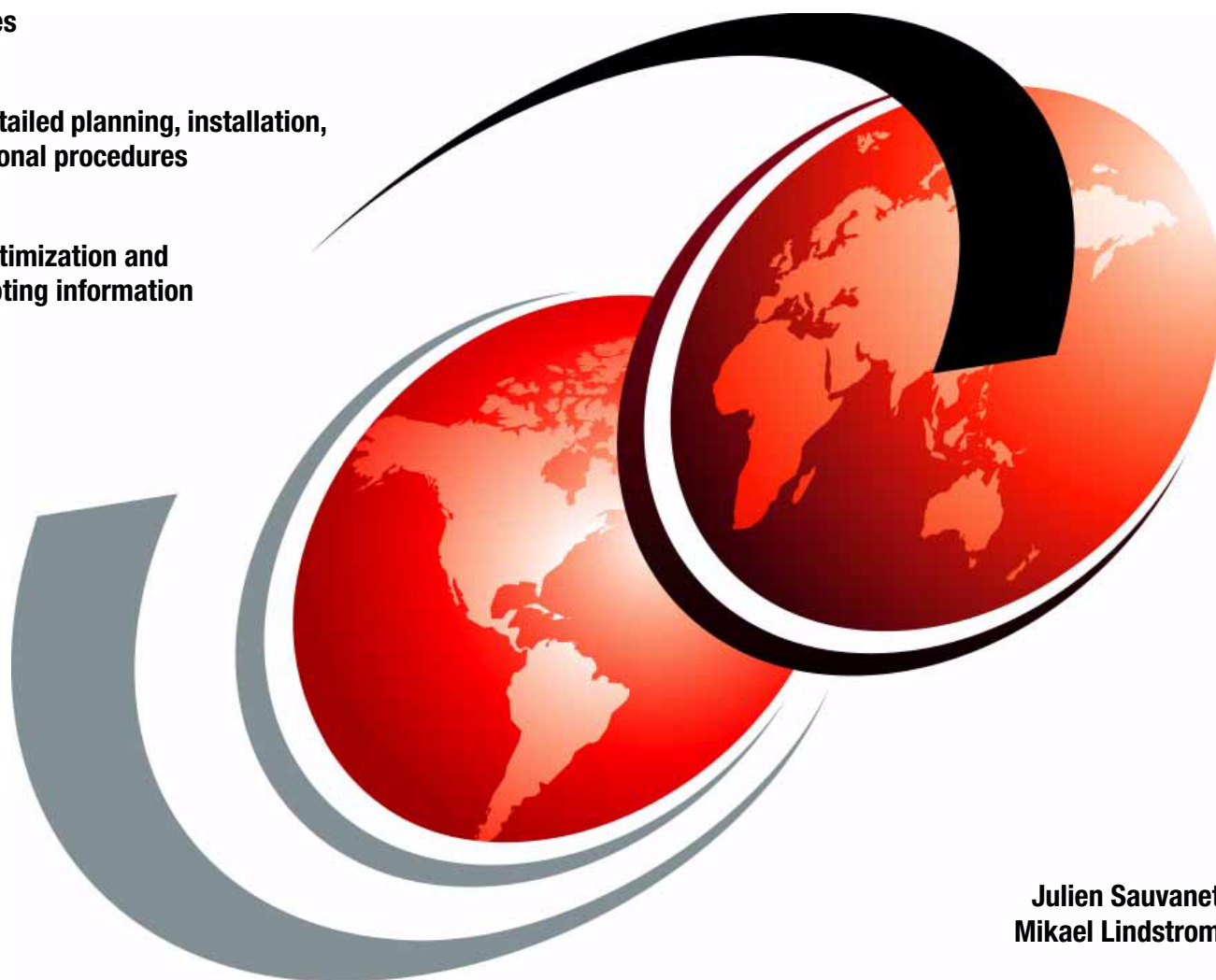


Tivoli Storage Manager for Virtual Environments - Data Protection for VMware Deployment Guide

Describes Data Protection for VMware 6.4 new features

Provides detailed planning, installation, and operational procedures

Includes optimization and troubleshooting information



Julien Sauvanet
Mikael Lindstrom



International Technical Support Organization

**Tivoli Storage Manager for Virtual Environments - Data
Protection for VMware Deployment Guide**

November 2013

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

First Edition (November 2013)

This edition applies to Version 6, Release 4 of IBM Tivoli Storage Manager for Virtual Environments (product number 5725-A44).

© Copyright International Business Machines Corporation 2013. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	vii
Trademarks	viii
Preface	ix
Authors	ix
Now you can become a published author, too!	x
Comments welcome	x
Stay connected to IBM Redbooks	x
Chapter 1. Architect corner	1
1.1 System context	2
1.2 Role and responsibilities	5
1.3 Key decisions to sketch your solution	6
1.3.1 Using Data Protection for VMware to protect Virtual Machines	6
1.3.2 Virtual or physical vStorage Backup Server	6
1.3.3 Protecting in-guest applications when there is a Tivoli Data Protection solution for your application.	6
1.3.4 Protecting in-guest applications when there is no Tivoli Data Protection solution for your application.	7
1.4 Design consideration scenarios	7
1.4.1 Scenario 1: Small environment	7
1.4.2 Scenario 2: Big environment	8
1.4.3 Scenario 3: Shared environment	10
Chapter 2. Tivoli Storage Manager for Virtual Environments: Data Protection for VMware product introduction	11
2.1 Tivoli Storage Manager solutions to protect VMware vSphere Environments	12
2.1.1 Tivoli Storage Manager Backup-Archive client within VMware guest option	12
2.1.2 Tivoli Storage Manager Backup-Archive client off host backup option	13
2.1.3 Data Protection for VMware DP for VMware option	15
2.1.4 FlashCopy Manager for VMware option	16
2.1.5 FlashCopy Manager within VMware guest option	17
2.1.6 Tivoli Storage Manager FastBack within a VMware guest option	17
2.2 Data Protection for VMware Solution components	18
2.2.1 Component definitions	18
2.3 New in Backup-Archive client and Data Protection for VMware V6.4	20
2.3.1 Incremental forever backup processing	20
2.3.2 Configuration wizard	21
2.3.3 Parallel backup from a single Tivoli Storage Manager instance	22
2.3.4 Expanding VM backup criteria	22
2.3.5 Controlling which disks in the VMware environment are processed	22
2.3.6 Protecting applications that run in virtual machine guests	22
2.3.7 Preserving VMware configuration attributes	22
2.3.8 Virtual machine templates and vApps	23
2.3.9 View VM backup status reports	23
2.3.10 Secure Sockets Layer communication	23
2.3.11 Role-based usage	23
2.3.12 Data Protection for VMware vCenter plug-in error messages	24
2.4 Product requirements: Supported platforms	24

Chapter 3. Planning the installation of Data Protection for VMware	25
3.1 Collecting and consolidating data protection policies	27
3.2 Learning about the Virtual Environment to protect it	27
3.2.1 VMware infrastructure	27
3.2.2 Virtual Machines	28
3.2.3 vCenter Server credentials considerations	29
3.2.4 Data Protection for VMware vCenter plug-in user roles	30
3.3 Protecting applications in a virtual environment	31
3.3.1 MS-SQL data protection	32
3.3.2 Exchange data protection	33
3.3.3 Active Directory data protection	34
3.3.4 Unstructured data protection	35
3.4 Communication ports between VMware and Tivoli Storage Manager components	36
3.5 Choosing your backup strategy	37
3.5.1 Periodic full backup	37
3.5.2 Incremental forever backup strategy	37
3.5.3 Backup strategy considerations	37
3.6 vStorage Backup Server	38
3.6.1 Data transfer and transport methods	38
3.6.2 vStorage Backup Server: Physical versus virtual	39
3.6.3 Physical vStorage Backup Server LUN access considerations	41
3.6.4 Virtual vStorage Backup Server HotAdd considerations	42
3.6.5 vStorage Backup Server Sizing	42
3.6.6 When to use multiple datamover agents	44
3.7 Storage location versus recovery features	44
3.8 Determining the location to start backup or restore	45
3.9 Effect of Data Protection for VMware backups on the Tivoli Storage Manager Server	46
3.9.1 How to handle CTL files (FULL-VM backup control files)	46
3.9.2 VM full-vm backup on physical tape or virtual tape	46
3.9.3 Incremental forever backup strategy consequence on Tivoli Storage Manager server database	47
3.10 VMware snapshots considerations	47
3.10.1 Snapshots limitation	47
3.10.2 VMDK file size and snapshot overhead	47
3.11 Data Protection for VMware considerations	49
3.11.1 Tivoli Storage Manager Backup Archive considerations	49
3.11.2 Multiple vCenter server support	49
3.12 Tivoli Storage Manager node naming convention for Data Protection for VMware resources	50
3.13 Deploying Data Protection for VMware in a shared environment	51
3.13.1 Back up in a shared environment	51
3.13.2 Determining what Data Protection for VMware nodes are needed	52
3.13.3 Examples of deployment implementations	55
3.13.4 Recovery in a shared environment	57
Chapter 4. Installation and configuration	59
4.1 Overview of component installation and configuration	60
4.1.1 Tivoli Storage Manager server configuration	61
4.2 Tivoli Storage Manager data mover: Backup and archive client	65
4.2.1 Installing Tivoli Storage Manager Backup-Archive client for Windows	65
4.2.2 Configuring Backup-Archive client as a datamover for Data Protection for VMware backup for Windows	67
4.2.3 Configuring Tivoli Storage Manager scheduler and web client for Windows	69

4.2.4	Installing Tivoli Storage Manager Backup-Archive client for Linux	69
4.2.5	Configuring Backup-Archive client as a datamover for Data Protection for VMware backup for Linux	70
4.2.6	Configuring Tivoli Storage Manager and web client for Linux.	71
4.2.7	Configuring multiple datamovers on the same vStorage Backup Server (proxy) .	71
4.3	Installing Data Protection for VMware features.	72
4.3.1	Installing Data Protection for VMware for Windows	72
4.3.2	Installing Data Protection for VMware for Linux	79
4.3.3	Default paths for installed components for Windows	87
4.3.4	Data Protection for VMware services for Windows.	88
4.3.5	Default paths of installed components for Linux	88
4.3.6	Data Protection for VMware services for Linux.	89
4.4	Data Protection for VMware vCenter plug-in configuration.	89
4.4.1	Using the vCenter plug-in wizard	89
4.4.2	Configuring the vCenter plug-in	90
4.4.3	Editing the vmcliprofile file for Linux	94
4.4.4	Editing the vmcliprofile file for Windows	97
Chapter 5.	Virtual machine backup	99
5.1	Configuring the datamover to control the backup scope and content.	100
5.2	VM backup by using vCenter plug-in	100
5.3	VM backup by using Backup-Archive GUI client.	105
5.4	VM backup by using the Backup/Archive Client command line	107
5.5	VM backup by using Data Protection for VMware CLI	113
5.6	Self-contained application protection	115
5.6.1	Enabling application protection for a VM.	115
5.7	VM backup optimization	117
Chapter 6.	Backup scheduling.	119
6.1	Backup scheduling	120
6.1.1	Backup schedule and backup strategy	120
6.1.2	Fine-tuning the Tivoli Storage Manager server.	121
6.1.3	Fine-tuning the datamover	121
6.1.4	Defining a schedule to back up VMs.	122
6.1.5	Updating or deleting a VM backup schedule.	124
Chapter 7.	Virtual machine recovery scenarios: Full or Item	125
7.1	Overview of recovery procedures	126
7.1.1	Full VM restoration	126
7.1.2	File level restoration	134
7.1.3	File level restoration from Windows VM backup	135
7.1.4	File level restoration from Linux VM backup	149
7.1.5	Instant recovery	155
7.1.6	Windows volume instant recovery.	155
7.1.7	Linux volume instant restore	159
7.2	Recovering data by using the Set Access and FromNode options.	164
Chapter 8.	Reporting that uses vCenter plug-in or SQL queries	167
8.1	Reporting by using vCenter plug-in.	168
8.2	Reporting by using SQL commands	169
8.2.1	Successful backup in a specified time frame	169
8.2.2	Unsuccessful backup in a specified time frame	170
8.2.3	Not backed up in a specified time frame.	170
8.2.4	Comparing successful full and successful incremental backups	171

8.2.5 Additional reporting information	172
Chapter 9. Problem determination and FAQs	173
9.1 Common errors	174
9.1.1 Common error messages	174
9.1.2 Restoration by using SAN transport method.	176
9.1.3 Incremental Forever and FULL-VM recovery issue	177
9.1.4 Plug-in management.	177
9.2 Analyzing error situations and getting support	177
9.2.1 Web resources	177
9.2.2 Tracing	178
9.2.3 Contacting IBM support: Opening a service request.	178
9.3 Frequently Asked Questions	180
Appendix A. VMware for the storage administrators	185
Server virtualization at a glance	186
Introduction to VMware vSphere	187
VMware terminology	189
Related publications	193
IBM Redbooks	193
Other publications	193
Online resources	193
Help from IBM	194

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.

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.

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

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

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

COPYRIGHT LICENSE:

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®	IBM®	Redpaper™
DB2®	Lotus®	Redbooks (logo)  ®
FlashCopy®	Passport Advantage®	Tivoli Storage Manager FastBack®
Global Technology Services®	Rational®	Tivoli®
GPFS™	Redbooks®	WebSphere®

The following terms are trademarks of other companies:

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

Microsoft, Windows, and the Windows logo 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.

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

Preface

This IBM® Redpaper™ publication helps you to install, tailor, configure, and use IBM Tivoli® Storage Manager for Virtual Environments - Data Protection for VMware. The features of Tivoli Storage Manager for Virtual Environments - Data Protection for VMware are described. Scenarios are provided for implementation of Tivoli Storage Manager Virtual Environment to protect virtual machines in several environments. This publication includes answers to common implementation errors and questions you might have that are related to the implementation of Data Protection for VMware.

Authors

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Poughkeepsie Center.

Julien Sauvanet is an IT Specialist, working in the Strategic Outsourcing Delivery at IBM Global Services, in France. He has 10 years of experience with Tivoli Storage Manager and other related storage products. He also is an IBM Certified Deployment Professional for Tivoli Storage Manager. His areas of expertise include the Tivoli Storage Manager product family, disk and tape subsystems, virtualization, and pSeries.

Mikael Lindstrom is an IBM Expert Certified Senior IT Specialist, working as a Nordic Storage Technical Lead and Backup and Recovery Lead Architect in Delivery Technology Engineering, which is part of IBM Global Technology Services® organization. He has 12 years of IT experience and has worked with IBM since 2006 in different leadership roles. He also is a member of the GTS Global Design Authority and GTS Europe Design Authority, where he provides technical governance and serves as the design authority for that technical domain. Mikael has several years of Tivoli Storage experience, including solutions architecture and implementing Tivoli Storage Manager. Mikael is an IBM Certified Deployment Professional on Tivoli Storage Manager, IBM Certified Solution Advisor on Tivoli Storage Solution, and IBM Certified Deployment Professional on Tivoli Storage Productivity Center. Mikael has authored several IBM Redbooks® publications, including, *IBM SmartCloud Virtual Storage Center Solution IBM Redbooks Solution Guide*, TIPS0991; *Tivoli Storage Manager V6.1 Technical Guide*, SG24-7718-00, and *Certification Study Guide Series: Tivoli Storage Manager V6.1*, SG24-7781-00. He also published several Tivoli Storage Manager white papers.

Thanks to the following people for their contributions to this project:

- ▶ Jason Basler, IBM, Tivoli Storage Manager Test Architect
- ▶ Pol Vander Eyken, IBM Global Technology Services, Tivoli Storage Manager
- ▶ Tommy Hueber, IBM Tivoli Storage Manager Consultant at THCS
- ▶ Jim Smith, IBM, Senior Technical Staff Member, Tivoli Storage Manager Architect
- ▶ Richard Vining, IBM, Client Experience Product Manager, Tivoli Storage Software, IBM Cloud & Smarter Infrastructure
- ▶ Daniel Wolfe, IBM Software Group, Tivoli Storage Software Advanced Technology (SWAT): Tivoli Storage Manager

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

<http://www.ibm.com/redbooks/residencies.html>

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form that is found at:

<http://www.ibm.com/redbooks>

- Send your comments in an email to:

redbooks@us.ibm.com

- Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

<http://www.facebook.com/IBMRedbooks>

- Follow us on Twitter:

<http://twitter.com/ibmredbooks>

- Look for us on LinkedIn:

<http://www.linkedin.com/groups?home=&gid=2130806>

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>

- Stay current on recent Redbooks publications with RSS Feeds:

<http://www.redbooks.ibm.com/rss.html>



Architect corner

This book gives direction and procedures to install, configure, and use Tivoli Storage Manager for Virtual Environments - Data Protection for VMware.

Before we describe the product, you should be aware of the effect the product might have on your organization. It can penetrate different technical components; therefore, it can affect related competencies that might be distributed among several teams.

This chapter provides a broader vision about implementing Data Protection for VMware products in a virtual environment. This chapter also describes the product interactions with the VMware virtualization layer, Operating Systems, disk storage, network components, tape storage, and other Tivoli Storage Manager products.

We introduce the product and its place within IT teams and environment in 1.1, “System context” on page 2.

In 1.2, “Role and responsibilities” on page 5, we give suggestions about how data protection operations can be distributed across the various teams.

This chapter includes the following topics:

- ▶ System context
- ▶ Role and responsibilities
- ▶ Key decisions to sketch your solution
- ▶ Design consideration scenarios

1.1 System context

Figure 1-1 shows the system context of a typical Data Protection for VMware solution for Tivoli Storage Manager for Virtual Environments and is intended to record the interactions it has with existing external systems in the IT infrastructure and with users.

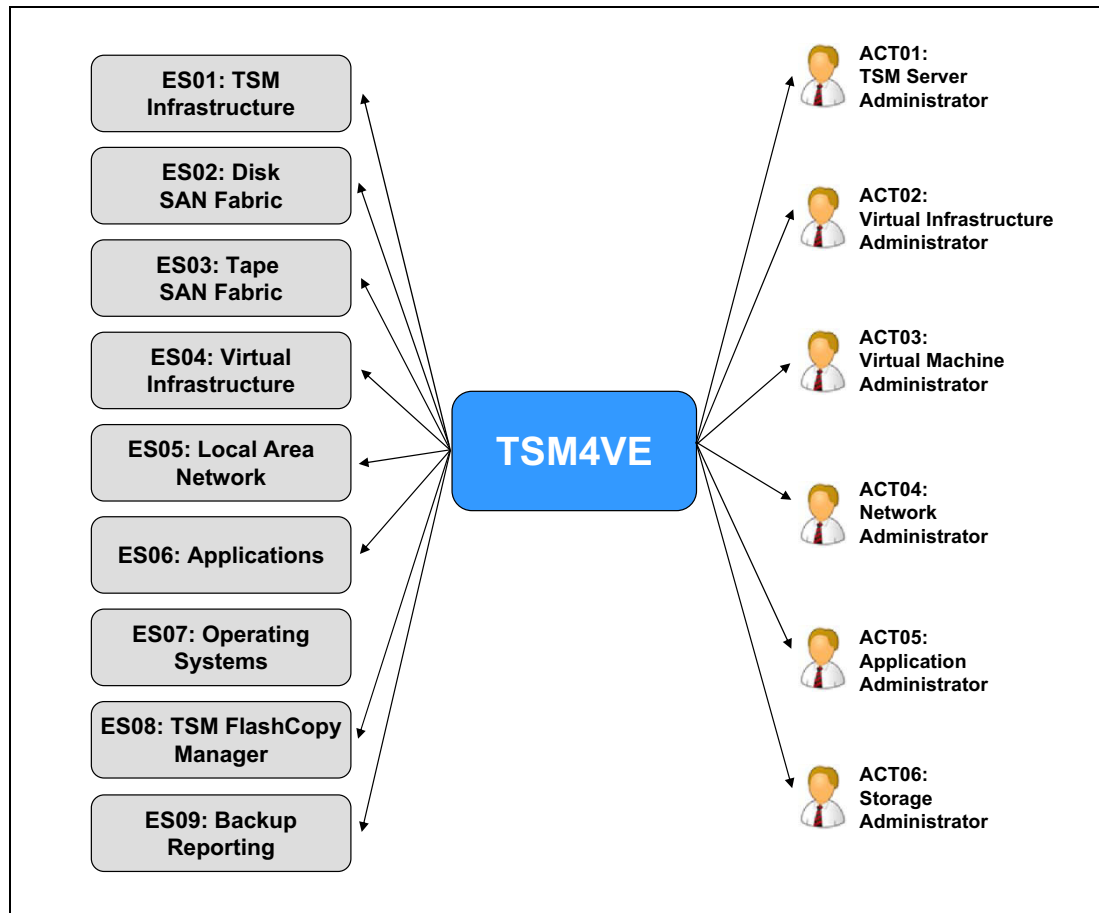


Figure 1-1 Tivoli Storage Manager for Virtual Environments: System context

Tivoli Storage Manager for 4VE and Tivoli Storage Manager for Virtual Environments are designing Data Protection for VMware Data Protection for VMware.

Table 1-1 shows how each user interacts with the solution.

Table 1-1 Users that are involved in a Data Protection for VMware deployment

ID	Name	Description
ACT01	Tivoli Storage Manager server administrator	The Tivoli Storage Manager Server administrator manages the Tivoli Storage Manager infrastructure (ES01), which is a required component for Tivoli Storage Manager 4VE. ACT01 provides essential services to Tivoli Storage Manager 4VE, such as, proxy node configuration, storage pool definition, and management and schedule and data retention definition. In Tivoli Storage Manager 4VE 6.4, most of those actions can be delegated to users by using the Tivoli Storage Manager 4VE vCenter plug-in (ACT02 or ACT03).
ACT02	Virtual Infrastructure administrator	ACT02 is the main customer of Tivoli Storage Manager 4VE. They use it as the main backup solution for all the guests that are hosted in the virtual infrastructure (ES04). They also provide access to vCenter and the underlying virtual infrastructure components to the Tivoli Storage Manager 4VE solution.
ACT03	Virtual Machine administrator	ACT03 is one of the Tivoli Storage Manager 4VE users. They rely on the solution to protect and restore the guests for which they have responsibility.
ACT04	Network Administrator	The network administrator must be aware of the strain the Tivoli Storage Manager VE solution puts in the network infrastructure element (ES05) and makes sure they provide an adequate infrastructure to support the backup solution requirements.
ACT05	Application Administrator	ACT05 is a stakeholder in the solution. They must be aware of how it works and what it can do for their specific application. In some cases, Tivoli Storage Manager 4VE is not enough to provide consistent application data backup and restore services. That can be determined only with the application administrator's help.
ACT06	Storage Administrator	The storage administrator is key in implementing and maintaining the Tivoli Storage Manager 4VE solution. They make sure that the Tivoli Storage Manager 4VE components have appropriate access to storage components where data is retrieved and stored.

Table 1-2 describes how the solution interacts with external systems.

Table 1-2 External systems that are affected by a Data Protection for VMware deployment

ID	Name	Description
ES01	Tivoli Storage Manager Infrastructure	The Tivoli Storage Manager infrastructure external service is a requirement for the Tivoli Storage Manager 4VE solution to function. It contains several components, such as, the Tivoli Storage Manager Server, library manager, storage pools, Tivoli Storage Manager nodes definition, and data retention policy. Without ES01, there cannot be a Tivoli Storage Manager 4VE solution.

ID	Name	Description
ES02	Disk SAN Fabric	This external service is where data to be backed up resides. In some cases, it can also include storage where back up data temporarily resides (before it is migrated to tape).
ES03	Tape SAN Fabric	This external service is where backed up data can be stored. It can be accessed almost directly by the Tivoli Storage Manager 4VE solution (as in the case of a physical proxy doing LAN-free backups) or indirectly (through the Tivoli Storage Manager server when storage pool migration occurs).
ES04	Virtual Infrastructure	This external service is the main interface for the Tivoli Storage Manager 4VE solution that enables data to be retrieved. It includes components like hypervisor, guests, and logical data stores where guest data is hosted. Guest definition is part of the data that is backed up by the Tivoli Storage Manager 4VE solution. It is through this external service that users of the Tivoli Storage Manager 4VE solution most likely interact (via a plug-in into the virtual infrastructure management solution).
ES05	Local Area Network	In most instances, LAN is the main transport for data being backed up and restored by the Tivoli Storage Manager 4VE solution. This service most likely is what determines the overall performance of the solution.
ES06	Applications	Applications constitute part of the data that is backed up by the Tivoli Storage Manager 4VE solution. In some cases, they might even be left out of the Tivoli Storage Manager 4VE solution because they cannot be consistently backed up and require another backup solution (such as a TDP agent).
ES07	Operating Systems	Operating Systems are part of the data that is backed up by the Tivoli Storage Manager 4VE solution. One of the main benefits of the solution is for providing quick and efficient recovery when operating system failures occur.
ES08	Tivoli Storage Manager FlashCopy® Manager	This external service might not always be present. However, when it is, it can interact with the Tivoli Storage Manager 4VE solution to provide quick backup of an entire virtual infrastructure by using FlashCopy on logical unit numbers (LUNs) that are used by logical data stores (where the guest data is).
ES09	Backup Reporting	This external service is used to view the status of all of the backup and restore tasks. Tivoli Storage Manager 4VE must interface with the reporting system directly or indirectly to report on job status.

The users that are listed in Table 1-2 on page 3 must be aware of and involved in the data protection product implementation.

1.2 Role and responsibilities

This section presents a summary of the roles responsibilities and tasks distribution across the teams and competencies.

Depending on the existing separations of duties, roles and responsibilities between the teams can vary. Figure 1-2 shows overview of the tasks distribution when Tivoli Storage Manager for Virtual Environments - Data Protection for VMware is implemented and used.

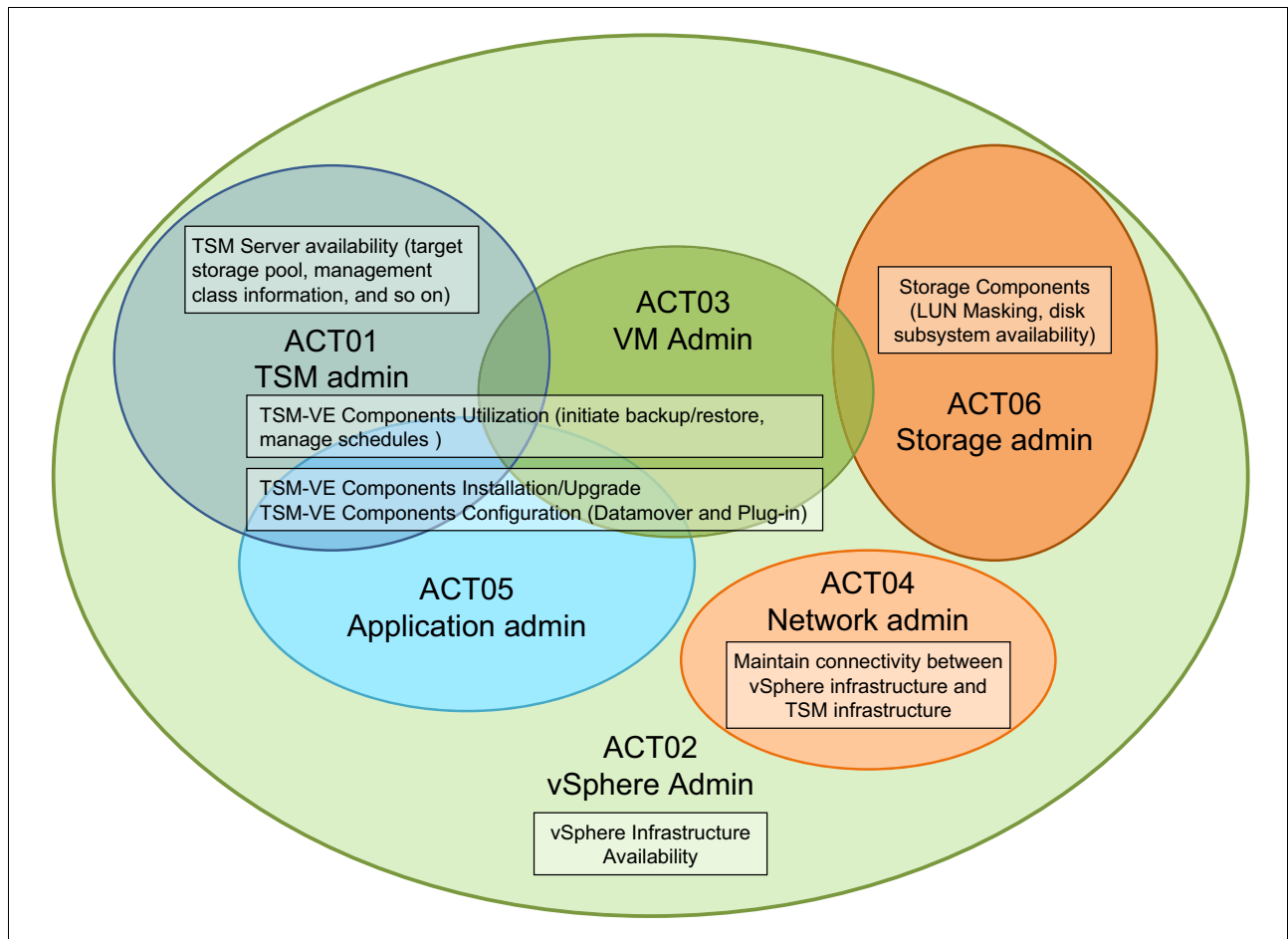


Figure 1-2 Tasks distribution across IT competencies

In Figure 1-2, bubble intersections mean that an operation can be done by Tivoli Storage Manager Administrators, Virtual Machine Administrators, or Application Administrators, depending on your IT organization. Thus, a bubble intersection means that there should be team communication. Each person that is responsible for a task can inform or request assistance of other peer users.

1.3 Key decisions to sketch your solution

The intent of this section is to help with some key decisions you must address when you are designing a solution to protect a virtual environment.

This information is not intended to replace the analysis of your environment and is not a complete set of decisions. However, some of the items might help you to sketch a design of what your solution might look like.

All of the points that are made in this section are described further throughout this publication.

1.3.1 Using Data Protection for VMware to protect Virtual Machines

In this section, we describe the following reasons to use Data Protection for VMware to protect virtual machines.

- ▶ It allows for self-service file-level restore by Virtual Machine Operating System support teams and users. A traditional approach requires restoring the VM image or building a VM with base operating systems and performing a file-level restore (overlay) onto the base operating system by using an In-Guest agent.
- ▶ Easy interaction with FlashCopy Manager for VMware, if needed.
- ▶ Integrated with Tivoli Storage Manager Server, disk, and physical and virtual tape library (VTL) based storage.
- ▶ Embedded backup report.

For more information about the features of Data Protection for VMware, see Chapter 2, “Tivoli Storage Manager for Virtual Environments: Data Protection for VMware product introduction” on page 11.

1.3.2 Virtual or physical vStorage Backup Server

The first consideration to determine which type of vStorage Backup Server should be used to transfer the data between the VMware environment and the Tivoli Storage Manager server is to determine whether physical or virtual proxies are used. You do not need to decide all one or the other. It is possible to use virtual proxies for part of an environment and physical proxies for another where it makes sense.

For more information about and a list of questions and items that guide you through the process of choosing your vStorage backup Server, see 3.6.2, “vStorage Backup Server: Physical versus virtual” on page 39.

1.3.3 Protecting in-guest applications when there is a Tivoli Data Protection solution for your application

The use of a Data Protection agent (TDP) for application protection is the recommended and supported solution for several applications. It provides the best recovery features.

For more information about how to protect your applications, see 3.3, “Protecting applications in a virtual environment” on page 31.

1.3.4 Protecting in-guest applications when there is no Tivoli Data Protection solution for your application

Because Tivoli Storage Manager for Virtual Environment relies on VMware snapshots, this method might provide the data consistency (through the VSS quiescent operations) when a Tivoli Data Protection solution does not exist to support a particular application.

For more information about how to protect your applications, see 3.3, “Protecting applications in a virtual environment” on page 31.

1.4 Design consideration scenarios

This section describes several implementation scenarios that are based on different environments.

The scenarios should not be used “as is” for a deployment. They are intended to be a design starting point only. To build a strong, robust, and comprehensive solution, read this entire paper.

1.4.1 Scenario 1: Small environment

In this scenario, we describe the implementation of Tivoli Storage Manager Virtual Environment to protect virtual machines in a small environment.

The small environment has the following characteristics:

- ▶ 10 TB total storage space
- ▶ Up to 150 Virtual machines (70 GB average size)
- ▶ 6% daily change rate
- ▶ Incremental forever backup strategy

In this case, and according to the best practices, the design includes the following components:

- ▶ One virtual vStorage Backup Server (Proxy)
- ▶ One Tivoli Storage Manager server
- ▶ Estimated disk storage space required is based on the following policy:

10 TB initial full + 614 GB Daily * NB days to be retained on Tivoli Storage Manager server where NB is the first full backup of virtual machine must be spread over several days, or another virtual proxy can be set up temporarily.

Tivoli Storage Manager deduplication (client side or server side) can be enabled. If it is, the Tivoli Storage Manager server must meet the minimum hardware requirement and the data must be stored on FILE-based volumes on the Tivoli Storage Manager server side. Carefully consider the Tivoli Storage Manager deduplication limitation, as described at the following website:

<https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Storage%20Manager/page/Deduplication>

Also, with deduplication, you must refine the storage pool space estimation. The design is shown in Figure 1-3.

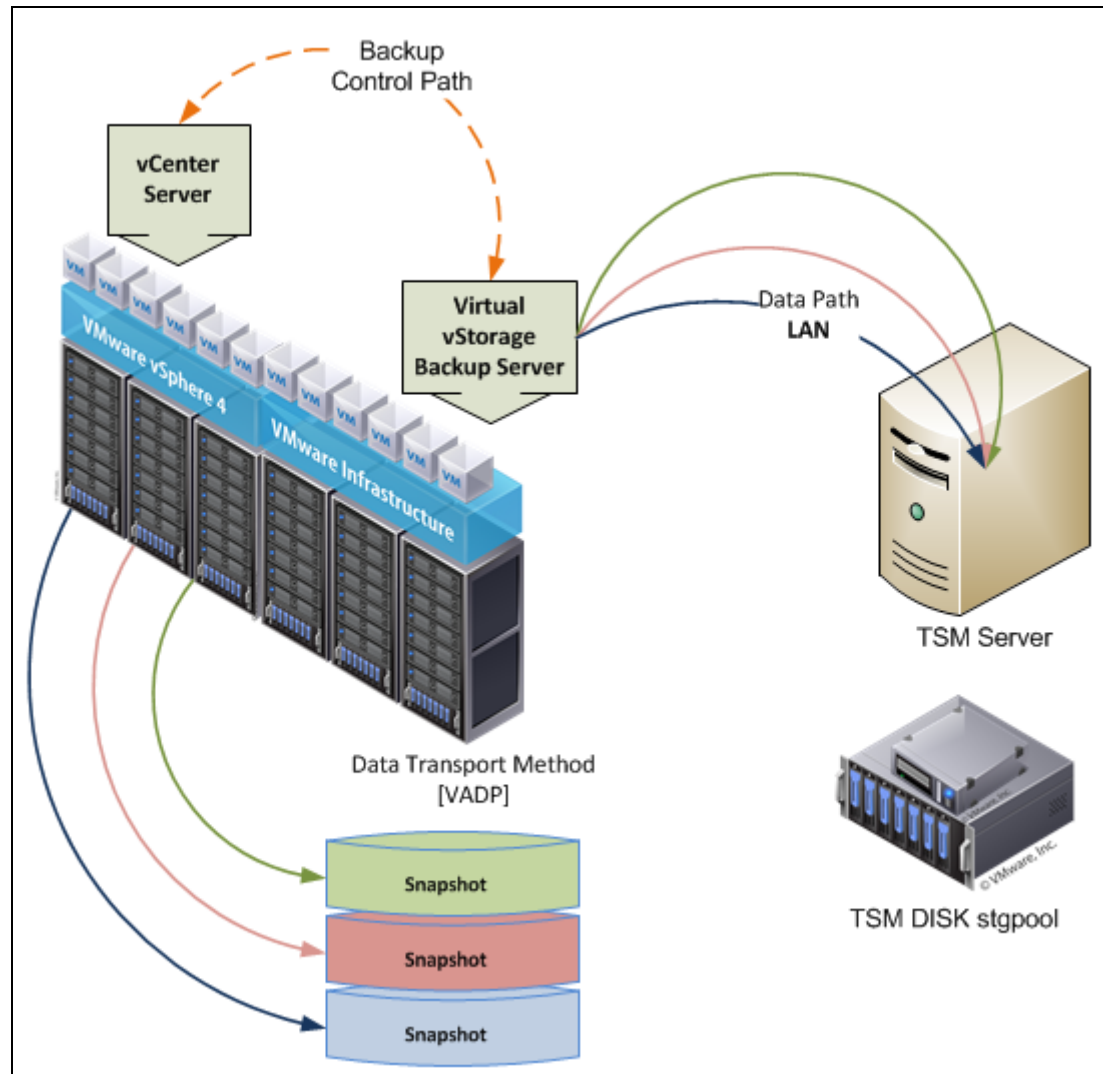


Figure 1-3 Tivoli Storage Manager: Virtual Environment small environment overview

1.4.2 Scenario 2: Big environment

In this scenario, we describe the implementation of Tivoli Storage Manager Virtual Environment to protect virtual machines in a big environment.

The big environment has the following characteristics:

- ▶ 80 TB total storage
- ▶ Up to 1500 virtual machines (50 GB average size)
- ▶ 6% daily change rate
- ▶ Incremental forever backup strategy

In this scenario and according to the best practices, the design includes the following components:

- ▶ Three virtual vStorage backup servers (Proxy)
- ▶ One Tivoli Storage Manager server

- Estimated disk storage space required is based on the following policy:
80 TB initial full + 5 TB daily * NB days to be retained on Tivoli Storage Manager server

At the time of this writing, we do not recommend the use of Tivoli Storage Manager deduplication in this environment, according the Tivoli Storage Manager deduplication limit that is described at this website:

<https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Storage%20Manager/page/Effective%20Planning%20and%20Use%20of%20IBM%20Tivoli%20Storage%20Manager%20V6%20Deduplication>

This increases the number of virtual vStorage Backup servers that are required, thus limiting the design scalability and increasing the number of Tivoli Storage Manager servers. It also requires high-performance disks to drive the Tivoli Storage Manager database.

Instead, consider the implementation of an appliance (such as, ProtecTier) to offload the deduplication process out of Tivoli Storage Manager servers. Also, consider the implementation of a physical proxy, with which you can use storage area network (SAN) and LAN-free transport to move the data from the datastore to virtual tapes (ProtecTier). Figure 1-4 shows the possible design (including a physical or virtual vStorage Backup server) and the deduplication implication.

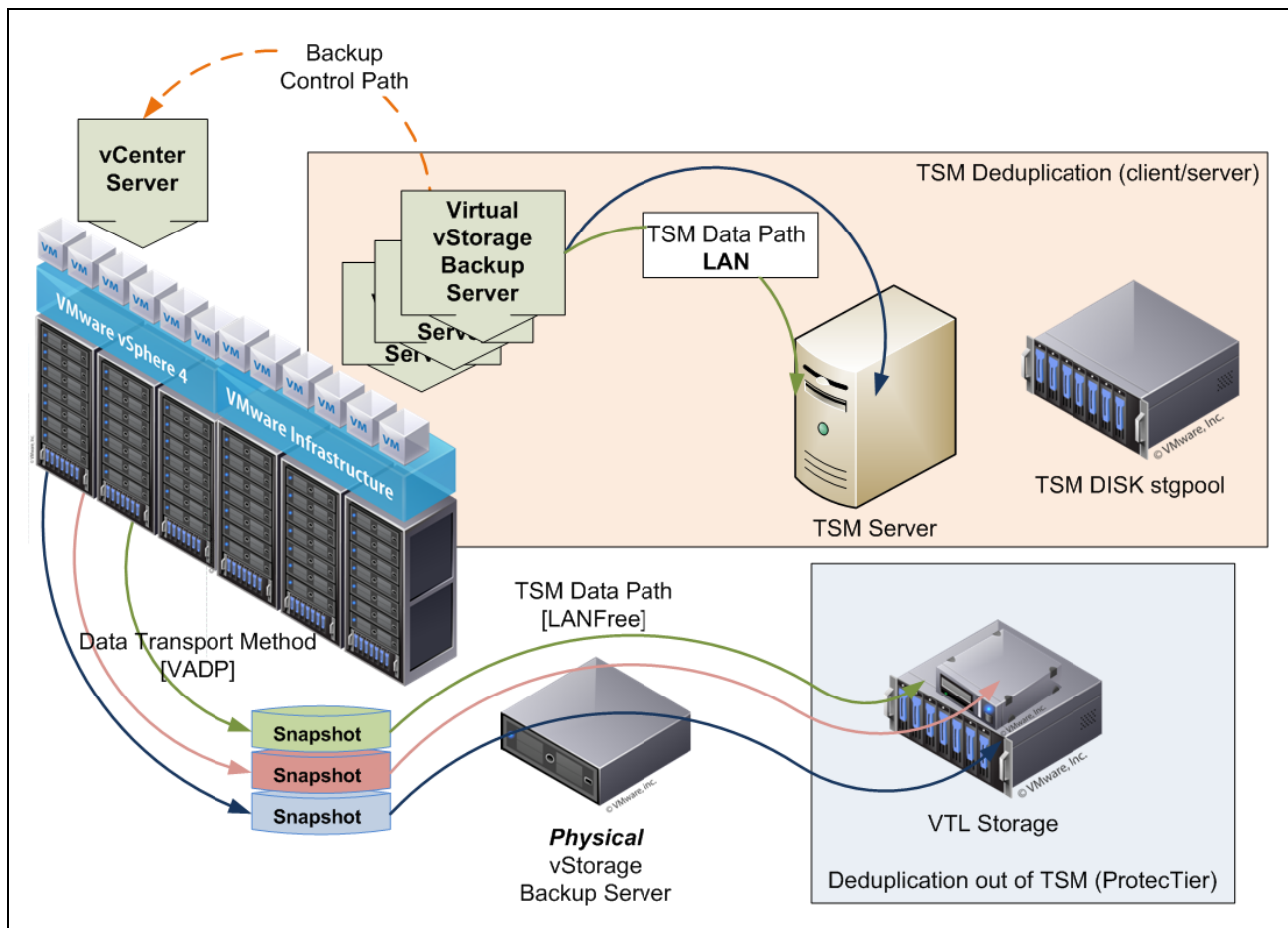


Figure 1-4 Tivoli Storage Manager: Big environment overview

In Figure 1-4 on page 9, the Red area at the top includes the Tivoli Storage Manager server. The vStorage Backup Server represents the area where the deduplication loads exists.

Blue area at the bottom includes the ProtecTier appliance or gateway, and represents the area where the deduplication load exists. In this case, the Tivoli Storage Manager server and the vStorage Backup Server machines are free of any load that is required by deduplication tasks.

1.4.3 Scenario 3: Shared environment

Tivoli Storage Manager for Virtual Environment - Data Protection for VMware can be implemented in a dedicated environment and in a shared one.

A shared environment includes the following examples:

- ▶ Virtual Machine to be managed separately (for example, multiple entities within same office)
- ▶ ESXi clusters to be managed separately (for example, one cluster per entity)
- ▶ Multiple vCenter Servers

In a shared environment, the small and big environment information that was provided in this chapter is still valid. In addition to this information, we describe here what should be considered and the design effects when the solution is implemented in a shared environment.

Depending on your environment, you might need to consider the implementation of Tivoli Storage Manager for Virtual Environment components as shared resources, for example, between different entities.

In a shared environment, one of the challenges is the security for connecting the VMware Infrastructure and to access the data after it is stored within Tivoli Storage Manager server. Some configuration can be done on the data mover node (the one that is accessing the VMware data and datastores) and on the data center node (the one managing the data after it was backed up to Tivoli Storage Manager server).

For more information about shared environment deployment, see 3.13, “Deploying Data Protection for VMware in a shared environment” on page 51.



Tivoli Storage Manager for Virtual Environments: Data Protection for VMware product introduction

Data Protection for VMware is a subset of Tivoli Storage Manager for Virtual Environments. Thus, in this publication, Data Protection for VMware can be used instead of Tivoli Storage Manager for Virtual Environments - Data Protection for VMware.

This chapter includes the following topics:

- ▶ Tivoli Storage Manager solutions to protect VMware vSphere Environments
- ▶ Data Protection for VMware Solution components
- ▶ New in Backup-Archive client and Data Protection for VMware V6.4
- ▶ Product requirements: Supported platforms

2.1 Tivoli Storage Manager solutions to protect VMware vSphere Environments

This document covers Data Protection for VMware and how to deploy it to protect VMware vSphere Environments. To give you a broader view of what is the Tivoli Storage Manager family to protect the data in VMware virtual machines, we review the following available features that you can use to protect your VMware environment:

- ▶ Tivoli Storage Manager Backup-Archive client within VMware guest
- ▶ Tivoli Storage Manager Backup-Archive client off host backup
- ▶ Data Protection for VMware DP for VMware
- ▶ FlashCopy Manager for VMware
- ▶ FlashCopy Manager within VMware guest
- ▶ IBM Tivoli Storage Manager FastBack® within a VMware guest

These options are described next.

2.1.1 Tivoli Storage Manager Backup-Archive client within VMware guest option

This option consists of protecting the data in the same way as for a physical machine. You can perform a backup (incremental or selective) or archive within the virtual machine, as shown in Figure 2-1 on page 13.

Note: The Backup-Archive client is supported within a virtual machine, as described in the IBM Technote that is available at this website:

<http://www-01.ibm.com/support/docview.wss?&uid=swg21239546>

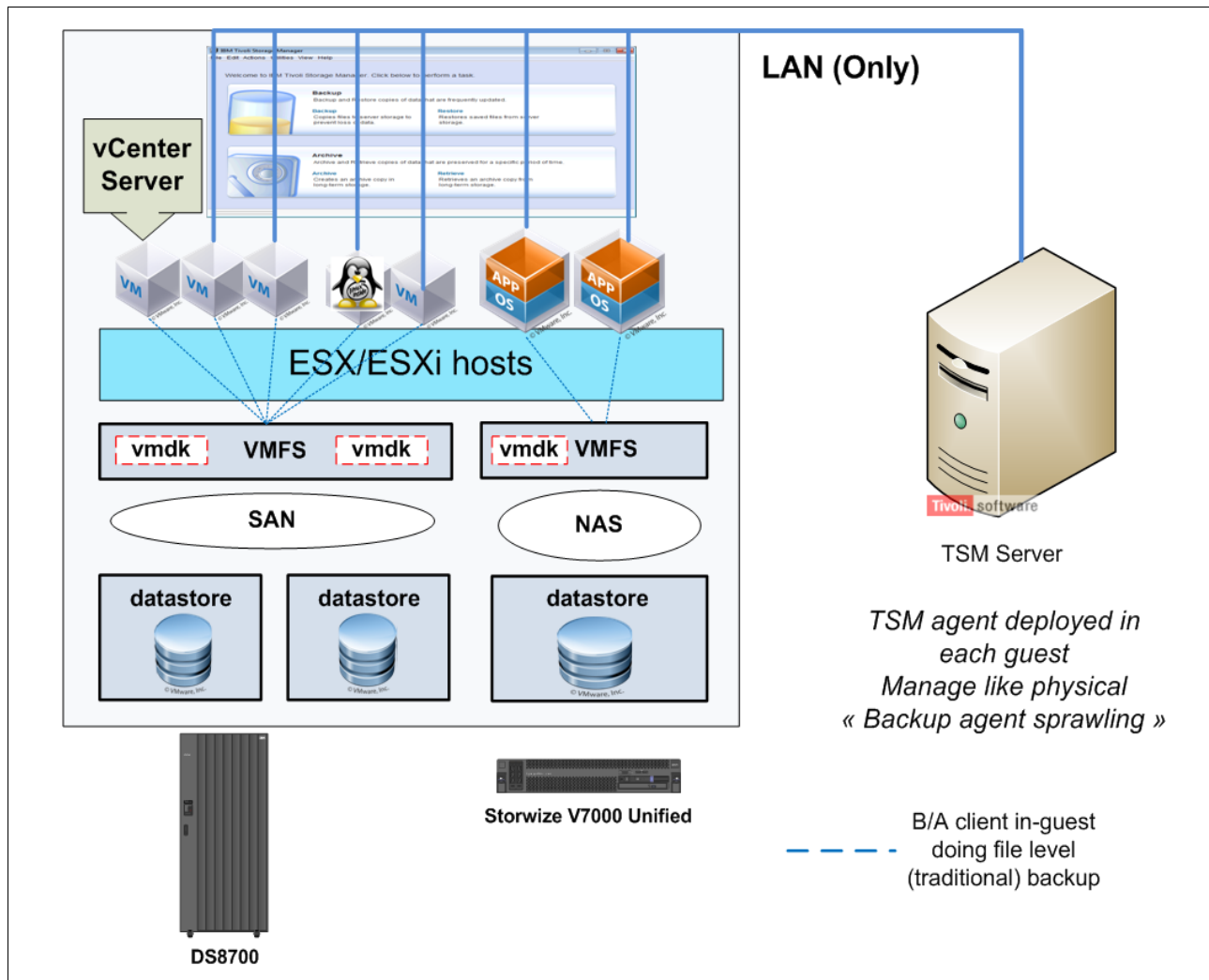


Figure 2-1 Backup-Archive client in-guest configuration

2.1.2 Tivoli Storage Manager Backup-Archive client off host backup option

As shown in Figure 2-2 on page 14, this option consists of making a snapshot of virtual machine (VM), full-vm FULL or full-vm INCREMENTAL. Data Protection for VMware includes an enablement file to upgrade the Backup-Archive client by adding incremental backups capability. It also includes a set of recovery features and a vSphere client plug-in.

The snapshot capability of the Tivoli Storage Manager Backup-Archive client was introduced in version 6.2. Snapshot capability means that the Backup-Archive client uses the VMware vStorage API for Data Protection (VADP) mechanism and relies on the VMware snapshot mechanism to back up the entire virtual machine. This option provides a fast, centralized, off-hosted, and scalable backup methodology.

For Windows virtual machines, you can perform a file-level backup by using the same snapshot functionality. This is called FULL-VM File Level backup (**VMbackuptype=File**), with which you can perform file-level restoration.

The file level backup method consists of making a new set of backup data without any relationship with the full-vm backups.

Note: The file-level backup is not supported for Linux virtual machine.

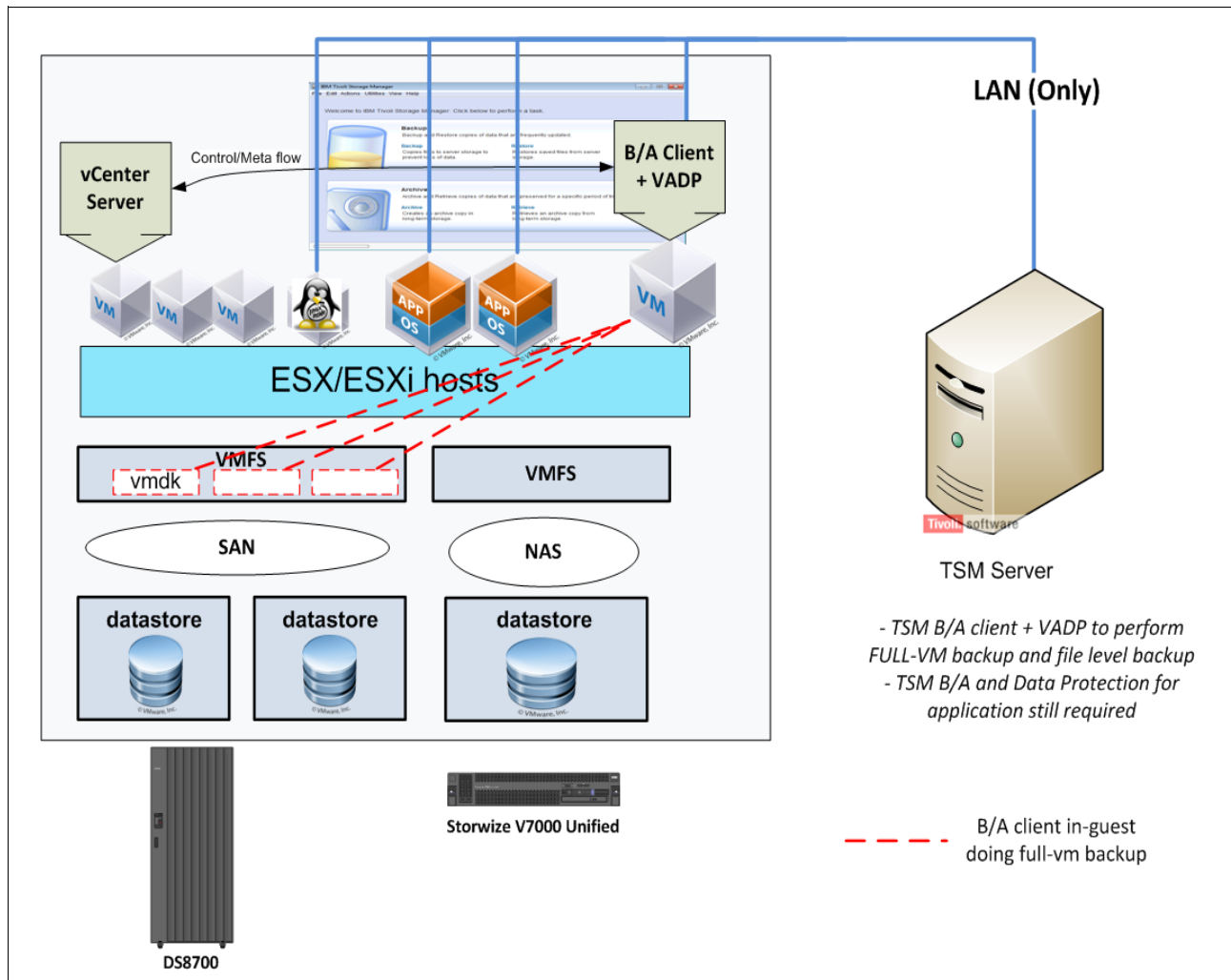


Figure 2-2 Backup-Archive client performing full-vm backup by using VMware API for Data Protection

2.1.3 Data Protection for VMware DP for VMware option

As shown in Figure 2-3, this option consists of making a snapshot of virtual machine, whether full-vm FULL or full-vm INCREMENTAL. Data Protection for VMware includes an enablement file to upgrade the Backup-Archive client by adding incremental backups capability. It also includes a set of recovery features and a vSphere client plug-in.

The recovery possibilities are: file recovery, virtual disk recovery, virtual machine recovery.

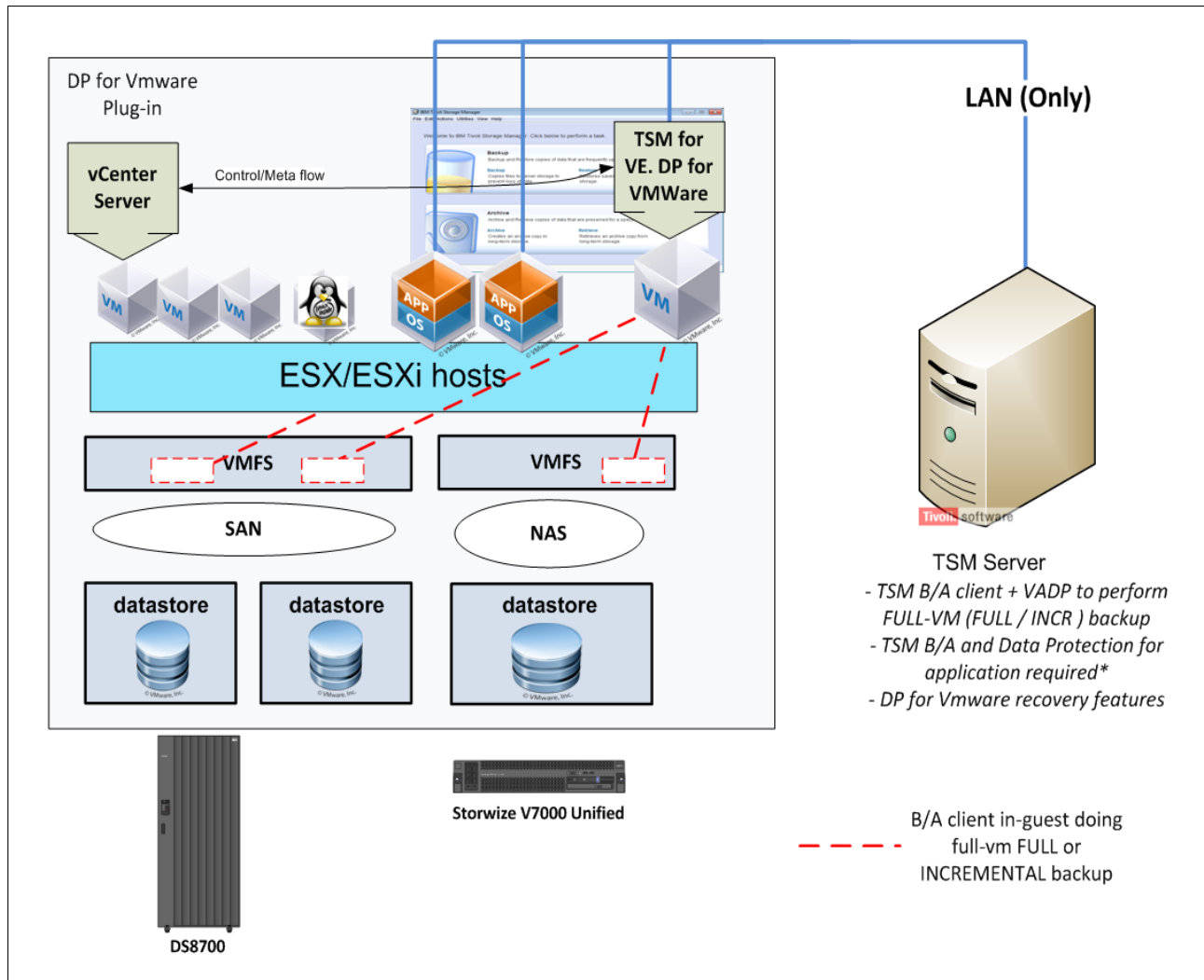


Figure 2-3 Backup-Archive client in-guest and Data Protection for VMware configuration

For more information about in-guest application protection, see 3.3, “Protecting applications in a virtual environment” on page 31.

2.1.4 FlashCopy Manager for VMware option

As shown in Figure 2-4, this option consists of making the snapshot at a datastore level by using Tivoli FlashCopy Manager for VMware. This solution is based on built-in FlashCopy (or snapshot) features of the back-end disk system.

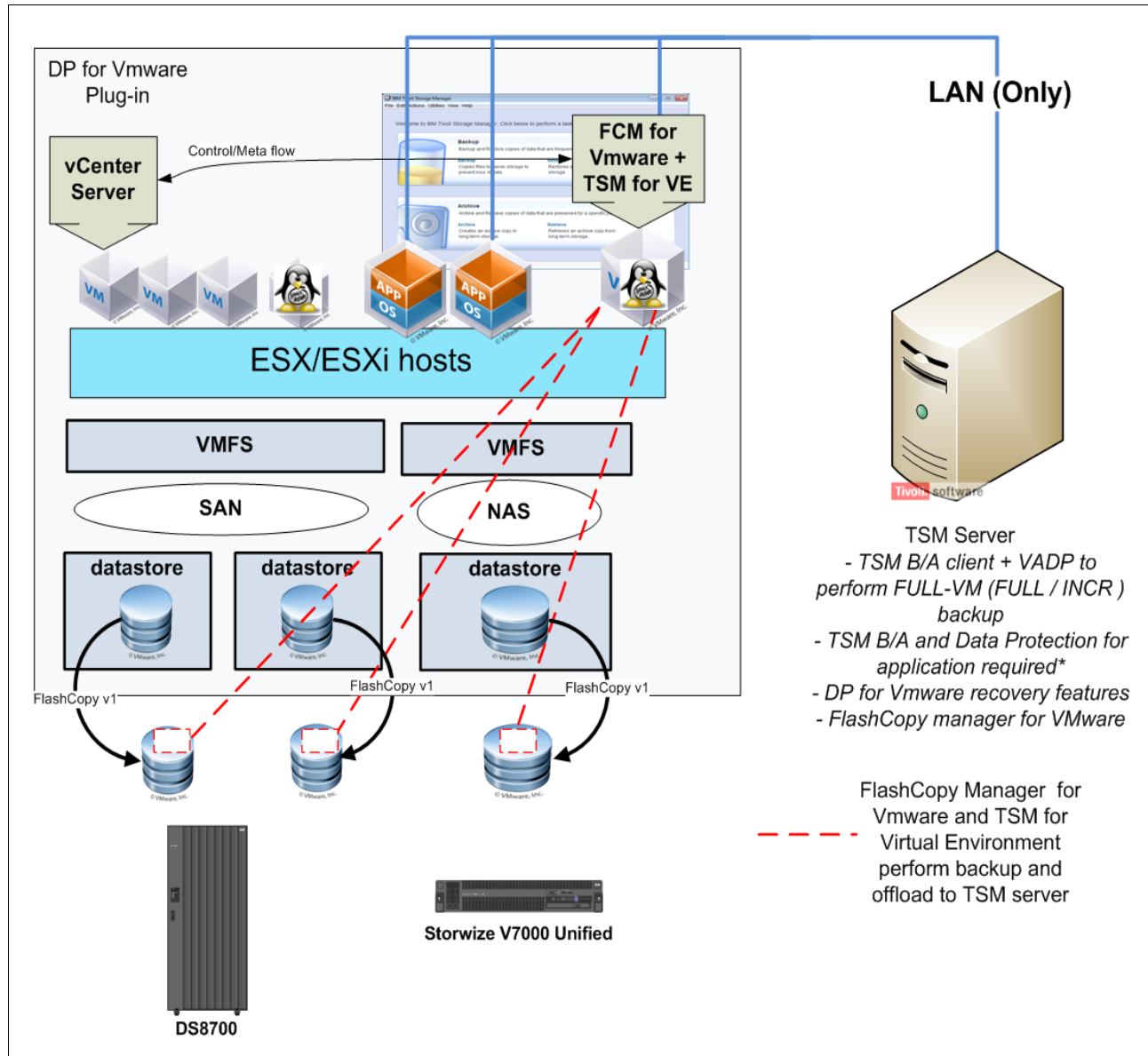


Figure 2-4 FlashCopy Manager for VMware configuration

The recovery possibilities are virtual disk, virtual machine, and datastore.

Tivoli FlashCopy Manager for VMware can also be combined with Data Protection for VMware so the FlashCopy images can be offloaded to the Tivoli Storage Manager server. This is important for providing disaster recovery capabilities that FlashCopy or snapshot solutions cannot provide on their own.

Tivoli FlashCopy Manager for VMware also brings its VMware vSphere plug-in, as does the Data Protection for VMware solution.

2.1.5 FlashCopy Manager within VMware guest option

As shown in Figure 2-5, this option consists of the use of FlashCopy Manager with the in-guest BA-Client to eliminate limitations of snapshots (such as, pRDM and clusters) while providing a powerful backup solution. These snapshot limitations are described in Chapter 3, “Planning the installation of Data Protection for VMware” on page 25.

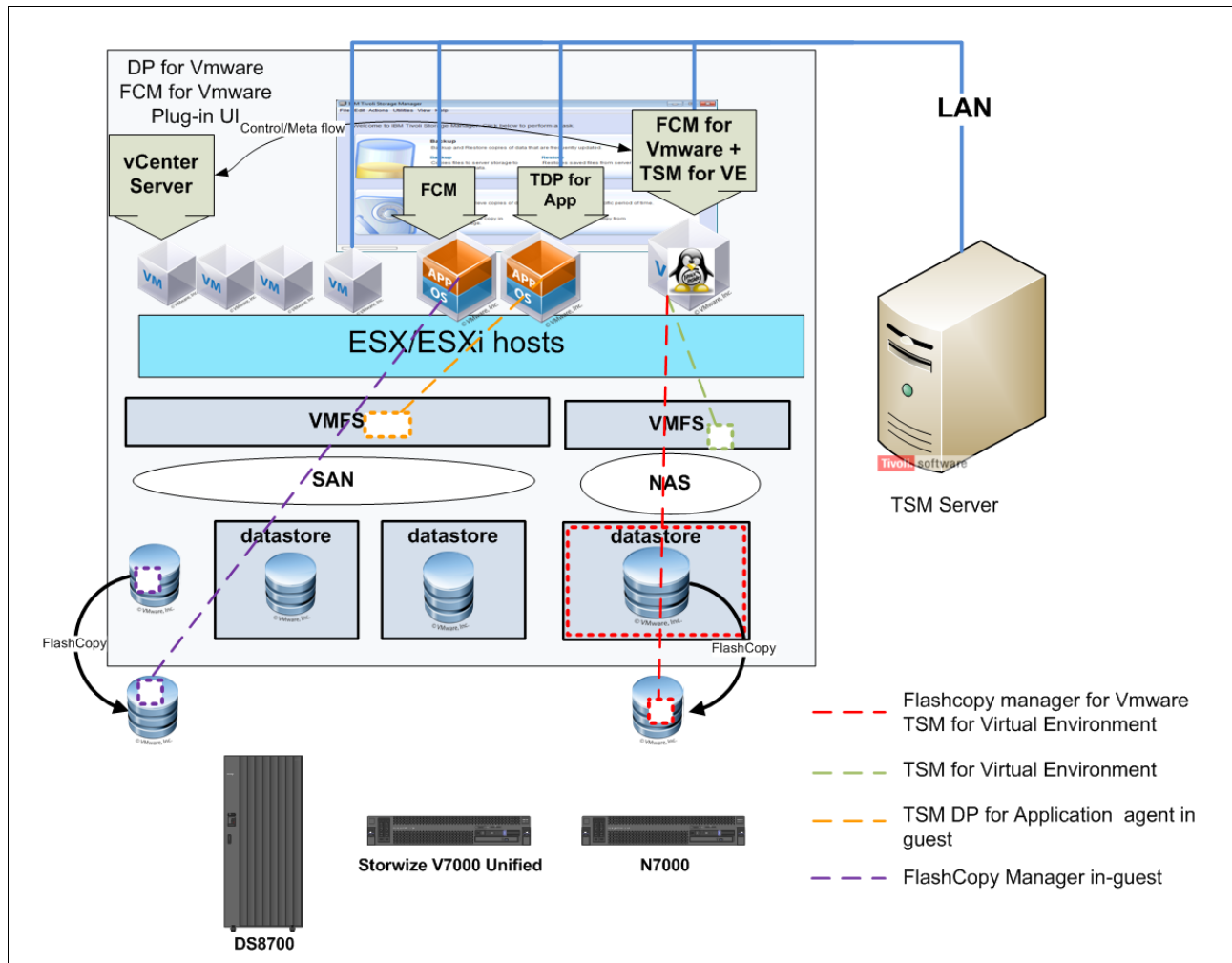


Figure 2-5 Combined configuration

You can use FlashCopy Manager in-guest and Data Protection for VMware to protect your data and all the virtual machines that do not host any database or database that is supported by the self-contained application protection. For more information, see 3.3, “Protecting applications in a virtual environment” on page 31.

2.1.6 Tivoli Storage Manager FastBack within a VMware guest option

This option uses Tivoli Storage Manager FastBack within the virtual machine. FastBack provides a lightweight, block-level incremental backup and near-instant restore solution for Windows and Linux guests. It can be effective for protecting smaller but critical application environments, and can be integrated with a Tivoli Storage Manager Server for a full service backup and recovery solution.

2.2 Data Protection for VMware Solution components

For more information about features and configuration information, see *Data Protection for VMware Installation and User Guide*, SC27-2898, which is available at this website:

http://pic.dhe.ibm.com/infocenter/tsminfo/v6r4/topic/com.ibm.itsm.ve.doc/b_ve_inst_user.pdf

Figure 2-6 shows how Data Protection for VMware looks and how its components interrelate with VMware and Tivoli Storage Manager server.

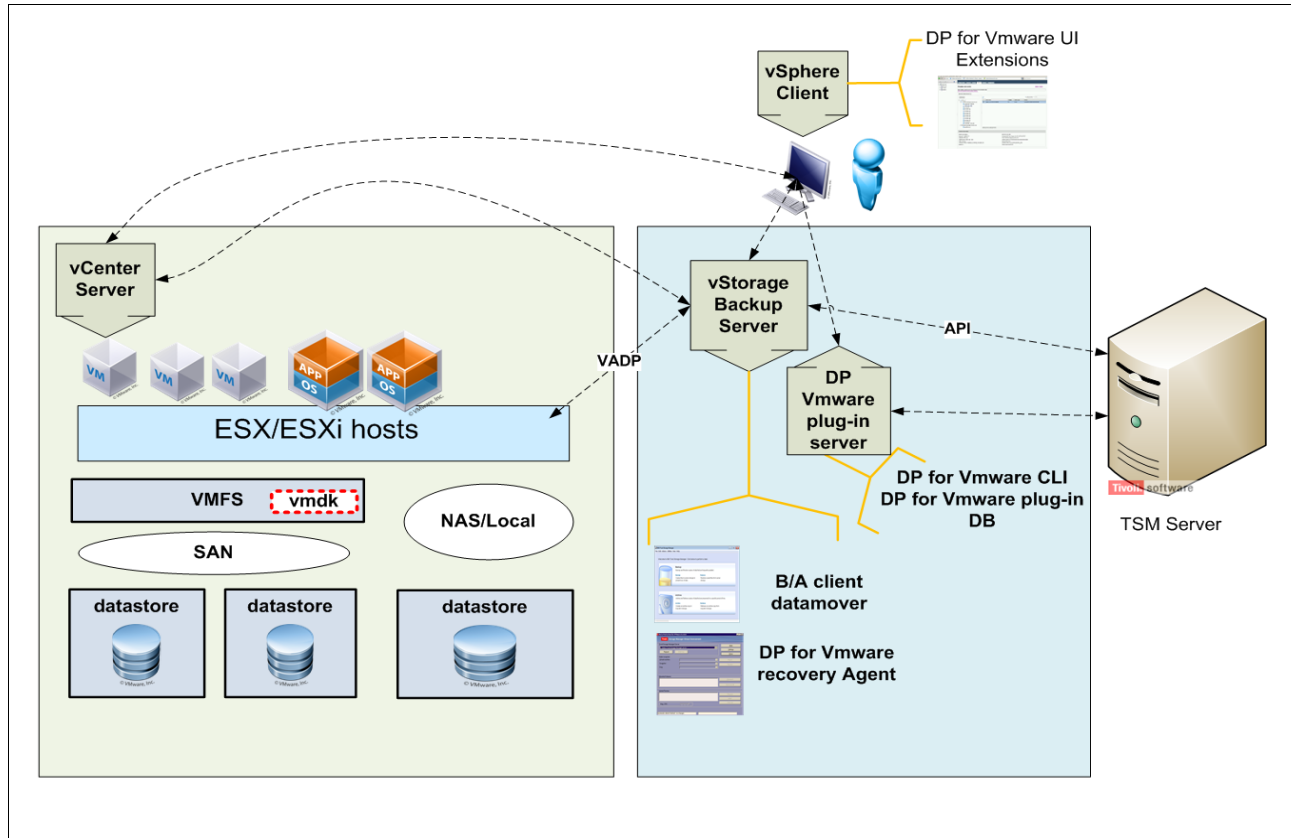


Figure 2-6 Data Protection for VMware components overview

2.2.1 Component definitions

In this section, we describe the Data Protection for VMware components that shown in Figure 2-6.

vStorage Backup Server

This is the machine where the Backup-Archive client is installed. The vStorage Backup Server can be a Virtual Machine or separate physical machine. For more information about how to choose between virtual or physical, see 3.6.2, “vStorage Backup Server: Physical versus virtual” on page 39.

Tivoli Storage Manager Backup-Archive client data mover

The data mover is an instance of the Backup-Archive client program, and is configured on a vStorage Backup Server. Thus, you can install the Backup-Archive client on a single vStorage Backup Server and create several logical instances or data movers from this single installation.

This component provides the following functionality:

- ▶ **FULL-VM backup**

Backs up virtual machines to Tivoli Storage Manager Server storage. Full VM backup copies the VM configuration information and performs a block level copy of VM disks to the Tivoli Storage Manager Server. The VM disk backup process involves reading blocks from a VMware guest disk snapshot by using the vStorage APIs for Data Protection (VADP) and writing the data to the Tivoli Storage Manager server by using the Tivoli Storage Manager API. These backups are managed and retained according to storage policies that are set up by the Tivoli Storage Manager administrator. The FULL-VM backup operation does not require a Data Protection for VMware license.

- ▶ **INCREMENTAL VM backup**

Backs up only the virtual machine data that changed since the last backup completed. The Backup-Archive client data mover relies on VMware's Change Block Tracking (CBT) to determine the changed blocks. The Data Protection for VMware license (which is included with the Data Protection for VMware installation package) is required to enable incremental backup in the Backup-Archive client data mover.

- ▶ **FULL-VM restore**

Restores a full or incremental VM backup. The entire VM (the VM configuration and VMDKs) is restored to the state it existed in when it was originally backed up.

The Backup-Archive client data mover can run on a Windows or Linux vStorage Backup Server and cross platform operations are supported. A Windows Backup-Archive client data mover can back up a Linux VM, and vice versa. A backup that is performed by a Linux proxy can be restored by a Windows proxy, and vice versa.

The Backup-Archive client data mover is not provided as part of the Data Protection for VMware installation package, but is a prerequisite. For more information, see *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients: Installation and User's Guide*, SC23-9791, and *IBM Tivoli Storage Manager for Windows Backup-Archive Clients: Installation and User's Guide*, SC23-9791, which are available at this website:

<http://publib.boulder.ibm.com/infocenter/tsminfo/v6r4/index.jsp>

Data Protection for VMware Recovery Agent

This agent is part of the Data Protection for VMware installation package and provides the following functionality:

- ▶ **File restore**

File restore can be performed in-guest or off-host on supported Windows and Linux machines. File restore is accomplished by using the DP for VMware Recovery Agent Mount function to expose a virtual disk snapshot from a Tivoli Storage Manager storage pool and copy the required files. The user chooses whether to expose a complete disk as an iSCSI LUN or a single partition from the selected disk as a local volume.

- Instant restore of a volume

Instant restore is a method of restoring the contents of a single volume that provides the user or application on-demand access to data while a background process restores the entire volume contents. To the user or application, the volume appears to contain all the restored data, even though the restore process is in-progress. Instant restore can be done from a full or incremental virtual machine backup. Instant restore is performed by using the DP for VMware Recovery Agent's Instant Restore function. Mount and Instant restore can use full or incremental backups that were created with the Backup-Archive client data mover.

Data Protection for VMware vCenter plug-in

This is the Tivoli Storage Manager extension to VMware vSphere windows client. This extension enables management of full VM backup and restore operations for multiple Backup-Archive client data mover nodes.

This plug-in is part of the Data Protection for VMware installation package. The VM command-line interface (VMCLI) for the vCenter plug-in also is provided.

The plug-in is powered by IBM WebSphere® application server engine and Derby database. Those components are installed on the vStorage Backup server or a separate machine.

Tivoli Storage Manager Server

The Tivoli Storage Manager Server provides the backup repository for the virtual machines that are protected.

2.3 New in Backup-Archive client and Data Protection for VMware V6.4

In this section, we describe the major enhancements that are new in version 6.4 of the Backup-Archive client and Data Protection for VMware. These enhancements help you with deployment, provide a fast and optimized backup method, and improve ease of administration.

For more information, see *IBM Tivoli Storage Manager for Virtual Environments Data Protection for VMware Installation and User Guide*, SC27-2898, which is available at this website:

http://publib.boulder.ibm.com/infocenter/tsminfo/v6r4/topic/com.ibm.itsm.ve.doc/b_ve_inst_user.pdf

2.3.1 Incremental forever backup processing

Virtual Machine incremental backup is achieved by using the Changed Block Tracking (CBT) VMware feature. In addition to the incremental capability, CBT is used to provide content aware backups to back up used areas of a disk only.

Incremental-forever backup uses Tivoli Storage Manager grouping technology to create synthetic-full recovery points by combining required blocks from previous backups with the changes from incremental backups that capture only new or changed data.

An incremental forever backup strategy minimizes backup windows while providing faster recovery of your data. Data Protection for VMware 6.4 provides a new 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 the following 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 because only changed blocks are identified.
- ▶ Minimizes impact to the client system.
- ▶ It reduces the length of the backup window.

In addition, the restore process is optimized because only the latest versions of blocks that belong to a restored backup are restored. Because the same area on the production disk is recovered only one time, the same block is not written to multiple times as implemented in older 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 use of the Periodic Full backup strategy.

Note: Incremental Forever backup processing relies on Change Block Tracking VMware feature. This feature is available under following conditions:

- ▶ The virtual machine that owns the disks to be tracked must be hardware version 7 or later (review the VM version information in the vSphere Client, Virtual Machine summary tab, or use the `dsrmc show vm all` command to display this information after the Backup-Archive client is configured to access the virtual center server).
- ▶ The host must be ESX/ESXi 4.0 or later.
- ▶ Virtual machine storage must not be (persistent or non-persistent) independent disk, meaning unaffected by snapshots.

Be aware that some events affect the CBT feature, thus on the Tivoli Storage Manager Incremental forever backup processing. The CBT might reset or lose track of incremental changes in following conditions:

- ▶ Power failure or hard shutdown.
- ▶ In vSphere 4.1 and earlier, Cold Migration (but not Storage vMotion) can reset but not disable CBT.
- ▶ In vSphere 5.0 and 5.1, Storage vMotion resets CBT.

2.3.2 Configuration wizard

Data Protection for VMware vCenter plug-in configuration no longer requires manual input. Use the wizard for an initial Data Protection for VMware vCenter plug-in configuration or to change the Tivoli Storage Manager Server, vCenter node, or VMCLI node.

2.3.3 Parallel backup from a single Tivoli Storage Manager instance

Protect VMware Environments by implementing parallel processing sessions with a single data mover (one Tivoli Storage Manager Backup/Archive client instance). This can be achieved by using the new parameters `vmmaxparallel`, `vmllimitperhost`, and `vmllimitperdatastore`.

2.3.4 Expanding VM backup criteria

Advanced criteria was added, so you can back up VMs by specifying the ESXi hosts cluster name, data store name, or wildcard character for virtual machine name.

2.3.5 Controlling which disks in the VMware environment are processed

When large virtual disks exist inside the virtual machines or when another application protects these disks, you can exclude these disks during routine virtual machine backup or restore operations.

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 that is 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.

2.3.6 Protecting applications that run in virtual machine guests

Data Protection for VMware protects Microsoft Exchange Server and Microsoft SQL Server applications that run inside virtual machine guests. Data Protection for VMware V6.4 backs up VM guests with 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

This feature is called self-contained applications protection.

Note: For more information about how to protect applications in a virtual environment, see 3.3, “Protecting applications in a virtual environment” on page 31.

2.3.7 Preserving VMware configuration attributes

A list of VMware configuration attributes that are preserved by Data Protection for VMware is provided in the Data Protection for VMware User guide, check “Preserving VMware configuration attribute information”.

For more information about the VMware configuration attributes that it managed, see this website:

http://pic.dhe.ibm.com/infocenter/tsminfo/v6r4/index.jsp?topic=%2Fcom.ibm.itsm.ve.doc%2Fr_ve_configattrib.html

2.3.8 Virtual machine templates and vApps

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

VM templates

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 in a vApp

The VMs in a vApp are identified in the Data Protection for VMware vCenter plug-in as VMs. While you can 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.

2.3.9 View VM backup status reports

By using the Data Protection for VMware vCenter plug-in, you can generate reports about the backup status of the VMs that are managed in the specified VMware data center domain. This function is based on the authority level that is assigned to your Tivoli Storage Manager administrator ID.

2.3.10 Secure Sockets Layer communication

Secure Sockets Layer (SSL) allows industry standard SSL-based secure communications between the Data Protection for VMware vCenter plug-in and the Tivoli Storage Manager server.

2.3.11 Role-based usage

Different Data Protection for VMware vCenter plug-in functions are based on the authority level that is assigned to your administrator ID. For more information about these roles, see *IBM Tivoli Storage Manager for Virtual Environments Data Protection for VMware Installation and User Guide*, SC27-2898.

2.3.12 Data Protection for VMware vCenter plug-in error messages

A complete list of GVM-prefix error messages is included in this release. For more information, see the appendix of *IBM Tivoli Storage Manager for Virtual Environments Data Protection for VMware Installation and User Guide*, SC27-2898.

2.4 Product requirements: Supported platforms

For more information about the hardware and software requirements for Data Protection for VMware V6.4, see this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg21611903>

We assume in this book that all the requirements are known and they are met.



Planning the installation of Data Protection for VMware

Data Protection for VMware must interrelate with several existing components, such as, the VMware infrastructure, identity management (for example, Active Directory), and the Tivoli Storage Manager backup server. The planning should cover subjects that must be answered before you start to implement the product.

This chapter describes the following requirements and goals you should meet when you are planning the installation:

- ▶ Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO): This helps you to estimate the backup frequency and required storage space.
- ▶ What type of restoration is needed (file, full-vm, or both)?
- ▶ Are there any applications that are hosted in VMware guests? If yes, consider the use of Tivoli Data Protection in-guest agent.
- ▶ Is there any virtual machine that cannot use or support snapshots?
What are the alternative solutions (in-guest Tivoli Storage Manager installation)?
- ▶ Do you need more than one backup policy?
- ▶ How many vCenter servers must you manage?
- ▶ What backup strategy fits best to your environment and requirements?
- ▶ What is the effect on the operational teams?
Distributing the new data protection roles and responsibilities

This chapter includes the following topics:

- ▶ Collecting and consolidating data protection policies
- ▶ Learning about the Virtual Environment to protect it
- ▶ Protecting applications in a virtual environment
- ▶ Communication ports between VMware and Tivoli Storage Manager components
- ▶ Choosing your backup strategy

- ▶ vStorage Backup Server
- ▶ Storage location versus recovery features
- ▶ Determining the location to start backup or restore
- ▶ Effect of Data Protection for VMware backups on the Tivoli Storage Manager Server
- ▶ VMware snapshots considerations
- ▶ Data Protection for VMware considerations
- ▶ Tivoli Storage Manager node naming convention for Data Protection for VMware resources
- ▶ Deploying Data Protection for VMware in a shared environment

3.1 Collecting and consolidating data protection policies

Two of the most important things when talking about data protection are the RTO and RPO. These two concepts define the backup frequency, retention policy, and the recovery constraints that lead to a consistent implementation of Data Protection for VMware as a data protection solution.

RTO refers to the amount of time it takes to restore a data set or application following a service disruption. RPO refers to the frequency of backups, and, therefore, the available recovery points in time to restore from.

In addition to RTO and RPO values, you must know the retention policy; that is, how long to keep the data on the Tivoli Storage Manager server storage.

Note: Multiple retention policies affect Data Protection for VMware implementation, which can lead to the creation of multiple sets of configurations.

3.2 Learning about the Virtual Environment to protect it

This section focuses on the relevant pieces of information you must collect when you are planning your deployment.

3.2.1 VMware infrastructure

The following information must be provided to better understand what the working area looks like. It consists of identifying the VMware components and how they might constrain the solution implementation:

- ▶ vSphere Version and vSphere information:
 - vSphere version?
 - vSphere Server IP address?
 - Is the vSphere Server virtual or physical? Is it clustered?
 - Where is the vSphere Server database? What is the database engine?
 - Is there is a naming convention for the Virtual Machine?
- ▶ Collect the following formation regarding the possible movement of virtual machine, which might affect the backup tasks:
 - Is there is any replication mechanism, such as, VMware Site Recovery Manager (SRM)?
 - Is the VMware Distributed Resource Scheduler (DRS) activated? If yes, which level of automation is configured?

Depending on how you configure the backup tasks, you should pay attention to these two VMware features (DRS and SRM) to avoid duplicated backups and prevent any failure because of a lack of access to new ESXi hosts and datastores, which are involved in the SRM movements.

For example, you have one datamover node that is dedicated to each ESXi host with proxynode relationship to a specific datacenter node. In such a case, if a virtual machine moved from one ESXi host to another via DRS (for instance), this can lead to the creation of multiple backups onto multiple datacenter nodes, thus performing several duplicate full backups.

Note: As part of the deployment, you must ensure that the vCenter Server and its database are protected. Data protection of this critical machine is done by installing Tivoli Storage Manager Backup-Archive client to protect files, and Tivoli Data protection agent for MS-SQL to protect the MS-SQL database. Whether the vCenter server is virtual, it should not be backed up by using Data Protection for VMware or any other snapshot-based backup. For more information about how to protect the vCenter Server, see this website:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1023985

- ▶ Datastore List, Type, Size, and BlockSize:
 - By using a list of datastores with their type, you can identify the different back-end disk attachment type. It is also the place to identify any Raw Device Mapping (disk that is directly connected to a Virtual Machine).
 - Is there is a relationship between a datastore and a virtual machine type? Are the virtual machines mixed up on datastore or is there is a rule for classifying them?
 - Gather the block size value for every datastore.
- ▶ ESXi Hosts topology: Collect information about datacenter and ESX/ESXi cluster:
 - It is important to understand the layout of the datacenter (or datacenters) that are managed by each Virtual Center Server. This helps to have a full picture of the Tivoli Storage Manager Nodes hierarchy and relationship. For more information, see 4.1.1, “Tivoli Storage Manager server configuration” on page 61.
 - Is there a rule that enforces each ESXi cluster to be isolated from all others?
- ▶ Virtualization level of your infrastructure:
 - Is the infrastructure 100% virtualized?
 - Is it possible to set up a physical machine to protect your VMware infrastructure?
- ▶ User ID management:
 - How is the USER ID management handled within the virtual environment?
 - Is there is a global or centralized user ID management; for example, LDAP or Active Directory?
- ▶ VMware administrators technical skills
 - Are they aware of Tivoli Storage Manager and its data protection concepts?

3.2.2 Virtual Machines

When talking about the virtual machine (VM), collect the following information that has a direct effect on the way the data protection solution is implemented:

- ▶ VM name and VM host name
- ▶ VM operating system
- ▶ Disk size
- ▶ VM disk characteristics (such as, vDisk, vRDM, pRDM)

- ▶ In-guest Application
- ▶ VMware hardware level for the Change Block Tracking feature availability
- ▶ Bus sharing and clustered machine
- ▶ Backup policy
- ▶ Comments

The following information also might be helpful:

- ▶ Member of a vApp?
- ▶ Backup windows: When can the VM be backed up?

Table 3-1 shows the minimum information that must be gathered when the deployment is planned.

Table 3-1 Example of deployment planning sheet to collect machine information

VM name	Operating system	Disk size (GB)	Disk type	In-guest application	VMware hardware level	VM bus sharing enabled (clustered)	Backup policy	Comments
RAPHEL	Linux	120	VDisk	Oracle	7	No	Daily +21 days	N/A
CLEMENCE	Windows	500	VDisk pRDM	N/A	8	No	Daily +7 days	File Server

Note: If a virtual machine is a member of a vApp, it is important to collect this information because it might be necessary to back up all of these virtual machines around the same time.

3.2.3 vCenter Server credentials considerations

VMware infrastructure management components often are integrated to User ID management tools, such as, Active Directory or Lightweight Directory Access Protocol (LDAP) catalogs. Credentials that are used by Data Protection for VMware features (Data Protection for VMware vCenter plug-in account and backup/recovery account) can also be managed by using User ID management tools.

To complete its data protection tasks, Data Protection for VMware must have credentials that are defined on the vCenter Server, with specific privileges per the IBM Technote that is available at this website:

<https://www-304.ibm.com/support/docview.wss?uid=swg21497028>

The vCenter server account that is created for data protection purposes does not include privileges to install the Data Protection for VMware vCenter plug-in. To install this plug-in, you need a privileged account.

However, if you plan to use the same user for vCenter plug-in usage and installation, you need the following extension privileges to be enabled (in the vSphere client, Roles management panel):

- ▶ Extension - Register extension
- ▶ Extension - Unregister extension
- ▶ Extension - Update extension

Note: We advise that you create a VMware role that is dedicated to Tivoli Storage Manager activities. If this is done, it is easier to manage later.

3.2.4 Data Protection for VMware vCenter plug-in user roles

The Data Protection for VMware vCenter plug-in provides an interface with which you can perform backup and recovery tasks. To achieve this, there is a connection between the vCenter plug-in and the Tivoli Storage Manager server that requires a Tivoli Storage Manager administrator ID to be defined and associated to the plug-in.

The availability of Data Protection for VMware vCenter plug-in functions is based on the authority level (classes) that is assigned to your Tivoli Storage Manager administrator ID.

Depending on which tasks you must control from the vCenter plug-in, you might need a different level of Tivoli Storage Manager user authority. For more information about these levels, see *IBM Tivoli Storage Manager for Virtual Environments Data Protection for VMware Installation and User Guide*, SC27-2898.

Figure 3-1 shows the Tivoli Storage Manager administrative privilege that is needed to use the Data Protection for VMware plug-in GUI.

	Role 4	Role 3	Role 2	Role 1
Summary	<i>Run now backup and restore</i>	<i>Role 4 plus reporting</i>	<i>Role 3 plus schedule operations for listed policy domains</i>	<i>All functions, including initial configuration</i>
Tivoli Storage Manager Admin ID Privilege Class	None	One of the following: Storage Operator Analyst	Policy (Restricted) or one of the following: Storage Operator Analyst	Policy (Unrestricted) or System
Backup Tab				
Run now backup	Yes	Yes	Yes	Yes
Scheduled backup	No ¹	No ¹	Yes within policy domains	Yes
View only (Managing Backup Schedules)	No	Yes	Yes	Yes
Delete a schedule (Managing Backup Schedules)	No ²	No ²	Yes within policy domains	Yes
Restore Tab				
Restore	Yes	Yes	Yes	Yes
Reports Tab				
Events	No	Yes	Yes	Yes
Recent Tasks	Yes	Yes	Yes	Yes
Backup Status	No	Yes	Yes	Yes
Data Center Occupancy	No	Yes	Yes	Yes
Configuration Tab				
Node Registration (Configuration Wizard)	No	No	No ³	Yes
Change Tivoli Storage Manager Admin ID Credentials (Edit Configuration Notebook)	Yes	Yes	Yes	Yes
Change VMCLI Node Password (Edit Configuration Notebook)	No	No	Yes	Yes
Change Plug-in Domains (Edit Configuration Notebook)	Yes ⁴	Yes ⁴	Yes ⁴	Yes
Change Data Mover Nodes (Edit Configuration Notebook)	No	No	No ³	Yes

1. When both Data Protection for VMware vCenter plug-in and Tivoli Storage FlashCopy® Manager for VMware are installed, an offloaded backup schedule is supported.
2. Run now schedules can be deleted. Scheduled backups cannot be deleted.
3. You cannot register the node because an unrestricted domain policy is required.
4. You can add or remove data centers; however, you cannot register data center nodes and their associated data mover nodes.

To view the Tivoli Storage Manager administrator ID authority level and corresponding Data Protection for VMware vCenter plug-in plug-in role:
1. Go to the Configuration window.
2. Click **Edit Configuration**.
3. The relevant information is shown on the Tivoli Storage Manager Server Credentials page.

Figure 3-1 Tivoli Storage Manager administrative privilege needed to use the Tivoli Storage Manager for VE plug-in GUI

This information is also available in the IBM Technote that is available at the following website:

http://pic.dhe.ibm.com/infocenter/tsminfo/v6r4/index.jsp?topic=%2Fcom.ibm.itsm.ve.doc%2Ffc_ve_tsmadmin.html&resultof%3D%2522%2572%256f%256c%2565%2522%2520

3.3 Protecting applications in a virtual environment

In this section, we describe how to handle application data protection in a virtualized VMware vSphere environment.

This section focuses on data protection for database and application products that are often hosted in VMware virtual server environments and gives guidance on choosing between the following generic types of data protection:

- ▶ Off-host data protection solutions that feature a backup/recovery agent that can be hosted off the hypervisor host, specifically Data Protection for VMware and Tivoli Storage FlashCopy Manager for VMware.
- ▶ In-guest data protection solutions that require the deployment of a backup/recovery agent in the guest machine; for example, Tivoli Storage Manager for Mail - Data Protection for Microsoft Exchange or Tivoli Storage Manager for Databases - Data Protection for Microsoft SQL.

There are several considerations that must be taken into account when you are choosing the appropriate data protection solution, including RTO, RPO, the type of storage (for example, virtual disks versus raw device mapping [RDM] disks), storage vendor, data layout, Tivoli Storage Manager server configuration, and long-term recovery requirements. While this section does not provide exhaustive details about all of these factors, it is meant as a starting point in evaluating different options that are available.

For more information, see this website:

<https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Storage%20Manager/page/Tivoli%20Storage%20Manager%20for%20Virtual%20Environments>

3.3.1 MS-SQL data protection

Figure 3-2 shows the product positioning when an MS-SQL database is protected.

use case	in-guest data protection	off-host data protection
SQL Server deployments that meet all the following conditions: • No Clustering • No need for recovery to an arbitrary PIT via transaction logs • No need to restore individual DBs or have native SQL backups to virtual disk within the VM	Use of an in-guest backup agent is not recommended. VM level backups will provide sufficient protection.	<i>Off-host agent:</i> <i>Data Protection for VMware or FlashCopy Manager for VMware</i> Off-host data protection for SQL databases is dependent on the recovery mode that has been configured: • For SQL databases configured in simple recovery mode, either Data Protection for VMware or FlashCopy Manager for VMware is recommended. • For SQL databases configured in standard recovery mode, Data Protection for VMware is recommended as it provides the ability to truncate logs after a successful backup operation.
SQL Server deployments that meet any of the following conditions: • Clustered servers (MSCS or VCS) • Always On Availability Groups deployed • Recovery to a arbitrary PIT via transaction logs is required • Recovery of a single database without disrupting other databases on the same server is required	<i>In-guest agent:</i> <i>Data Protection for Microsoft SQL or FlashCopy Manager for Windows</i> Use of an in-guest backup agent is recommended.	Data Protection for VMware and FlashCopy Manager are not recommended for these type of SQL deployments and use cases:

Figure 3-2 In-guest MS-SQL data protection product positioning

3.3.2 Exchange data protection

Figure 3-3 shows the product positioning when an Exchange database is protected.

use case	in-guest data protection	off-host data protection
Exchange single-instance deployments that meet all the following conditions: • No clustering • No Database Availability Group (DAG) configurations • No special RPO requirements which would necessitate log recovery	<i>in-guest agent:</i> <i>Data Protection for Microsoft Exchange</i> or <i>FlashCopy Manager for Windows</i> If you have deployed FlashCopy Manager for VMware to protect your virtual machine environment, in-guest backups are recommended.	<i>Off-host agent:</i> <i>Data Protection for VMware</i> Data Protection for VMware is recommended for stand-alone instances of Exchange • Exchange transaction logs can be configured to be truncated after a successful backup operation • IBM Tivoli Storage Manager FastBack for Exchange can be used in conjunction with full VM backups to achieve message level recovery
Exchange deployments for which any of the following conditions exist: • Clustered servers • Database Availability Group (DAG) configurations • RPO requirements which necessitate log recovery	<i>in-guest agent:</i> <i>Data Protection for Microsoft Exchange</i> or <i>FlashCopy Manager for Windows</i> In-guest backups are recommended In-guest backups provide the following advantages: • Recovery of individual databases and/or servers can be coordinated with other resources (e.g., for clustered servers or DAG configurations) • Recovery to specific point-in-time states based on log recovery can be achieved to satisfy RPO requirements Message level recovery can be achieved through the native in-guest agent interfaces	Data Protection for VMware and FlashCopy Manager are not recommended for these type of Exchange deployments and use cases:

Figure 3-3 In-guest Exchange data protection product positioning

3.3.3 Active Directory data protection

Figure 3-4 shows the product positioning when an Active Directory is protected.

use case	in-guest data protection	off-host data protection
Active Directory - stand-alone domain controller configuration	<i>in-guest agent:</i> <i>Windows Backup-Archive client</i> In-guest backup of Microsoft Active Directory is only recommended if the customer requires object-level recovery of Active Directory objects which is only available in the Backup-Archive client	<i>Off-host agent:</i> <i>Data Protection for VMware or FlashCopy Manager for VMware</i> Data Protection for VMware and/or FlashCopy Manager for VMware are the recommended solutions for Active Directory servers deployed on stand-alone domain controllers
Active Directory - multiple domain controller configuration	<i>in-guest agent:</i> <i>Windows Backup-Archive client</i> In-guest backups of Microsoft Active Directory is recommended when protecting Active Directory deployments on multiple domain controllers • The Windows Backup-Archive will notify all participating domain controllers during a recovery operation so that the Active Directory synchronization mechanism is properly notified. • Object-level recovery of Active Directory objects is supported.	Data Protection for VMware and FlashCopy Manager for VMware are not recommended for this type of Active Directory deployment:

Figure 3-4 In-guest Active Directory Data protection product positioning

3.3.4 Unstructured data protection

Figure 3-5 shows the product positioning when virtual machines with unstructured data are protected.

Windows and Linux virtual servers (unstructured data)	On an exception basis, consider in-guest backups of Windows virtual machines hosting file/web servers (unstructured) data for the following use cases. <i>in-guest agent:</i> <i>Windows Backup-Archive client or Linux Backup-Archive client</i> Deployment of the Windows Backup-Archive client should be considered for virtual machines that have specific backup policies on individual files/directories which cannot be satisfied by off-host backup or when administrators expect to receive a large volume of file-level restore requests. The in-guest backup should be limited to only the files/directories with special policy/management considerations. <i>in-guest agent:</i> <i>FlashCopy Manager for Windows or FlashCopy Manager for Linux</i> Deployment of FlashCopy Manager for Windows should be considered for achieving recovery point objectives (RPO) which could not be adequately achieved using off-host backups. Note that FlashCopy Manager for Windows can only be used for RDM disks in physical-compatibility mode or iSCSI attached disks.	<i>Off-host agent:</i> <i>Data Protection for VMware or FlashCopy Manager for VMware</i> Data Protection for VMware and/or FlashCopy Manager for VMware are the recommended solutions for Windows virtual machines hosting file/web servers (unstructured data). These solutions provide several advantages versus in-guest backups including: • Incremental forever backup provides efficient, block-level backup of virtual machine guests • Block-level backups can serve for recovery of entire machine, single disk, or individual files/directories (single-pass backup) • No additional management of in-guest agent
Other operating systems (unstructured data)	<i>in-guest agent:</i> <i>Backup-Archive client</i> Deployment of the Backup-Archive client should be considered for virtual machines that are hosting operating systems other than Windows-based or Linux-based operating systems and there is a requirement for individual file recovery. This would also be recommended for legacy deployments of Windows and Linux that are no longer supported by the Data Protection for VMware Recovery agent, e.g., Windows 2000.	<i>Off-host agent:</i> <i>Data Protection for VMware or FlashCopy Manager for VMware</i> Data Protection for VMware and/or FlashCopy Manager for VMware are the recommended solutions for Windows virtual machines hosting file/web servers (unstructured data). The advantages of these solutions are the same as those listed above.

Figure 3-5 In-guest unstructured data protection product positioning

3.4 Communication ports between VMware and Tivoli Storage Manager components

Because Data Protection for VMware, VMware components, and Tivoli Storage Manager server must interrelate with each other, be sure that all the required communication ports are opened for communication flows between those components. The ports that are involved and the correct direction is described next.

Figure 3-6 shows the communications ports that might be used, depending on your implementation of Data Protection for VMware. Arrows show the direction of each flow.

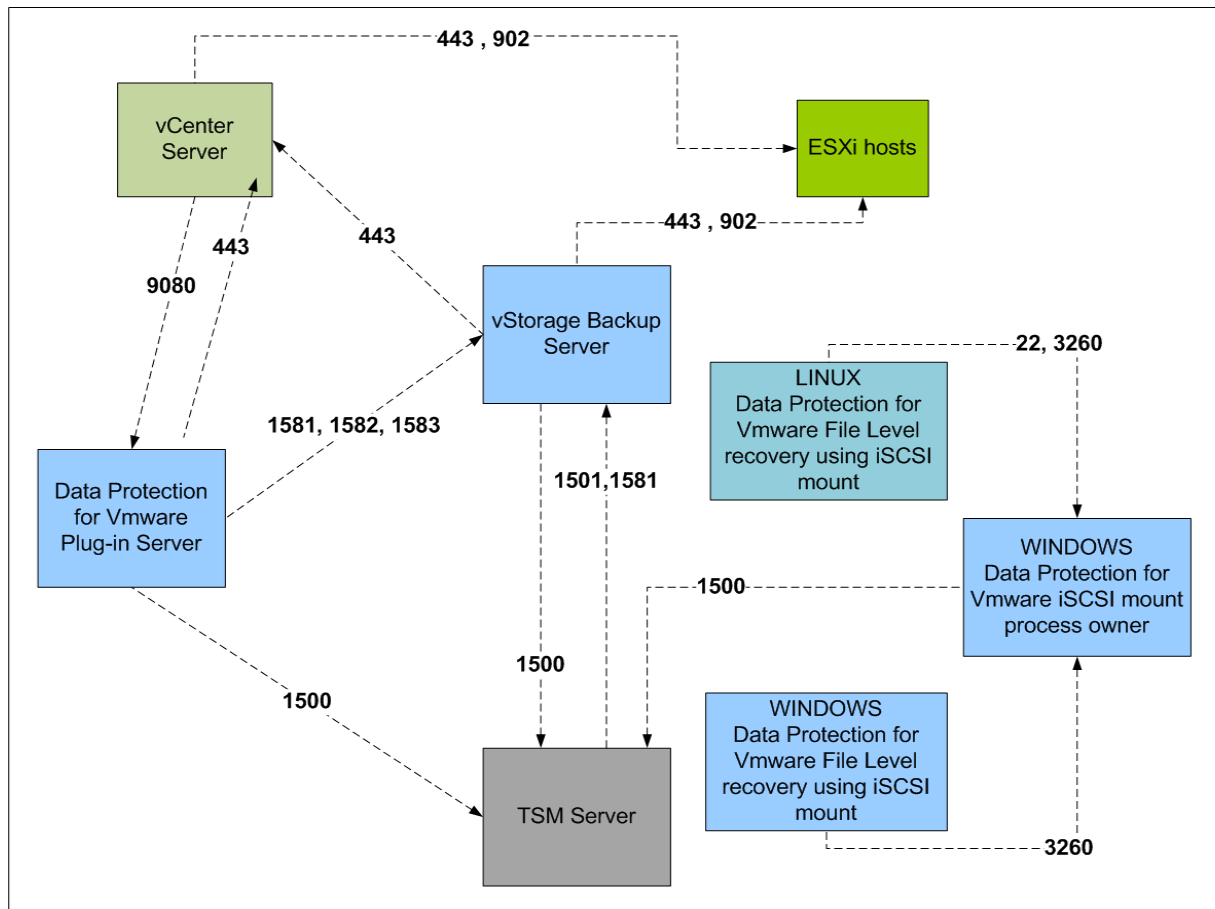


Figure 3-6 Communication ports that are used by Data Protection for VMware

Each component is distributed into several boxes intentionally. However, feature boxes with the same color might be on the same machine.

A list of ports that are used by VMware components is available at this website:

<http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1012382>

This information is also available in the IBM Technote that is available at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg21625297>

3.5 Choosing your backup strategy

Consider the two available strategies, depending on your needs: periodic full backup and incremental forever backup. These strategies are described next.

3.5.1 Periodic full backup

A periodic full backup strategy includes weekly full backups that are followed by daily incremental backups, as shown in Figure 3-7.



Figure 3-7 Periodic full backup strategy

3.5.2 Incremental forever backup strategy

An incremental forever backup strategy includes an initial full backup followed by an ongoing sequence of incremental backups, as shown in Figure 3-8.

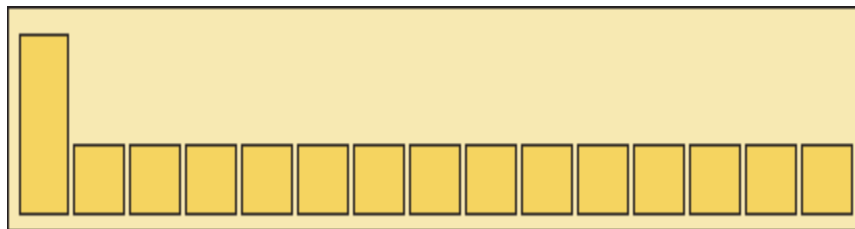


Figure 3-8 Incremental forever backup strategy

3.5.3 Backup strategy considerations

As shown in Figure 3-7, the periodic full backup strategy stores more data than the incremental forever backup strategy. Also, each full backup data set often contains a large amount of data that is duplicated from the previous full backup (not all data changes every week).

Another factor to consider is the backup version, retention, and expiration process because it differs from the previous Data Protection for VMware version. Backup expiration was based on the full-vm backups and was independent of the number of intermediate incremental backups.

With incremental-forever in version 6.4, each backup is treated as an independent recovery point where its retention is managed without a connection to whether a backup is full or incremental. A good setup is to consider the use of the **retextra** backup copy group parameter to control the expiration, and use **verexists NoLimit**. Then, it does not matter if you run several backups daily because you manage your retention in days, not version.

Depending of what type of protection you want, it might be of interest to choose the periodical full virtual machine backup method; for example, create an “out-of-cycle” backup. This type of backup is a good way to create a separate backup set for archiving purposes.

Another good reason to use the Periodic Full backup is when you plan to store the data on physical tape. The periodic full backup regularly stores an entire picture of the virtual machine on tape, then it stores contiguous blocks of data on that tape. This configuration reduces the number of tapes that are required in a restore.

The backup method leads to vStorage Backup Server sizing and estimation of the required inbound and outbound capabilities that are required to meet your service level agreement. For more information about the vStorage Backup Server sizing, see 3.6.5, “vStorage Backup Server Sizing” on page 42.

3.6 vStorage Backup Server

The vStorage Backup Server is the host moving the data between the vSphere infrastructure and the Tivoli Storage Manager server. For more information, see 2.2, “Data Protection for VMware Solution components” on page 18.

3.6.1 Data transfer and transport methods

There are two data movements that are used when a virtual machine is backed up: *Data Transfer* and *Data Transport*, which represents the different data paths between VMware components and Tivoli Storage Manager components, as shown in Figure 3-9 on page 39.

Data Transfer refers to the I/O between the vStorage Backup server and the Tivoli Storage Manager Server.

Data Transport refers to the I/O between the ESXi datastore and the vStorage Backup Server.

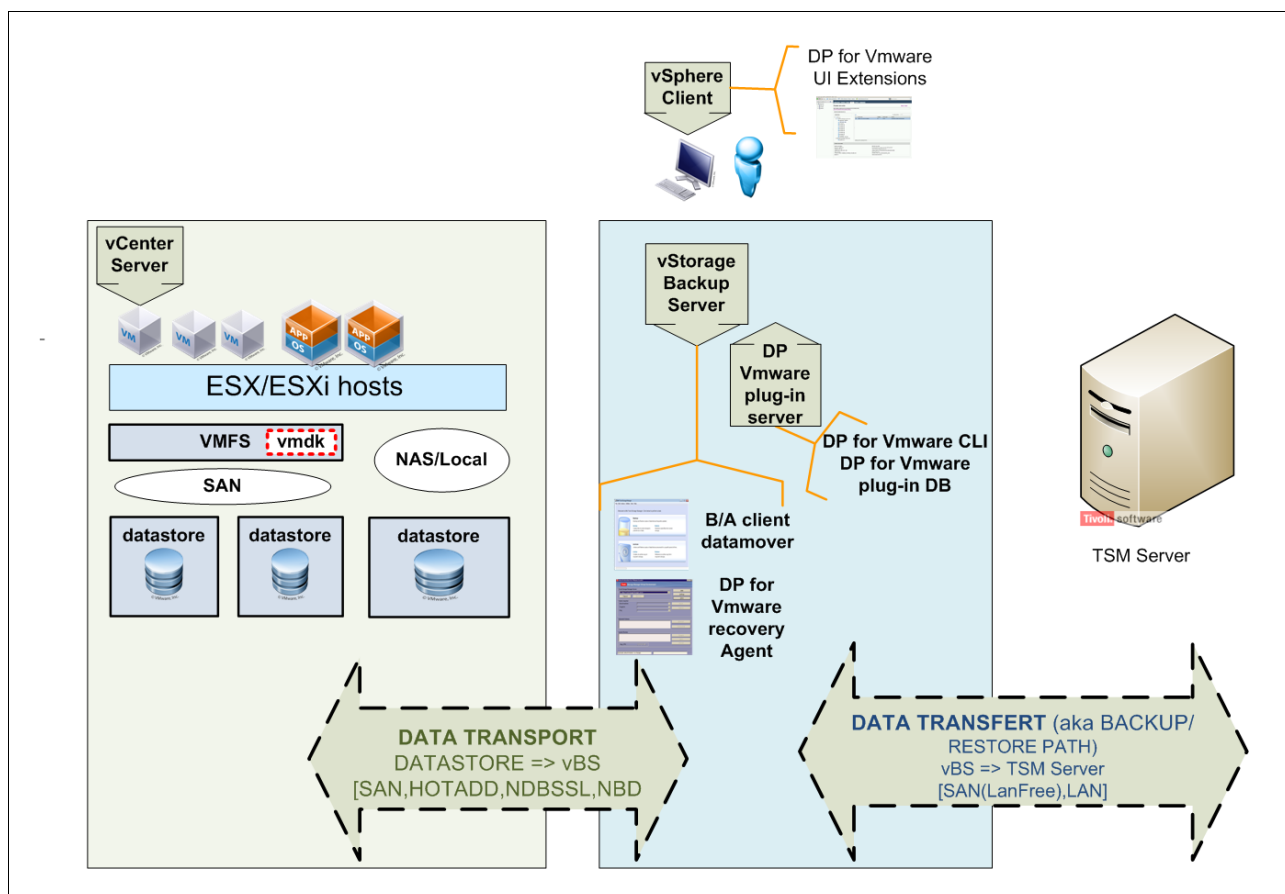


Figure 3-9 Data Transfer and Data Transport explanation

The methods that are used for data transfer from datastore to vBS and from vBS to the Tivoli Storage Manager server can affect the per-session performance of Data Protection for VMware backups and restores. These methods are not available in every case and their availability depends on the type of vStorage Backup Server that is to be used. For more information, see 3.6.2, “vStorage Backup Server: Physical versus virtual” on page 39.

3.6.2 vStorage Backup Server: Physical versus virtual

There are many considerations when deciding whether to use a physical or virtual vStorage backup server. Table 3-2 is a suggested list of items that can help when you are choosing the best vStorage Backup Server for your environment.

Table 3-2 Comparison of physical versus virtual backup server

vStorage Backup Server location/item	Virtual Backup Server	Physical Backup Server ^d
Environment fully virtualized	Applicable	N/A
Off host the backup load (move the load from ESX to another machine)	Applicable ^a	Applicable

Tivoli Storage Manager LANFREE support (be aware of tape limitation, prefer VTL)	N/A	Applicable
10GE LAN bandwidth	Applicable	N/A
Use DISK/FILE only storage to store backups	Applicable	N/A
Disk backend systems with low throughput capability	Applicable	N/A
Plan to use the FlashCopy Manager for VMware ^b	N/A	Applicable
High number of virtual machine backup (more than 60 vmdk) must run in parallel to fulfill the backup window ^c	N/A	Applicable
ESXi hosts and datastore separation	N/A	Applicable ^e
Multiple vSphere environment	N/A	Applicable ^e
Shared Environment	Applicable ^f	Applicable ^f

^a Off host can be achieved by using virtual vStorage Backup Server by dedicating an ESXi host to run the virtual vStorage Backup Server.

^b FlashCopy Manager for VMware requires a Linux machine to be installed. However, the vmcli agent can reach out to any data mover remotely that is configured on Windows or Linux vBS.

^c When a virtual vStorage Backup Server is used, you might reach the limitation of four (max SCSI controllers) * 15 (max devices per SCSI controller) vmdk added to the vStorage Backup Server while backing up (Hotadd transport method). It means that one virtual vStorage Backup Server cannot manage more than 60 vmdk file backups at the same time, meaning less than 60 VM can be backed up at the same time. Every vmdk above this limit is backed up by using NBD (LAN transport method) instead of hotadd.

^d When you are planning to use a physical vStorage Backup Server, it is preferred to use a Windows operating system. There are some known reservation conflict issues when a SAN transport is used on a Linux physical vStorage Backup Server, as documented in the following Backup-Archive client known limitation article:
<http://www-01.ibm.com/support/docview.wss?uid=swg21615236>

^e When ESXi hosts and datastore are isolated from one another, it might be easier to implement a physical vBS that is shared between all the ESXi clusters. This configuration helps avoid deploying several virtual vBS.

^f For more information about how to manage a shared environment, see 3.13, "Deploying Data Protection for VMware in a shared environment" on page 51.

Depending on your choice, Table 3-3 shows the available data transport.

Table 3-3 Data Transport availability (ESXi datastore to vBS and vice versa)

Transport method	Available to Virtual vBS?	Available to Physical vBS?	Comments
NBD	Yes	Yes	N/A
NBDSSL	Yes	Yes	N/A
SAN	No	Yes	Uses direct SAN connection to datastore (for SAN-attached datastores only).
HOTADD	Yes	No	Uses SAN connection (via ESX host) for SAN-attached volumes, which are nearly as efficient as the SAN transport. For NFS datastores, provides more efficient transport than NBD.

Table 3-4 shows the data transfer method that can be used to protect the virtual machine.

Table 3-4 Data Transfer availability (vBS to Tivoli Storage Manager and vice versa)

Transfer method	Available to Virtual vBS	Available to Physical vBS	Comments
LAN	Yes	Yes	Data transfers over LAN to Tivoli Storage Manager server
LAN-free	No	Yes	Data transfers over SAN to Tivoli Storage Manager server storage pool devices (Tape or Virtual Tape) LAN-free with disk is possible by using IBM GPFS™. LAN-free cannot be used with client-side deduplication.

3.6.3 Physical vStorage Backup Server LUN access considerations

If your vStorage Backup Server is a physical machine and you plan to use the SAN transport method, each of the vStorage Backup Servers must have a SAN access to every logical unit number (LUN) that comprises your VMware environment.

For Windows 2003 and Windows 2008, you must disable the automount via the diskpart utility.

On Windows 2008 platform, in addition to the automount, set the SAN policy as described next.

SAN transport method

Complete the following steps on each vStorage Backup Server that use the SAN transport method to access VMware data. These tasks ensure that the disk management policy is properly set up on your environment.

1. Ensure that the Windows 2008 or 2008 R2 SAN policy is set to `OnlineAll` by using `diskpart.exe`.
2. Run the following commands:
 - `automount disable`
 - `automount scrub`
 - `san policy OnlineAll`
 - `exit`
3. Run the commands to check your current configuration. The following output is the output that you must have as per the product documentation:

```
C:\Program Files\Tivoli\TSM\baclient>diskpart
```

```
Microsoft DiskPart version 6.1.7600
```

```
Copyright (C) 1999-2008 Microsoft Corporation.
```

```
On computer: BROADSWORD
```

```
DISKPART> automount
```

Automatic mounting of new volumes disabled.

DISKPART> san

SAN Policy : Online All

DISKPART> exit

Leaving DiskPart...

C:\Program Files\Tivoli\TSM\baclient>

4. To avoid a known recovery issue, follow the recommendations that are documented at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg1IC80972>

For more information about LAN-free and Data Protection for VMware, see this website:

<https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Storage%20Manager/page/Recommendations%20for%20Using%20LAN-free%20with%20Tivoli%20Storage%20Manager%20for%20Virtual%20Environments>

When strong security rules that control LUN access are in place, you can switch the LUNs that are mapped to a physical vStorage Backup Server to read-only access. This can be done by using the diskpart utility that updates the SAN disk attributes. Thus, the SAN transport method for full-vm recovery does not work.

For more information, see this website:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1035096

3.6.4 Virtual vStorage Backup Server HotAdd considerations

When a virtual vStorage Backup Server is used, the default and fastest access to the data that must be backed up is the HotAdd transport.

Consider the following points when you are planning to use HotAdd transport:

- ▶ The transport works only in a virtual vStorage Backup Server where the ESXi host system has access to the datastore that contains the virtual disks of the Virtual Machine that is backed up.
- ▶ Place the virtual vStorage Backup Server in a datastore with a block size larger than or equal to the datastores that contains the virtual machine's to back up
- ▶ Create more virtual SCSI adapters within the VM to support multi-session backups that require larger numbers of HotAdd disk attachments at the same time. Each SCSI bus allows for 15 more attached disks.
- ▶ VM with an IDE bus cannot be backed up via HotAdd.

3.6.5 vStorage Backup Server Sizing

In this section, we describe the steps that you must take to properly size your vStorage Backup Server.

Scenario description

Our scenario includes the following components:

- ▶ Backup strategy is incremental forever
- ▶ Backup window is 10 hours
- ▶ The total amount of data is 10 TB (even if you know that the CBT optimizes the amount of backed up data)
- ▶ Data change daily rate is 10%
- ▶ Per process throughput capability is 80 GB per hour

Estimating the daily backup workload

Our scenario includes the following daily backup workload:

- ▶ For FULL (first backup): 10240 GB
- ▶ For Incremental (ongoing backups with change daily rate 10%): 102 GB

Calculating the required aggregate throughput

The required aggregate is the total amount of data that is divided by the per-process throughput that is based on the backup window.

The per-process throughput depends on the method of reading and writing data. How do you plan to send or store the data on the Tivoli Storage Manager Server? How fast is your VMware back-end disk subsystem? You must take into account the client side de-duplication, LAN-free path, an dVSTOR transport mode (NDB versus HOTADD).

You can tune the read throughput by using the datamover parallelization features **Vmlimitperdatastore** and **Vmlimitperhost**. Depending on where your bottleneck is, tune these two values to fit your environment and to get the maximum read performance.

Based on our assumptions, the following aggregate is required:

- ▶ For FULL (first backup): $10240 / 10 = 1024$ GB per hour
- ▶ For Incremental (ongoing backups): $1024 / 10 = 102$ GB per hour

Calculating the number of concurrent processes (parallelization)

The number of concurrent processes can be calculated by using the following formula:

Aggregate throughput / Per process throughput = number of concurrent processes

You can achieve this multi-streaming by using the **Vmmxparallel** datamover parallelization feature. This parameter is used with the two that manage the read performance: **Vmlimitperdatastore** and **Vmlimitperhost**.

Based on our assumption, the following concurrent processes are needed:

- ▶ For FULL (first backup): $1024 \text{ GB/h} / 80 \text{ GB per hour} = 13$ processes
- ▶ For INC (ongoing backups): $102 \text{ GB/h} / 80 \text{ GB per hour} = 2$ processes

Note: The FULL backup is done once or occasionally. For the sizing, hold the calculation that is based on incremental assumptions (in our case, two processes).

Checking for other constraints and refining the calculation, if needed

With the sizing completed, verify that inbound and outbound requirements for the vStorage Backup Server are met.

Other constraints means, Where can your bottleneck be? To find out, review the following read and write factors that are involved on the data protection tasks:

- ▶ VMware vSphere Datastore outbound throughput (aggregated read throughput)
- ▶ Tivoli Storage Manager Server Inbound capacity

Although some guidelines are provided for proxy host resource requirements, it is not the intent of this document to provide specific guidance on hardware or system configurations of physical or virtual proxy hosts. Hardware configuration (or in the case of a virtual machine, resource allocation) should be defined by a qualified system engineer that is familiar with hardware capabilities, I/O throughput, and other system requirements.

IBM Techline provides a service for pre-sales configuration of Tivoli Storage Manager hardware, including Data Protection for VMware proxy sizing. For more information, consult with your IBM Tivoli sales representative or an IBM Business Partner.

For more information about vStorage Backup server sizing, see this website:

<http://www.ibm.com/developerworks/wikis/display/tivolistoragemanager/Guide+to+vStorage+Backup+Server+%28Proxy%29+Sizing>

3.6.6 When to use multiple datamover agents

The following are two examples of when you must set up more than one Backup-Archive client that is acting as a datamover for full-vm backups. The different datamover nodes can be defined on the same vStorage Backup Server:

- ▶ When more than one virtual machine is restored through the vCenter plug-in
When a full-vm recovery task is started by using the vCenter plug-in, the datamover that is involved in this transaction cannot be used by the plug-in for another operation until the end of that recovery; the dsm client acceptor daemon (**dsmcad**) is tied up by the plug-in. Therefore, you must have multiple datamover nodes that are defined to restore more than one virtual machine at a time by using the vCenter plug-in.
- ▶ When the vStorage Backup Server must manage more than one vCenter server or when the security and user management within virtual infrastructure dictates it.

For more information about security and shared environment considerations, see 3.13, “Deploying Data Protection for VMware in a shared environment” on page 51.

For more information about how to define multiple datamovers on one vStorage Backup Server, see 3.11.2, “Multiple vCenter server support” on page 49.

3.7 Storage location versus recovery features

Depending on the storage where the backed up data is, some Data Protection for VMware features might not be available or are available with lower performance. These conditions are summarized in Table 3-5 on page 44.

Table 3-5 Feature availability that is based on vStorage Backup Server and storage type

vStorage Backup Server	Physical			Virtual		
Storage & Features	DISK/FILE	Virtual Tape Library	Physical Tape	DISK/FILE	Virtual Tape Library	Physical Tape
LAN-free	No	Yes	Yes	No	No	No

vStorage Backup Server	Physical			Virtual		
Tivoli Storage Manager deduplication	Yes (FILE)	No	No	Yes (FILE)	No	No
FULL VM Backup	Yes	Yes	Yes	Yes	Yes	Yes
INCR VM Backup	Yes	Yes	Yes ^a	Yes	Yes	Yes
FULL VM Restore	Yes	Yes	Yes	Yes	Yes	Yes
File Level restore	Yes	Yes	Yes (lower performance expected)	Yes	Yes	Yes (lower performance expected)
Instant Volume restore	Yes	Yes	No	Yes	Yes	No

^a The incremental VM backup process must recall and read CTL files to determine the differences between previous and current status. This can slow down the backup if the CTL files are stored on physical tape. As a best practice, always store CTL files on the fastest available access volume (for example, Disk or File). For more information, see the configuration guidelines documentation at this website:

http://pic.dhe.ibm.com/infocenter/tsminfo/v6r3/index.jsp?topic=%2Fcom.ibm.itsm.ve.doc%2Fve_mount_tape.html

3.8 Determining the location to start backup or restore

Depending on the task you must start, you can choose among vStorage Backup Server, virtual machine, or the Data Protection for VMware vCenter plug-in. The available options are summarized in Table 3-6.

Table 3-6 Availability of Data Protection for VMware operation depending of the location

Location Task	vStorage Backup Server	Virtual Machine	vCenter plug-in
Full or Incremental VM Backup	Using Backup-Archive client GUI or CLI	N/A	Data Protection for VMware plug-in interface, back up Tab
FULL VM Restore	using Backup-Archive client GUI or CLI	N/A	Data Protection for VMware plug-in interface, restore Tab
Instant Volume restore	N/A	Using Data Protection for VMware recovery agent	N/A
File Level restore	Using Data Protection for VMware recovery agent	Using Data Protection for VMware recovery agent	N/A

As shown in Table 3-6 on page 45, almost all recovery tasks can be done from the vStorage Backup Server, except the Instant Volume Restore. When you are planning the deployment, remember that the more operations you start from the vStorage Backup Server, the less time

you spend deploying and maintaining Backup-Archive client and Data Protection for VMware recovery agent across all the virtual machines. To reduce this workload, you might deploy Data Protection for VMware recovery agent only on a virtual machine where you plan to perform Instant Volume Restore operations.

3.9 Effect of Data Protection for VMware backups on the Tivoli Storage Manager Server

In this section, we describe some of the Tivoli Storage Manager Server design decisions that must be made when you are planning to use Data Protection for VMware to protect virtual machines.

3.9.1 How to handle CTL files (FULL-VM backup control files)

It is advised to store CTL files on a disk or file-based device class. This increases the FULL-VM Incremental backup, restore, and Item level recovery performance.

To effectively manage CTL files, create a dedicated storage pool (without migration) on the Tivoli Storage Manager server. To estimate the size of the disk-based storage pool that is required to store CTL files of FULL-VM backup, use the following formula:

(Total defined size of your vmdks in MB/128) x 73 KB x number of backups performed within the retention period

Where 128 is the size in MB of the virtual machine data chunks that is processed by Tivoli Storage Manager (worst case) and 73 KB is the size of the associated control file.

Assume 1 TB to back up, one backup per day, retaining data for 14 days:

$(102400 / 128) \times 73 \times 14 = 8 \text{ GB}$

You can roughly estimate the CTL storage pool size to 1% of the total defined size of your vmdks.

The following Technote helps you calculate the maximum space that CTL can use and thus estimates how large the CTL destination pool can be:

<http://www-01.ibm.com/support/docview.wss?uid=swg21624758>

3.9.2 VM full-vm backup on physical tape or virtual tape

If you plan to store FULL-VM backup on physical tapes, you must enable the filespace collocation on the storage pool where the datacenter node stores its data, as you do on physical tape.

Note: For more information about tape-only implementation, see this website:

http://pic.dhe.ibm.com/infocenter/tsminfo/v6r3/index.jsp?topic=%2Fcom.ibm.itsm.ve.doc%2Fr_ve_mount_tape.html

3.9.3 Incremental forever backup strategy consequence on Tivoli Storage Manager server database

With the new incremental forever backup method, you might have to tune the datamover Backup-Archive client to avoid adding too many objects in the Tivoli Storage Server database. The incremental forever backup method can lead to several entries in the Tivoli Storage Manager Server database, which affects the database performance and scalability. You can use options (**mbobjrefreshthresh** or **mbpctrefreshthresh**) to adjust scalability within Tivoli Storage Manager.

For more information, see *IBM Tivoli Storage Manager for Virtual Environments Data Protection for VMware Installation and User Guide*, SC27-2898.

3.10 VMware snapshots considerations

In this section, we describe the considerations for VMware snapshots.

3.10.1 Snapshots limitation

There are several contexts where VMware snapshots are not possible. The list of Snapshot Limitations (vSphere 5.x) is available at this website:

http://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc_50%2FGUID-53F65726-A23B-4CF0-A7D5-48E584B88613.html

You must consider the following limitations when you are deploying Data Protection for VMware because the product uses the VMware snapshot technology:

- ▶ VMware does not support snapshots of raw disks, RDM physical mode disks, or guest operating systems that use an iSCSI initiator in the guest.
- ▶ Virtual machines with independent disks must be powered off before you take a snapshot. Snapshots of powered-on or suspended virtual machines with independent disks are not supported.
- ▶ Snapshots are not supported with PCI vSphere Direct Path I/O devices.
- ▶ VMware does not support snapshots of virtual machines that are configured for bus sharing. If you require bus sharing, consider running backup software in your guest operating system as an alternative solution. If your virtual machine has snapshots that prevent you from configuring bus sharing, delete (consolidate) the snapshots.

Although in some cases backup via snapshots is not possible, the Tivoli Storage Manager product family helps you to protect the data by implementing an in-guest Tivoli Storage Manager agent or Tivoli Storage Manager FastBack agent to allow you to protect the data accordingly.

3.10.2 VMDK file size and snapshot overhead

Because the snapshots are to be used for backup purposes, you must pay attention to the VMware maximums that are described in this section when you are setting up a virtual machine's storage.

The maximum vmdk file size differs among versions of ESX/ESXi and among versions of VMFS.

On ESXi 5.0 and newly formatted VMFS5, a standard 1 MB block size is available, as shown in Table 3-7.

Table 3-7 Maximum file size depending block size for ESXi 5.x with VMFS5

Block Size	Maximum File size
1 MB	2 TB - 512 Bytes

On ESX/ESXi 4.1 and ESXi 5.0 that uses a VMFS3 datastore, the maximum file size corresponds to the block size of the VMFS datastore, as shown in Table 3-8.

Table 3-8 Maximum file size depending block size for ESX/ESXi 4.1 and ESXi 5.0 with VMFS3

Block size	Maximum file size
1 MB	256 GB
2 MB	512 GB
4 MB	1 TB
8 MB	2 TB - 512 Bytes

On ESX/ESXi 4.0, the maximum file size corresponds to the block size of the VMFS3 datastore, as shown in Table 3-9.

Table 3-9 Maximum file size depending block size for ESX/ESXi 4.0

Block Size	Maximum file size
1 MB	256 GB - 512 Bytes
2 MB	512 GB - 512 Bytes
4 MB	1 TB - 512 Bytes
8 MB	2 TB - 512 Bytes

Overhead for the snapshot is approximately 2 GB for a disk size of 256 GB. If snapshots are to be used, consider the overhead while you decide the size of the disks, as shown in Table 3-10.

Table 3-10 Snapshots overhead

Maximum VMDK size	Maximum Overhead	Maximum size less overhead
256 GB - 512 Bytes	2 GB	254 GB
512 GB - 512 Bytes	4 GB	508 GB
1 TB - 512 Bytes	8 GB	1016 GB
2 TB - 512 Bytes	16 GB	2032 GB

VMware recommends that you create virtual disks that are smaller than the maximum size minus the overhead to enable the use of features, such as, snapshot, cloning, and independent-non-persistent disks.

3.11 Data Protection for VMware considerations

In this section, we describe considerations and resources for more information for Data Protection for VMware.

3.11.1 Tivoli Storage Manager Backup Archive considerations

Because the Backup-Archive client is the datamover for Data Protection for VMware operations, the following limitations apply for Data Protection for VMware operations:

- ▶ Tivoli Storage Manager V6.4 Windows backup-archive client known problems and limitations:
<http://www-01.ibm.com/support/docview.wss?uid=swg21608413>
- ▶ Tivoli Storage Manager V6.4 UNIX and Linux backup-archive client known problems and limitations:
<http://www-01.ibm.com/support/docview.wss?uid=swg21608417>
- ▶ Data Protection for VMware V6.4 limitations (Data Protection for VMware, those not related to Backup-Archive):
<http://www-01.ibm.com/support/docview.wss?uid=swg21609441>
- ▶ Technote about Microsoft Cluster of virtual machines:
<http://www-01.ibm.com/support/docview.wss?uid=swg21600617>
- ▶ VMware best practice guide about Windows Domain controller within a virtual machine:
http://www.vmware.com/files/pdf/Virtualizing_Windows_Active_Directory.pdf

3.11.2 Multiple vCenter server support

Because the Data Protection for VMware plug-in is attached to a vCenter server, you cannot use the plug-in to support more than one vCenter. The following limitation occurs: you cannot manage the backup of virtual machines that are managed by different vCenter servers or perform restores across VMware infrastructure that is managed by different vCenter.

If you want to use the plug-in to start backup or recovery tasks on virtual machines that are spread over multiple VMware datacenter and managed by multiple vCenter servers, you need as many plug-in servers as you have vCenter server. Then, each of your plug-in servers has a plug-in installed and attached to one vCenter server.

When you are not using the Data Protection for VMware plug-in, one vStorage Backup Server can be configured to address more than one vCenter server by creating multiple client option files that reference each of the vCenter servers you might need to manage (VMCHOST parameter). The same proxy (vStorage Backup Server) can act as a datamover for several vCenters, so it can act as a datamover for several distinct VMware infrastructures.

The Figure 3-10 shows the Backup-Archive client datamover option file configuration that you might have in a multiple vCenter configuration.

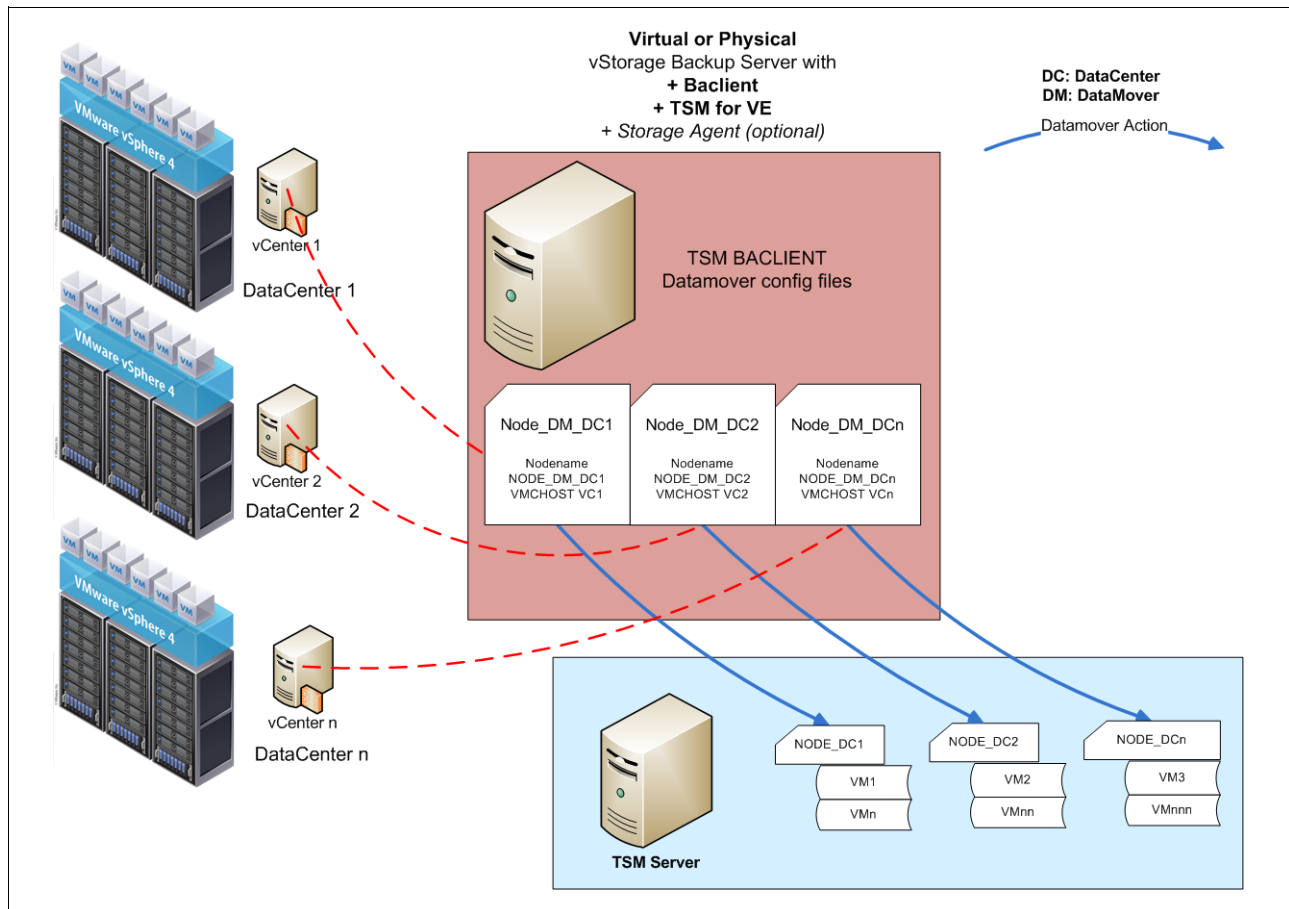


Figure 3-10 Multiple vCenter support setup: Datamover

3.12 Tivoli Storage Manager node naming convention for Data Protection for VMware resources

A naming convention helps you to determine the role of every component and its interactions. Table 3-11 suggests a naming convention for client <cli>.

Table 3-11 Tivoli Storage Manager node naming convention

Role	Description	Tivoli Storage Manager node Names
vCenter node	The virtual Tivoli Storage Manager node that represents the vCenter.	<cli>_<vCenterServer>_VCnn
Data center node	Node that maps to a data center. The data center nodes hold the data of virtual machine within this data center.	<cli>_<vCenterServer>_DCnn

Role	Description	Tivoli Storage Manager node Names
Data Protection for VMware command-line interface node	The Tivoli Storage Manager Client node that connects the Data Protection for VMware command-line interface to the Tivoli Storage Manager Server and the data mover node.	<cli>_<vCenterServer>_VCLInn
Tivoli Storage Manager data mover node	The Tivoli Storage Manager node name for the Tivoli Storage Manager Backup-Archive client that is installed on the vStorage Backup Server. These nodes perform the data movements. You can have multiple Tivoli Storage Manager data mover nodes for each vStorage Backup Server. You can have multiple datacenters that are backed up by one datamover node.	<cli>_<vStorage Backup ServerHostname>_DMnn

3.13 Deploying Data Protection for VMware in a shared environment

Data Protection for VMware can be implemented in dedicated and shared environments.

A shared environment can be on of the following examples:

- ▶ VM that is to be managed separately (for example, multiple branch within same Client)
- ▶ ESXi clusters to be managed separately (for example, one cluster per branch)
- ▶ Multiple vCenter Server
- ▶ Security constraints that split up the environment (for example, User ID management)

In a shared environment, all the information that was provided previously in this chapter is still valid. In addition to this information, we described what should be considered and what the effects are on the design when the solution is implemented in a shared environment.

3.13.1 Back up in a shared environment

Depending on your environment, you might need to consider the implementation of Data Protection for VMware components as shared resources between different entities. In this section, we describe the new dependencies that come with shared implementation. Remember that as you consider the information in this section, you must take into account the vBS sizing.

In a shared environment, one challenge is the security for connecting the VMware infrastructure and to access the data after it is stored within the Tivoli Storage Manager server. Some configuration can be done on the datamover node (the one accessing the VMware data and datastores) and on the datacenter node (the one managing the data after they are backed up to the Tivoli Storage Manager server).

The following information helps you to determine the shared configuration that can be done according to your environment.

3.13.2 Determining what Data Protection for VMware nodes are needed

In this section, we describe what your node definition can be depending on your shared environment, taking into account the user security rules.

Figure 3-11 on page 53 shows the decision tree that is used when you have a single vCenter server. In this figure, we assume that a branch is a vSphere datacenter.

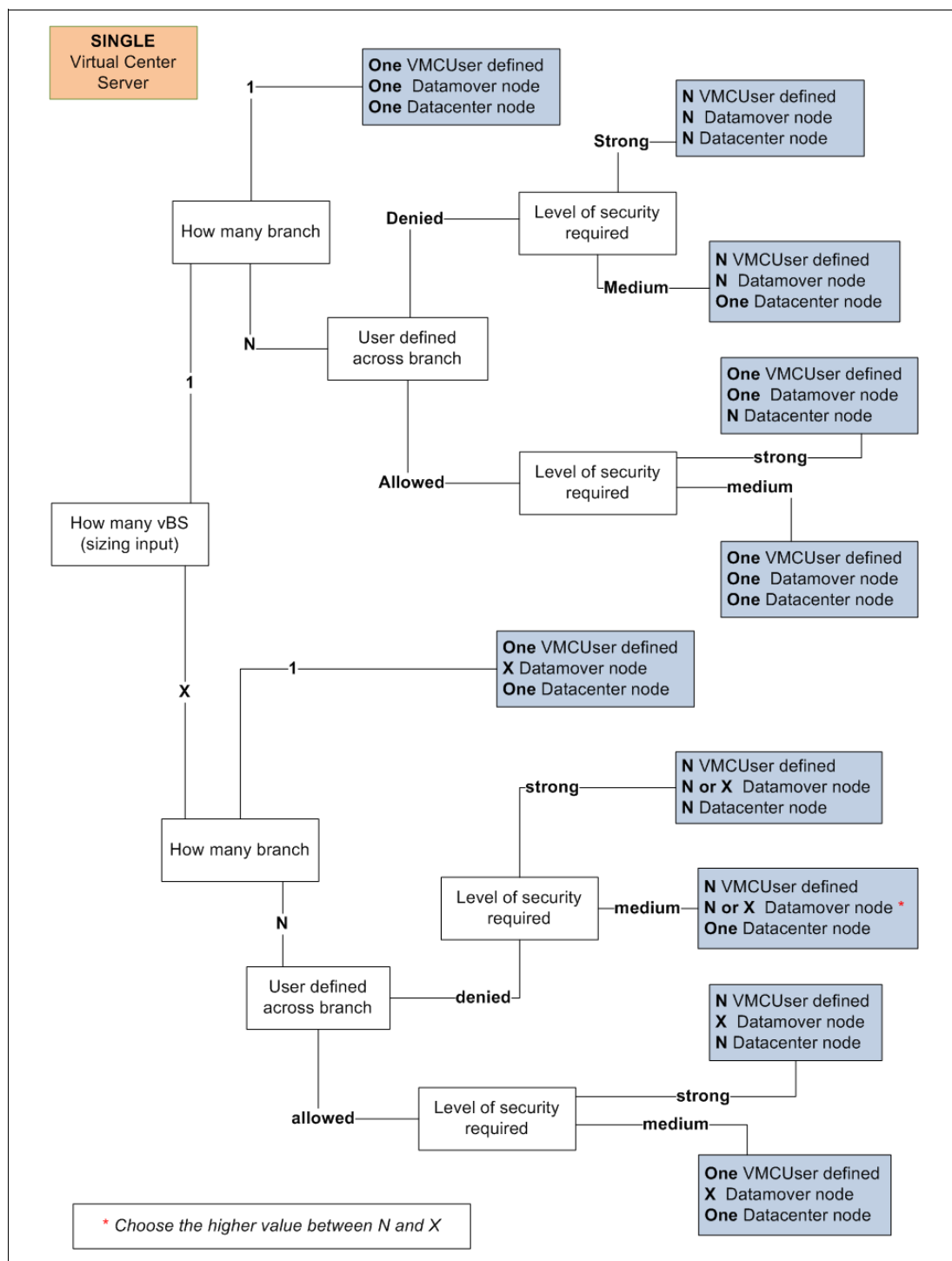


Figure 3-11 Single vCenter server decision tree

Figure 3-12 shows the decision tree that is used when you have multiple vCenter servers. In this figure, we assume that a branch is a vSphere datacenter.

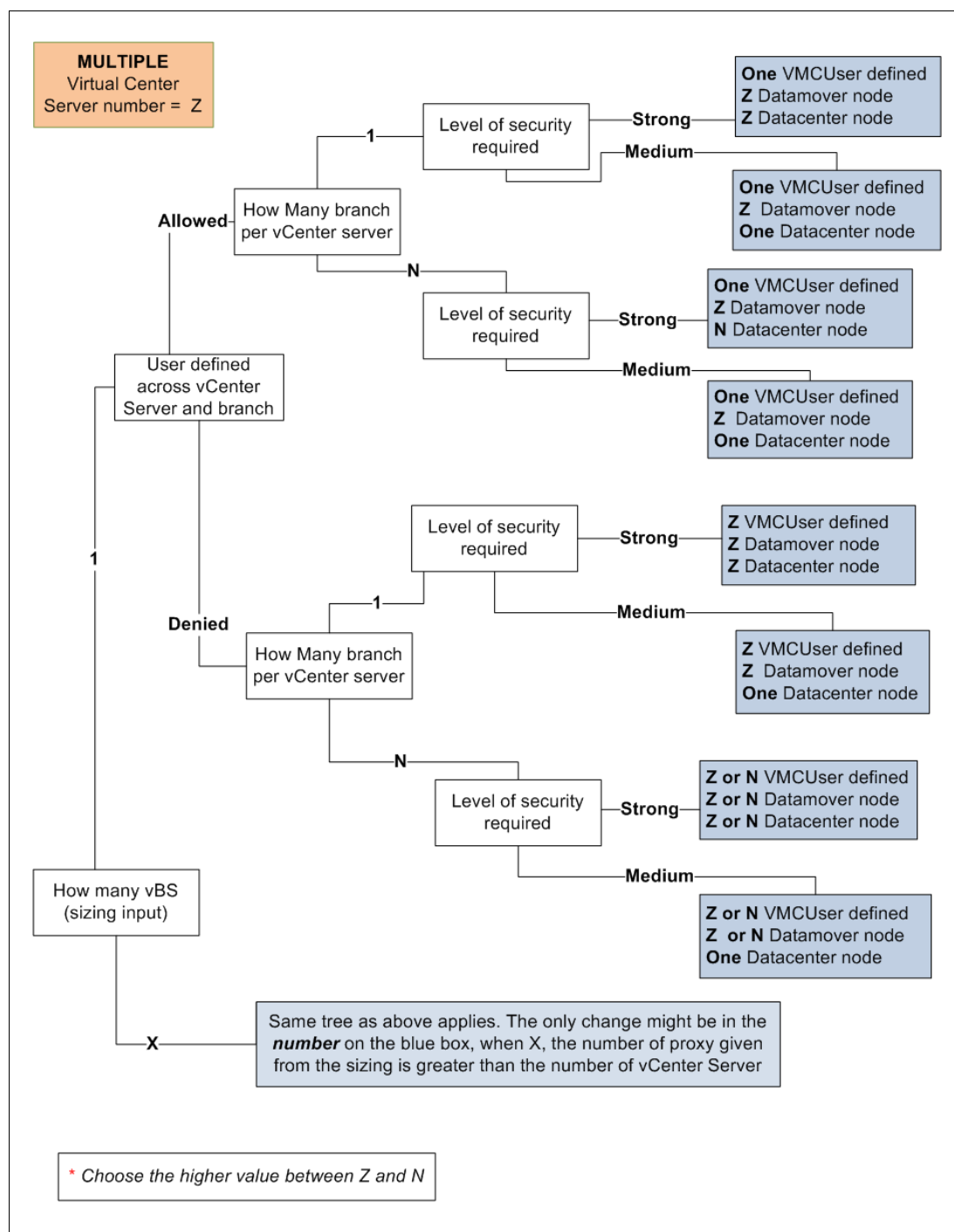


Figure 3-12 Decision tree with multiple vCenter servers

Note: In a shared environment, security requirements dictate the number of vStorage Backup Servers and how many Tivoli Storage Manager datacenter nodes you must implement; that is, it must fit with the sizing requirements.

3.13.3 Examples of deployment implementations

In this section, we describe implementation scenarios for deploying Data Protection for VMware.

One datamover node, one datacenter node for all data

This scenario includes the following features:

- ▶ The Tivoli Storage Manager datacenter node is the sharing point.
- ▶ One datamover node is attached to the vCenter server.
- ▶ All of the data is stored onto the same repository (datacenter node).
- ▶ One VMware user (datamover **VMCuser**) performs all the snapshot operations.
- ▶ For recovery, data access control can be restricted by using the **from node** option of the Data Protection for VMware recovery agent after the **set access** restrictions are applied.
- ▶ A low level of data access management security is required.

Figure 3-13 shows this scenario. In this figure, we assume that a branch is a vSphere datacenter.

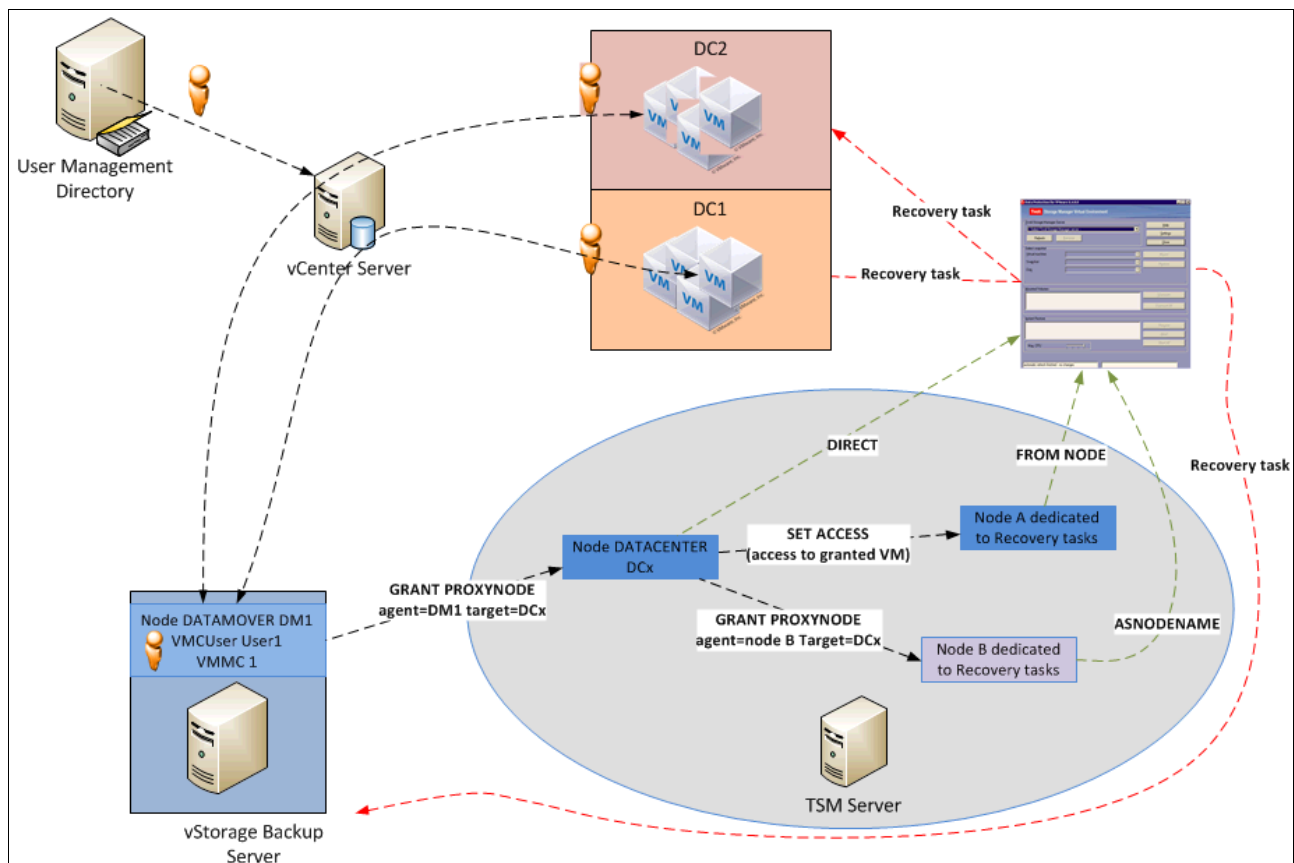


Figure 3-13 One datacenter node for all the data

One datamover node, one datacenter node per branch

This scenario includes the following features:

- ▶ The vBS is the sharing point.
- ▶ One datamover node is attached to the vCenter server.

- Data movement is performed by the same datamover to multiple datacenter nodes.
- One VMware user (datamover **VMCuser**) performs all of the snapshots operations.
- Each branch is stored within its own datacenter node.
- Consider the use of physical vBS.
- Data access control can be restricted by using the **from node** or **asnodename** options of the Data Protection for VMware recovery agent after the **set access** or **grant proxynode** authorization are applied.
- A medium level of data access management security is required.

Figure 3-14 shows this scenario. In this figure, we assume that a branch is a vSphere datacenter.

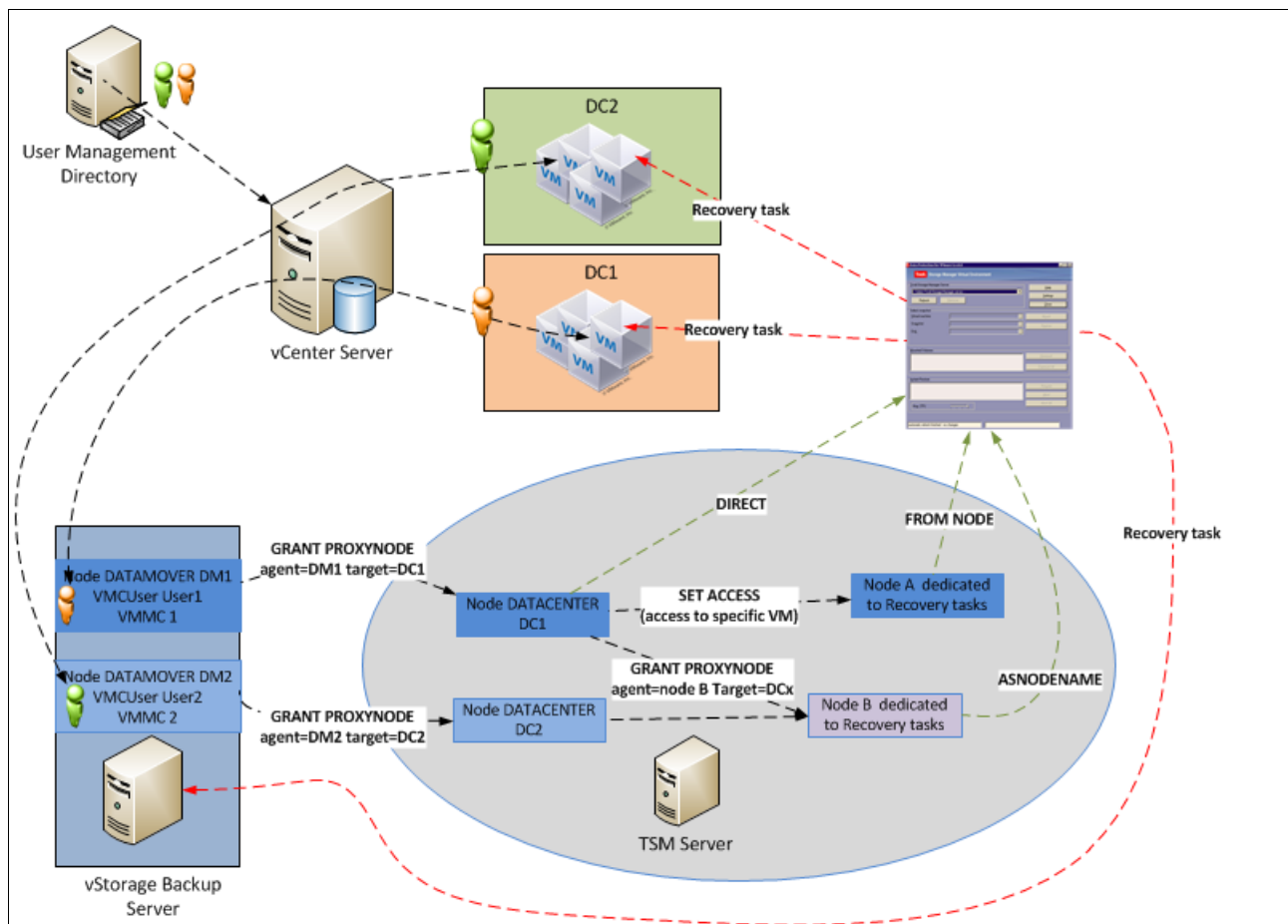


Figure 3-14 One datacenter node for each branch/vSphere DC

One datamover per datacenter node per branch

This scenario includes the following features:

- Required configuration when multiple vCenter exist in the shared environment.
- There is a one-to-one relationship between datamover and datacenter node and each branch has its own datamover and datacenter nodes.
- Easy data access controls management.
- Brings the possibility to configure multiple VMware users (datamover **VMCuser** parameter) to perform backup (one user per branch for instance).

- Consider the use of Virtual vBS because it is more scalable and easier to deploy.
- A strong level of data access management security is required.

Figure 3-15 shows this scenario. In this figure, we assume that a branch is a vSphere datacenter.

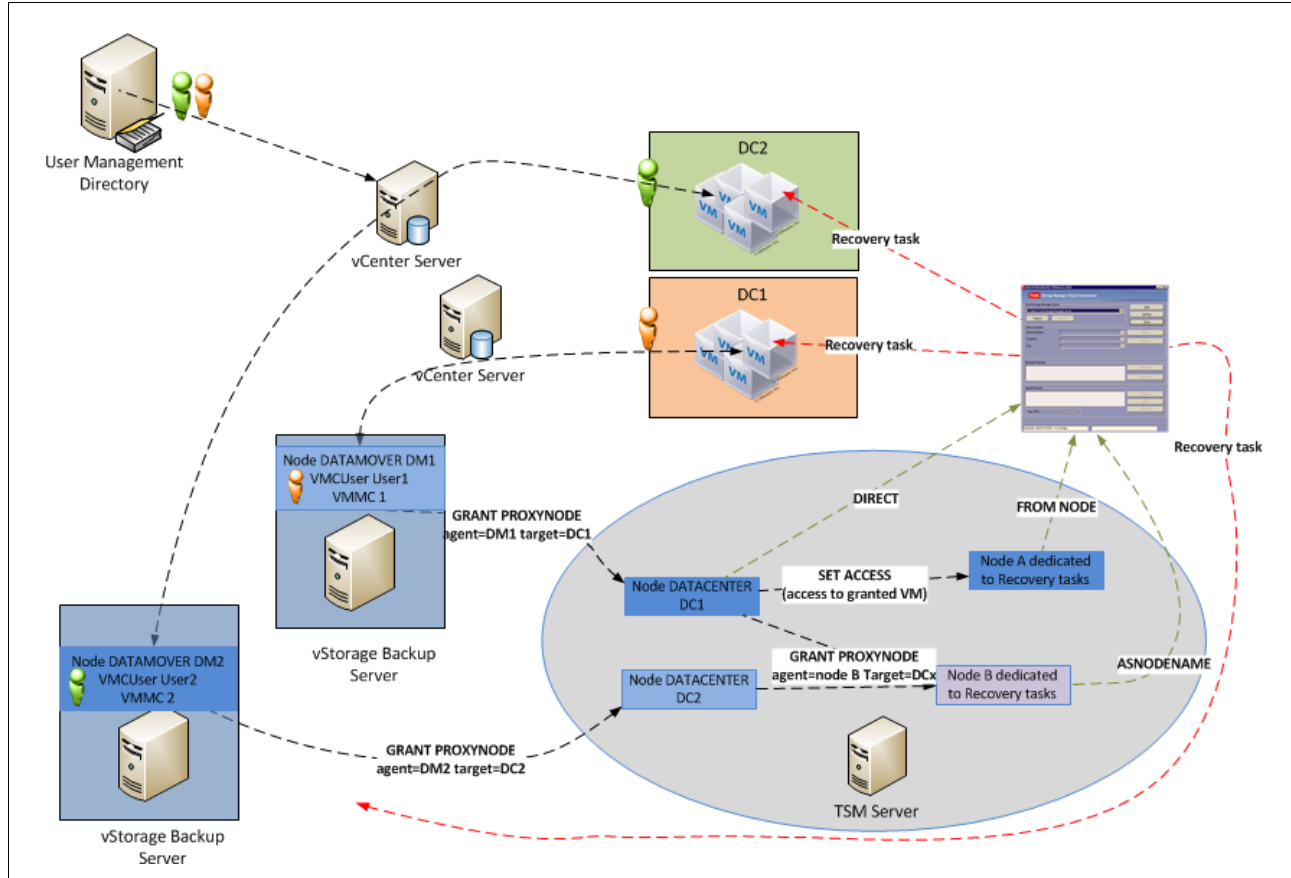


Figure 3-15 Dedicated datacenter and datamover nodes for each branch

3.13.4 Recovery in a shared environment

Data Protection for VMware Recovery agent has three different options to access the virtual machine snapshots that are held by the datacenter node, as shown in Figure 3-16 on page 58.

Tivoli Storage Manager Server information

Server address: warden.storage.usca.ibm.com

Server port: 1500

Node access method:

☐ Asnodename
Authenticate using a proxy node to access the VM backups that are in the target node. The authentication node must have been granted "proxy" authority to perform operations on behalf of the target node.

☒ Fromnode
Authenticate using a node with access limited only to the snapshot data of specific VMs in the target node. The authentication node must have been granted limited access to the target node using "set access" command.

☐ Direct
Authenticate directly to the target node (the node where the VM backups are located).

Authentication node:

Password:

Target Node: CLEM_OVERLORD_DC01

OK Cancel

Figure 3-16 Data Protection for VMware REcovery agent: Data Access control

Depending on how you configure the node relationship, you choose among Asnodename, FromNode, or Direct.

The Asnodename option requires the proxynode relationship to be configured. Every virtual machine that is held by **TargetNode** that is specified can be accessed for the restore operation.

The FromNode option requires the **set access** configuration to be done. Only virtual machines that are explicitly allowed with the **set access** command can be used for recovery. The interface displays all the virtual machines that are held by the specified TargetNode. For more information about how to use the **set access** command and **FromNode** option, see 7.2, "Recovering data by using the Set Access and FromNode options" on page 164.

Direct connection means that you connect to the Tivoli Storage Manager server by using the datacenter node credentials. No setup is required.



Installation and configuration

This chapter describes the procedures that are used to install and configure the Tivoli Storage Manager Backup Archive Client and all the Data Protection for VMware components.

Windows and Linux operating systems are covered in this chapter.

This chapter includes the following topics:

- ▶ Overview of component installation and configuration
- ▶ Tivoli Storage Manager data mover: Backup and archive client
- ▶ Installing Data Protection for VMware features
- ▶ Data Protection for VMware vCenter plug-in configuration

4.1 Overview of component installation and configuration

Table 4-1 summarizes the basic steps that are involved in deploying the Data Protection for VMware solution.

Table 4-1 Steps to deploy Data Protection for VMware solution

Task	Recommend Steps
Ensure prerequisites are in place	Prerequisite requirements are listed in Chapter 3, "Planning the installation of Data Protection for VMware" on page 25.
Configure Tivoli Storage Manager server	Register required nodes and grant required proxy relationships. Define management class or copy group that is used to control the target storage pool for the VM backups and the VM backup retention. For more information, see the Tivoli Storage Manager Information Center at this website: http://pic.dhe.ibm.com/infocenter/tsminfo/v6r4/index.jsp?topic=%2Fcom.ibm.itsm.client.doc%2Ft_protect_wf.html
Install Backup-Archive client (Data Mover) on vStorage Backup Server.	Install Backup-Archive client data mover on vStorage Backup Server.
Configure Backup-Archive client Data Mover on vStorage Backup Server	FULL-VM specific options in the dsm.opt file (dsm.sys for Linux): <pre> VMCHOST vcenter.server VMCUSER vcenteradminid VMFULLTYPE vstor VMBACKUPTYPE fullvm DOMAIN.VMFULL "ALL-VM" </pre> If required, specify the following management classes to be used: VMC (VM backup data) and VMCTLMC (control files). Configure vCenter access: dsmc set password -type=vm vcenter vcenteradminid password. Validate configuration by performing the following: Attempt to list vCenter VMs in DOMAIN.VMFULL <pre> dsmc show vm all </pre> To enable Tivoli Storage Manager server scheduling and integration with vCenter plug-in, complete the following steps: 1. Start the GUI (dsm.exe) and go to the menu Utilities → Setup Wizard to setup Tivoli Storage Manager web client. 2. Verify the CAD (Client Acceptor Daemon) works by opening: <a href="http://<datamover_hostname>:1581">http://<datamover_hostname>:1581 in a browser. You should see the Backup-Archive client GUI. 3. Verify that Backup-Archive client GUI is working (accessed via browser). Click File → Connection information to verify that the Remote Client Agent can be started.

Install VE enablement file on the vStorage Backup Server	Install the Enablement File from the Data Protection for VMware installation package. In addition to installing the Enablement file, install the following Data Protection for VMware components at this time (this prepares you for follow-on tasks): ▶ Data Protection for VMware Recovery Agent ▶ Recovery Agent command-line interface (CLI) ▶ Documentation If the Data Protection for VMware Plug-in is to be installed on the vStorage Backup Server, it can also be selected.
Deploy DP for VMware Recovery Agent on vStorage Backup Server	The DP for VMware Recovery Agent was installed on the vStorage Backup Server in the previous step. Start the DP for VMware Recovery Agent and mount a VM backup snapshot to test file recovery. Deploying the DP for VMware Recovery Agent on the vStorage Backup Server is a recommend starting point.
Deploy DP for VMware vCenter Plug-In	Install the Data Protection for VMware plug-in (if not previously installed on the vStorage backup server). Configure the vCenter plug-in by using the wizard or by editing the <code>vmcli profile</code> configuration file.

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

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

Remove any version of IBM Tivoli Storage Manager FastBack on the machine. The Data Protection for VMware installation procedure checks for the existence of FastBack on the Server. If it is found, the installation fails.

4.1.1 Tivoli Storage Manager server configuration

Complete the following steps to configure the Tivoli Storage Manager Server:

1. Define domain and policies.

With the information gathered throughout the planning phases, you can create domains and all the policies that answer your retention needs.

Create the management classes for Data (DAT) and Control (CTL) files.

For more information about estimating the size of the CTL storage pool, see 3.9, “Effect of Data Protection for VMware backups on the Tivoli Storage Manager Server” on page 46. The rough estimate is 1% of the data that is backed up.

Note: It is preferred that no deduplication enabled storage pools are used to store CTL files. The best storage device to store these full-vm control files is DISK storage pool.

2. Register Data Protection for VMware nodes on Tivoli Storage Manager Server and define their relationship.

The vCenter plug-in and all the data movement rely on the set of node definitions and relationships. Make sure the Tivoli Storage Manager node definitions for datacenters map to the associated VMware datacenters.

If the vCenter plug-in is not used, you do not need to define Tivoli Storage Manager CLI and vCenter node names. However, it is recommended to use the datacenter node convention and have the data mover (or movers) back up data on behalf of the datacenter node (that is, maintain the data mover and data center proxy node relationship and use the **-asnode=datacenternode** option on dsm/dsmc).

Figure 4-1 shows the nodes and relationship between all of the nodes that are involved in a Virtual Machine (VM) backup operation.

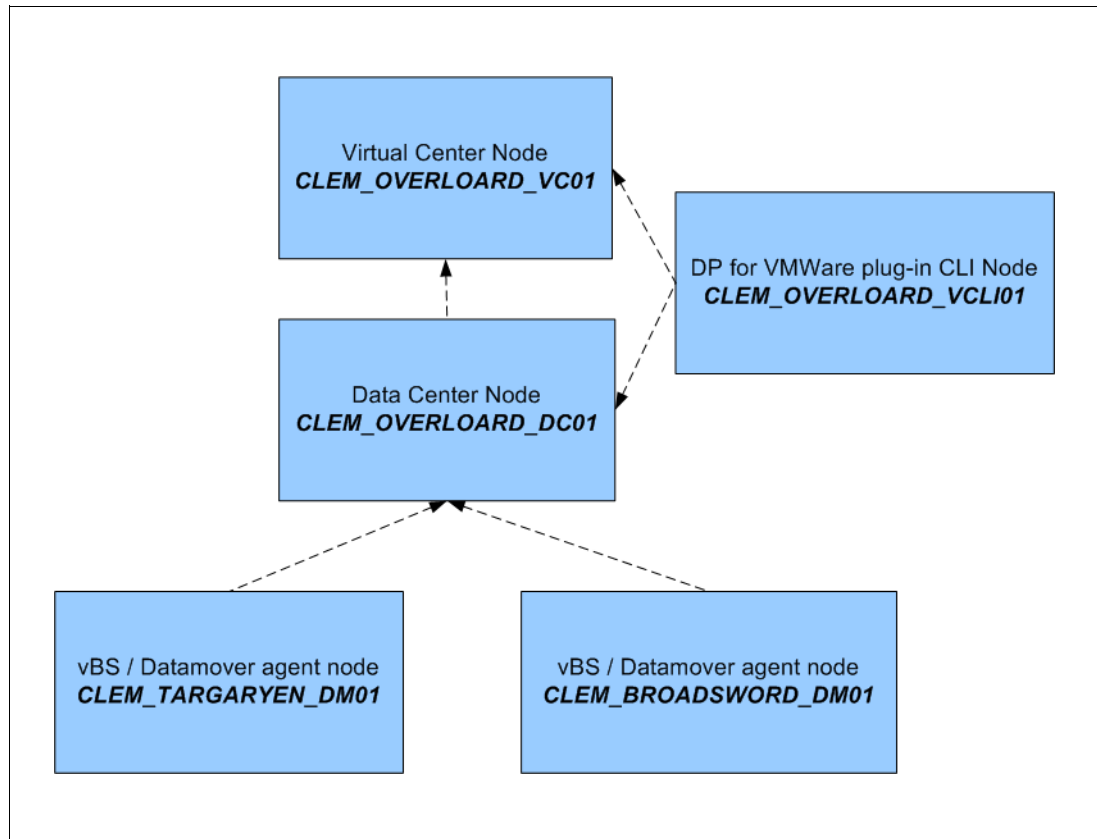


Figure 4-1 Tivoli Storage Manager Node relationship

The relationship includes the following components:

- Datamover agent node

The Tivoli Storage Manager node ID that performs the backup. You can have multiple Tivoli Storage Manager data mover nodes for each vStorage Backup Server. This node must be authorized to back up data on behalf of the data center target node with the **grant proxynode** command. No VM file space exists under this node.

- Datacenter node

A virtual node that maps to a VMware data center. This is the node that owns the VM backup data and contains file spaces for backed up VMs.

- Virtual Center node

A virtual node that maps to a VMware vCenter and is used by the vSphere plug-in.

- Data Protection for VMware CLI node

A common node that is used by the vSphere plug-in GUI to control backup and restore operations.

Note: This chapter provides the commands to register the Tivoli Storage Manager nodes manually on the server to better explain the proxy relationship. However, the Data Protection for VMware vCenter plug-in wizard helps you in this task. You can choose to define those nodes manually or let the DP for VMware plug-in wizard do it for you.

3. Configure the Management class to determine the retention and storage location.

Define the VMDC and VMCTLC management classes on Tivoli Storage Manager.

Example 4-1 shows the commands to create the environment used for this book.

Example 4-1 Lab environment

```

DEFINE DEVCLASS LARGEFILE1 devtype=file mountlimit=50 maxcapa=10G
dir=/tsmdedup1,/tsmdedup2,/tsmdedup3,/tsmdedup4,/tsmdedup5,/tsmdedup6,/tsmdedup7
DEFINE STGPPOOL RAPH-DAT LARGEFILE1 POOLTYPE=PRIMARY HI=100 LO=90 RECLAIM=100
reclaimpro=4 identifyprocess=0 colloc=group MAXSCRATCH=100 deduplicate=yes
reusedelay=0
DEFINE STGPPOOL RAPH-CTL LARGEFILE1 POOLTYPE=PRIMARY HI=100 LO=90 RECLAIM=100
reclaimpro=4 identifyprocess=0 colloc=group MAXSCRATCH=2 deduplicate=yes
reusedelay=0
DEFINE DOMAIN RAPH DESCRIPTION='TSM4VE 6.4 Book'
DEFINE POLICYSET RAPH STANDARD Description='TSM4VE'
DEFINE MGMT RAPH STANDARD D3DAT
DEFINE COPYGROUP RAPH STANDARD D3DAT TYPE=BACKUP DESTINATION=RAPH-DAT
VERE=NoLimit VERD=1 RETEXTRA=14 RETONLY=14
DEFINE COPYGROUP RAPH STANDARD D3DAT TYPE=ARCHIVE DESTINATION=RAPH-DAT RETVER=3
DEFINE MGMT RAPH STANDARD D3CTL
DEFINE COPYGROUP RAPH STANDARD D3CTL TYPE=BACKUP DESTINATION=RAPH-CTL
VERE=NoLimit VERD=1 RETEXTRA=14 RETONLY=14
DEFINE COPYGROUP RAPH STANDARD D3CTL TYPE=ARCHIVE DESTINATION=RAPH-CTL RETVER=3
ASSIGN defmgmt RAPH standard D3DAT
ACTIVATE policyset RAPH STANDARD
REGISTER NODE CLEM_OVERLOAD_VC01 secret domain=RAPH
REGISTER NODE CLEM_OVERLOAD_DC01 secret domain=RAPH MAXNUMP=80
deduplication=clientorserver
REGISTER NODE CLEM_TARGARYEN_DM01 secret domain=RAPH
REGISTER NODE CLEM_BROADSWORD_DM01 secret domain=RAPH
REGISTER NODE CLEM_OVERLORD_VCLI01 secret domain=RAPH
grant proxynode target=CLEM_OVERLOAD_VC01
agent=CLEM_OVERLORD_VCLI01,CLEM_OVERLOAD_DC01
grant proxynode target=CLEM_OVERLOAD_DC01
agent=CLEM_BROADSWORD_DM01,CLEM_TARGARYEN_DM01,CLEM_OVERLORD_VCLI01

```

Figure 4-2 shows the infrastructure that was used for this book.

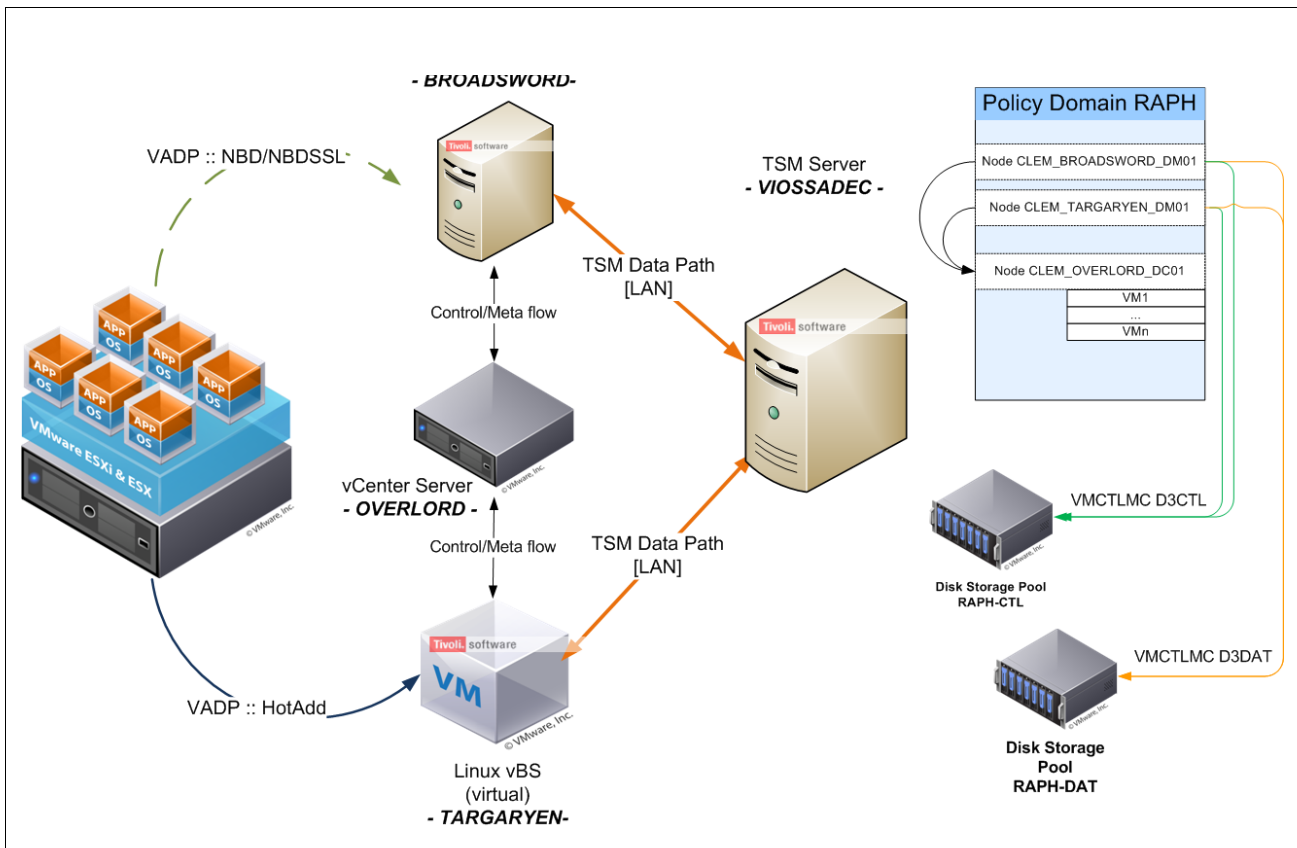


Figure 4-2 Overview of the Virtual Environment

We use two different methods to access the data. The first method uses the network (NBD/NBDSSL) between BROADSWORD and the vSphere infrastructure. The second method uses the HotAdd protocol because TARGARYEN is a VM that is hosted within the vSphere virtual environment that we must protect.

4.2 Tivoli Storage Manager data mover: Backup and archive client

In this section, we describe the steps that used to install and configure the Tivoli Storage Manager Backup-Archive client on a Windows and a Linux machine

Note: In a standard Data Protection for VMware environment, a separate `dsm.opt` file (Windows) or `dsm.sys` file stanza (Linux) is used for each Tivoli Storage Manager data mover node. This allows you to specify different options depending on the activity associated to each node.

When multiple datamover nodes are configured on one vStorage Backup Server, specify a different **TCPClientPort** for client acceptor **daemon**, **schedlogname**, and **errorlogname** option for each `dsm.opt` file or `dsm.sys` file stanza.

When client side deduplication is enabled and these datamover nodes have the authority to move data for the same data center node, each `dsm.opt` file or `dsm.sys` file stanza must include a different value for the **dedupcachepath** option.

4.2.1 Installing Tivoli Storage Manager Backup-Archive client for Windows

Complete the following steps to install the Tivoli Storage Manager Backup-Archive client for Windows:

1. Locate the Backup-Archive client package and start the installer (`setup.exe` file). The Welcome window opens, as shown in Figure 4-3.

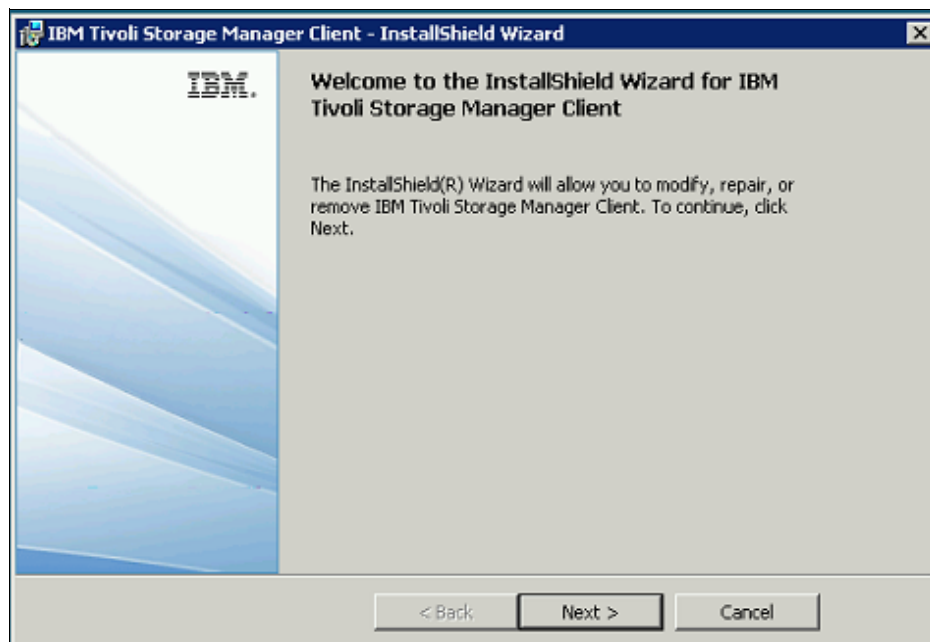


Figure 4-3 Welcome Backup-Archive client window

2. Click **Next** and then select **Custom installation**, as shown in see figure Figure 4-4 on page 66.

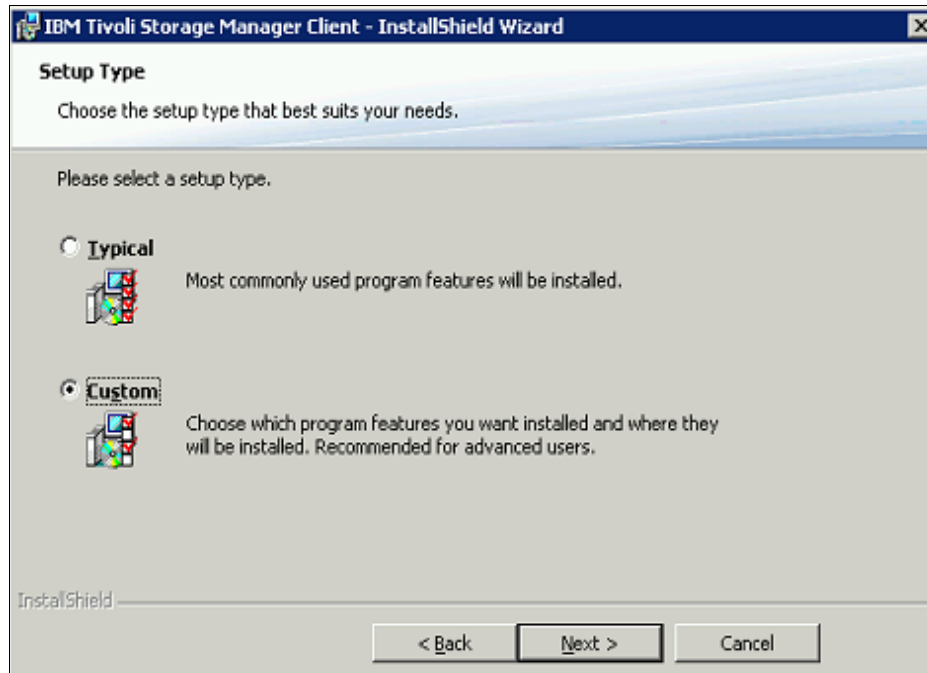


Figure 4-4 Choose Custom installation

3. Select all of the components, as shown in Figure 4-5.

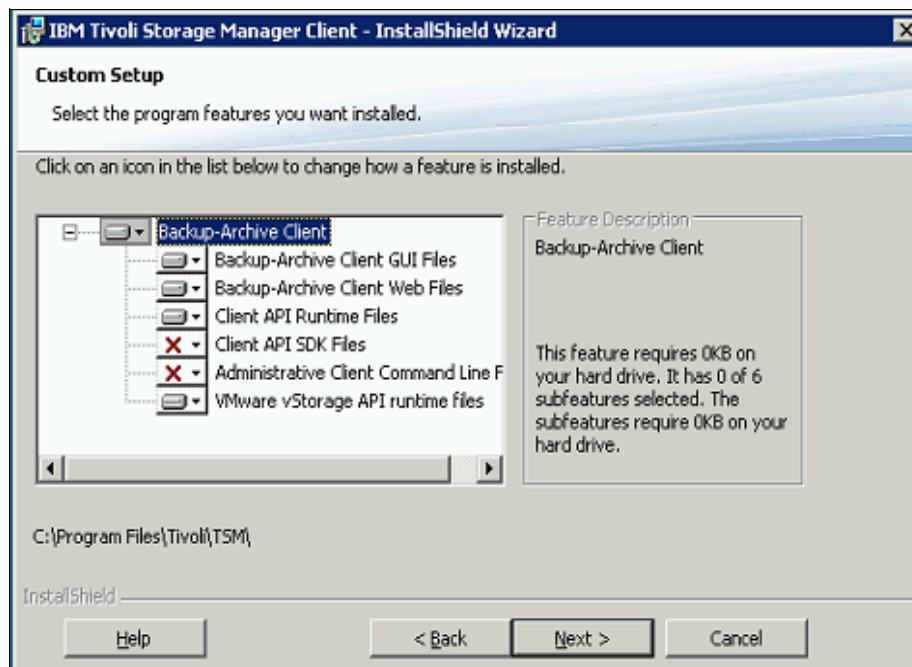


Figure 4-5 Custom selection of Backup-Archive client components

The Datamover activity can be done only if you select VMware vStorage API runtime files.

4. After the components are selected, click **Next** and then **Install**.

The installation takes several minutes. When the installation is complete, the window that is shown in Figure 4-6 on page 67 opens. Click the **Finish**.

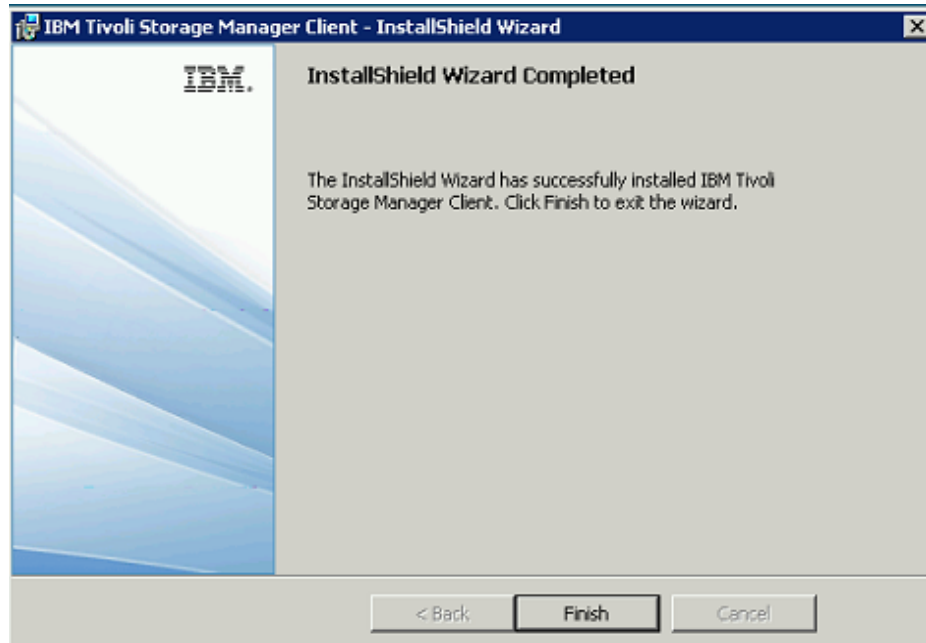


Figure 4-6 Installer completed

After the installation is completed, continue with the configuration.

4.2.2 Configuring Backup-Archive client as a datamover for Data Protection for VMware backup for Windows

Complete the following steps to configure the Backup-Archive client as a datamover for Data Protection for VMware for Windows:

1. Set up the environment variable of the Backup-Archive client to point to the correct datamover configuration file (in our case, the dsm_dm01.opt file).
2. Open a command line prompt and enter the following commands. These commands define environment variables for Tivoli Storage Manager configuration files, installation directory, and a log directory (in our case, c:\exploit\logs):

```
mkdir c:\exploit\logs
SETX /M DSM_CONFIG "C:\Program files\Tivoli\TSM\baclient\dsm_dm01.opt"
SETX /M DSM_DIR "C:\Program files\Tivoli\TSM\baclient"
SETX /M DSM_LOG "C:\exploit\logs"
```

The configuration of Backup-Archive client as a datamover to perform FULL-VM backup is made in the dsm.opt file on a Windows machine.

Example 4-2 shows the configuration file that was used for this book for the datamover Broadsword.

Example 4-2 Datamover configuration file for BROADSWORD

```
** TSM server connection
TCPSEVERADDRESS viossadec
TCPPOINT 1500
nodename CLEM_BROADSWORD_DM01
*asnodename CLEM_OVERLOAD_DC01
passwordaccess generate
schedmod prompted
```

```

MANAGEDSERVICES WEBCLIENT SCHEDULE
errorlogname C:\exploit\logs\dsmeror_dm01.log
schedlogname c:\exploit\logs\dsmsched_dm01.log
errorlogret 7 D
schedlogret 7 D
** TSM4VE Setup *****
** TSM4VE connection
VMCHOST overlord
VMCUSER raphael
*VMCPW - use dsmc set password
VMC D3DAT
VMCTLMC D3CTL
VMBACKUPTYPE FULLVM
VMFULLTYPE VSTOR
VMVSTORTRANSPORT san:hotadd:nbd
** TSM4VE multithread
VMMAXParallel 20
VMLIMITPERDatastore 10
VMLIMITPERHost 10
** TSM4VE RDM
Vmprocessvmwithprdm YES
VMPROCESSVMWITHINDEPENDENT YES
**Backup Scope
DOMAIN.VMFULL "VMHOST=ironthron"
** TSM4VE Setup *****
** Data reduction
DEDUPLICATION          yes
DEDUPCACHEsize         2048
COMPRESSION             yes

```

3. After the dsm.opt file is created, register the password for vCenter connection by using the Tivoli Storage Manager Client command-line interface, as shown in the following example:

```
dsmc set password -type=vm overlord raphael PASSWORD
```

Where **overlord** is the value specified as **VMCHOST** parameter and **raphael** is the value specified as **VMCUSER** parameter in the datamover configuration file.

Note: If you use a configuration file other than dsm.opt or if the DSM_CONFIG environment variable does not point to the right datamover configuration file, specify it by using the **-optfile dsmc** command line option.

4. Validate the connection with the vCenter server by running the following command. It displays VM information that is managed by the defined vCenter server (filtered by **DOMAIN.VMFULL** parameter):

```
dsmc show vm all
```

4.2.3 Configuring Tivoli Storage Manager scheduler and web client for Windows

If you plan to schedule backups or use the vCenter plug-in to start backups, create a Client acceptor Daemon service (CAD), CAD-managed scheduler service, and remote client agent service. These services are required for the vCenter plug-in to communicate with the datamover and for the Tivoli Storage Manager server to trigger action by using its central scheduler. The following commands are used for this book.

```
set DSM_DIR=c:\progra~1\tivoli\tsm\baclient
```

```
dsmcutil install scheduler /name:"TSM_SCHED_DM01" /optfile:%DSM_DIR%\dsm_dm01.opt  
/autostart:no /password:secret /startnow:no /node:CLEM_BROADSWORD_DM01
```

```
dsmcutil install cad /name:"TSM_CAD_DM01" /cadschedname:"TSM_SCHED_DM01"  
/optfile:%DSM_DIR%\dsm_dm01.opt /autostart:yes /password:secret /startnow:no  
/node:CLEM_BROADSWORD_DM01
```

```
dsmcutil install remote /name:"TSM_AGENT_DM01" /optfile:%DSM_DIR%\dsm_dm01.opt  
/partnername:"TSM_CAD_DM01" /password:secret /startnow:no  
/node:CLEM_BROADSWORD_DM01
```

4.2.4 Installing Tivoli Storage Manager Backup-Archive client for Linux

To have the datamover functions available, three packages are required. The following command lines are used to install the packages:

- ▶ rpm -ivh gskcrypt64-8.0.14.14.linux.x86_64.rpm
- ▶ rpm -ivh TIVsm-API64.x86_64.rpm
- ▶ rpm -ivh TIVsm-BA.x86_64.rpm

Note: VMware operations cannot be run when the hardware plug-in product TIVsm-BAhdw is installed and loaded. Uninstall the hardware product or set the option DONTLOAD PIHDW in the options file to prevent the hardware plug-in from being loaded. Alternatively, you can uninstall the TIVsm_BAhdw package if it is not needed for snapshot operations.

Note: The VDDK libraries on a Linux proxy have a dependency on libexpat.so.0, but most current Linux distributions are shipping libexpat.so.1 instead.

A workaround is to create a symbolic link to libexpat.so.1 with the name libexpat.so.0 in the /lib or /usr/lib directory.

For more information, see this website:

<http://www.vmware.com/support/developer/vddk/VDDK-510-ReleaseNotes.html>

Define the Tivoli Storage Manager-related environment variables to make them available for root users by using the following command set:

```
echo "  
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin  
export DSM_CONFIG=/opt/tivoli/tsm/client/ba/bin/dsm.opt  
export DSM_DIR=/opt/tivoli/tsm/client/ba/bin  
export DSMI_DIR=/opt/tivoli/tsm/client/api/bin64  
export DSMI_CONFIG=/opt/tivoli/tsm/client/api/bin64/dsm.opt  
export DSM_LOG=/exploit/logs  
export DSMI_LOG=/exploit/logs  
" >> $HOME/.profile
```

Note: Do not link \$DSMI_DIR files with the \$DSM_DIR files for any reason. The vCenter plug-in generates a file named dsm.sys in the \$DSMI_DIR directory for its own purposes.

You might have trouble with the fuse library. This library is required and not always installed on the system. For more information about this library, see the IBM Technote at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg21577631>

4.2.5 Configuring Backup-Archive client as a datamover for Data Protection for VMware backup for Linux

Complete the following steps to configure the Backup-Archive client as a datamover for Data Protection for VMware backup for Linux:

1. Configure the client option files (dsm.opt and dsm.sys), as shown in Example 4-3 and Example 4-4.

Example 4-3 Datamover's configuration file, Targaryen dsm.opt file

```
ServerName viossadec
```

Example 4-4 Datamover's configuration file, Targaryen dsm.sys file

```
ServerName viossadec  
** TSM server connection  
TCPSERVERADDRESS viossadec  
TCPPOPT 1500  
nodename CLEM_targaryen_DM01  
*asnodename CLEM_OVERLOARD_DC01  
passwordaccess generate  
schedmod prompted  
MANAGESERVICES WEBCLIENT SCHEDULE  
errorlogname /exploit/logs/dsmerror_dm01.log  
schedlogname /exploit/logs/dsmsched_dm01.log  
errorlogret 7 D  
schedlogret 7 D  
  
** TSM4VE connection  
VMCHOST overlord  
VMCUSER raphael  
*VMCPW - use dsmc set password  
VMC D3DAT  
VMCTLMC D3CTL
```

```

VMBACKUPTYPE FULLVM
VMFULLTYPE VSTOR
VMVSTORTTRANSPORT san:hotadd
** TSM4VE multithread
VMMAXParallel 3
VMLIMITPERDatastore 10
VMLIMITPERHost 10
** TSM4VE RDM
Vmprocessvmwithprdm YES
VMPROCESSVMWITHINDEPENDENT YES
**Backup Scope
DOMAIN.VMFULL "VMHOST=ironthron"

** Data reduction
DEDUPLICATION          yes
DEDUPCACHESIZE         2048
COMPRESSION            yes
** end of file

```

2. After the dsm.opt and dsm.sys files are created, register the password for vCenter connection, as shown in the following example:

```
dsmc set password -type=vm overlord raphael PASSWORD
```

Where **overlord** is the value that is specified for **VMCHOST** parameter and **raphael** is the value that is specified for **VMCUSER** parameter in the dsm.opt file.

4.2.6 Configuring Tivoli Storage Manager and web client for Linux

This setup is achieved by entering the following command:

```
chkconfig --add dsmcad
```

Immediately start the service and verify that it is running, as shown in the following example:

```

targaryen:/etc/init.d # /opt/tivoli/tsm/client/ba/bin/rc.dsmcad start
Starting dsmcad: done

targaryen:/etc/init.d # /opt/tivoli/tsm/client/ba/bin/rc.dsmcad status
Checking dsmcad: running
targaryen:/etc/init.d #

```

4.2.7 Configuring multiple datamovers on the same vStorage Backup Server (proxy)

Whatever the platform, if you must create more than one data mover, repeat the configuration tasks for both Backup-Archive client and services, as many as you need instances of the datamover.

By doing so, you can perform the following tasks:

- ▶ Contact more than one vCenter server from the same vStorage Backup Server.
- ▶ Store data into different Datacenter Node, then apply a different backup policy.
- ▶ Contact more than one Tivoli Storage Manager server.

- Dedicate a datamover node to a special resource within a datacenter (for example, one DM per cluster).

4.3 Installing Data Protection for VMware features

In this section, we describe the steps to install and configure Data Protection for VMware features, including the Data Protection for VMware vCenter plug-in.

4.3.1 Installing Data Protection for VMware for Windows

Complete the following steps to install Data Protection for VMware for Windows:

1. Locate and run the installer logged on as Administrator, as shown in Figure 4-7.

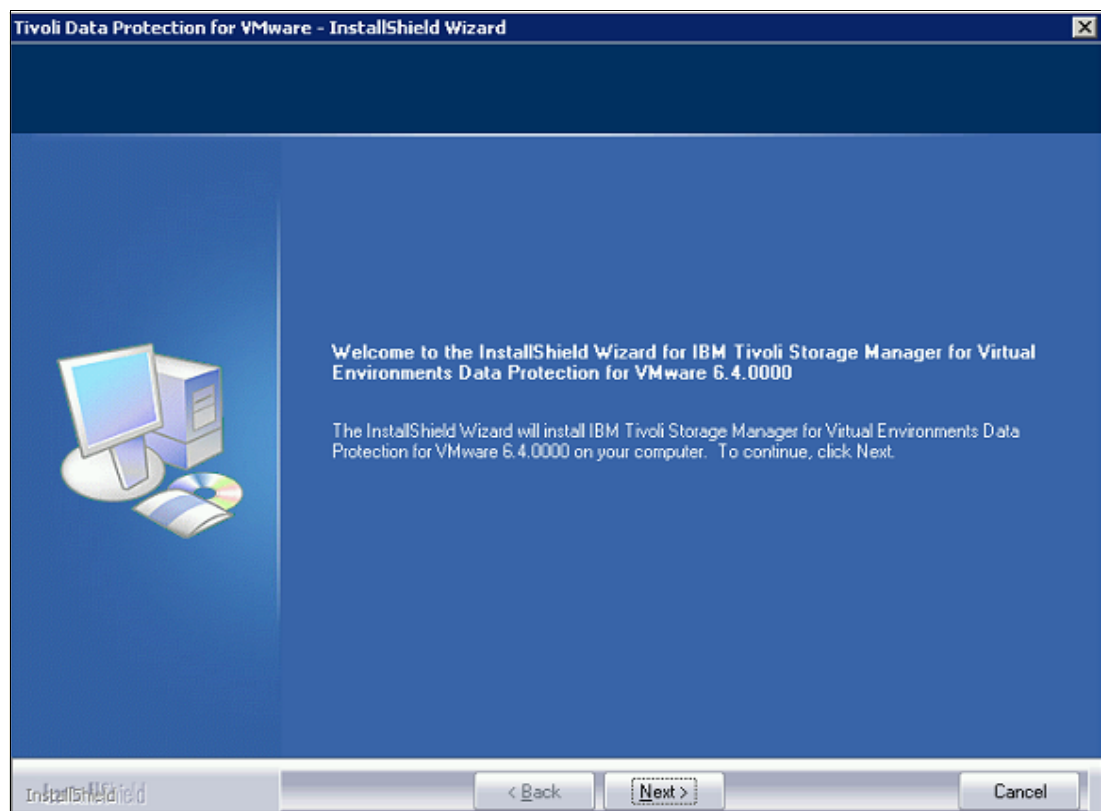


Figure 4-7 Data Protection for VMware installer Welcome window

2. Accept the license agreement as shown in Figure 4-8.

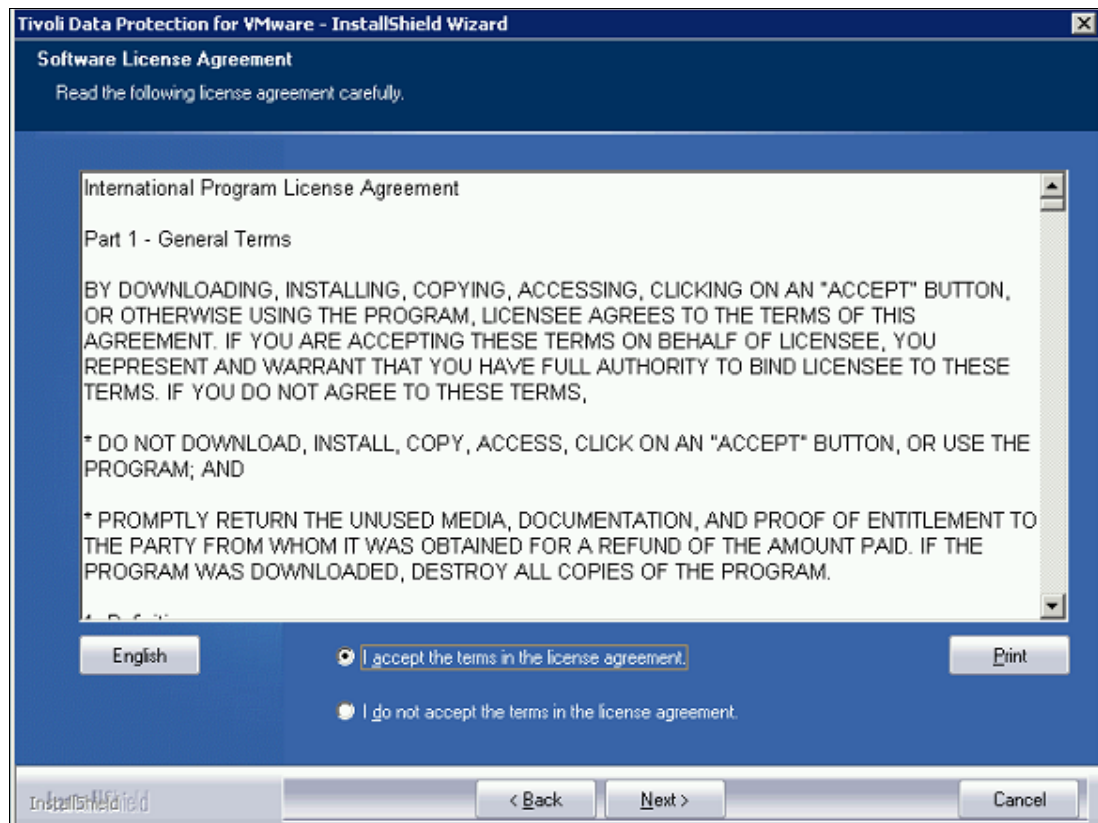


Figure 4-8 Data Protection for VMware license agreement

3. Click **Next**. In the next window, leave the installation path as default and click **Next**.

4. Select the components that you want to install, as shown in Figure 4-9.

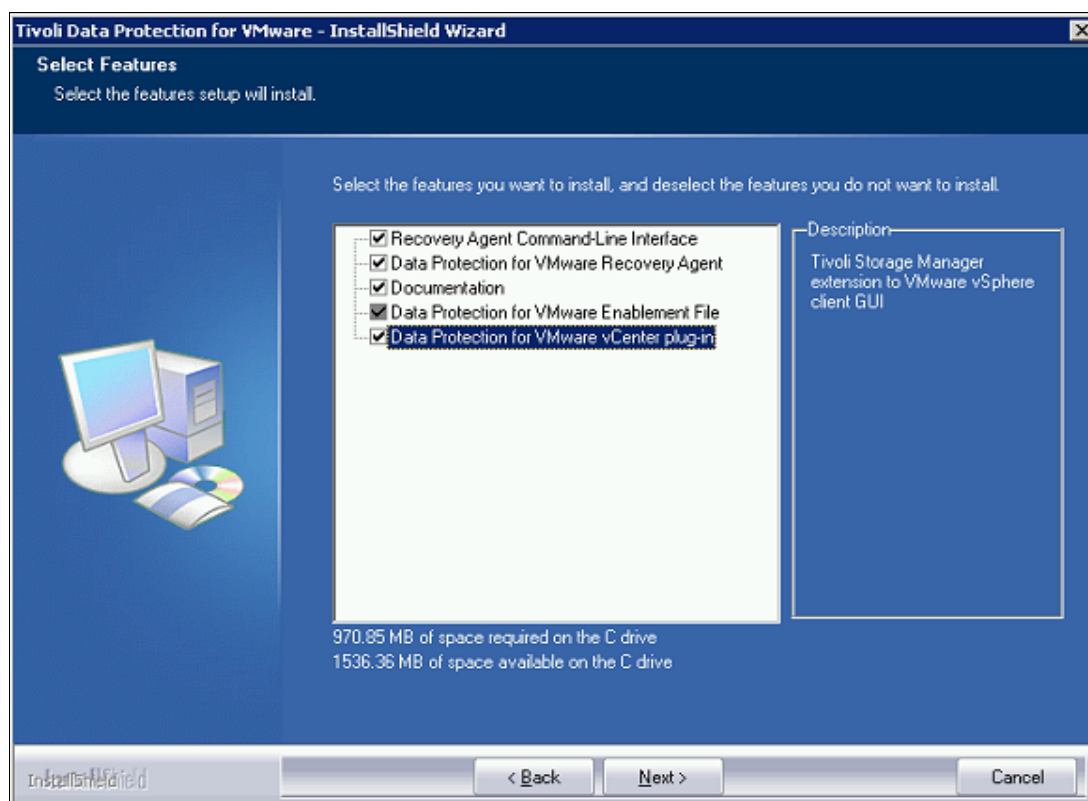


Figure 4-9 Data Protection for VMware components selection

You use the Data Protection for VMware Enablement file to perform incremental forever backups.

The Data Protection for VMware Command-Line and Recovery Agent (GUI) are the tools with which you can perform item-level recovery.

The Data Protection for VMware vCenter plug-in setup prompt for credentials to connect to the vCenter server to deploy the plug-in. For more information, see 3.2.3, “vCenter Server credentials considerations” on page 29.

After you select the components, the wizard helps you through the basic configuration steps that are required to customize Data Protection for VMware services and recovery agent interfaces, as shown in Figure 4-10.

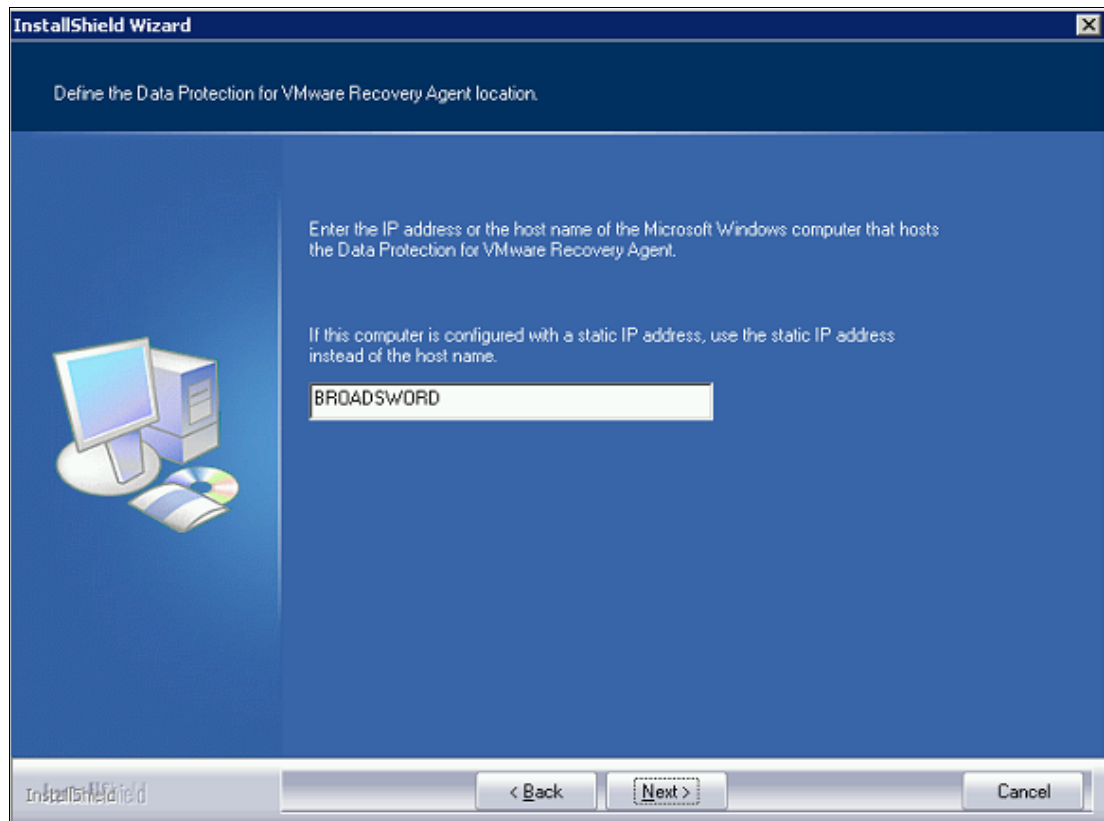


Figure 4-10 Information on which machine will host the DP for VMware recovery agent interface

If you selected to install the vCenter plug-in, the window that is shown in Figure 4-11 opens.

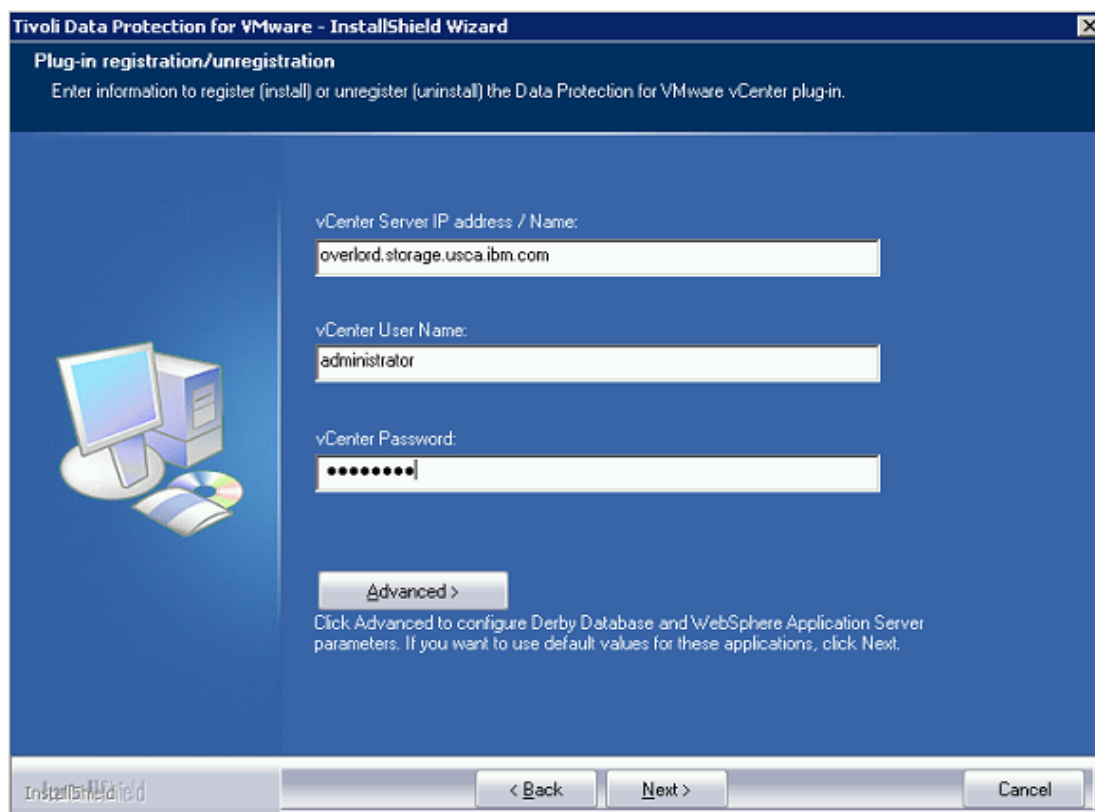


Figure 4-11 vCenter plug-in deployment information

Note: We use administrator user name in Figure 4-11 to install the plug-in on the vCenter server. As described in 3.2.3, “vCenter Server credentials considerations” on page 29, you can use the same user as the one that is defined to perform the backups. In our setup, the user is raphael.

After the installation completes, the window that is shown in Figure 4-12 opens and provides you information about the communication ports.

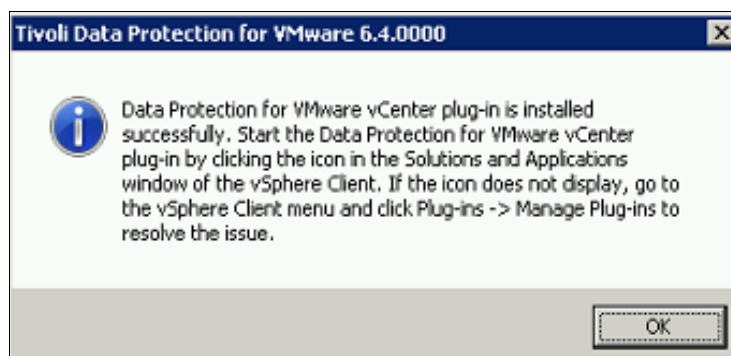


Figure 4-12 Information message on DP for VMware recovery agent

As shown in Figure 4-13, the next window provides information about required open firewall ports.



Figure 4-13 Display message about firewall and used ports

Figure 4-14 shows the Installation Complete message panel. It contains information about how to handle upgrades, compatibilities between Backup-Archive client, Data Protection for VMware, and FlashCopy Manager for VMware.

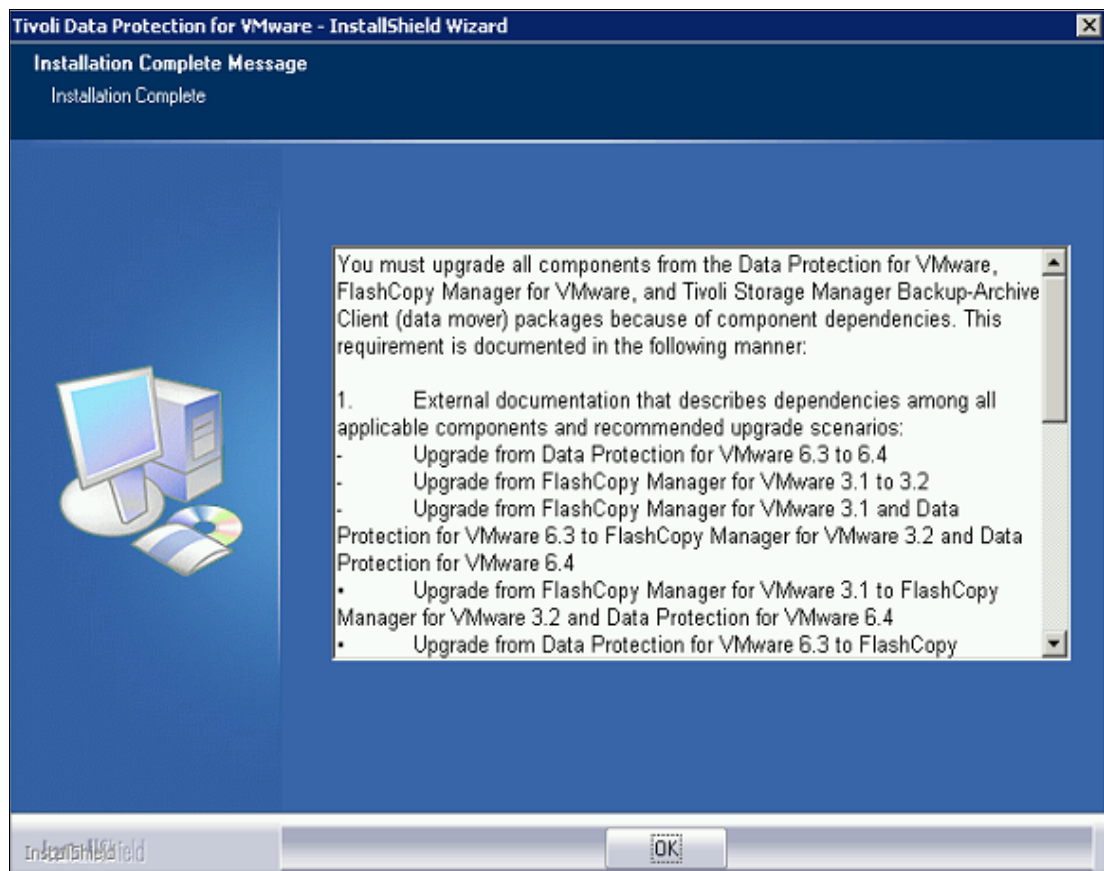


Figure 4-14 Installation complete panel with component upgrade information

5. Restart your computer, as shown in Figure 4-15.

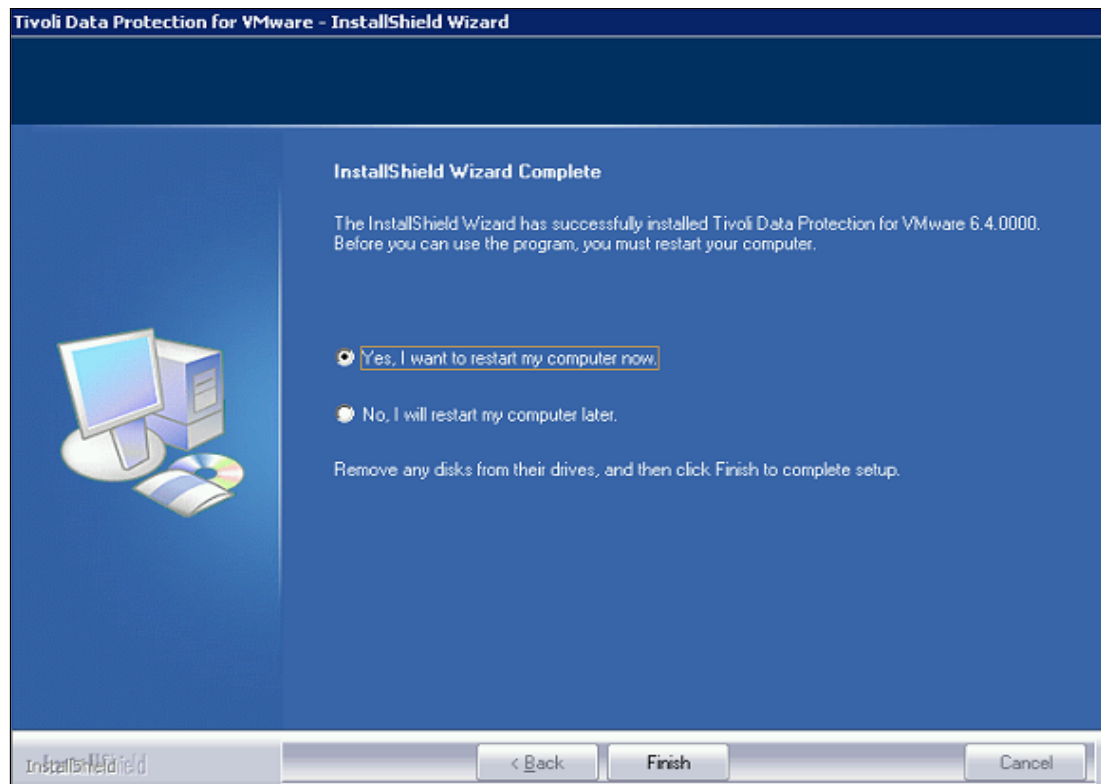


Figure 4-15 Restart your computer

There is no other configuration required to perform VM backups after the Data Protection for VMware is installed because operations are managed by the datamover that was configured. However, the vCenter plug-in does require configuration before you can use it. For more information, see 4.4, "Data Protection for VMware vCenter plug-in configuration" on page 89.

4.3.2 Installing Data Protection for VMware for Linux

Complete the following steps to install Data Protection for VMware for Linux:

1. Locate and run the installer, logged in as root.
2. Start the `install-Linux.bin` file. The wizard opens, as shown in Figure 4-16.

Note: If you do not have a X11 (graphical) based environment, use the option `-i` when you start the installer.

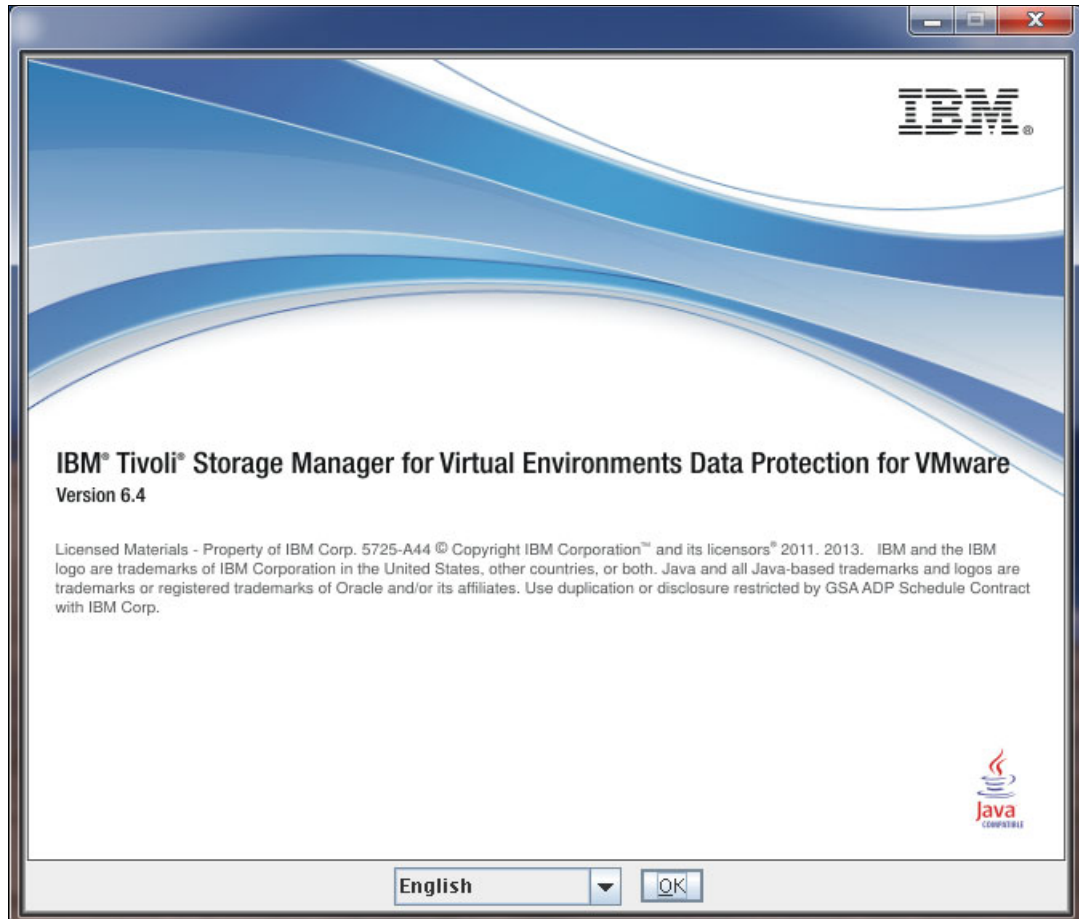


Figure 4-16 Linux Data Protection for VMware Installer Wizard

3. Click **OK** to see the Welcome window. As shown in Figure 4-17, the Welcome window lists all of the steps that are done for the product installation.

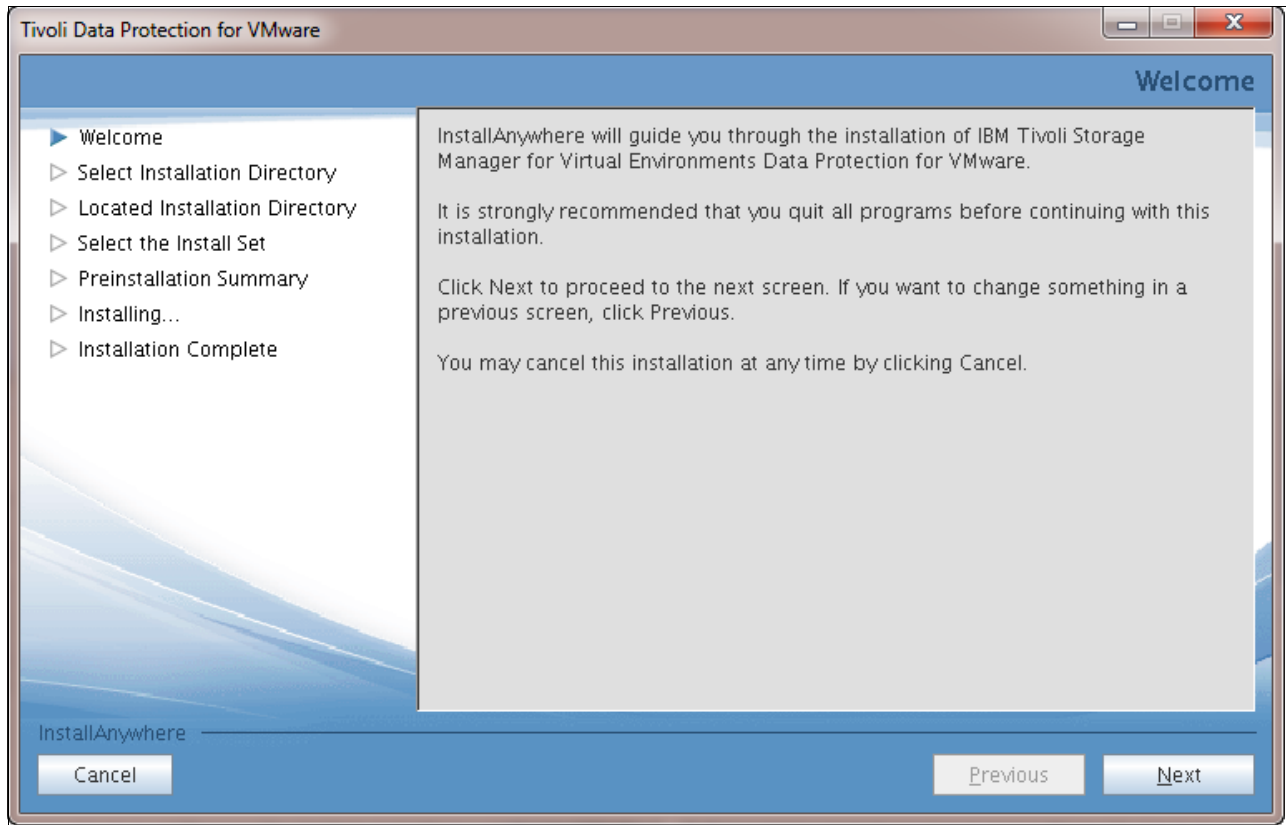


Figure 4-17 Data Protection for VMware Installer Welcome Screen

4. Click **Next**. Accept the license agreement and click **Next**. The installation path selection window opens, as shown in Figure 4-18.

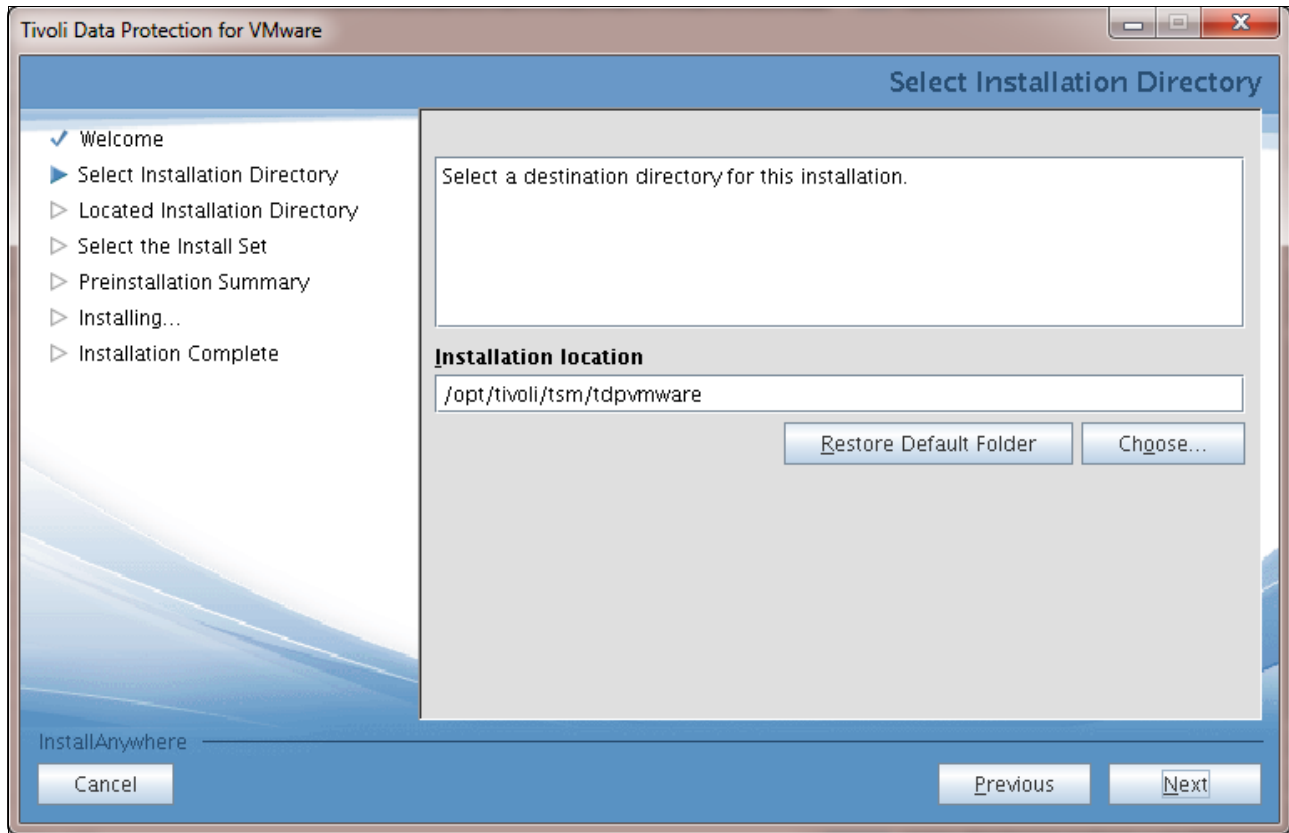


Figure 4-18 Data Protection for VMware Linux Installation path

5. Leave the default installation path and click **Next**.

6. Select the components that you want to install, as shown in Figure 4-19.

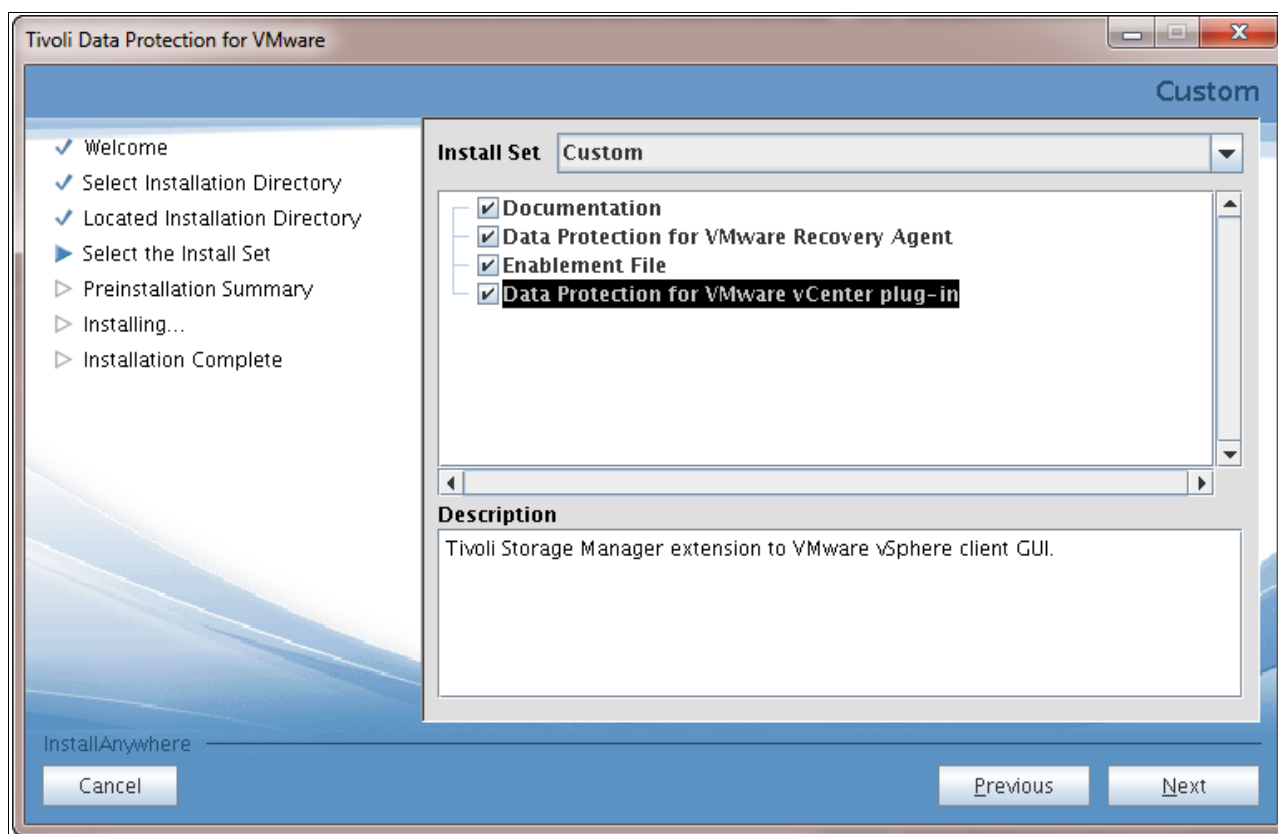


Figure 4-19 Data Protection for VMware components selection

You use the Data Protection for VMware Enablement file to perform incremental forever backup.

The Data Protection for VMware Command-Line and Recovery Agent (GUI) are the tools with which you perform item level recovery.

The Data Protection for VMware vCenter plug-in setup prompts for credentials to connect to the vCenter server to deploy the plug-in. For more information, see 3.2.3, “vCenter Server credentials considerations” on page 29.

If you selected the vCenter plug-in to be installed, the window this is shown in Figure 4-20 opens.

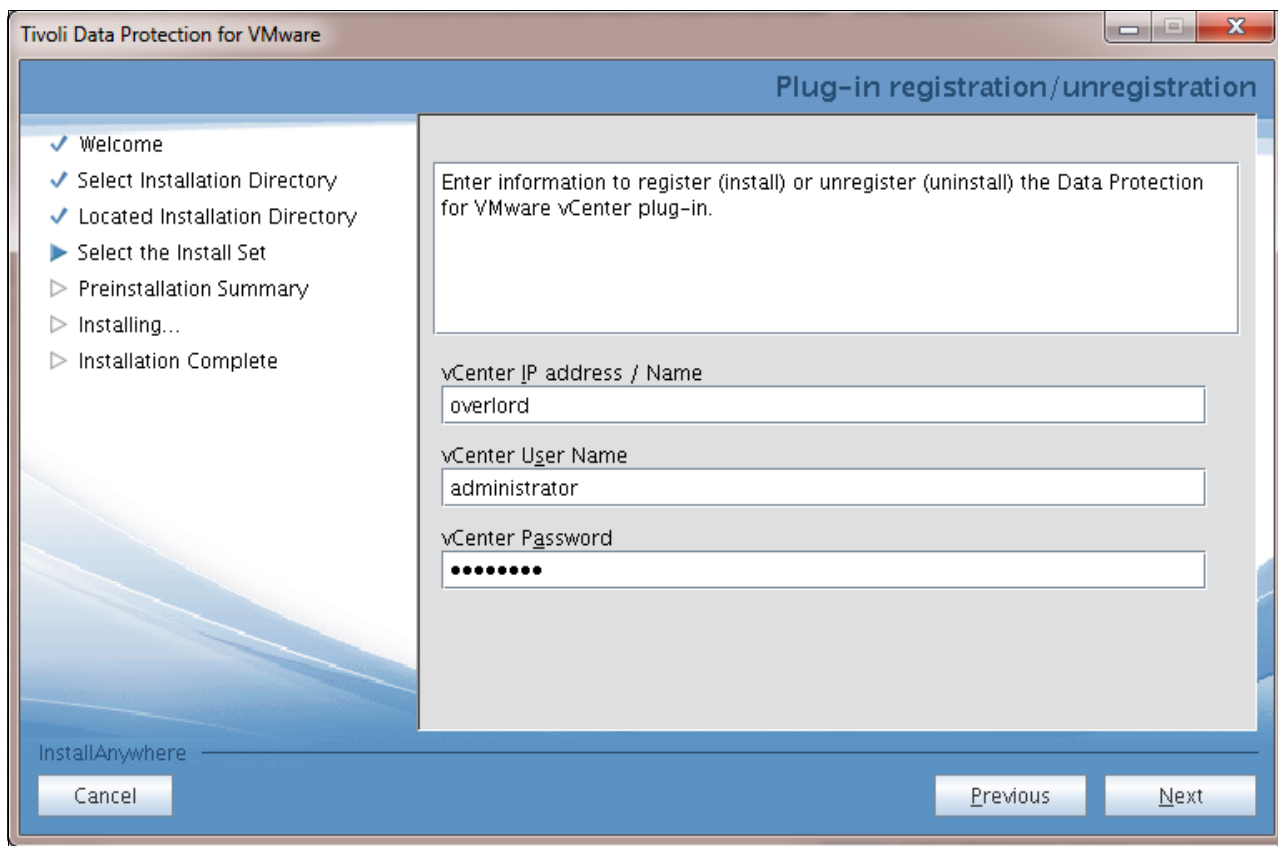


Figure 4-20 Data Protection for VMware vCenter plug-in credentials

Note: We use administrator as the user name in Figure 4-11 to install the plug-in on the vCenter server. As described in 3.2.3, “vCenter Server credentials considerations” on page 29, you can use the same user as the one that is defined to perform the backups. In our setup, raphael is the user.

During the vCenter plug-in installation, a Linux user account named `tdpvmware` is created. This user must be used for every recovery operation. It also owns the vCenter plug-in services WebSphere Application Server service.

7. After you enter all the required information, click **Next**. Leave the default options that are shown in the next window. Click **Next**. The information window that is shown in Figure 4-21 opens.

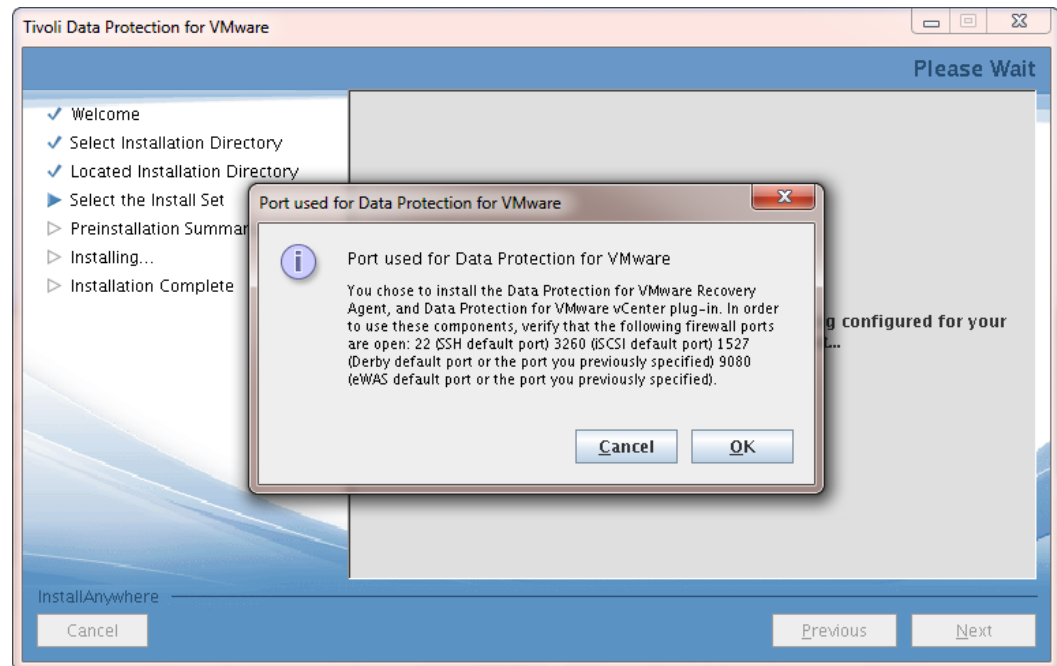


Figure 4-21 Display message about firewall and used ports

8. Click **OK** and review the pre-installation summary, as shown in Figure 4-22. If you want to follow the progress of the installation process, write down the name of the log file, which often is `/root/IA-TDPVMware-xx.log`. Click **Install** to proceed with the installation.

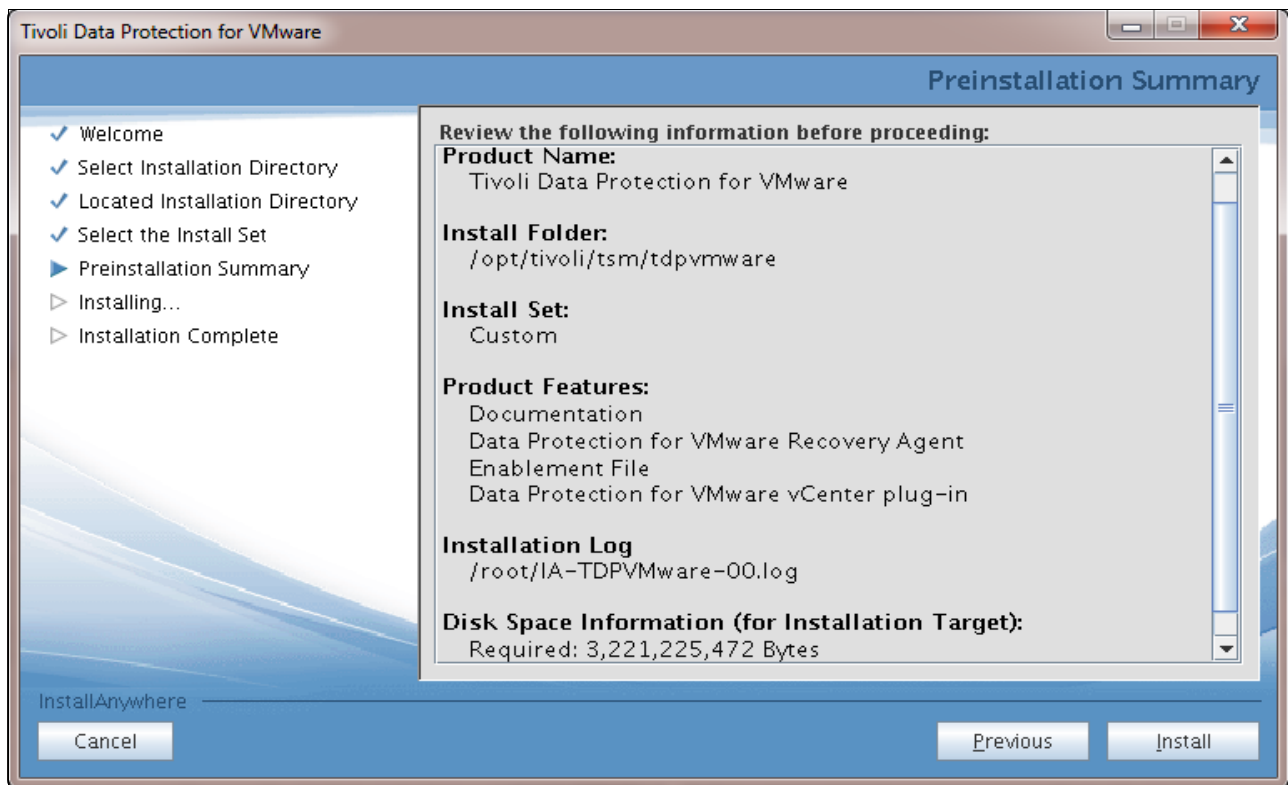


Figure 4-22 Data Protection for VMware Linux Pre installation summary

After the installation completes, the window that is shown in Figure 4-23 opens. It provides information about how to handle upgrades, and the compatibilities between Backup-Archive client, Data Protection for VMware, and FlashCopy Manager for VMware.

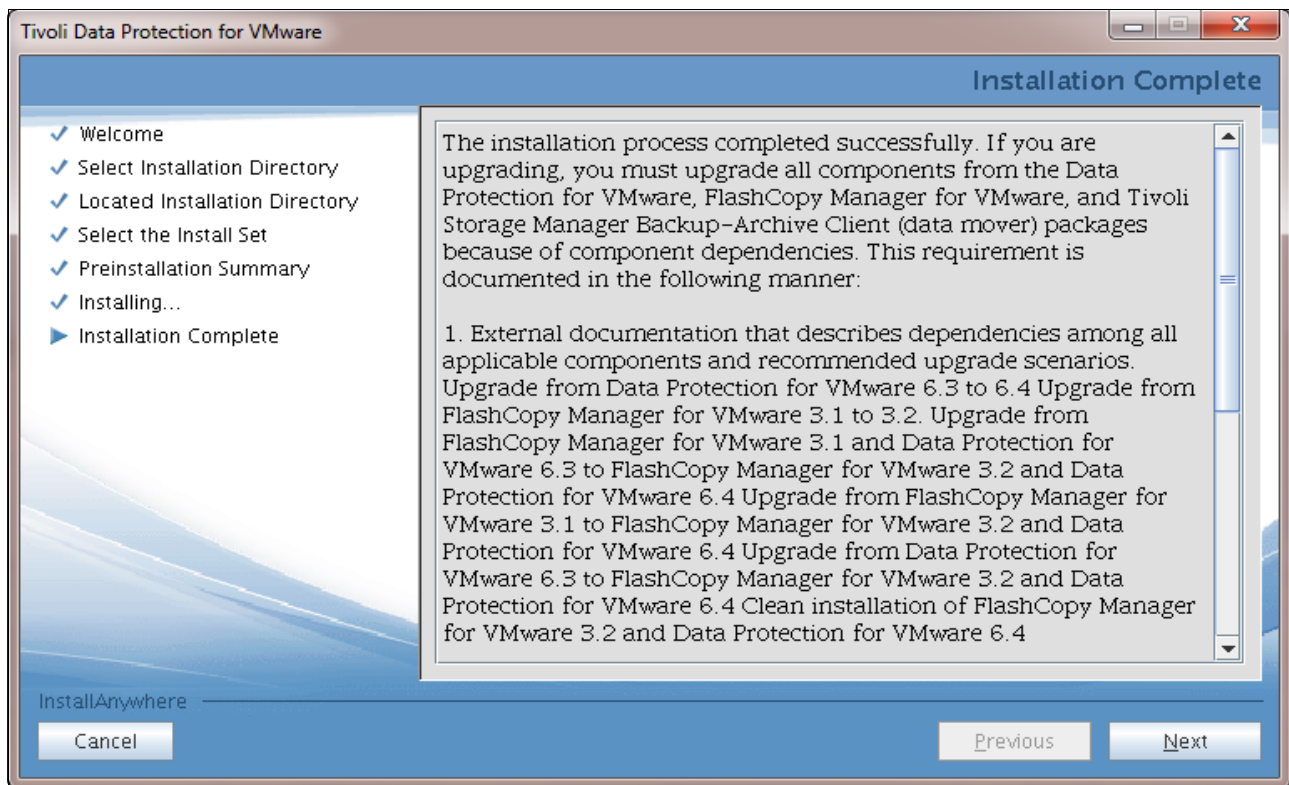


Figure 4-23 Installation complete and upgrade information

No reboot is required on Linux platforms to complete the Data Protection for VMware installation. The last window that opens is a summary of what was installed, as shown in Figure 4-24.

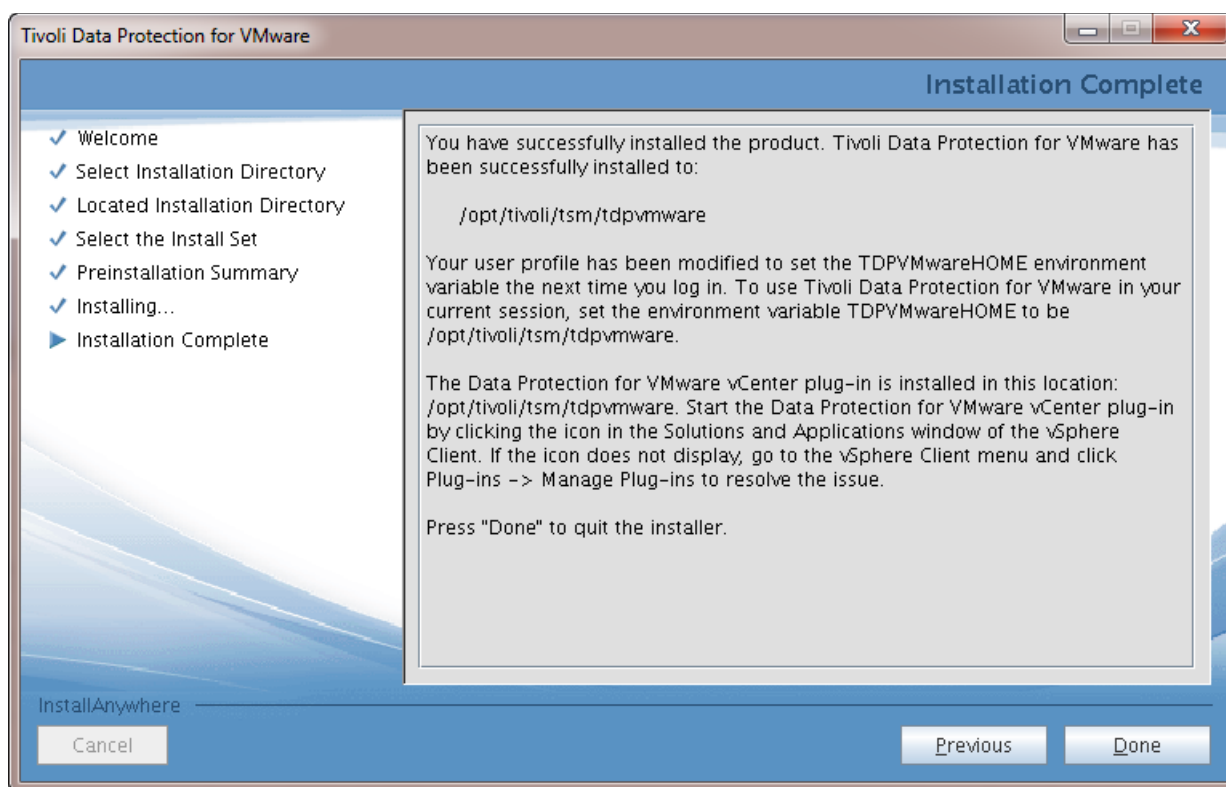


Figure 4-24 Data Protection for VMware Linux Installation Complete window

There is no other configuration required to perform VM backups after the Data Protection for VMware is installed because operations are managed by the datamover that was configured. However, the vCenter plug-in does require configuration. For more information, see 4.4, “Data Protection for VMware vCenter plug-in configuration” on page 89.

4.3.3 Default paths for installed components for Windows

The following default installation directory is used for the Data Protection for VMware Recovery Agent:

(32-bit) C:\Program Files\Tivoli\TSM\TDPVMware\mount
(64-bit) C:\Program Files (x86)\Tivoli\TSM\TDPVMware\mount

The following default installation directory is used for the Data Protection for VMware Recovery Agent logs are:

C:\ProgramData\Tivoli\TSM\TDPVMware\shell
C:\ProgramData\Tivoli\TSM\TDPVMware\mount

The following default installation directory is used for the Recovery Agent CLI:

(32-bit) C:\Program Files\Tivoli\TSM\TDPVMware\shell
(64-bit) C:\Program Files (x86)\Tivoli\TSM\TDPVMware\shell

The following installation directory is used for the Data Protection for VMware vCenter plug-in:

(32-bit) C:\Program Files\Common Files\Tivoli\TDPVMware

(64-bit) C:\Program Files (x86)\Common Files\Tivoli\TDPVMware

This destination cannot be modified by the Choose Destination Location page.

The Data Protection for VMware CLI places log files in the following directory (plug-in log):

(32-bit) C:\Program Files\Common Files\Tivoli\TDPVMware\VMwarePlugin\logs

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

The following default installation directory is used for the embedded WebSphere Application Server:

C:\IBM\tivoli\tsm\tdpvmware\ewas\.

The following Derby Database (database for vmcli command line) is used:

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

The vmcliprofile file (configuration of the vCenter plug-in) is in the following directories:

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

4.3.4 Data Protection for VMware services for Windows

The following services are defined on a Windows platform where the plug-in and recovery agent are installed:

- ▶ WebSphere Application Server (plug-in database):
IBM WebSphere Application Server v8.0 – TSMVE plug-in
- ▶ Service for plug-in CLI interface (read its configuration from the vmcliprofile file)
Data Protection for VMware vCenter command-line interface
- ▶ Data Protection Interface – Recovery agent:
Data Protection for VMware Recovery Agent

4.3.5 Default paths of installed components for Linux

The following default installation directory is used for the Data Protection for VMware Recovery Agent:

/opt/tivoli/tsm/tdpvmware

The following default installation directory is used for the Recovery Agent CLI:

/opt/tivoli/tsm/tdpvmware/mount

The following Derby Database (database for vmcli command line) is used:

/home/tdpvmware/tdpvmware

The following installation directory is used for the Data Protection for VMware vCenter plug-in:

/opt/tivoli/tsm/tdpvmware/common

The following default installation directory is used for the embedded WebSphere Application Server:

```
/opt/tivoli/tsm/tdpvmware/common/ewas
```

Data Protection for VMware recovery agent logs are placed in the following paths on Linux systems:

```
<user.home>/tivoli/tsm/ve/mount/log  
/opt/tivoli/tsm/TDPVMware/mount/engine/var
```

The vmcli profile file (configuration of the vCenter plug-in) is in the following directory:

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

The Data Protection for VMware CLI places log files in the following directory (plug-in log):

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

4.3.6 Data Protection for VMware services for Linux

WebSphere Application Server (plug-in database):

```
/etc/init.d/ewas
```

The following init scripts can be used to stop and start the embedded WebSphere Application Server service:

```
/etc/init.d/ewas stop  
/etc/init.d/ewas start
```

Service for plug-in CLI interface (read its configuration from vmcli profile file) is in the following directory:

```
/etc/init.d/vmcli
```

The vmcli daemon can be stopped and restarted by using the following commands:

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

4.4 Data Protection for VMware vCenter plug-in configuration

There are two ways to configure the plug-in. You can use the vCenter plug-in wizard from the vSphere Client or you can edit the vmcli profile file directly on the machine that holds the vCenter plug-in services.

4.4.1 Using the vCenter plug-in wizard

To access the wizard, start the Data Protection for VMware vCenter plug-in by clicking the icon in the Solutions and Applications window of the vSphere Client. In the Getting Started window, go to the Configuration window and click **Run Configuration Wizard**.

Depending on your environment, you might have to setup Internet Explorer options to display the plug-in. For more information, see Chapter 7 of the *IBM Tivoli Storage Manager for Virtual Environments Data Protection for VMware Installation and User Guide*, SC27-2898.

When the vCenter plug-in is in Linux, you must specify the LD_LIBRARY_PATH in the tdpvmware user profile (\$HOME/.profile). Add the following line in the tdpvmware user profile and restart the ewas and vmclid daemons:

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

If you plan to use the vCenter wizard, you must provide a Tivoli Storage Manager administrator with system privileges so you can register the nodes and perform all the configuration steps.

You can define a dedicated Tivoli Storage Manager administrator for such a task, or use administrator as defined earlier in this documentation; for example, the administrator account that is linked to CLEM_OVERLORD_VCLI01 node. Grant the appropriate level of authority so it can be used to define nodes by using the plug-in wizard, as shown in the following example:

```
GRANT AUTHORITY CLEM_OVERLORD_VCLI01 classes=system
```

Figure 4-25 shows the plug-in wizard.

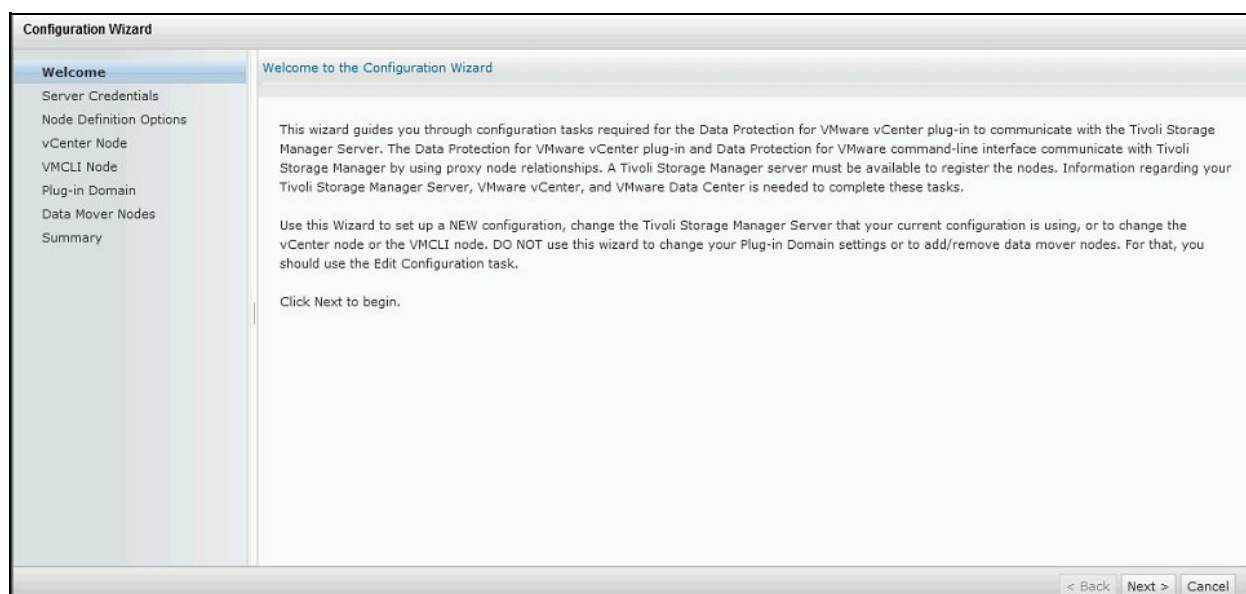


Figure 4-25 Data Protection for VMware vCenter plug-in configuration wizard

4.4.2 Configuring the vCenter plug-in

Complete the following steps to configure the vCenter plug-in:

1. Enter Tivoli Storage Manager server address, TCP port, and administrative ID to issue commands on the Tivoli Storage Manager server, as shown in Figure 4-26 on page 91.

Note: In the following wizard graphics sequence, we chose to not register the node by using the wizard because they were registered in a previous chapter. If you want to register the nodes by using this wizard, select the **Register node** option.

Configuration Wizard

☒ Welcome
☒ **Server Credentials**
 Node Definition Options
 vCenter Node
 VMCLI Node
 Plug-in Domain
 Data Mover Nodes
 Summary

Tivoli Storage Manager Server Credentials

Enter the credential information for the Tivoli Storage Manager Server to use for this product. If you enter a Tivoli Storage Manager Server Administrator ID, make sure that it has unrestricted policy privilege.

Tivoli Storage Manager Server Address

Example: server123.domain.com

Tivoli Storage Manager Server Port

Example: 1500

☒ Use this Tivoli Storage Manager Server Administrator ID to configure TSM objects.

Tivoli Storage Manager Admin ID

Tivoli Storage Manager Admin Password

☐ Save this ID and password for use by all users in future sessions. This overwrites any currently saved values. Enter a blank ID and password to clear any saved values.

Tivoli Storage Manager Admin Port

Example: 1500

☐ Use SSL communications on the Admin Port. Only select this option if the Admin Port is configured as a SSL port in the TSM server. [Learn more...](#)

< Back Next > Cancel

Figure 4-26 Server Credentials information

Pay attention to the account that is specified here and the Save this ID and password for all users in future session... option. For more information about the required privileges to perform operations from this plug-in, and to determine the most suitable Tivoli Storage Manager administrator ID to be recorded here after the setup is done and the nodes are registered, see 3.2.4, “Data Protection for VMware vCenter plug-in user roles” on page 30. (You can modify this account later.)

2. As shown in Figure 4-27, define the node definition options, which are used later in the wizard when defining the datamover and datacenter nodes are defined.

Configuration Wizard

☒ Welcome
☒ Server Credentials
☒ **Node Definition Options**
 vCenter Node
 VMCLI Node
 Plug-in Domain
 Data Mover Nodes
 Summary

Tivoli Storage Manager Node Definition Options

Enter a prefix identifier string to use when naming new Tivoli Storage Manager nodes. Also select the policy domain for the nodes to be registered.

Having a common prefix in the node names makes it easier for the Tivoli Storage Manager Server administrator to identify the nodes in this configuration. This field is optional and allows up to 20 characters.

Append this prefix to node names

Example: MYGROUP

Select the Tivoli Storage Manager Policy Domain to use when registering new nodes

Policy Domain Name:	RAPH
Active Policy Set:	STANDARD
Activated Default Management Class:	D3DAT
Description:	TSM4VE 6.4 Book
Backup Retention (Grace Period):	30
Archive Retention (Grace Period):	365

< Back Next > Cancel

Figure 4-27 Node definitions convention

3. Define the vCenter Node, as shown in Figure 4-28. You can choose whether to define it or use an existing one. In our case, we already defined all the nodes, as described in 4.1.1, “Tivoli Storage Manager server configuration” on page 61.

The screenshot shows the 'Configuration Wizard' window for 'Tivoli Storage Manager vCenter Node'. The left sidebar lists the steps: Welcome, Server Credentials, Node Definition Options, vCenter Node (selected), VMCLI Node, Plug-in Domain, Data Mover Nodes, and Summary. The main area contains the following text: 'A vCenter node is a Tivoli Storage Manager virtual node that represents your vCenter to the Tivoli Storage Manager Server. Register the vCenter node by entering the node and password. If you want to use an existing node, clear the Register Node check box and enter that existing node.' Below this, there is a text field for 'Tivoli Storage Manager vCenter Node name' with the value 'CLEM_OVERLORD_VC01' and an example 'ID_VCHOSTNAME'. There is an unchecked checkbox for 'Register Node'. Below the checkbox are two text fields for 'New Password' and 'Verify New Password'. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

Figure 4-28 vCenter Node name

4. Enter the VMCLI node, as shown in Figure 4-29. You can choose whether to define it or use an existing one. In our case, we already defined all the nodes, as described in 4.1.1, “Tivoli Storage Manager server configuration” on page 61.

The screenshot shows the 'Configuration Wizard' window for 'Tivoli Storage Manager VMCLI Node'. The left sidebar lists the steps: Welcome, Server Credentials, Node Definition Options, vCenter Node, VMCLI Node (selected), Plug-in Domain, Data Mover Nodes, and Summary. The main area contains the following text: 'A VMCLI node connects the Data Protection for VMware command-line interface to the Tivoli Storage Manager Server and to the Tivoli Storage Manager data mover nodes. Register a VMCLI node by entering the node and password. If you want to use an existing node, clear the Register Node check box and enter that existing node.' Below this, there is a text field for 'Tivoli Storage Manager VMCLI Node name' with the value 'CLEM_OVERLORD_VCLI01' and an example 'ID_VMCLI'. There is an unchecked checkbox for 'Register Node'. Below the checkbox are two text fields for 'New Password' and 'Verify New Password'. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

Figure 4-29 VMCLI node name

5. Select the Domain or DataCenter to protect, as shown in Figure 4-30.

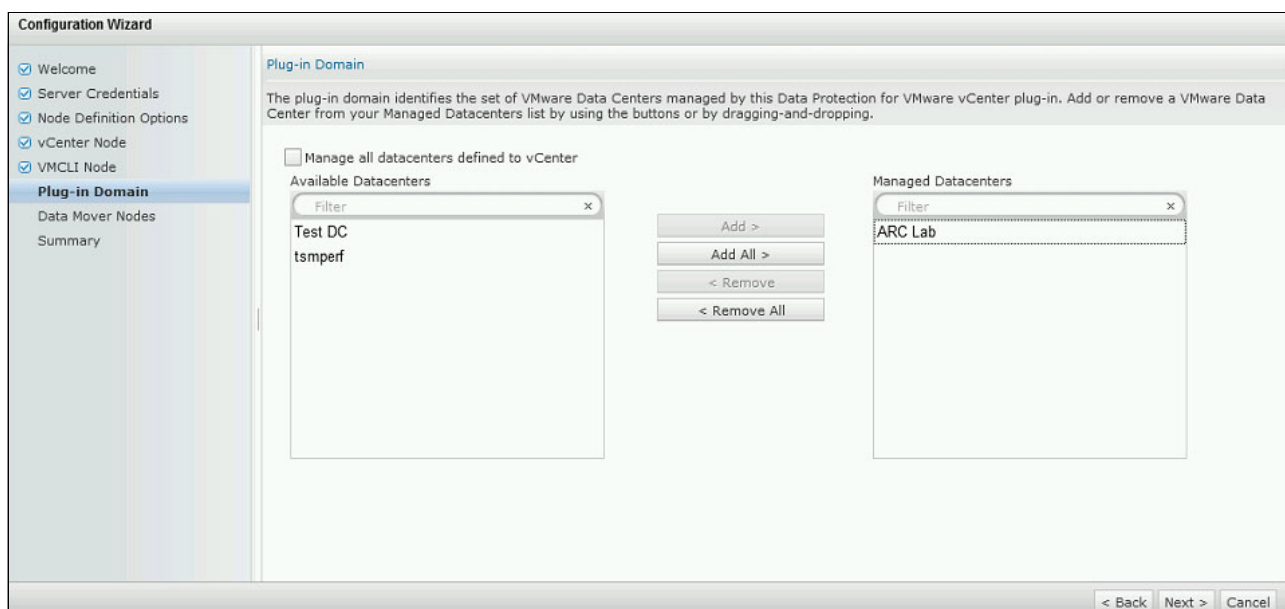


Figure 4-30 Specify the DataCenter in scope of the plug-in

6. Define the datamover and test its availability, as shown in Figure 4-31. In this window, you can use the drop-down list and select **Add** if you want to add more datamovers. You also can choose to define it or use an existing one. In our case, we have registered the nodes, as described in 4.1.1, “Tivoli Storage Manager server configuration” on page 61.

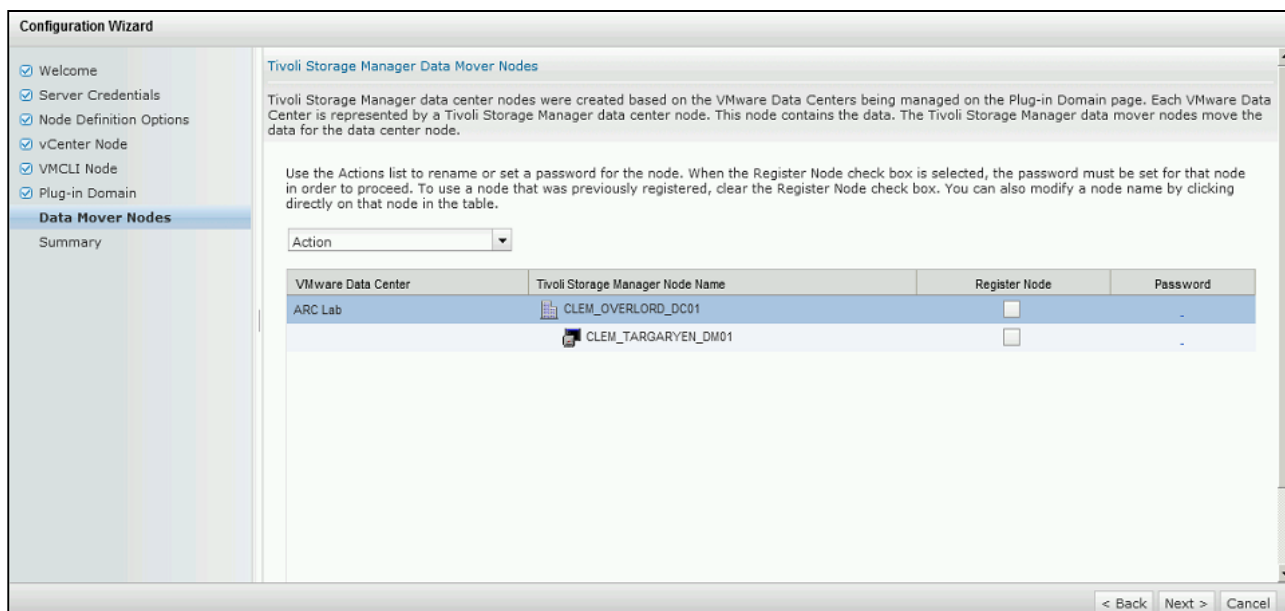


Figure 4-31 Define the datamover nodes associated to data center

After these steps are completed, the wizard runs all of the tasks automatically according to the information that is provided through the wizard. It then displays a Configuration Status panel, as shown in Figure 4-32.

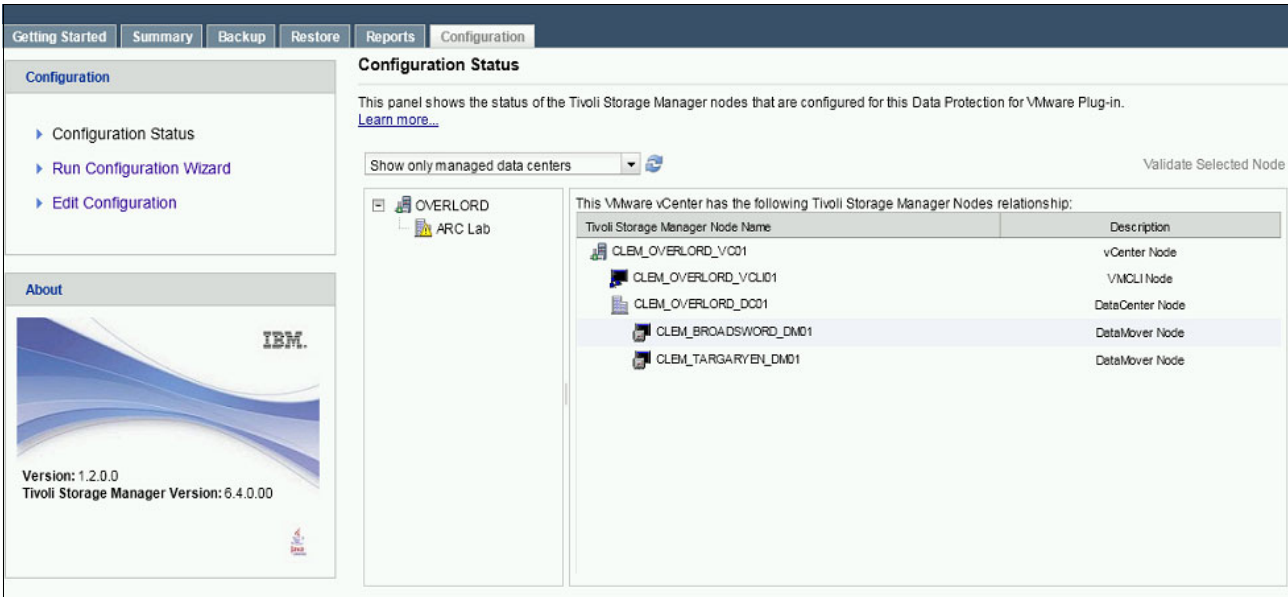


Figure 4-32 Configuration Status panel

If the wizard reports an error during the datamover configuration, check that the Client Acceptor daemon is running on your datamover. For more information about identifying what service must be checked depending on your platform, see 4.2.3, “Configuring Tivoli Storage Manager scheduler and web client for Windows” on page 69 or 4.2.6, “Configuring Tivoli Storage Manager and web client for Linux” on page 71.

4.4.3 Editing the vmcliprofile file for Linux

Editing the `vmcliprofile` file represents an alternative to the plug-in wizard. It should not be considered as the primary method to use to configure the plug-in.

Complete the following steps:

1. Edit the `/opt/tivoli/tsm/tdpvmware/common/scripts/vmcliprofile` and complete it with the appropriate values.

Note: For the `VE_DATACENTER_NAME` parameter, the name of the datacenter is case-sensitive (left side of the “::”, in our example ARC Lab)

Example 4-5 on page 95 shows the `vmcliprofile` file that was created for this book.

Example 4-5 The vmcli profile file that was used in our setup

```
>>> VMCLI
VE_TSM_SERVER_NAME      viossadec.storage.usca.ibm.com
VE_TSM_SERVER_PORT      1500
VE_TSMCLI_NODE_NAME     clem_overlord_vcli01
VE_VCENTER_NODE_NAME    clem_overlord_vc01
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             # backend
specific recon interval setting in seconds default 600s = 10 min
VMCLI_RECON_INTERVAL_TSM 1200           # backend
specific recon interval 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
VE_DATACENTER_NAME      ARC Lab::CLEM_OVERLORD_DC01
<<<
```

2. After the file is correct, set up the password for the node `VE_TSMCLI_NODE_NAME` (`CLEM_OVERLORD_VCLI01`), as shown in Example 4-6. We are logged on as `tdpvmware` user.

Example 4-6 Setup password for node

```
echo secret > pwd.txt
vmcli -f set_password -I pwd.txt
```

3. Restart the WebSphere Application server, as shown in Example 4-7.

Example 4-7 Restart the WebSphere Application Server

```
/opt/tivoli/tsm/tdpvmware/common/scripts/ewas stop
/opt/tivoli/tsm/tdpvmware/common/scripts/ewas start
```

- Restart the Data Protection for VMware CLI, as shown in Example 4-8.

Example 4-8 Restart Data Protection for VMware CLI

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmclid stop  
/opt/tivoli/tsm/tdpvmware/common/scripts/vmclid start
```

- Validate your configuration by running the **inquire_config** query of the **vmcli** command line, as shown in Example 4-9. We are logged on as **tdpvmware** to issue this command.

Example 4-9 Validate the configuration with inquire_config query

```
tdpvmware@targaryen:/opt/tivoli/tsm/client/api/bin64>  
/opt/tivoli/tsm/tdpvmware/tsmcli/bin64/tsmcli -f inquire_config -v  
CLEM_OVERLORD_VC01 -s viossadec -n CLEM_OVERLORD_VCLI01 -p 1500  
Tivoli Storage Manager Command Line Wrapper for Virtual Environments s Version:  
6.4.0.00  
Build Date: Fri Oct 5 11:05:02 2012  
Tivoli Storage Manager API Version 64001  
Tivoli Storage Manager Command Line Wrapper Compile Version 64000  
#PARAM OPERATION_TYPE 4  
#PHASE_COUNT 4  
#PHASE PREPARE  
#PARAM BACKUP_TYPE=0  
#PARAM TSM_SERVER_NAME=VIOSSADEC  
#PARAM TSM_SERVER_PORT=1500  
#PARAM TSMCLI_NODE_NAME=CLEM_OVERLORD_VCLI01  
#PARAM VCENTER_NODE_NAME=CLEM_OVERLORD_VC01  
#PARAM DATACENTER_NODE_NAME=  
#PARAM OFFLOAD_HOST_NAME=  
#PARAM TSM_OPTFILE=/tmp/T4VE_92D4Gs  
#PARAM INPUT_FILE=  
#PARAM TRACEFILE=  
#PARAM TRACEFLAGS=  
#PHASE INITIALIZE  
#PHASE INQUIRE_DATACENTER_NODES  
#CHILD datacenternode:CLEM_OVERLORD_DC01  
#PARENT vcenternode:CLEM_OVERLORD_VC01  
#PHASE INQUIRE_PROXY_NODES  
#CHILD targetnode:CLEM_OVERLORD_DC01  
#PARENT peernode:CLEM_TARGARYEN_DM01  
#CHILD hladdress:targaryen.storage.usca.ibm.com  
#PARENT peernode:CLEM_TARGARYEN_DM01  
#CHILD lladdress:56961  
#PARENT peernode:CLEM_TARGARYEN_DM01  
#CHILD targetnode:CLEM_OVERLORD_DC01  
#PARENT peernode:CLEM_BROADSWORD_DM01  
#CHILD hladdress:broadsword.storage.usca.ibm.com  
#PARENT peernode:CLEM_BROADSWORD_DM01  
#CHILD lladdress:50073  
#PARENT peernode:CLEM_BROADSWORD_DM01  
STATUS=success  
#END
```

4.4.4 Editing the vmcliprofile file for Windows

Editing the vmcliprofile file represents an alternative to the plug-in wizard. It should not be considered as the primary way to configure the plug-in.

Edit the C:\Program Files\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts\vmcliprofile file and complete it with the appropriate values (in this case, we are using a 32-bit system).

Example 4-10 shows the vmcliprofile file that was created for this book.

Example 4-10 The vmcliprofile file that was used in our setup

```
>>> VMCLI
VE_TSM_SERVER_NAME      viossadec.storage.usca.ibm.com
VE_TSM_SERVER_PORT      1500
VE_TSMCLI_NODE_NAME     clem_overlord_vcli01
VE_VCENTER_NODE_NAME    clem_overlord_vc01
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              # backend
specific recon interval setting in seconds default 600s = 10 min
VMCLI_RECON_INTERVAL_TSM 1200            # backend
specific recon interval 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
VE_DATACENTER_NAME      ARC Lab::CLEM_OVERLORD_DC01
<<<
```

6. Validate your configuration by running the **inquire_config** query on the vmcli command line. Run this command as administrator and using the syntax that is shown in Example 4-11.

Example 4-11 vmcli command syntax

```
C:\Program Files\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts>vmcli -f
inquire_config -t TSM
#TASK 3863 inquire_config 20130215233105140
#PARAM DOMAIN=datacentername:ARC Lab
#PARAM INSTALLED=TSM
#RUN 3818 20130215233105140
#LANG en_US
#PARAM BACKEND=TSM
#PARAM OPERATION_TYPE 4
#PHASE_COUNT 4
#PHASE PREPARE
#PARAM BACKUP_TYPE=0
#PARAM TSM_SERVER_NAME=VIOSSADEC.STORAGE.USCA.IBM.COM
#PARAM TSM_SERVER_PORT=1500
#PARAM TSMCLI_NODE_NAME=CLEM_OVERLORD_VCLI01
#PARAM VCENTER_NODE_NAME=CLEM_OVERLORD_VC01
#PARAM DATACENTER_NODE_NAME=
#PARAM OFFLOAD_HOST_NAME=
#PARAM TSM_OPTFILE=C:\Users\ADMINI~1\AppData\Local\Temp\2\T4VCD97.tmp
#PARAM INPUT_FILE=
#PARAM TRACEFILE=
#PARAM TRACEFLAGS=
#PHASE INITIALIZE
#PHASE INQUIRE_DATACENTER_NODES
#CHILD datacenternode:ARC Lab::CLEM_OVERLORD_DC01
#PARENT vcenternode:CLEM_OVERLORD_VC01
#PHASE INQUIRE_PROXY_NODES
#CHILD targetnode:CLEM_OVERLORD_DC01
#PARENT peernode:CLEM_TARGARYEN_DM01
#CHILD hladdress:targaryen.storage.usca.ibm.com
#PARENT peernode:CLEM_TARGARYEN_DM01
#CHILD lladdress:60758
#PARENT peernode:CLEM_TARGARYEN_DM01
#CHILD targetnode:CLEM_OVERLORD_DC01
#PARENT peernode:CLEM_BROADSWORD_DM01
#CHILD hladdress:broadsword.storage.usca.ibm.com
#PARENT peernode:CLEM_BROADSWORD_DM01
#CHILD lladdress:50073
#PARENT peernode:CLEM_BROADSWORD_DM01
#PARAM STATUS=success
#END RUN 3818 20130215233108593
#END TASK 3863
#INFO FMM16014I The return code is 0.
#END
```



Virtual machine backup

This chapter describes the available backup modes and shows the available interfaces to start a virtual machine (VM) backup.

Depending on your role in the infrastructure, you might need to start a VM backup (but not necessarily from the same machine), taking into account your company's User management. To address this, you can perform a backup from different locations and different interfaces by using Data Protection for VMware.

This chapter includes the following topics:

- ▶ Configuring the datamover to control the backup scope and content
- ▶ VM backup by using vCenter plug-in
- ▶ VM backup by using Backup-Archive GUI client
- ▶ VM backup by using the Backup/Archive Client command line
- ▶ VM backup by using Data Protection for VMware CLI
- ▶ Self-contained application protection
- ▶ VM backup optimization

5.1 Configuring the datamover to control the backup scope and content

It is important that you pay particular attention to what you specify in the datamover's configuration file. This file is read every time the datamover carries out a backup task, regardless of which interface starts the backup (Backup-Archive client GUI, command-line, plug-in, or plug-in command line). Therefore, some filters that are established in the datamover option file might be applied. All of those filters are overridden at backup time except the `exclude.vmdisk` filter, as shown in the following examples:

- ▶ `exclude.vmdisk "VM1" "HARD DISK 2,"`
- ▶ `exclude.vmdisk "VM1" "HARD DISK 3,"`
- ▶ `exclude.vmdisk "VM2*" "HARD DISK 2,"`
- ▶ `exclude.vmdisk "VM3?0" "HARD DISK 2,"`

The following DOMAIN.VMFULL filters also are available:

- ▶ VMFOLDER
- ▶ ALL-VM
- ▶ ALL-WINDOWS
- ▶ VMHOST
- ▶ VMHOSTCLUSTER
- ▶ VMDATASTORE
- ▶ VM name with Wildcard
- ▶ VM name
- ▶ VM list

`Exclude.vmdisk` that is listed in the option file might be applied as a filter, unless you specify something else. This is possible only with the Backup-Archive client command line.

5.2 VM backup by using vCenter plug-in

In this section, we describe the steps that are used to perform a VM backup by using the Data Protection for VMware vCenter plug-in.

Per the permission that is granted to Tivoli Storage Administrator that is associated with the plug-in, you might create every type of task (backup, restore, or schedules). For more information about what tasks are allowed depending on your privileges, see 3.2.4, "Data Protection for VMware vCenter plug-in user roles" on page 30.

Go to **vSphere client** → **Solutions and Applications** and select your plug-in icon.

Go to the Backup tab and click **Schedule a backup**, as shown in Figure 5-1. The only way to start a backup through the vCenter plug-in is to schedule it for now or a later time. The schedule can be reused, modified, or restarted at your convenience.

Note: Take care with the configuration work that is done in the datamover option file. If any disk exclusion **EXCLUDE.VMDISK** is in place, this restriction applies wherever the backup is started.

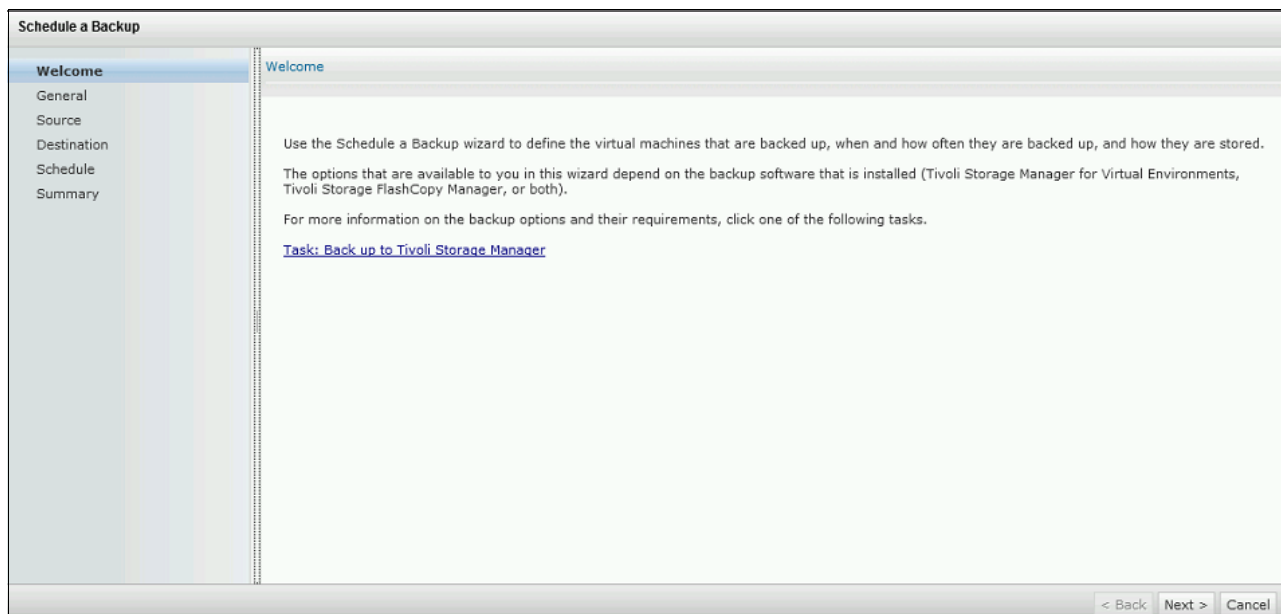


Figure 5-1 Backup schedule wizard

Complete the following steps to start a VM backup:

1. Define a schedule Name and description, as shown in Figure 5-2.



Figure 5-2 Enter schedule name and description

2. Select one or several VMs that are protected, as shown in Figure 5-3.

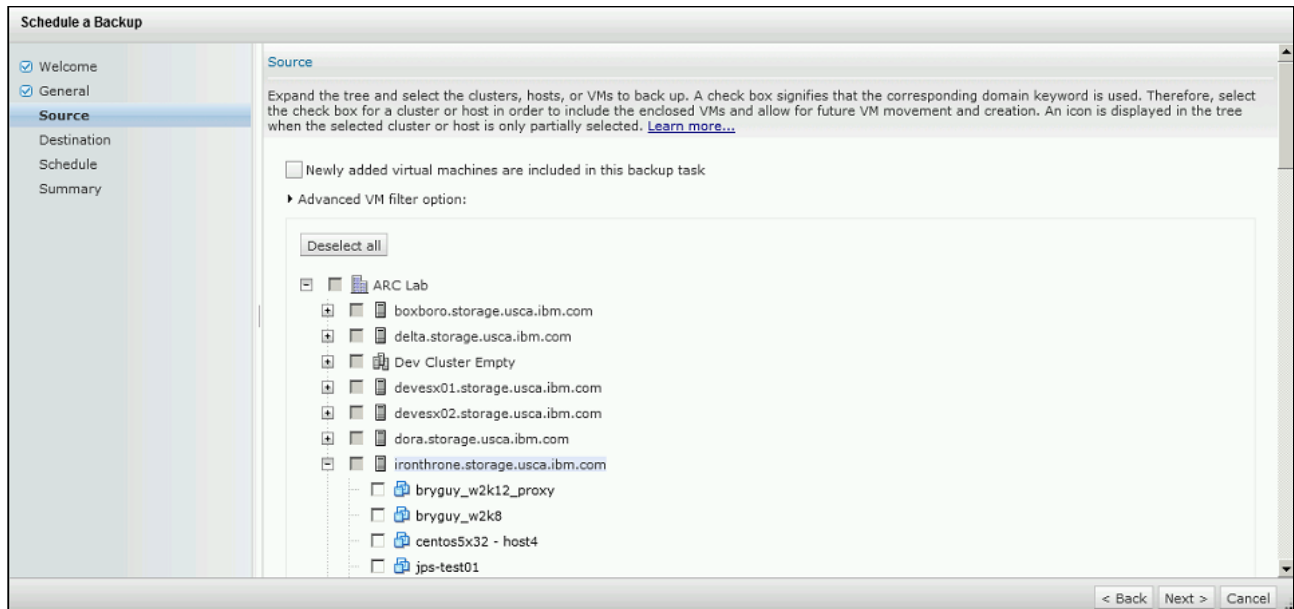


Figure 5-3 Selection of the virtual machines to be backed up

3. Select the datamover that is involved in this backup (the one that is responsible to transfer the data from the datastore to the Tivoli Storage Manager server, as shown in Figure 5-4.

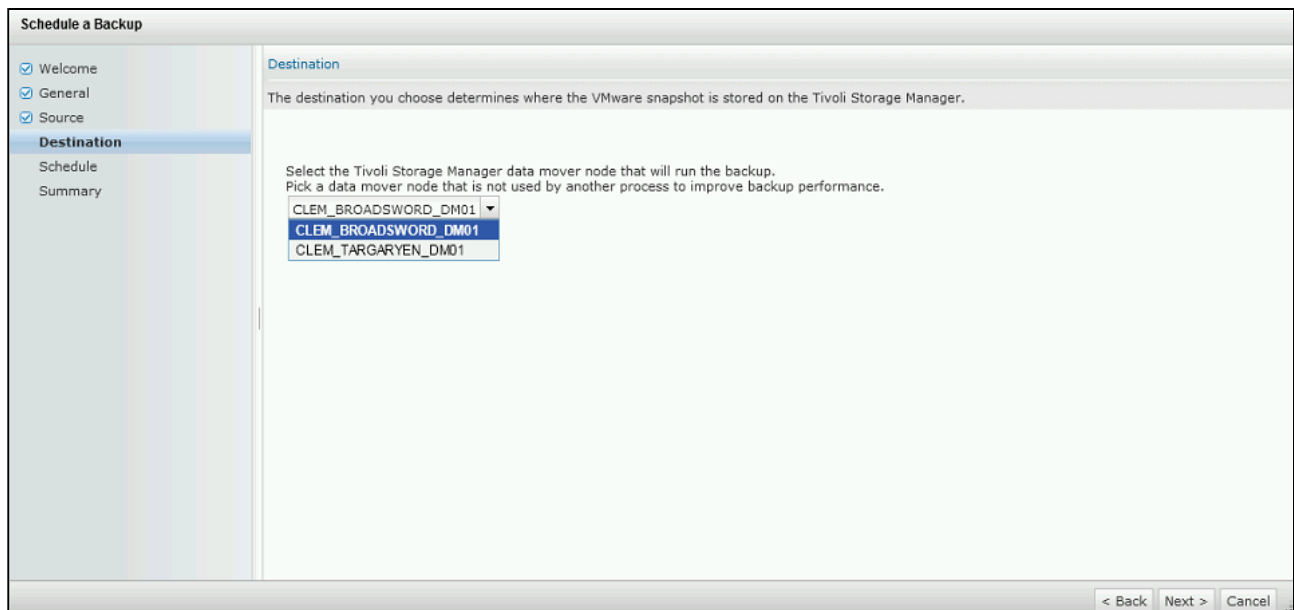


Figure 5-4 Select the datamover that transfers the VM backup data to the Tivoli Storage Manager server

Pay attention to the option “Newly added virtual machines are included in this backup task”. By selecting this option, the schedule being created includes every new VM that is created from this moment, if the new VM matches the selection criteria that is specified for this schedule task. This option is selected by default.

4. Specify the start time and backup type (run now or specify date and time), as shown in Figure 5-5.

Schedule a Backup

Welcome
General
Source
Destination
Schedule
Summary

Schedule

When to start the backup:
☒ Run the backup now
☐ Schedule for later

Select a backup strategy and type. [Learn more...](#)

Backup strategy:
Incremental forever (default)

Backup type:
☒ Incremental
☐ Full

< Back Next > Cancel

Figure 5-5 Specify the backup start time and the backup type

5. Define the schedule start date, start time, day of running and frequency, as shown in Figure 5-6.

Schedule a Backup

Welcome
General
Source
Destination
Schedule
Repetition
Summary

Repetition

* Date and time of the first backup:
2/19/2013 8:45 PM

☐ Back up weekly

☐ Back up every
months

☒ Back up on the following days of the week

☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday
☒ Friday ☐ Saturday ☐ Sunday

< Back Next > Cancel

Figure 5-6 Define schedule details

The schedule that is created in the vCenter plug-in does not create a Tivoli Storage Manager server schedule while the option **Run the backup now** is selected. Otherwise, the plug-in creates a Tivoli Storage Manager server schedule.

The following window opens if the **Schedule for later** option is selected. If the **Run the backup now** option is selected, the wizard goes directly to the last window, which is a summary of the task definition, as shown in Figure 5-7.

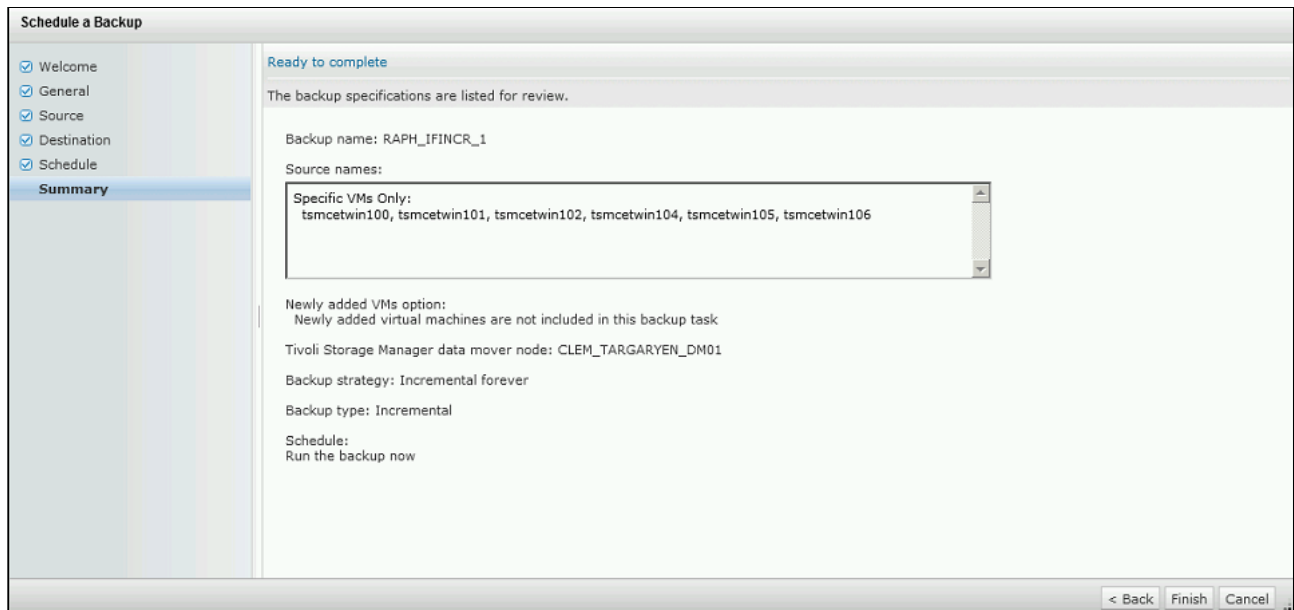


Figure 5-7 Summary of backup schedule task creation

6. Click **Finish** and the backup starts if the **Run the backup now** option was chosen.

If the Schedule for later option was selected, the window that is shown in Figure 5-8 opens to report the schedule creation that is performed on the Tivoli Storage Manager server.

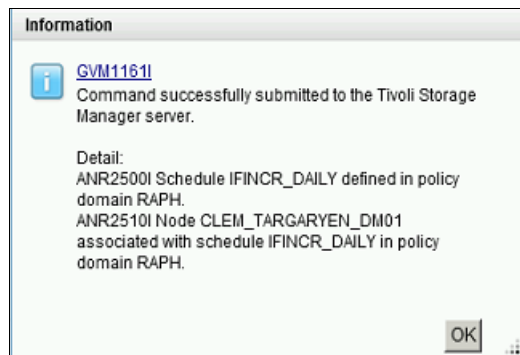


Figure 5-8 Result of Tivoli Storage Manager schedule creation

In this window, you can see that the schedule was successfully defined on the Tivoli Storage Manager server and associated to the datamover node that was specified in the wizard.

On the Tivoli Storage Manager server side, the schedule is shown in Example 5-1.

Example 5-1 Sample schedule

tsm: VIOSSADEC>q sched RAPH f=d

```
Policy Domain Name: RAPH
Schedule Name: IFINCR_DAILY
Description: Daily backup IFINCR for tsmcet101
Action: Backup
Subaction: VM
Options: -vmfulltype=vstor -vmbackuptype=fullvm
-asnodename=CLEM_OVERLORD_DC01 -domain.vmfull="VM=tsmcetwin101"
-MODE=IFIncremental
Objects:
Priority: 5
Start Date/Time: 02/19/13 20:45:00
Duration: 1 Hour(s)
Schedule Style: Enhanced
Period:
Day of Week: Mon,Tue,Wed,Thu,Fri
Month: Any
Day of Month: Any
Week of Month: Any
Expiration:
Last Update by (administrator): CLEM_OVERLORD_VCLI01
Last Update Date/Time: 02/18/13 21:51:45
Managing profile:
```

5.3 VM backup by using Backup-Archive GUI client

Complete the following steps to start a full VM backup (FULL) from the Backup-Archive client GUI:

1. Go to the installation directory: C:\Program Files\tivoli\tsm\baclient (for Windows) or /opt/tivoli/tsm/baclient/bin (for Linux).
2. Start the GUI interface (specify the **asnodename** option) to be authenticated as data center node name. For more information about node name and proxy relationships, see 4.1.1, “Tivoli Storage Manager server configuration” on page 61.
3. Click **Menu** → **Action** → **Backup VM**.
4. Select your ESXi Host and VM.

If you do not know where your VM is, use the Search feature (the Search button in the interface), as shown in Figure 5-9 on page 106. Click **Filter** when the search is completed.

Note: By using the search and filter options, you can select VMs by using one criteria. If you search a second machine by using other criterion, the first VM selection is lost.

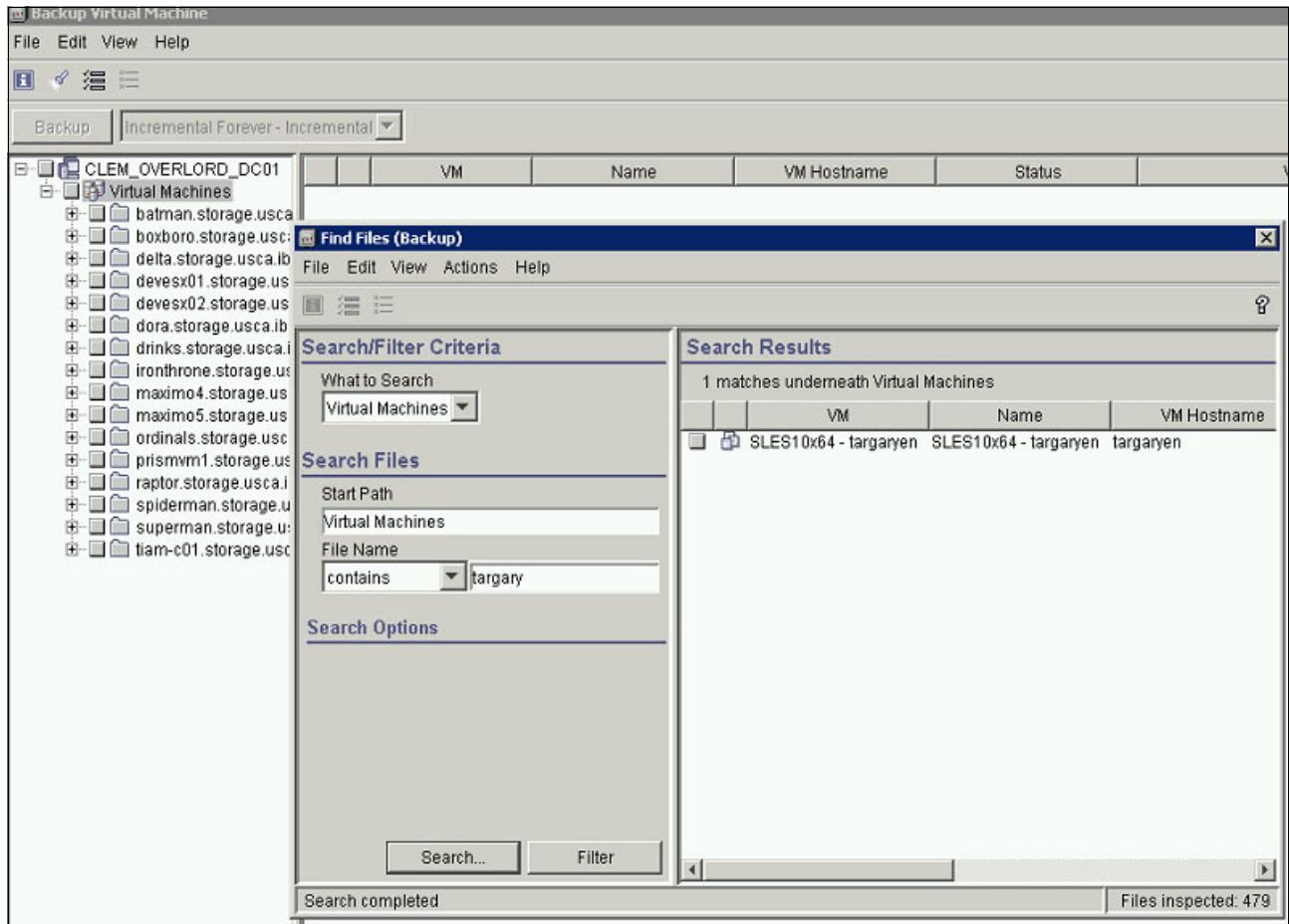


Figure 5-9 Search menu to find your virtual machine

- When you select your VM (one or many), choose the backup mode (as shown in see Figure 5-10) and click **Backup**.

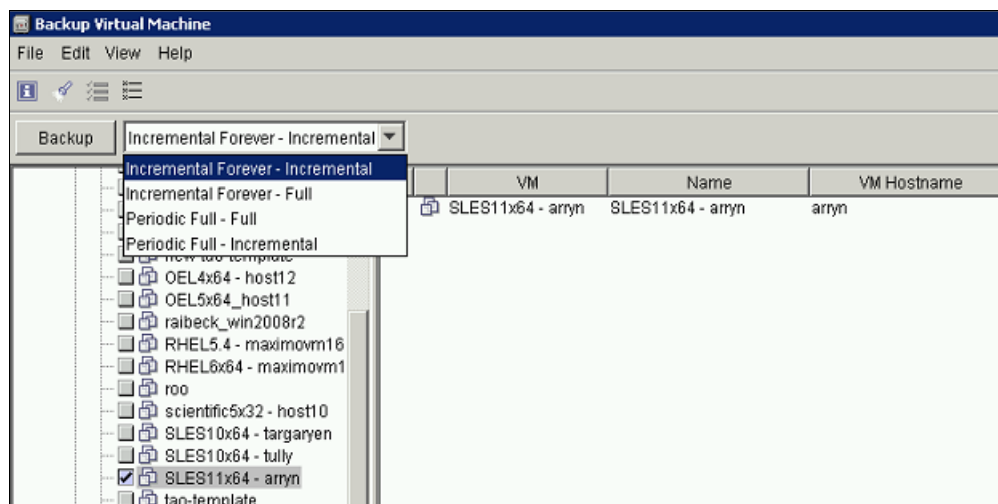


Figure 5-10 Select backup mode

The backup status window opens in which statistics about the running backup are shown.

Note: Be careful with the configuration work that is done in the datamover option file. If any disk exclusion **EXCLUDE.VMDISK** is in place, this restriction applies to your selection.

5.4 VM backup by using the Backup/Archive Client command line

Use the **dsmc backup VM** command to perform the backup. Remember to specify the **asnodename** option to be authenticated as data center node name. For more information about node name and proxy relationships, see 4.1.1, “Tivoli Storage Manager server configuration” on page 61.

You can control the mode by specifying the **-mode** parameter. Choose among IFFULL, IFINCR, FULL, INCR respectively Incremental Forever FULL, Incremental Forever Incremental, Full, or Incremental (with regular FULL).

When the command line is used, the following choices are available to define the scope of the virtual machine to be protected:

- ▶ You can use a wildcard character to specify the VM name so it becomes a list of virtual names.
- ▶ Use the **VMHOST** option to back up all VMs within a host.
- ▶ Use the **VMFOLDER** option to specify a VMware folder as a list of VMs.
- ▶ Use the **VMHOSTCLUSTER** option to include all the VMs within a cluster.
- ▶ Use the **VMDATASTORE** option to protect all the VMs that are held by the datastore.

Note: You can use the **-preview** command line option before you start your backup so that you can validate that the command is correct and view the list of VMs that are selected based on the filters you applied.

Notice that a combination of filter parameters is possible.

Note: The maximum number of characters for the **DOMAIN.VMFULL** value is 1024 when used on the command line. The **DOMAIN.VMFULL** characters limit in the configuration file is 6000.

For more information, see the IBM Technote at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg21632150>

Example 5-2 shows a preview of the backup command, including the **VMDATASTORE** option.

Example 5-2 Back up command with VMDATASTORE option

```
targaryen:/opt/tivoli/tsm/client/ba/bin # dsmc backup vm
-DOMAIN.VMFULL="VMDATASTORE=xiv_cet_1" -preview -asnodename=CLEM_OVERLORD_DC01
IBM Tivoli Storage Manager
Command Line Backup-Archive client Interface
Client Version 6, Release 4, Level 0.1
Client date/time: 02/19/13 11:19:00
(c) Copyright by IBM Corporation and other(s) 1990, 2012. All Rights Reserved.
```

Node Name: CLEM_TARGARYEN_DM01
 Session established with server VIOSSADEC: AIX
 Server Version 6, Release 3, Level 4.0
 Server date/time: 02/19/13 11:20:10 Last access: 02/19/13 11:06:40

Accessing as node: CLEM_OVERLORD_DC01
 2013-02-19T11:19:03.812-08:00 [2AB9C14D57C0 info 'Default'] Initialized channel manager
 2013-02-19T11:19:03.812-08:00 [2AB9C14D57C0 info 'Default'] Current working directory: /opt/tivoli/tsm/client/ba/bin
 2013-02-19T11:19:03.812-08:00 [2AB9C14D57C0 trivia 'Default'] buffer is 'NPTL 2.4'
 2013-02-19T11:19:03.812-08:00 [2AB9C14D57C0 verbose 'ThreadPool'] Thread info: Min Io, Max Io, Min Task, Max Task, Max Thread, Keepalive, exit idle, idle secs, max fds: 2, 21, 2, 10, 31, 4, true, 600
 2013-02-19T11:19:03.812-08:00 [2AB9C14D57C0 trivia 'ThreadPool'] Thread pool launched
 Full BACKUP VM of virtual machines specified in DOMAIN.VMFULL option.

1. vmName: win2008r2 - baratheon
 DomainKeyword: vmdastore=xiv_cet_1
 VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
 VMDK[1]Name: '[xiv_cet_1] win2008r2 - baratheon/win2008r2 - baratheon-000001.vmdk'
 VMDK[1]Status: Included
2. vmName: tsmcetwin94
 DomainKeyword: vmdastore=xiv_cet_1
 VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
 VMDK[1]Name: '[xiv_cet_1] tsmcetwin94/tsmcetwin94.vmdk'
 VMDK[1]Status: Included
3. vmName: tsmcetwin93
 DomainKeyword: vmdastore=xiv_cet_1
 VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
 VMDK[1]Name: '[xiv_cet_1] tsmcetwin93/tsmcetwin93.vmdk'
 VMDK[1]Status: Included
4. vmName: tsmcetwin95
 DomainKeyword: vmdastore=xiv_cet_1
 VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
 VMDK[1]Name: '[xiv_cet_1] tsmcetwin95/tsmcetwin95.vmdk'
 VMDK[1]Status: Included
5. vmName: RHEL6x64 - maximovm18
 DomainKeyword: vmdastore=xiv_cet_1
 VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
 VMDK[1]Name: '[xiv_cet_1] RHEL6x64 - maximovm18/RHEL6x64 - maximovm18.vmdk'
 VMDK[1]Status: Included
6. vmName: tsmcetwin92
 DomainKeyword: vmdastore=xiv_cet_1
 VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
 VMDK[1]Name: '[xiv_cet_1] tsmcetwin92/tsmcetwin92.vmdk'
 VMDK[1]Status: Included
7. vmName: SLES11x64 - arryn
 DomainKeyword: vmdastore=xiv_cet_1
 VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)

```

        VMDK[1]Name: '[xiv_cet_1] SLES11x64 - arryn/SLES11x64 - arryn.vmdk'
        VMDK[1]Status: Included
8. vmName: tsmcetwin91
    DomainKeyword: vmdastore=xiv_cet_1
    VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
    VMDK[1]Name: '[xiv_cet_1] tsmcetwin91/tsmcetwin91.vmdk'
    VMDK[1]Status: Included
9. vmName: win2008x64 - vStorage Backup Server1
    DomainKeyword: vmdastore=xiv_cet_1
    VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
    VMDK[1]Name: '[xiv_cet_1] win2008x64 - vStorage Backup
Server1/win2008x64 - vStorage Backup Server1-000009.vmdk'
    VMDK[1]Status: Included
    VMDK[2]Label: 'Hard disk 2' (Hard Disk 2)
    VMDK[2]Name: '[xiv_cet_1] win2008x64 - vStorage Backup
Server1/win2008x64 - vStorage Backup Server1_1-000008.vmdk'
    VMDK[2]Status: Included
10. vmName: tsmcetwin105
    DomainKeyword: vmdastore=xiv_cet_1
    VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
    VMDK[1]Name: '[xiv_cet_1] tsmcetwin105/tsmcetwin105.vmdk'
    VMDK[1]Status: Included
11. vmName: SLES10x64 - tully
    DomainKeyword: vmdastore=xiv_cet_1
    VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
    VMDK[1]Name: '[xiv_cet_1] SLES10x64 - tully/SLES10x64 - tully.vmdk'
    VMDK[1]Status: Included
12. vmName: win2008r2x64 - winterfell
    DomainKeyword: vmdastore=xiv_cet_1
    VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
    VMDK[1]Name: '[xiv_cet_1] win2008r2x64 - winterfell/win2008r2x64 -
winterfell.vmdk'
    VMDK[1]Status: Included
    VMDK[2]Label: 'Hard disk 2' (Hard Disk 2)
    VMDK[2]Name: '[xiv_cet_2] win2008r2x64 - winterfell/win2008r2x64 -
winterfell.vmdk'
    VMDK[2]Status: Included
    VMDK[3]Label: 'Hard disk 3' (Hard Disk 3)
    VMDK[3]Name: '[xiv_cet_4] win2008r2x64 - winterfell/win2008r2x64 -
winterfell.vmdk'
    VMDK[3]Status: Included
    VMDK[4]Label: 'Hard disk 4' (Hard Disk 4)
    VMDK[4]Name: '[xiv_cet_3] win2008r2x64 - winterfell/win2008r2x64 -
winterfell.vmdk'
    VMDK[4]Status: Included

```

Total number of virtual machines processed: 12

Accessing as node: CLEM_OVERLORD_DC01

Example 5-3 shows a preview of the backup command, including the **VMDATASTORE** and **VMHOSTCLUSTER** options.

Example 5-3 Backup command that includes the VMDATASTORE and VMHOSTCLUSTER options

```
targaryen:/opt/tivoli/tsm/client/ba/bin # dsmc backup vm
-DOMAIN.VMFULL="VMHOSTCLUSTER=ARC Lab;VMDATASTORE=xiv_cet_3" -preview
-asnodename=CLEM_OVERLORD_DC01
IBM Tivoli Storage Manager
Command Line Backup-Archive client Interface
  Client Version 6, Release 4, Level 0.1
  Client date/time: 02/19/13  11:29:39
(c) Copyright by IBM Corporation and other(s) 1990, 2012. All Rights Reserved.

Node Name: CLEM_TARGARYEN_DM01
Session established with server VIOSSADEC: AIX
  Server Version 6, Release 3, Level 4.0
  Server date/time: 02/19/13  11:30:54  Last access: 02/19/13  11:29:25

Accessing as node: CLEM_OVERLORD_DC01
2013-02-19T11:29:48.143-08:00 [2AED25D907C0 info 'Default'] Initialized channel
manager
2013-02-19T11:29:48.144-08:00 [2AED25D907C0 info 'Default'] Current working
directory: /opt/tivoli/tsm/client/ba/bin
2013-02-19T11:29:48.144-08:00 [2AED25D907C0 trivia 'Default'] buffer is 'NPTL 2.4'
2013-02-19T11:29:48.144-08:00 [2AED25D907C0 verbose 'ThreadPool'] Thread info: Min
Io, Max Io, Min Task, Max Task, Max Thread, Keepalive, exit idle, idle secs, max
fds: 2, 21, 2, 10, 31, 4, true, 600
2013-02-19T11:29:48.144-08:00 [2AED25D907C0 trivia 'ThreadPool'] Thread pool
launched
Full BACKUP VM of virtual machines specified in DOMAIN.VMFULL option.
```

1. vmName: tsmcetlnx84
DomainKeyword: vmdatastore=xiv_cet_3
VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
VMDK[1]Name: '[xiv_cet_3] tsmcetlnx84/tsmcetlnx84.vmdk'
VMDK[1]Status: Included
2. vmName: tsmcetlnx80
DomainKeyword: vmdatastore=xiv_cet_3
VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
VMDK[1]Name: '[xiv_cet_3] tsmcetlnx80/tsmcetlnx80.vmdk'
VMDK[1]Status: Included
VMDK[2]Label: 'Hard disk 2' (Hard Disk 2)
VMDK[2]Name: '[xiv_cet_3] tsmcetlnx80/tsmcetlnx80_1.vmdk'
VMDK[2]Status: Included
3. vmName: tsmcetwin108
DomainKeyword: vmdatastore=xiv_cet_3
VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
VMDK[1]Name: '[xiv_cet_3] tsmcetwin108/tsmcetwin108.vmdk'
VMDK[1]Status: Included
4. vmName: tsmcetwin101
DomainKeyword: vmdatastore=xiv_cet_3
VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)
VMDK[1]Name: '[xiv_cet_3] tsmcetwin101/tsmcetwin101.vmdk'
VMDK[1]Status: Included

Total number of virtual machines processed: 4
Accessing as node: CLEM_OVERLORD_DC01

Example 5-4 shows a preview of the backup command using wildcard filter.

Example 5-4 Backup command that uses wildcard filter

```
targaryen:/opt/tivoli/tsm/client/ba/bin # dsmc backup vm "*tsmportal*" -preview  
-asnodename=CLEM_OVERLORD_DC01
```

IBM Tivoli Storage Manager

Command Line Backup-Archive client Interface

Client Version 6, Release 4, Level 0.1

Client date/time: 02/18/13 18:19:31

(c) Copyright by IBM Corporation and other(s) 1990, 2012. All Rights Reserved.

Node Name: CLEM_TARGARYEN_DM01

Session established with server VIOSSADEC: AIX

Server Version 6, Release 3, Level 4.0

Server date/time: 02/18/13 18:20:41 Last access: 02/18/13 18:20:09

Accessing as node: CLEM_OVERLORD_DC01

2013-02-18T18:19:36.059-08:00 [2B8AD65727C0 info 'Default'] Initialized channel manager

2013-02-18T18:19:36.060-08:00 [2B8AD65727C0 info 'Default'] Current working directory: /opt/tivoli/tsm/client/ba/bin

2013-02-18T18:19:36.060-08:00 [2B8AD65727C0 trivia 'Default'] buffer is 'NPTL 2.4'

2013-02-18T18:19:36.060-08:00 [2B8AD65727C0 verbose 'ThreadPool'] Thread info: Min Io, Max Io, Min Task, Max Task, Max Thread, Keepalive, exit idle, idle secs, max fds: 2, 21, 2, 10, 31, 4, true, 600

2013-02-18T18:19:36.060-08:00 [2B8AD65727C0 trivia 'ThreadPool'] Thread pool launched

Full BACKUP VM of virtual machines '*tsmportal*'.

```
1. vmName: win2008x64 - tsmportal  
   DomainKeyword: vm=*tsmportal*  
   VMDK[1]Label: 'Hard disk 1' (Hard Disk 1)  
   VMDK[1]Name: '[xiv_cet_7] win2008x64 - tsmportal/win2008x64 -  
tsmportal-000003.vmdk'  
   VMDK[1]Status: Included
```

Total number of virtual machines processed: 1

Accessing as node: CLEM_OVERLORD_DC01

Example 5-5 shows the command that is used to back up all VMs that contain a pattern of tsm in their name.

Example 5-5 Backup of all virtual machines with tsm in their name

```
targaryen:/opt/tivoli/tsm/client/ba/bin # dsmc backup vm "*tsmp*" -mode=IFINCR
-asnodename=CLEM_OVERLORD_DC01
```

IBM Tivoli Storage Manager

Command Line Backup-Archive client Interface

Client Version 6, Release 4, Level 0.1

Client date/time: 02/18/13 18:27:31

(c) Copyright by IBM Corporation and other(s) 1990, 2012. All Rights Reserved.

Node Name: CLEM_TARGARYEN_DM01

Session established with server VIOSSADEC: AIX

Server Version 6, Release 3, Level 4.0

Server date/time: 02/18/13 18:28:40 Last access: 02/18/13 18:28:04

Accessing as node: CLEM_OVERLORD_DC01

2013-02-18T18:27:34.396-08:00 [2B7D8C30D7C0 info 'Default'] Initialized channel manager

2013-02-18T18:27:34.396-08:00 [2B7D8C30D7C0 info 'Default'] Current working directory: /opt/tivoli/tsm/client/ba/bin

2013-02-18T18:27:34.397-08:00 [2B7D8C30D7C0 trivia 'Default'] buffer is 'NPTL 2.4'

2013-02-18T18:27:34.397-08:00 [2B7D8C30D7C0 verbose 'ThreadPool'] Thread info: Min Io, Max Io, Min Task, Max Task, Max Thread, Keepalive, exit idle, idle secs, max fds: 2, 21, 2, 10, 31, 4, true, 600

2013-02-18T18:27:34.397-08:00 [2B7D8C30D7C0 trivia 'ThreadPool'] Thread pool launched

Full BACKUP VM of virtual machines '*tsmp*'.

Backup VM command started. Total number of virtual machines to process: 1

Accessing as node: CLEM_OVERLORD_DC01

Starting Full VM backup of VMware Virtual Machine 'win2008x64 - tsmportal'

mode: 'Incremental Forever - Incremental'

target node name: 'CLEM_OVERLORD_DC01'

data mover node name: 'CLEM_TARGARYEN_DM01'

application protection type: 'TSM VSS'

application(s) protected: 'MS SQL 2008'

Creating snapshot for virtual machine 'win2008x64 - tsmportal'

Backing up Full VM configuration information for 'win2008x64 - tsmportal'

16,658 VM Configuration [Sent]

Processing snapshot

disk: [xiv_cet_7] win2008x64 - tsmportal/win2008x64 - tsmportal-000003.vmdk (Hard Disk 1)

Capacity: 42,949,672,960

Data to Send: 304,218,112

Transport: (hotadd)[sending]

Volume --> 42,949,672,960 [xiv_cet_7] win2008x64 - tsmportal/win2008x64 - tsmportal-000003.vmdk (Hard Disk 1) [Sent]

Successful Full VM backup of VMware Virtual Machine 'win2008x64 - tsmportal'

mode: 'Incremental Forever - Incremental'

```
target node name:      'CLEM_OVERLORD_DC01'
data mover node name:  'CLEM_TARGARYEN_DM01'
```

Statistics for Virtual Machine 'win2008x64 - tsmportal'.

```
Total number of objects inspected:      1
Total number of objects backed up:      1
Total number of objects updated:        0
Total number of objects rebound:        0
Total number of objects deleted:        0
Total number of objects expired:        0
Total number of objects failed:         0
Total number of bytes inspected:        40.00 GB
Total number of bytes transferred:      295.88 MB
Data transfer time:                     56.13 sec
Network data transfer rate:             5,292.29 KB/sec
Aggregate data transfer rate:           903.49 KB/sec
Objects compressed by:                  0%
Total data reduction ratio:             99.30%
Elapsed processing time:                00:05:28
Removing snapshot for virtual machine 'win2008x64 - tsmportal'
Deleted directory
/tmp/vmware-root/422c02e7-b351-03fd-979a-4f64b8abfea6-vm-99448/hotadd
```

Backup VM command complete

```
Total number of virtual machines backed up successfully: 1
  virtual machine win2008x64 - tsmportal backed up to nodename CLEM_OVERLORD_DC01
Total number of virtual machines failed: 0
Total number of virtual machines processed: 1
```

5.5 VM backup by using Data Protection for VMware CLI

When you are using the vCenter plug-in, the underlying backup command is similar to the following example:

```
/opt/tivoli/tsm/tdpvmware/tsmcli/bin64/tsmcli -f backup -d CLEM_OVERLORD_DC01 -o
CLEM_TARGARYEN_DM01 -I /tmp/vmcli7860162774735009123tmp -s
vio ssadec.storage.usca.ibm.com -p 1500 -n clem_overlord_vcli01 -t IFINCR
```

Where **-I /tmp/vmcli7860162774735009123tmp** is an input file that contains the list of VMs to back up.

The following format of this file must be used:

```
vmname:MYVM1
vmname:MYVM2
```

This command runs on the datamover machine (vStorage Backup Server).

Note: Be careful with the configuration work that is done in the datamover option file. If any disk exclusion **EXCLUDE.VMDISK** is in place, this restriction applies wherever the backup is started.

Example 5-6 shows how to start an Incremental Forever backup of machine tsmcetwin101.

Example 5-6 Incremental Forever back up of machine tsmcetwin101

```
echo "vmname:tsmcetwin101" > /tmp/myvmcli  
/opt/tivoli/tsm/tdpvmware/tsmcli/bin64/tsmcli -f backup -d CLEM_OVERLORD_DC01 -o  
CLEM_TARGARYEN_DM01 -I /tmp/myvmcli -s viossadec.storage.usca.ibm.com -p 1500 -n  
clem_overlord_vcli01 -t IFINCR
```

Tivoli Storage Manager Command Line Wrapper for Virtual Environments s Version:
6.4.0.00

Build Date: Fri Oct 5 11:05:02 2012

Tivoli Storage Manager API Version 64001

Tivoli Storage Manager Command Line Wrapper Compile Version 64000

```
#PARAM OPERATION_TYPE 1  
#PHASE_COUNT 4  
#PHASE PREPARE  
#PARAM BACKUP_TYPE=3  
#PARAM TSM_SERVER_NAME=VIOSSADEC.STORAGE.USCA.IBM.COM  
#PARAM TSM_SERVER_PORT=1500  
#PARAM TSMCLI_NODE_NAME=CLEM_OVERLORD_VCLI01  
#PARAM VCENTER_NODE_NAME=  
#PARAM DATACENTER_NODE_NAME=CLEM_OVERLORD_DC01  
#PARAM OFFLOAD_HOST_NAME=CLEM_TARGARYEN_DM01  
#PARAM TSM_OPTFILE=/tmp/T4VE_of8Ra0  
#PARAM INPUT_FILE=/tmp/myvmcli  
#PARAM TRACEFILE=  
#PARAM TRACEFLAGS=  
#PHASE INITIALIZE  
#PARAM OBJECT=vmname:tsmcetwin101
```

...

```
#CHILD VersionsSinceLastFull:5  
#PARENT vmname:tsmcetwin101  
#CHILD FragmentationPercent:2  
#PARENT vmname:tsmcetwin101  
#CHILD ExtraDataPercent:0  
#PARENT vmname:tsmcetwin101  
#CHILD NumberOfTSMObjects:280  
#PARENT vmname:tsmcetwin101  
#CHILD AppProtectionType:VMware  
#PARENT vmname:tsmcetwin101  
#CHILD Template:No  
#PARENT vmname:tsmcetwin101  
#CHILD TotalIncrementalSize:13824  
#PARENT vmname:tsmcetwin101  
STATUS=success  
#END
```

```
rm /tmp/myvmcli
```

5.6 Self-contained application protection

As described in 3.3, “Protecting applications in a virtual environment” on page 31, Data Protection for VMware can protect Microsoft SQL and Microsoft Exchange without any local agent installed in the VM.

In prior releases (before V6.4), 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. This is the default behavior in the current version as well.

The Applications logs truncation feature is controlled by the **INCLUDE.VMTSMVSS** datamover parameter. 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.

5.6.1 Enabling application protection for a VM

To enable this feature, complete the following steps on the datamover node:

1. On Linux datamover, before you attempt to use this feature, verify that Java run time is installed and set in the PATH. Otherwise, you encounter the following type of error:

```
02/15/13 14:56:25 ANS9489E Java Runtime Environment (JRE) was not found.
02/15/13 14:56:25 ANS9415E Failed to copy
'/opt/tivoli/tsm/client/ba/bin/vmtsmvss/BackupMon.exe' to
'C:\Users\ADMINI~1\AppData\Local\Temp\TSM\BackupMon.exe' with VMware RC=6510 on
the virtual machine.
02/15/13 14:56:25 ANS9398E IBM Tivoli Storage Manager application protection
failed to initialize on virtual machine 'win2008x64 - tsmportal'. See the error
log for more details.
02/15/13 14:56:25 ANS1228E Sending of object 'win2008x64 - tsmportal' failed
```
2. On the Linux datamover, add **INCLUDE.VMTSMVSS <vmname>** to the client options file (dsm.opt) or the client system options file (dsm.sys).
3. On the Windows datamover, add **INCLUDE.VMTSMVSS <vmname>** to the client options file (dsm.opt).
4. Register the VM user credentials that are used by Tivoli Storage Manager to trigger the Truncate operation. The guest VM user must have permission to create Volume Shadow Copies and to truncate SQL Server logs, as shown in the following example:

```
dsmc set password -type=vmguest <vmname> Windows_account secret
```

After this process is completed, when a Full VM (full or incremental) backup is started, the log truncate operation is triggered on the VM. If the log truncate operation fails, an exception is logged but the Full VM backup continues.

Note: This functionality is supported for Windows and Linux datamover, even if it applies to Microsoft Windows VM only.

Example 5-7 shows a backup with self-contained application protection enabled.

Example 5-7 Example with Self Contained Application protection enabled

```
targaryen:~ # dsmc backup vm "win2008x64 - tsmportal" -mode=IFINCR
-asnodename=CLEM_OVERLORD_DC01
IBM Tivoli Storage Manager
Command Line Backup-Archive client Interface
  Client Version 6, Release 4, Level 0.1
  Client date/time: 02/18/13  22:57:34
(c) Copyright by IBM Corporation and other(s) 1990, 2012. All Rights Reserved.

Node Name: CLEM_TARGARYEN_DM01
Session established with server VIOSSADEC: AIX
  Server Version 6, Release 3, Level 4.0
  Server date/time: 02/18/13  22:58:44  Last access: 02/18/13  22:19:00

Accessing as node: CLEM_OVERLORD_DC01
2013-02-18T22:57:38.440-08:00 [2B2B7432C7C0 info 'Default'] Initialized channel
manager
2013-02-18T22:57:38.440-08:00 [2B2B7432C7C0 info 'Default'] Current working
directory: /root
2013-02-18T22:57:38.440-08:00 [2B2B7432C7C0 trivia 'Default'] buffer is 'NPTL 2.4'
2013-02-18T22:57:38.440-08:00 [2B2B7432C7C0 verbose 'ThreadPool'] Thread info: Min
Io, Max Io, Min Task, Max Task, Max Thread, Keepalive, exit idle, idle secs, max
fds: 2, 21, 2, 10, 31, 4, true, 600
2013-02-18T22:57:38.440-08:00 [2B2B7432C7C0 trivia 'ThreadPool'] Thread pool
launched
Full BACKUP VM of virtual machines 'win2008x64 - tsmportal'.

Backup VM command started. Total number of virtual machines to process: 1
Accessing as node: CLEM_OVERLORD_DC01
Starting Full VM backup of VMware Virtual Machine 'win2008x64 - tsmportal'
  mode: 'Incremental Forever - Incremental'
  target node name: 'CLEM_OVERLORD_DC01'
  data mover node name: 'CLEM_TARGARYEN_DM01'
application protection type: 'TSM VSS'
application(s) protected: 'MS SQL 2008'

Creating snapshot for virtual machine 'win2008x64 - tsmportal'
Backing up Full VM configuration information for 'win2008x64 - tsmportal'
  16,658 VM Configuration [Sent]
Processing snapshot
  disk: [xiv_cet_7] win2008x64 - tsmportal/win2008x64 -
tsmportal-000003.vmdk (Hard Disk 1)
  Capacity: 42,949,672,960
  Data to Send: 35,586,048
  Transport: (hotadd)[sending]
Volume --> 42,949,672,960 [xiv_cet_7] win2008x64 - tsmportal/win2008x64 -
tsmportal-000003.vmdk (Hard Disk 1) [Sent]
< 33.95 MB> [ -]
Successful Full VM backup of VMware Virtual Machine 'win2008x64 - tsmportal'
  mode: 'Incremental Forever - Incremental'
  target node name: 'CLEM_OVERLORD_DC01'
  data mover node name: 'CLEM_TARGARYEN_DM01'
```

Statistics for Virtual Machine 'win2008x64 - tsmportal'.

```
Total number of objects inspected:          1
Total number of objects backed up:          1
Total number of objects updated:            0
Total number of objects rebound:           0
Total number of objects deleted:            0
Total number of objects expired:            0
Total number of objects failed:             0
Total number of bytes inspected:            40.00 GB
Total number of bytes transferred:          37.43 MB
Data transfer time:                        5.34 sec
Network data transfer rate:                 6,510.81 KB/sec
Aggregate data transfer rate:               343.45 KB/sec
Objects compressed by:                     0%
Total data reduction ratio:                 99.92%
Elapsed processing time:                    00:01:41
Removing snapshot for virtual machine 'win2008x64 - tsmportal'
Deleted directory
/tmp/vmware-root/422c02e7-b351-03fd-979a-4f64b8abfea6-vm-99448/hotadd
```

Backup VM command complete

```
Total number of virtual machines backed up successfully: 1
  virtual machine win2008x64 - tsmportal backed up to nodename CLEM_OVERLORD_DC01
Total number of virtual machines failed: 0
Total number of virtual machines processed: 1
```

5.7 VM backup optimization

In addition to the incremental forever strategy, you can fine-tune the following datamover configuration to reduce the amount of data that is processed by the backup operations:

- Exclude operating system swap file or paging space from the backup

It appears that the swap file or paging space (whatever it is called depending on the operating system), represents a significant part of active data, which is processed daily when the VM is backed up. To remove this useless data from the backup, configure the operating system to store this swap or paging file into a separate disk so it can be excluded from the full-vm backup.

- Exclude hard disk that contains data that is backed up by in-guest agent

Whenever it is possible, exclude the disk that contains data that is processed by another backup agent. This typically applies when you protect an in-guest application by using a Tivoli Data Protection agent.

- Compression and client side deduplication

The client side deduplication can be enabled to save bandwidth and the amount of space that is stored on the Tivoli Storage Manager server. It requires that the target storage pool on Tivoli Storage Manager server is enabled to store deduplicated data, thus defined on a compatible device class (**FILE** device class) and with **DEDUPLICATE=YES** parameter.

In addition to client side deduplication, you can enable the client compression.

Notice that the compression cannot be turned on without the client side deduplication.



Backup scheduling

In this chapter, we describe the available strategies to schedule your virtual machine (VM) backup. We also list the goals that must be met when you are building your backup schedule plan.

We provide guidance about how to tune the datamover and Tivoli Storage Manager server as well to reduce the backup window by using the Backup-Archive client multi-session, deduplication, and compression features.

6.1 Backup scheduling

The most important things to consider when you define your backup policy are how to meet your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the application or data that is protected. By using this information, you can define the schedule plan and backup policy. You must consider the infrastructure that is already available to back up your virtual environment, including the number of vStorage Backup Servers and their throughput capabilities, the number of VMs, the paths to data and backup storage, and the Tivoli Storage Manager server ingestion capacity.

Data Protection for VMware provides the ability to schedule backups of a large collection of VMware virtual machines, which provides an automated backup solution that allows for the automatic discovery of newly created virtual machines and provides parallel backup of multiple virtual machines. This can be implemented in a way that minimizes the impact to any single VMware ESX or ESXi host.

The combination of the new incremental-forever and multi-session backup capabilities enables a larger VMware environment to be protected with fewer vStorage backup servers.

6.1.1 Backup schedule and backup strategy

The following two approaches are available for VM backup scheduling:

- Incremental Forever

Incremental Forever is the preferred backup method when day-to-day VM protection is performed.

When you are choosing this method, you must create only one schedule and specify the IFINCR backup mode. The first backup that is done is an Incremental Forever Full (IFFULL), and every subsequent backup is Incremental Forever (IFINCR).

For more information about Incremental Forever backup strategy, see 3.5, “Choosing your backup strategy” on page 37.

For more information about scheduling, see this website:

<https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Storage%20Manager/page/Recommendations%20for%20Scheduling%20with%20Tivoli%20Storage%20Manager%20for%20Virtual%20Environments%206.4>

- Periodic Full

This method creates a complex set of schedules and requires an estimation of Full backup elapsed time to distribute them across the Full + Incremental backup cycle (for example, over a week or month).

The Periodic Full strategy can be selected to perform an out-of-cycle backup; for example, to address archiving needs or when data is stored on physical tapes (regularly reaggregate the data on tape).

If the strategy is to perform Full + Incremental backups, the following two methods can be used to automate your VE backups:

- Batched full:

- Full VM backups during extended time (for example, weekend), incremental during weekdays.
- Easiest approach to configure because it minimizes schedule definitions.

- Backup window considerations and does not optimize usage of vStorage backup server.
- Rotating full:
 - Full and incremental backups are interleaved each day
 - Distributes backup workload or window throughout the week
 - More complex scheduling

For more information about the Periodic Full backup strategy, see 3.5, “Choosing your backup strategy” on page 37.

6.1.2 Fine-tuning the Tivoli Storage Manager server

We assume in this book that the Tivoli Storage Manager server is properly configured. For more information about the Tivoli Storage Manager server, see the Tivoli Storage Manager Information Center at this website:

<http://www.ibm.com/developerworks/mydeveloperworks/wikis/home/wiki/Tivoli%20Documentation%20Central/page/Tivoli%20Storage%20Manager>

The Tivoli Storage Manager server must be properly configured to manage the incoming VM backup data, especially when a large quantity of sessions that are run at the same time and even more when deduplication is enabled.

Depending on where you choose to store the VM backup, you might have to tune the following parameters:

- ▶ **MaxSessions**
- ▶ **NumOpenVolsAllowed**

For the datacenter nodes that carry and hold the data in the Tivoli Storage Manager server, you might tune the following parameters:

- ▶ **COMPRESSION**
- ▶ **DEDUPLICATION**

Note: Pay attention to set up the right node on the Tivoli Storage Manager server. On the client side, you tune the datamover node. However, because of the proxy relationship, on the server side, you tune options for the datacenter node; that is, the one that is connected during the backup (**asnodename** option).

6.1.3 Fine-tuning the datamover

As there are options to tune on the Tivoli Storage Manager server side, you have some on the Backup-Archive client side to enable features, such as, client side deduplication, compression, and multi-sessions.

The following parameters might be configured in the `dsm.opt` (Windows) or `dsm.sys` (Linux) file, depending on your operating system:

- ▶ **VMMAXParallel**
- ▶ **VMLIMITPERDatastore**
- ▶ **VMLIMITPERHost**
- ▶ **DEDUPLICATION**
- ▶ **DEDUPCACHESIZE**

- ▶ DEDUPCACHEPath
- ▶ COMPRESSION

6.1.4 Defining a schedule to back up VMs

In addition to setting up backup schedules with the vCenter plug-in wizard, schedules can be defined via the Tivoli Storage Manager administrative interface (command-line or administration center GUI). The scheduling of backups should be carefully planned.

Schedules that are created with the vCenter plug-in can be viewed through the Tivoli Storage Manager Server administrator interface. However, schedules that are created directly via the Tivoli Storage Manager Server administrator interface are not shown on the VCenter plug-in.

When the Data Protection for VMware vCenter plug-in is used, there are two different options to specify the scope of virtual machines to be processed by a schedule, which is controlled by the Newly Added Virtual Machine option. If this option is enabled, the scope is specified by the parameter **VMHOST**; if it is not, a list of VMs are used instead.

Note: The VM list cannot exceed 512 characters, as shown in Figure 6-1.

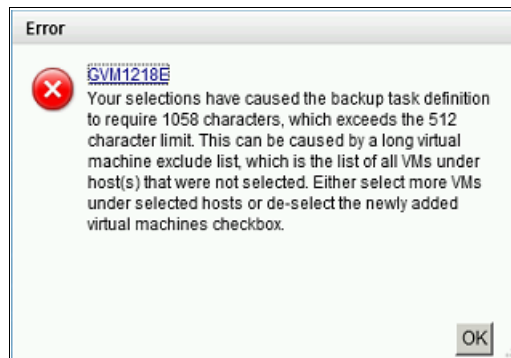


Figure 6-1 Error message: VM list is too long

When the administrative command-line is used to define schedules, the same syntax that is used for the **dsmc** command-line using **DOMAIN.VMFULL** applies. For more information about available options, see 5.4, “VM backup by using the Backup/Archive Client command line” on page 107.

Complete the following steps to create a schedule with the DP for VMware vCenter plug-in, and to see the command that is issued by the plug-in on the Tivoli Storage Manager server:

1. Open the plug-in and in the Backup tab, click **Create schedule**.
2. Go through the wizard until the Summary window opens, as shown in Figure 6-2 on page 123.

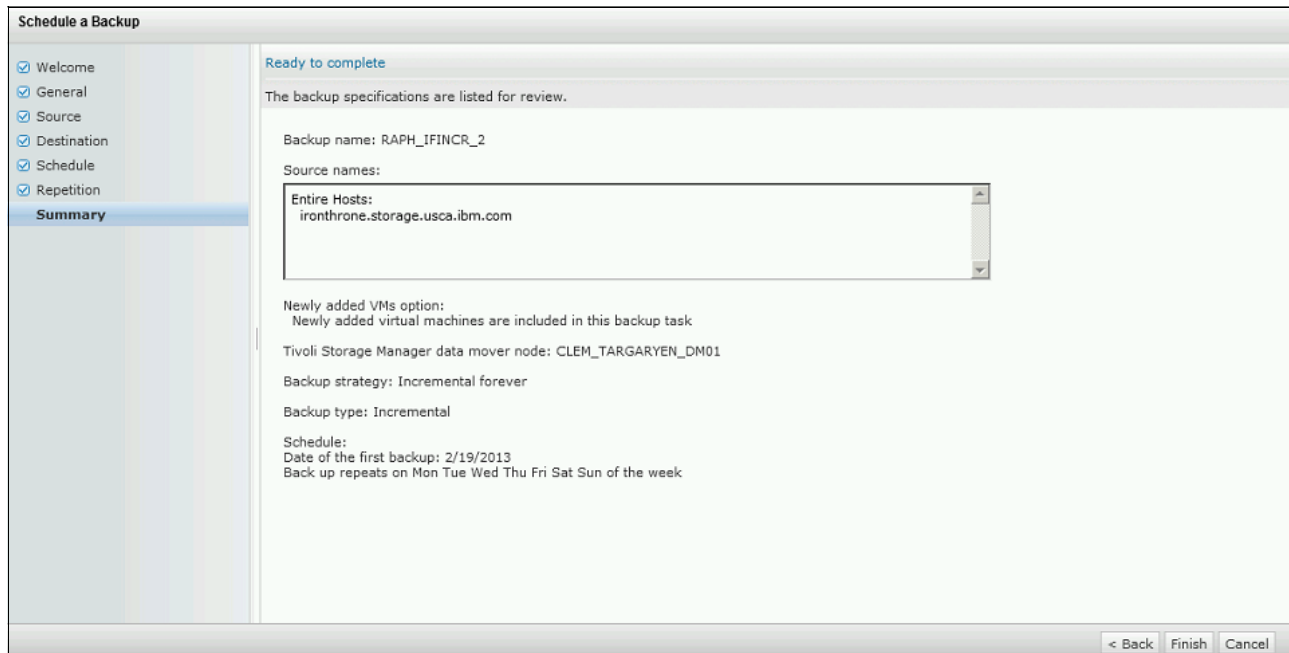


Figure 6-2 Define a backup schedule

3. Click **Finish** to create the schedule.

The following corresponding commands are sent by the plug-in to the Tivoli Storage Manager server:

```
DEFINE SCHEDULE RAPH RAPH_IFINCR_2 Type=Client DESCription='IFINCR of ironthroner
virtual machines' ACTION=Backup SUBACTION=VM OPTIONS='-vmfulltype=vstor
-vmbackuptype=fullvm -asnodename=CLEM_OVERLORD_DC01
-domain.vmfull="VMHOST=ironthroner.storage.usca.ibm.com" -MODE=IFIncremental'
STARTDate=02/19/2013 STARTTime=23:00:00 SCHEDStyle=Enhanced
DAYofweek=Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday
```

```
DEFINE ASSOCIATION RAPH RAPH_IFINCR_2 CLEM_BROADSWORD_DM01
```

The following example shows a daily backup of all the VMs within the datastore that is named xiv_cet_1:

```
DEFINE SCHEDULE RAPH RAPH_IFINCR_3 Type=Client DESCription='IFINCR xiv_cet_1
datastore' ACTION=Backup SUBACTION=VM OPTIONS='-vmfulltype=vstor
-vmbackuptype=fullvm -asnodename=CLEM_OVERLORD_DC01
-domain.vmfull="VMDATASTORE=xiv_cet_1" -MODE=IFIncremental' STARTDate=02/19/2013
STARTTime=23:00:00 SCHEDStyle=Enhanced DAYofweek=any
```

6.1.5 Updating or deleting a VM backup schedule

To update or delete a scheduled task, you can use the Data Protection for VMware plug-in or the administrative command-line.

Using the plug-in, go to the Backup tab, select the schedule you want to delete, right-click, and select **Delete**, as shown in Figure 6-3.

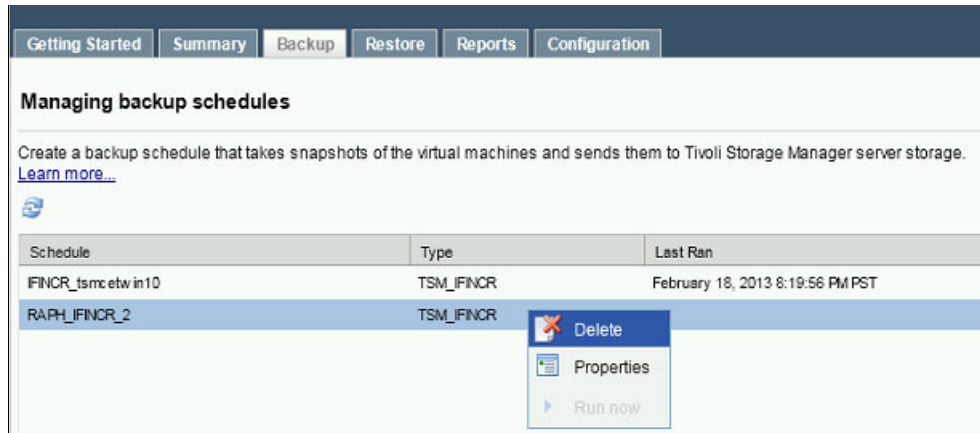


Figure 6-3 Editing or deleting a schedule

To modify a schedule, follow the same procedure to modify the schedule, but select **Properties** from the drop-down menu instead.

Using the administrative command-line, run the **UPDATE SCHEDULE** or **DELETE SCHEDULE** command to manage your schedules.



Virtual machine recovery scenarios: Full or Item

This chapter provides guidance on how to restore a virtual machine (VM) and describes the step-by-step procedures to perform the following tasks:

- ▶ Restore a full virtual machine
- ▶ Restore files to a virtual machine
- ▶ Volume (disk) Recovery for a virtual machine

The two available restore interfaces also are described in this chapter.

This chapter includes the following topics:

- ▶ Overview of recovery procedures
- ▶ Recovering data by using the Set Access and FromNode options

7.1 Overview of recovery procedures

Data Protection for VMware provides the following restoration modes:

- ▶ Full VM restoration
- ▶ File Level restoration
- ▶ Volume instant restore

For more information about the options that are available to you to perform the recovery, see 3.8, “Determining the location to start backup or restore” on page 45.

7.1.1 Full VM restoration

Full VM restoration can be done through the Backup-Archive client GUI or command line or by using the Data Protection for VMware vCenter plug-in.

VM restoration does not require any disk staging. The VM is created in the ESXi host as part of the restoration steps. The datamover sends the data directly from the Tivoli Storage Manager server to the datastore.

FULL VM restoration by using Data Protection for VMware vCenter plug-in

By using the plug-in, you can restore one or many VMs as a single task. However, you cannot rename the VMs when you are restoring more than one in the same task. Therefore, if you restore VMs that still exist, you must create one task for each restoration.

Complete the following steps to perform a FULL VM restoration by using the Data Protection for VMware vCenter plug-in:

1. Go to the plug-in Restore tab.
2. Select the **Active and Inactive** filter.

3. Browse and select the VMs that you want to restore, as shown in Figure 7-1.

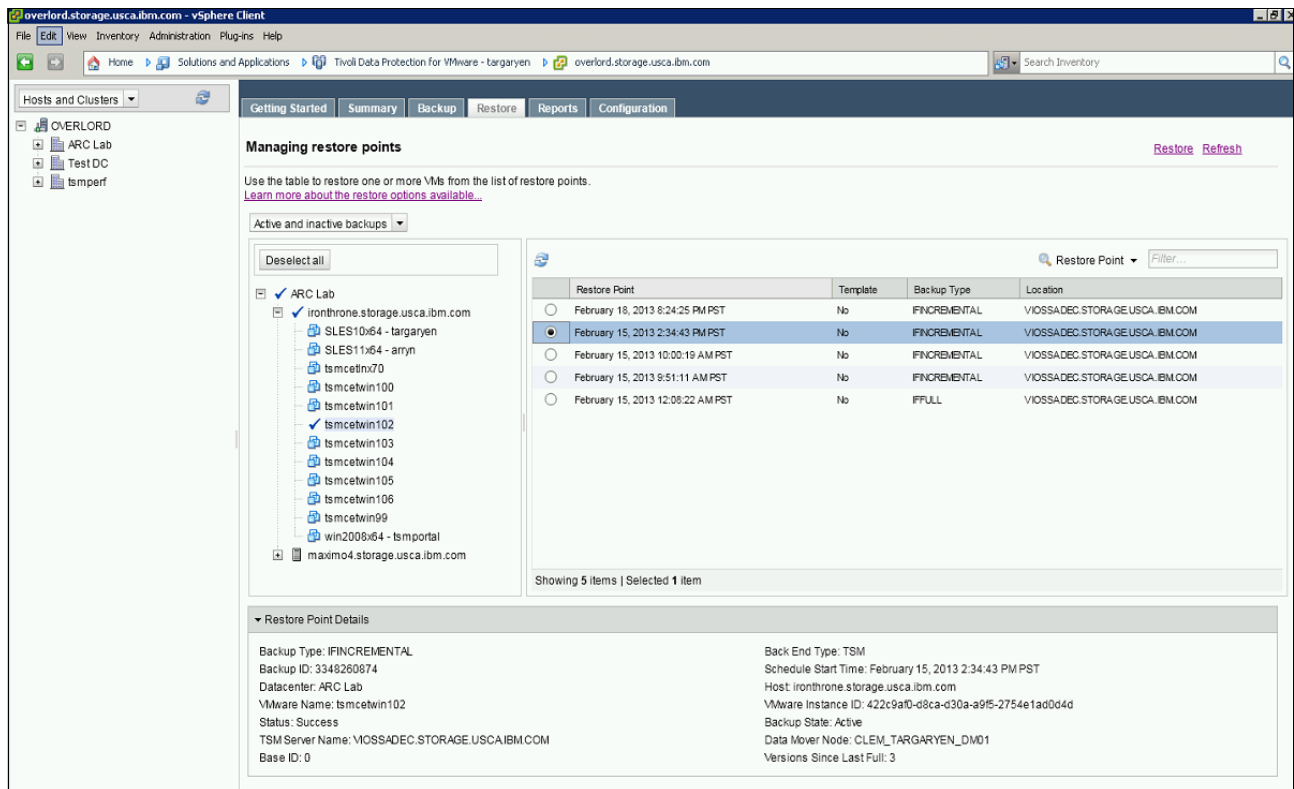


Figure 7-1 VM selection for restore

4. Click the **Restore** link in the upper right side of the window. The Restore Location wizard opens and a summary of your source selection is shown, as shown Figure 7-2. Click **Next**.

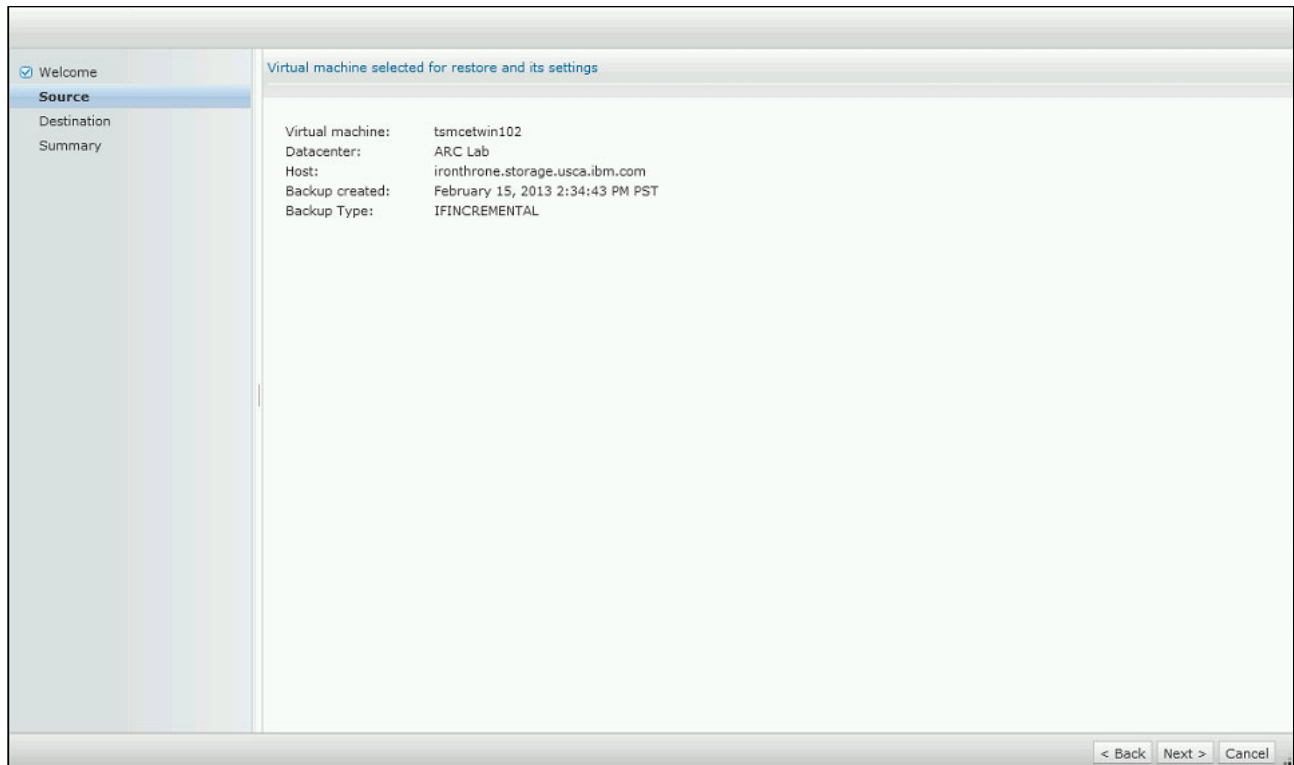


Figure 7-2 Restore Location wizard

5. Select the restore destination (**Original** or **Alternate Location**).

6. If you selected Alternate location, enter the ESXi host name, the new VM Name (if only one VM is selected), and the datastore and datacenter, as shown in Figure 7-3.

Destination for the single virtual machine restore

Select the destination of the selected virtual machine. The VM can be restored to a different VM, data store or host to preserve the original VM. All new VMs and data stores must be created before starting the restore wizard.

☐ Restore to original location

☒ Restore to alternate location

Virtual machine name
tsmcetwin102_restore

Select the data center to use for the restore destination
ARC Lab (original)

Select the ESX Host to use for the restore destination
spiderman.storage.usca.ibm.com

Select the data store used for the restore destination
ds8k_svt_1

Select the Tivoli Storage Manager data mover node that runs the restore. This is the node name for the Tivoli Storage Manager client that is installed on the vStorage backup server. Pick a data mover node that is not used by another process to improve restore performance.
CLEM_TARGARYEN_DM01

< Back Next > Cancel

Figure 7-3 Alternate Location Information wizard

7. Review the summary and click **Finish**, as shown in Figure 7-4.

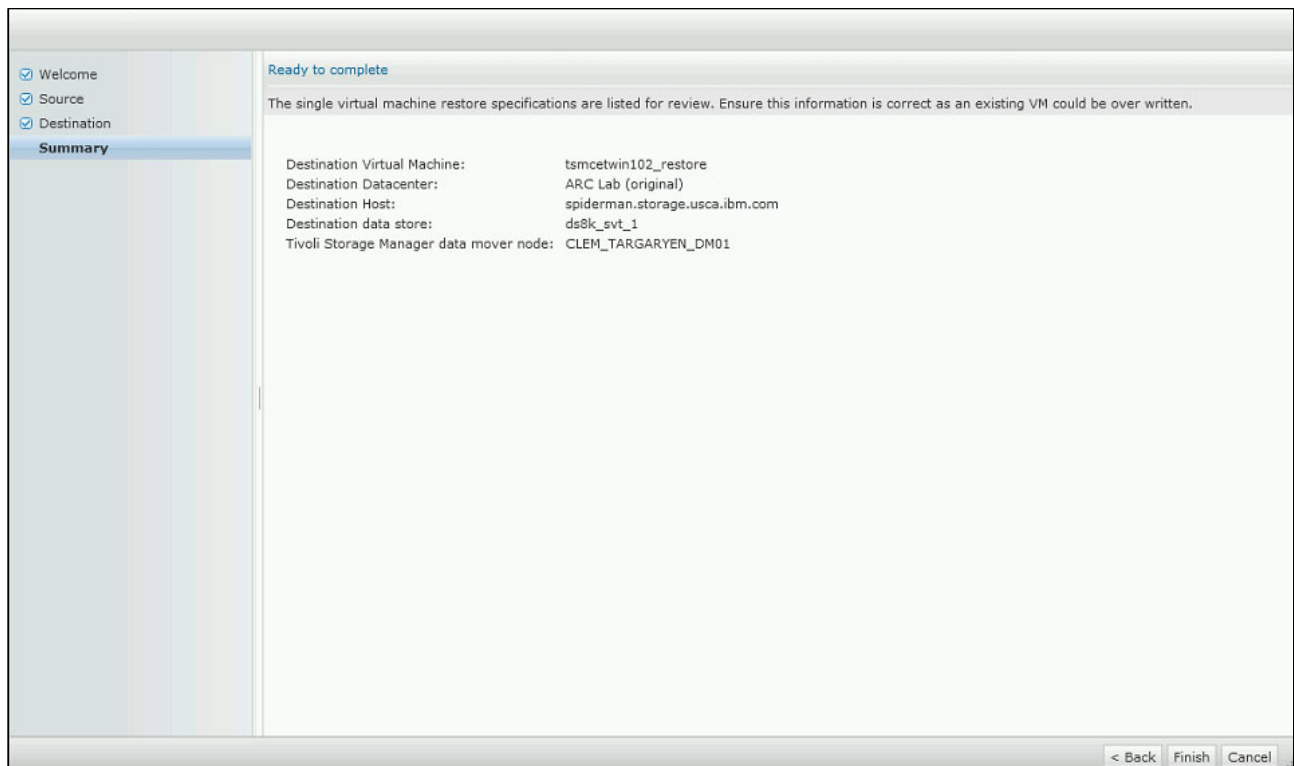


Figure 7-4 Restore wizard information summary

You can follow the restoration process by using the Reports tab, Recent Tasks panel.

Example for multiple VM selection: Without rename

In this example, we assume that the original VMs were deleted or moved away by using VMware tools.

Complete the following steps:

1. Go to the plug-in Restore tab.
2. Select the **Active and Inactive** filter.

3. Browse and select the VMs that you want to restore, as shown in Figure 7-5.

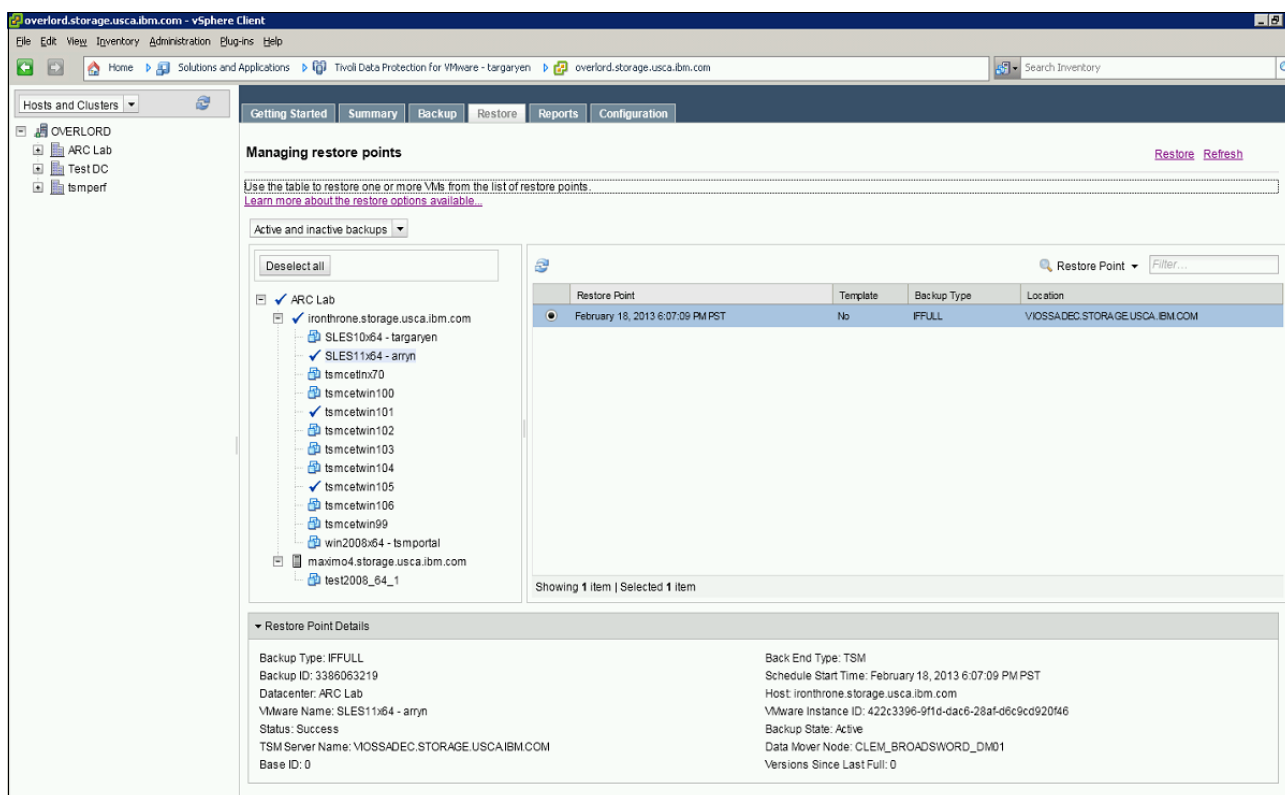


Figure 7-5 Multiple VM selection for restore

4. Click the **Restore** link in the upper right side of the window. The Restore Location wizard opens and a summary of your source selection is shown, as shown in Figure 7-6. Click **Next**.

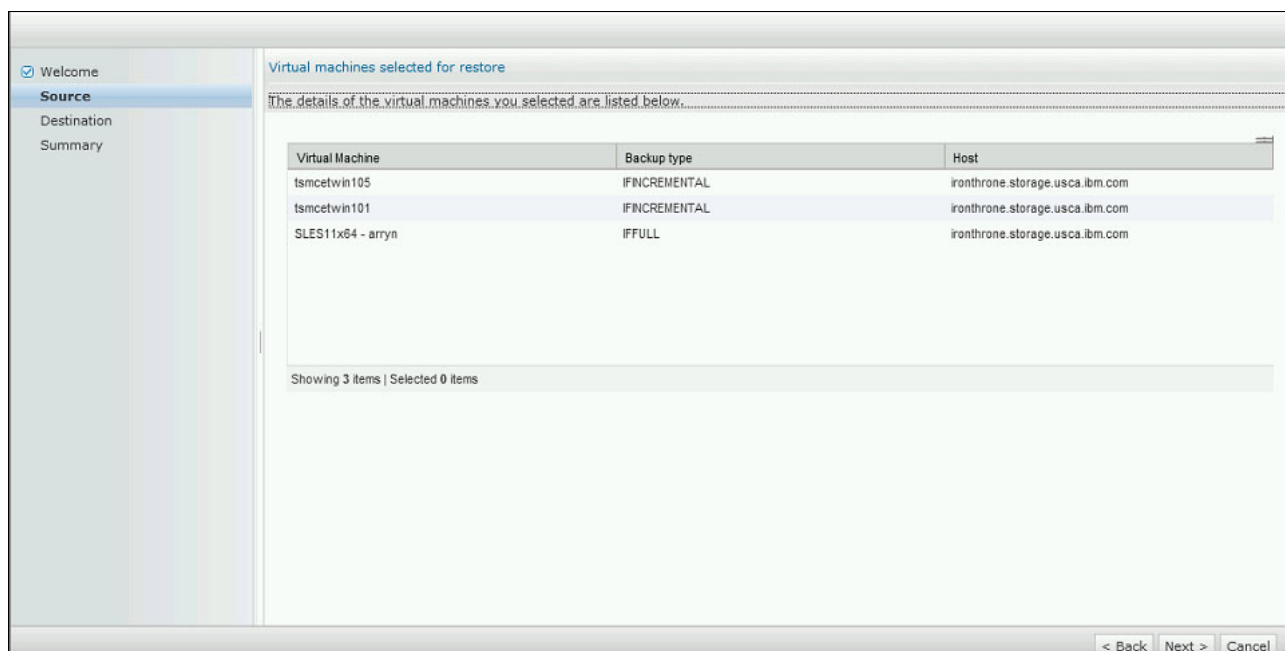


Figure 7-6 VM Restore Location wizard

5. Select the restore destination (**Original** or **Alternate Location**).
6. If you selected Alternate location, enter the ESXi host name, the new VM Name (if only one VM is selected), the datastore, and datacenter, as shown in Figure 7-7. Click **Next**.

Destination for the restore

All the virtual machines are restored to the selected data center, the selected host and the selected data store.

☐ Restore to original location
☒ Restore to alternate location

Select the data center to use for the restore destination

ARC Lab (original)

Destination ESX host

spiderman.storage.usca.ibm.com

Destination data store

ds8k_svt_1

Select the Tivoli Storage Manager data mover node that runs the restore. This is the node name for the Tivoli Storage Manager client that is installed on the vStorage backup server. Pick a data mover node that is not used by another process to improve restore performance.

CLEM_TARGARYEN_DM01

< Back Next > Cancel

Figure 7-7 Alternate location restore information

7. Review the summary and click **Finish** when complete. You can follow the restoration process by using the Reports tab, Recent Tasks panel.

FULL VM restoration by using Backup-Archive client

This task must be started from the vStorage Backup Server Backup-Archive client.

Complete the following steps to restore a VM:

1. Start the GUI by using the **asnodename** option.
2. Go to **Menu** → **Actions** → **Restore VM**.

3. To select the VM to be restored, use the search option to locate it in the backup repository, as shown in Figure 7-8.

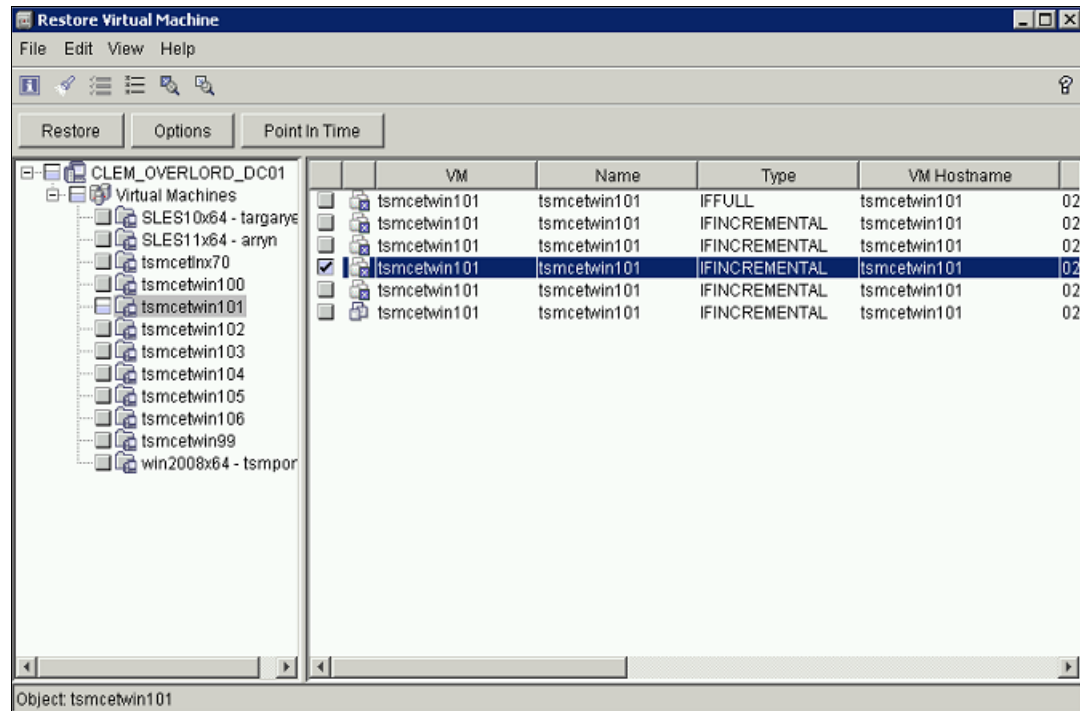


Figure 7-8 Select the virtual machine to restore

4. Choose the restoration location (**Original location** or **Following location**), as shown in Figure 7-9.

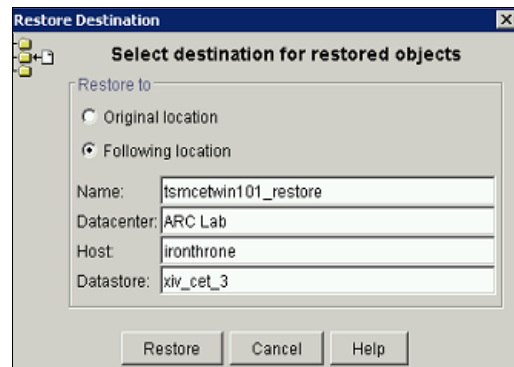


Figure 7-9 Enter alternate location information

5. Click **Restore**.

If the restoration takes place in an alternative location, be prepared to answer the following questions:

- ▶ What is the new virtual machine name?
- ▶ On which datacenter is it?
- ▶ Hosted by which ESX or ESXi Host?
- ▶ On which Datastore?

When you select the Original location option, the VM must be powered off so it can be erased.

When you select the Following location option, the target name of the VM that is restored must be a non-existing one.

The following command line is used to restore the VM tsmcetwin101 in the same location:

```
dsmc restore vm tsmcetwin101 -asnodename=CLEM_OVERLORD_DC01
```

The following command line is used to restore the latest version of VM tsmcetwin101 to an alternate location:

```
dsmc restore vm tsmcetwin101 -vmname=tsmcetwin101_restore -datastore=xiv_cet_1  
-host=ironthrone.storage.usca.ibm.com -datacenter="ARC Lab"  
-asnodename=CLEM_OVERLORD_DC01
```

If you want to choose an older version, you can use the **pitdate/pittime** option or the **pick** option, as shown in the following example:

```
dsmc restore vm tsmcetwin101 -vmname=tsmcetwin108_restore -datastore=xiv_cet_1  
-host=ironthrone.storage.usca.ibm.com -datacenter="ARC Lab"  
-asnodename=clem_overlord_dc01 -pick -inact
```

If you want to restore only a disk on a virtual machine, the Backup-Archive client command line can be used. The following example shows the syntax that is used to restore a previous version of the hard disk0 of tsmcetwin101 to an alternative datastore:

```
dsmc restore vm "tsmcetwin101:-vmdk=Hard Disk 0" -datastore=xiv_cet_1  
-asnodename=clem_overlord_dc01 -pick -inact
```

7.1.2 File level restoration

The table in chapter 3.8, “Determining the location to start backup or restore” on page 45 provides information on where you can use the Data Protection for VMware Recovery Agent to restore files. However, we advise that you run the Data Protection for VMware recovery agent from the vStorage Backup Server because it is easier to manage (less installation and maintenance) and the operation is done by a backup operator (not a user).

Differences between iSCSI mount and Virtual Volume mount

There are important differences between DP for VMware Recovery Agent interfaces on Windows and Linux.

The recovery agent for Windows mounts the snapshots from the Tivoli Storage Manager server as one of the following components:

- ▶ A virtual volume partition mount to the system that is running the recovery agent (Windows only).
- ▶ As a disk (iSCSI target) that is shared out to the same or different systems. The system that mounts this disk (iSCSI initiator) can be Windows or Linux.

The Recovery Agent interface for Linux facilitates the iSCSI mount steps but does not mount a snapshot directly from the Tivoli Storage Manager server. Instead, it depends on the iSCSI mount that is performed by a Windows Recovery Agent.

Virtual volume mount is for an individual disk partition and iSCSI mount is for an entire virtual disk.

7.1.3 File level restoration from Windows VM backup

In this section, we describe file level restoration from a Windows VM backup.

The first step is to start Data Protection for VMware recovery agent by using the Start menu shortcut from the vStorage Backup Server.

Note: For Windows VM, if the snapshot contains a Dynamic disk or GUID partition table, you cannot mount it by using the virtual volume mount (the exception FBSM7019E is thrown). You must use iSCSI mount instead.

File restore from a full VM backup

Complete the following steps to perform a file restore from a full VM backup:

1. Open the Data Protection for VMware Recovery Agent, as shown in Figure 7-10.

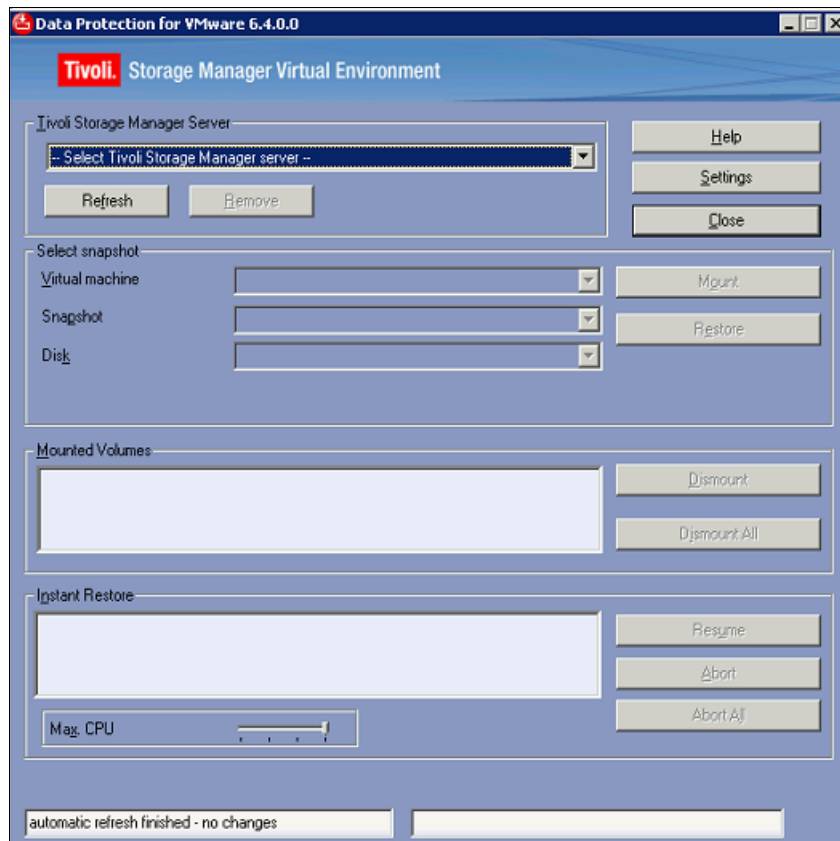


Figure 7-10 Data Protection for VMware Recovery Agent

2. Establish the connection with the Tivoli Storage Manager server, as shown in Figure 7-11.

Tivoli Storage Manager Server information

Server address:

Server port:

Node access method:

☐ Asnodename
Authenticate using a proxy node to access the VM backups that are in the target node. The authentication node must have been granted "proxy" authority to perform operations on behalf of the target node.

☐ Fromnode
Authenticate using a node with access limited only to the snapshot data of specific VMs in the target node. The authentication node must have been granted limited access to the target node using "set access" command.

☒ Direct
Authenticate directly to the target node (the node where the VM backups are located).

Authentication node:

Password:

Target Node:

Figure 7-11 Credentials for Tivoli Storage Manager connection

The following settings are available:

- Asnodename (datamover connect as datacenter node)
- Fromnode (specify a node with restricted access. Use full when you must isolate a VM within the same datacenter)
- Direct (datacenter node credentials)

3. Select the VM and the snapshot date and time, as shown in Figure 7-12.

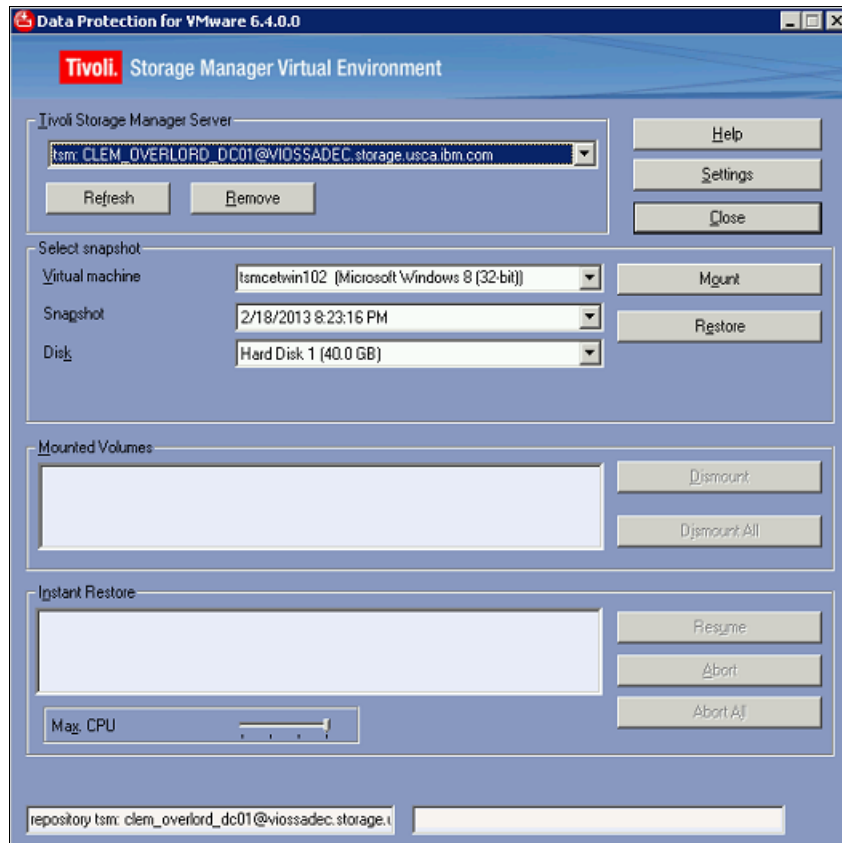


Figure 7-12 VM and snapshot selection

4. Mount the volume by using Virtual volume or iSCSI mount:

- Virtual volume: This part of the procedure is specific to Virtual Volume mount operations; it is a single step operation. You must select only the volume that you want to mount, as shown in Figure 7-13. Click **OK**.

Select mount destination

Create virtual device for:
tsmoeetwin102, Hard Disk 1, 2/18/2013 8:23:16 PM

☐ Mount as an iSCSI target

Target name:

Initiator name:

☒ Create virtual volume from selected partition:

Partition number	Size	File System	Label
0	350 MB	NTFS	System Reserved
1	33.8 GB	NTFS	<No Label>

☒ Show only mountable partitions
☒ Mount virtual volume as read only

☒ Assign the following drive letter:
D:\

☐ Mount in the following empty NTFS folder:

Figure 7-13 Disk selection and mount

The mounted volume is shown as the drive letter that you specified, as shown in Figure 7-14.

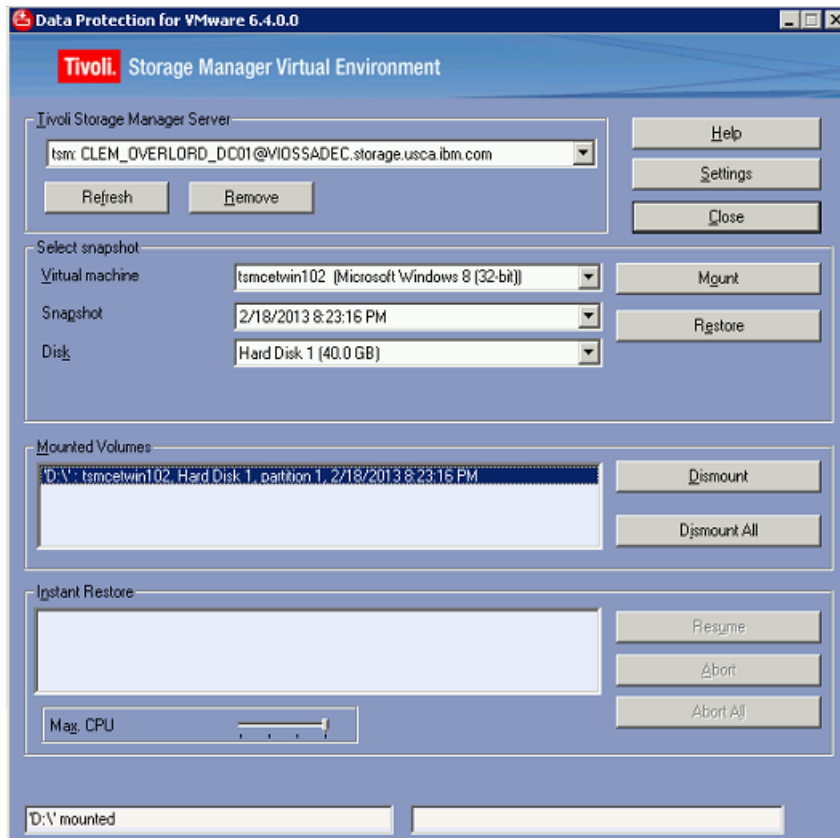


Figure 7-14 Snapshot that is mounted and ready to browse

The volume appears in Windows Explorer and you can browse as a local volume. You can now copy your data back on the vStorage Backup Server or directly to the VM.

After your file recovery copy is completed, click **Dismount** and close the Data Protection for VMware Recovery agent.

– iMount

This part of the procedure covers the steps that are specific to iSCSI mount procedure.

The first two steps set up the iSCSI communication: determine the initiator Name and configure the iSCSI discovery to connect to this initiator and perform local connection to the target that are exposed, as shown in Figure 7-15 and Figure 7-16 on page 141.

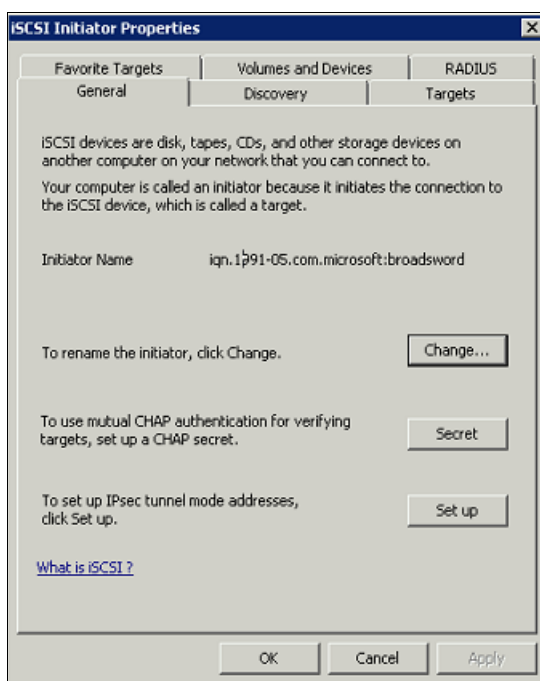


Figure 7-15 General tab: iSCSI initiator ID

The second step must be done on the machine where the volume is mounted. In our example, this is the same machine, the vStorage Backup Server.

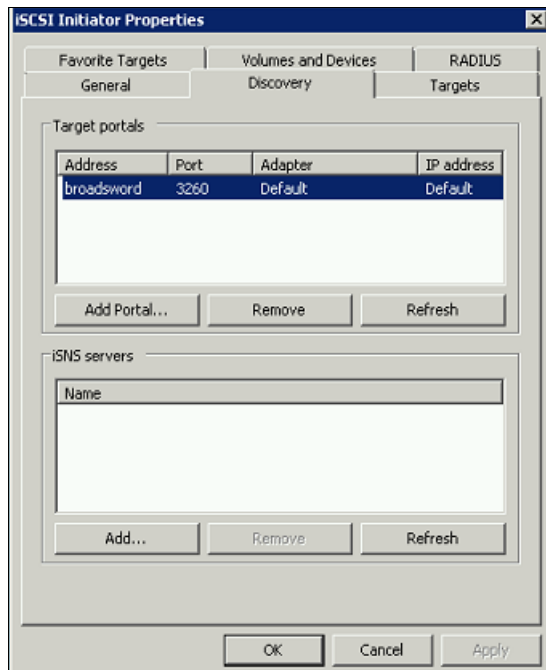


Figure 7-16 Discovery tab: Configure local connection

By using the discovery setup, you can find the volume to be exposed as a target by the Data Protection for VMware Recovery Agent. Specify the initiator name, target name, and mount, as shown in Figure 7-17 on page 142 and Figure 7-18 on page 143.

Select mount destination

Create virtual device for:
tsmcelwin99, Hard Disk 2, 2/15/2013 3:15:41 PM

☒ Mount as an iSCSI target

Target name:

Initiator name:

 Make sure port 3260 is open on any firewall between this computer and the initiator.

☐ Create virtual volume from selected partition:

Partition number	Size	File System	Label
FB5M7019E The selected disk is not a Basic, MBR-based disk.			

☒ Show only mountable partitions

☒ Mount virtual volume as read only

☐ Assign the following drive letter:

☐ Mount in the following empty NTFS folder:

Figure 7-17 Specify target name before iMount

The target name is a name that is used to identify the volume to be mounted.

The initiator name is the name of your iSCSI initiator (the vStorage Backup Server initiator ID).

Enter the information and click **OK** to show iSCSI target (iMount operation), as shown in Figure 7-20 on page 145.

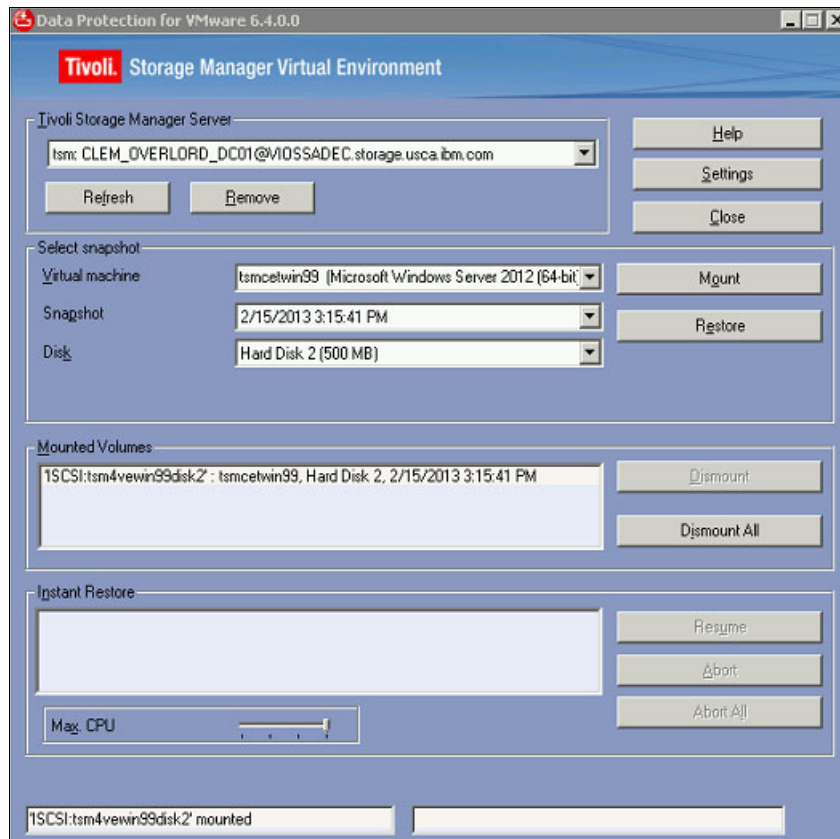


Figure 7-18 iMount done

5. Connect to iSCSI target, as shown in Figure 7-19.

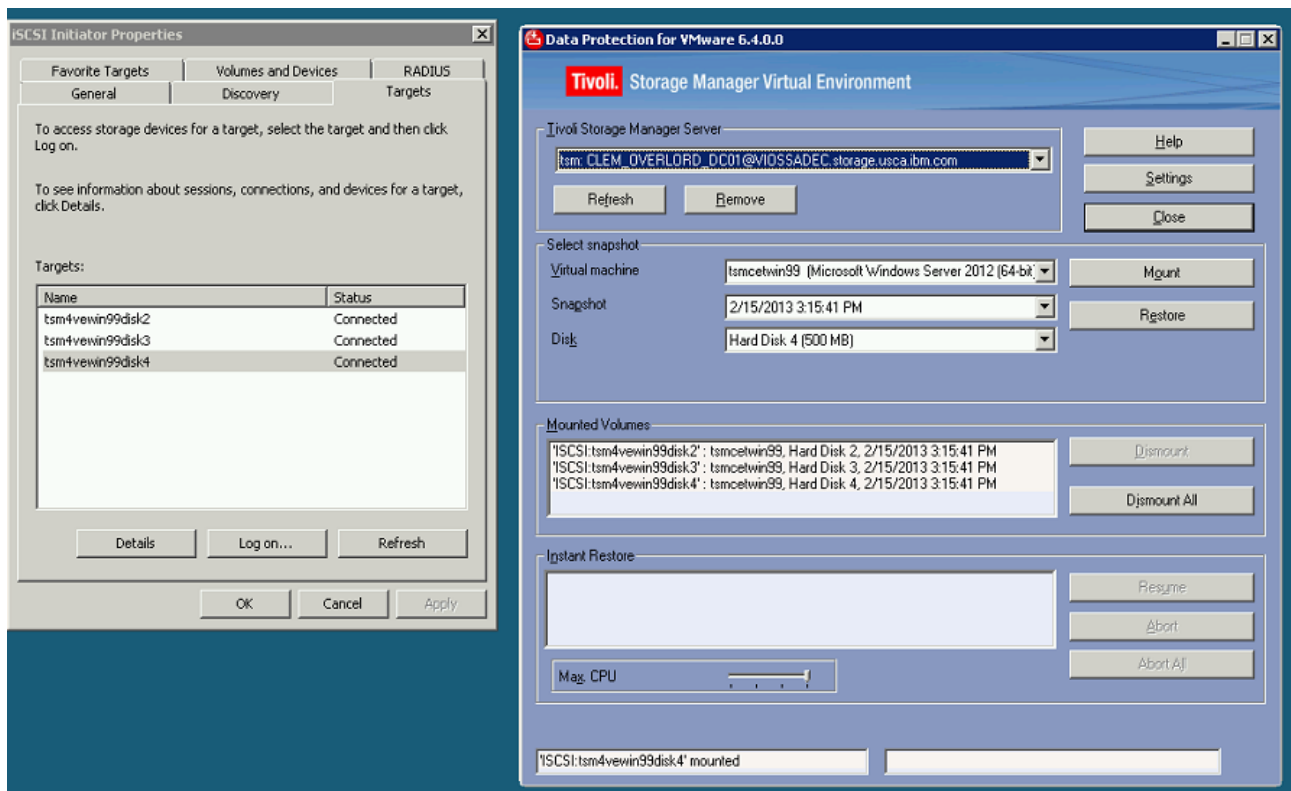


Figure 7-19 Connection between the iSCSI targets and the mounted volumes in Data Protection for VMware interface

6. After your volume (or volumes) is mounted, go to the iSCSI initiator properties and check the Targets tab. The targets should appear, if not, click **Refresh**.

7. Go to the Windows disk manager to set those targets as local disks.

Import the Volume by using the volume manager (LVM or Disk Manager). If the volume is spanned over multiple disks, mount all of them and use the Import Foreign Disk option in the disk manager, as shown in Figure 7-20, Figure 7-21 on page 146, Figure 7-22 on page 146, and Figure 7-23 on page 147.

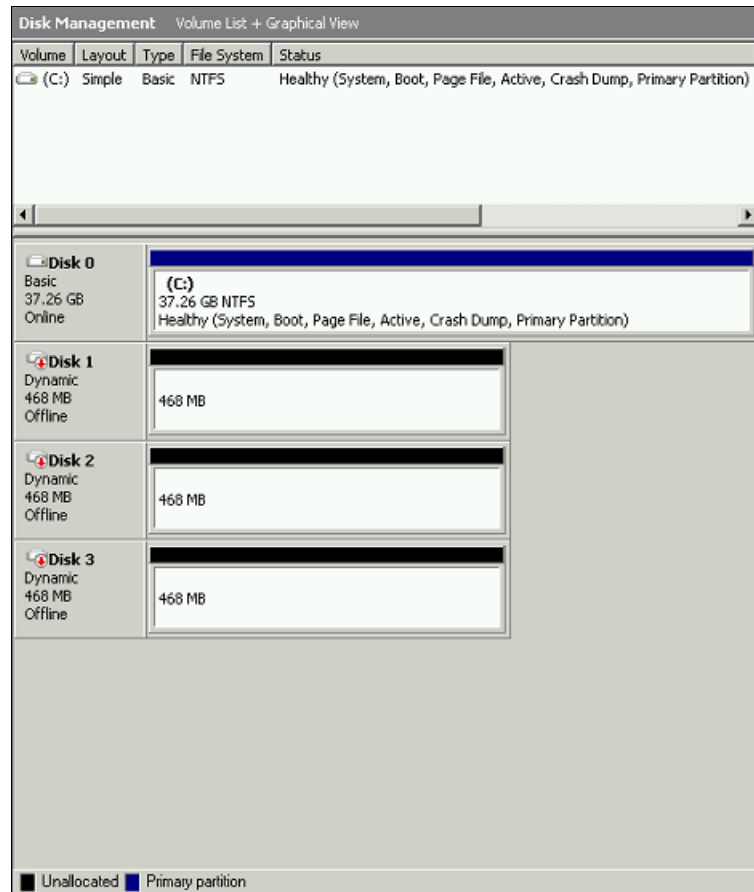


Figure 7-20 Windows Disk manager

Right-click the exposed disks (Offline) and change them to Online, as shown in Figure 7-21 on page 146.

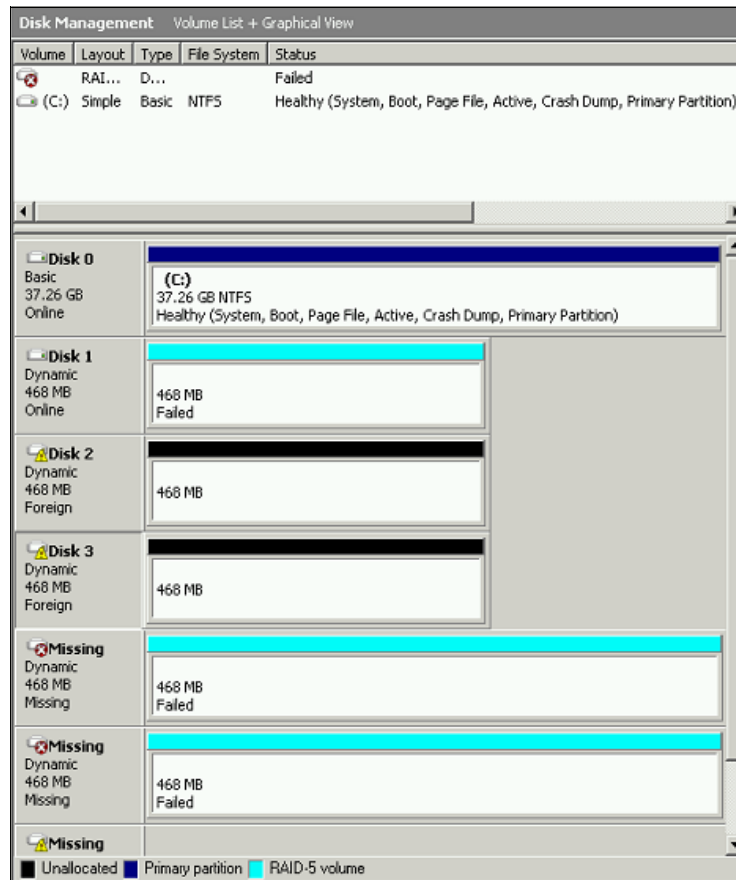


Figure 7-21 Change the disk online to import them

In this case, the three targets represent a spanned volume. When a volume is spanned, you must mount all disks that belong to this spanned disk.

Right-click one of the disks that is marked as Missing and select **Import Foreign Disk**. The message that is shown in Figure 7-22 is displayed.

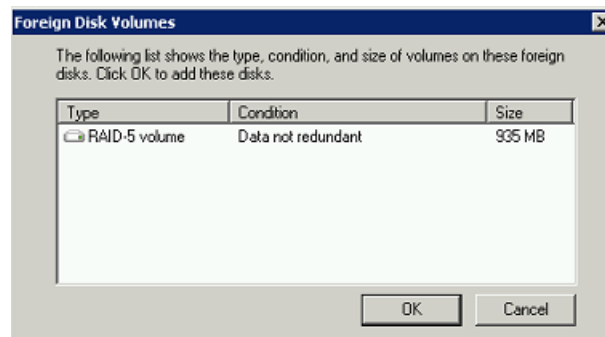


Figure 7-22 Foreign Disk pop-up window

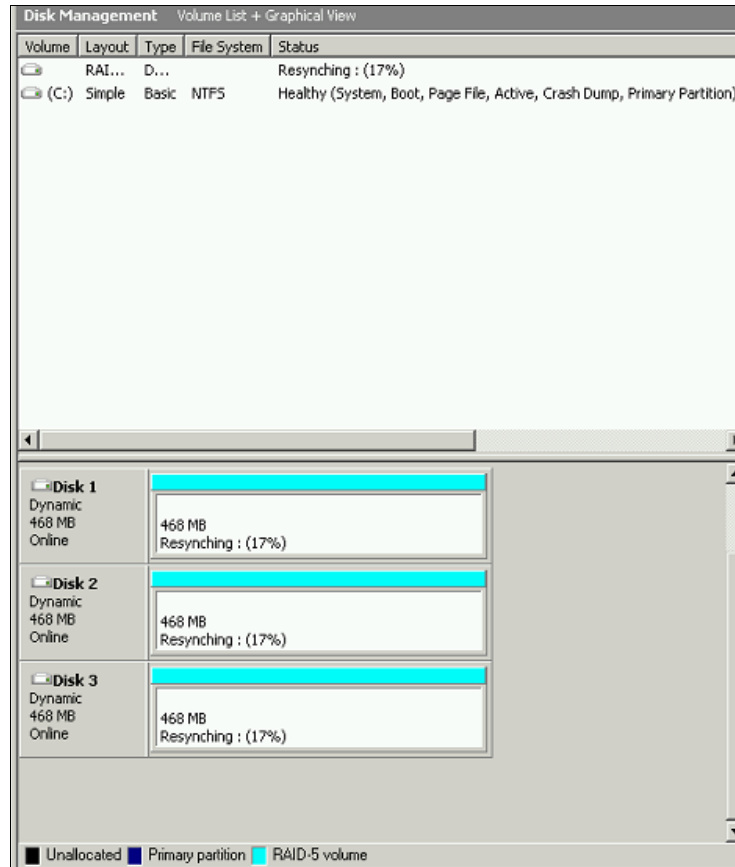


Figure 7-23 Disk import in progress

8. After the disk is analyzed by the disk manager, it is ready to browse and copy back the files. Use XCOPY to preserve ACL if needed.

When you finish the restore, close Windows Explorer, return to the iSCSI interface and disconnect the targets.

Go to the Targets tab, click **Target** → **Details**. In the Sessions tab, click **Log Off**.

9. Close your browser

10. Dismount the snapshot:

- Virtual volume operation: Click **Dismount**.
- iMount operation: Disconnect the iSCSI targets (switch to offline disks on the disk manager and log off from the targets), as shown in Figure 7-24 on page 148.

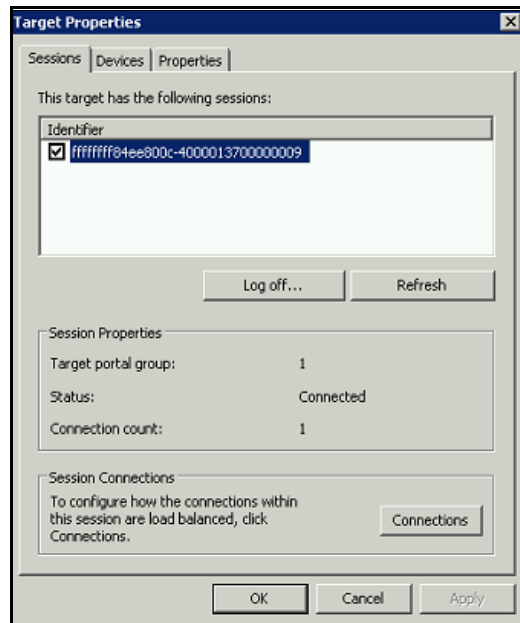


Figure 7-24 iSCSI properties - Targets Tab - Session - LogOff

As shown in Figure 7-25, the iSCSI Properties window shows that all targets are inactive.

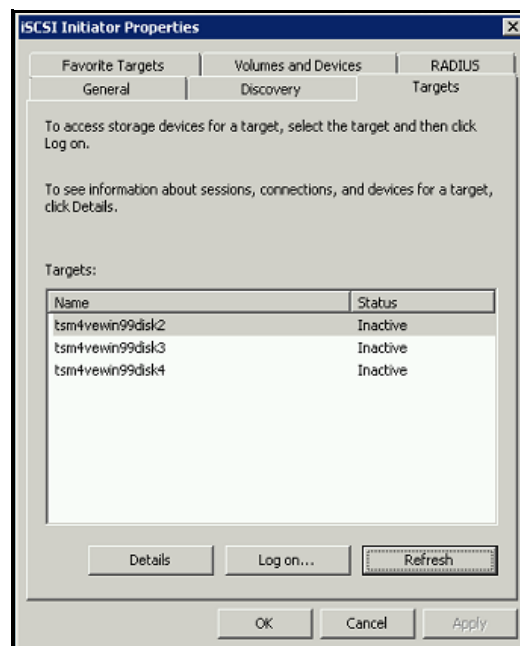


Figure 7-25 Targets are inactive

11. Dismount the volume from the Data Protection for VMware agent, as shown in Figure 7-26.

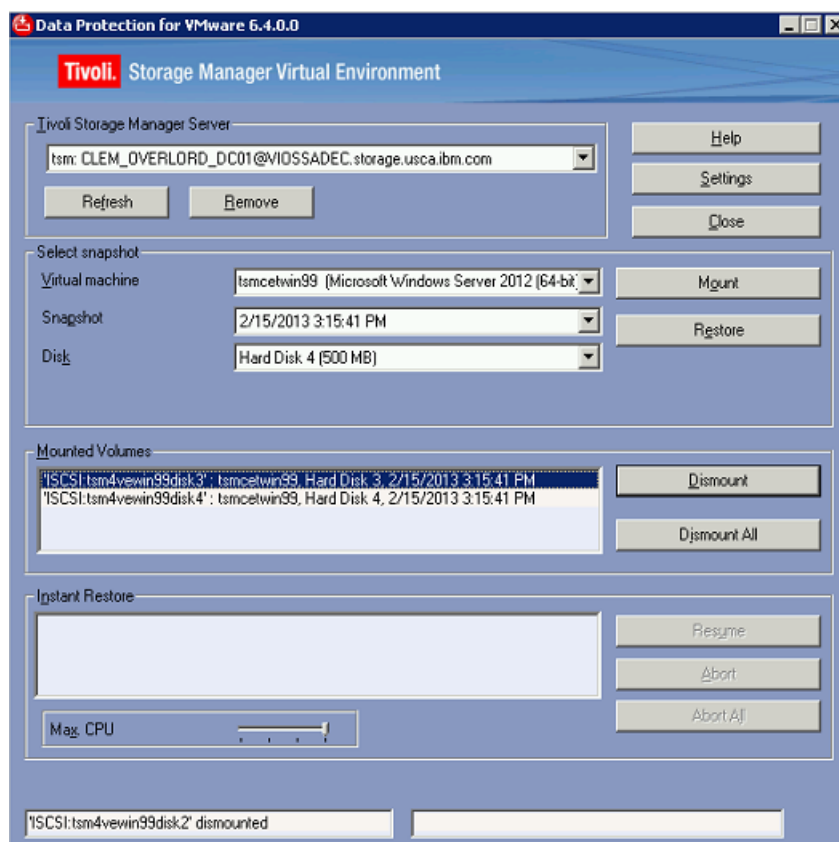


Figure 7-26 Dismount the snapshots

12. Click **Close** to close the Data Protection for VMware Recovery Agent by clicking.

7.1.4 File level restoration from Linux VM backup

The following two methods can be used to perform a file level restoration from Linux virtual machine backup:

- ▶ 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 (CLI), Cygwin, and OpenSSH on a Windows system. Use the Data Protection for VMware Recovery Agent GUI on the Linux machine

The following example guides you through the first method (which is preferred). The iSCSI targets are exposed to a Linux machine by the DP for VMware recovery agent from a Windows platform. Therefore, the steps are approximately the same as for Windows iMount. Expose the target corresponding to your snapshot to the Linux machine as shown in Figure 7-27 on page 150, by using the Linux iSCSI initiator ID.

Complete the following steps:

1. Connect to the one of the following Linux systems from which you want to access the data (it can be the same machine as the backup source, but it is not mandatory). Check that the iSCSI service is running, and start it if it is not, running:

– Red Hat:

```
service iscsi status  
service iscsi start
```

– SUSE:

```
service open-iscsi status  
service open-iscsi start
```

2. Determine the initiator name of the Linux machine, as shown in the following example:

```
targaryen:/opt/tivoli/tsm/client/ba/bin # cat /etc/iscsi/initiatorname.iscsi  
InitiatorName=iqn.1996-04.de.suse:01:4d91dddb45da
```

3. Configure the Data Protection for VMware to expose the snapshot to this initiator, as shown in Figure 7-27.

Select mount destination

Create virtual device for:
SLES10x64 - targaryen, Hard Disk 1, 2/15/2013 5:13:29 PM

☒ Mount as an iSCSI target

Target name:
targayendisk1

Initiator name:
iqn.1996-04.de.suse:01:4d91dddb45da

Make sure port 3260 is open on any firewall between this computer and the initiator.

☐ Create virtual volume from selected partition:

Partition number	Size	File System	Label
1	33.0 GB	EXT3	<No Label>

☒ Show only mountable partitions
☒ Mount virtual volume as read only

☒ Assign the following drive letter:
D:\

☐ Mount in the following empty NTFS folder:

Browse...

OK Cancel

Figure 7-27 Enter Linux initiator and target information

4. On the Linux machine, control that the target is properly exposed by using the command that is shown in Example 7-1.

Example 7-1 Command to expose target on Linux machine

```
targaryen:/opt/tivoli/tsm/client/ba/bin # iscsiadm -m discovery -t sendtargets -p  
broadsword.storage.usca.ibm.com
```

```
9.52.171.159:3260,1 targaryendisk1
```

Where broadsword.storage.usca.ibm.com is the machine where the Data Protection for VMware recovery agent is run.

5. Log in to the target by using the command that is shown in Example 7-2.

Example 7-2 Commands to log in to target

```
targaryen:/opt/tivoli/tsm/client/ba/bin # iscsiadm -m discovery -t sendtargets -p  
broadsword.storage.usca.ibm.com --login
```

```
9.52.171.159:3260,1 targaryendisk1
```

```
Logging in to [iface: default, target: targaryendisk1, portal: 9.52.171.159,3260]
```

```
Login to [iface: default, target: targaryendisk1, portal: 9.52.171.159,3260]:  
successful
```

6. Validate by using the **fdisk** command that the connection succeeded, as shown in Example 7-3.

Example 7-3 fdisk command to validate successful connection

```
targaryen:/opt/tivoli/tsm/client/ba/bin # fdisk -l
```

```
Disk /dev/sda: 42.9 GB, 42949672960 bytes
```

```
255 heads, 63 sectors/track, 5221 cylinders
```

```
Units = cylinders of 16065 * 512 = 8225280 bytes
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1		1	262	2104483+	82	Linux swap / Solaris
/dev/sda2	*	263	4570	34604010	83	Linux

```
Disk /dev/sdb: 42.9 GB, 42949672960 bytes
```

```
255 heads, 63 sectors/track, 5221 cylinders
```

```
Units = cylinders of 16065 * 512 = 8225280 bytes
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sdb1		1	262	2104483+	82	Linux swap / Solaris
/dev/sdb2	*	263	4570	34604010	83	Linux

Non-Logical Volume Manager volume

To access the data for a non-Logical Volume Manager (LVM) volume, complete the following steps:

1. Mount the device to a mount point of your choice. In our environment, the mount point is instance /mnttest, as shown in Example 7-4 on page 152.

Example 7-4 Mount the device

```
targaryen:/opt/tivoli/tsm/client/ba/bin # mkdir /mnttest
targaryen:/opt/tivoli/tsm/client/ba/bin # mount /dev/sdb2 /mnttest
targaryen:/opt/tivoli/tsm/client/ba/bin # ls -l /mnttest
total 116
drwxr-xr-x 3 root root 4096 Feb 15 16:26 CDF_Local
drwxr-xr-x 2 root root 4096 Sep 23 10:09 bin
drwxr-xr-x 3 root root 4096 Feb 14 18:25 boot
drwxr-xr-x 5 root root 4096 Sep 23 09:12 dev
drwxr-xr-x 7 root root 4096 Feb 15 15:52 downloads
drwxr-xr-x 79 root root 8192 Feb 14 21:09 etc
drwxr-xr-x 3 root root 4096 Feb 13 15:02 exploit
drwxr-xr-x 4 root root 4096 Feb 7 11:23 home
drwxr-xr-x 10 root root 4096 Sep 23 09:29 lib
drwxr-xr-x 5 root root 4096 Feb 14 01:21 lib64
drwx----- 2 root root 16384 Sep 23 09:11 lost+found
drwxr-xr-x 3 root root 4096 Feb 14 01:04 media
drwxr-xr-x 4 root root 4096 Feb 14 04:28 mnt
drwxr-xr-x 5 root root 4096 Feb 15 16:51 opt
drwxr-xr-x 2 root root 4096 Sep 23 09:12 proc
drwxr-xr-x 2 root root 4096 Jan 29 13:12 recovery
drwx----- 27 root root 4096 Feb 15 14:52 root
drwxr-xr-x 3 root root 8192 Feb 14 04:30 sbin
drwxr-xr-x 4 root root 4096 Sep 23 09:12 srv
drwxr-xr-x 3 root root 4096 Jan 29 13:18 staging
drwxr-xr-x 3 root root 4096 Sep 23 09:12 sys
drwxrwxrwt 19 root root 4096 Feb 15 17:00 tmp
drwxr-xr-x 14 root root 4096 Sep 23 10:02 usr
drwxr-xr-x 15 root root 4096 Feb 14 16:39 var
```

2. Copy the data back to your Linux machine.
3. Dismount the file system and disconnect from the iSCSI target by using the command that is shown in Example 7-5.

Example 7-5 Dismount file system example

```
umount /mnttest
targaryen:/exploit/logs # iscsiadm --mode node --logout
Logging out of session [sid: 1, target: targaryendisk1, portal: 9.52.171.159,3260]
Logout of [sid: 1, target: targaryendisk1, portal: 9.52.171.159,3260]: successful
```

LVM volume

If you perform file level recovery in a Linux virtual guest machine that uses LVM and when iSCSI exposure is used to the same machine from which the data was backed up, duplicate disks are exposed to the machine. In that case, it is important to ensure that file level information is available for restoration. When you are performing file level restore from a Linux disk with LVM information, it might be easier to perform the operation to a secondary Linux machine on which no duplicate disk signature issues occur. For more information, see the IBM Technote at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg21501082>

Otherwise, follow the procedure the is described next.

You can identify when disk is LVM by using the **fdisk** command, as shown in Example 7-6.

Example 7-6 Linux fdisk output

```
targaryen:/exploit/logs # fdisk -l
```

Disk /dev/sda: 42.9 GB, 42949672960 bytes
255 heads, 63 sectors/track, 5221 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1		1	262	2104483+	82	Linux swap / Solaris
/dev/sda2	*	263	4570	34604010	83	Linux

Disk /dev/sdb: 524 MB, 524288000 bytes
64 heads, 32 sectors/track, 500 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

Device	Boot	Start	End	Blocks	Id	System
/dev/sdb1		1	500	511984	8e	Linux LVM

Disk /dev/sdc: 524 MB, 524288000 bytes
64 heads, 32 sectors/track, 500 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

Device	Boot	Start	End	Blocks	Id	System
/dev/sdc1		1	500	511984	8e	Linux LVM

Disk /dev/sdd: 524 MB, 524288000 bytes
64 heads, 32 sectors/track, 500 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes

Device	Boot	Start	End	Blocks	Id	System
/dev/sdd1		1	500	511984	8e	Linux LVM

For an LVM volume, complete the following tasks:

1. List the exposed disks by using the **lvm pvscan** command, as shown in Example 7-7.

Example 7-7 List disks by using lvm command

```
targaryen:/exploit/logs # lvm pvscan
```

PV	/dev/sdd1	VG test1	lvm2	[496.00 MB / 0	free]
PV	/dev/sdc1	VG test1	lvm2	[496.00 MB / 0	free]
PV	/dev/sdb1	VG test1	lvm2	[496.00 MB / 488.00 MB	free]
Total: 3 [1.45 GB] / in use: 3 [1.45 GB] / in no VG: 0 [0]					

In our example, test1 is the volume group that is available on the exposed disks.

2. List the available logical volume in the exposed disks by using the **lvm lvs** command, as shown in Example 7-8.

Example 7-8 List available logical volume

```
targaryen:/exploit/logs # lvm lvs
```

LV	VG	Attr	LSize	Origin	Snap%	Move	Log	Copy%
lvmtest	test1	-wi---	1000.00M					

In our example, `lvmtest` is the logical volume that is available in the volume group `test1` in the exposed disks.

3. Import the exposed volume group by using the **`lvm lvchange`** command, as shown in Example 7-9.

Example 7-9 Import exposed volume group

```
lvm lvchange -a y test1
```

4. Mount the logical volume so it becomes reachable by using a file system, as shown in Example 7-10.

Example 7-10 Mount logical volume commands

```
targaryen:/exploit/logs # mkdir /lnx90recovery
targaryen:/exploit/logs # mount /dev/mapper/test1-lvmtest /lnx90recovery
targaryen:/exploit/logs # ls -l /lnx90recovery
total 38140
-rw-r--r-- 1 root root 3537189 Jan 29 18:10 afile.bin
-rw-r--r-- 1 root root 5095951 Jan 29 18:10 cfile.bin
-rw-r--r-- 1 root root 1935979 Jan 29 18:10 dfile.bin
-rw-r--r-- 1 root root 2374121 Jan 29 18:10 ffile.bin
drwx----- 2 root root 16384 Jan 29 18:09 lost+found
-rw-r--r-- 1 root root 26029241 Jan 29 18:11 sfile.bin
```

5. Copy the data by using the copy command, specify the **`--preserve=all`** option so you retrieve the file permissions as well.
6. After the copy operation completes, run the commands that are in Example 7-11 to unmount the file system and LVM definitions.

Example 7-11 Sample commands to unmount file system

```
targaryen:~ # umount /lnx90recovery
targaryen:~ # lvm lvremove test1
Do you really want to remove active logical volume "lvmtest"? [y/n]: y
Logical volume "lvmtest" successfully removed
targaryen:~ # lvm vgremove test1
Volume group "test1" successfully removed
```

7. Disconnect from the targets, as shown in Example 7-12.

Example 7-12 Sample commands to disconnect from the targets

```
targaryen:~ # iscsiadm --mode node --logout
Logging out of session [sid: 5, target: lnx90disk3, portal: 9.52.171.159,3260]
Logging out of session [sid: 6, target: lnx90disk2, portal: 9.52.171.159,3260]
Logging out of session [sid: 7, target: lnx90disk1, portal: 9.52.171.159,3260]
Logout of [sid: 5, target: lnx90disk3, portal: 9.52.171.159,3260]: successful
Logout of [sid: 6, target: lnx90disk2, portal: 9.52.171.159,3260]: successful
Logout of [sid: 7, target: lnx90disk1, portal: 9.52.171.159,3260]: successful
```

The command that is provided with **`--mode node --logout`** disconnect all of the targets. If you want to disconnect from specific target, add **`--targetname <targetname>`** to the command.

7.1.5 Instant recovery

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 in reference to the Data Protection for VMware Recovery Agent because it must be installed on the guest machine that contains the volume to be restored. Local volumes must have an assigned drive letter.

Note: If a disk cannot be parsed, an error message is displayed and the Instant Restore window is closed. For example, this occurs when the disk is dynamic or a GUID partition table (GPT).

Instant restore destination volumes must be on basic disks or simple volumes on dynamic disks.

7.1.6 Windows volume instant recovery

Complete the following steps to perform an instant recovery on Windows (you must have a volume with of the same or greater size already on the local system):

1. Open the Data Protection for VMware recovery agent and enter the Tivoli Storage Manager server credentials information, as shown in Figure 7-28.

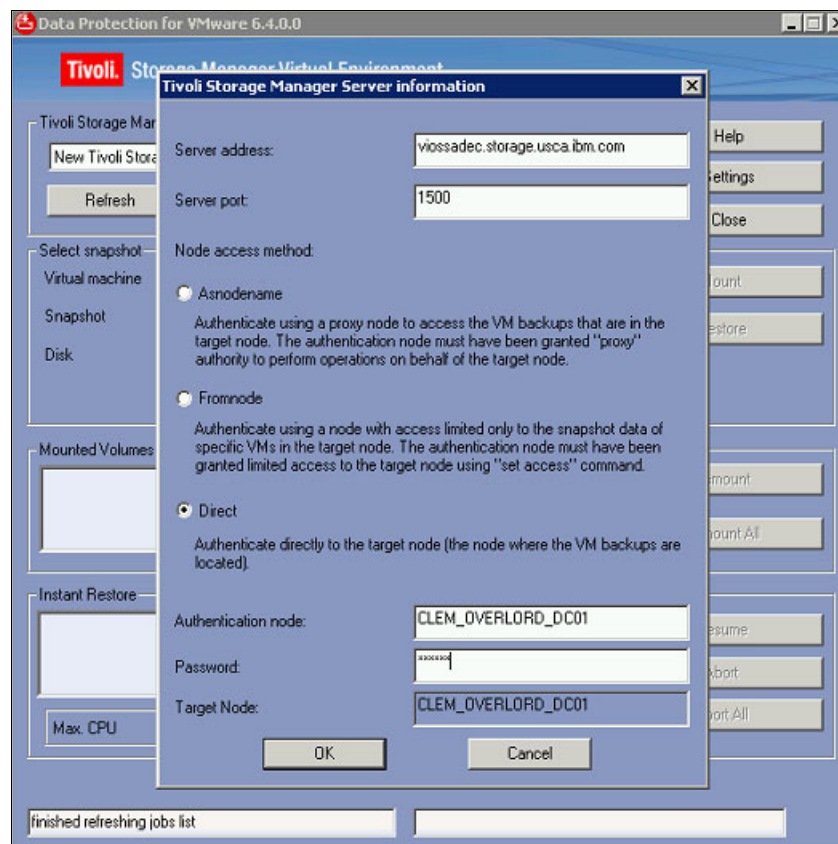


Figure 7-28 Tivoli Storage Manager credentials

2. Select the VM, snapshot date and time, the disk to be restored, and then click **Restore**, as shown in Figure 7-29.

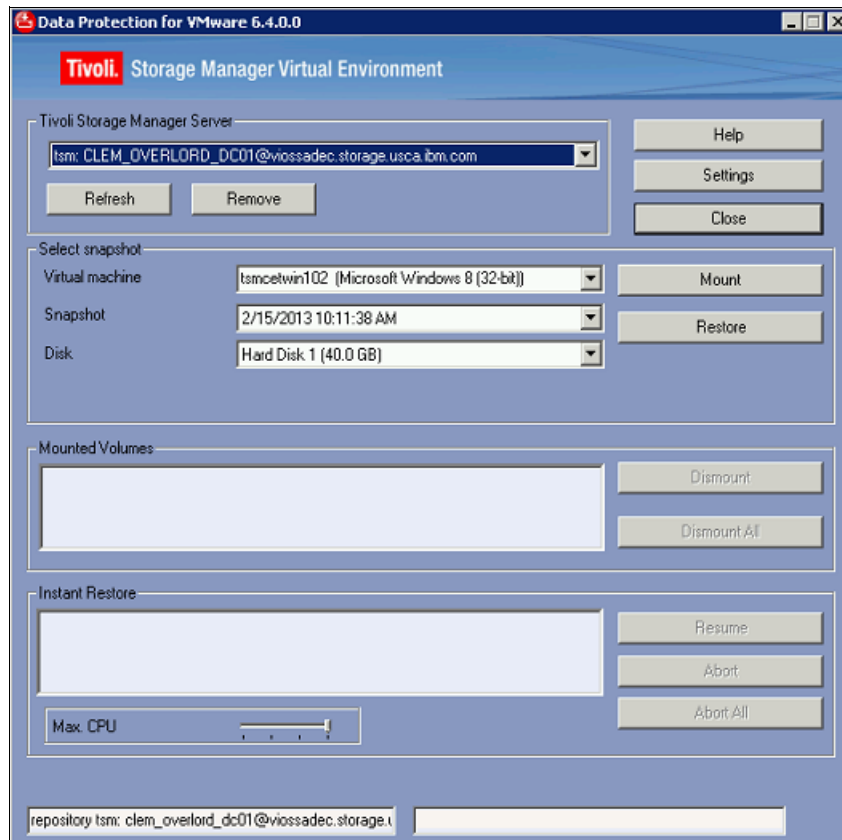


Figure 7-29 VM and snapshot selection

3. Choose the partition to be restored (if more than one is defined in the mounted disk) and the local destination where the data is to be restored, as shown in Figure 7-30.

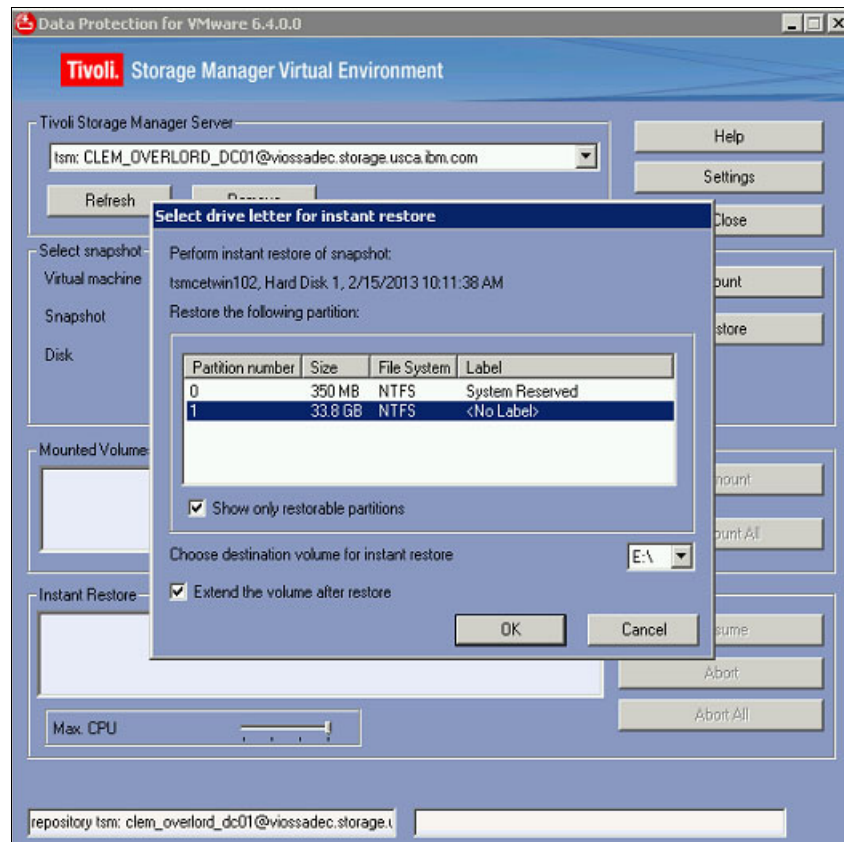


Figure 7-30 Select the volume to be restored and the destination

4. Accept the warning saying that the target volume will be erased, as shown in Figure 7-31.

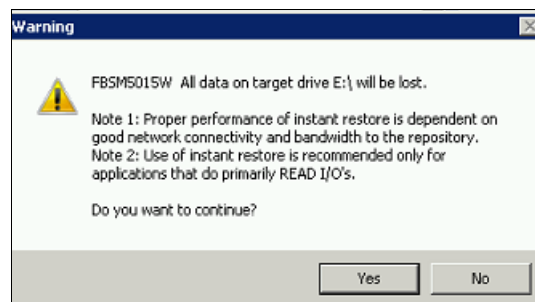


Figure 7-31 Warning message window

The background restore starts, as shown in Figure 7-32.

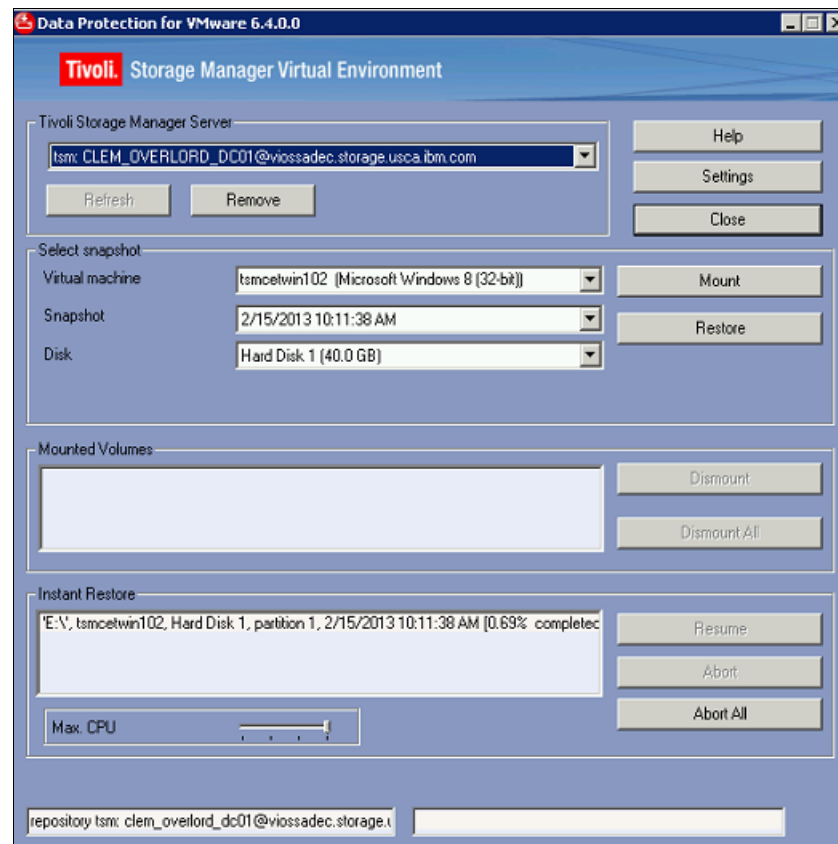


Figure 7-32 Instant restore monitoring: Restore in background

- Wait a few moments and then open your browser and browse to the volume, as shown in Figure 7-33.

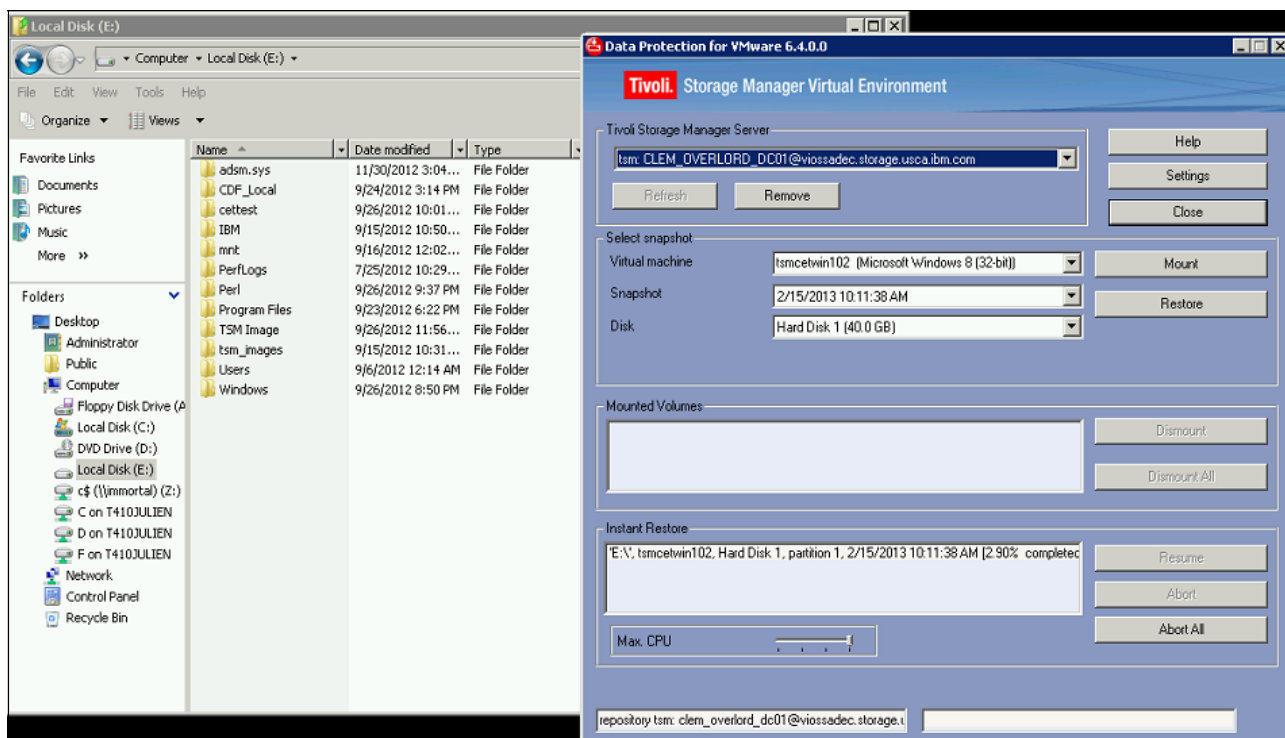


Figure 7-33 Browse to the volume that is being restored

Note: You can restore a file from this volume, even if it is not yet fully restored. A second Tivoli Storage Manager session is established to restore the requested data quicker.

After the background restore successfully, close the Data Protection for VMware recovery agent.

7.1.7 Linux volume instant restore

There are some requirements that must be met before you can use the Instant restore function on a Linux machine. The following components must be configured before you attempt the instant restore from a Linux box:

- Installed and configured on a Windows system: Cygwin, Data Protection for VMware Recovery Agent.
- Installed and configured the Linux Data Protection for VMware Recovery agent, iSCSI initiator, Secure Shell (SSH), perl, and mdadm.

Configuration prerequisite tasks

There are several prerequisite configuration tasks that must be completed before the instant restore function can be used.

Configuring Windows Cygwin SSH server

Use the following command to configure the SSH server on Windows machine. The account `cyg_server` is created to manage this service, as shown in Example 7-13 for the setup used for this book.

Example 7-13 `sshd` cygwin service setup

```
Administrator@broadsword ~$ ssh-host-config
*** Query: Overwrite existing /etc/ssh_config file? (yes/no) yes
*** Info: Creating default /etc/ssh_config file
*** Query: Overwrite existing /etc/sshd_config file? (yes/no) yes
*** Info: Creating default /etc/sshd_config file
*** Info: Privilege separation is set to yes by default since OpenSSH 3.3.
*** Info: However, this requires a non-privileged account called 'sshd'.
*** Info: For more info on privilege separation read
/usr/share/doc/openssh/README.privsep.
*** Query: Should privilege separation be used? (yes/no) no
*** Info: Updating /etc/sshd_config file

*** Query: Do you want to install sshd as a service?
*** Query: (Say "no" if it is already installed as a service) (yes/no) yes
*** Query: Enter the value of CYGWIN for the daemon: [] ntsec tty
*** Info: On Windows Server 2003, Windows Vista, and above, the
*** Info: SYSTEM account cannot setuid to other users -- a capability
*** Info: sshd requires. You need to have or to create a privileged
*** Info: account. This script will help you do so.

*** Info: You appear to be running Windows XP 64bit, Windows 2003 Server,
*** Info: or later. On these systems, it's not possible to use the LocalSystem
*** Info: account for services that can change the user id without an
*** Info: explicit password (such as passwordless logins [e.g. public key
*** Info: authentication] via sshd).

*** Info: If you want to enable that functionality, it's required to create
*** Info: a new account with special privileges (unless a similar account
*** Info: already exists). This account is then used to run these special
*** Info: servers.

*** Info: Note that creating a new user requires that the current account
*** Info: have Administrator privileges itself.

*** Info: The following privileged accounts were found: 'cyg_server' .

*** Info: This script plans to use 'cyg_server'.
*** Info: 'cyg_server' will only be used by registered services.
*** Query: Do you want to use a different name? (yes/no) no
*** Query: Please enter the password for user 'cyg_server':
*** Query: Reenter:

*** Info: The sshd service has been installed under the 'cyg_server'
*** Info: account. To start the service now, call `net start sshd' or
*** Info: `cygrunsrv -S sshd'. Otherwise, it will start automatically
*** Info: after the next reboot.

*** Info: Host configuration finished. Have fun!
```

```
Administrator@broadsword ~  
$ set CYGWIN 'ntsec tty'
```

```
Administrator@broadsword ~  
$ set | grep CYGWIN  
CYGWIN='ntsec tty'
```

```
Administrator@broadsword ~
```

Preparing the Windows system to receive a connection through SSH server

Complete the following steps:

1. After the Cygwin installation wizard completes successfully, set the following Microsoft Windows environment variables: from the Microsoft Windows Start menu, select **Control Panel** → **System**. In the System Properties window, click the **Advanced** tab, then click **Environment Variables**. The Environment Variables pane opens for you to update the following components:
 - Add the full path of the Cygwin\bin directory to the Microsoft Windows %PATH% system environment variable. The full path must be the first value that specified in the %PATH% system environment variable. The following example shows the full path statement if Cygwin is installed on your C:\ drive:
C:\cygwin\bin
 - Add CYGWIN as a Microsoft Windows user environment variable with the value ntsec tty, as shown in the following example:
CYGWIN="ntsec tty"
2. After these environment variables are added, restart Windows so that these variable updates are applied.

Editing the Cygwin environment configuration files

Complete the following steps:

1. On the Windows system, modify the C:\cygwin\etc\passwd entry for the cyg_server user to allow login, as shown in Example 7-14.

Example 7-14 cygwin environment configuration files

```
cyg_server:*:1001:513:Privileged  
server,U-BROADSWORD\cyg_server,S-1-5-21-1698724744-3087467771-2608222269-1001:/home/cyg_server:/bin/bash
```

2. Create the /home/cyg_server directory, and make cyg_server user the owner of this directory. Use the cygwin shell for these commands, as shown in the following example:
mkdir home/cyg_server; chown cyb_server /home/cyg_server

Edit the sshd configuration files

Complete the following steps:

1. On the Windows machine, modify the configuration file C:\cygwin\etc\sshd_config to enable the public key authentication method. Example 7-15 shows the lines that are to be tuned and unmarked.

Example 7-15 Cygwin sshd_config file

```
# The default requires explicit activation of protocol 1
Protocol 2
HostKey /etc/ssh_host_rsa_key
HostKey /etc/ssh_host_dsa_key
RSAAuthentication yes
PubkeyAuthentication yes
# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile /home/cyg_server/.ssh/authorized_keys
```

2. Edit the configuration file C:\cygwin\etc\hosts.allow, as shown in Example 7-16.

Example 7-16 Edit configuration file

```
ALL : localhost 127.0.0.1/32 [::1]/128 [::ffff:127.0.0.1]/128 : allow
sshd: ALL : allow
ALL : PARANOID : deny
```

Configuring the cygwin SSH exchange keys between Linux and Windows

Complete the following steps:

1. On the Linux machine, generate the public key from that machine, as shown in Example 7-17.

Example 7-17 Generate public key

```
targaryen:~ # ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
75:40:7d:c4:10:e3:72:bd:e5:eb:7f:c8:65:23:9b:0b root@targaryen
The key's randomart image is:
+--[ DSA 1024]-----+
|      .o.+=.      |
|      o.oo        |
|      o +.. .     |
|      . + +       |
|      S . .       |
|      . .+        |
|      E .+=.      |
|      .o+ .       |
|      ...+        |
+-----+

```

2. Send the public key to the Windows machine that is hosting the cygwin server, as shown in Example 7-18.

Example 7-18 Send public key to Windows machine that is hosting the cygwin server

```
targaryen:~/.ssh # scp id_dsa.pub cyg_server@broadsword:/home/cyg_server/
```

3. Return to the Windows system, open a cygwin terminal as cyg_user and configure the public key as an authorized key, as shown in Example 7-19. The file id_rsa.pub is the file that is sent from the Linux box.

Example 7-19 Configure public key as an authorized key

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

Cygwin sshd service is ready, reload it to force the configuration refresh

On the Windows machine, open a DOS CLI to submit the commands, as shown in Example 7-20.

Example 7-20 Sample commands to force configuration refresh

```
C:\Users\Administrator>net stop sshd
The CYGWIN sshd service is stopping.
The CYGWIN sshd service was stopped successfully.
```

```
C:\Users\Administrator>net start sshd
The CYGWIN sshd service is starting.
The CYGWIN sshd service was started successfully.
```

Start the Instant restore

From the Linux system, the following overall steps that are used to perform instant recovery (a volume with of the same or greater size must be ready on the local system):

1. Open the Data Protection for VMware Recovery Agent and enter Tivoli Storage Manager server credentials information, as shown in Figure 7-34 on page 164.
2. Select the VM, snapshot date/time, disk to be restored, and click **Restore**.
3. Choose the partition to be restored (if more than one defined in the mounted disk) and the local destination where the data will be restored.
4. Accept the warning that the target volume will be erased.

The background restore starts

5. Wait a few moments before you browse the file system.
6. After the background restore operation completes, you can close the Data Protection for VMware agent.

The following steps show the Instant Restore process:

1. Start the Data Protection for VMware recovery agent, as shown in the following example:

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

2. Open the Settings tab (as shown in Figure 7-34) and enter the information based on the set up that was completed.

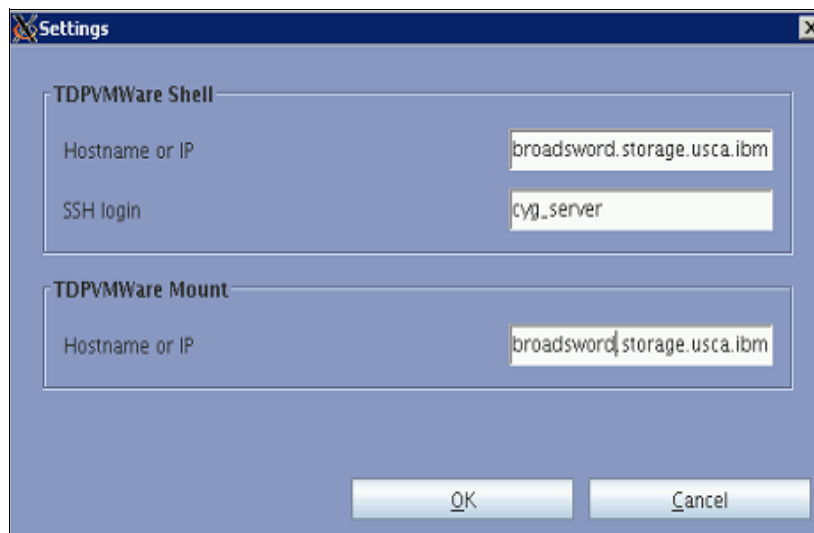


Figure 7-34 Settings tab

3. Enter the information to connect to the Tivoli Storage Manager server. All the connections are made through the Windows DP for VMware recovery agent on behalf of the Linux agent.
4. After you select your VM, snapshot data/time, and disk, click **Restore**.
5. Select the destination disk for the restored data.

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.
6. After the restoration is successful, close the Data Protection for VMware recovery agent interface.

7.2 Recovering data by using the Set Access and FromNode options

Depending on your environment, you might need to restrict data access when data is recovered data. One of the solutions is to separate the data across multiple datacenter nodes or to use the **FromNode** option during the recovery task.

In this section, we describe how the **FromNode** option works. By using **FromNode**, you can manage data access within a datacenter node. This access is configured by using the **set access** command from the client side.

Complete the following steps to configure this access:

1. By using the **dsnc** command, connect to the Tivoli Storage Manager server as datacenter node and grant access to the specific virtual machine from the node that is specified in the recovery agent as **Authentication node**, as shown in Example 7-21 on page 165.

Example 7-21 Set access example

```
[root@warden bin]# dsmc -virtualnodename=clem_overlord_dc01
IBM Tivoli Storage Manager
Command Line Backup-Archive client Interface
  Client Version 6, Release 4, Level 0.1
  Client date/time: 03/25/2013 13:53:10
(c) Copyright by IBM Corporation and other(s) 1990, 2012. All Rights Reserved.

Node Name: CLEM_OVERLORD_DC01
Please enter your user id <CLEM_OVERLORD_DC01>:

Please enter password for user id "CLEM_OVERLORD_DC01":

tsm> set access backup -type=VM tsmcetwin92 clem_julien_dm01
ANS1148I 'Set Access' command successfully completed
tsm>
```

The node name `clem_julien_dm01` now has access only to virtual machine `tsmcetwin92`, which is stored within the `CLEM_OVERLORD_DC01` datacenter node.

2. When the Data Protection for VMware recovery agent interface is started, define a Tivoli Storage Manager server connection by using the `FromNode` option that is configured to access the VM snapshot that must be mounted, as shown in Figure 7-35.

Tivoli Storage Manager Server information

Server address:

Server port:

Node access method:

☐ Asynodename
Authenticate using a proxy node to access the VM backups that are in the target node. The authentication node must have been granted "proxy" authority to perform operations on behalf of the target node.

☒ Fromnode
Authenticate using a node with access limited only to the snapshot data of specific VMs in the target node. The authentication node must have been granted limited access to the target node using "set access" command.

☐ Direct
Authenticate directly to the target node (the node where the VM backups are located).

Authentication node:

Password:

Target Node:

Figure 7-35 Tivoli Storage Manager Server connection

If you try to access to a virtual machine snapshot that was allowed with the set access command, the error message that is shown in Figure 7-36 opens.

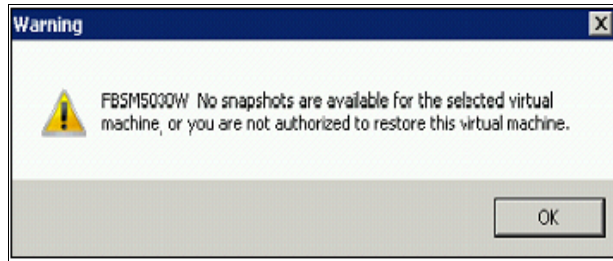


Figure 7-36 Error message that VM snapshot access was not granted

3. Select the VM and the snapshots from which you need to read, as shown in Figure 7-37.

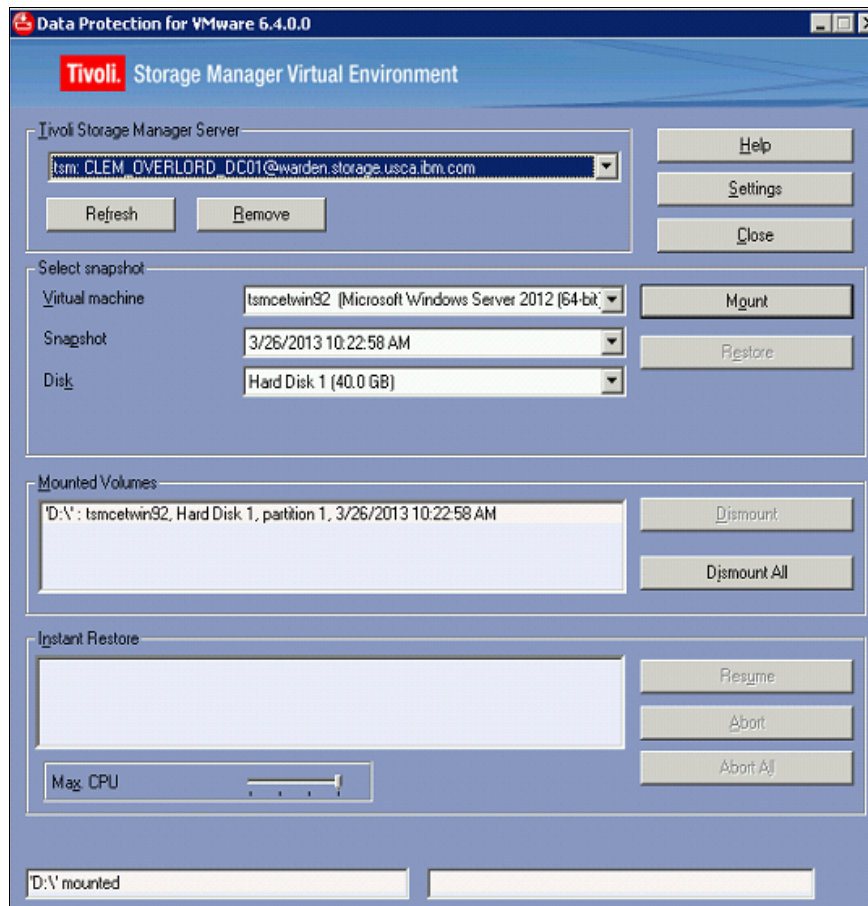


Figure 7-37 VM snapshots mounted



Reporting that uses vCenter plug-in or SQL queries

This chapter describes the following types of reports that are available by using Data Protection for VMware:

- ▶ Reports that can be displayed natively in the Tivoli Storage Manager Data Protection for VMware vSphere client plug-in user interface
- ▶ Reports that can be created by mining information in the Tivoli Storage Manager Server database by using SQL SELECT statements and the administrative command-line client.

Note: Tivoli Storage Manager server 6.3.3 or above is required to have these reports available.

This chapter includes the following topics:

- ▶ Reporting by using vCenter plug-in
- ▶ Reporting by using SQL commands

8.1 Reporting by using vCenter plug-in

The vCenter plug-in has the following built-in reports that show the backup activity:

- ▶ Back up Status of virtual machines (VMs)
- ▶ VMs without backups
- ▶ VM with a completion date more than seven days in the past
- ▶ VM with a backup status other than success
- ▶ VM that has backup but the VM does not exist in the vCenter
- ▶ How Much Data is Being Managed for a Datacenter: A report to determine how much space is used in the Tivoli Storage Manager Server to manage a VMware vSphere datacenter.

To access these reports, open the plug-in and go to the Reports tab and click **Backup Status**, as shown in Figure 8-1.

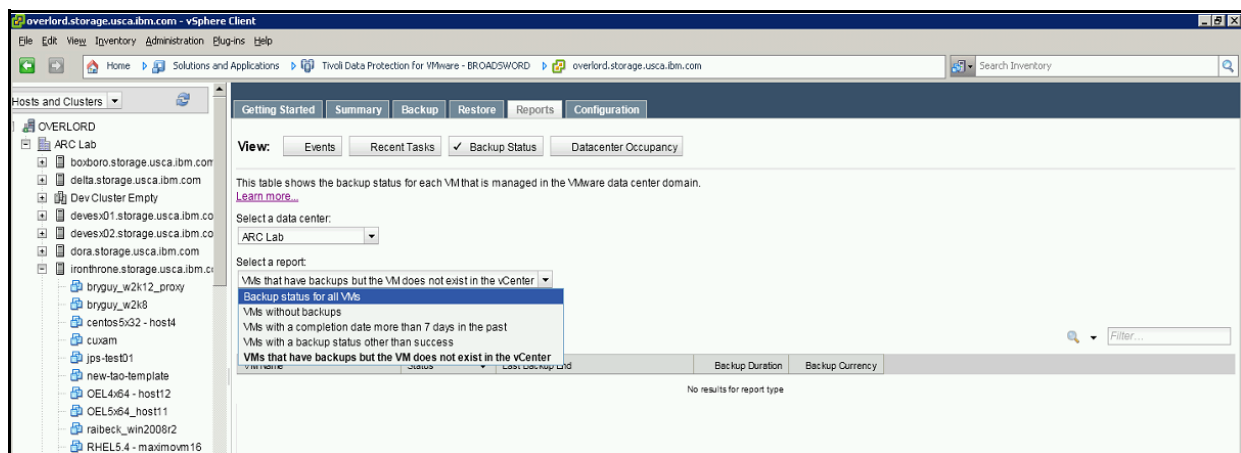


Figure 8-1 Built-in VM backups reports

There is also a report about the datacenter occupancy, as shown in Figure 8-2.

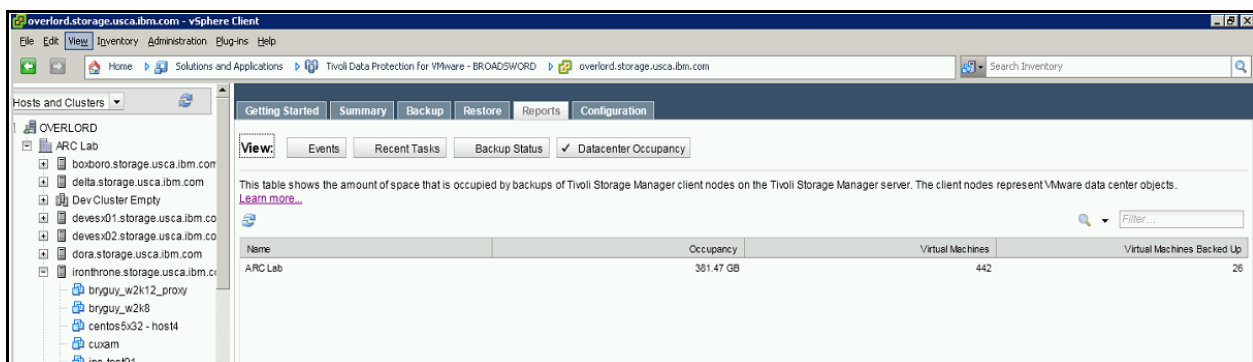


Figure 8-2 DP for VMware vCenter plug-in: Datacenter Occupancy

The following tabs also are available in the reporting:

- **Events:** A report that displays the status of the most recent events that completed within the last three days.
- **Recent Tasks:** Used to verify the progress of a backup or restore task that completed in the last hour or was recently started. The information identifies tasks in real time and includes steps that were already completed. Tivoli Storage Manager for Virtual Environments backups that are scheduled with a Tivoli Storage Manager server are not displayed in the table.

8.2 Reporting by using SQL commands

You can run your own reports by querying the Tivoli Storage Manager server tables. In this section, we provide several examples of what you can do to report your VM backup activity.

Queries that use a SUMMARY_EXTENDED table can be run with Tivoli Storage Manager server version 6.3.3 or above.

8.2.1 Successful backup in a specified time frame

The first scenario that we describe is Successful Backup in Last 24 hours, which is a report to list all the VMs that were protected the last 24 hours, including backup type and number of bytes processed, as shown in the following example:

```
select SUB_ENTITY,ACTIVITY_TYPE,SUCCESSFUL,BYTES from SUMMARY_EXTENDED where
START_TIME>current_timestamp - 24 hours and ENTITY like '%CLEM%DM01' and SUB_ENTITY
IS NOT NULL AND SUCCESSFUL='YES'
```

You can tune this query by using a script instead, as shown in Example 8-1.

Example 8-1 Script to report completed backups last \$1 hours managed by datamover \$2

```
define script REPORTOK_VM desc="VM backup stats for $1 hours , managed by
datamover $2"
update script REPORTOK_VM "select SUB_ENTITY,ACTIVITY_TYPE,SUCCESSFUL,BYTES from
SUMMARY_EXTENDED where END_TIME>current_timestamp - $1 hours and ENTITY like '$2'
and SUB_ENTITY IS NOT NULL and SUCCESSFUL='YES'" line=10
```

```
tsm: VIOSSADEC>run REPORTOK_VM 90 CLEM_BROADSWORD_DM01
SLES11x64 - arryn Incremental Forever - Full YES 33559807580
ANR1462I RUN: Command script REPORTOK_VM completed successfully.
```

```
tsm: VIOSSADEC>run REPORTOK_VM 3 CLEM_TARGARYEN_DM01
tsmcetwin101 Incremental Forever - Incremental YES 315571611
tsmcetwin103 Incremental Forever - Incremental YES 324618405
tsmcetwin104 Incremental Forever - Incremental YES 862156452
tsmcetwin102 Incremental Forever - Incremental YES 812572325
ANR1462I RUN: Command script REPORTOK_VM completed successfully.
```

8.2.2 Unsuccessful backup in a specified time frame

In this scenario, we create a What Failed Last 24 hours report. The report shows which VM backups failed in the last 24 hours, including information about its datacenter node and the reason for the failure, as shown in the following example:

```
select nodename,message from actlog where DATE_TIME>current_timestamp - 24 hours
and MSGNO=4174
```

8.2.3 Not backed up in a specified time frame

In this scenario, we create a Not Backed up Since report. By using this report, you can determine which virtual machines were not backed up since a specified time, including the last backup date, as shown in the following example:

```
select substr(FILESPACE_NAME,9,50) as "Virtual Machine",date(backup_end) from
FILESPACES where filespace_name like '%VMFUL%' and backup_end<=current_timestamp -
24 hours and node_name like '%CLEM%' order by backup_end asc
```

You can tune this query by using a script instead, as shown in Example 8-2.

Example 8-2 Script to report missed backup since \$1 days for \$2 DC node

```
define script NOTBACKEDUP_VM desc="VM not backed up since $1"
update script NOTBACKEDUP_VM "select substr(FILESPACE_NAME,9,50),date(backup_end)
from FILESPACES where filespace_name like '%VMFUL%' and
backup_end<=current_timestamp - $1 days and node_name='$2' order by backup_end
asc" line=10
tsm: VIOSSADEC>run NOTBACKEDUP_VM 1 CLEM_OVERLORD_DC01
tsmcetlnx70                2013-02-15
tsmcetwin99                2013-02-15
SLES10x64 - targaryen      2013-02-15
tsmcetwin100               2013-02-18
tsmcetwin105               2013-02-18
tsmcetwin106               2013-02-18
win2008x64 - tsmportal     2013-02-18
SLES11x64 - arryn          2013-02-19
ANR1462I RUN: Command script NOTBACKEDUP_VM completed successfully.
```

8.2.4 Comparing successful full and successful incremental backups

It is often helpful to know how many incremental backups are being successfully run relative to the number of full backups that are being successfully run. Comparing these two numbers can provide insight into a backup trend for a VM, such as, errors that prevent incremental backups from being taken because of change block tracking (CBT) failures or other compatibility issues.

This report is designed for the Tivoli Storage Manager V6.4 incremental forever VM backup model and must be modified to report on the older “full plus incremental” model before version V6.4, as shown in the following example:

```
select x.SUB_ENTITY as "VM NAME", (select count(*) from summary_extended y where
x.SUB_ENTITY=y.SUB_ENTITY and entity like '%DM%' and ACTIVITY_TYPE='Incremental
Forever - Full' and SUCCESSFUL='YES' and START_TIME>CURRENT_DATE - INTERVAL '14'
DAY) as "IFFULL", (select count(*) from summary_extended y where
x.SUB_ENTITY=y.SUB_ENTITY and entity like '%DM%' and ACTIVITY_TYPE='Incremental
Forever - Incremental' and SUCCESSFUL='YES' and START_TIME>CURRENT_DATE - INTERVAL
'14' DAY) as "IFINCR" from summary_extended x group by SUB_ENTITY ORDER BY IFFULL
DESC, IFINCR DESC
```

You can tune this query by using a script instead, as shown in Example 8-3.

Example 8-3 Query comparing number of full versus incremental backups for each virtual machine

```
tsm: WARDEN>select x.SUB_ENTITY as "VM NAME", (select count(*) from
summary_extended y where x.SUB_ENTITY=y.SUB_ENTITY and entity like '%DM%' and
ACTIVITY_TYPE='Incremental Forever - Full' and SUCCESSFUL='YES' and
START_TIME>CURRENT_DATE - INTERVAL '14' DAY) as "IFFULL", (select count(*) from
summary_extended y where x.SUB_ENTITY=y.SUB_ENTITY and entity like '%DM%' and
ACTIVITY_TYPE='Incremental Forever - Incremental' and SUCCESSFUL='YES' and
START_TIME>CURRENT_DATE - INTERVAL '14' DAY) as "IFINCR" from summary_extended x
group by SUB_ENTITY ORDER BY IFFULL DESC, IFINCR DESC
```

VM NAME	IFFULL	IFINCR
tsmcetwin94	11	4
tsmcetwin105	9	6
tsmcetwin107	9	6
tsmcetwin106	9	5
tsmcetwin110	9	5
tsmcetwin101	9	4
tsmcetwin97	9	4
tsmcetwin102	8	6
tsmcetwin99	7	6
tsmcetwin100	5	9
tsmcetwin103	0	15
tsmcetwin104	0	15
tsmcetwin108	0	15
tsmcetwin109	0	15
tsmcetwin93	0	15
tsmcetwin95	0	15
tsmcetwin96	0	15
tsmcetwin98	0	15
tsmcetwin92	0	10
tsmcetwin91	0	6

8.2.5 Additional reporting information

For more information about the Tivoli Storage Manager Data Protection for VMware vCenter plug-in reporting, see this website:

https://www.ibm.com/developerworks/community/wikis/form/anonymous/api/wiki/93193ba0-be33-4733-9b03-9ab823a7475c/page/36548a5d-a9df-4e5a-ae3a-eada9f2f37ee/attachment/b8166859-548e-4504-b70f-989e865fa8f8/media/DPforVMware_Reporting640_V20130905.pdf



Problem determination and FAQs

This chapter provides answers to issues or any questions you might have that are related to the implementation of Data Protection for VMware.

This chapter includes the following topics:

- ▶ Common errors
- ▶ Analyzing error situations and getting support
- ▶ Frequently Asked Questions

9.1 Common errors

When you receive an error message, review the known limitations pages to be sure that it is not a behavior that is already referenced. For more information, see 3.11.1, “Tivoli Storage Manager Backup Archive considerations” on page 49.

9.1.1 Common error messages

In this section, we describe common error messages that help in problem determination.

ANS9365E VMware vStorage API error

Error message:

ANS9365E VMware vStorage API error.

TSM function name : visdkWaitForTask

TSM file : vmvisdk.cpp (2933)

API return code : 78

API error message : A general system error occurred: Protocol error from VMX.

ANS4151E Failure mounting Virtual Machine xxxxxxx. RC=115

Possible solution

Check the Network Time Protocol daemon (NTPD) service on the ESX host.

ANS9365E VMware vStorage API error

Error message

ANS9365E VMware vStorage API error.

TSM function name : visdkWaitForTask

TSM file : vmvisdk.cpp (2933)

API return code : 78

API error message: Cannot create a quiesced snapshot because the create snapshot operation exceeded the time limit for holding off I/O in the frozen virtual machine.

Possible solution

Check the Volume Shadow Copy Services (VSS) messages on Host, check free space on C:, and check VMtools installation on VM guest.

ANS9365E VMware vStorage API error

Error message

ANS9365E VMware vStorage API error.

TSM function name: VixDiskLib_Open

TSM file : vmvddksdk.cpp (1428)

API return code : 13

API error message: You do not have access rights to this file

ANS4148E Full VM backup of Virtual Machine 'xxxxxxx' failed with RC -1

Possible solution

Check that your proxy has ping or network access to the ESX server that is hosting the virtual machine (VM) at the backup time.

ANS1403E Error loading a required Library

Error message

ANS1403E Error loading a required Library: vixDiskLib.dll, Win32 rc=126 DLL

ANS4152E Failure initializing VMware virtual machine environment. RC=-303. Refer to client dserror.log for detailed error messages.

Possible solution

During Backup/Archive Client installation, VMware backup tools must be selected in the custom installation path to allow Tivoli Storage Manager VMware backups to take place.

ANS9365E VMware vStorage API error

Error message

ANS9365E VMware vStorage API error.

TSM function name : vddksdkWrite

TSM file : vmvddksdk.cpp (2271)

API return code : 16007

API error message : You have requested access to an area of the virtual disk that is out of bounds

ANS0361I DIAG: ANS1111I VmRestoreExtent(): VixDiskLib_Write FAILURE startSector=1 sectorSize=1 byteOffset=512, rc=-1

ANS5283E The operation was unsuccessful.

Possible solution

The datastore is on NetApp or Nseries NAS storage and was aligned by using the mbalign utility of the storage vendor. APAR IC84544 was opened for this issue. Contact IBM support if the fix is not yet available. For more information, see the IBM Tivoli Storage Manager support website at:

<http://www-947.ibm.com/support/entry/portal/support>

ANS9365E VMware vStorage API error

Error message

ANS9365E VMware vStorage API error.

TSM function name : VixDiskLib_Write

TSM file : vmvddksdk.cpp (2485)

API return code : 1

API error message : Unknown error

ANS0361I DIAG: ANS1111I VmRestoreExtent(): VixDiskLib_Write FAILURE startSector=512 sectorSize=512 byteOffset=262144, rc 4398

ANS5226E The virtual machine backup operation failed

or

ANS9365E VMware vStorage API error.

TSM function name : vddksdkWrite

TSM file : vmvddksdk.cpp (2271)

API return code : 1

API error message : Unknown error

ANS0361I DIAG: ANS1111I VmRestoreExtent(): VixDiskLib_Write FAILURE startSector=512 sectorSize=512 byteOffset=262144, rc=-1

ANS5226E The virtual machine backup operation failed

Possible solution

This points to an incorrect configuration of the Windows 2008 or Windows 2008 R2 proxy where the SAN POLICY setting was not set to OnlineAll. For more information, see Tivoli Storage Manager DOC APAR IC77216 and VMware KB 1035096.

ANS1403E Error loading a required Library

Error message

01/06/2012 14:53:57 ANS1403E Error loading a required Library: libvixMntapi.so, Linux rc=libfuse.so.2: cannot open shared object file: No such file or directory
DLL

ANS4152E Failure initializing VMware virtual machine environment. RC=-303. Refer to client dsmerror.log for detailed error messages.

Possible solution

There are two possible causes for this error. The LD_LIBRARY_PATH environment variable is not set or does not include /opt/tivoli/tsm/client/ba/bin, or required software packages are missing from the host.

Set and export the LD_LIBRARY_PATH environment variable to point to the client installation directory. For example, export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin.

To perform backups or restores of VMware virtual machines by using a Backup-Archive client on a Novell SUSE Linux system, the libfuse.so.2 shared object library must be installed. Install libfuse version 2.

To perform backups or restores of VMware virtual machines by using a Backup-Archive client on a Red Hat Enterprise Linux system, the libfuse.so.2, libxml2.so, and libexpat.so shared object libraries must be installed. Install fuse-libs version 2.

For more information, see the IBM Technote that is available at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg21577631>

9.1.2 Restoration by using SAN transport method

FULL VM restore by using the storage area network (SAN) or HotAdd transport method might silently fail because of a write error. The consequence of this failure is that the VM is not find the operating system at restart.

You might have trouble when you are restoring a FULL VM by using the LAN-free Path. This is documented in the APAR IC80972 and fixed in version 6.4, which is already available.

FULL VM restore by using SAN transport method (between the vBS and the datastore) might be slower than expected when you are restoring a thin disk. This is documented in a VMware article because it is caused by the disk manager APIs. For thin disk restore, NBDSSL is faster, and NBD is even faster.

For more information, see this website:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1035096

The virtual machine template backups cannot be restored by using SAN transport because they cannot be backed up over the SAN.

9.1.3 Incremental Forever and FULL-VM recovery issue

You might experience an error while a FULL-VM recovery is performed if the virtual machine name contains the string JOB (all in uppercase).

For more information about this error, see this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg1IC85707>

9.1.4 Plug-in management

You might need to manually remove or unregister the Data Protection for VMware plug-in from the vSphere vCenter server.

For more information about how to perform this task, see the IBM Technote that is available at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg21595585>

More information also is available in the *Re-register the Data Protection for VMware vCenter plug-in* section of the product manual, which is available at this website:

http://pic.dhe.ibm.com/infocenter/tsminfo/v6r4/topic/com.ibm.itsm.ve.doc/r_ve_gui_troubleshoot.html

9.2 Analyzing error situations and getting support

In this section, we describe tools that are available to help you resolve error conditions. We direct you to resources for more information and help in resolving errors.

9.2.1 Web resources

If you are experiencing problems with your Data Protection for VMware installation, see the following Tivoli Storage Manager Support website and search the knowledge base:

<http://www-01.ibm.com/software/sysmgmt/products/support/IBMTivoliStorageManager.html>

Various Technotes are available that might give you some hints to solve the issue on your own

For more information about dedicated Data Protection for VMware support, see this website:

http://www-947.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager_for_Virtual_Environments

If you do not find a solution and you are entitled to support, collect the information by using the process that is described at this website:

<https://www-304.ibm.com/support/docview.wss?uid=swg21497489>

9.2.2 Tracing

You can activate tracing for your VMware backups or restores by doing the completing the following steps:

1. Edit and save your `dsmvddk.opt` file to enable VMware trivia tracing by changing LogLevels from 1 to 6, as shown in the following example:

```
# 0-quiet, 1-panic, 2-error, 3-warning, 4-info, 5-verbose, 6-trivia
vixDiskLib.transport.LogLevel = "6"
vixDiskLib.nfc.LogLevel = "6"
```

2. Edit your `dsm.opt` file to activate tracing in the Tivoli Storage Manager client, as shown in the following example:

```
TRACEFLAGS VM
TRACEFILE vmtrace.out
```

3. Rerun the failing backup or restore. Make sure to revert these changes after the issue is re-created.

9.2.3 Contacting IBM support: Opening a service request

This section provides information that you should review before you contact IBM Support.

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.

To obtain help from IBM Software Support, complete the following steps:

1. Ensure that you completed the following prerequisites:

- Set up a subscription and support contract.

The type of contract that you need depends on the type of product you are using. For IBM distributed software products (including, but not limited to, IBM Tivoli, Lotus®, and Rational® products and IBM DB2® and IBM WebSphere products that run on Microsoft Windows or on operating systems such as IBM AIX® or Linux), enroll in IBM Passport Advantage® by using one of the following methods:

- Online: See the Passport Advantage website at:

<http://www.ibm.com/software/lotus/passportadvantage>

Click **How to enroll** and follow the instructions.

- By telephone: Call 1-800-IBMSERV (1-800-426-7378) in the United States. For the telephone number to call in your country, see the IBM Software Support Handbook at this website:

<http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html>

Click **Contacts**.

- Determine the business impact of your problem.

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. The following levels are used:

- Severity 1 Critical business impact: You cannot use the program, which results 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 was implemented.
- Describe your problem and gather background information.

When you are 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 the following 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.

2. Follow the instructions in “Submitting the problem to IBM Software Support” on page 179.

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 the telephone number to call in your country, see the IBM Software Support Handbook at this website:

<http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html>

Click **Contacts**.

9.3 Frequently Asked Questions

An up-to-date Frequently Asked Questions (FAQ) section is available in the IBM Wiki, which is available at this website:

<https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Storage%20Manager/page/FAQ>

There you can find various documentation resources that are used to answer the following questions:

- ▶ Question 1: Does Data Protection for VMware provide support for virtual machines that are created by VMware's vCloud Director?

Answer: The Tivoli Field Guide provides information about support for virtual machines that are created by VMware's vCloud Director. The guide is available at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg27024601>

- ▶ Question 2: Can LAN-free that uses tape devices be used with a vStorage backup server running in a virtual machine?

Answer: No. As of this writing, LAN-free data movement is not supported by a VMware guest machine. For more information about operations that are supported from VMware guest machines, see the technote *IBM Tivoli Storage Manager guest support for Virtual Machines and Virtualization*.

- ▶ Question 3: Which TCP/IP ports are used for communication between a Tivoli Storage Manager vStorage backup server and other components in the VMware environment?

Answer: The Tivoli Storage Manager vStorage backup server communicates to the VMware Virtual Center by using https on port 443. If you are using the NBD or NBDSSL transport, port 902 is used for communication to the ESX server for the data movement.

For more information, see the VMware article *TCP and UDP Ports required to access vCenter Server, ESX hosts, and other network components* or 3.4, "Communication ports between VMware and Tivoli Storage Manager components" on page 36.

- ▶ Question 4: What version of the VMware Virtual Disk Development Kit (VDDK) does Tivoli Storage Manager Data Protection for VMware and Backup-Archive client use?

Answer: The following VDDK levels are used by Tivoli Storage Manager:

- Tivoli Storage Manager V6.2.2 VDDK 1.2.1. For more information, see this website:

<http://www.vmware.com/support/developer/vddk/VDDK-1.2.1-Relnotes.html>

- Tivoli Storage Manager V6.3. uses VDDK 5.0. For more information, see this website:

<http://www.vmware.com/support/developer/vddk/VDDK-500-ReleaseNotes.html>

- Tivoli Storage Manager V6.4 uses VDDK 5.0. For more information, see this website:

<http://www.vmware.com/support/developer/vddk/VDDK-501-ReleaseNotes.html>

- ▶ Question 5: What Tivoli Storage Manager administrative privilege is needed to use the 6.4 and 6.3 Data Protection for VMware - Data Protection for VMware vSphere Client plug-in user interface?

Answer: For more information, see the IBM Technote that is available at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg21584416>

- Question 6: Does Data Protection for VMware protect virtual machine configuration information?

Answer: Yes. For more information about how Data Protection for VMware protects virtual machine configuration that is stored in the .vmx file, see the IBM Technote for 6.4 and IBM Technote for 6.3.

- Question 7: Can Tivoli Storage Manager protect a virtual machine that is deployed in a vApp?

Yes. For more information about how Data Protection for VMware protects virtual machines that are deployed in a vApp, see the IBM Technote that is available at this website:

<http://www-01.ibm.com/support/docview.wss?uid=swg21579252>

- Question 8: Can I recover individual files from a VMware virtual machine backup from a machine that is in a remote office over a WAN link?

Yes. The supported approach is to use the Data Protection for VMware Recovery Agent on a machine local to the Tivoli Storage Manager server to mount the backup data to a local Windows or Linux machine. You then use Windows sharing (CIFS) or NFS on Linux to share the data to the remote office.

- Question 9: Is Change Block Tracking supported on raw device mapping (RDM) volumes?

Answer: Change Block Tracking is supported on RDM volumes that were provisioned in the virtual compatibility mode (vRDM). RDM volumes that were provisioned in the physical compatibility mode (pRDM) do not support snapshots or change block tracking.

- Question 10: What is the difference between the Tivoli Storage Manager Backup-Archive client and Data Protection for VMware - Data Protection for VMware?

The Tivoli Storage Manager Backup-Archive client can be used to protect VMware virtual machines or with Data Protection for VMware. The following features of the different offerings are available:

- Backup-Archive client: Full virtual machine (full-vm) backup and recovery that uses the VMware vStorage APIs for Data Protection
- Data Protection for VMware:
 - Full virtual machine (full-vm) backup and recovery that uses the VMware vStorage APIs for Data Protection (via the Backup-Archive client)
 - Incremental backup of virtual machines (via the Backup-Archive client)
 - Granular file level recovery
 - Near-instant volume recovery

- Question 11: How does retention policy in Tivoli Storage Manager 6.4 work with full and incremental VM backups?

Answer: Data Protection for VMware manages backup retention differently in version 6.4 than in 6.3 when the new incremental-forever capability is used. With incremental-forever in version 6.4, each backup is treated as an independent recovery point where its retention is managed without a connection to whether a backup is full or incremental.

For example, suppose that you set up a management class without a limit on the number of versions (VERExists=noLimit) and limit the retention of each backup to no more than 45 days (RETEExtra=45). With a daily backup, you end up with 45 recovery points where older backups expire after 45 days. With this model, more ad hoc backups can be taken that do not cause earlier recovery points to expire early, but you might end up with more than 45 recovery points retained.

- Question 12: How does retention policy in Tivoli Storage Manager 6.3 work with full and incremental VM backups?

Answer: Data Protection for VMware manages backup retention that is based on the full-vm backups and independently of the number of intermediate incremental backups.

For example, suppose that you set up a management class to retain three versions (VERExists=3) and that a full backup is scheduled on the weekend and incremental backups are scheduled on each of the five weekdays. The Tivoli Storage Manager Server retains the three full-vm backups and their dependent incremental backups. When the fourth full-vm backup is stored on the server, the first full backup and its five incremental backups are marked for expiration.

In addition to VERExists, the retain extra versions attribute (RETExt ra) can be used to manage virtual machine backups.

- Question 13: How do I select the management class that is associated with a VM backup?

Virtual machine backups are assigned to the default management class unless the user specifies the VMMC Backup-Archive client option to use a different management class.

You can specify the VMCTLMC Backup-Archive client option to control the storage pool destination for the virtual machine control files. This is used with backups that are stored to tape media. For more information about the use of tape media and the VMCTLMC option, see the Technote *Data Protection for VMware Tape Support Statement*.

- Question 14: Should a vStorage server be a physical machine or VM guest?

The vStorage server refers to a machine where the Backup-Archive client is installed. The vStorage server can be a VM guest machine or an off-host physical machine.

The following considerations should be reviewed when you are installing the Backup-Archive client on an off-host physical machine:

- Offloads backup from ESX / ESXi host:
 - Supports a SAN data path from VMware storage to Backup-Archive client and from Backup-Archive client to Tivoli Storage Manager server.
 - Typically direct SAN access is the best-performing solution.

The following considerations should be reviewed when you are installing the Backup-Archive client within a VM guest:

- Potentially a more economical solution:
 - Supports a HOTADD data path from VMware storage, which makes use of data movement across the SAN.
 - Typically preferable to use more datamovers so that each cluster is protected by its own datamover.
 - Might be practical if there are times when the backup window is available and increased CPU workload from the backup does not affect product workload. When the Backup-Archive client is running, there is an increased CPU workload (especially if deduplication and compression are performed). A virtual machine cluster can absorb this workload. But, when there is a high consolidation ratio and host workloads are running all of the time, a virtual machine on a dedicated host for backup might be required.
- Question 15: Can I use Tivoli Storage Manager Backup-Archive client compression with Data Protection for VMware?

Answer: Tivoli Storage Manager Backup-Archive client compression can be used only with client-side data deduplication. If you try to use Backup-Archive client compression without data deduplication, you receive a warning and the backup proceeds without compression.

- Question 16: What are the options for using encryption with Data Protection for VMware?

Answer: Encryption encompasses the data path (in-flight) and data storage (at-rest). In the Data Protection for VMware environment, data is transferred from the VMware storage to the Tivoli Storage Manager vStorage server (this is commonly referred to as *the transport*), then from the Tivoli Storage Manager vStorage Server to the Tivoli Storage Manager Server where the data is stored on disk or tape.

For the transport between the VMware storage and the vStorage server, the network block device (NBD) can be used with SSL to protect the data in-flight. For more information, see the Tivoli Storage Manager Backup-Archive client option VMVSTORTTRANSPORT to set the transport to nbdssl.

For data that is sent between the Tivoli Storage Manager vStorage server to the Tivoli Storage Manager Server, SSL can be used to protect the data in-flight. For more information about configuring SSL communication between the Tivoli Storage Manager agents and the Tivoli Storage Manager Server, see the Tivoli Storage Manager product documentation.

Data at rest in the Tivoli Storage Manager Server storage repository can be protected with device encryption (for example, tape encryption).

Backup-Archive client encryption is not supported with Data Protection for VMware.

- Question 17: Does Data Protection for VMware support a full-VM backup and restore of Windows 2000?

Yes. Full-VM backup and recovery are independent of the virtual machine operating system, so any operating system configuration is supported. For more information about other types of recovery operations, such as, near-instant volume restore and individual file recovery, see the Tivoli Storage Manager Data Protection for VMware software requirements for supported operating systems and file systems.

- Question 18: How do I set up scheduled virtual machine backups?

Answer: The steps for setting up the Tivoli Storage Manager Backup-Archive client to perform scheduled virtual machine backups are described in the white paper *Recommendations for Scheduling with Data Protection for VMware 6.4*.

- Question 19: How do I set up backups that use SAN transport or LAN-free backup?

The steps for setting up the Tivoli Storage Manager Backup-Archive client to perform virtual machine backups that use the SAN transport or LAN-free are described in the white paper *Recommendations for Using LAN-free with Data Protection for VMware*.

- Question 20: Are virtual machine templates supported?

Yes. Beginning with Tivoli Storage Manager for Virtual Environments 6.4, virtual machine template backup and restore are now supported. A new VMENABLETEMPLATEBACKUPS option controls whether templates are included in backups.



VMware for the storage administrators

This appendix provides an overview of a server virtualization and describes the components of a VMware solution. It is intended to provide the minimum required background knowledge about server virtualization to help you with the implementation of Data Protection for VMware.

This appendix includes the following topics:

- ▶ Server virtualization at a glance
- ▶ Introduction to VMware vSphere
- ▶ VMware terminology

Server virtualization at a glance

An ESX Server virtualizes the resources of the physical system for the virtual machines to use. Figure A-1 shows how multiple virtual machines share physical devices. It shows two virtual machines, each configured with the following components:

- ▶ One CPU
- ▶ An allocation of memory and a network adapter (NIC)
- ▶ Two virtual disks (with one virtual machine that is directly attached to physical disk; that is, physical raw device mapping)

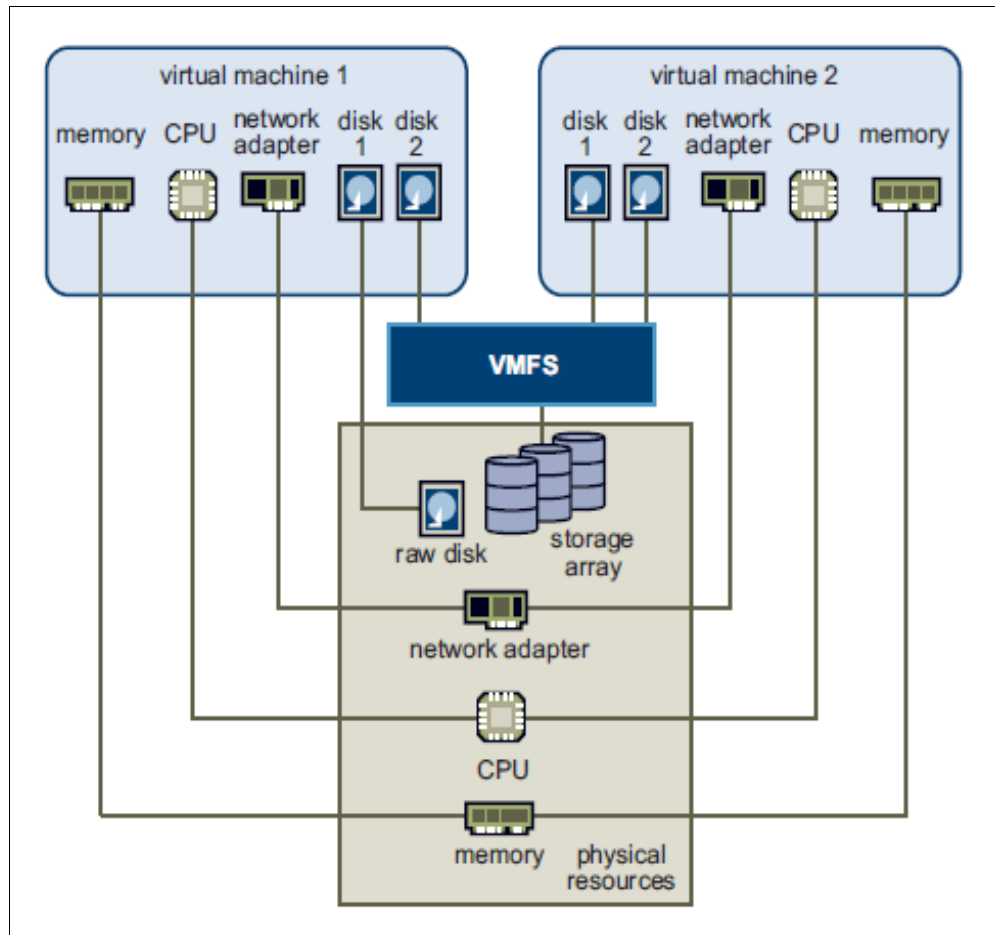


Figure A-1 What is virtualization

The virtual machines each use one of the CPUs on the server and access non-contiguous pages of memory, with part of the memory of one virtual machine that is swapped to disk (this is not shown in Figure A-1). The two virtual network adapters are connected to two physical network adapters.

The disks are mapped by using the following configuration:

- ▶ Disk 1 of virtual machine 1 is mapped directly to a raw disk. This configuration can be advantageous under certain circumstances.
- ▶ Disk 2 of virtual machine 1 and both disks of virtual machine 2 are on the virtual machine file system (VMFS), which is on a storage area network (SAN) storage array. VMFS ensures that appropriate locking and security is in place always.

Introduction to VMware vSphere

VMware vSphere is a virtualization platform that can transform a traditional data center and industry-standard hardware into a shared mainframe-like environment. Hardware resources can be pooled to run varying workloads and applications with different service-level needs and performance requirements. VMware vSphere is the enabling technology to build a private or public cloud infrastructure.

The components of VMware vSphere fall into the following categories: Infrastructure services, application services, and the VMware vCenter Server. Figure A-2 shows the VMware vSphere platform.

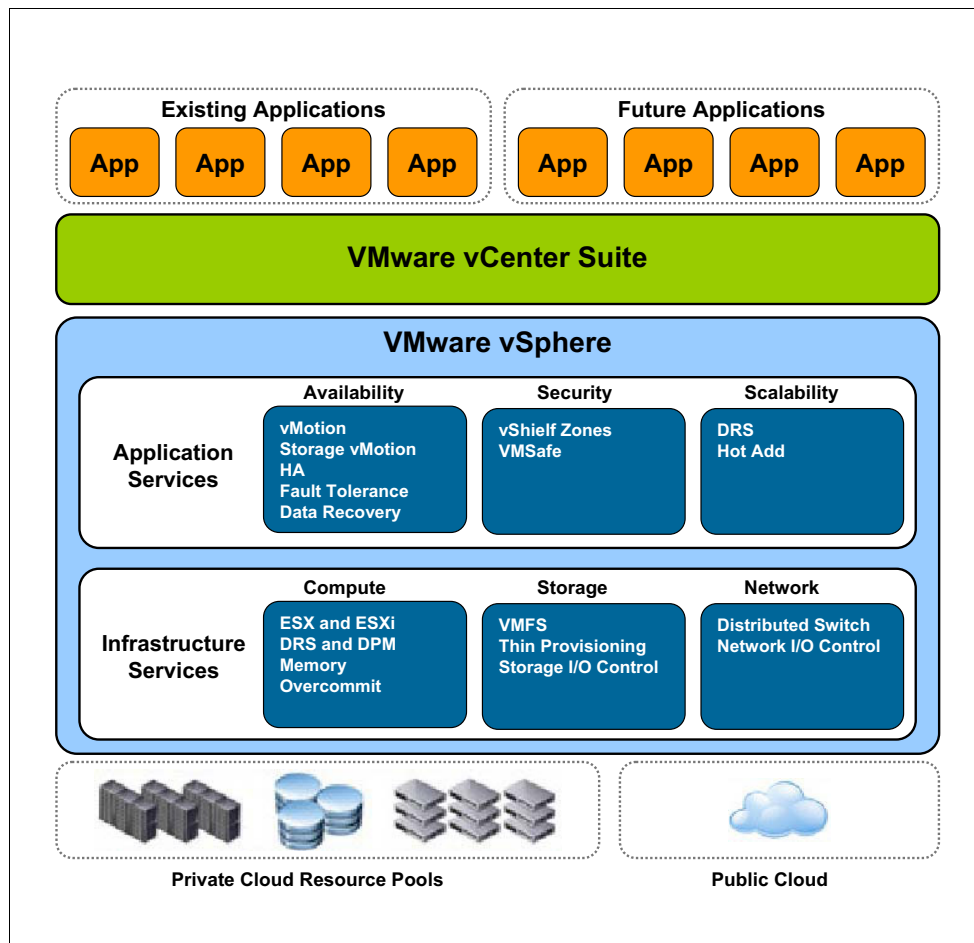


Figure A-2 VMware vSphere platform

Infrastructure services

Infrastructure services virtualizes the server hardware, storage, and network resources. The services within the infrastructure services category are the foundation of the VMware vSphere platform.

Application services

The components that are categorized as application services address availability, security, and scalability concerns for all applications that are running on the vSphere platform, regardless of complexity of the application.

VMware vCenter Server

VMware vCenter Server, formerly known as VMware VirtualCenter, provides the foundation for management of the vSphere platform. VMware vCenter Server provides centralized management of configurations and aggregated performance statistics for clusters, hosts, virtual machines, storage, and guest operating systems. VMware vCenter Server scales to provide management of large enterprises and grants administrators the ability to manage more than 1,000 hosts and up to 10,000 virtual machines from a single console.

VMware vCenter Server is also an extensible management platform. By using the open plug-in architecture, VMware and its partners can directly integrate with vCenter Server, such as, IBM and the Data Protection for VMware vCenter plug-in user interface. This ability extends the capabilities of the vCenter platform and adds functionality.

Figure A-3 shows the main pillars of functionality that are provided by VMware vCenter Server.

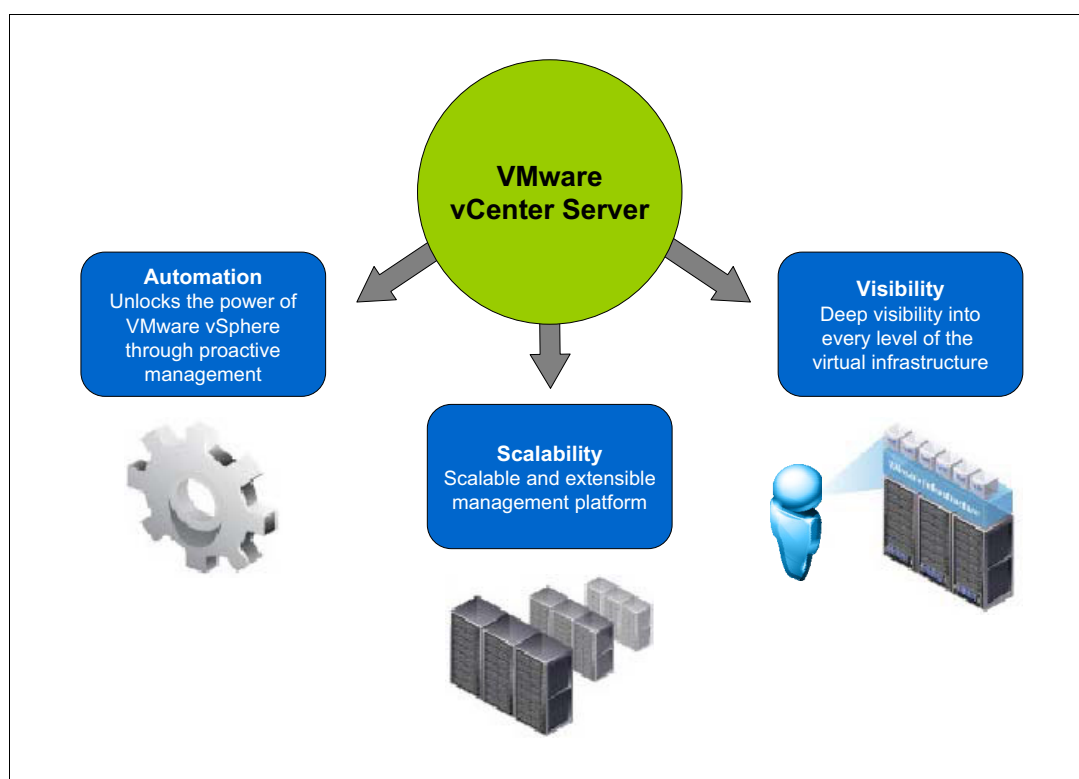


Figure A-3 Pillars of VMware vCenter Server

VMware terminology

The following terminology is commonly used when VMware or its components are described:

- **Changed Block Tracking**

Provides the foundation for incremental or differential (Tivoli Storage Manager implementation uses incremental) backup of virtual disks and allows only active portions of a virtual disk (that is, content aware) to be returned. Changed Block Tracking does not work in the following cases:

- When the virtual hardware version is 6 or earlier.
- The virtual disk is a physical compatibility RDM.
- The virtual disk is attached to a shared virtual SCSI bus.
- In-guest, which refers to software that is installed within a VM guest machine.
- Off-host, which refers to physical machine that is not part of virtualized environment (that is, not on the ESX or ESXi host).

- **Datacenter**

A datacenter is the primary container of inventory objects, such as, hosts and virtual machines. From the datacenter, you can add and organize inventory objects. Typically, you add hosts, folders, and clusters to a datacenter. The vCenter server can contain multiple datacenters. For example, datacenters can be used to represent organization units or map group applications to development, testing and production, and so on. Inventory objects can interact within datacenters, but interaction across datacenters is limited. For example, you can move a virtual machine with vMotion technology across hosts within a datacenter but not to a host in another datacenter.

The recommended best practice is to have a Tivoli Storage Manager target node map to a VMware datacenter. During a vStorage based backup, each VM in the datacenter is represented as a separate file space in the Tivoli Storage Manager target node.

- **Datastore**

A datastore is a logical container that holds virtual machine files and other files that are necessary for virtual machine operations. Datastores can exist on different types of physical storage, including local storage, iSCSI, Fibre Channel SAN, or NFS. The datastore can be VMFS-based or NFS-based.

- **ESX**

Service Console is a standard Linux environment through which a user has privileged access to the VMware ESX kernel. By making use of this Linux based privileged access, you can manage your environment by installing agents and drivers and running scripts and other Linux environment code.

- **ESX Cluster**

A cluster acts and can be managed as a single entity. It represents the aggregate computing and memory resources of a group of physical x86 servers that are sharing network and storage arrays. For example, if the group contains eight servers with four dual-core CPUs each running at 4 GHz and 32 GB of memory, the cluster has an aggregate 256 GHz of computing power and 256 GB of memory available for running virtual machines. An ESX cluster can be used for High Availability and load balancing.

► ESXi

VMware ESXi is designed to make the server a computing appliance. Accordingly, VMware ESXi behaves more like firmware than traditional software. To provide hardware-like security and reliability, VMware ESXi does not support a privileged access environment, such as, the Service Console for management of VMware ESXi. To enable interaction with agents, VMware provisioned CIM Providers through which monitoring and management tasks (which are traditionally done through Service Console agents) can be performed. VMware provided remote scripting Environments (such as, vCLI and PowerCLI) to allow the remote running of scripts.

► Folder

A folder is a container that is used to group objects and organize them into hierarchies. Folders provide a natural structure on which to apply permissions.

► Host

A VMware host (also referred to as *just a host*) refers to the computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

► Snapshot

A VMware snapshot is a copy of the state and data of a virtual machine at a specific point. The Backup-Archive client starts a VMware snapshot of a virtual machine. For more information, see this website:

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1015180

► Storage VMotion

Storage VMotion enables the migration of virtual machines from one datastore to another datastore without service interruption. This allows administrators, for example, to offload virtual machines from one storage array to another to perform maintenance, reconfigure LUNs, resolve out-of-space issues, and upgrade VMFS volumes.

► vCenter Server

The central point for configuring, provisioning, and managing virtualized IT Environments. The vCenter Server unifies resources from individual hosts so that those resources can be shared among virtual machines in the entire datacenter. It accomplishes this by managing the assignment of virtual machines to the hosts and the assignment of resources to the virtual machines within a host that is based on the policies that the system administrator sets. By using vCenter Server, you have access to advanced vSphere features, such as, VMware Distributed Resource Scheduler (DRS), VMware High Availability (HA), and VMware vMotion.

► VMFS

A high-performance cluster file system for ESX or ESXi virtual machines.

► vMotion

Enables the migration of running virtual machines from one physical server to another without service interruption. With vMotion, resources can be dynamically reallocated to virtual machines across physical servers.

- ▶ vSphere Client

A client interface that is installed on a Windows machine that allows users to connect remotely to a vCenter Server or an ESX or ESXi host. VMware offers third-party developers and partners the ability to extend the vSphere Client with custom menu selections and toolbar icons that provide access to custom capabilities, such as, Tivoli Storage Manager vCenter plug-in for FCM and Data Protection for VMware.

- ▶ vStorage APIs for Data Protection (VADP)

The next generation of VMware's data protection framework that was introduced in vSphere 4.0. VADP enables backup products to perform centralized, efficient, off-host LAN-free backup of vSphere virtual machines. VADP uses the snapshot capabilities of VMware vStorage VMFS to enable backup without requiring downtime for virtual machines.

Related publications

The publications that are listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

The following IBM Redbooks publication provides more information about the topic in this document. Note that this publication might be available in softcopy only:

- ▶ *Tivoli Storage Manager as a Data Protection Solution*, SG24-8134

You can search for, view, download or order this document and other Redbooks, Redpapers, Web Docs, draft, and more materials, at this website:

<http://www.ibm.com/redbooks>

Other publications

The following publications are also relevant as further information sources:

- ▶ *IBM Tivoli Storage Manager for Virtual Environments Data Protection for VMware Installation and User Guide*, SC27-2898
- ▶ *IBM Tivoli Storage Manager for UNIX and Linux Backup-Archive Clients: Installation and User's Guide*, SC23-9791
- ▶ *IBM Tivoli Storage Manager for Windows Backup-Archive Clients: Installation and User's Guide*, SC23-9791

Online resources

The following websites are also relevant as further information sources:

- ▶ IBM Tivoli Storage Manager publications:
<http://publib.boulder.ibm.com/infocenter/tsminfo/v6r4/index.jsp>
- ▶ Preserving VMware configuration attribute information:
http://pic.dhe.ibm.com/infocenter/tsminfo/v6r4/index.jsp?topic=%2Fcom.ibm.itsm.ve.doc%2Fr_ve_configattrib.html
- ▶ Data Protection for VMware product requirements:
<http://www-01.ibm.com/support/docview.wss?uid=swg21611903>

Help from IBM

IBM Support and downloads:

<http://www.ibm.com/support>

IBM Global Services:

<http://www.ibm.com/services>



Tivoli Storage Manager for Virtual Environments - Data Protection for VMware Deployment Guide

Describes Data Protection for VMware 6.4 new features

Provides detailed planning, installation, and operational procedures

Includes optimization and troubleshooting information

This IBM Redpaper publication helps you to install, tailor, configure, and use Tivoli Storage Manager for Virtual Environments - Data Protection for VMware. The features of Tivoli Storage Manager for Virtual Environments - Data Protection for VMware are described. Scenarios are provided for implementation of Tivoli Storage Manager Virtual Environment to protect virtual machines in several environments.

This publication includes answers to common implementation errors and questions you might have that are related to the implementation of Data Protection for VMware.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks