for the Recovery Agent application.

FBP1305I Try and buy license. days left.

Explanation: The license file is valid.

System action: Operation completed successfully.

User response: The Recovery Agent application is ready for operations.

FBP2001I Unmount selected session? All data will be lost.

Explanation: Data that was written to the virtual mounted volume is lost when the volume is unmounted. Applications that currently use the mounted volume might become unstable when the volume is unmounted.

System action: The system waits for a user response.

User response: Close any applications that are accessing the mounted volume before you unmount it.

FBP2002I Unmount all sessions? All data will be lost.

Explanation: Data that was written to the virtual mounted volumes is lost when the volumes are unmounted. Applications that currently use the

mounted volumes might become unstable when the volumes are unmounted.

System action: The system waits for a user response.

User response: Close any applications that are accessing the mounted volumes before you unmount them.

FBP2003I End all sessions? All data will be lost.

Explanation: Ending the instant restore sessions causes the loss of all data that was written to the restored volumes. The restored volumes display as unformatted and require reformatting.

System action: The system waits for a user response.

User response: Specify OK to end the instant restore sessions. All data that was written during these sessions is lost. Specify Cancel to continue the instant restore sessions.

FBP2004I End selected session? All data will be lost.

Explanation: Ending the instant restore session causes the loss of all data that was written to the restored volume. The restored volume displays as unformatted and requires reformatting.

System action: The system waits for a user response.

User response: Specify OK to end the instant restore session. All data that was written during this session is lost. Specify Cancel to continue the instant restore session.

FBP2005I No snapshots exist in the selected node.

Explanation: Either no snapshot was completed, or the selected Tivoli Storage Manager node is not the node that owns the snapshots.

System action: No snapshot is shown.

User response: If Tivoli Storage Manager for Virtual Environments snapshots were completed, select the Tivoli Storage Manager node that owns the snapshots.

FBP3002W The specified mount point directory contains data. If you continue, the data in this directory will be lost. Do you want to continue?

Explanation: The selected mount point contains data. The mount process redirects this mount point to the mounted virtual volume. The existing data is inaccessible until the virtual volume is unmounted.

System action: The system waits for a user response.

User response: Specify an empty mount point for the virtual volume.

FBP3003W The total size of write operations to the mount point must not exceed the value of the Cache size option.

Explanation: The cache location stores write operations from the mounted virtual volumes and instant restore sessions. The cache size is defined by the Cache size option that is specified in the Recovery Agent GUI that runs on the Windows system.

System action: If the value of the Cache size option is exceeded, the instant restore sessions and write operations to virtual volumes might be lost.

User response: Make sure that the value of the Cache size option is sufficient for the write operations from instant restore sessions and mounted volumes. The total size of write operations must not exceed the cache size.

FBP3004W The snapshot file system is not compatible with the machine operating system.

Explanation: The Recovery Agent successfully parsed the partition structure of the disk. However, no supported partitions were located. Volume-level operations, such as 'Instant Restore' and 'Mount as Virtual Volume', are not supported for this snapshot. Partitions formatted using FAT, NTFS, EXT2, EXT3, EXT4 or ReiserFS file-systems are supported.

System action: Instant restore and mount operations are disabled.

User response: To restore data from the selected snapshot, use the Recovery Agent on a Windows system. Mount the disk snapshot by specifying the 'Mount as iSCSI target' option. For more information, see the product documentation.

FBP3005W No snapshots are available for the selected virtual machine. Or, the Authentication node is not authorized to restore this virtual machine.

Explanation: No snapshots were located for the selected virtual machine. Either no snapshot completed successfully, or if the 'From node' access method was used, the Authenticate node does not have permission to restore the selected virtual machine.

System action: The operation is canceled.

User response: If the 'From node' access method is used, make sure sufficient permissions are set for the Authentication node. See the product documentation for details and an example of how to set permissions by using the Tivoli Storage Manager Backup-Archive client 'set access' command.

FBP3006W The selected snapshot will not be protected from expiration during this operation. See the product documentation for information about expiration.

Explanation: When the 'From node' authentication method is used, the Authentication node is granted Read-only access to the target node with the 'set access' command. The target node owns the snapshot. As a result, the snapshot cannot be marked as being in use on the server. Therefore, the snapshot might expire while the restore operation is in progress.

System action: The system waits for a user response.

User response: If you proceed, disable the expiration process for the snapshot during the operation. Or, make sure that no snapshots are created for the restored machine during the restore operation. Otherwise, cancel the restore operation.

FBP5003W *target volume* : The repository is not loaded. Load the repository and resume the session.

Explanation: The instant restore session is unable to resume since the Recovery Agent failed to reestablish connection to the Tivoli Storage Manager server where the backup snapshots are located. The restored volume is inaccessible while the session is paused.

System action: The instant restore session is paused.

User response: Click "Select TSM server" in the Recovery Agent GUI to connect to the Tivoli Storage Manager server and resume the instant restore session.

FBP5005W Windows indicates the destination volume *target volume* might be a network-mapped drive. If volume *target volume again* is confirmed as a network-mapped drive, the operation fails. Continue anyway?

Explanation: The Recovery Agent does not support instant restore sessions to a network-mapped drive.

System action: The instant restore session is canceled.

User response: Specify a destination volume that is not on a network-mapped drive.

FBP5007W Read block from the source has failed. The problem might have been caused by a network failure. See log file for more details. If the problem was caused by a network failure, correct the problem and resume the session.

Explanation: The instant restore session is unable to retrieve data from the Tivoli Storage Manager server. As a result, the instant restore session is paused. The problem might be caused by a network failure. The

restored volume is inaccessible while the session is paused.

System action: The instant restore session is paused.

User response: Check the Recovery Agent logs for information regarding the cause of the problem. After resolving the issue, resume the session.

FBP5008W There are open handles to the volume being restored (*volume name*). Close any application (such as Windows Explorer or a command prompt) that might be accessing this volume and try again. If you select Ignore, applications using these handles might become unstable once the restore process begins.

Explanation: The target volume for the restore is in use. Restoring a volume to a viewable storage volume involves overwriting data on that existing storage volume. After the restore begins, the current volume contents are permanently erased.

System action: The system waits for a user response.

User response: Close any application (such as Windows Explorer or a command prompt) that might be accessing this volume and try the operation again. If you select Ignore, applications that currently use these open handles might become unstable when the restore operation begins.

FBP5010W System is low on memory. Write operations to virtual volumes might be lost.

Explanation: Changes that are done on mounted volumes are written to memory. As a result, the Recovery Agent can use a large amount of RAM when it operates in read/write mode.

System action: Write operations to virtual volumes might be lost.

User response: Dismount some of the mounted volumes (when possible) or mount the volumes as read-only. The value of the 'Read Ahead cache size' option affects the memory usage. See information about setting this option in the product documentation.

FBP5011W Recovery Agent still has *number of mounted volumes* volumes mounted. Stopping Recovery Agent might cause the system to become unstable. Are you sure you want to stop the Recovery Agent?

Explanation: Stopping the Recovery Agent without first dismounting the virtual volumes might cause both the system and active applications to become unstable.

System action: The system waits for a user response.

User response: Specify No to prevent the Recovery Agent from stopping, then dismount any mounted volumes. Specify Yes to stop the Recovery Agent, even though both the system and active applications might become unstable.

FBP5012W The Recovery Agent still has *number of active sessions* active instant restore session. These sessions will be paused and the restored volumes will appear unformatted, until the Recovery Agent service restarts. Are you sure you want to stop the Recovery Agent?

Explanation: Stopping the Recovery Agent without waiting for the restore to complete makes the restored volumes display as if they are unformatted. The restore process resumes when the Recovery Agent service restarts.

System action: The system waits for a user response.

User response: Specify No to prevent the Recovery Agent from stopping and to continue the instant restore session. Specify Yes to stop the Recovery Agent, even though the volumes that are still being processed display as if they are unformatted. Do not attempt to format these volumes as such an attempt causes data loss.

FBP5013W Abort selected sessions? All data is lost and volumes require reformatting.

Explanation: Aborting the instant restore sessions causes the loss of all data that was written to the restored volumes. The restored volumes display as unformatted and require reformatting.

System action: The system waits for a user response.

User response: Specify Yes to abort the instant restore sessions. All data that was written to the restored volumes during these sessions is lost. Specify No to continue the instant restore sessions.

FBP5015W All data on target drive *volume name* will be lost. Note 1: Successful instant restore processing requires sufficient network connectivity and bandwidth to the repository. Note 2: Use of instant restore is recommended only for applications that primarily issue READ I/O's. Do you want to continue?

Explanation: Instant restore processing overwrites data on the target storage volume. A sufficient data transfer rate from the Tivoli Storage Manager server is required for a successful instant restore operation.

System action: The system waits for a user response.

User response: Click YES to confirm that you understand the effects and to start the instant restore operation.

FBP5017W There are open files on the volume mounted on: *mounted volume name*. A forced dismount invalidates all of the open files. Are you sure you want to continue?

Explanation: The virtual volume that is being dismounted is in use by another application. For example, the volume might be open in Windows Explorer. For virtual iSCSI devices, the iSCSI initiator is still logged on to the device. Forcing this volume to dismount might cause the files or applications that are accessing the volume to become unstable.

System action: The system waits for a user response.

User response: Identify and close any files or applications that are accessing the volume. Or, select Continue to ignore the warning message and continue dismounting the volume. For iSCSI devices, make sure that the iSCSI initiator is logged off the device.

FBP5018W The volume selected for restore is located on a clustered disk. See the product documentation for guidelines when restoring clustered volumes. Failure to follow these guidelines might result in data loss, if a hardware or Windows error occurs. Do you want to continue?

Explanation: Instant restore of a volume in a clustered environment is supported. Other volumes in the cluster are not affected. You can work with the cluster and with the restored volume in parallel. During the instant restore operation, the disk that is being restored cannot fail over if the node fails.

System action: The system waits for a user response.

User response: Specify YES to confirm that you understand the guidelines and to start the instant restore operation.

FBP5020W The Virtual Volume Driver is not yet registered. Recovery Agent can register the driver now. During registration, a Microsoft Windows Logo warning may be displayed. Accept this warning to allow the registration to complete. Do you want to register the Virtual Volume Driver now?

Explanation: User should register the Virtual Volume Driver in order to work with the Recovery Agent. This message is displayed following the first attempt to mount after a silence install, since the driver registration is not performed in silent install.

System action: The system waits for a user response.

User response: Specifying Yes will start the registration process. After registration the Recovery Agent application is ready for operations.

FBP5021W The mounted volume '*mounted volume name*' is in use. Dismounting the volume might cause the application that is using it to become unstable. Do you want to continue?

Explanation: The virtual volume that is being dismounted is in use by another application. For example, the volume might be open in Windows Explorer. For virtual iSCSI devices, the iSCSI initiator is still logged on to the device.

System action: The system waits for a user response.

User response: Identify and close any applications that are accessing the volume. Or, specify 'Continue' to ignore the warning message and continue dismounting the volume. For iSCSI devices, make sure that the iSCSI initiator is logged off the device.

FBP5023W There are active instant restore sessions. These sessions will be paused and the restored volumes will appear unformatted, until the application finishes loading and resumes the sessions. Do you want to continue?

Explanation: Opening the Recovery Agent UI from the 'Start>All Programs' menu stops the service. The active instant restore sessions are paused until the application finishes loading and resumes the sessions.

System action: The system waits for a user response.

User response: Specify Yes to stop the service and load the Recovery Agent UI. This action pauses and then resumes the instant restore sessions. Specify No to not load the Recovery Agent UI. This action leaves the instant restore sessions to run in the background in service mode.

FBP5025W There are '*num active sessions*' sessions using the write cache. Updates to the cache settings are processed when there are no active sessions that use the cache. Do you want to continue?

Explanation: Updates to the write cache settings were detected. These updates are applied when there are no active sessions that use the cache.

System action: The Recovery Agent application operates with the existing write cache settings.

User response: Update the write cache settings when there are no active sessions that use the cache.

FBP5026W The size of the write cache is *num write cache percentage*% full.

Explanation: Mount and instant restore sessions that run on a Linux machine use the Recovery Agent Virtual Volume write cache for write operations. The Cache size is approaching its maximum limit. Linux mount

and instant restore sessions might fail when the cache size reaches its limit.

System action: None.

User response: Do not start a new Recovery Agent mount or instant restore session on the Linux machine until the Virtual Volume write 'Cache size' value decreases. See information about setting this option in the product documentation.

FBP5028W **The file system of the selected partition (*partition format*) might not be supported by the current operating system. The appropriate File System driver must be installed for Windows to read the volume. Do you want to continue?**

Explanation: The partition file system must be supported and recognized by the Windows operating system where the volume is mounted. This condition is required to view the file structure of the mounted partition. It is recommended to mount volumes with native Linux file systems on a Linux machine.

System action: The system waits for a user response.

User response: Make sure the appropriate file system driver is installed on the Windows operating system where the volume is mounted.

FBP5029W **The connection to Tivoli Storage Manager server was lost.**

Explanation: The connection between the Recovery Agent application and the Tivoli Storage Manager server was lost.

System action: Mounted volumes might become inaccessible. The instant restore sessions are paused.

User response: Check the Recovery Agent logs for information regarding the connection failure. After resolving the issue, resume any paused instant restore sessions.

FBP5030W **No snapshots are available for the selected virtual machine. Or, the Authentication node is not authorized to restore this virtual machine.**

Explanation: No snapshots were located for the selected virtual machine. Either no snapshot completed successfully, or if the 'From node' access method was used, the Authenticate node does not have permission to restore the selected virtual machine.

System action: The operation is canceled.

User response: If the 'From node' access method is used, make sure sufficient permissions are set for the Authentication node. See the product documentation for details and an example of how to set permissions by

using the Tivoli Storage Manager Backup-Archive client 'set access' command.

FBP5031W **Some snapshots are currently mounted. If you continue, these snapshots will be dismounted. If a mounted volume is currently being used by an application, the application might become unstable. Do you want to continue?**

Explanation: Opening the Recovery Agent UI from the 'Start>All Programs' menu stops the service. The active mounted volumes are dismounted.

System action: The system waits for a user response.

User response: Close any application (such as Windows Explorer or a command prompt) that might be accessing the mounted volumes. Then, open the Recovery Agent UI. If you continue without closing the applications that are accessing the mounted volumes, these applications might become unstable.

FBP5032W **The selected snapshot will not be protected from expiration during this operation. See the product documentation for information about expiration.**

Explanation: When the 'From node' authentication method is used, the Authentication node is granted Read-only access to the target node with the 'set access' command. The target node owns the snapshot. As a result, the snapshot cannot be marked as being in use on the server. Therefore, the snapshot might expire while the restore operation is in progress.

System action: The system waits for a user response.

User response: If you proceed, disable the expiration process for the snapshot during the operation. Or, make sure that no snapshots are created for the restored machine during the restore operation. Otherwise, cancel the restore operation.

FBP5033W **No snapshots exist in the selected node.**

Explanation: Either no snapshot was completed, or the selected Tivoli Storage Manager node is not the node that owns the snapshots.

System action: No snapshot is shown.

User response: If Tivoli Storage Manager for Virtual Environments snapshots were completed, select the Tivoli Storage Manager node that owns the snapshots.

FBP7003E **The folder:*folder name* is invalid.**

Explanation: The specified path is not a valid folder path.

System action: The system waits for a user response.

User response: Specify a valid folder path.

FBP7004E **The folder:***folder name***could not be created.**

Explanation: The system failed to create the requested folder.

System action: The operation is canceled.

User response: Check the Recovery Agent logs for information about why the folder was not created.

FBP7005E *folder name* **is not empty. Only empty folders can be used as a mount point.**

Explanation: The system can mount a volume snapshot only to an empty folder.

System action: The operation is canceled.

User response: Specify an empty folder path.

FBP7006E **snapshot size** (*snapshot size*) **is larger than target size** (*partition name*)

Explanation: The volume size of the destination location must be equal to, or greater than, the size of the original volume on the snapshot to be restored.

System action: The instant restore operation is canceled.

User response: Specify a target volume with a size equal to, or greater than, the source volume on the snapshot to be restored.

FBP7007E **A valid iSCSI target name must be specified. Valid iSCSI names consist of the following items: lower-case English characters, digits, '.', ':' and '-'.**

Explanation: When a snapshot is exposed as an iSCSI target, a valid iSCSI target name must be entered.

System action: The system waits for a user response.

User response: Specify a valid iSCSI target name.

FBP7008E **A valid iSCSI initiator name must be specified. Valid iSCSI names consist of the following items: lower-case English characters, digits, '.', ':' and '-'.**

Explanation: The specified iSCSI initiator is not a valid initiator name. When a snapshot is exposed as an iSCSI target, a valid initiator name must be specified by the user.

System action: The system waits for a user response.

User response: Specify a valid iSCSI initiator name.

FBP7009E **A valid folder name must be specified.**

Explanation: The path to the folder is invalid or was not specified. The path to the mount point for the volume snapshot must include an empty folder.

System action: The system waits for a user response.

User response: Specify a valid path to an empty folder.

FBP7012E **Already connected to a Tivoli Storage Manager server. To connect to a different server, or to a different node within the server, select the current server from the list and click 'Remove'.**

Explanation: Recovery Agent can connect only to a single Tivoli Storage Manager server and node.

System action: The operation is canceled.

User response: Remove the existing connection by selecting the server from the list and click 'Remove'. You cannot remove a connection to a server that has active mounted volumes or instant restore sessions.

FBP7013E **Instant restore is not supported in Tape Mode.**

Explanation: Instant restore of snapshot data that is stored on tape is not supported.

System action: The operation is canceled.

User response: Either migrate the snapshot data to a disk storage pool, or use a different restore method.

FBP7014E **Cannot mount more than one snapshot in Tape Mode.**

Explanation: Only a single snapshot can be mounted when the snapshot data is stored on a tape.

System action: The operation is canceled.

User response: Dismount the currently mounted snapshot before you attempt to mount another snapshot.

FBP7015E **No local volume is available as a destination for instant restore.**

Explanation: Instant restore is done to a local volume that has a volume letter and is not the system volume.

System action: The operation is canceled.

User response: Make sure you have a local volume that has a volume letter and that is not the system volume as a destination for the instant restore.

FBP7016E The Recovery Agent 'Read Ahead size' option requires a value of 0 through 8192.

Explanation: The Recovery Agent 'Read Ahead size' value specifies the number of extra data blocks retrieved from the storage device after a read request is sent to a single block.

System action: The system waits for a user response.

User response: Specify a valid 'Read Ahead size' value of 0 through 8192. See information about setting this option in the product documentation.

FBP7017E The Recovery Agent 'Read Ahead cache size' option requires a value of 1000 through 75000. The value must also be at least 1 block larger than the value of the 'Read Ahead size' option.

Explanation: Recovery Agent 'Read Ahead cache size' value specifies the size of the cache where the 'Read Ahead' extra data blocks are stored.

System action: The system waits for a user response.

User response: Specify a valid 'Read Ahead cache size' value of 1000 through 75000 and at least 1 block larger than the value of the 'Read Ahead size' option. See information about setting this option in the product documentation.

FBP7018E The Recovery Agent was unable to read the snapshot data from the Tivoli Storage Manager server.

Explanation: The required data does not exist on the server or the data is inaccessible. Inaccessible data is typically caused by a 'Storage type' configuration that does not match the actual storage where the data is stored. Recovery Agent cannot read data stored on Tape or VTL if storage type is set to 'Disk'.

System action: The operation is canceled.

User response: Click 'Settings' in the Recovery Agent GUI and select the correct storage device from which to mount the snapshot. You can select 'Disk/File', 'Tape', or 'VTL'. When the storage type is changed, you must restart the Recovery Agent for the changes to take effect. Also, check the Recovery Agent logs and the Tivoli Storage Manager server activity log for any additional errors.

FBP7019E The selected disk is not a basic disk with an MBR partition style.

Explanation: Recovery Agent could not parse the partition structure of the disk, because the disk is not a Basic, MBR-based disk. Volume-level operations, such as 'Instant Restore' and 'Mount as Virtual Volume', are not supported for this snapshot.

System action: Volume-level operations are disabled.

User response: Use other methods, such as 'Mount as iSCSI target', to restore data from the selected snapshot.

FBP7020E The partitions in the selected disk are not formatted with a supported file system.

Explanation: Recovery Agent successfully parsed the partition structure of the disk. However, none of the partitions use these supported file systems: FAT, NTFS, EXT2, EXT3, EXT4, or ReiserFS. As a result, volume-level operations, such as 'Instant Restore' and 'Mount as Virtual Volume', are not supported for this snapshot.

System action: Volume-level operations are disabled.

User response: Use other methods, such as 'Mount as iSCSI target', to restore data from the selected snapshot.

FBP7021E Select the node access method.

Explanation: Three node authentication methods are available to access snapshots on the Tivoli Storage Manager server: 'Asnodename' authenticates with a proxy node, 'Fromnode' authenticates with a node that contains limited access, and 'Direct' authenticates directly.

System action: The system waits for a user response.

User response: Specify the node authentication method to access the snapshots on the Tivoli Storage Manager Server. See information about these three methods in the product documentation.

FBP7022E You must specify a Tivoli Storage Manager server name or IP.

Explanation: Recovery Agent requires this information to access the virtual machines backup snapshots on the Tivoli Storage Manager Server.

System action: The system waits for a user response.

User response: Specify the host name or IP address of the Tivoli Storage Manager Server where the backup snapshots are located.

FBP7023E You must specify a valid Tivoli Storage Manager Server port.

Explanation: Recovery Agent requires this information to access the virtual machines backup snapshots on the Tivoli Storage Manager Server.

System action: The system waits for a user response.

User response: Specify the port number that is used by the Tivoli Storage Manager Server where the backup snapshots are located.

FBP7024E You must specify an authentication node.

Explanation: No authentication node was specified. Specify the Tivoli Storage Manager node that owns the snapshots.

System action: The system waits for a user response.

User response: Specify the Tivoli Storage Manager node that owns the snapshots. See information about the node authentication methods in the product documentation.

FBP7025E You must specify a target node.

Explanation: Recovery Agent provides three node authentication methods. When 'Fromnode' or 'Asnodename' are selected, a target node must be specified. The target node is the Tivoli Storage Manager node where the virtual machine backups are located.

System action: The system waits for a user response.

User response: Specify the target node where the virtual machine backups are located. See information about the node authentication methods in the product documentation.

FBP7026E You must specify a node password.

Explanation: No password was specified for the authentication node.

System action: The system waits for a user response.

User response: Enter the password of the Tivoli Storage Manager node that owns the virtual machine snapshots.

FBP7027E The Recovery Agent 'Driver timeout' option requires a value of 60 through 300.

Explanation: The Recovery Agent 'Driver timeout' option specifies the amount of time (in seconds) to process data requests from the file system driver. When processing does not complete within the specified time, the request is canceled and an error is returned to the file system driver.

System action: The system waits for a user response.

User response: Specify a valid 'Driver timeout' value of 60 through 300. See information about setting this option in the product documentation.

FBP7028E The Recovery Agent 'Write cache size' option requires a value of 1 through upper limit

Explanation: During Linux instant restore and mount operations, the Recovery Agent on the Windows backup proxy host saves data changes in the write

cache folder. The maximum cache size is 90% of the available space for the selected folder.

System action: The system waits for a user response.

User response: Specify a valid Virtual Volume write 'Cache size' value. See information about setting this option in the product documentation.

FBP7029E The Recovery Agent CLI mount command is missing one or more required parameters.

Explanation: The Recovery Agent CLI mount command cannot complete without all required parameters.

System action: The operation is canceled.

User response: Issue the 'TDPVMwareShell.exe -h mount' (Windows) or 'TDPVMwareShell.exe -h mount dump' (Linux) command to view the required parameters. Then, issue the mount command again with all required parameters.

FBP7030E Repository 'repository name' was not found

Explanation: The Tivoli Storage Manager Server connection specified in the Recovery Agent '-rep' tag was not found.

System action: The operation is canceled.

User response: Correct the Recovery Agent CLI command '-rep' tag to identify the Tivoli Storage Manager Server where the backup snapshots are located.

FBP7031E A valid iSCSI target name must be specified. Valid iSCSI names consist of the following items: lower-case English characters, digits, '.', ':', and '-'.

Explanation: When a snapshot is exposed as an iSCSI target, a valid iSCSI target name must be entered.

System action: The operation is canceled.

User response: Specify a valid iSCSI target name.

FBP7032E Mount target 'mount target' is not valid.

Explanation: The specified mount path is not a valid folder path.

System action: The operation is canceled.

User response: Specify a valid folder path.

FBP7033E Reparse point '*reparse point*' was not found and cannot be created

Explanation: The specified mount target path was not found and cannot be created.

System action: The operation is canceled.

User response: Specify a valid folder path.

FBP7035E Failed to load partition '*partition*'

Explanation: The Recovery Agent was unable to retrieve the partition list from the disk snapshot.

System action: The operation is canceled.

User response: Check the Recovery Agent logs for information about why the partition list was not retrieved.

FBP7036E Incorrect partition number '*partition number*'

Explanation: The specified partition was not found on the disk snapshot.

System action: The operation is canceled.

User response: Specify a valid partition number.

FBP7037E 'Cache size' must be at least 1GB.

Explanation: Mount and instant restore sessions that run on a Linux machine use the Recovery Agent Cache for write operations.

System action: The system waits for a user response.

User response: Specify a valid size for the 'Write Cache' size field. 'Cache size' must be at least 1 GB.

FBP7038E The value of the Recovery Agent write 'Cache size' option must not exceed *max size in GBGB*

Explanation: During Linux instant restore and mount operations, the Recovery Agent on the Windows backup proxy host saves data changes in the write cache folder. The maximum cache size is 90% of the available space for the selected folder.

System action: Linux mount and instant restore sessions might fail when the cache size reaches its limit.

User response: Do not start a new Recovery Agent mount or instant restore session on the Linux machine until the Virtual Volume write 'Cache size' value decreases. See information about setting this option in the product documentation.

FBP8001E resume failed

Explanation: The instant restore session is unable to resume. As a result, the instant restore session pauses. The restored volume is inaccessible while the session is paused.

System action: The instant restore session pauses.

User response: Check the Recovery Agent logs for information about why the resume failed. After the issue is resolved, resume the session.

FBP8002E failed to mount because of too many mount points

Explanation: The Recovery Agent supports a maximum of 128 simultaneously mounted snapshots. That maximum was exceeded.

System action: The mounting operation is canceled.

User response: Dismount at least one of the currently mounted snapshots before an attempt to mount another snapshot.

FBP8003E failed to dismount *mounted volume name*

Explanation: The Recovery Agent failed to dismount the mounted snapshot. This issue might be caused by a disconnection from the Tivoli Storage Manager server that owns the snapshots.

System action: The dismount operation is canceled.

User response: Check the Recovery Agent logs for information about why the dismount operation failed.

FBP8004E failed to load *repository name*

Explanation: The Recovery Agent failed to expose the snapshots of the specified Tivoli Storage Manager server.

System action: The operation is canceled.

User response: Verify that the correct Tivoli Storage Manager server and node that own the snapshots are specified.

FBP8007E Virtual Volume Driver not enabled

Explanation: Mount operations require a working Recovery Agent Virtual Volume Driver.

System action: The mount operations are canceled.

User response: Check the Recovery Agent logs for information about why the Virtual Volume Driver is not enabled.

FBP8008E snapshot not found.

Explanation: The selected snapshot was not found on the Tivoli Storage Manager server.

System action: The operation is canceled.

User response: Click Refresh in the Recovery Agent GUI to load the current snapshots on the Tivoli Storage Manager server.

FBP8009E already mounted

Explanation: The selected snapshot was already mounted to the requested target.

System action: None.

User response: The mounted snapshot is available for use.

FBP8012E target is a network-mapped drive

Explanation: Mounting snapshots to a network-mapped drive is not supported.

System action: The mount operation is canceled.

User response: Specify a target drive that is not on a network-mapped drive.

FBP8015E volume letter is in use. Select another

Explanation: The selected drive letter for the mount operation is in use.

System action: The mount operation is canceled.

User response: Select a target drive letter that is not in use.

FBP8016E failed to mount

Explanation: The Recovery Agent failed to complete the mount operation.

System action: The mount operation is canceled.

User response: Check the Recovery Agent logs for information about why the mount operation failed to complete.

FBP8019E failed to stop

Explanation: The current request to abort the selected instant restore session failed because the Recovery Agent could not locate the selected session.

System action: None.

User response: The abort request for the instant restore session was already done.

FBP8020E failed to finalize the session

Explanation: The product encountered an internal error when it attempted to finalize the instant restore session.

System action: The operation is canceled.

User response: Check the Recovery Agent logs for information about why the session did not finalize.

FBP8023E target partition is too small

Explanation: The volume size of the destination location must be equal to, or greater than, the size of the original volume on the snapshot to be restored.

System action: The instant restore operation is canceled.

User response: Specify a target volume with a size equal to, or greater than, the source volume on the snapshot to be restored.

**FBP8024E load repository *repository name* failed:
error message**

Explanation: The Recovery Agent failed to expose the snapshots of the specified Tivoli Storage Manager server.

System action: The operation is canceled.

User response: Verify that the correct Tivoli Storage Manager server and Node that own the snapshots are specified.

FBP8025E repository inaccessible. Dismounting volume

Explanation: The Recovery Agent is unable to retrieve data from the Tivoli Storage Manager server. As a result, the currently mounted snapshots are dismounted.

System action: Mounted snapshots are dismounted.

User response: Check the Recovery Agent logs for information about why the repository is inaccessible.

FBP8026E '*path to repository*' inaccessible or not a repository

Explanation: The Recovery Agent failed to expose the snapshots of the specified Tivoli Storage Manager server.

System action: The operation is canceled.

User response: Verify that the correct Tivoli Storage Manager server and Node that own the snapshots are specified.

FBP8027E failed to open repository

Explanation: The Recovery Agent failed to expose the snapshots of the specified Tivoli Storage Manager server.

System action: The operation is canceled.

User response: Verify that the correct Tivoli Storage Manager server and Node that own the snapshots are specified.

FBP8029E session stopped by user

Explanation: The user requested to abort the instant restore session. Aborting the instant restore sessions causes all data that was written to the restored volume to be lost.

System action: The instant restore session ends.

User response: The restored volume is shown as unformatted and requires reformatting.

FBP8031E Failed to protect the snapshot data

Explanation: The selected snapshot cannot be protected from expiration. As a result, the instant restore session cannot start. When the 'From node' authentication method is used, the Authentication node is granted Read-only access to the target node with the 'set access' command. The target node owns the snapshot. As a result, the snapshot cannot be marked as being in use on the server and might expire during the instant restore session.

System action: The instant restore session is canceled.

User response: Specify the Tivoli Storage Manager node that owns the snapshots and start the instant restore. See information about the node authentication methods in the product documentation.

FBP8032E failed to unmount volume

Explanation: The target volume for the restore operation is in use. As a result, the instant restore operation did not start. Restoring a volume to a viewable storage volume involves overwriting data on that existing storage volume. After the restore session begins, the data on the existing volume is permanently erased.

System action: The instant restore session is canceled.

User response: Close any application (such as Windows Explorer or a command prompt) that might be accessing this volume. Then, try the operation again.

FBP8033E failed to restore blocks

Explanation: The instant restore operation is either unable to retrieve data from the Tivoli Storage Manager server or unable to write data to the target volume.

System action: The instant restore session ends.

User response: Check the Recovery Agent logs for information about why the blocks failed to restore. The restored volumes display as unformatted and require reformatting.

FBP8034E failed to mount volume

Explanation: The Recovery Agent failed to mount the target volume and start the instant restore operation.

System action: The instant restore operation is canceled.

User response: Check the Recovery Agent logs for information regarding why the target volume could not be mounted.

FBP8036E Failed to finalize

Explanation: The Recovery Agent failed to finalize the instant restore session.

System action: The instant restore session is canceled.

User response: Check the Recovery Agent logs for information about the cause of the problem. The restored volumes might display as unformatted and require reformatting.

FBP8037E initialization failed. See logs for the reason

Explanation: The Recovery Agent failed to initialize the instant restore operation.

System action: The instant restore operation is canceled.

User response: Check the Recovery Agent logs for information about the cause of the problem.

FBP8041E cannot restore to a dynamic disk

Explanation: Instant restore to a dynamic volume is not supported.

System action: The instant restore operation is canceled.

User response: Select a basic volume as the instant restore target. Then, try the operation again.

FBP8042E cannot restore to clustered disk

Explanation: Instant restore of a volume in a clustered environment is supported. However, the user canceled the restore to a volume in a clustered environment.

System action: The instant restore operation is canceled.

User response: Select a different volume as the instant restore target. Then, try the operation again.

FBP8043E failed to create bitmap

Explanation: The Recovery Agent failed to create the required internal data structure for the instant restore operation.

System action: The instant restore operation is canceled.

User response: Check the Recovery Agent logs for information about why the data structure was not created.

FBP8044E failed to scramble first block

Explanation: The Recovery Agent failed to overwrite the first sector of the disk.

System action: The instant restore operation is canceled.

User response: Check the Recovery Agent logs for information about why the overwrite to disk failed.

FBP8045E failed to notify driver

Explanation: The Recovery Agent failed to notify the kernel driver regarding the start of the instant restore session.

System action: The instant restore operation is canceled.

User response: Check the Recovery Agent logs for information about why the driver was not notified.

FBP8046E failed to unscramble first block

Explanation: The Recovery Agent failed to overwrite the first sector of the disk.

System action: The instant restore session ends.

User response: Check the Recovery Agent logs for information about why the overwrite to disk failed. The restored volumes might display as unformatted and require reformatting.

FBP8047E cannot restore to a FAT volume. Format target volume as NTFS

Explanation: Instant restore to a volume formatted as an FAT32 file system is not supported.

System action: The instant restore operation is canceled.

User response: Format the volume as an NTFS file system. Then, try the operation again.

FBP8048E session not responding

Explanation: The instant restore session did not respond to the abort request within 5 minutes. As a result, the instant restore session was forcibly stopped.

System action: The instant restore session ends.

User response: Check the Recovery Agent logs for information about why the Recovery Agent did not respond to the abort request. The restored volumes might display as unformatted and require reformatting.

FBP8050E failed to create first block file

Explanation: The Recovery Agent failed to create a memory-mapped file for the instant restore session.

System action: The instant restore operation is canceled.

User response: Check the Recovery Agent logs for information regarding why the memory-mapped file was not created.

FBP8051E cannot restore to disk with signature '0'

Explanation: Instant restore is not supported for disks without an MBR disk signature.

System action: The instant restore operation is canceled.

User response: Select an instant restore target volume on an MBR disk that contains a disk signature.

FBP8052E Recovery Agent is currently initializing.

Explanation: Mount and instant restore operations cannot proceed when the Recovery Agent is initializing.

System action: The mount or instant restore operation is canceled.

User response: Wait until the Recovery Agent completes initializing. Then, try the operation again.

FBP8053E failed to read data from server

Explanation: The Recovery Agent failed to expose the snapshots of the specified Tivoli Storage Manager server.

System action: The operation is canceled.

User response: Verify that the correct Tivoli Storage Manager server and Node that own the snapshots are specified. Check the Recovery Agent logs for more information.

FBP9000E failed connecting to a kernel driver

Explanation: Instant restore operations require a working Recovery Agent kernel driver.

System action: The instant restore operations are canceled.

User response: Check the Recovery Agent logs for information about why the Recovery Agent failed to connect to the driver.

FBP9001E Incompatible Virtual Volume Driver (FBVV) Version , expecting *expected major version.expected minor version* , installed *installed major version.installed minor version*

Explanation: The kernel driver version does not match the Recovery Agent version. A valid driver is required for the Recovery Agent to work properly.

System action: The Recovery Agent application closes.

User response: The Recovery Agent was not installed correctly. Follow the Recovery Agent installation instructions in the product documentation.

FBP9002E Cannot initialize Windows Sockets.

Explanation: The Recovery Agent failed to initialize the Windows Sockets DLL file.

System action: The Recovery Agent application closes.

User response: Check the Windows events logs for errors related to this issue. Also check the Recovery Agent logs for information about why the Windows Sockets DLL file failed to initialize.

FBP9003E Cannot obtain the application data directory path

Explanation: The Recovery Agent was unable to retrieve the application data directory path from the operating system.

System action: The Recovery Agent application closes.

User response: Check the Windows events log for errors related to this issue. Also check the Recovery Agent logs for information about why the Recovery Agent was unable to obtain the application data directory path.

FBP9004E Cannot create directory *directory name*

Explanation: The Recovery Agent failed to create the application data directory.

System action: The Recovery Agent application closes.

User response: Check the Windows events logs for any errors. Check the Recovery Agent logs for information about why the Recovery Agent failed to create the application data directory.

FBP9005E failed to initialize *module name* module

Explanation: The Recovery Agent failed to initialize.

System action: The Recovery Agent application closes.

User response: Check the Recovery Agent logs for information about why the Recovery Agent failed to initialize.

FBP9006E another instance of Recovery Agent is already running

Explanation: Only one active Recovery Agent instance is supported. This issue is encountered when multiple users are logged on to the system and attempting to run the Recovery Agent.

System action: The Recovery Agent is not started.

User response: Either close the current Recovery Agent instance or run the Recovery Agent on a different system.

FBP9007E unable to install the Recovery Agent

Explanation: The Recovery Agent failed to install. A valid installation is required for the Recovery Agent to function properly.

System action: The Recovery Agent is not started.

User response: Follow the Recovery Agent installation instructions in the product documentation.

FBP9009E Registration of Virtual Volume Driver failed. Check the file *file name*\\installFBVV.log for more information Do you want to retry registering the Virtual Volume Driver?

Explanation: The Virtual Volume Driver must be registered correctly in order for the Recovery Agent to function correctly.

System action: The system waits for a user response.

User response: >Check the Recovery Agent logs for information about why the Recovery Agent failed to register the driver. Click 'Retry' to make another attempt to register the driver or click 'Cancel' to end the operation.

FBP9010E Write Cache is full.

Explanation: Mount and instant restore sessions that run on a Linux machine use the Recovery Agent Virtual Volume write cache for write operations. Linux mount and instant restore sessions might fail when the cache size reaches its limit.

System action: Write operations to the Linux instant restore and virtual volumes might be lost.

User response: Unmount some of the mounted

volumes on the Linux machine to make available space in the write cache. Instant restore volumes on the Linux machine might display as unformatted. When the cache is full, all data that is written to the Linux instant restore volumes is lost.

Appendix D. Tivoli support information

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

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

Communities and other learning resources

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

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

User groups

Tivoli Global Storage Virtual User Group

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

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

ADSM.ORG

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

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

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

Tivoli Storage Manager community on Service Management Connect

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

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

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

Tivoli Storage Manager wiki on developerWorks®

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

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

Tivoli Support Technical Exchange

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

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

Other social media sites

LinkedIn

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

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

Twitter

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

Tivoli education resources

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

Tivoli Education and Certification website

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

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

Education Assistant

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

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

Searching knowledge bases

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

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

Searching the Internet

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

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

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

From the support website, you can search various resources:

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

Using IBM Support Assistant

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

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

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

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

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

Finding product fixes

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

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

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

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

If you have not previously customized the site:

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

Receiving notification of product fixes

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

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

Contacting IBM Software Support

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

1. Ensure that you have completed the following prerequisites:
 - a. Set up a subscription and support contract.
 - b. Determine the business impact of the problem.
 - c. Describe the problem and gather background information.
2. Follow the instructions in “Submitting the problem to IBM Software Support” on page 177.

Setting up and managing support contracts

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

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

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

Determining the business impact

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

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

Describing the problem and gathering background information

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

To save time, know the answers to these questions:

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

Submitting the problem to IBM Software Support

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

Online

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

By telephone

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

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

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

Accessibility features

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

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

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

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

- Screen magnifiers and content zooming
- High contrast mode

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

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

Vendor software

The Tivoli Storage Manager product family includes certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for the accessibility information about its products.

IBM and accessibility

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

Notices

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

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

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

*IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
U.S.A.*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

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

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



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

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

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.

Glossary

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

The following cross-references are used in this glossary:

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

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

A

absolute mode

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

access control list (ACL)

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

access mode

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

ACK See acknowledgment.

acknowledgment (ACK)

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

ACL See access control list.

activate

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

active-data pool

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

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

active file system

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

active policy set

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

active version

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

activity log

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

adaptive subfile backup

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

administrative client

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

administrative command schedule

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

administrative privilege class

See privilege class.

administrative session

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

administrator

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

agent node

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

aggregate

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

aggregate data transfer rate

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

application client

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

archive

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

archive copy

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

archive copy group

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

archive-retention grace period

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

association

The defined relationship between a client

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

audit

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

authentication rule

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

authority

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

authorization rule

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

authorized user

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

AutoFS

See automounted file system.

automatic detection

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

automatic migration

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

automounted file system (AutoFS)

A file system that is managed by an

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

B

backup-archive client

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

backup copy group

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

backup retention grace period

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

backup set

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

backup set collection

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

backup version

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

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

C

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

cache file

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

CAD See client acceptor daemon.

central scheduler

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

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

client acceptor

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

client acceptor daemon (CAD)

See client acceptor.

client domain

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

client node

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

client node session

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

client option set

A group of options that are defined on

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

client options file

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

client-polling scheduling mode

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

client schedule

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

client/server

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

client system-options file

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

client user-options file

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

closed registration

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

collocation

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

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

collocation group

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

commit point

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

communication method

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

communication protocol

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

compression

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

configuration manager

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

conversation

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

copy backup

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

copy group

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

copy storage pool

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

D**daemon**

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

damaged file

A physical file in which read errors have been detected.

database backup series

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

database snapshot

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

data center

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

data deduplication

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

data manager server

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

data mover

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

data storage-management application-programming interface (DSMAPI)

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

data store

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

deduplication

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

default management class

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

demand migration

The process that is used to respond to an

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

desktop client

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

destination

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

device class

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

device configuration file

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

disaster recovery manager (DRM)

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

disaster recovery plan

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

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

domain

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

DRM See disaster recovery manager.

DSMAPI

See data storage-management application-programming interface.

dynamic serialization

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

E

EA See extended attribute.

EB See exabyte.

EFS See Encrypted File System.

Encrypted File System (EFS)

A file system that uses file system-level encryption.

enterprise configuration

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

enterprise logging

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

error log

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

estimated capacity

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

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

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

event record

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

event server

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

exabyte (EB)

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

exclude

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

exclude-include list

See include-exclude list.

expiration

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

expiring file

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

extend

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

extended attribute (EA)

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

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

external library

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

F

file access time

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

file age

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

file device type

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

file server

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

file space

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

file space ID (FSID)

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

file state

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

file system migrator (FSM)

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

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

file system state

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

frequency

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

FSID See file space ID.

FSM See file system migrator.

full backup

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

fuzzy backup

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

fuzzy copy

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

G

GB See gigabyte.

General Parallel File System (GPFS™)

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

gigabyte (GB)

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

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

global inactive state

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

Globally Unique Identifier (GUID)

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

GPFS See General Parallel File System.

GPFS node set

A mounted, defined group of GPFS file systems.

group backup

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

GUID See Globally Unique Identifier.

H

hierarchical storage management (HSM)

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

hierarchical storage management client (HSM client)

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

HSM See hierarchical storage management.

HSM client

See hierarchical storage management client.

I

ILM See information lifecycle management.

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

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

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

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

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

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

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

individual mailbox restore
See mailbox restore.

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

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

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

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

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

J

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

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

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

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

K

KB See kilobyte.

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

L

LAN See local area network.

LAN-free data movement

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

LAN-free data transfer

See LAN-free data movement.

leader data

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

library

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

library client

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

library manager

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

local

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

local area network (LAN)

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

local shadow volume

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

LOFS See loopback virtual file system.

logical file

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

logical occupancy

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

logical unit number (LUN)

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

logical volume

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

logical volume backup

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

Logical Volume Snapshot Agent (LVSA)

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

loopback virtual file system (LOFS)

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

LUN See logical unit number.

LVSA See Logical Volume Snapshot Agent.

M

macro file

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

mailbox restore

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

managed object

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

managed server

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

management class

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

maximum transmission unit (MTU)

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

MB See megabyte.

media server

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

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

megabyte (MB)

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

metadata

Data that describes the characteristics of data; descriptive data.

migrate

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

migrated file

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

migration

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

migration job

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

migration threshold

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

mirroring

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

mode

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

modified mode

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

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

mount limit

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

mount point

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

mount retention period

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

mount wait period

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

MTU See maximum transmission unit.

N

Nagle algorithm

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

named pipe

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

NAS file server

See network-attached storage file server.

NAS file server node

See NAS node.

NAS node

A client node that is a network-attached

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

native file system

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

native format

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

NDMP

See Network Data Management Protocol.

NetBIOS (Network Basic Input/Output System)

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

network-attached storage file server (NAS file server)

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

Network Basic Input/Output System

See NetBIOS.

Network Data Management Protocol (NDMP)

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

network data-transfer rate

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

node A file server or workstation on which the

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

node name

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

node privilege class

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

non-native data format

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

O

offline volume backup

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

online volume backup

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

open registration

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

operator privilege class

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

options file

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

originating file system

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

orphaned stub file

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

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

P

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

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

partial-file recall mode

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

password generation

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

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

pattern-matching character

See wildcard character.

physical file

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

physical occupancy

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

plug-in

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

policy domain

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

policy privilege class

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

policy set

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

premigrated file

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

premigrated files database

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

premigration

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

premigration percentage

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

primary storage pool

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

privilege class

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

profile

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

profile association

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

Q**quota**

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

R

randomization

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

raw logical volume

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

rebind

To associate all backed-up versions of a file with a new management class name. For example, a file that has an active backup version is rebound when a later version of the file is backed up with a different management class association. See also bind, management class.

recall To copy a migrated file from server storage back to its originating file system using the hierarchical storage management client. See also selective recall.

receiver

A server repository that contains a log of server and client messages as events. For example, a receiver can be a file exit, a user exit, or the server console and activity log. See also event.

reclamation

The process of consolidating the remaining data from many sequential-access volumes onto fewer, new sequential-access volumes.

reclamation threshold

The percentage of space that a sequential-access media volume must have before the server can reclaim the volume. Space becomes reclaimable when files are expired or are deleted.

reconciliation

The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems.

During the reconciliation process, data that is identified as no longer needed is removed.

recovery log

A log of updates that are about to be written to the database. The log can be used to recover from system and media failures. The recovery log consists of the active log (including the log mirror) and archive logs.

register

To define a client node or administrator ID that can access the server.

registry

A repository that contains access and configuration information for users, systems, and software.

remote

For hierarchical storage management products, pertaining to the origin of migrated files that are being moved. See also local.

resident file

On a Windows system, a complete file on a local file system that might also be a migrated file because a migrated copy can exist in server storage. On a UNIX or Linux system, a complete file on a local file system that has not been migrated or premigrated, or that has been recalled from server storage and modified. See also file state.

restore

To copy information from its backup location to the active storage location for use. For example, to copy information from server storage to a client workstation.

retention

The amount of time, in days, that inactive backed-up or archived files are kept in the storage pool before they are deleted. Copy group attributes and default retention grace periods for the domain define retention.

retrieve

To copy archived information from the storage pool to the workstation for use. The retrieve operation does not affect the archive version in the storage pool. See also archive.

root user

A system user who operates without restrictions. A root user has the special rights and privileges needed to perform administrative tasks.

S

SAN See storage area network.

schedule

A database record that describes client operations or administrative commands to be processed. See also administrative command schedule, client schedule.

scheduling mode

The type of scheduling operation for the server and client node that supports two scheduling modes: client-polling and server-prompted.

scratch volume

A labeled volume that is either blank or contains no valid data, that is not defined, and that is available for use. See also volume.

script A series of commands, combined in a file, that carry out a particular function when the file is run. Scripts are interpreted as they are run. See also Tivoli Storage Manager command script.

Secure Sockets Layer (SSL)

A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

selective backup

The process of backing up certain files or directories from a client domain. The files that are backed up are those that are not excluded in the include-exclude list. The files must meet the requirement for serialization in the backup copy group of the management class that is assigned to each file. See also incremental backup.

selective migration

The process of copying user-selected files from a local file system to server storage and replacing the files with stub files on the local file system. See also demand migration, threshold migration.

selective recall

The process of copying user-selected files from server storage to a local file system. See also recall, transparent recall.

serialization

The process of handling files that are modified during backup or archive processing. See also shared dynamic serialization, shared static serialization, static serialization.

server A software program or a computer that provides services to other software programs or other computers. See also client.

server options file

A file that contains settings that control various server operations. These settings affect such things as communications, devices, and performance.

server-prompted scheduling mode

A client/server communication technique where the server contacts the client node when tasks must be done. See also client-polling scheduling mode.

server storage

The primary, copy, and active-data storage pools that are used by the server to store user files such as backup versions, archive copies, and files migrated from hierarchical storage management client nodes (space-managed files). See also active-data pool, copy storage pool, primary storage pool, storage pool volume, volume.

session

A logical or virtual connection between two stations, software programs, or devices on a network that allows the two elements to communicate and exchange data for the duration of the session. See also administrative session.

session resource usage

The amount of wait time, processor time, and space that is used or retrieved during a client session.

shadow copy

A snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shadow volume

The data stored from a snapshot of a volume. The snapshot can be taken while applications on the system continue to write data to the volumes.

shared dynamic serialization

A value for serialization that specifies that a file must not be backed up or archived if it is being modified during the operation. The backup-archive client retries the backup or archive operation a number of times; if the file is being modified during each attempt, the backup-archive client will back up or archive the file on its last try. See also dynamic serialization, serialization, shared static serialization, static serialization.

shared library

A library device that is used by multiple storage manager servers. See also library.

shared static serialization

A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. The client attempts to retry the operation a number of times. If the file is in use during each attempt, the file is not backed up or archived. See also dynamic serialization, serialization, shared dynamic serialization, static serialization.

snapshot

An image backup type that consists of a point-in-time view of a volume.

space-managed file

A file that is migrated from a client node by the hierarchical storage management (HSM) client. The HSM client recalls the file to the client node on demand.

space management

See hierarchical storage management.

space monitor daemon

A daemon that checks space usage on all file systems for which space management is active, and automatically starts threshold migration when space usage on a file system equals or exceeds its high threshold.

sparse file

A file that is created with a length greater than the data it contains, leaving empty spaces for the future addition of data.

special file

On AIX, UNIX, or Linux systems, a file that defines devices for the system, or temporary files that are created by processes. There are three basic types of special files: first-in, first-out (FIFO); block; and character.

SSL See Secure Sockets Layer.

stabilized file space

A file space that exists on the server but not on the client.

stanza A group of lines in a file that together have a common function or define a part of the system. Stanzas are usually separated by blank lines or colons, and each stanza has a name.

startup window

A time period during which a schedule must be initiated.

static serialization

A copy-group serialization value that specifies that a file must not be modified during a backup or archive operation. If the file is in use during the first attempt, the backup-archive client cannot back up or archive the file. See also dynamic serialization, serialization, shared dynamic serialization, shared static serialization.

storage agent

A program that enables the backup and restoration of client data directly to and from storage attached to a storage area network (SAN).

storage area network (SAN)

A dedicated storage network tailored to a specific environment, combining servers, systems, storage products, networking products, software, and services.

storage hierarchy

A logical order of primary storage pools, as defined by an administrator. The order is typically based on the speed and capacity of the devices that the storage pools use. The storage hierarchy is defined by identifying the next storage pool in a storage pool definition. See also storage pool.

storage pool

A named set of storage volumes that is the destination that is used to store client

data. See also active-data pool, copy storage pool, primary storage pool, storage hierarchy.

storage pool volume

A volume that has been assigned to a storage pool. See also active-data pool, copy storage pool, primary storage pool, server storage, volume.

storage privilege class

A privilege class that gives an administrator the authority to control how storage resources for the server are allocated and used, such as monitoring the database, the recovery log, and server storage. See also privilege class.

stub A shortcut on the Windows file system that is generated by the hierarchical storage management (HSM) client for a migrated file that allows transparent user access. A stub is the sparse file representation of a migrated file, with a reparse point attached.

stub file

A file that replaces the original file on a local file system when the file is migrated to storage. A stub file contains the information that is necessary to recall a migrated file from server storage. It also contains additional information that can be used to eliminate the need to recall a migrated file. See also migrated file, resident file.

stub file size

The size of a file that replaces the original file on a local file system when the file is migrated to server storage. The size that is specified for stub files determines how much leader data can be stored in the stub file. The default for stub file size is the block size defined for a file system minus 1 byte.

subscription

In a storage environment, the process of identifying the subscribers to which the profiles are distributed. See also enterprise configuration, managed server.

system privilege class

A privilege class that gives an administrator the authority to issue all server commands. See also privilege class.

T

tape library

A set of equipment and facilities that support an installation's tape environment. The tape library can include tape storage racks, mechanisms for automatic tape mounting, a set of tape drives, and a set of related tape volumes mounted on those drives.

tape volume prefix

The high-level-qualifier of the file name or the data set name in the standard tape label.

target node

A client node for which other client nodes (called agent nodes) have been granted proxy authority. The proxy authority allows the agent nodes to perform operations such as backup and restore on behalf of the target node, which owns the data.

TCA See trusted communications agent.

TCP/IP

See Transmission Control Protocol/Internet Protocol.

threshold migration

The process of moving files from a local file system to server storage based on the high and low thresholds that are defined for the file system. See also automatic migration, demand migration, migration job, selective migration.

throughput

In storage management, the total bytes in the workload, excluding overhead, that are backed up or restored, divided by elapsed time.

timeout

A time interval that is allotted for an event to occur or complete before operation is interrupted.

Tivoli Storage Manager command script

A sequence of Tivoli Storage Manager administrative commands that are stored in the database of the Tivoli Storage Manager server. The script can run from any interface to the server. The script can include substitution for command parameters and conditional logic. See also macro file, script.

tombstone object

A small subset of attributes of a deleted object. The tombstone object is retained for a specified period, and at the end of the specified period, the tombstone object is permanently deleted.

Transmission Control Protocol/Internet Protocol (TCP/IP)

An industry-standard, nonproprietary set of communication protocols that provides reliable end-to-end connections between applications over interconnected networks of different types. See also communication method.

transparent recall

The process that is used to automatically recall a migrated file to a workstation or file server when the file is accessed. See also selective recall.

trusted communications agent (TCA)

A program that handles the sign-on password protocol when clients use password generation.

U

UCS-2 A 2-byte (16-bit) encoding scheme based on ISO/IEC specification 10646-1. UCS-2 defines three levels of implementation: Level 1-No combining of encoded elements allowed; Level 2-Combining of encoded elements is allowed only for Thai, Indic, Hebrew, and Arabic; Level 3-Any combination of encoded elements are allowed.

UNC See Universal Naming Convention.

Unicode

A character encoding standard that supports the interchange, processing, and display of text that is written in the common languages around the world, plus many classical and historical texts.

Unicode-enabled file space

Unicode file space names provide support for multilingual workstations without regard for the current locale.

Universally Unique Identifier (UUID)

The 128-bit numeric identifier that is used to ensure that two components do not have the same identifier. See also Globally Unique Identifier.

Universal Naming Convention (UNC)

The server name and network name combined. These names together identify the resource on the domain.

UTF-8 Unicode Transformation Format, 8-bit encoding form, which is designed for ease of use with existing ASCII-based systems. The CCSID value for data in UTF-8 format is 1208. See also UCS-2.

UUID See Universally Unique Identifier.

V**validate**

To check a policy set for conditions that can cause problems if that policy set becomes the active policy set. For example, the validation process checks whether the policy set contains a default management class.

version

A backup copy of a file stored in server storage. The most recent backup copy of a file is the active version. Earlier copies of the same file are inactive versions. The number of versions retained by the server is determined by the copy group attributes in the management class.

virtual file space

A representation of a directory on a network-attached storage (NAS) file system as a path to that directory.

virtual mount point

A directory branch of a file system that is defined as a virtual file system. The virtual file system is backed up to its own file space on the server. The server processes the virtual mount point as a separate file system, but the client operating system does not.

virtual volume

An archive file on a target server that represents a sequential media volume to a source server.

volume

A discrete unit of storage on disk, tape or other data recording medium that supports some form of identifier and parameter list, such as a volume label or input/output control. See also scratch volume, server storage, storage pool, storage pool volume.

volume history file

A file that contains information about volumes that have been used by the server for database backups and for export of administrator, node, policy, or server data. The file also has information about sequential-access storage pool volumes that have been added, reused, or deleted. The information is a copy of volume information that is recorded in the server database.

Volume Shadow Copy Service (VSS)

A set of Microsoft application-programming interfaces (APIs) that are used to create shadow copy backups of volumes, exact copies of files, including all open files, and so on.

VSS See Volume Shadow Copy Service.

VSS Backup

A backup operation that uses Microsoft Volume Shadow Copy Service (VSS) technology. The backup operation produces an online snapshot (point-in-time consistent copy) of Microsoft Exchange data. This copy can be stored on local shadow volumes or on Tivoli Storage Manager server storage.

VSS Fast Restore

An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves the data by using a file-level copy method.

VSS Instant Restore

An operation that restores data from a local snapshot. The snapshot is the VSS backup that resides on a local shadow volume. The restore operation retrieves the data by using a hardware assisted restore method (for example, a FlashCopy operation).

VSS offloaded backup

A backup operation that uses a Microsoft Volume Shadow Copy Service (VSS) hardware provider (installed on an alternate system) to move IBM Data Protection for Microsoft Exchange data to the Tivoli Storage Manager server. This type of backup operation shifts the backup load from the production system to another system.

VSS Restore

A function that uses a Microsoft Volume Shadow Copy Service (VSS) software provider to restore VSS Backups (IBM Data Protection for Microsoft Exchange database files and log files) that reside on Tivoli Storage Manager server storage to their original location.

W

wildcard character

A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace the wildcard character.

workload partition (WPAR)

A partition within a single operating system instance.

workstation

A terminal or personal computer at which a user can run applications and that is usually connected to a mainframe or a network.

worldwide name (WWN)

A 64-bit, unsigned name identifier that is unique.

WPAR See workload partition.

WWN See worldwide name.

Index

A

- accessibility features 179
- Active Directory
 - verify replication 111
- Active Directory domain controllers 36
- application protection
 - Active Directory domain controllers 36
 - Microsoft Exchange Server 33
 - Microsoft SQL Server 33
 - self-contained 107
 - USN Rollback 36
- automated client failover
 - overview 14

B

- backup
 - cluster 92
 - data store 92
 - incremental forever
 - description 11
 - parallel 95
 - periodic full
 - description 12
 - templates 13
 - vApp 13
 - vCloud scenario 79
 - vmcli command 40
 - vSphere scenario 80

C

- customer support
 - contacting 176

D

- Data Protection for VMware Recovery
 - Agent 108
- disability 179
- disks
 - control 13, 87
 - Data Protection applications 91
- documentation 6
- domain controller
 - verify replication 111

E

- errors 121

F

- failover
 - client 14
- FBP1001I 157
- FBP1003I 157

- FBP1005I 157
- FBP1008I 157
- FBP1009I 158
- FBP1011I 158
- FBP1013I 158
- FBP1014I 158
- FBP1100I 158
- FBP1101I 158
- FBP1102I 158
- FBP1103I 158
- FBP1104I 158
- FBP1300I 158
- FBP1301W 158
- FBP1302E 159
- FBP1303E 159
- FBP1304E 159
- FBP1305I 159
- FBP5003W 160
- FBP5005W 160
- FBP5007W 160
- FBP5008W 161
- FBP5010W 161
- FBP5011W 161
- FBP5012W 161
- FBP5013W 161
- FBP5015W 161
- FBP5017W 162
- FBP5018W 162
- FBP5020W 162
- FBP5021W 162
- FBP5023W 162
- FBP5025W 162
- FBP5026W 162
- FBP5028W 163
- FBP5029W 163
- FBP5030W 163
- FBP5031W 163
- FBP5032W 163
- FBP5033W 163
- FBP7003E 163
- FBP7004E 164
- FBP7005E 164
- FBP7006E 164
- FBP7007E 164
- FBP7008E 164
- FBP7009E 164
- FBP7012E 164
- FBP7013E 164
- FBP7014E 164
- FBP7015E 164
- FBP7016E 165
- FBP7017E 165
- FBP7018E 165
- FBP7019E 165
- FBP7020E 165
- FBP7021E 165
- FBP7022E 165
- FBP7023E 165
- FBP7024E 166
- FBP7025E 166
- FBP7026E 166

- FBP7027E 166
- FBP7028E 166
- FBP7029E 166
- FBP7030E 166
- FBP7031E 166
- FBP7032E 166
- FBP7033E 167
- FBP7035E 167
- FBP7036E 167
- FBP7037E 167
- FBP7038E 167
- FBP8001E 167
- FBP8002E 167
- FBP8003E 167
- FBP8004E 167
- FBP8007E 167
- FBP8008E 168
- FBP8009E 168
- FBP8012E 168
- FBP8015E 168
- FBP8016E 168
- FBP8019E 168
- FBP8020E 168
- FBP8023E 168
- FBP8024E 168
- FBP8025E 168
- FBP8026E 168
- FBP8027E 169
- FBP8029E 169
- FBP8031E 169
- FBP8032E 169
- FBP8033E 169
- FBP8034E 169
- FBP8036E 169
- FBP8037E 169
- FBP8041E 169
- FBP8042E 169
- FBP8043E 170
- FBP8044E 170
- FBP8045E 170
- FBP8046E 170
- FBP8047E 170
- FBP8048E 170
- FBP8050E 170
- FBP8051E 170
- FBP8052E 170
- FBP8053E 170
- FBP9000E 170
- FBP9001E 171
- FBP9002E 171
- FBP9003E 171
- FBP9004E 171
- FBP9005E 171
- FBP9006E 171
- FBP9007E 171
- FBP9009E 171
- FBP9010E 171
- files

- restore overview 26, 113
- restore task (Linux) 31, 117
- restore task (Windows) 28, 113

- fixes, obtaining 176
- full VM instant restore
 - environment requirements 15
 - iSCSI network 16
 - scenarios 102
 - validation scenarios 105

G

- get_password_info
 - vmcli command 60
- glossary 185

H

- heuristics 81

I

- IBM Support Assistant 175
- incremental forever
 - description 11
- inquire_config
 - vmcli command 47
- inquire_detail
 - vmcli command 51
- instant restore
 - overview 26, 113
 - task (Linux) 31, 117
 - task (Windows) 29, 115
- Internet, searching for problem resolution 175, 176

K

- keyboard 179
- knowledge bases, searching 175

L

- LAN environment 24

M

- megablocks 81
- messages
 - Data Protection for VMware Recovery Agent 149
 - Data Protection for VMware vSphere GUI 131
- mounting snapshots 24

O

- operating systems
 - Linux 24
 - Windows 24

P

- Passport Advantage 176
- periodic full
 - description 12

- problem determination 121
 - describing problem for IBM Software Support 177
 - determining business impact for IBM Software Support 177
 - submitting a problem to IBM Software 177
- publications
 - download v

R

- replication
 - verify Active Directory 111
 - verify domain controller 111
- restore
 - databases 108
 - instant
 - full VM requirements 15
 - templates 13
 - vApp 13
 - vCloud scenario 101
 - vmcli command 43
 - vSphere scenario 102
- Restore VM
 - with application protection enabled 107

S

- self-contained application protection
 - configuring 35
- set_domian
 - vmcli command 54
- set_mapping
 - vmcli command 54
- set_option
 - vmcli command 56
- set_password
 - vmcli command 58
- snapshots
 - mounting 24
- software support
 - describing problem for IBM Software Support 177
 - determining business impact for IBM Software Support 177
 - submitting a problem 177
- Software Support
 - contacting 176
- start_guest_scan
 - vmcli command 61
- support contract 176
- support information 173
- support subscription 176

T

- templates 13
- troubleshooting 121

U

- USN Rollback 36

V

- vApp 13
- VM backup 81, 84
- vmcli command
 - backup 40
 - get_password_info 60
 - inquire_config 47
 - inquire_detail 51
 - restore 43
 - set_domain 54
 - set_mapping 54
 - set_option 56
 - set_password 58
 - start_guest_scan 61
- volumes
 - restore overview 26, 113
 - restore task (Linux) 31, 117
 - restore task (Windows) 28, 113



Product Number: 5725-A44

Printed in USA