

Protecting the VMware Environment with IBM Spectrum Protect

Mikael Lindstrom

Julien Sauvanet

Pol Vander Eyken

Sean Sperry

Nathan Best

Rennad Murugan



Storage



Redpaper



International Technical Support Organization

**Protecting the VMware Environment with IBM
Spectrum Protect**

December 2017

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

First Edition (December 2017)

This edition applies to Version 8, Release 1.2, of IBM Spectrum Protect for Virtual Environments and Version 4, Release 1.6 of IBM Spectrum Protect Snapshot for VMware family of products.

© Copyright International Business Machines Corporation 2017. 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	xi
Comments welcome	xi
Stay connected to IBM Redbooks	xii
Chapter 1. Architecture corner	1
1.1 System context	2
1.2 Roles and responsibilities	4
1.3 Solution guidance	5
1.4 Requirements	5
1.4.1 Requirements gathering	6
1.5 Architectural decisions	7
1.6 Data Protection for VMware features	10
1.6.1 The features of IBM Spectrum Protect for Virtual Environments	10
1.6.2 Virtual or physical vStorage Backup Server	11
1.6.3 Protecting in-guest applications	12
1.6.4 Protecting in-guest applications when there is no Data Protection solution for your application	12
1.7 Using IBM Spectrum Protect Snapshot for VMware	13
1.7.1 What features IBM Spectrum Protect Snapshot provides	13
1.7.2 IBM Spectrum Protect Snapshot use cases	13
1.7.3 Backup technology selection	14
1.7.4 Benefits of using IBM Spectrum Protect Snapshot	14
1.8 Design consideration scenarios	14
1.8.1 Use case 1: Small environment	14
1.8.2 Scenario 2: Large environment	16
1.8.3 Scenario 3: Shared environment	17
Chapter 2. Product introduction	19
2.1 IBM Spectrum Protect solutions that protect VMware vSphere environments	20
2.1.1 IBM Spectrum Protect backup-archive client within VMware guest	20
2.1.2 IBM Spectrum Protect backup-archive client off-host backup option	21
2.1.3 IBM Spectrum Protect for Virtual Environments	22
2.1.4 IBM Spectrum Protect Snapshot for VMware option	23
2.1.5 IBM Spectrum Protect Snapshot For Windows/UNIX	24
2.2 Data Protection for VMware components	24
2.2.1 Component overview	24
2.3 New enhancements	28
2.4 Hardware and software requirements	28
Chapter 3. Installation roadmap	29
3.1 Collecting and consolidating data protection policies	30
3.2 Deployment planning	30
3.2.1 VMware infrastructure	30
3.2.2 Virtual machines	32

3.2.3 vCenter server credentials considerations	32
3.2.4 Simplified file-level recovery model.	33
3.2.5 IBM Spectrum Protect administrator ID authority levels	34
3.3 Protecting applications in a virtual environment	35
3.3.1 SQL data protection	36
3.3.2 Exchange data protection	37
3.3.3 Active Directory Data Protection.	38
3.3.4 Unstructured Data Protection	39
3.4 Communication ports between VMware and IBM Spectrum Protect components	39
3.5 Enabling the backup strategy	40
3.5.1 Incremental forever backup strategy.	41
3.6 vStorage Backup Server	41
3.6.1 Datamover parallelism capabilities	41
3.6.2 Data transfer and data transport methods	42
3.6.3 vStorage Backup Server: Virtual versus physical	43
3.6.4 Physical vStorage Backup Server LUN access considerations	45
3.6.5 Virtual vStorage Backup Server HotAdd considerations.	46
3.6.6 vStorage Backup Server sizing.	46
3.6.7 When to use multiple datamover agents.	48
3.7 Storage location versus recovery features	49
3.8 Determining the location to start backup or restore	50
3.9 Design points	50
3.9.1 How to handle CTL files (FULL-VM backup control files)	50
3.9.2 VM full-vm backup on physical tape or virtual tape.	51
3.10 VMware snapshots considerations	51
3.10.1 Snapshots limitation	51
3.10.2 VMDK file size and snapshot overhead	51
3.11 Data Protection for VMware considerations	52
3.11.1 IBM Spectrum Protect Known Issues and Limitations	52
3.11.2 Multiple vCenter server support	52
3.12 Determine the naming convention	54
3.13 Data Protection for VMware in a shared environment	54
3.13.1 Backup in a shared environment	54
3.13.2 Determining what Data Protection for VMware nodes are needed.	55
Chapter 4. Installation and configuration	59
4.1 Overview of component installation and configuration	60
4.1.1 IBM Spectrum Protect server configuration	60
Chapter 5. Virtual machine backup	63
5.1 Configuring the Datamover	64
5.2 VM backup using vCenter plug-in	64
5.3 VM backup by using Datamover client	70
5.4 VM backup by using the Datamover Client command line	71
5.5 VM backup by using Data Protection for VMware CLI	77
5.6 Protection for in-guest applications	79
5.6.1 Enabling application protection for a VM.	79
5.7 VM backup optimization	81
Chapter 6. Backup scheduling	83
6.1 Backup scheduling	84
6.1.1 Backup schedule and backup strategy	84
6.1.2 Backup scheduling and VMware tags.	84
6.1.3 Fine-tuning the IBM Spectrum Protect server.	85

6.1.4	Fine-tuning the datamover	86
6.1.5	Defining a schedule to back up VMs	86
6.1.6	Updating or deleting a VM backup schedule	88
Chapter 7. Virtual environment recovery	89
7.1	Overview of recovery procedures	90
7.1.1	Recovery scenario selection use cases	90
7.1.2	Performance considerations	91
7.1.3	Full VM restoration	93
7.1.4	Virtual machine instant access	99
7.1.5	Virtual machine instant recovery	102
7.1.6	File level restoration	104
7.1.7	Microsoft SQL Server object recovery	105
7.2	Overview of recovery procedures using the IBM Spectrum Protect Snapshot for VMware GUI	113
7.2.1	Virtual machine recovery	113
7.2.2	Virtual machine virtual disk recovery	114
7.2.3	Virtual machine individual file recovery	116
7.2.4	Complete datastore recovery	118
Chapter 8. Reporting	121
8.1	Native reports	122
8.1.1	Events	123
8.1.2	Recent tasks	123
8.1.3	Backup Status	123
8.1.4	Application Protection page	125
8.2	SQL reports	126
8.2.1	Successful backup in a specified time frame	126
8.2.2	Unsuccessful backup in a specified time frame	126
8.2.3	Not backed up in a specified time frame	126
8.2.4	Additional reporting information	127
8.3	VMware vSphere Web Client	128
Chapter 9. Disaster recovery	129
9.1	Disaster recovery key point indicators	130
9.2	Disaster recovery requirements	130
9.2.1	Assess the recovery needs	130
9.2.2	Disaster recovery level definitions	130
9.3	Disaster recovery use cases	132
9.3.1	Business requirements	132
9.3.2	Active data including versioning	132
Chapter 10. Problem determination and FAQs	135
10.1	Common errors	136
10.1.1	Common error messages	136
10.1.2	Restoration by using SAN transport method	136
10.1.3	Plug-in management	136
10.2	Analyzing errors	137
10.2.1	Web resources	137
10.3	How to open a call with IBM Support	138
10.3.1	Contacting IBM support: Opening a service request	138
10.4	Frequently asked questions	139
Related publications	141

IBM Redbooks	141
Other publications	141
Online resources	141
Help from IBM	142

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

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 jurisdictions 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 provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AIX®	IBM Spectrum Protect™	Redbooks®
DB2®	IBM Spectrum Scale™	Redbooks (logo)  ®
developerWorks®	Lotus®	Storwize®
FlashCopy®	Passport Advantage®	Tivoli®
Global Technology Services®	PowerVM®	WebSphere®
IBM®	ProtecTIER®	XIV®
IBM Spectrum™	Rational®	

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

In memory of Daniel Wolfe.

While backup is a topic of much discussion, development, and strategy, the name of the game is rapid recovery. Given the explosive growth of data in our Client environments, there is a need to provide solutions to our Clients that meet their *recovery time objective* and *recovery point objective* needs.

Traditional backups of files, databases, and similar objects sent across networks (LAN or SAN) to backup servers provide a degree of recoverability, but the speed of backup and recovery is constrained by resource capacity (server, network, storage, and so on). This results in longer backup and recovery times. Data growth is steadily making the problem worse. A new approach to rapid recovery is required to meet requirements of single file recoveries and recoveries of large data sets.

The new approach is snapshot technology. The ability to make point-in-time snapshots with limited impact to the application while rapidly recovering large data sets by reverting to a snapshot greatly reduces the recovery time for these data sets.

This IBM® Redbooks® publication has been written to identify the IBM software that enhances the ability to deliver rapid recovery and gives directions and procedures to design, install, configure, and use IBM Spectrum™ Protect for Virtual Environments and IBM Spectrum Protect™ Snapshot for VMware. While the two products work hand in hand to provide a comprehensive protection to VMware environments, the two products are separate and are installed and configured separately.

Authors

This paper was produced by a team of specialists from around the world.

Mikael Lindstrom is a Senior Technical Staff Member in Resiliency, an IBM Certified Senior Architect and an IBM Inventor within the IBM Global Technology Services® Technology, Innovation and Automation organization. Mikael has 16 years of IT experience in different environments of which 12 years with IBM Spectrum Protect products and Storage. He is currently focused on helping customers solving their challenges around resiliency, and developing global technology and optimization strategies which is fit for the future with a deep involvement in building future-proof Software Defined Resiliency Hybrid Cloud infrastructure. He has co-authored several Redbooks publications and white papers related to IBM Spectrum Protect products and Software Defined Storage.

Julien Sauvanet is an IBM Certified Expert IT Specialist, working in the French Infrastructure Services organization. He is also involved in architecture and deployments world wide optimizing for implementing latest technology, strategy, and architecture for Global Technology Services with a focus on IBM Spectrum Protect (formerly IBM Tivoli® Storage Manager) products. Julien has more than 13 years of experience with IBM Spectrum Protect and other related storage products. Julien is also a subject matter expert in system and storage virtualization (such as IBM PowerVM®, VMware, IBM Storwize® and IBM ProtecTIER® products). Julien has co-authored two other IBM Redbooks publications and also published several IBM Tivoli Storage Manager white papers at IBM developerWorks®.

Pol Vander Eyken is an IT Specialist, working in the Technology Support Services back-end department in the IBM Global Technology Services division, Belgium providing support to customers worldwide. He has 24 years of IT experience with IBM of which 13 years were with IBM Spectrum Protect and other related storage products. His areas of expertise include the IBM Spectrum Protect product family, disk and tape subsystems, virtualization, and in-depth knowledge of problem determination. He is specialized in IBM Spectrum Protect interactions with Virtual environments (VMware, Hyper-V) and IBM Spectrum Protect for Workstations.

Sean Sperry has over 30 years of experience in IT, IT Management, and Consulting. He has worked in numerous technical environments in such roles as Educator, UNIX/Windows System Administrator, Database Administrator, Consultant, and Architect. In his current position, Sean works for IBM performing technical enablement for IBM Systems Storage products including IBM Spectrum Protect. He has published several white papers on technical and process aspects of systems management, produces commercial education, speaks world-wide at conferences and events, and works through social media to promote and educate customers and sellers about IBM products.

Nathan Best is an IT Specialist with a degree in Computer Science from Western Carolina University and 11 years of experience in the storage and backup and recovery field. Nathan has spent 9 of those 11 years designing and delivering resiliency services to IBM's Global Technology Services customers.

Rennad Murugan is a Managing Consultant with IBM Systems Storage Lab Services organization. He has spent more than 12 years working with IBM Spectrum Protect products (previously known as Tivoli Storage Manager) both in a support role and as a client-facing Managing Consultant. His current role covers customers in all industries across North America and Canada. He is an IBM Certification Exam Developer for IBM Spectrum Protect and has co-authored two other publications on this subject. He enjoys working and interacting with customers in the field because this provides him the ability to relay feedback in real-time to the development team to help improve the product in an agile manner.

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

Jason Basler
Senior Technical Staff Member, Test Architect IBM Spectrum Protect, IBM Systems

Chris Zaremba
Senior Technical Staff Member, IBM Spectrum Protect Architect, IBM Systems

Art Roy
IBM Storage Software Advanced Technology, IBM Systems

Jim Smith
Senior Technical Staff Member, IBM Spectrum Protect Architect, IBM Systems

Dan Thompson
Spectrum Storage Technical Specialist, IBM Systems

Bert Dufrasne
Certified IT Specialist and Project Manager, IBM Technical Support Organization

Kurt Rybczyk
Retired from IBM

Paula Rae Cross
Retired from IBM

Holly King
User Experience Designer, IBM Hybrid Cloud

Liudyte Baker
Information Development, IBM Systems

Diana Moose
Information Development, IBM Systems

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:
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:
ibm.com/redbooks
- ▶ Send your comments in an email:
redbooks@us.ibm.com
- ▶ Mail your comments:
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>



Architecture corner

Before we describe the solution, you should be aware of the effect the products might have on your organization. It hooks up to multiple technical components; therefore, it can affect related competencies that might be distributed among several teams.

This chapter gives a broad understanding of the architecture and how to design and implement 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, other IBM Spectrum Protect products and its place within IT teams and environment. We briefly describe requirements in 1.4, “Requirements” on page 5.

We also give suggestions about how data protection operations can be distributed across the various teams.

This chapter includes the following topics:

- ▶ System context
- ▶ Roles and responsibilities
- ▶ Solution guidance
- ▶ Requirements
- ▶ Architectural decisions
- ▶ Data Protection for VMware features
- ▶ Design consideration scenarios

1.1 System context

Figure 1-1 illustrates the system context of a typical IBM Spectrum Protect for Virtual Environments - Data Protection for VMware and IBM Spectrum Protect Snapshot for VMware solution. This solution is used to record the interactions with existing external systems in the IT infrastructure, and with human actors/users.

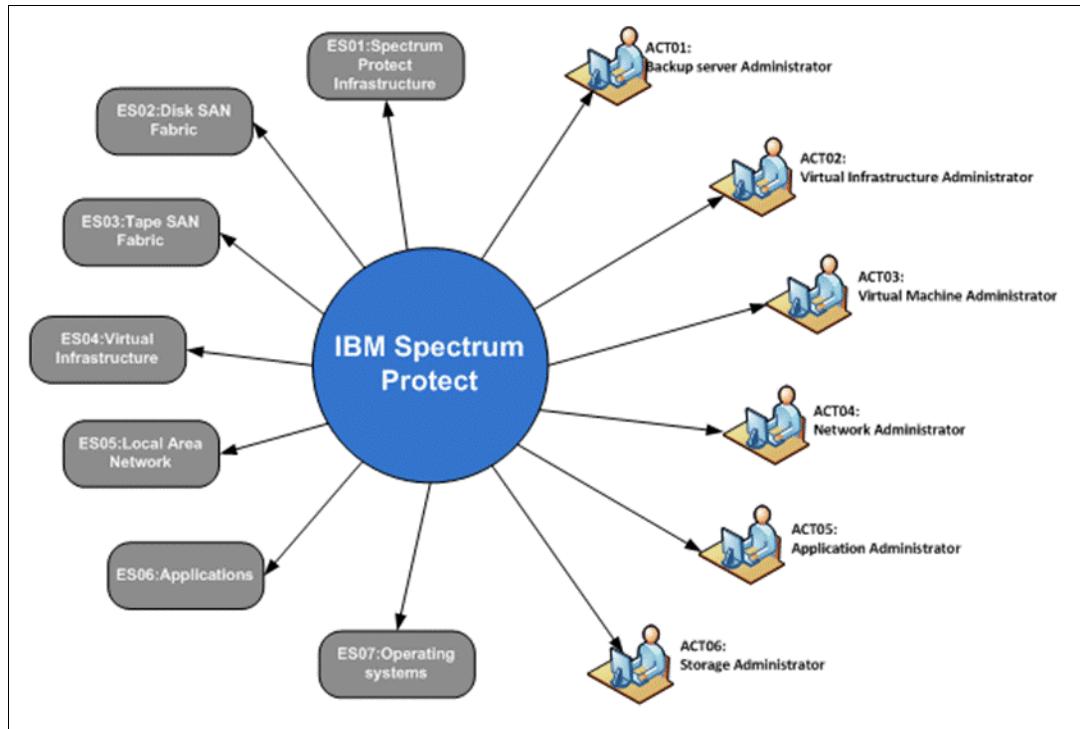


Figure 1-1 IBM Spectrum Protect Data Protection for Virtual Environments: System context

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

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

ID	Name	Description
ACT01	IBM Spectrum Protect Server Administrator	The IBM Spectrum Protect Server administrator manages the IBM Spectrum Protect infrastructure (ES01). ACT01 provides essential services, such as, proxy node configuration, storage pool definition, and management and schedule and data retention definition.
ACT02	Virtual Infrastructure Administrator	ACT02 is the main customer of IBM Spectrum Protect. IBM Spectrum Protect is used as the main backup solution for all the guests that are hosted in the virtual infrastructure (ES04). The administrator also provides access to vCenter and the underlying virtual infrastructure components to the IBM Spectrum Protect solution.
ACT03	Virtual Machine Administrator	ACT03 is one of the IBM Spectrum Protect users. This actor relies 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 IBM Spectrum Protect 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, IBM Spectrum Protect 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 providing storage for the IBM Spectrum Protect solution. The administrator ensures that the IBM Spectrum Protect 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	IBM Spectrum Protect Infrastructure	The IBM Spectrum Protect infrastructure is a requirement for the IBM Spectrum Protect solution to function. It contains several components, such as, the IBM Spectrum Protect server, storage pools, IBM Spectrum Protect nodes definition, and data retention policy.
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 IBM Spectrum Protect solution (as in the case of a physical proxy doing LAN-free backups) or indirectly (through the IBM Spectrum Protect server when storage pool migration occurs).

ID	Name	Description
ES04	Virtual Infrastructure	This external service is the main interface for the IBM Spectrum Protect solution that enables data to be restored. It includes components like hypervisor, guests, and logical datastores where guest data is hosted. Guest configuration information is part of the data that is backed up by the IBM Spectrum Protect Data Protection for VMware solution. It is through this external service that users of the IBM Spectrum Protect solution most likely interact (via the new integrated vCenter UI or 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 IBM Spectrum Protect 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 IBM Spectrum Protect solution. In some cases, these might even be left out of the IBM Spectrum Protect solution because they cannot be consistently backed up and require another backup solution (such as a DP agent).
ES07	Operating Systems	Operating Systems are part of the data that is backed up by the IBM Spectrum Protect solution. The main benefit of the solution is to permit fewer recovery steps after an operating system failure.
ES08	IBM Spectrum Protect Manager Snapshot	This external service might not always be present. However, when it is, it can interact with the IBM Spectrum Protect solution to provide quick backup and restore of an entire virtual infrastructure by leveraging hardware storage snapshot solutions provided by the back end storage.
ES09	Backup Reporting	This external service is used to view the status of all of the backup and restore tasks. IBM Spectrum Protect must interface with the reporting system directly or indirectly to report on job status.

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

1.2 Roles and responsibilities

This section presents a summary of roles and responsibilities across the teams. Depending on the existing separations of duties, roles and responsibilities between the teams can vary.

Figure 1-2 shows an overview of the task distribution when IBM Spectrum Protect Data Protection for VMware is implemented and used.

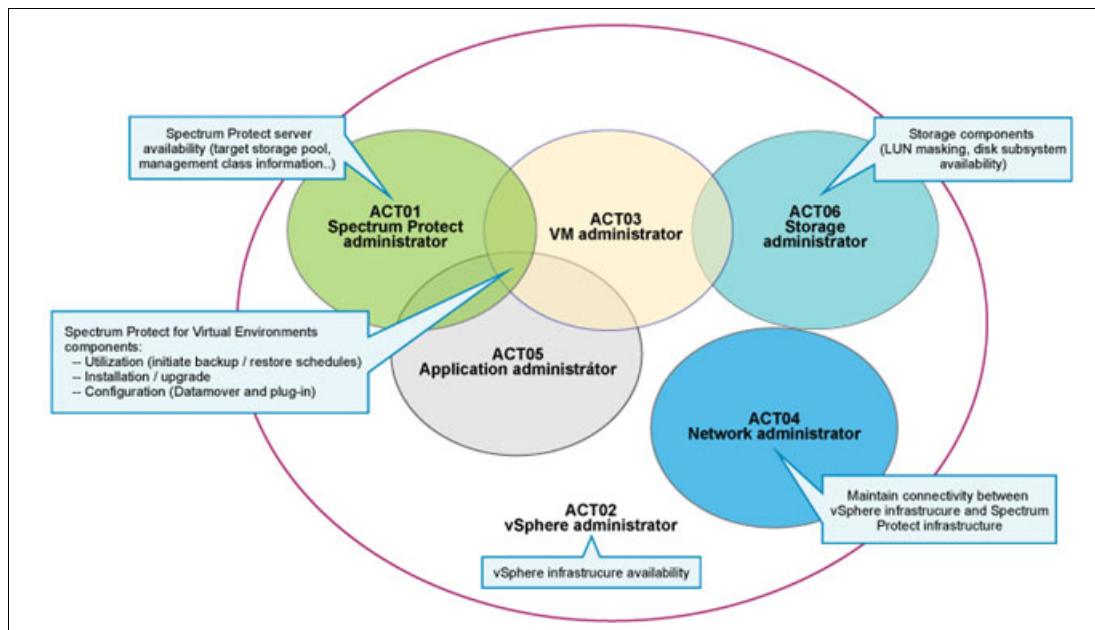


Figure 1-2 Tasks distribution across IT competencies

In Figure 1-2, bubble intersections mean that an operation can be done by IBM Spectrum Protect Administrators, Virtual Machine Administrators, Or Application Administrators, depending on your IT organization. This requires good team communication. Each person that is responsible for a task should inform or request assistance of other peer users.

1.3 Solution guidance

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

This information is not intended to replace the analysis of your environment and is not a complete set of decisions to make, but it will help you to sketch a design of what your solution might look like, what must be considered to build a data protection solution on hypervisor that meets customer requirements, and the typical customer requirements you need to consider.

Remember: Data Protection for VMware is tight to VMware infrastructure components and interrelates with network, storage, and security components, all managed by VMware.

1.4 Requirements

To build a solution we need to understand what the system has to do, which functions the solution must provide. The non-functional requirements for a business system are usually the capacity, the performance, and the service level agreements (SLAs). These can have a profound effect on cost and how the business system is accepted by both the users and the people responsible for supporting that system, while not directly affecting the functionality of the system as seen by the users.

The two most important requirements of data protection are the *recovery time objectives* (RTO) and *recovery point objectives* (RPO). These two concepts define backup frequency, retention policy, and 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 after a service disruption. RPO refers to the available recovery points in time to restore from. In addition to RTO and RPO values, you must decide about the retention policy, that is how long to keep the data on the IBM Spectrum Protect Server storage.

Remember multiple retention policies have an impact on Data Protection for VMware implementation. This can lead to the creation of multiple sets of configurations.

1.4.1 Requirements gathering

Gather requirements using the following steps:

1. Collect information about the Virtual Environment:
 - VMware infrastructure in general (vCenter, ESXi, Datastores, guests, and so on)
 - VMware vSphere version build levels
 - Security aspects (Firewalls, who is allowed to access what? VMware vCenter user roles and credentials considerations)
 - VMware tags
 - Storage, network, and SAN capabilities/limits
 - How many vCenter servers must you manage?
2. Collect and consolidate data protection policy requirements:
 - What backup and restore strategy fits best to your environment and requirements (RTO and RPO)?
 - Do you need more than one backup policy?
 - What type of restoration is needed (file-level, full-vm, or both)?
3. List the possible road blocks:
 - Firewalls
 - What is the enforced access security policy?
 - Are there guests that cannot use or support snapshots?
 - If yes, consider using the IBM Spectrum Protect Snapshot for VMware or in-guest IBM Spectrum Protect Client and/or Data Protection agents.
 - What are the alternatives?
 - Are there any applications hosted in VMware guests? For the following apps, there is the Application Protection feature:
 - MS-SQL Data Protection
 - Exchange Data Protection
 - Active Directory Data Protection
4. Backup solution requirements:
 - IBM Spectrum Protect for Virtual Environments - [Data Protection for VMware](#).
 - IBM Spectrum Protect [Snapshot for VMware](#).

- The required communication ports between VMware and IBM Spectrum Protect components:
 - IBM Spectrum Protect for Virtual Environments - Data Protection for [VMware](#).
 - IBM Spectrum Protect [Snapshot for VMware](#).
5. What kind of workload will the data protection solution represent for the operational teams?

1.5 Architectural decisions

One of the most important steps in developing a solution design is that the architectural decisions meets the backup and recovery requirements. Table 1-3 focuses on Virtual Environment data protection solution and highlights key benefits of both IBM Spectrum Protect Snapshot for VMware (hardware snapshot) IBM Spectrum Protect Data Protection for Virtual Environment (Data Protection for VMware) and the combination of the two products.

This table focuses on using vSphere .vmdk files. If you are using VMware virtual volume (VVol), the IBM Spectrum Protect Data Protection for VMware version 8.1 provides the same capabilities as IBM Spectrum Protect Snapshot for VMware.

Table 1-3 Benefits of the IBM Spectrum Protect

	IBM Spectrum Protect Snapshot for VMware	IBM Spectrum Protect Data Protection for VMware	Combination of the two products
Highlights			
<i>Cost</i>	\$	\$\$	\$\$
<i>Protection level</i>	Medium, because the data copy is on the same disk system	Good, because we have multiple data copy stored onto another disk/tape system	Very good, because you combined the advantages of the two products
<i>Disaster recovery</i>	Yes, given integration with storage mirroring functions to allow snapshot backups at a remote site ^a	Yes, thanks to IBM Spectrum Product node replication	Yes
Key benefits			
<i>Leading-edge data reduction</i>	Yes	Yes, leveraging VMware change block tracking (CBT) and IBM Spectrum Protect data deduplication	Yes
<i>Fast efficient disk based backup and restore operations</i>	Yes	No	Yes

	IBM Spectrum Protect Snapshot for VMware	IBM Spectrum Protect Data Protection for VMware	Combination of the two products
<i>Data deduplication feature included at no extra cost</i>	No data deduplication, but data reduction available when using space-efficient flashcopy volumes	Yes	Yes, when the data are stored onto the IBM Spectrum Protect server
<i>Replication processing included at no extra cost</i>	No, replication is done using PPRC and needs to be purchased as a license	Yes using IBM Spectrum Protect Node replication	Yes using IBM Spectrum Protect node replication
<i>Data deduplication at both source and target side</i>	No deduplication	Yes, if the data are stored on Disk or an Appliance doing deduplication (for example, ProtecTIER)	Yes, if the data are stored on Disk or an Appliance doing deduplication (for example, ProtecTIER)
<i>Low cost scalability and optimized for long term retention</i>	No	Yes, when sending data to a tape storage pool	Yes, when sending data to a tape storage pool
Efficiency and cost			
<i>Optimized for high-speed storage area network (SAN) backup operations</i>	N/A, snapshots are created within the storage device, no data movement across the SAN for backup & restore actions	Yes if the data is transferred via a physical vBS to the IBM Spectrum Protect Server on a Tape or VTL	Yes if the data is transferred via a physical vBS to the IBM Spectrum Protect Server on a Tape or VTL
Availability			
<i>Offsite copy capability</i>	Yes, using storage mirroring functions (for example, MM, GM, SRDF) which requires another license on the disk system	Yes, using IBM Spectrum Protect node replication - no extra cost	Yes
<i>Appliance based replication</i>	Yes, (MM, GM, IBM XIV® mirroring, EMC SRDF)	Yes, if IBM Spectrum Protect uses ProtecTIER as backup storage	Yes
<i>Client recovery</i>	Very easy and fast. Attaching flashcopy targets to an auxiliary ESXi host. VM and VMDK level restores still require a data copy from the backup datastore to the primary datastore	Data needs to be restored to VMware datastore. Can take time depending on the amount of data to recover.	Yes

	IBM Spectrum Protect Snapshot for VMware	IBM Spectrum Protect Data Protection for VMware	Combination of the two products
<i>Retention policy flexibility, ability to keep more or less data at recovery site</i>	Yes, mirror integration allows for different snapshot retention policies at remote site and primary site	Yes, even more using dissimilar policy of IBM Spectrum Protect node replication	Yes
Scalability			
<i>Solution scalability</i>	As scalable as the storage disk subsystem is, IBM FlashCopy® and Snapshot operation are limited to storage system capacity.	Ease of scale. Single IBM Spectrum Protect instance can manage up to 6 PB without IBM Spectrum Protect deduplication, up to 1 PB total (100 TB ingest per day) when IBM Spectrum Protect deduplication is enabled	Yes
<i>Global data deduplication across IBM Spectrum Protect servers</i>	No	Yes, when using same Appliance for all IBM Spectrum Protect servers (for example, ProtecTIER)	Yes, when using same Appliance for all IBM Spectrum Protect servers (for example, ProtecTier)

a. DR would require combination of FlashCopy + PPRC to replication the data out of the box, to be recoverable elsewhere

Note: There are performance and feature limitations when using tape with IBM Spectrum Protect Data Protection for VMware.

In addition to Table 1-3 on page 7, some other advantages to consider when using both IBM Spectrum Protect Data Protection for VMware and IBM Spectrum Protect Snapshot for VMware are:

- ▶ VMware tagging support for virtual machines backups
- ▶ Fast access to virtual machine disks (VMDKs) for granular recovery
- ▶ VMDK sub-disk level parallel restore available as of version 8.1
- ▶ Preservation of all virtual machine (VM) attributes
- ▶ Offload all I/O for backup to IBM Spectrum Protect
- ▶ Unified graphical user interface (GUI) showing all backup versions

The followings points that must be considered and reviewed, and included when implementing the data protection solution:

- ▶ How to perform full backup of a VMware based virtual machine
- ▶ How and where to initiate an item level recovery, depending of the recovery type
- ▶ How to handle application data protection within virtual machine (how to protect servers with application data, such as database servers and mail servers)
- ▶ How to handle the data stored in the registry of a Windows Domain Controller
- ▶ Which vStorage Backup Server (vBS) platforms to choose

- ▶ What type of hardware to use for the vBS is virtual machine (physical or a virtual platform)
- ▶ Which transport method must be selected when backup virtual machines
- ▶ Physical vStorage Backup Server LUN access considerations
- ▶ Storage location versus recovery features
- ▶ From which location can I initiate backup or restore
- ▶ Impact of IBM Spectrum Protect Data Protection for VMware backups on the IBM Spectrum Protect Server
- ▶ VMDK file size and snapshot overhead
- ▶ Multiple vCenter Server support
- ▶ Placement of vStorage Backup Server

1.6 Data Protection for VMware features

This section explains when it is appropriate to use IBM Spectrum Protect for Virtual Environments - Data Protection for VMware.

1.6.1 The features of IBM Spectrum Protect for Virtual Environments

Data protection for VMware provides the following benefits:

- ▶ Allows for self-service file-level restore by virtual machine operating system support teams and end users.
- ▶ Easy interaction with IBM Spectrum Protect Snapshot for VMware, if needed.
- ▶ Support for vVols enabling VM backups located on persistent snapshots.
- ▶ Integrated with the IBM Spectrum Protect Server using disk, physical and virtual tape library (VTL) based storage.
- ▶ Embedded backup report.
- ▶ Leverages VMware Tags to easily tailor backup domain, schedules and policies assignments for Backups.
- ▶ Seamless integration with the VMware vCenter Web Client interface using the IBM Spectrum Protect for Virtual Environment - Data Protection Extension.

The File Level Recovery interface is the new way of restoring both Windows and Linux files from an HTTP based interface. It brings a huge enhancement in the file recovery area and unified the procedure for the two operating systems. This is an “End User” interface or “Self Service” that allow any authorized user to access the content of his machine’s backup, the Virtual machine that the user has specified in the first FLR screen when he logged in. Authentication is managed by Active Directory, so we do not have any credential management to perform at vBS level.

Figure 1-3 shows you a typical implementation of File Recovery Interface and all the interactions with the other components such as IBM Spectrum Protect server and client’s virtual machines. It shows how the FLR interface is integrated with the client’s global authentication mechanism (for example, ActiveDirectory).

Note: Backup and Restore are represented on different machines to highlight the flows, but they could be installed on the same machine.

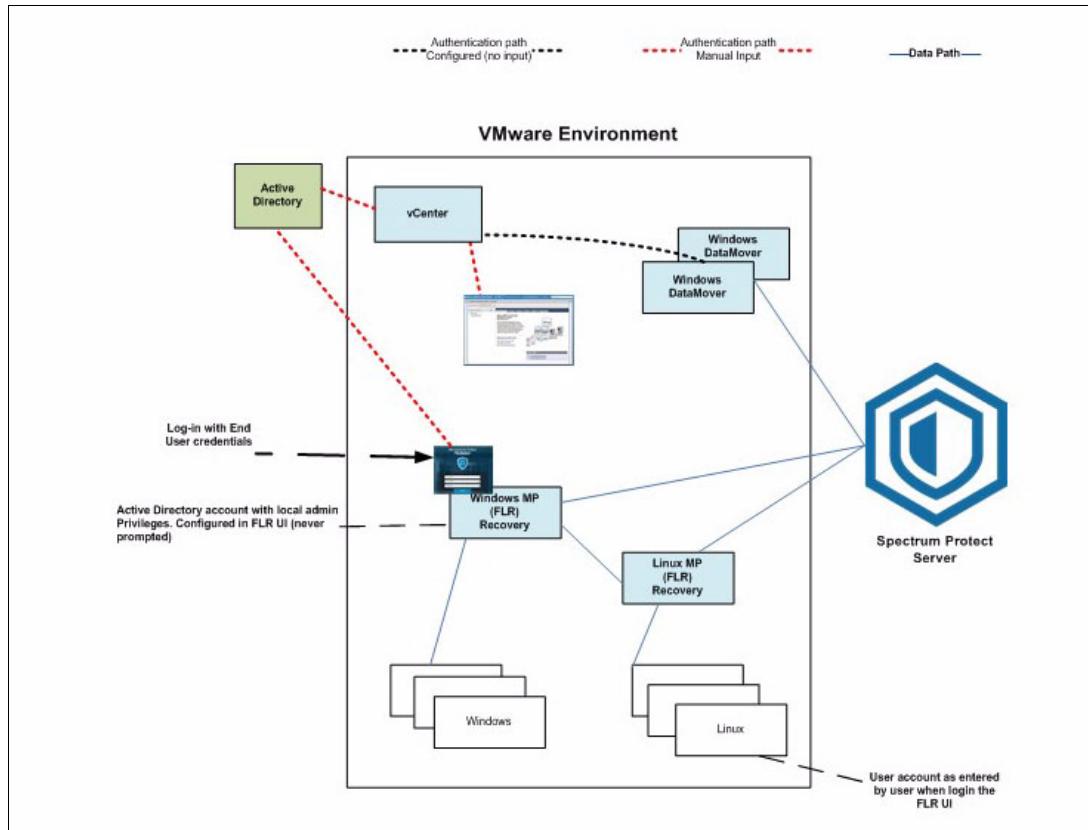


Figure 1-3 File Recovery Interface overview

Although the new File Level recovery interface is much easier than doing old fashion mount operation, it requires slightly more setup at first:

- ▶ To enable file restore capability, the Data Protection for VMware vSphere GUI must be installed on a Windows system.
- ▶ To enable file restore for a Linux virtual machine, in addition to installing Data Protection for VMware on a Windows system, a Linux mount proxy system must also be configured.
- ▶ For windows file recovery, you will need to define a Domain account with local admin privilege so that the FLR can do all of the file copying for you, automatically, unapparently.
- ▶ For Linux file recovery, the target VM where you want to restore the file must have NFS client service up and running.

In a firewall environment, it also means that few additional ports must be opened. See the Figure 3-7 on page 40 Communication ports that are used by Data Protection for VMware where we list all the required ports in a firewall environment.

For more information about the features of Data Protection for VMware, see Chapter 2, “Product introduction” on page 19.

1.6.2 Virtual or physical vStorage Backup Server

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, “Data transfer and data transport methods” on page 42.

1.6.3 Protecting in-guest applications

The use of a Data Protection agent (DP) for application protection is the recommended and supported solution for several applications.

For more information about how to protect your applications, see 3.3, “Protecting applications in a virtual environment” on page 35.

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

IBM Spectrum Protect Data Protection for VMware relies on VMware snapshots, this method can provide the data consistency for Windows (through the Microsoft VSS snapshot operations) when no IBM Data Protection solution exists to support a particular application. Linux VMs are only capable by default of crash-consistent backups, though it is possible to configure [pre-freeze and pre-thaw scripts to supplement consistency](#).

For more information about how to protect your applications, see 3.3, “Protecting applications in a virtual environment” on page 35.

1.7 Using IBM Spectrum Protect Snapshot for VMware

This section discuss when it is appropriate to use IBM Spectrum Protect Snapshot.

1.7.1 What features IBM Spectrum Protect Snapshot provides

IBM Spectrum Protect Snapshot provides the following features:

- ▶ Off-host backup via VMware snapshots from hardware-based snapshots of VMFS and NFS datastores
- ▶ Backup versions retained as persistent hardware snapshots in storage device exploiting native storage copy services, e.g., block-level incremental nature of the hardware snapshots
- ▶ Datastore, vm, VMDK and file-level restore from the hardware-based snapshots
- ▶ IBM Spectrum Protect integration, restores from local, hardware snapshot or IBM Spectrum Protect server

Figure 1-4 shows the integration between VMware and IBM Spectrum Protect Snapshot and DP for VMware components.

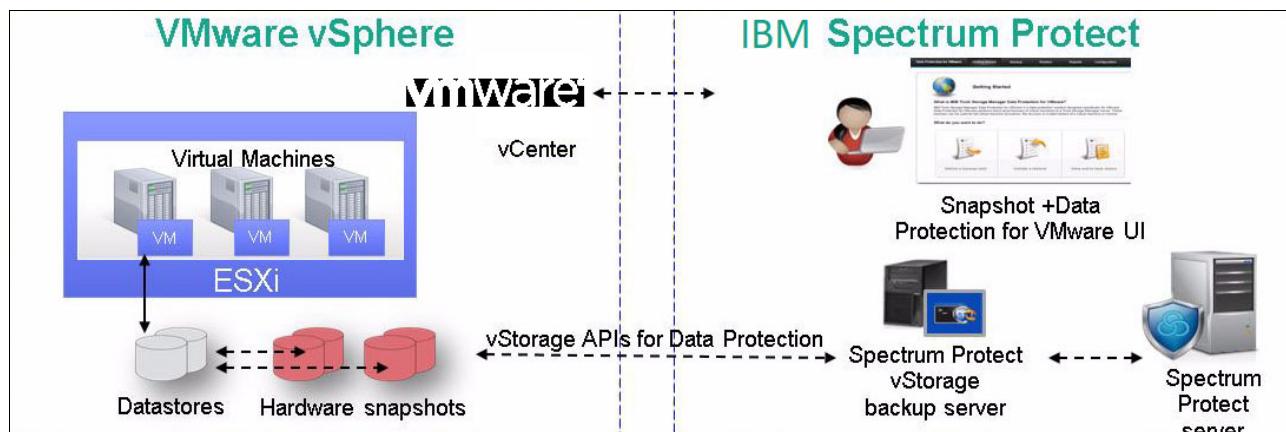


Figure 1-4 VMware and IBM Spectrum Protect Snapshot and DP for VMware components interactions

1.7.2 IBM Spectrum Protect Snapshot use cases

This IBM Redpaper publication describes the following use cases:

- ▶ Recover entire virtual machine or individual disks from hardware snapshot if VM is damaged or deleted. This is basically done by copying the data from the snapshot
- ▶ Instantly restore a datastore and all of the provisioned virtual machines by reverting the hardware snapshot. This is done by reverting the hardware snapshot.
- ▶ Recover files and folders from hardware snapshot by attaching vmdk(s) to virtual machine. this is achieved by attaching the snapshot which make the content accessible.
- ▶ All recovery options available using Data Protection for VMware if backups are off-loaded from hardware snapshots. In this case, all the data are read from IBM Spectrum Protect Server storage pools via IBM Spectrum Protect DP for VMware.

1.7.3 Backup technology selection

Table 1-4 compares backup technologies.

Table 1-4 Selecting a backup technology

	Conventional “Streaming Backup”	Hardware Snapshots
Backup Window	Function of data transfer rate and virtual machine size	Near-instantaneous (with supported devices)
RTO (Recovery Time Objectives)	Function of data transfer rate and virtual machine size	Near-instantaneous (with supported devices)
RPO (Recovery Point Objectives)	Daily (more frequent is possible not practical)	Hourly (more frequent is possible)
Geographic Location requirement (backup data location requirements)	Backup data stored in backup Server Supports off-site copies and replicas	Backup data is off-site when using hardware mirroring. Without using hardware mirroring backup data is co-located in the source
Retention requirements	Cost effective technology for long-term retention (>30 days)	Most appropriate for short term retention

1.7.4 Benefits of using IBM Spectrum Protect Snapshot

Using IBM Spectrum Protect Snapshot for VMware provides the following benefits:

- ▶ Smaller VM Change Block Tracking Snapshots during data backup to IBM Spectrum Protect
- ▶ Faster Hardware based Snapshot of VMware Datastore
- ▶ Faster VM Restore based on hardware snapshot

1.8 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 book.

Keep in mind while reading this chapter, that at any time the components IBM Spectrum Protect Snapshot can be used, as highlighted previously in the book, to keep data on disk array or to reduce the virtual machine backup impact (reduce snapshot time therefore reduce snapshot datastore usage).

1.8.1 Use case 1: Small environment

This section contains a brief explanation of what could be the implementation to protect a virtual machine 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 vBS sizing, refer to sizing section, the design includes the following components:

- ▶ One virtual vStorage Backup Server (Proxy)
- ▶ One IBM Spectrum Protect server
- ▶ Estimated disk storage space required is based on the following policy:
10 TB initial full + 614 GB Daily * Number_Of_Versions to be retained on IBM Spectrum Protect server

Remember, the first full backup of all the virtual machines must be spread over several days. For example, backup 50 machines on the first day, 50 machines on the second day, last 50 machines on the third day, or an additional virtual vBS can be set up temporarily if the network and server resources can accommodate the load. IBM Spectrum Protect deduplication (either client side or server side) can be enabled.

If so, the IBM Spectrum Protect server must meet the minimum hardware requirement and the data must be stored on container based volumes on the IBM Spectrum Protect server side. Also, with deduplication, you have to refine the storage pool space estimation.

IBM Spectrum Protect deduplication (client side or server side) can be enabled. If it is, the IBM Spectrum Protect server must meet the minimum hardware requirement and the data must be stored on Container Pool based volumes on the IBM Spectrum Protect server side.

Also, with deduplication, you must refine the storage pool space estimation. The design is shown in Figure 1-5.

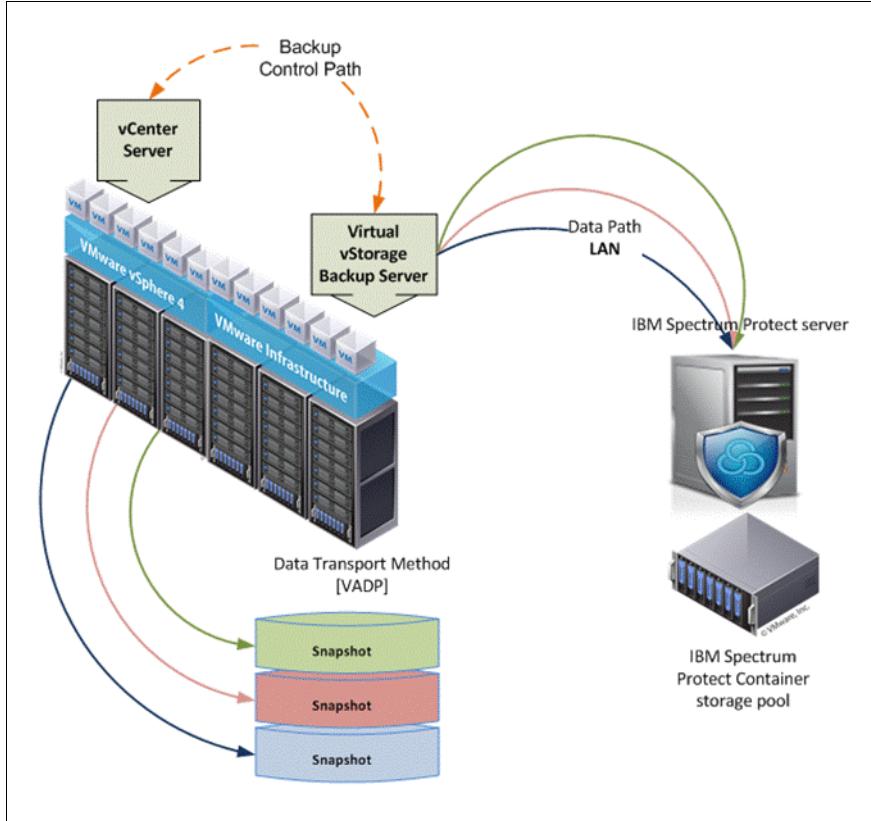


Figure 1-5 IBM Spectrum Protect: Virtual Environment small environment overview

1.8.2 Scenario 2: Large environment

In this scenario, we describe the implementation of IBM Spectrum Protect to protect virtual machines in a large customer environment.

The large environment has the following characteristics:

- ▶ 4 PB total storage
- ▶ Up to 1500 virtual machines (100 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:

- ▶ Eight virtual vStorage backup servers (Proxy)
- ▶ One IBM Spectrum Protect 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 IBM Spectrum Protect server

With IBM Spectrum Protect server v8.1.0 we use one large Blueprint IBM Spectrum Protect server architecture. Consider the implementation of a physical vBS, allowing you to use SAN and LAN-Free transport to move the data from the datastore to IBM Spectrum Protect servers disk containers.

Figure 1-6 shows the possible design (including a physical or virtual vStorage Backup server) and the deduplication implication.

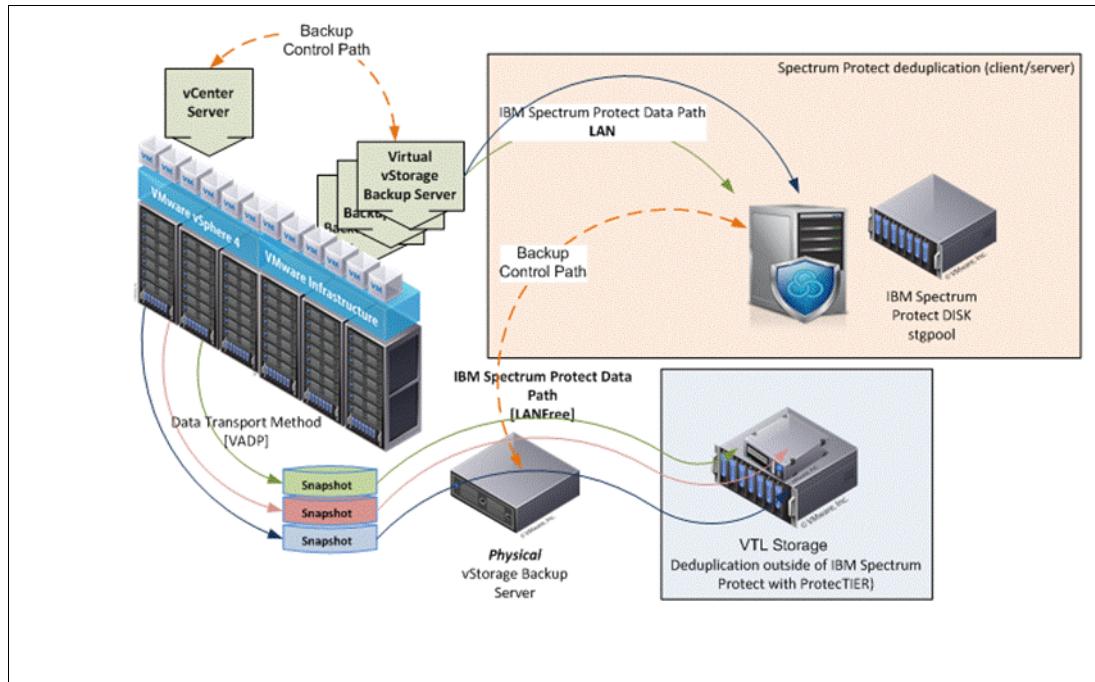


Figure 1-6 IBM Spectrum Protect: Big environment overview

1.8.3 Scenario 3: Shared environment

IBM Spectrum Protect for Virtual Environment 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)
- ▶ VMware vSphere (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 IBM Spectrum Protect 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 IBM Spectrum Protect server. Part of the configuration can be done on the data mover node (the one that is accessing the VMware data and datastore) and on the datacenter node (the one owning the data after it was backed up to IBM Spectrum Protect server).

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



Product introduction

This chapter includes the following topics:

- ▶ IBM Spectrum Protect solutions that protect VMware vSphere environments
- ▶ Data Protection for VMware components
- ▶ New features per version
- ▶ Hardware and software requirements

2.1 IBM Spectrum Protect solutions that protect VMware vSphere environments

You can use IBM Spectrum Protect for Virtual Environments and IBM Spectrum Protect Snapshot to protect VMware vSphere environments. This chapter provides an overview of the IBM Spectrum Protect family and describes how you can use this software solution to protect the VMware virtual machines. You can learn about and the following available features:

- ▶ IBM Spectrum Protect backup archive client within the VMware guest
- ▶ IBM Spectrum Protect for Virtual Environments - Data Protection for VMware to do off host backup
- ▶ IBM Spectrum Protect Snapshot for VMware

2.1.1 IBM Spectrum Protect backup-archive client within VMware guest

This feature protects the data in the same way as for a physical machine. You can perform a backup (incremental or selective) or archive operation within the virtual machine, as shown in Figure 2-1 on page 20.

Tip: You can use the backup-archive client within a virtual machine, as described in the [IBM Tivoli Storage Manager \(TSM\) and IBM Spectrum Protect guest support for Virtual Machines and Virtualization](#) Technote.

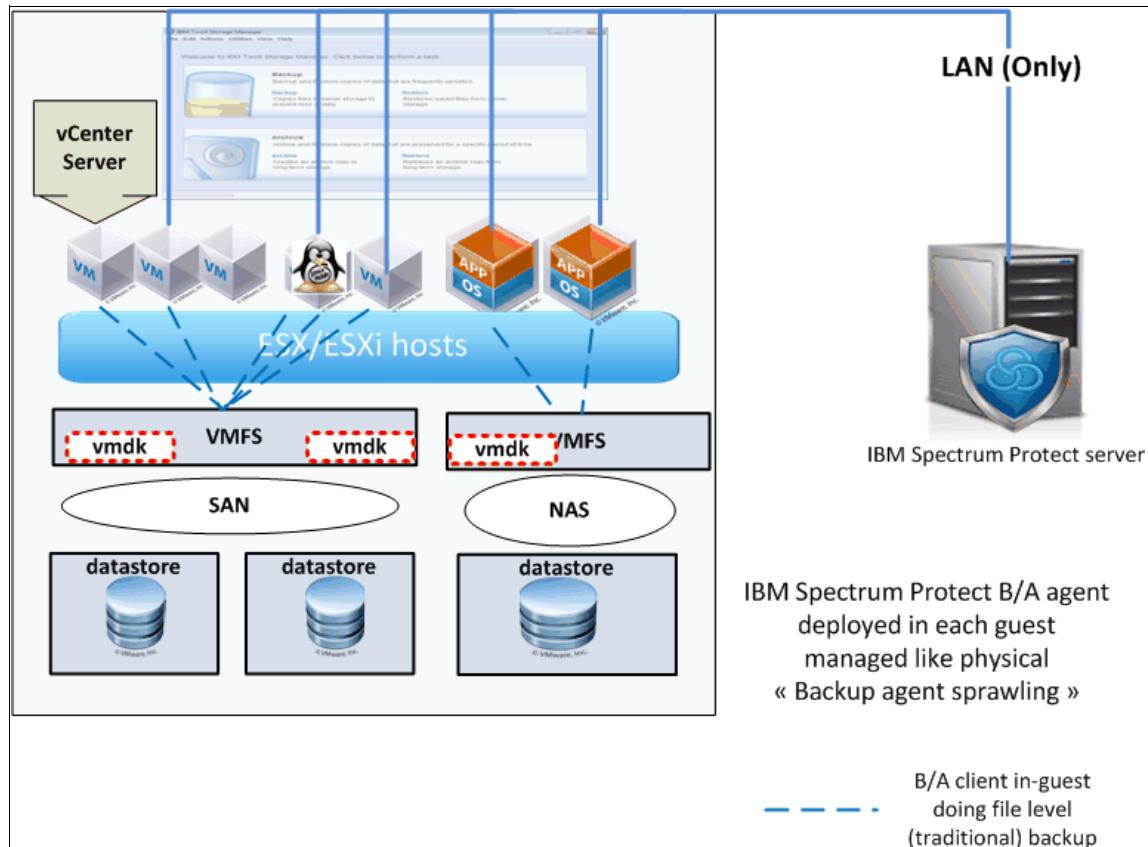


Figure 2-1 Backup archive client in-guest configuration

2.1.2 IBM Spectrum Protect backup-archive client off-host backup option

As shown in Figure 2-2, this option feature consists of taking a snapshot of a virtual machine (VM), by using the incremental forever - full or incremental backup method. Up to and including version 7.1.x, the IBM Spectrum Protect Backup-Archive client can be used in conjunction with the IBM Spectrum Protect for Virtual Environments - Data protection for VMware enablement file to leverage the incremental VM backup capability.

Without that enablement file, only Periodic full VM backups and restores are possible. Starting with version 8.1, only the data mover client included in the IBM Spectrum Protect for Virtual Environments - Data protection for VMware package can be used to do VM backups; the standard 8.1 backup-archive client cannot be used anymore for VM backups.

The capability to leverage VMware snapshots means the backup-archive client (from 6.2 to 7.1) or data mover client (starting with 8.1) uses the VMware vStorage API for Data Protection (VADP) mechanism and relies on the VMware snapshot mechanism to back up an entire virtual machine. This option provides a fast, centralized, off-hosted, and scalable backup methodology.

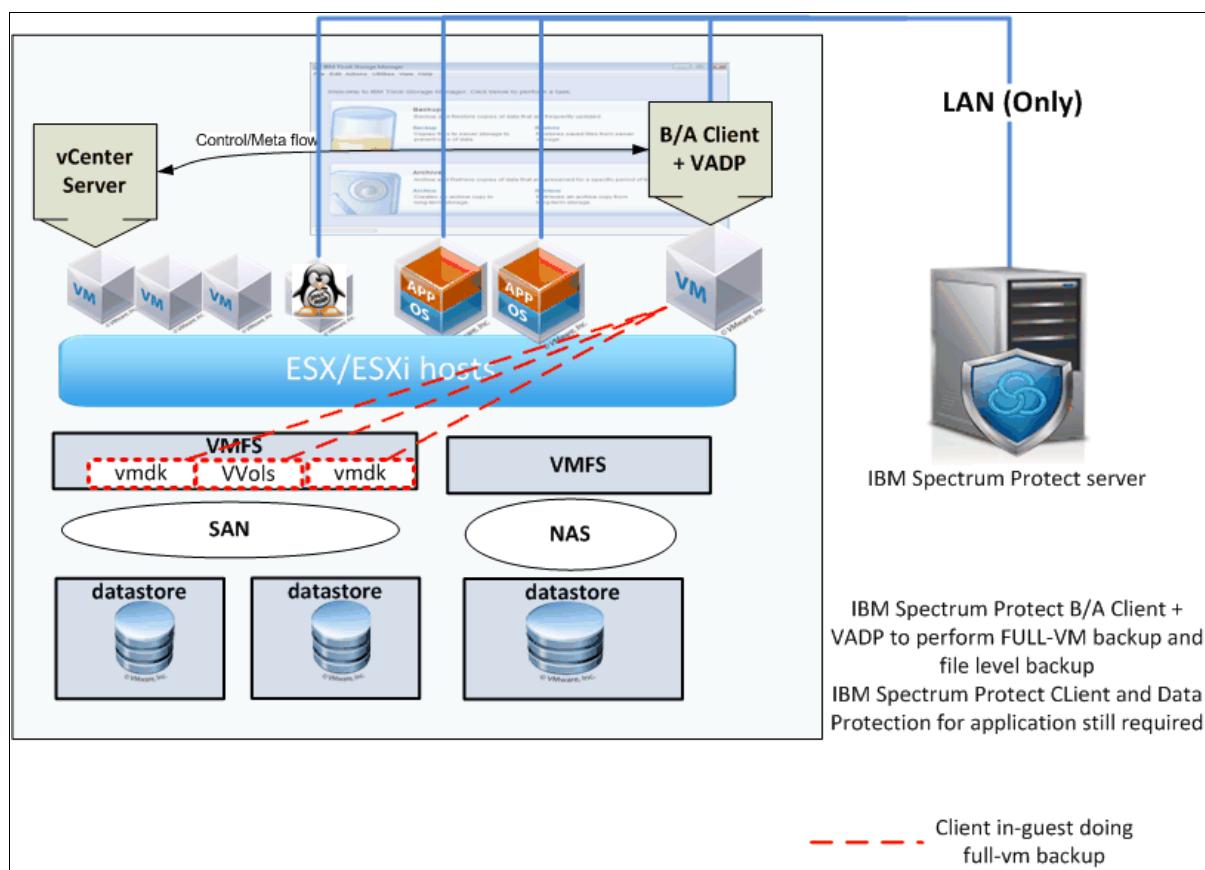


Figure 2-2 Backup-archive client: Full-VM backup by using VMware API for Data Protection

2.1.3 IBM Spectrum Protect for Virtual Environments

As shown in Figure 2-3, this feature consists of the full Data Protection for VMware capabilities:

- ▶ Protect VMs using incremental forever - full and incremental backups
- ▶ Full VM restores
- ▶ Full VM Instant Access and Restores
- ▶ File-level restores
- ▶ New starting with 8.1.2: backups and restores to and from local persistent snapshots on VMware vVols datastores.

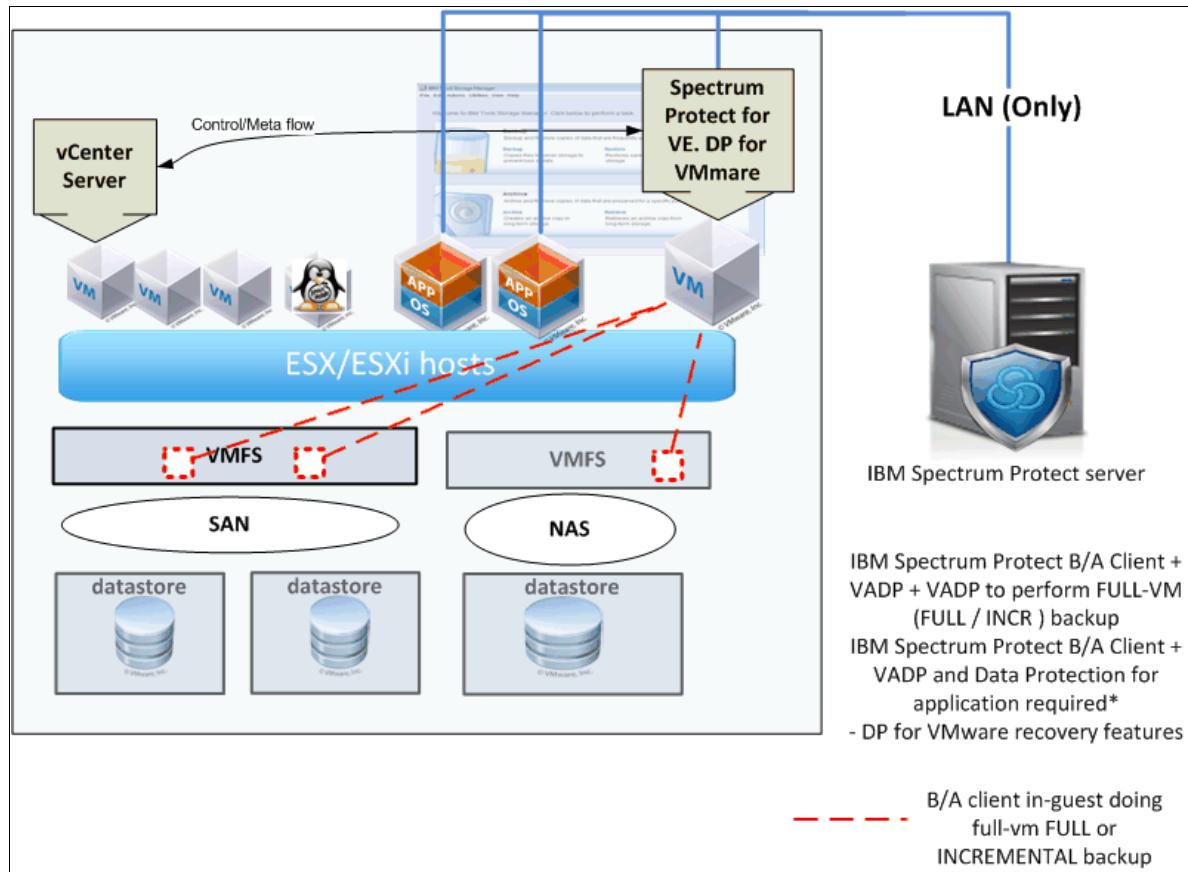


Figure 2-3 Backup-archive client in-guest and Data Protection for VMware configuration

2.1.4 IBM Spectrum Protect Snapshot for VMware option

As shown in Figure 2-4, this feature consists of taking a snapshot at a VMware datastore-level by using the IBM Spectrum Protect Snapshot for VMware solution. This solution is based on built-in snapshot features of the back-end disk system.

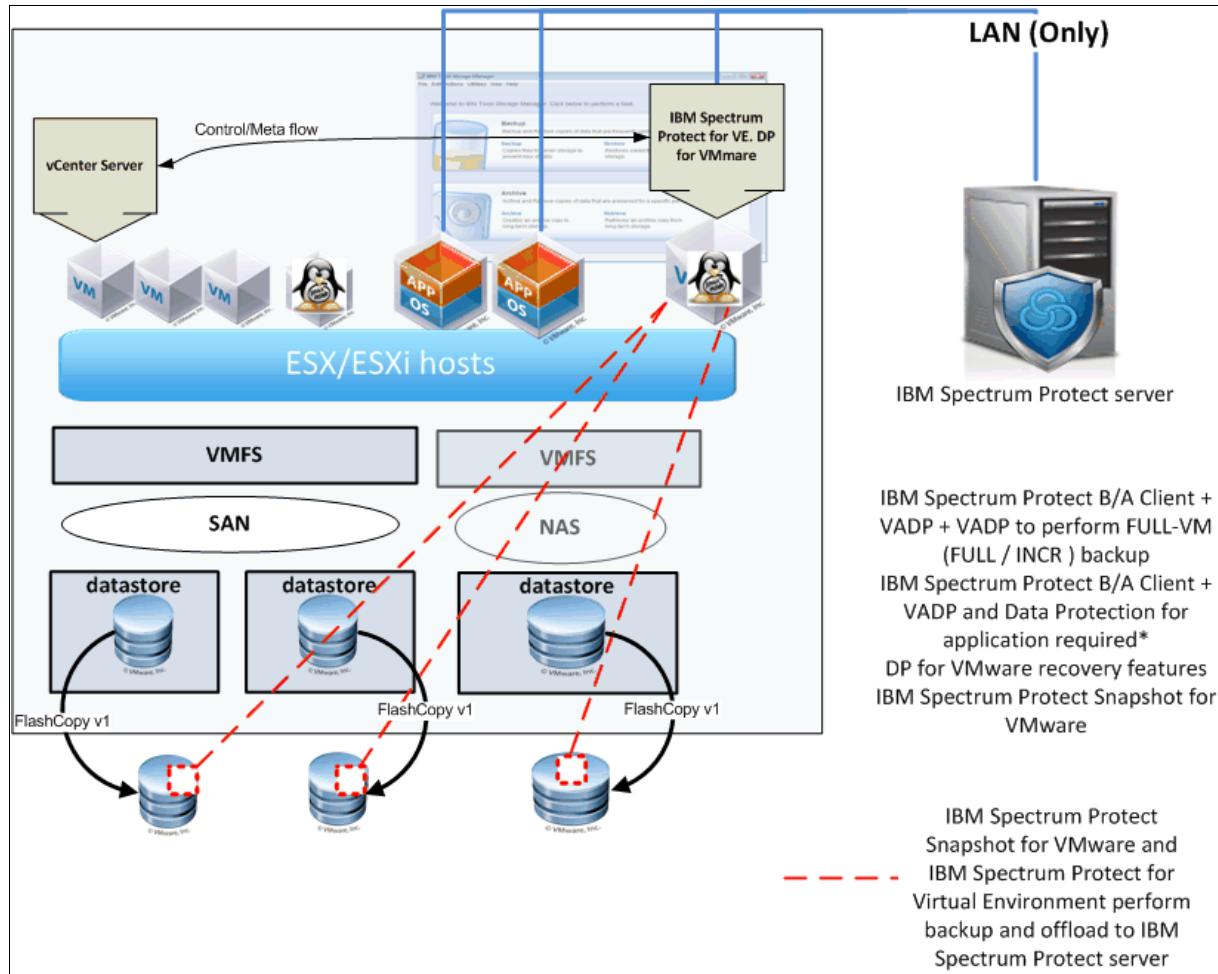


Figure 2-4 IBM Spectrum Protect Snapshot for VMware configuration

You can recover data by using one of the following methods:

- ▶ File
- ▶ Virtual disk
- ▶ Virtual machine
- ▶ Datastore

IBM Spectrum Protect Snapshot can also be combined with Data Protection for VMware so that the snapshot images can be offloaded to the IBM Spectrum Protect server. This feature is important because it provides disaster recovery capabilities that VMware snapshots cannot provide. IBM Spectrum Protect Snapshot for VMware includes the IBM Data Protection extension for vSphere Web client, which is similar to the Data Protection for VMware solution.

2.1.5 IBM Spectrum Protect Snapshot For Windows/UNIX

As shown in Figure 2-5, this option consists of the use of Snapshot with the in-guest backup-archive client to eliminate limitations of snapshots (such as pRDM and clusters) while providing a powerful backup solution. For information about snapshot limitations, see Chapter 3, “Installation roadmap” on page 29.

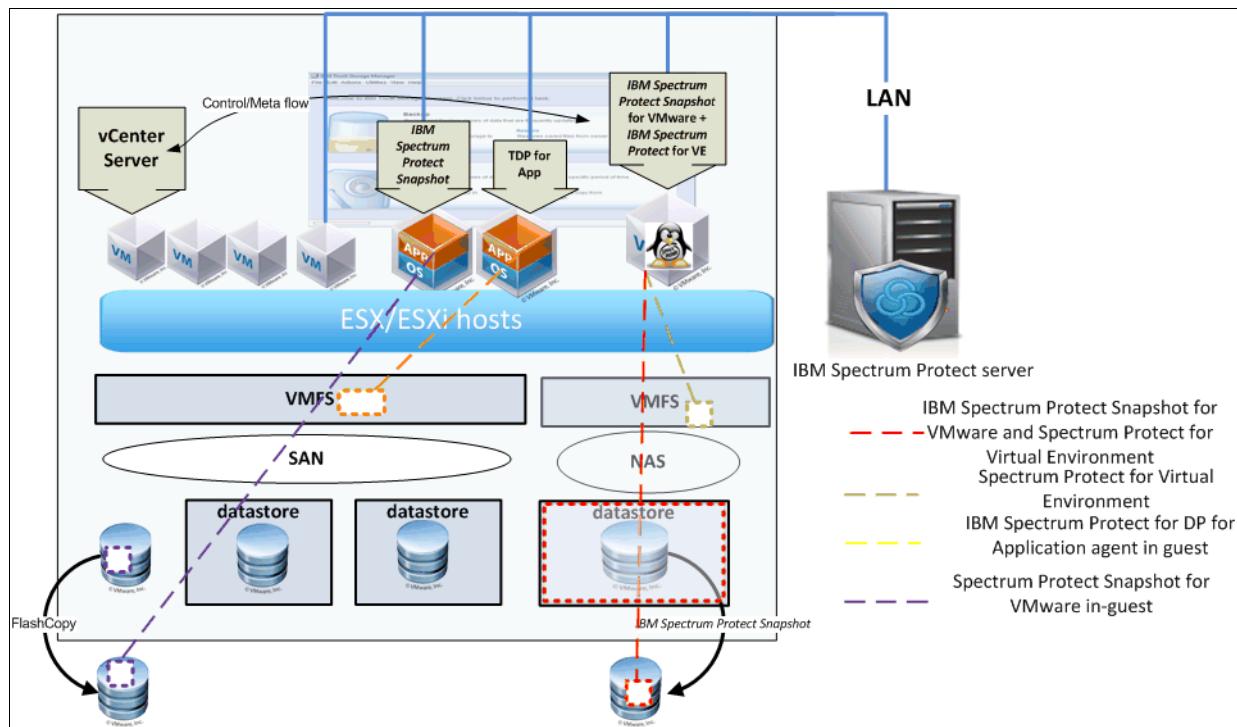


Figure 2-5 Combined configuration

You can use the Snapshot in-guest and Data Protection for VMware solution to protect your data and all the virtual machines that do not host a database or database that is supported by the self-contained application protection. For more information, see section 3.3, “Protecting applications in a virtual environment” on page 35.

2.2 Data Protection for VMware components

For more information about features and configuration information for the Data Protection for VMware components, see the *Data Protection for VMware Installation Guide* and the *Data Protection for VMware User’s Guide*, available in the [IBM Spectrum Protect for Virtual Environments documentation](#).

2.2.1 Component overview

Data Protection for VMware consists of several components.

vStorage Backup Server

The vStorage Backup Server can be a virtual machine or separate physical machine. This is the machine where the data mover is installed. For more information about how to choose between a virtual machine or a physical machine, see section 3.6.3, “vStorage Backup Server: Virtual versus physical” on page 43.

IBM Spectrum Protect data mover

The data mover node is an instance of the data mover, and is configured on a vStorage Backup Server. Thus, you can install the data mover client on a single vStorage Backup Server and create several logical instances or data mover nodes from this single installation. Starting version 8.1, the data mover must be installed in from the packaged install application.

This component provides the following functions:

- ▶ Incremental Forever Full (IFFUL) and Incremental (IFINCR) VM backup

Backs up virtual machines to IBM Spectrum Protect Server storage. A full VM backup operation copies the VM configuration information and performs a block-level copy of VM disks to the IBM Spectrum Protect 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 IBM Spectrum Protect server by using the IBM Spectrum Protect API. These backups are managed and retained according to storage policies that are set up by the IBM Spectrum Protect administrator.

To use this feature a Data Protection for VMware license is required.

This backup solution requires only one initial full backup. Afterward, an ongoing (forever) sequence of incremental backups occurs. The incremental forever backup solution provides these advantages:

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

Starting with version 8.1.2, the IFFULL and IFINCR VM backups for guests located in vVol datastores can be located in persistent snapshots using the data mover client option 'VMBACKUPLOCATION'.

- ▶ Periodic Full (FULL) and Incremental (INCR) VM backup

This type of backups also sends a block-level copy of the VM guest but the difference is that the INCR backups rely to the last FULL backup image and to avoid a too long dependency chain, regular FULL backups need to be programmed.

This type of backup is deprecated and only possible with versions 6.2 up to 7.1

- ▶ 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 backed up.

The data mover client can run cross-platform operations. For example, a Windows data mover client can back up a Linux VM, and vice versa.

A backup that is performed by a Linux data mover client can be restored by a Windows data mover client, and vice versa.

- ▶ **Fast VM revert**

This is a restore type specific for VM guests residing on vVol for which a backup was done using the data mover client option 'VMBACKUPLOCATION LOCAL'.

It reverts from such a backup that is a persistent snapshot type.

The following backup types are included for these versions:

- ▶ [IBM Knowledge Center for V7.1.6](#)
- ▶ [IBM Knowledge Center for V8.1.2](#)

Data Protection for VMware recovery agent

This data protection has the following options:

- ▶ **Incremental Forever Full (IFFUL) and Incremental (IFINCR) VM backup**

Backs up virtual machines to IBM Spectrum Protect Server storage. A full VM backup operation copies the VM configuration information and performs a block-level copy of VM disks to the IBM Spectrum Protect 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 IBM Spectrum Protect server by using the IBM Spectrum Protect API. These backups are managed and retained according to storage policies that are set up by the IBM Spectrum Protect administrator.

To use this feature a Data Protection for VMware license is required.

This backup solution requires only one initial full backup. Afterward, an ongoing (forever) sequence of incremental backups occurs. The incremental forever backup solution provides these advantages:

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

Starting with version 8.1.2, the IFFULL and IFINCR VM backups for guests located in vVol datastores can be located in persistent snapshots using the data mover client option 'VMBACKUPLOCATION'.

- ▶ **Periodic Full (FULL) and Incremental (INCR) VM backup**

This is type of backups also sends a block-level copy of the VM guest but the difference is that the INCR backups rely to the last FULL backup image and to avoid a too long dependency chain, regular FULL backups need to be programmed.

This type of backups is deprecated and only possible with versions 6.2 up to 7.1

- ▶ **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 backed up.

The data mover client can run cross-platform operations. For example, a Windows data mover client can back up a Linux VM, and vice versa.

A backup that is performed by a Linux data mover client can be restored by a Windows data mover client, and vice versa.

- ▶ Fast VM revert

This is a restore type specific for VM guests residing on vVol for which a backup was done using the data mover client option 'VMBACKUPLOCATION LOCAL'.

It reverts from such a backup that is a persistent snapshot type.

The following backup types are included for these versions:

- ▶ [IBM Knowledge Center for V7.1.6](#)
- ▶ [IBM Knowledge Center for V8.1.2](#)

Data Protection for VMware GUI Web Interface

The Data Protection for VMware GUI Web Interface enables the user to manage full VM backup and restore operations for multiple backup-archive client data-mover nodes on a variety of backup and restore configurations.

The VM command-line interface (VMCLI) is also available to perform most of the same functions as done with the GUI.

The GUI powered by an IBM WebSphere® Application Server engine and Derby database. Those components are installed on the vStorage backup server or a separate machine.

The tool is included in the installation package and runs on the IBM Spectrum Protect Data Protection for VMware vStorage Backup Server.

Data Protection for Vmware Extension (plug-in)

This extension is targeted to VMware administrators that can monitor and perform backup and restores from within their vCenter web client. It is powered by the same IBM WebSphere Application Server engine and Derby database than one used for the Data Protection for VMware web GUI.

Data Protection file-level restore (FLR) web GUI

This web interface is target for end users to enable them to do file-level restore only of the guests they have access to without the help of a IBM Spectrum Protect or VMware administrator.

It is powered by the same IBM WebSphere Application Server engine and Derby database than one used for the Data Protection for VMware web GUI.

IBM Spectrum Protect server

The IBM Spectrum Protect server provides the backup repository for the virtual machines that are protected.

2.3 New enhancements

This section provides information about the various capabilities added within each new version of the product. The IBM Spectrum Protect team keeps updating the product all the time.

The list of all new features can be found on the following websites:

- ▶ [IBM Spectrum Protect DP for VMware](#)
- ▶ [IBM Spectrum Protect Snapshot for VMware](#)

2.4 Hardware and software requirements

Your system must meet the hardware and software requirements for Data Protection for VMware V8.1.0. See the document named "[IBM Spectrum Protect for Virtual Environments - All Requirements Doc](#)" to understand all of the requirements.



Installation roadmap

Data Protection for VMware must interrelate with several existing components, such as the VMware infrastructure, identity management (for example, Active Directory), and the IBM Spectrum Protect 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 Data Protection in-guest agent.
- ▶ Is there any virtual machine that cannot use or support snapshots?
- ▶ Are you using vVol Datastores?
- ▶ What is the type of IBM Spectrum Protect storage pool that will be used and whether there are any special considerations for keeping the VMCTL files in a dedicated disk storage pool (tape and cloud pools)?
- ▶ What are the alternative solutions (in-guest IBM Spectrum Protect 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?

This chapter includes the following topics:

- ▶ Collecting and consolidating data protection policies
- ▶ Deployment planning
- ▶ Protecting applications in a virtual environment
- ▶ Communication ports between VMware and IBM Spectrum Protect components
- ▶ Enabling the backup strategy
- ▶ vStorage Backup Server

- ▶ Storage location versus recovery features
- ▶ Determining the location to start backup or restore
- ▶ Design points
- ▶ VMware snapshots considerations
- ▶ Data Protection for VMware considerations
- ▶ Determine the naming convention
- ▶ Data Protection for VMware in a shared environment

3.1 Collecting and consolidating data protection policies

Two of the most important things about data protection are the Recovery Time Objective (RTO) and Recovery Point Objective (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 IBM Spectrum Protect 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 Deployment planning

This section focuses on the relevant information you need to 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:

- ▶ VMware vCenter information:
 - vCenter version
 - vCenter Server IP address
 - Virtual or physical vCenter Server? Is it clustered?
 - Where is the vCenter 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 IBM Spectrum Protect Backup-Archive client to protect files, and Data protection agent for MS-SQL to protect the MS-SQL database.

- ▶ 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.
 - Information about vWols if they exist.
- ▶ 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 IBM Spectrum Protect Nodes hierarchy and relationship. For more information, see 4.1.1, “IBM Spectrum Protect server configuration” on page 60.
 - 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 IBM Spectrum Protect 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	Comment
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 as documented in the “[vCenter Server privileges required for the Data Protection for VMware vSphere GUI and data mover](#)” manual.

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: A good practice is to create dedicated VMware roles:

- ▶ One role set at the vCenter level with the minimal permissions.
See “[Using Roles to Assign Privileges](#)” VMware documentation about these minimal system level permissions.
- ▶ When you add a custom role and do not assign any privileges to it, the role is created as a *read-only* role with three system-defined privileges:
 - **System → Anonymous**
 - **System → View**
 - **System → Read**
- ▶ Then one (or more if security policies enforce that) per datacenter object with the required Data Protection for Vmware permissions.

Each user that will be used to perform backup and recovery operations can be assigned to these roles to inherit the appropriate permissions.

3.2.4 Simplified file-level recovery model

Beginning with IBM Spectrum Protect for VMware 7.1.3, an intuitive web-based portal provides self-service file recovery with no administrator assistance required where end user does not need to know IBM Spectrum Protect. No software is required on the end user system.

Figure 3-1 shows IBM Spectrum Protect for Virtual Environment file-level recovery capabilities. For more information, see the following hardware and software [requirements](#) for IBM Spectrum Protect for Virtual Environments.

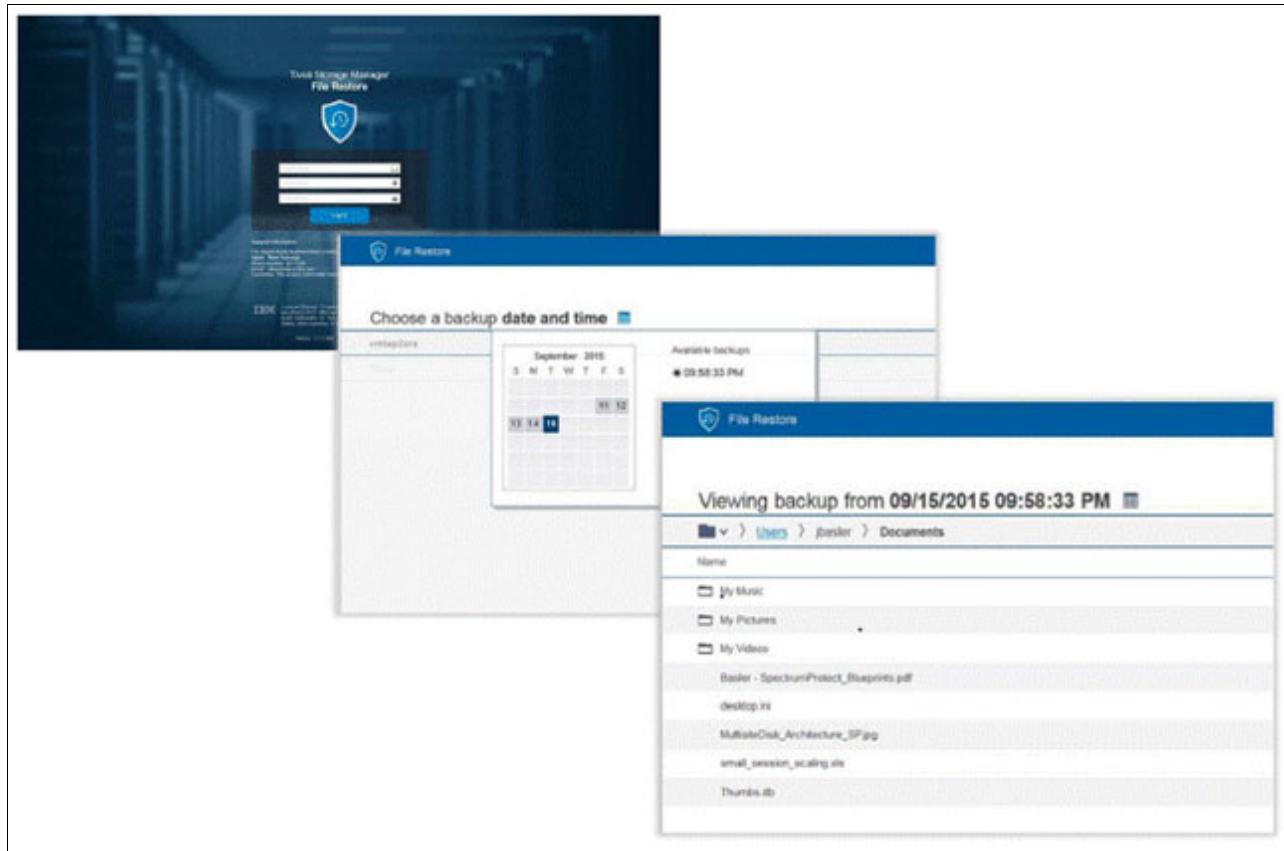


Figure 3-1 Intuitive web-based portal for self-service file recovery overview

The IBM Spectrum Protect for Virtual Environment - Data Protection for VMware simplified file-level recovery procedure is designed to meet an “Help Desk” oriented model (from three to one team). Less skills are required and the recovery time can be reduced by 50% because less steps and less people/teams are needed. File-Level Restore (FLR) combines ease of recovery and rapid validation. The user only needs to perform the following steps:

1. Point the web browser to the IBM Spectrum Protect File Recovery Service URL.
2. On the sign-on screen, enter the VM guest name and the associated credentials.
3. Choose the recovery point (backup image date).
4. Then, select the target location to restore to.
5. Click restore.
6. The process is done.

3.2.5 IBM Spectrum Protect administrator ID authority levels

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 IBM Spectrum Protect server that requires an IBM Spectrum Protect 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 IBM Spectrum Protect administrator ID.

Depending on which tasks you must control from the vCenter plug-in, you might need a different level of IBM Spectrum Protect user authority. For more information about these levels, see [IBM Spectrum Protect for Virtual Environments Data Protection for VMware User's Guide](#).

Figure 3-2 shows the IBM Spectrum Protect administrative privilege that is needed to use the Data Protection for VMware plug-in GUI. This information can be found in detail in the official “Data Protection for VMware vSphere GUI user roles” product documentation available here.

	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 Domain (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 3-2 IBM Spectrum Protect administrative privilege needed to use the IBM Spectrum Protect for VE plug-in GUI

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 IBM Spectrum Protect Snapshot for VMware.

- ▶ In-guest data protection solutions that require the deployment of a backup/recovery agent in the guest machine; for example, **IBM Spectrum Protect for Mail** → **Data Protection for Microsoft Exchange** or **IBM Spectrum Protect for Databases** → **Data Protection for Microsoft SQL**.
- ▶ In-guest data protection solution leveraging hardware snapshots like IBM Spectrum Protect Snapshot for Windows and IBM Spectrum Protect Snapshot for Linux.

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, IBM Spectrum Protect 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 about [IBM Spectrum Protect Data Protection for VMware](#), see IBM developerWorks.

3.3.1 SQL data protection

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

use case	in-guest data protection	off-host data protection
Exchange single-instance deployments that meet all the following conditions: <ul style="list-style-type: none"> • No clustering • No Database Availability Group (DAG) configurations • No special RPO requirements which would necessitate log recovery 	<p><i>in-guest agent:</i> Data Protection for Microsoft Exchange or FlashCopy Manager for Windows</p> <p>If you have deployed FlashCopy Manager for VMware to protect your virtual machine environment, in-guest backups are recommended.</p>	<p><i>Off-host agent:</i> Data Protection for VMware</p> <p>Data Protection for VMware is recommended for stand-alone instances of Exchange</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Clustered servers • Database Availability Group (DAG) configurations • RPO requirements which necessitate log recovery 	<p><i>in-guest agent:</i> Data Protection for Microsoft Exchange or FlashCopy Manager for Windows</p> <p>In-guest backups are recommended</p> <p>In-guest backups provide the following advantages:</p> <ul style="list-style-type: none"> • 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 	<p>Data Protection for VMware and FlashCopy Manager are not recommended for these type of Exchange deployments and use cases:</p>

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

3.3.2 Exchange data protection

Figure 3-4 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: <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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 3-4 In-guest Exchange data protection product positioning

3.3.3 Active Directory Data Protection

Figure 3-5 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> Windows Backup-Archive client 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> Data Protection for VMware or FlashCopy Manager for VMware 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> Windows Backup-Archive client In-guest backups of Microsoft Active Directory is recommended when protecting Active Directory deployments on multiple domain controllers <ul style="list-style-type: none">• 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 3-5 In-guest Active Directory Data Protection product positioning

3.3.4 Unstructured Data Protection

Figure 3-6 shows the product positioning when virtual machines with unstructured data are protected.

<p>Windows and Linux virtual servers (unstructured data)</p>	<p>On an exception basis, consider in-guest backups of Windows virtual machines hosting file/web servers (unstructured) data for the following use cases.</p> <p><i>in-guest agent:</i> <i>Windows Backup-Archive client or Linux Backup-Archive client</i></p> <p>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.</p> <p><i>in-guest agent:</i> <i>FlashCopy Manager for Windows or FlashCopy Manager for Linux</i></p> <p>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.</p>	<p>Off-host agent: <i>Data Protection for VMware or FlashCopy Manager for VMware</i></p> <p>Data Protection for VMware and/or FlashCopy Manager for VMware are the recommended solutions for Windows virtual machines hosting file/web servers (unstructured data).</p> <p>These solutions provide several advantages versus in-guest backups including:</p> <ul style="list-style-type: none"> • 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
<p>Other operating systems (unstructured data)</p>	<p><i>in-guest agent:</i> <i>Backup-Archive client</i></p> <p>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.</p>	<p>Off-host agent: <i>Data Protection for VMware or FlashCopy Manager for VMware</i></p> <p>Data Protection for VMware and/or FlashCopy Manager for VMware are the recommended solutions for Windows virtual machines hosting file/web servers (unstructured data).</p> <p>The advantages of these solutions are the same as those listed above.</p>

Figure 3-6 In-guest unstructured data protection product positioning

3.4 Communication ports between VMware and IBM Spectrum Protect components

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

Figure 3-7 shows the communications ports that might be used, depending on your implementation of Data Protection for VMware. Arrows show the direction of each flow.

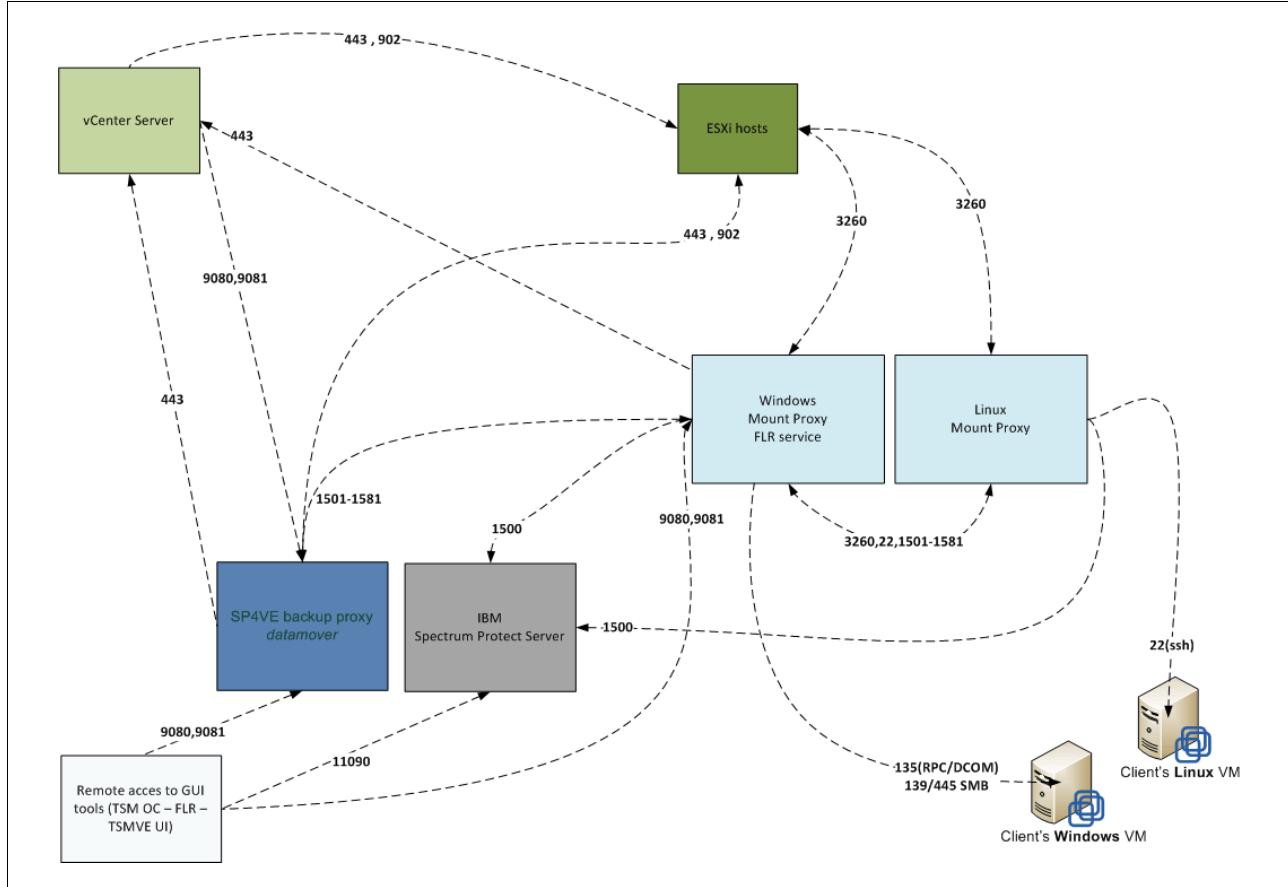


Figure 3-7 Communication ports that are used by Data Protection for VMware

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

This information is also available in the *Open communication ports required by IBM Spectrum Protect Data Protection for Virtual Environments 8.1* [IBM Technote](#).

A list of [TCP and UDP Ports required](#) by VMware components is available.

3.5 Enabling the backup strategy

Prior to version 8.1 there were two available backup strategies; *incremental forever* and *periodic full*. With version 8.1, periodic full is no longer available. The incremental forever strategy is described in this section.

3.5.1 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

3.6 vStorage Backup Server

The vStorage Backup Server (vBS) is the host moving the data between the vSphere infrastructure and the IBM Spectrum Protect server. Many times known as a proxy. For more information, see 2.2, “Data Protection for VMware components” on page 24.

3.6.1 Datamover parallelism capabilities

Starting with 7.1.1, these options were available: **VMMAXPARALLEL**, **VMLIMITPERDATASTORE**, and **VMLIMITPERHOST**.

Starting with 8.1.0, these options were available: **VMMAXBACKUPSESSIONS** and **VMMAXRESTORESESSIONS**.

Starting with 8.1.2, this option was added: **VMMAXRESTOREPARALLELDISKS**.

Parallelism for backups

For more information about parallelism, see the [optimized backup](#) topic in IBM Knowledge Center.

There are several levels of parallelism for backups:

- ▶ VM level parallelism

The data mover client can backup multiple guests in parallel. The client options to tune this include **VMMAXPARALLEL**, which describes how many guests are allowed to be processed in parallel. To avoid hitting the resource limits of the vSphere environment, the following options are needed: **VMLIMITPERDATASTORE** and **VMLIMITPERHOST**.

- ▶ vmdk level parallelism

The data mover client can back up several vmdk disks of the same guest in parallel. There are no options for that level, including in clients starting with version 8.1.

- ▶ Sub-disk level parallelism

The data mover client can back up one vmdk disk using parallel threads. To tune that, use the **VMMAXBACKUPSESSIONS** option.

Parallelism for restores

For more information about parallelism for restores, see the [Restoring a virtual disk using multiple sessions](#) topic in IBM Knowledge Center.

There are several levels of parallelism for restores:

- ▶ VM level parallelism is not available
- ▶ vmdk level parallelism

Starting with version 8.1.2, the data mover client can restore multiple vmdk disks of the same guests. To do so, use **VMMAXRESTOREPARALLELDISKS**.

- ▶ Sub-disk level parallelism

Starting with version 8.1, the data mover client can restore a single vmdk disk using up to 10 restore threads by using the **VMMAXRESTORESESSIONS** option.

3.6.2 Data transfer and data 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 IBM Spectrum Protect components, as shown in Figure 3-9 on page 43.

Data transfer refers to the I/O between the vStorage Backup server and the IBM Spectrum Protect Server. Data transport refers to the I/O between the ESXi datastore and the vStorage Backup Server. Data transport is basically the media used to transfer the data between the datamover client and the VMware datastore.

NBD is the most reliable and easiest data transport to set up. When in doubt, go with NBD. Also, HotAdd provides very good VM restore performance with a virtual datamover, so consider having a dedicated datamover for restores configured with HotAdd. The following data transport options are available:

- ▶ NBD (which is IP-network based)
- ▶ HotAdd
- ▶ NDBSSL
- ▶ NBD
- ▶ SAN

Review the [VMware documentation](#) about the transport types.

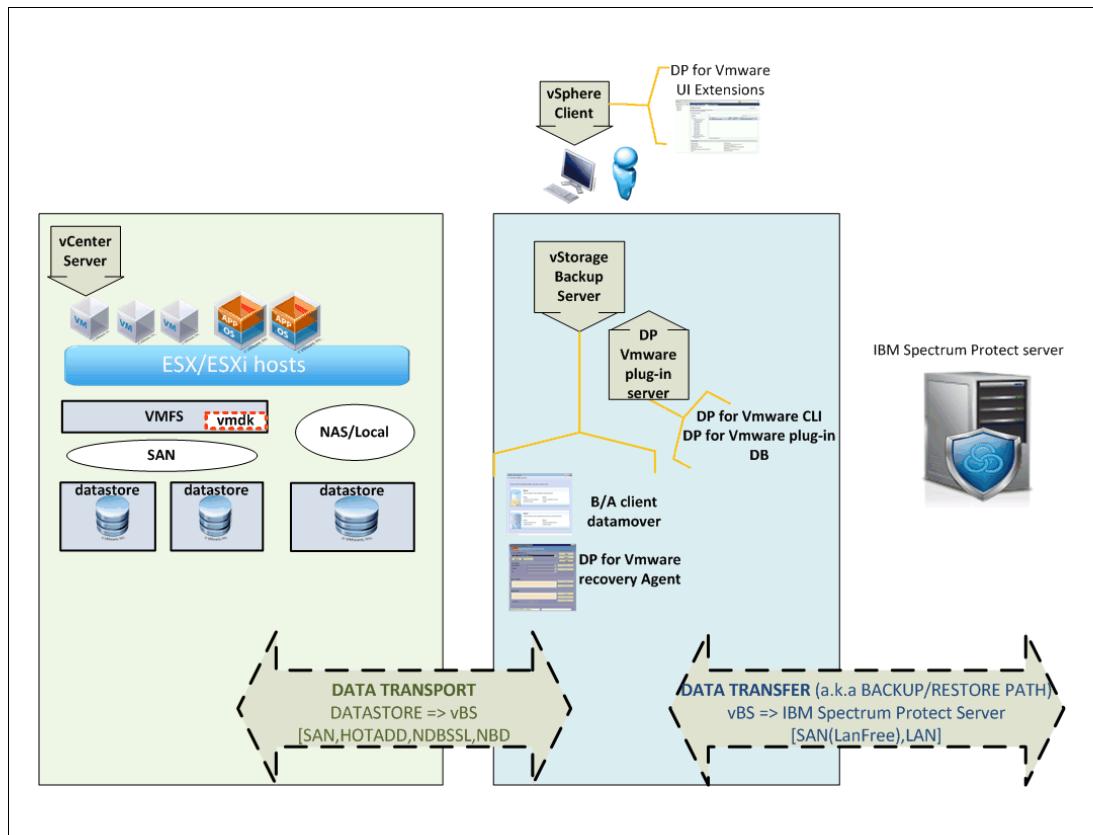


Figure 3-9 Data transfer and data transport explanation

The methods that are used for data transfer from datastore to vBS and from vBS to the IBM Spectrum Protect 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 “vStorage Backup Server: Virtual versus physical”.

3.6.3 vStorage Backup Server: Virtual versus physical

There are many considerations when deciding whether to use a physical or virtual vStorage backup server. Table 3-2 on page 44 is a suggested list of items that can help when you are choosing the best vStorage Backup Server for your environment.

Many factors need to be considered in choosing the appropriate solution but two simple rules can be applied:

- ▶ If you plan on using LAN-free technology for moving data from the data mover into the IBM Spectrum Protect server, then you will need to use a physical data mover, otherwise consider using a virtual data mover if this requirement does not exist in your environment.
- ▶ Regardless of the type of data mover, the data mover must have appropriate, dedicated resources available.

Table 3-2 Comparison of physical versus virtual backup server

vStorage Backup Server location/item	Virtual Backup Server	Physical Backup Server ^a
Environment fully virtualized	Applicable	N/A
Off host the backup load (move the load from ESX to another machine)	Applicable ^b	Applicable
IBM Spectrum Protect LAN-FREE support (be aware of tape limitation, prefer VTL)	N/A	Applicable
10 GbE LAN bandwidth	Applicable	N/A
Use DISK/FILE only storage to store backups	Applicable	N/A
Disk backend systems with low throughput capacity	Applicable	N/A
Plan to use the IBM Spectrum Protect Snapshot for VMware ^c	N/A	Applicable
High number of virtual machine backup (more than 60 vmdk) must run in parallel to fulfill the backup window ^d	N/A	Applicable
ESXi hosts and datastore separation	N/A	Applicable ^e
Multiple vSphere environment	N/A	Applicable ^f
Shared Environment	Applicable ^g	Applicable ^h

- a. If you do not have 10 Gbps and are planning to use physical vStorage Backup Server and LAN-Free, there are some limitations as documented in the Backup-Archive client [known limitation article ANS9365E VMware vStorage API error, API return code: 16000](#).
- b. Off host can be achieved by using virtual vStorage Backup Server by dedicating an ESXi host to run the virtual vStorage Backup Server.
- c. IBM Spectrum Protect Snapshot 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.
- d. 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.
- 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. See footnote e.
- g. For more information about how to manage a shared environment, see 3.13, “Data Protection for VMware in a shared environment” on page 54.
- h. See footnote g.

For more information about how to manage a shared environment, see 3.13, “Data Protection for VMware in a shared environment” on page 54.

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 IBM Spectrum Protect and vice versa)

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

3.6.4 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 Server, 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 Server 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. Example 3-1 shows the output that you must have as per the product documentation.

Example 3-1 Output

```
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>
```

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.

3.6.5 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.
- Recommended Virtual SCSI controller type for the vBS: VMware Paravirtual.
- Using the data mover proxy host settings with the Windows diskpart utility:
 - SAN policy set to OfflineAll
 - automount disabled
- 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.

3.6.6 vStorage Backup Server sizing

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

Obtaining an exact data mover sizing can be a difficult task as many factors must be taken into consideration: the compute and network structure (what is traditionally considered as “feeds and speeds”), the use cases (steady-state backup as opposed to initial full backups or various recovery scenarios) and the nature of the data (for example, average daily change rate).

Because many of these answers require observation, it is much more practical to determine the number of data movers based on the estimated size of the protected environment and adjust accordingly.

The general, simple rule

To make the sizing much easier, IBM Spectrum Protect team have created a simple sizing rule to use a data mover for every 100 TB of vSphere data. For example, if the total virtual machine size of your vSphere environment is 150 TB, it is recommended to start with two data movers to protect this environment.

Note that the total virtual machine size of your vSphere environment can simply be the total used size reported by the vSphere Web Client or via the VMware PowerCLI (for example, `get-vm | Select Name, UsedSpaceGB`; refer to VMware documentation on what this value represents in your environment).

The 100 TB vSphere data general rule was obtained using the following assumptions:

- ▶ 10 GbE (or HotAdd / SAN equivalent) available on all data paths in the environment, specifically the path from the datastore to the data mover and then to the IBM Spectrum Protect server
- ▶ 5% average daily change rate
- ▶ 8 hour backup window

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): 10,240 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 IBM Spectrum Protect 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 `Vmlimitperdatasource` 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)

IBM Spectrum Protect Data Protection for VMware now includes a number of parallelization options to customize your configuration in the most efficient way. Parallelization can be achieved at the VM, disk, or sub-disk level.

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`. Version 8.1 includes `vmmxbackupsessions`, which will set the maximum number of data movement sessions during the backup operation.

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 IFINCR (ongoing backups): $102 \text{ GB/h} / 80 \text{ GB per hour} = 2$ processes

Note: The FULL backup is done once. 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.

Any constraints like bottlenecks? 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)
- ▶ IBM Spectrum Protect 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 IBM Spectrum Protect hardware, including Data Protection for VMware proxy sizing. For more information, consult with your IBM Spectrum Protect sales representative or an IBM Business Partner.

3.6.7 When to use multiple datamover agents

The preferred practice is to have only one data mover node defined per vBS.

This is because the control over the backup or restore parallelism is done at node level and that multiple nodes running concurrently on one vBS do not know of each other and compete for the same system resources. If this type of situation is not carefully controlled, the vBS quickly can run out of resources.

Here are two examples when more than one data mover might be needed on a same vBS:

- ▶ 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, “Data Protection for VMware in a shared environment” on page 54.

For more information about how to define multiple datamovers on one vStorage Backup Server, 3.11.2, “Multiple vCenter server support” on page 52.

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.

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

vStorage Backup Server	Physical				Virtual			
Storage & features	Container Pool	DISK/FILE	Virtual Tape Library	Physical Tape	Container Pool	DISK/FILE	Virtual Tape Library	Physical Tape
LAN-free	No	No	Yes	Yes	No	No	No	No
IBM Spectrum Protect deduplication	Yes: Inline or client	Yes: Server or client	No	No	Yes: Inline or client	Yes: Server or Client	No	No
FULL VM Backup	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
INCR VM Backup	Yes	Yes	Yes	Yes ^a	Yes	Yes	Yes	Yes
FULL FM Restore	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
File Level restore	Yes	Yes	Yes	Yes (lower performance expected)	Yes	Yes	Yes	Yes (lower performance expected)
Instant Volume restore	Yes	Yes	Yes	No	Yes	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](#).

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 on 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, Backup 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 the File level restore web GUI or Data Protection web GUI Restore → Mount tabs + guest OS native copy function or the Recovery Agent native GUI + guest OS native copy function	Using the File level restore web GUI or Data Protection web GUI Restore → Mount tabs + guest OS native copy function or the Recovery Agent native GUI + guest OS native copy function	Using the File level restore web GUI or Data Protection for VMware plug-in (starting with 8.1) Restore → Mount tabs + guest OS native copy function
Full VM Instant Access/Restore	Using the CLI and TDP 4 VE web GUI	NA	Using the plug-in Restore tab

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 should consider Data Protection for VMware recovery agent only on a virtual machine where you plan to perform Instant Volume Restore operations.

3.9 Design points

In this section we describe some IBM Spectrum Protect Server design decisions needed, when planning to deploy 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 IBM Spectrum Protect 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 technote, [Understanding metadata for VM backups](#), which helps you calculate the maximum space that CTL can use and so estimates how large the CTL destination pool can be.

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

For more information about tape-only implementation, see the [Tape Configuration Guidelines](#) in IBM Knowledge Center.

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 limitations (vSphere 6.5) is available in [vSphere 5 Documentation Center Snapshot Limitations](#) topic.

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.
- ▶ Snapshots provide a point-in-time image of the disk that backup solutions can use, but Snapshots are not meant to be a robust method of backup and recovery. Large numbers of snapshots are difficult to manage, consume large amounts of disk space, and are not protected in the case of hardware failure.
- ▶ Snapshots can negatively affect the performance of a virtual machine. Performance degradation is based on how long the snapshot or snapshot tree is in place, the depth of the tree, and how much the virtual machine and its guest operating system have changed from the time you took the snapshot.

Although in some cases backup via snapshots is not possible, you can protect the data by implementing an in-guest IBM Spectrum Protect agent.

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.

Review the [VMware documentation](#) on block size.

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 3-7.

Table 3-7 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 suggests 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.

Be aware that starting the IBM Spectrum Protect version 7.1.6, a new parameter called **vmdatastorethreshold** has been introduced, to prevent out-of-space errors during virtual machine backups. Use the **vmdatastorethreshold** option to set the threshold percentage of space usage for each VMware datastore of a virtual machine.

When you initiate a virtual machine backup, the client checks the data usage of the VMware datastores before the virtual machine snapshot is created. If the threshold is exceeded in any of the VMware datastores, the virtual machine is not backed up.

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 IBM Spectrum Protect Known Issues and Limitations

The following limitations apply for Data Protection for VMware operations:

- ▶ Technote [IBM Spectrum Protect Data Protection for VMware 8.1 limitations](#).
- ▶ Technote [IBM Spectrum Protect Data Protection for VMware 7.1 limitations](#).
- ▶ Technote [IBM Snapshot for VMware 4.1 Limitations](#).
- ▶ Technote [FLR Limitations](#).
- ▶ Technote about [Microsoft Cluster of virtual machines](#).
- ▶ VMware best practice guide about [Windows Domain controller within a virtual machine](#).

3.11.2 Multiple vCenter server support

This section describes vCenter mapping.

Each vCenter maps to an IBM Spectrum Protect server. You can have multiple clusters within the vCenter but they would all go to the same IBM Spectrum Protect server so you can share as many vCenters to IBM Spectrum Protect servers. You can have 1, 2, 3, ... N vCenter servers going to the same IBM Spectrum Protect server, however, you can not do the reverse and break-up a single vCenter to more than one IBM Spectrum Protect server.

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. 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 (the **VMHOST** 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.

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

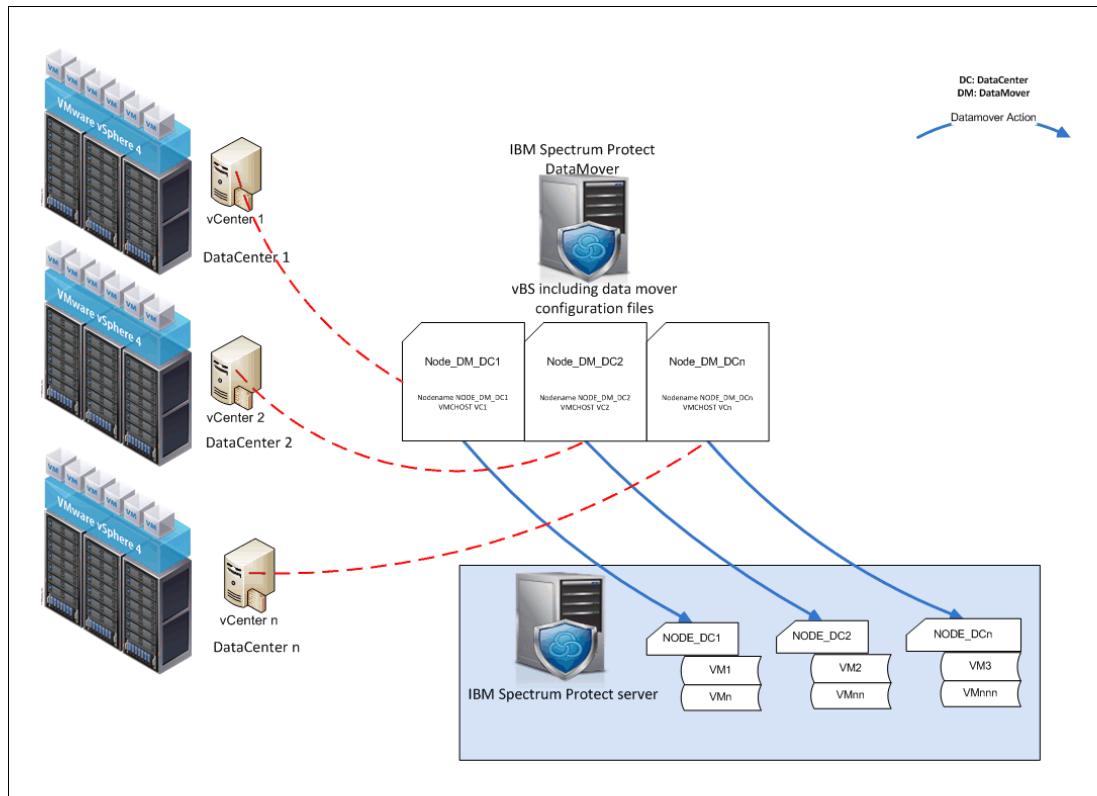


Figure 3-10 Multiple vCenter support setup: Datamover

3.12 Determine the naming convention

A naming convention helps you to determine the role of every component and its interactions. Table 3-8 suggests a naming convention for client <cli>.

Table 3-8 IBM Spectrum Protect node naming convention

Role	Description	IBM Spectrum Protect node Names
vCenter node	The virtual IBM Spectrum Protect 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
Data Protection for VMware command-line interface node	The IBM Spectrum Protect Client node that connects the Data Protection for VMware command-line interface to the IBM Spectrum Protect Server and the datamover node.	<cli>_<vCenterServer>_VCLInnnn
IBM Spectrum Protect data mover node	The IBM Spectrum Protect node name for the IBM Spectrum Protect Backup-Archive client that is installed on the vStorage Backup Server. These nodes perform the data movements. You can have multiple IBM Spectrum Protect 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 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 one 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 Backup 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 IBM Spectrum Protect 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 IBM Spectrum Protect 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

Based on your security requirements you might end up with a complex set of DP for VMware components and its associated nodes definition. This section guide you through a decision tree highlighting what are the question to be answered and the impact on your IBM Spectrum Protect DP for VMware implementation.

Figure 3-11 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.

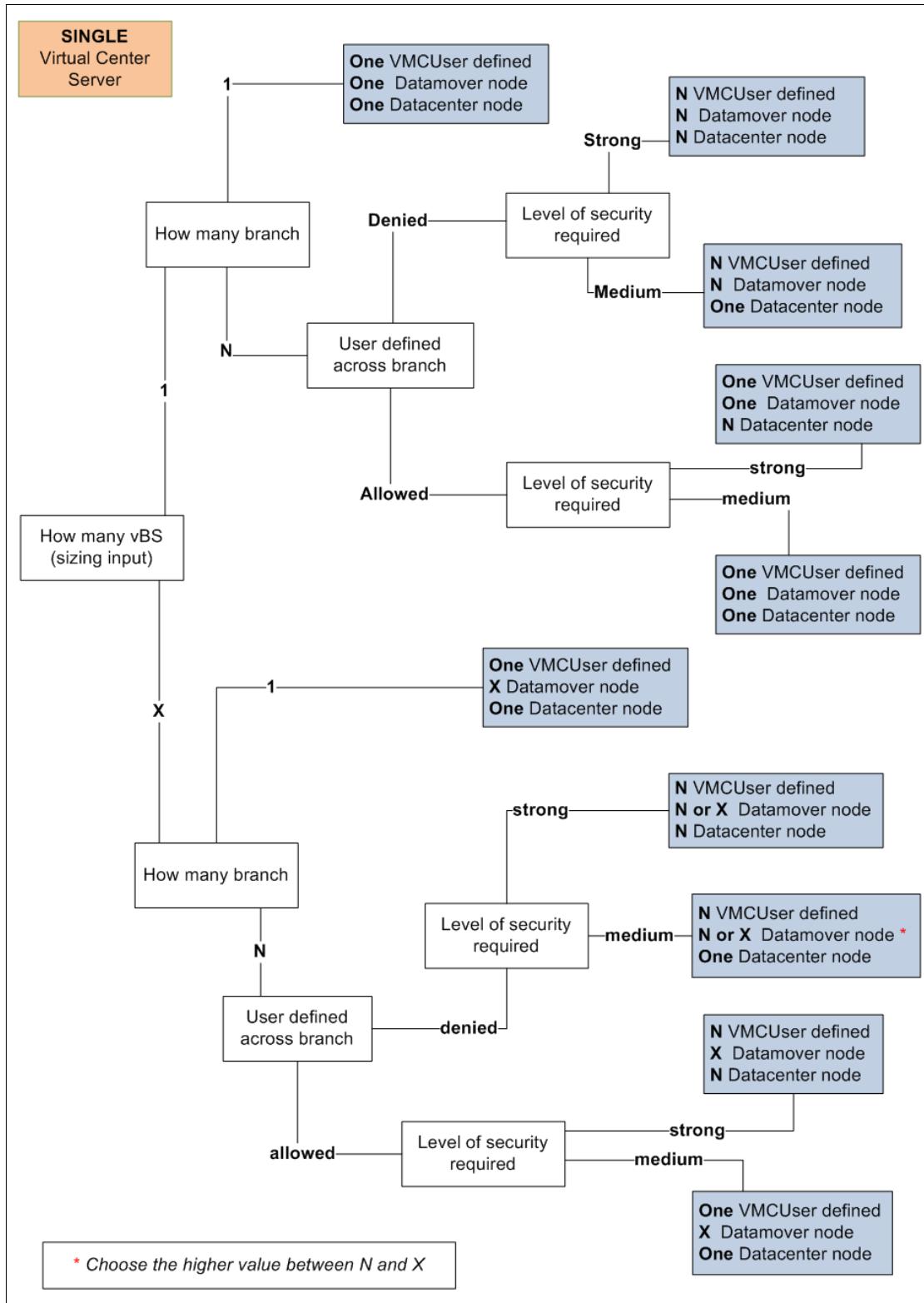


Figure 3-11 Single vCenter server decision tree

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.

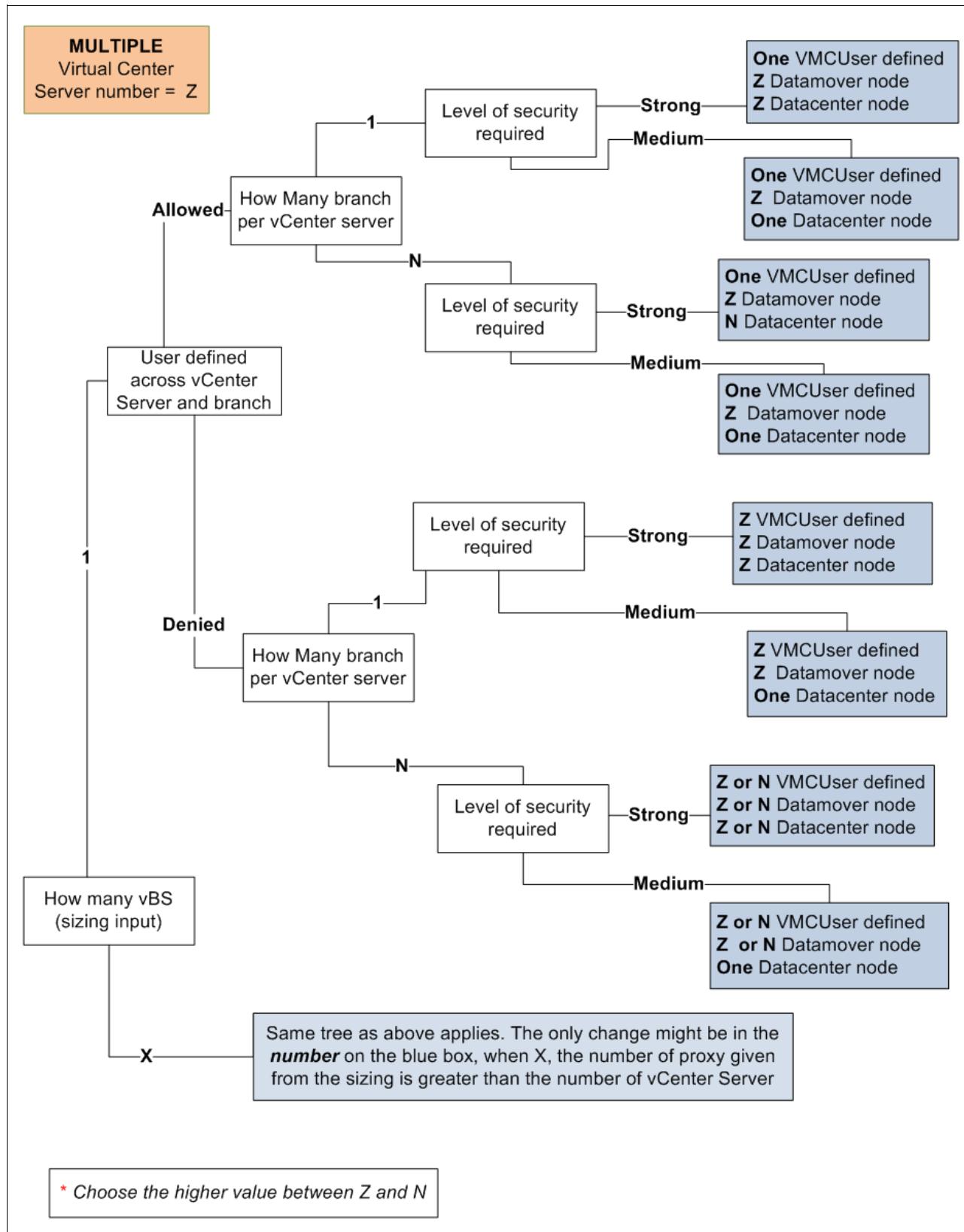


Figure 3-12 Decision tree with multiple vCenter servers

Note: In a shared environment, security requirements dictate the number of vStorage Backup Servers and how many IBM Spectrum Protect datacenter nodes you must implement. It must fit with the sizing requirements.



Installation and configuration

This chapter describes the procedures that are used to install and configure the IBM Spectrum Protect for Virtual Environments - Data Protection for VMware components.

Windows and Linux operating systems are covered in this chapter.

This chapter includes the following topic:

- ▶ Overview of component installation and 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	Recommended steps
1. Ensure prerequisites are in place	Prerequisite requirements are listed in Chapter 3., “Installation roadmap” on page 29.
2. Configure IBM Spectrum Protect server	Define the domain, policy, device class, storage pool, management class and copy group that will be used to control the target storage pool for the VM backups and the VM backup retention. For more information, see the IBM Spectrum Protect documentation in IBM Knowledge Center.
3. Install Data Protection for VMware	Install the Data Protection for VMware (if not previously installed on the vStorage backup server).

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.

Review the [All Requirements](#) document in IBM Support.

Do not install the standard BA client prior to the installation of the IBM Spectrum Protect Data Protection for VMware product, it is slightly different from the bundled version and will not function as intended.

4.1.1 IBM Spectrum Protect server configuration

Below steps are examples how to configure SP server. Complete the following steps to configure the IBM Spectrum Protect Server:

1. Define domain and policies:
 - define domain ispve
 - define policy ispve ispve
2. Define device class:
 - define dev ispve_ctl devtype=file mountlimit=50 maxcapacity=10g dir=/stg1,/stg2
 - define dev ispve_data library=libr1 devt=lto format=drive mountret=1
3. Define storage pools for IBM Spectrum Protect for VMware data and control files
 - define stgpool ispve_ctl ispve_ctl pooltype=primary hi=100 lo=90 maxscratch=50
 - define stgpool ispve_data ispve_data pooltype=primary hi=90 lo=80 maxscratch=100

To estimate the size of the CTL storage pool, consider Example 4-1.

Example 4-1 CTL storage pool size estimation formula

A virtual machine with a single vmdk of 100GB, with an average 10% daily change rate of data, with 15 days retention policy.

The total retained data is the original source data (100GB) plus the daily amount of data changed ($10\% * 100\text{GB} = 10\text{GB}$) times the number of days retained (15). The total is $(100\text{ GB}) + (10\text{GB} * 15 \text{ days}) = 100\text{GB} + 150\text{GB} = 250\text{GB}$. To estimate the amount of VMCTLMC data required multiply the retained data by 0.2%: $250\text{GB} * 0.2\% = 0.5\text{GB}$ or 512 MB of disk storage.

In summary:

Original source data = 100 GB

Total retained data = $100\text{ GB} + (100\text{ GB} * .10 \text{ change rate} * 15 \text{ days}) = 100\text{ GB} + 150\text{ GB} = 250\text{ GB}$

VMCTLMC data required = $250\text{ GB} * 0.002 \text{ VMCTLMC estimate} = 0.5\text{ GB}$

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. CTL data is always to remain on disk.

4. Define the management classes for Data (DAT) and Control (CTL) files:

- define mgmt ispve ispve_ispve_ctl
- define mgmt ispve ispve_ispve_data

5. Define the copygroups:

- define copygroup ispve_ispve_ctl type=backup dest=ispve_ctl verexist=nolimit verdelete=nolimit retex=30 reto=30
- define copygroup ispve_ispve_ispve_data type=backup dest=ispve_data verexist=nolimit verdelete=nolimit retex=30 reto=30

6. Assign a default management class:

- assign defm ispve_ispve_ispve_data

7. Activate the policy:

- activate policy ispve_ispve



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
- ▶ VM backup using vCenter plug-in
- ▶ VM backup by using Datamover client
- ▶ VM backup by using the Datamover Client command line
- ▶ VM backup by using Data Protection for VMware CLI
- ▶ Protection for in-guest applications
- ▶ VM backup optimization

5.1 Configuring the Datamover

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 (data mover, 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:

Starting with 8.1, there are two approaches when defining the backup scope:

- ▶ The IBM Spectrum Protect Administrator approach, which uses the '`-domain.vmfull`' data mover client option from the backup client command line, schedule definition or data mover option file with the following domain-level parameters: `all-vm`, `all-windows`, `vmhost`, `vmfolder`, `vmhostcluster`, `vmdatastore`, `vmresourcepool`, `vmhostfolder`, and `vmdatacenter`.

For a comprehensive list of available `domain.vmfull` parameters, review the [Client options reference](#) technote in IBM Knowledge Center.

- ▶ The VMware administrator approach:

- a. First enabling the data mover for VMware tags with the following options:
 - '`vmtagdatamover`'
 - '`vmtagdefaultdatamover`'
 - '`-domain.vmfull=schedule-tag`'
- b. Then assigning tags to the appropriate VMware objects in the vSphere environment.

You can assign data protection tags to the following types of inventory objects:

- Datacenter
- Folder (Host and Cluster folders and VM and Template folders)
- Host
- Host cluster
- Resource pool
- Virtual machine

For more information, see the [Data protection tagging overview](#) topic in IBM Knowledge Center.

5.2 VM backup 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 the IBM Spectrum Protect Administrator who is associated with the plug-in, you might create every type of task (backup, restore, or schedules):

1. Go to **vSphere client** → **Solutions and Applications** and select your plug-in icon.
2. Go to the Backup tab and click **Create a backup**, as shown in Figure 5-1 on page 65. 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.

It should be noted that if you wish to manage a schedule through the graphical interfaces, you should create the schedule through the graphical interface. It is possible to manually create the intended schedules on the IBM Spectrum Protect server, but they may not function as intended.

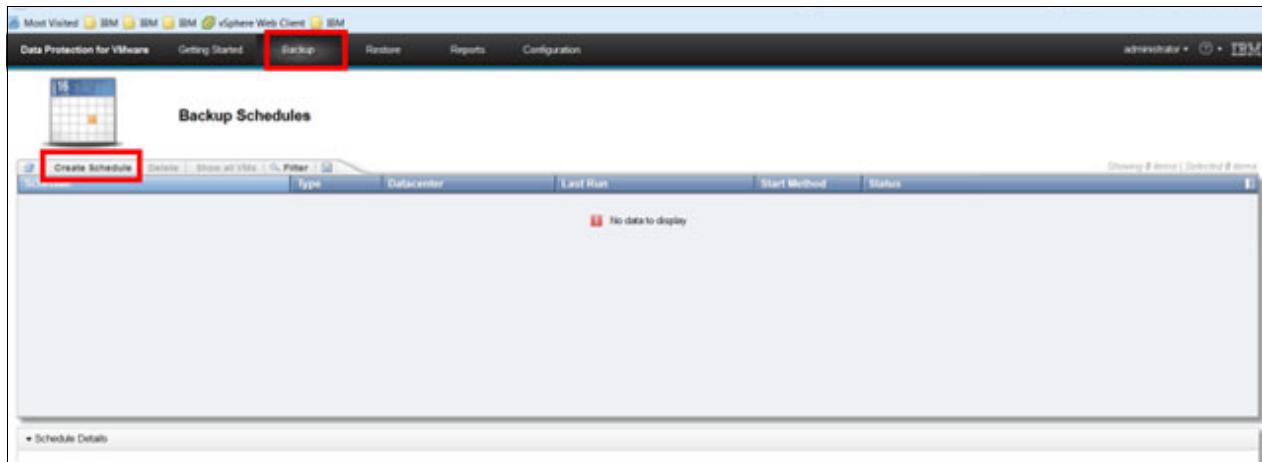


Figure 5-1 Creating a schedule

The next screen you will see is the Backup schedule wizard, shown in Figure 5-2.

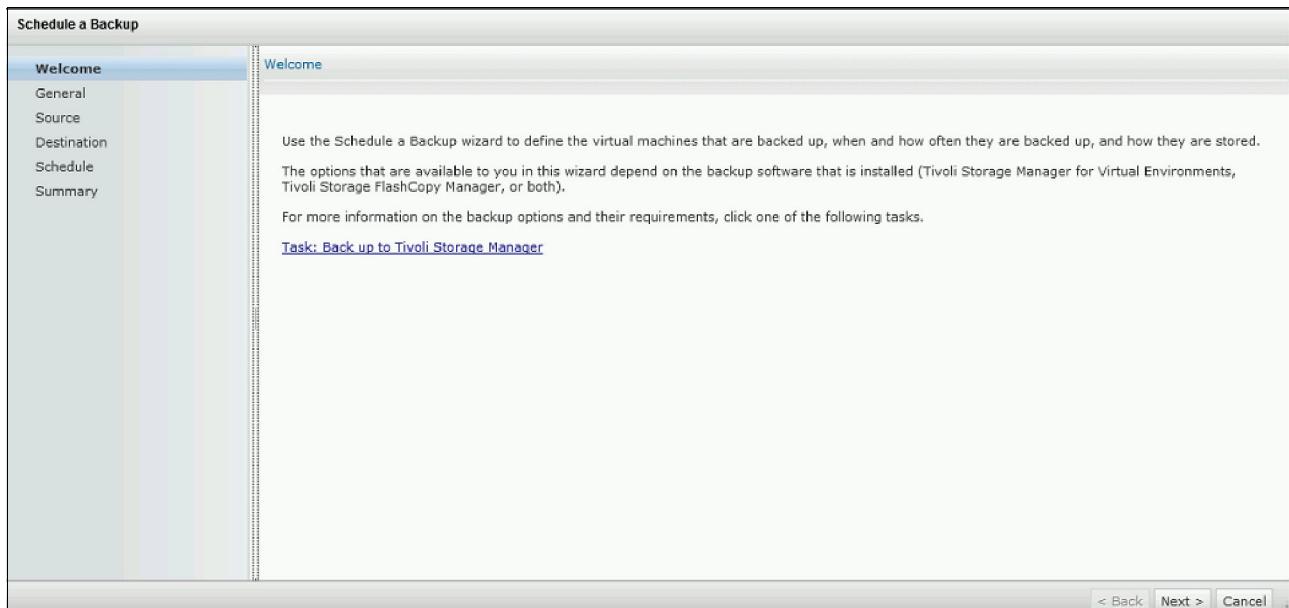


Figure 5-2 Backup schedule wizard

Complete the following steps to start a VM backup:

1. Define a schedule Name and description, as shown in Figure 5-3.

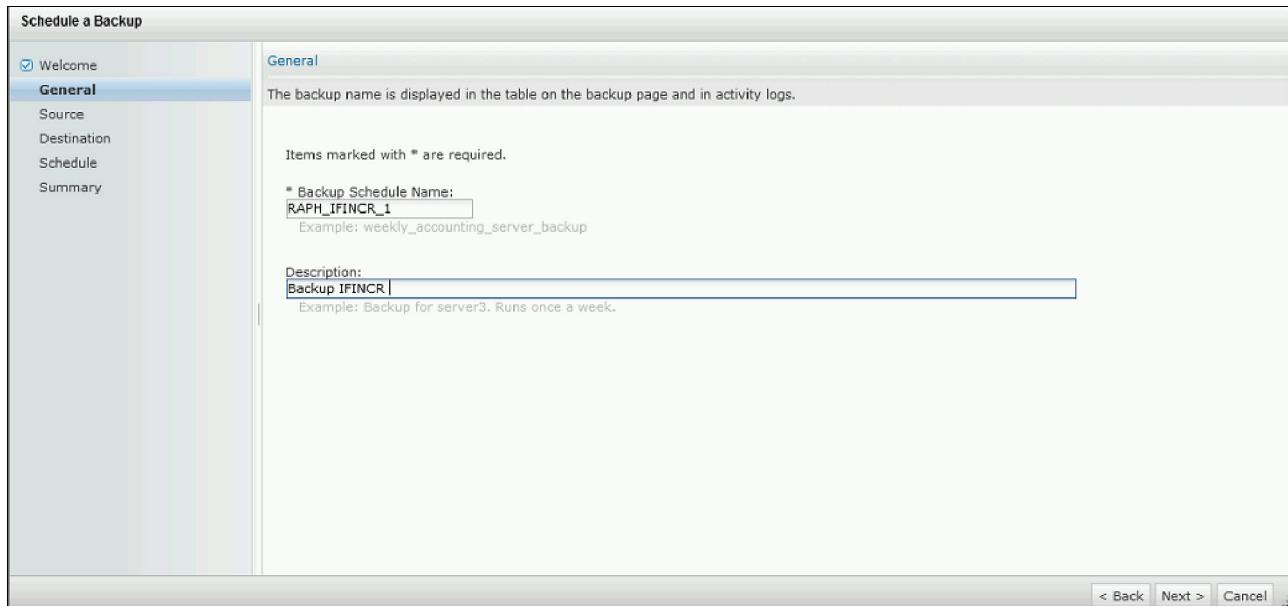


Figure 5-3 Enter schedule name and description

2. Select one or several VMs to be protected, as shown in Figure 5-4.

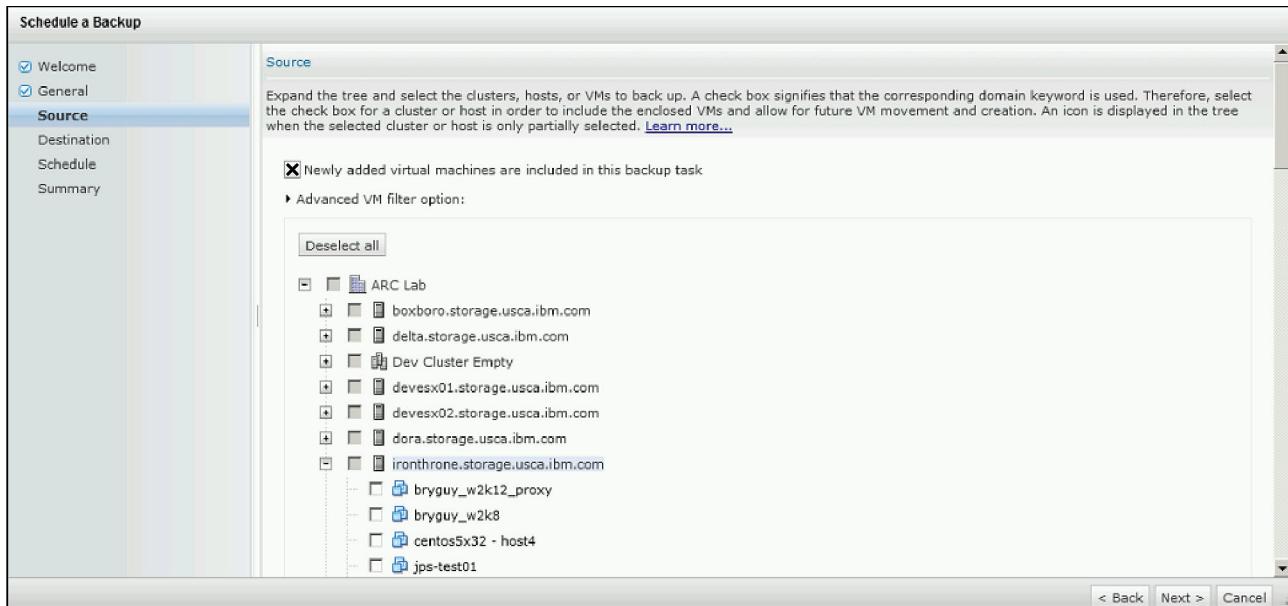


Figure 5-4 Selection of the virtual machines to be backed up

Pay attention to the **Newly added virtual machines are included in this backup task** option. 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 scheduled task. This option is selected by default.

3. Select the datamover that will be used for this backup (the one that is responsible for transferring the data from the datastore to the IBM Spectrum Protect server), as shown in Figure 5-5.

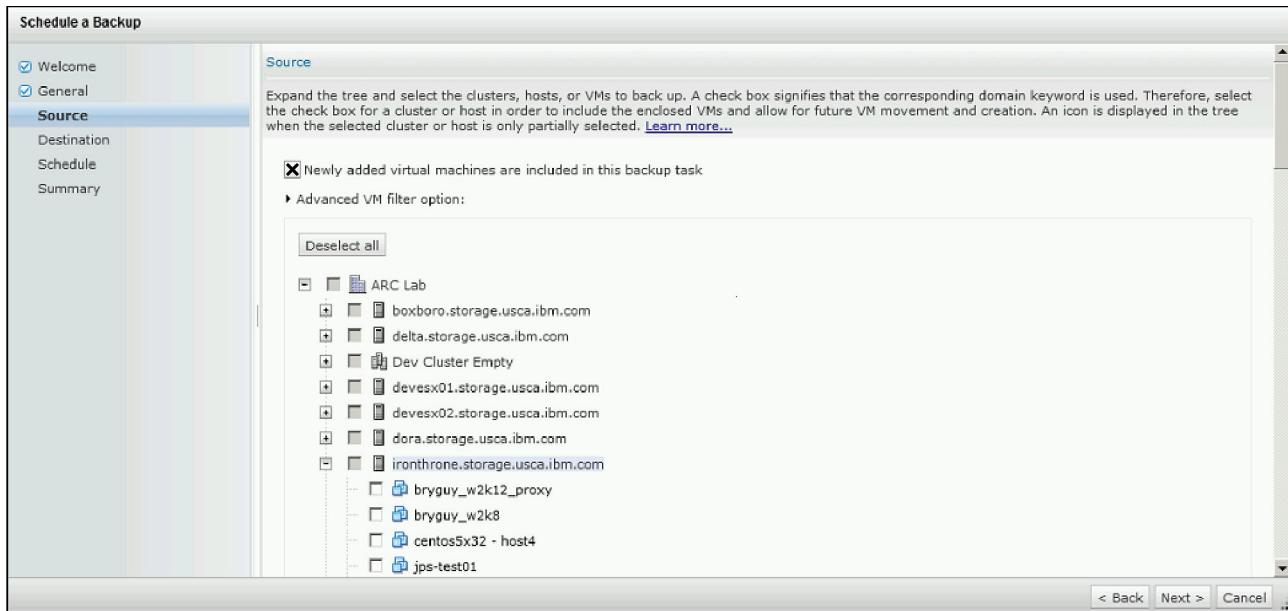


Figure 5-5 Select the datamover that transfers the VM backup data to the IBM Spectrum Protect server

4. Select how you would like to start the backup. The default is **Run the backup now**, which will invoke the backup of your VMs immediately, as shown in Figure 5-6.

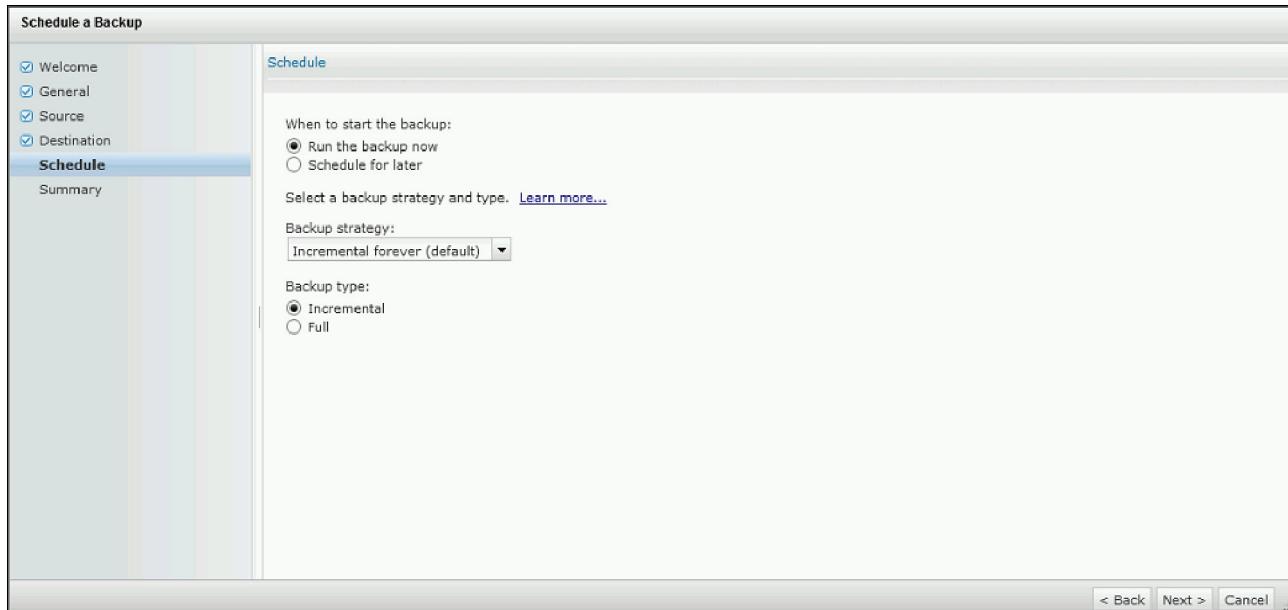


Figure 5-6 Specify the backup start time and the backup type

- If you select **Schedule for later**, this option enables you to define the schedule start date, start time, and frequency of backups, as shown in Figure 5-7.

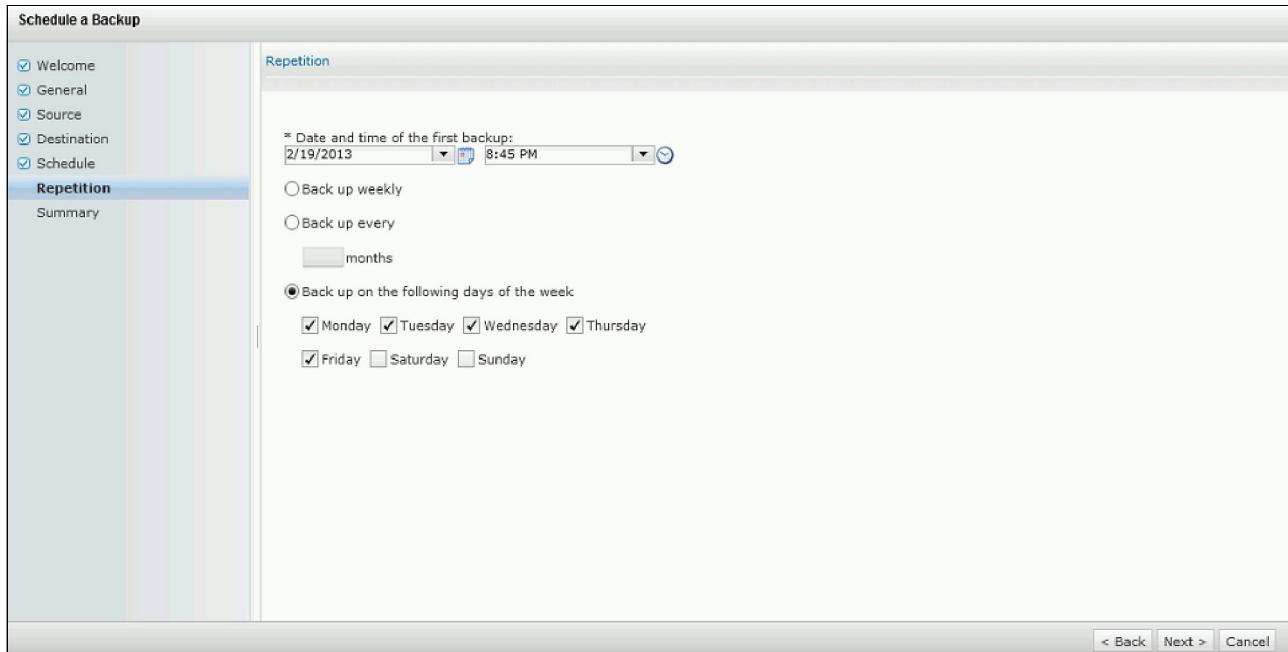


Figure 5-7 Define schedule details

When you create a schedule with the **Run the backup now** option, IBM Spectrum Protect for VMware does not define an IBM Spectrum Protect server schedule. If you create a schedule with **Schedule for later** selected, IBM Spectrum Protect for VMware defines an IBM Spectrum Protect server schedule:

- 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 IBM Spectrum Protect server.

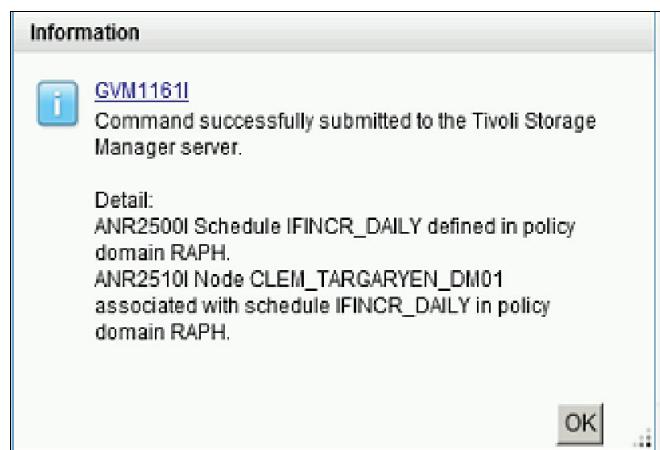


Figure 5-8 Result of IBM Spectrum Protect schedule creation

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

- 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 5-9.

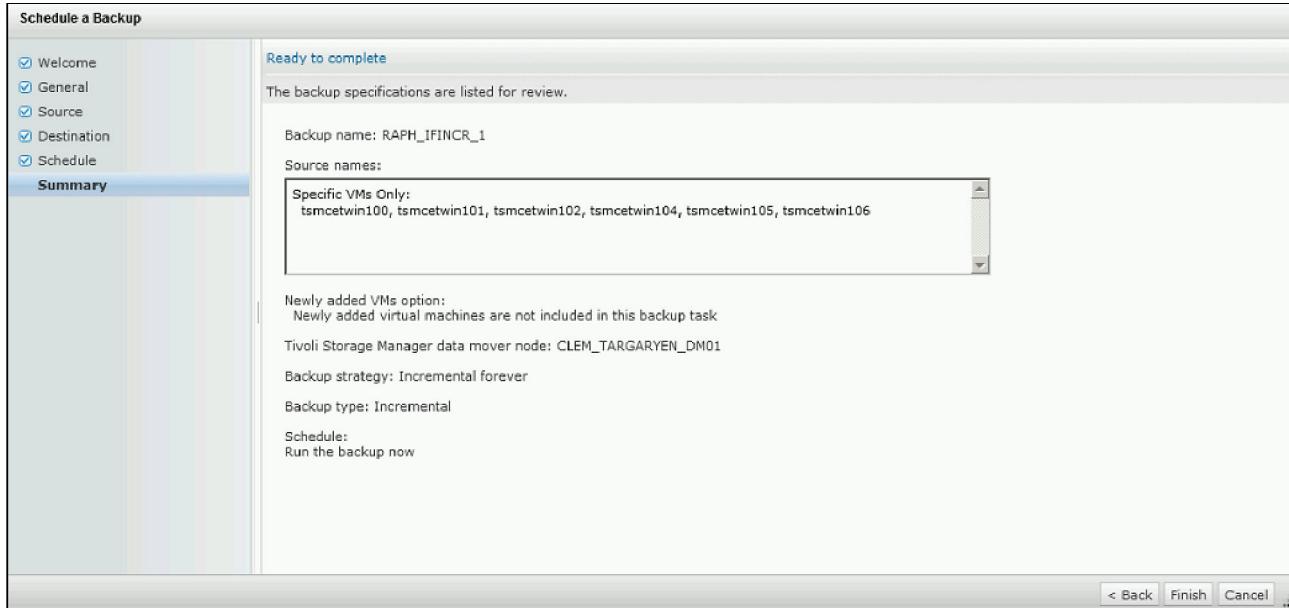


Figure 5-9 Summary of backup schedule task creation

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

On the IBM Spectrum Protect 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 Datamover client

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

1. Go to the installation directory: C:\Program Files\tivoli\tsm\baclient (on Windows) or /opt/tivoli/tsm/baclient/bin (on Linux).
2. Ensure that you specify the **asnodename** option in the dsm.opt (on Windows) or dsm.sys (on Linux), so that you can authenticate as the data center node name and not the data mover node.
3. Start the GUI interface.
4. Click **Menu** → **Action** → **Backup VM**.
5. 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 5-10. 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.

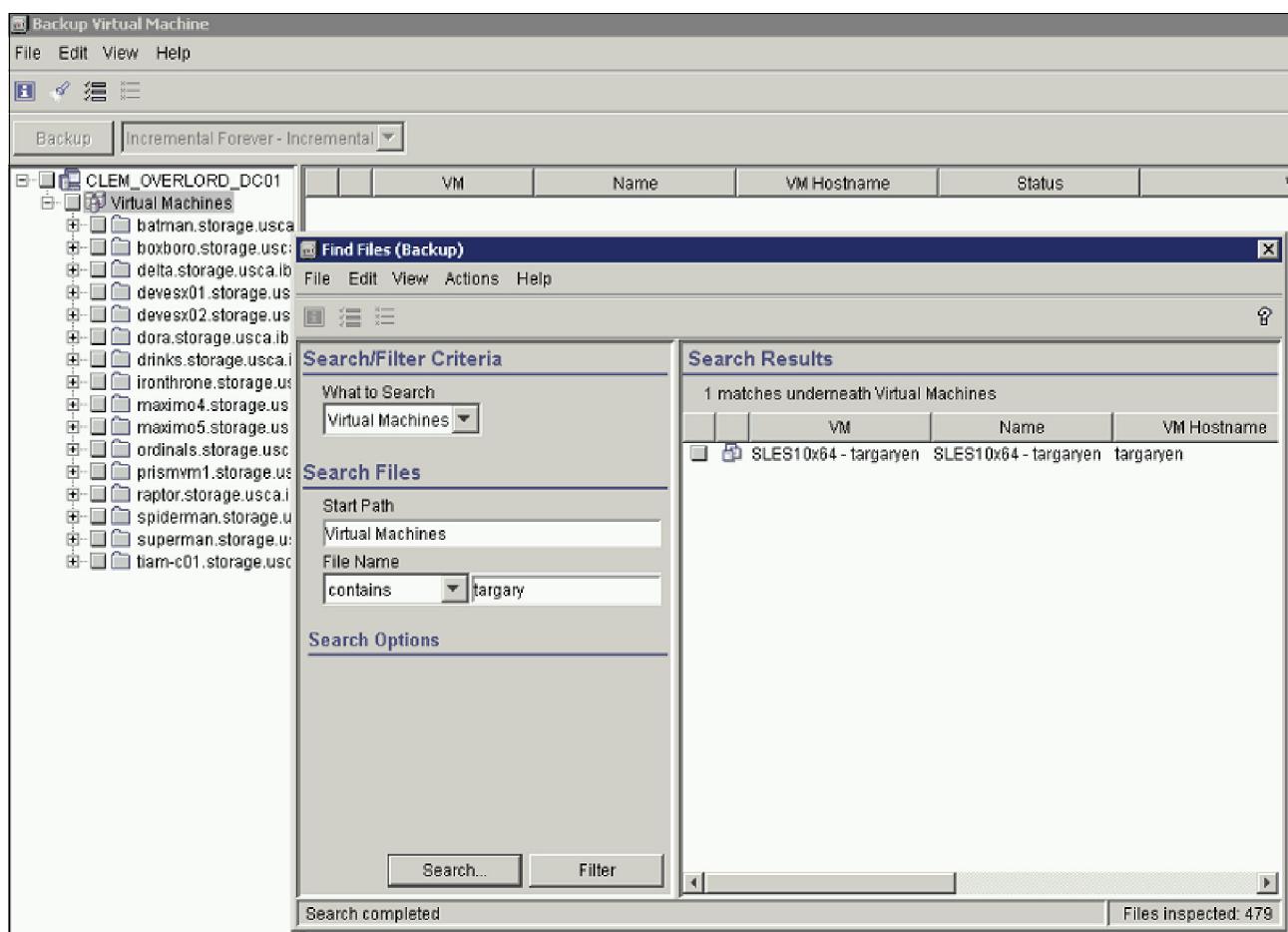


Figure 5-10 Search menu to find your virtual machine

- When you select your VM (one or many), choose the backup mode (see Figure 5-11) and click **Backup**.

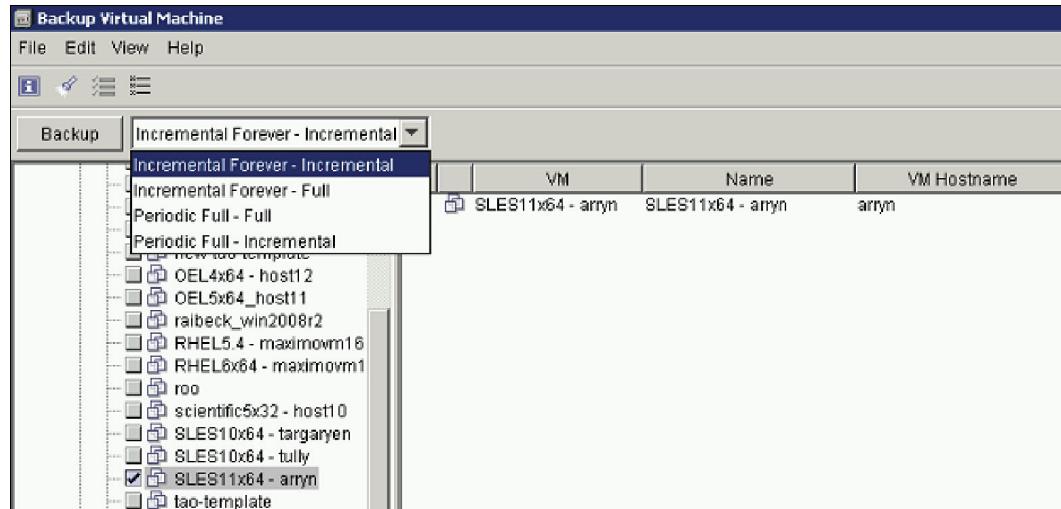


Figure 5-11 Select backup mode

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 Datamover 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.

You can control the mode by specifying the **-mode** parameter. Choose among IFFULL (Incremental Forever Full) and IFINCR (Incremental Forever Incremental).

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 the '**-domain.vmfull**' option with the following parameters: **a11-vm**, **a11-windows**, **vmhost**, **vmfolder**, **vmhostcluster**, **vmdatasstore**, **vmresourcepool**, **vmhostfolder**, **vmdatcenter**.

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 (dsm.opt) is 6000.

For more information, see the following IBM Technote about [using long specifications](#).

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: vmd datastore=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: vmd datastore=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: vmd datastore=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: vmd datastore=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: vmd datastore=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: vmd datastore=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: vmd datastore=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: vmdatadstore=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'  
2013-02-18T18:19:36.060-08:00 [2B8AD65727C0 verbose 'ThreadPool'] Thread info: M  
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*'.  
targaryen:/opt/tivoli/tsm/client/ba/bin #
```

```
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 tsmpl in their name.

Example 5-5 Backup of all virtual machines with tsmpl 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
viossadec.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=VIOSSEDCEC.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 Protection for in-guest applications

As described in 3.3, “Protecting applications in a virtual environment” on page 35, 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 IBM Spectrum Protect server completed successfully. As a result, logs were not truncated on the application server. In the current version, logs are truncated by default.

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.

For more information, see the [Virtual machine include options](#) technote on this function in IBM Knowledge Center.

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 IBM Spectrum Protect 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 an IBM Spectrum Protect Data Protection agent.

If you exclude disks from a backup, do not alternate backups of the same guest with the disks included.
- ▶ 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 IBM Spectrum Protect server.

If a deduplication cache is defined but the amount of data is large the deduplication cache may be exceeded which will cause the cache to be reset and impact backup performance.

If protecting a large amount of data with a deduplication cache it may be necessary to split the backup across multiple datamovers. Only one cache may be defined per data mover.

For more information, see the [Client-side data deduplication](#) topic in IBM Knowledge Center.



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 Spectrum Protect server as well as to reduce the backup window by using the datamover client multi-session, deduplication, and compression features.

This chapter includes the following topic:

- ▶ Backup scheduling

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 IBM Spectrum Protect 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 (optimized backup) enables a larger VMware environment to be protected with fewer vStorage backup servers. With IBM Spectrum Protect Data Protection for VMware 8.1, optimized backup support is available at a VM level or at the VMDK level to support a variety of [client options](#).

6.1.1 Backup schedule and backup strategy

Previous to version 8.1 two backup mode approaches were available, periodic full, and incremental forever. With version 8.1, periodic full backups are no longer supported. The following approach is 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 using this method, you must create only one schedule and specify the IFFINCR backup mode. The first backup that is done is an Incremental Forever Full (IFFULL), and every subsequent backup is Incremental Forever Incremental (IFFINCR).

For more information about the Incremental Forever backup strategy, see 3.5, “Enabling the backup strategy” on page 40.

For more information about [scheduling with Tivoli Storage Manager for Virtual Environments](#), see the IBM developerWorks wiki.

6.1.2 Backup scheduling and VMware tags

With the most recent versions (starting with 7.1.6) of IBM Spectrum Protect for VMware, together with VMware vSphere 6 update 1 or later release, the use of a VMware tag is possible to facilitate the backup management, and therefore the backup scheduling.

The VMware tag allows you to attach metadata to objects in the vSphere inventory to make these objects more sortable and searchable.

If you use the IBM Data Protection extension to manage backups, you can exclude virtual machines from backup operations or set the retention policy of virtual machine backups.

If you use the data mover, use the `vmtagdatamover` option to enable tagging support in the datamover client. When this option is enabled, the client manages backups of VMware virtual machines according to the backup management tags that are set by the IBM Data Protection extension of the vSphere Web Client. These tags can also be set with other tools, such as VMware vSphere PowerCLI version 5.5 R2 or later.

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

While tagging was available in version 7.1.6, it has been greatly expanded in version 8.1. More details about [data protection tagging](#) are available in IBM Knowledge Center.

Tags are interesting for the scheduling because they represent a new key to filter the virtual machines to be backed-up. Using a tag simplifies the exclusion of virtual machines, and can also be used by external scheduling scripting methods. See Figure 6-1 for an example of how you can configure backups using VMware tags in the vCenter web client.

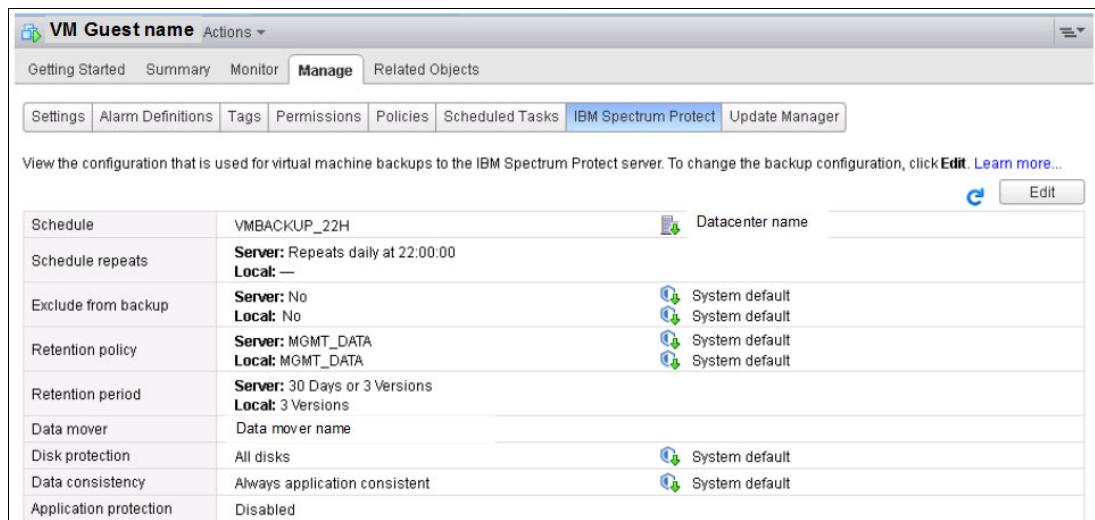


Figure 6-1 Configuring backups using VMware tags in vCenter web client

6.1.3 Fine-tuning the IBM Spectrum Protect server

The IBM Spectrum Protect server must be properly configured to manage the incoming VM backup data, especially when a large quantity of sessions 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**
- ▶ **Maxnummp**

For the datacenter nodes that carry and hold the data in the IBM Spectrum Protect server, you might tune the following parameters:

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

Note: 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; which is connected during the backup (`asnode name` option). Take note of the available tuning options in the [Session settings and schedules for a proxy operation](#) topic on IBM Knowledge Center.

6.1.4 Fine-tuning the datamover

As with options to tune on the IBM Spectrum Protect server side, you have some options on the datamover 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`

6.1.5 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 IBM Spectrum Protect server administrative interface (command-line or Operation Center GUI). The scheduling of backups should be carefully planned.

Schedules that are created with the vCenter plug-in can be viewed through the IBM Spectrum Protect server administrator interface. However, schedules that are created directly via the IBM Spectrum Protect 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 is used instead.

Note: The VM list cannot exceed 512 characters, as shown in Figure 6-2.

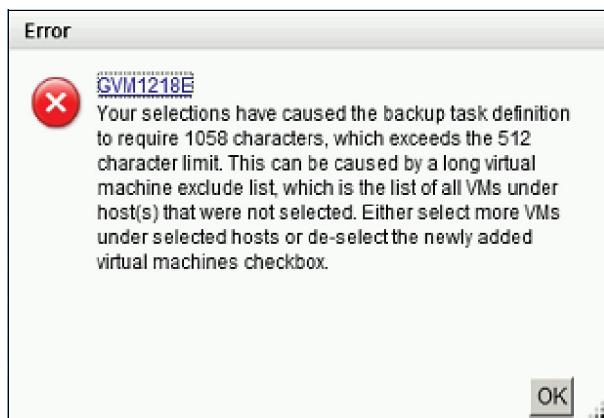


Figure 6-2 Error message: VM list is too long

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 Datamover Client command line” on page 71.

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 IBM Spectrum Protect 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 6-3.

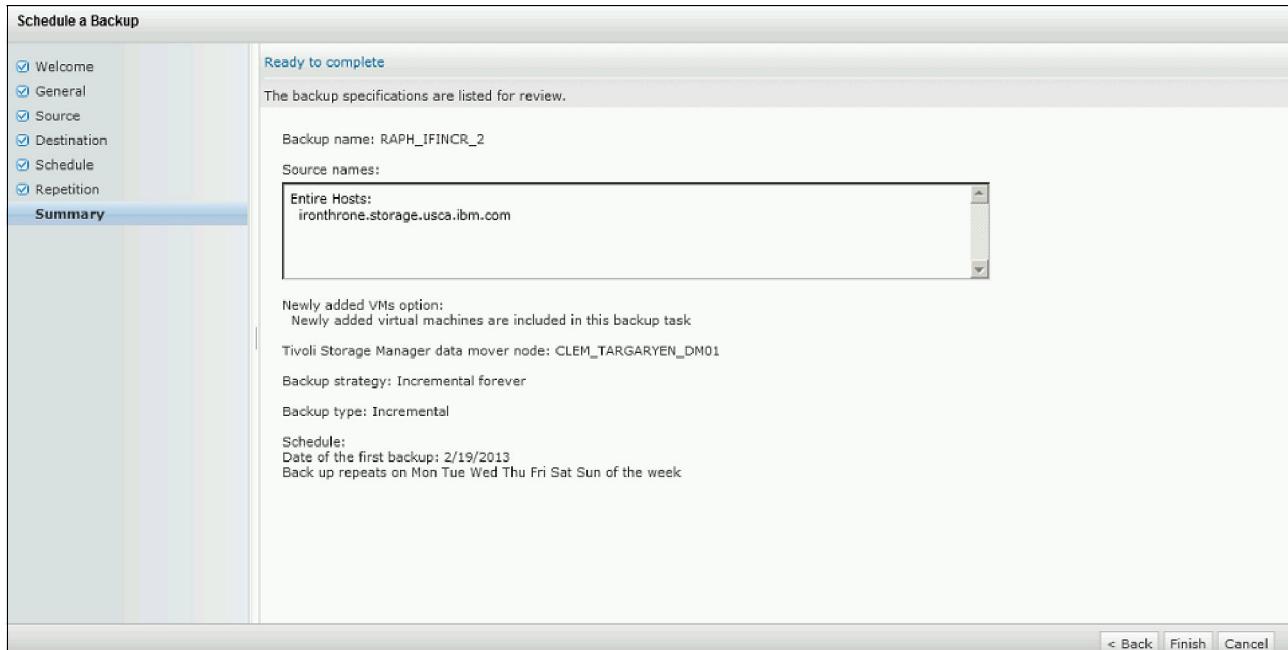


Figure 6-3 Define a backup schedule

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

The following corresponding commands are sent by the plug-in to the IBM Spectrum Protect server:

```
DEFINE SCHEDULE RAPH RAPH_IFINCR_2 Type=Client DESCription='IFINCR of ironthrone
virtual machines' ACTion=Backup SUBACTion=VM OPTions='-vmfulltype=vstor
-vmbackuptype=fullvm -asnodename=CLEM_OVERLORD_DC01
-domain.vmfull="VMHOST=ironthrone.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
```

6.1.6 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 6-4.

The screenshot shows a software interface titled "Managing backup schedules". At the top, there's a navigation bar with tabs: Getting Started, Summary, Backup (which is selected), Restore, Reports, and Configuration. Below the title, there's a brief description: "Create a backup schedule that takes snapshots of the virtual machines and sends them to Tivoli Storage Manager server storage." and a "Learn more..." link. The main area displays a table of backup schedules:

Schedule	Type	Last Ran
IFNCR_tsmctw in10	TSM_IFNCR	February 18, 2013 8:19:56 PM PST
RAPH_IFNCR_2	TSM_IFNCR	

A context menu is open over the "RAPH_IFNCR_2" row, showing three options: "Delete" (with a red X icon), "Properties" (with a gear icon), and "Run now" (with a play icon).

Figure 6-4 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.

New with version 8.1.2:

You can use the `schedgroup` client option to create a group that contains multiple schedules. You can then use the IBM Spectrum Protect vSphere Client plug-in to assign the schedule group to an object in the VMware vSphere Web client rather than an individual schedule. An example of the use of this option is to group multiple daily local backup schedules with a single IBM Spectrum Protect server backup schedule.

More `schedgroup` option details can be found in IBM Knowledge Center.



Virtual environment recovery

This chapter provides guidance on how to recover your data, whether it is an entire virtual machine (VM), a file within a virtual machine, an entire datastore or even an application item (for example, MS-SQL database).

The chapter covers all the scenarios available when using either IBM Spectrum Protect Data Protection for VMware or IBM Spectrum Protect Snapshot for VMware and describes the step-by-step procedures to do these activities:

- ▶ Restore a full virtual machine
- ▶ Restore files to a virtual machine
- ▶ Volume (disk) Recovery for a virtual machine
- ▶ Restore a datastore
- ▶ Fast revert from local backup (vVol persistent snapshot)

The two available restore interfaces also are described in this chapter.

This chapter includes the following topics:

- ▶ Overview of recovery procedures
- ▶ Overview of recovery procedures using IBM Spectrum Protect for Snapshot for VMware

7.1 Overview of recovery procedures

Data Protection for VMware provides the following restoration modes:

- ▶ Full VM restoration
- ▶ File-level restoration
- ▶ Virtual machine instant restore/instant access
- ▶ Other supported item level recovery (for MS-SQL and Exchange objects)
- ▶ Fast revert from local backup (vVol persistent snapshot)

Depending on what type of recovery you want to perform, you might leverage different interfaces from different places. Table 7-1 gives you the starting place for the recovery procedure.

Table 7-1 Starting point for recovery procedure

Task (where to start recovery)	vBS (datamover proxy)	Guest (within VM)	vSphere	Anywhere
FULL VM Restore	Using Baclient	N/A	Using vCenter plug-in (IBM Data Protection contextual menu)	Using web-based or vCenter plug-in
FULL-VM and Volume Instant Restore	N/A	Using web-based interface	Using vCenter plug-in	Using web-based or vCenter plug-in
File level restore	Using new web-based FLR interface or DP for VMware Recovery Agent	Using new web-based FLR interface or DP for VMware Recovery Agent	Using vCenter plug-in (manual mount operations)	Using FLR web interface or by setting up a Recovery Agent
MS-SQL Database Recovery	N/A	Data Protection for SQL 7.1 and DP for VMware Recovery Agent	N/A	N/A
MS Exchange mailbox item recovery	N/A	FastBack for MS Exchange and DP for VMware Recovery Agent	N/A	N/A
Who is doing the operation?	IBM Spectrum Protect Admin	Virtual machine admin/user	User or VMware Admin	User

7.1.1 Recovery scenario selection use cases

There are several possibilities to recover your data. To help you make the appropriate decisions on which interfaces (Table 7-1) to use when it comes time to recover data, consider the following information:

- ▶ If you need to recover a file or set of files. It is better to use the File Level Recovery (FLR) interface from any place you want. Including the target virtual machine is not necessary. This interface allows you to find the file using the search feature of the FLR interface. This approach could be useful if you or the requester are not sure where the file was, for example in case of deletion.

- ▶ If you need to recover a drive or file system (from an operating standpoint) there are different options, depending on volume layout, the options are:
 - If the drive for a Windows virtual machine (or file system for a Linux virtual machine) is spanned between multiple VM's disk file (VMDK), you should use the Mount options from the vCenter plug-in or web-based DP for VMware user interface. In this case, a wizard guides you to make the data available as a network share to the target virtual machine (managing all of the required .vmdk files to be mounted, whatever the layout).
 - If the drive or file system to recover is large (for instance, if it represents more than 50% of the total virtual machine size), you would better off restoring the whole virtual machine using either the command line or web-based interface, then attaching the restored .vmdk file to the target virtual machine to proceed with data recovery.
- ▶ If you need to recover an entire VMDK, you have two options depending of the size and amount of data to be recovered. The first option works well when the VMDK is large, or when the number of files and folder is large. The second option works in a situation where not much data needs to be restored:
 - You can restore the entire virtual machine and then attach the restored VMDK to the existing running virtual machine. Then you have the data available for copy to original location, or you can decide to keep this new vmdk as running one and proceed with deletion of the old one.
 - You can use the File Level Recovery interface, select all the files and directories needed, and restore them onto the virtual machine. Keep in mind that the time required for processing the volume level information might slow down this process, especially if the volume contains lots of entries (directories and files)
- ▶ If you need to recover the entire virtual machine, you have three options, all of which can be done through the command line interface or web user interface:
 - The first option is to do a standard virtual machine recovery.
 - The second option is to restore the virtual machine using the “instant restore” mode. This way, you bring the virtual machine online within a minute for end user operations, while data is moved from IBM Spectrum Protect server storage to VMware datastore (using storage vmotion).
 - The third option is to use the “instant access” mode. This option enables you to access the virtual machine within a minute to perform validation and other integrity testing or any read-only operations. Notice that when using this recovery mode, all write operations are temporary and are not committed. This is a temporary space, and all modifications will be lost when the virtual machine is stopped (that is, when stopping the instance access operations)
- ▶ If you need to validate a backup, the most efficient way is to use the instant recovery option. It can be initiated through the IBM Spectrum Protect web interface.

To summarize, whatever the type of restoration you need, first consider the size of the data to be recovered, because that leads you to different recovery methods.

7.1.2 Performance considerations

For recovery tasks, there are two things to be considered from a performance perspective: Data Transport and VMDK type.

Data transport

Data transport is basically the media used to transfer the data between the datamover client and the VMware datastore.

For recovery, the most efficient transport observed from various testing is NBD (IP-network based). This VMware vSphere [Documentation Center](#) gives in-depth information about what transport to use for recovery.

From an IBM Spectrum Protect client perspective, this is controlled by the VMSTORTRANSPORT option within the datamover option file (or directly at the command line). The transport used for recovery is not related to transport used at backup time, thus, recovery transport can be different than the one used for the backup.

Thick or Thin VMDK

When creating a .vmdk file for a virtual machine (VM), you have the choice between Thick EagerZeroed, Thick LazyZeroed, or Thin VMDK type. Thick disks occupy the entire space, including unused space in the overlaid file system, and are therefore not efficient with space utilization. Thin disk consumes only the space used by the overlaid operating system or application, but have underlying performance concerns for high-I/O workloads.

There might be a performance impact on recovery operations when you use thick eager zeroed rather than thick lazy zeroed or thin VMDK file. However, if your back-end disks system is supported for hardware acceleration, such as vSphere Storage APIs - Array Integration (VMware VAAI), this is not an issue.

The purpose of the VAAI is to offload some tasks which are using resources, from the ESXi host to the back-end disk system. This is the case for the zeroing operation. When provisioning an eagerzeroedthick VMDK, a SCSI command is issued to write zeroes to disk blocks. Again, this initialization request uses host resources, such as CPU cycles, DMA buffers, and SCSI commands in the HBA queue.

One of the most common operations on virtual disks is initializing large extents of the disk with zeroes to isolate virtual machines and promote security. ESXi hosts can be configured to enable the **WRITE_SAME** SCSI command to zero out large portions of a disk. This offload task will zero large numbers of disk blocks without transferring the data over the transport link, so the zeroing operation takes much less time than without VAAI.

The hardware acceleration support can be determined using the vSphere web interface, or by entering the command line shown in Example 7-1 on page 92.

Figure 7-1 shows the back-end devices and Hardware Acceleration support status.

Name	Type	Capacity	Operational State	Hardware Acceleration	Drive Type	Transport
IBM Fibre Channel Disk (naa:600507680c8080129800...)	disk	2.00 TB	Attached	Supported	Non-SSD	Fibre Channel
IBM Fibre Channel Disk (naa:600507680c8080129800...)	disk	2.00 TB	Attached	Supported	Non-SSD	Fibre Channel
LSI Serial Attached SCSI Disk (naa:800509e000000000...)	disk	58.67 GB	Attached	Unknown	SSD	Block Adapter
IBM Fibre Channel Disk (naa:600507680c8080129800...)	disk	2.00 TB	Attached	Supported	Non-SSD	Fibre Channel

Figure 7-1 Back-end devices and Hardware Acceleration support status

The command line (Example 7-1) shows that the **HardwareAcceleratedInit** feature is enabled, so the zeroing operation is optimized (when creating lazy zeroed VMDK).

Example 7-1 HardwareAcceleratedInit

```
~ # esxcli system settings advanced list --option /DataMover/HardwareAcceleratedInit  
Path: /DataMover/HardwareAcceleratedInit
```

```
Type: integer
Int Value: 1
Default Int Value: 1
Min Value: 0
Max Value: 1
String Value:
Default String Value:
Valid Characters:
Description: Enable hardware accelerated VMFS data initialization (requires
compliant hardware)
~ #
```

If the VMware attached back-end disk system does not support the HardwareAcceleration, the choice between Thick Lazy Zeroed and others (Thin or Thick Lazy Zero) becomes critical because it has a great impact on recovery performance.

Thin disk will improve the time to recover the data, which might be interesting if the disks to create are large in size and not filled up. It has to be carefully decided, because it could have an impact on virtual machine I/O performance afterwards. However, if for some reason performance is too bad for production use, you can still ask the VMware administrator to convert the thin disk to a thick disk afterwards. Note that it will be an offline operation.

If the VMware attached back-end disk does support the HardwareAcceleration, there is a small performance effect between all of these Thick/Thin vmdk modes.

Thick VMDK should be used in most cases.

I/O activity consideration while doing instant restore operations

As you would expect, any intense I/O activity on a virtual machine (when doing virtual machine instant recovery) or against a datastore (when doing virtual machine recovery) has a significant effect on recovery performance.

It is worth mentioning that for virtual machine instant recovery, you should avoid doing too much modification (I/O activity) to the virtual machine because of the mechanism involved in such cases. If too many changes occur on that particular virtual machine, the delta file (which is created by VMware Storage vMotion while copying the data from the iSCSI target to its final datastore) might reach the 8 TB limitation as of v7.1 and cause the process to hang or crash.

7.1.3 Full VM restoration

Full VM restoration can be accomplished by using the backup archive client GUI, the command-line interface, the Data Protection for VMware web-based interface, or the contextual menu available when the IBM Spectrum Protect for Virtual Environment plug-in is deployed on the vSphere center server.

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 IBM Spectrum Protect server to the datastore.

Depending on the backup proxy location, you can decide to restore the data from the IBM Spectrum Protect server to the VMware datastore using either HotAdd, LAN, or SAN transport. Usually, LAN transport performs better than the other options. The transport selection can be configured in the datamover's option file with the **VMVSTORTRANSPORT** parameter.

Full VM restoration using the vSphere web interface

To recover an existing Virtual machine (still registered within the vCenter server) to a previous state, complete the following steps:

1. On the VMware vSphere Web Client shown in Figure 7-2, right-click the VM that you want to restore and select **All IBM Data Protection Actions** → **Restore**.

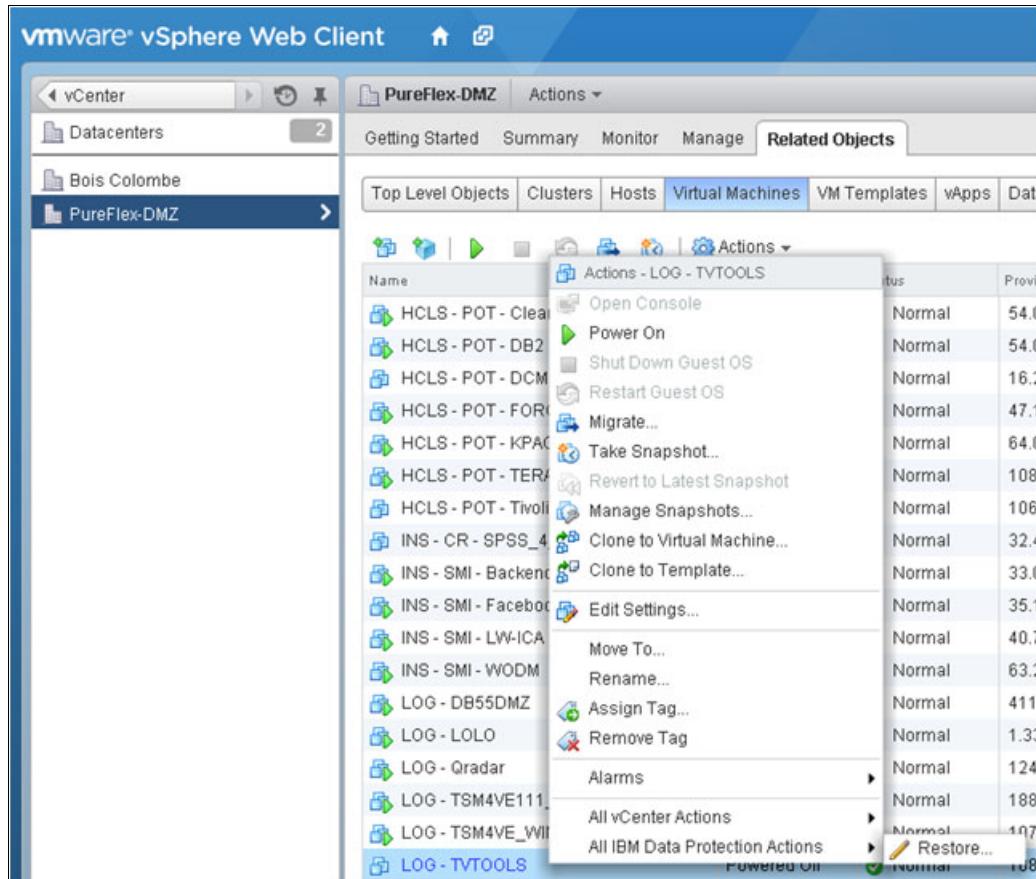


Figure 7-2 Main menu

2. Select the wanted Restore Point (Figure 7-3).

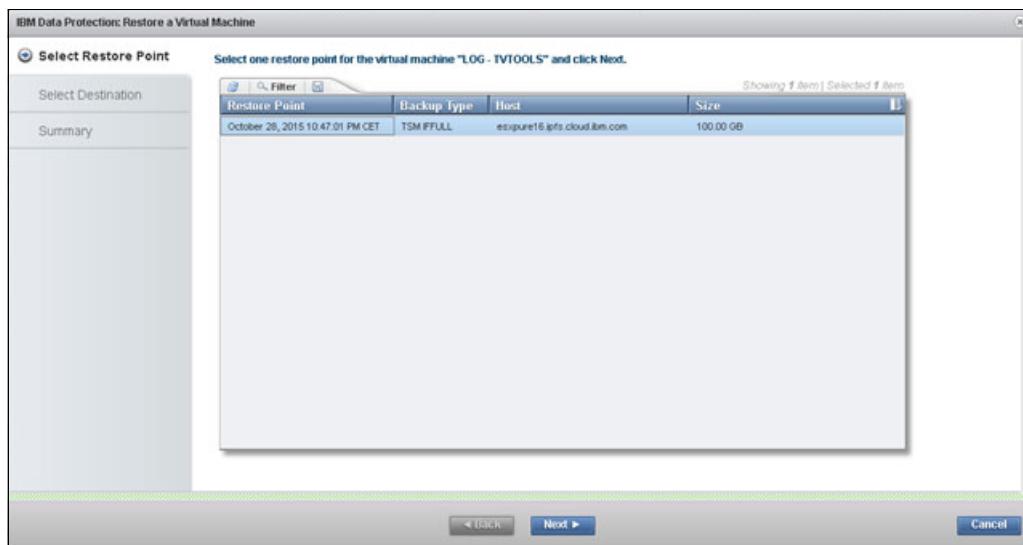


Figure 7-3 Select restore point

3. Click **Select Destination** (Figure 7-4) and select from the provided options.

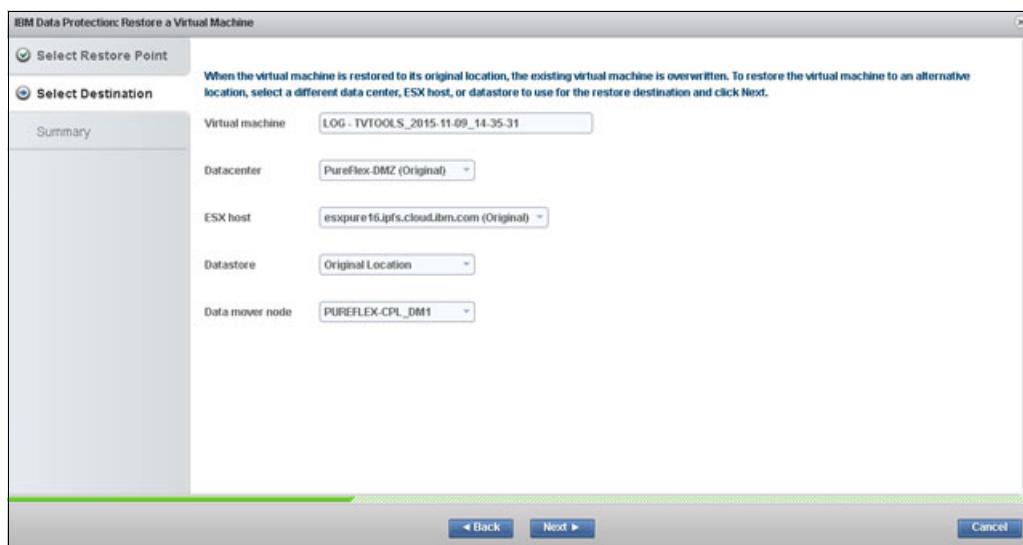


Figure 7-4 Select destination

Full VM restoration using Data Protection for Vsphere web interface

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.

The first activity is to log into the Data Protection for VMware screen (Figure 7-5).



Figure 7-5 Data Protection for VMware log in

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. Browse and select the VMs that you want to restore.
3. Choose your snapshot date (Figure 7-6).

The screenshot shows the "Restore Points" screen of the Data Protection for VMware interface. At the top, there is a navigation bar with tabs for "Getting Started", "Backup", "Restore", "Reports", and "Configuration". Below the navigation bar, there are three status indicators: "Restore Points", "Instant Access/Restore Status", and "Mount Status". The main area is titled "Restore Points" and features a thumbnail of a document with a red arrow pointing to it. To the right of the thumbnail is a table titled "Restore Point". The table has columns for "Restore Point", "Template", "Backup Type", and "Location". There are two rows in the table:

Restore Point	Template	Backup Type	Location
November 7, 2015 3:17:12 AM CET	No	IFINCREMENTAL	192.168.60.9
November 4, 2015 3:12:58 PM CET	No	IFINCREMENTAL	192.168.60.9

Figure 7-6 Choose snapshot

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. Click **Full VM Restore** among the proposed options and click **Next**.
5. Source information is displayed per your previous snapshot selection. Click **Next**.
6. Select the restore destination (**Original** or **Alternate Location**).

- If you selected **Restore to alternate location**, enter the VMware vSphere (ESXi) host name, the new VM Name (if only one VM is selected), and the datastore and datacenter (Figure 7-7).

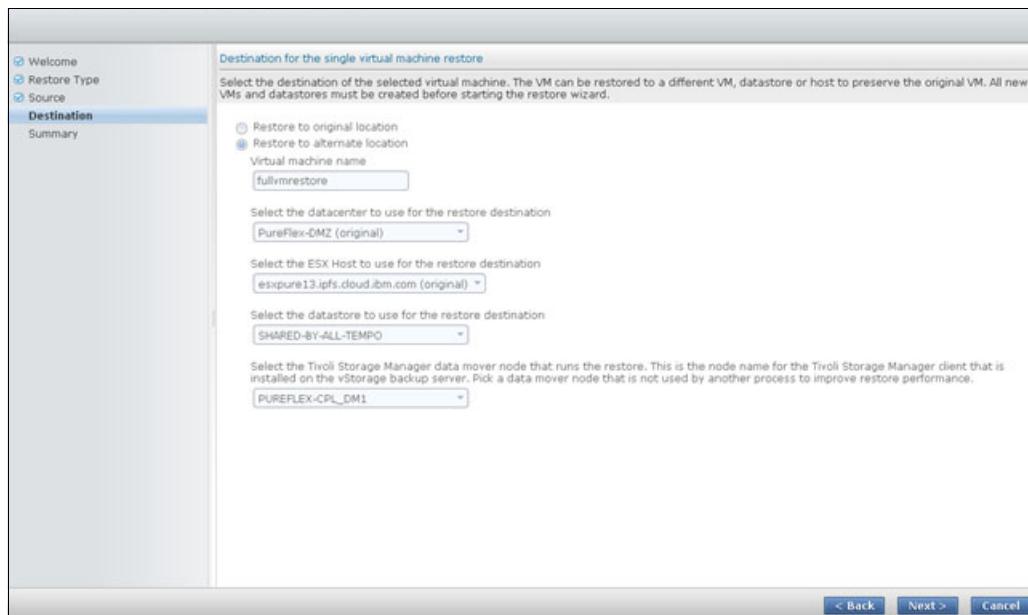


Figure 7-7 Select alternate location

- You can follow the restoration process by using the Recent Tasks panel of the Reports tab (Figure 7-8).

Name	Progress	Details	Start Time
Full Restore (6664)	Processed 72.69 MB	Processing virtual machine: 1 / 1	November 10, 2015 11:36:45 AM CET

Task Details

Task Name: Full Restore (6664)
Source VM: LOG-TSM4VE_WINMP
Task Type: Restore
Task Creation Time: November 10, 2015 11:36:45 AM CET
Datacenter Node: PUREFLEX-CPL_VS55DMZ
Server: 192.168.60.9
Virtual Machines Processed: 0
Virtual Machines Failed: 0

Task ID: 6664
Target VM: fullvmrestore
Back End Type: TSM
Status: Running
Data Mover Node: PUREFLEX-CPL_DM1
Bytes Processed: 72.69 MB
Virtual Machines Restored: 0

Figure 7-8 Restoration process

The information about the recovery process is available to the VMware administrator, within the Vsphere web interface. As you would do with the IBM Spectrum Protect for VMware web interface, you can track the progress of the recovery and the expected size of the VM to be recovered (Figure 7-9).

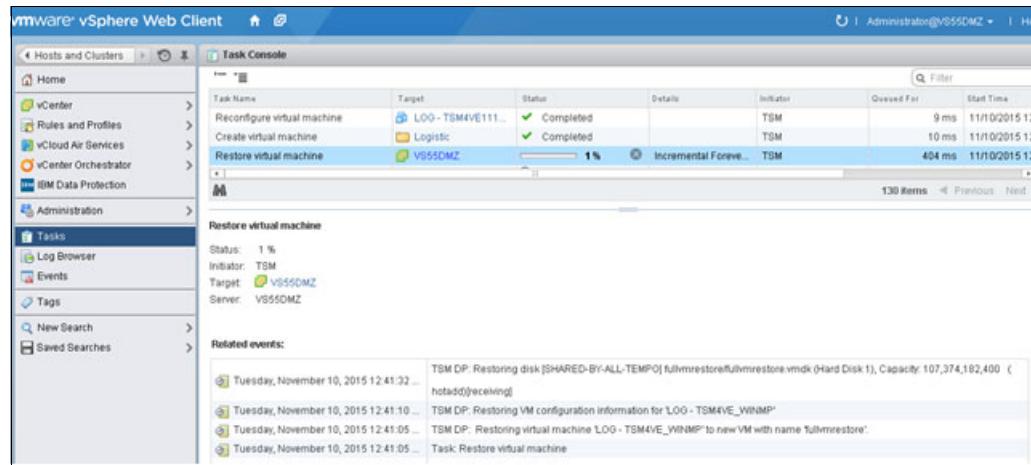


Figure 7-9 Track recovery progress

When the operation is completed, the web interface shows it as a completed task, including all statistics regarding the amount of data transferred and performance and location indications.

The virtual machine can be powered on and resume to normal operations.

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.
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 Click **Next**.
5. Select the restore destination (**Restore to original** or **alternate location**).
6. If you selected **Restore to alternate location**, enter the ESXi host name, the new VM Name (if only one VM is selected), the datastore, and datacenter. Click **Next**.
7. Review the summary and click **Finish** when complete. You can follow the restoration process by using Recent Tasks panel of the Reports tab.

Full VM restoration by using Backup-Archive client UI or command line

If for some reason you prefer to use the command line or the traditional backup-archive client user interface to recover a virtual machine, this is still possible.

All of the steps required to recover a virtual machine using command line or backup-archive client user interface are explained in the official [IBM Spectrum Protect publications](#).

Be aware that virtual machine recovery operations is part of the baclient documentation, because it does not leverage any of the IBM Spectrum Protect for VMWare features.

Information about the command line for IBM Spectrum Protect for VMware operations (such as instant restore, instant access, and so on) is on the [vmrestoretype page](#) in IBM Knowledge Center.

7.1.4 Virtual machine instant access

The purpose of instant access is to give you access to the virtual machine within a minute, but solely for read-only purposes. To enable this feature, refer to the official documentation describing all of the environment requirements and steps to [configure your environment for full virtual machine instant restore operations](#).

This is a very good feature to perform recovery assessment or any validation test to ensure that your backups are properly done. If you need that virtual machine to remain online after your testing, it is better to use the virtual machine instant restore, which is described later in this document.

The instant access process uses the iSCSI method to present the VMDK and virtual machine's system file on the datastore that was specified when creating the instant access, through the wizard. When the instant access is done, the virtual machine is powered on using the files virtually stored on datastore. Figure 7-10 shows you the steps and components used to perform an instant access operation.

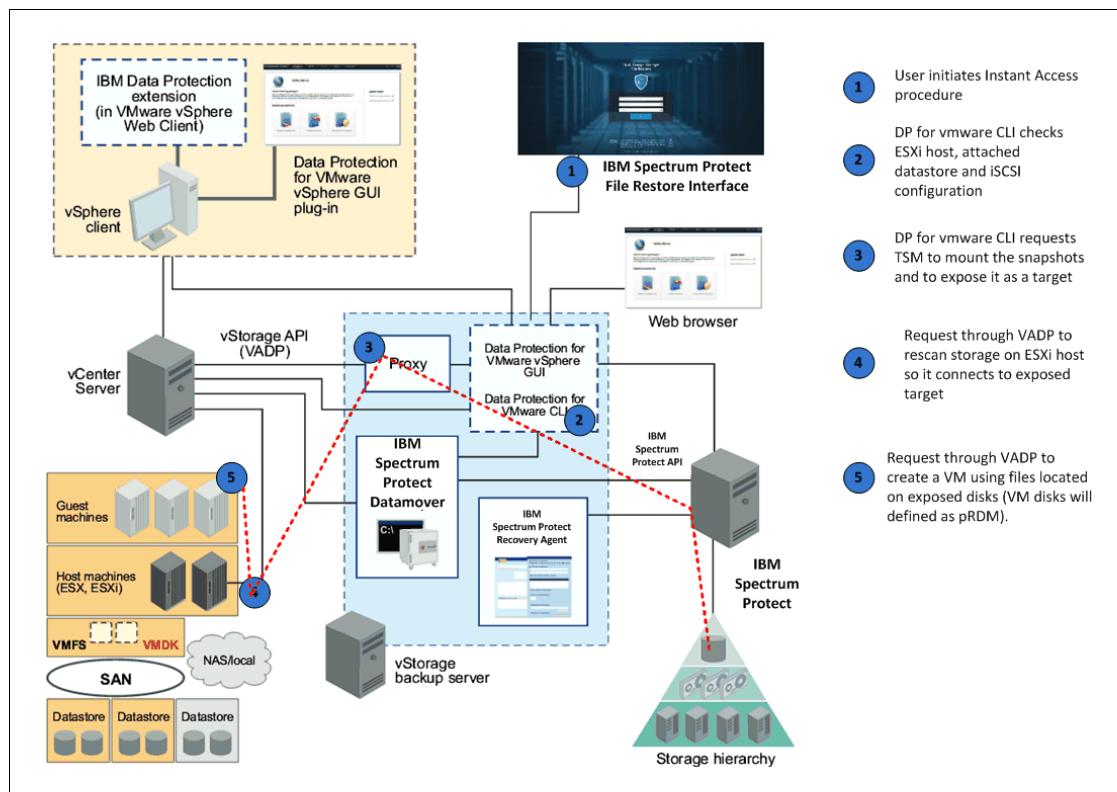


Figure 7-10 Instant access operation flow

After you have completed all of the operations, power off the virtual machine and perform cleanup actions using the web interface wizard. The cleanup steps include removing the virtual machine from inventory, disconnecting the iSCSI target from ESXi hosts, and dismounting the snapshot from the IBM Spectrum Protect server.

To perform an instant access using the web interface wizard, complete the following steps:

1. Open and connect to the web-based interface, which is the same as the previous menu from the web interface.
2. Select the appropriate mode for recovery, which in this case is **Full VM Instant Access**. You have the option to specify whether the VM should be automatically powered on (Figure 7-11).
3. Enter all required VMware environment information where the instant access takes place, such as Datacenter, Datastore, ESXi Host, and Virtual Machine Name.

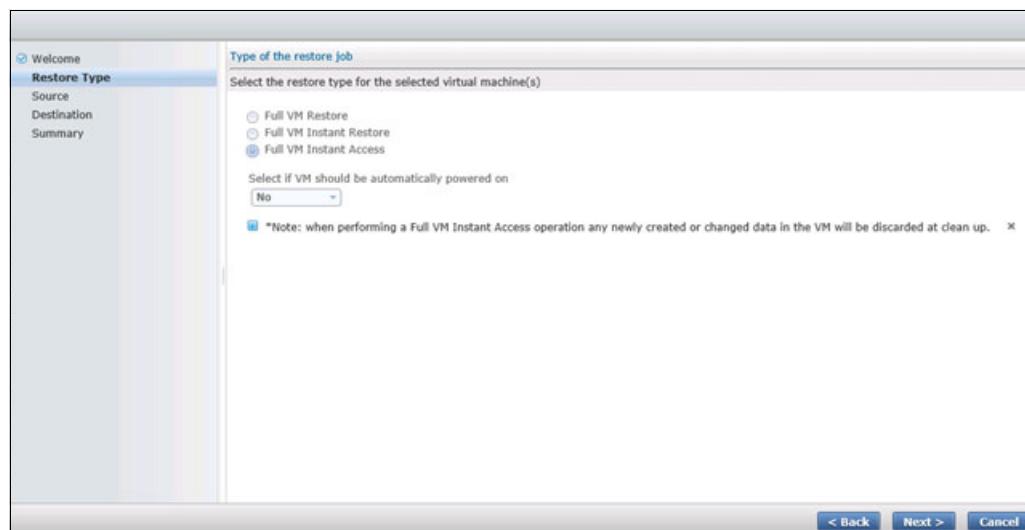


Figure 7-11 Select restore type

Figure 7-12 shows the iSCSI target details, accessible through the ESXi host configuration properties, within the Storage Adapters section.

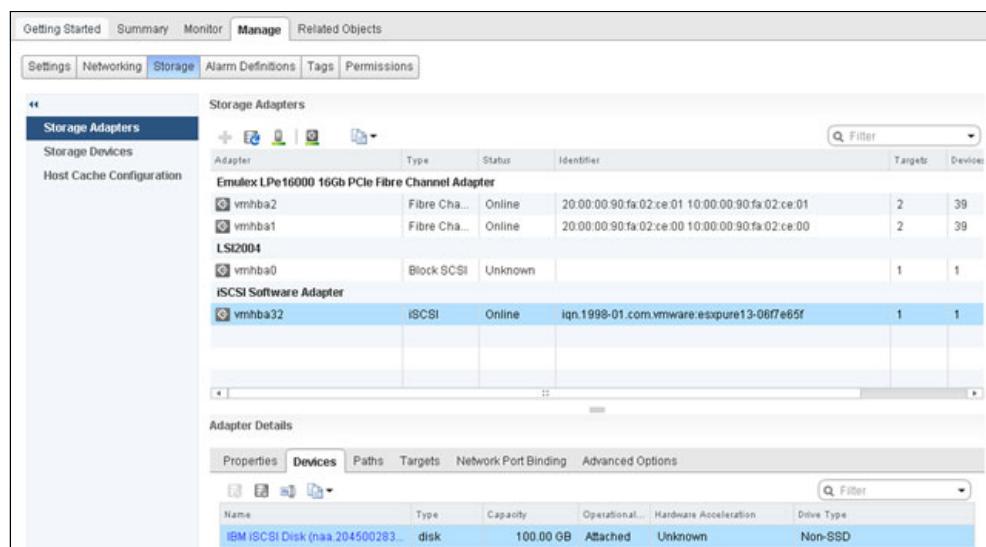


Figure 7-12 iSCSI target details

On that same view, in the Targets tab within the Adapter details section, you can see the IP address of the iSCSI target, basically the Mount Proxy (Windows mount proxy). The iSCSI target is exposing the volume from IBM Spectrum Protect Server to the ESXi hosts, making the virtual machine instantaneously accessible for user operations.

Figure 7-13 shows the view on the IBM Spectrum Protect for VMware web interface side, the proof that there is an instance access process running.

Start Time	Restore Type	Status	Action Needed	ESX Host	Source VM	Target VM
11/10/2015 14:38:06	Instant Access	<input checked="" type="checkbox"/> Success	Dismount	espxre13.pts.cloud.ibm.com	LOG - TSM4VE_WI...	testinstanceaccess

Figure 7-13 Instance access process running

4. On that same view (Instant Access/restore Status) you can gather more detailed information by selecting one of the available operations and clicking **VM details** above the list. You see detailed information of the Virtual machine state and disks (Figure 7-14).

[0] VMDK Disk	Disk Name:	Hard disk 1
	Disk Type:	RDM or SAN
	Disk Size:	104,857,600 KB
	Disk Mode:	persistent
	Disk File Name:	[SHARED-BY-ALL-TEMPO] testinstanceaccess/testinstanceaccess-000001.vmdk
	UUID:	02000000000204500283eeb558f5265636f7665
	Device Name:	vml.02000000000204500283eeb558f5265636f7665
	Disk Path:	Active
	iSCSI Address:	192.168.60.103:3260
	iSCSI Name:	testinstanceaccess-hard5disk01

Figure 7-14 VM details

5. After the validation or any operations required to be run against that virtual machine are over, the instant access must be dismounted. To do so, power off the virtual machine and go back to the IBM Spectrum Protect for VMware web interface to proceed with the dismount steps.
6. On the “Instant Access/Restore status” panel, click the appropriate line containing the virtual machine that you want to remove and click **Dismount**.

The dismount triggers the following operations on the VMware side (Figure 7-15):

1. Delete virtual machine.
2. Rescan HBA (to refresh iSCSI targets).

Task Name	Target	Status	Details	Initiator	Oversub For	Stat
Remove Internet iSCSI static targets	esposure13.ipfs.clo...	Completed		TSM	33 ms	11/1
Rescan HBA	esposure13.ipfs.clo...	Completed		TSM	3 ms	11/1
Delete virtual machine	testinstanceaccess	Completed		TSM	6 ms	11/1
Initiate guest OS shutdown	testinstanceaccess	Completed		Administrator	10 ms	11/1

Figure 7-15 Task Console

7.1.5 Virtual machine instant recovery

Unlike instant access, instant recovery allows you to recover the virtual machine in a minute and to keep it running afterwards, with any modification you could make against that same virtual machine whilst restore is running in background.

Indeed, the instant recovery brings the virtual machine online for you to resume business as quickly as possible, and performs a storage vMotion in the background in order to move the data back to a vSphere datastore. Storage vMotion copies the data from the IBM Spectrum Protect for VMware exposed targets to its traditional datastore.

Within a minute after starting an instant restore, the virtual machine is ready for read/write operations, while the restore is in progress in the background.

Figure 7-16 shows the steps and components involved in an Instant restore operation.

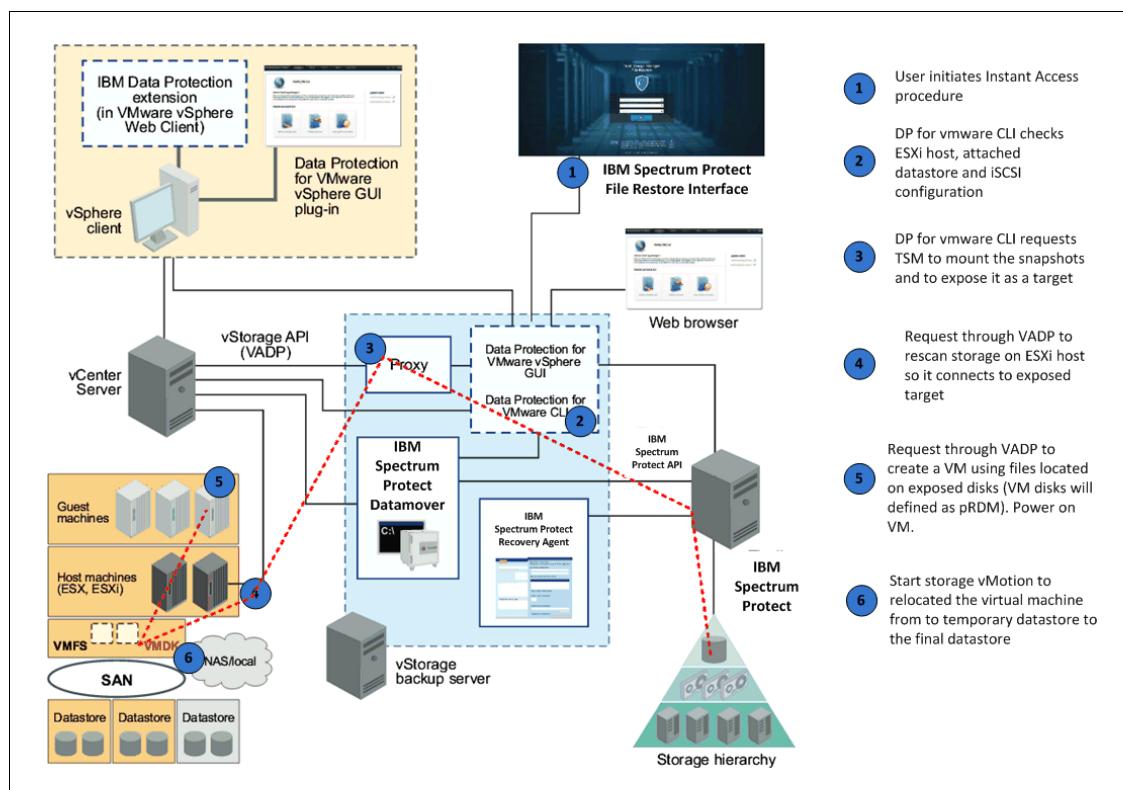


Figure 7-16 Instant restore flow

To start an instant recovery process, open the IBM Spectrum Protect for VMware web interface and go into Restore | Restore points. Browse and select the virtual machine that you want to recover, select the appropriate snapshot date, and click **Restore** → **Instant restore**.

After you start the Instant restore operation, you can see the progress, first in the Recent Tasks tab, and later on the Restore tab and the Instant Access/Restore status tab.

Figure 7-17 shows details of the Recent Task tab, at the beginning of the Instant Restore operation.



Figure 7-17 Details of the Recent Task tab

As soon as the first metadata is restored, the virtual machine is powered on, a virtual machine snapshot is performed, and the storage vMotion is triggered to move the data from the IBM Spectrum Protect target volume to the vSphere datastore, the one that you provided in the wizard.

In the IBM Spectrum Protect for VMware web interface, if you go to the Restore tab, you do not see the status of an instant restore because this view shows only ongoing instant access or failed instant restore. To monitor the progress, you can either check it by using the command line or by using the vSphere web interface in the task view.

Figure 7-18 shows an example of a command-line query from the mount proxy, giving the list of instant restore ongoing.

```
c:\Program Files\Tivoli\TSM\baclient>dsmc query vn * -UMRESToretype=instantr -optfile=dsm.FLR_MP_WIN.opt
IBM Tivoli Storage Manager
Command Line Backup-Archive Client Interface
  Client Version 7, Release 1, Level 3.0
  Client date/time: 11/10/2015 16:06:55
<c> Copyright by IBM Corporation and other(s) 1990, 2015. All Rights Reserved.

Node Name: FLR_MP_WIN
Session established with server TSMSRV-DMZ: AIX
  Server Version 7, Release 1, Level 3.0
  Server date/time: 11/10/2015 16:00:39  Last access: 11/10/2015 16:00:14

Query for Virtual Machines with active Instant Restore sessions
#      Start Date        UM Name      ESX Host      Type      vMotion      Backed up UM Name
1  11/10/2015 15:56:50  testInstan-  espure13.ipfs-  IR      running      LOG - TSM4VE_WIN-
                         trestore          .cloud.ibm.co-          MP

c:\Program Files\Tivoli\TSM\baclient>
```

Figure 7-18 Example of command line query from the mount proxy

As a VMware administrator you can also track all of these operations using the task console of your vSphere web interface (Figure 7-19).

Task Name	Target	Status	Details	Initiator	Queued For	Start Time
Relocate virtual machine	testinstantrestore	33 %	Copying Virtual Ma...	TSM	6 ms	11/10/2015 4:0...
Power On virtual machine	testinstantrestore	Completed		TSM	7 ms	11/10/2015 3:5...
Create virtual machine snapshot	testinstantrestore	Completed		TSM	7 ms	11/10/2015 3:5...

Figure 7-19 Track all of these operations using the task console

When the storage vMotion (understand the data copy from IBM Spectrum protect to vSphere datastore) is completed, all of the cleanup operation is done automatically by IBM Spectrum Protect for VMware without any manual intervention. At the end of the operation, the virtual machine has been restored onto the specified datastore and is now fully ready for normal operations. All the modifications performed during the restore are committed through the snapshot mechanism at the end of the storage vMotion.

7.1.6 File level restoration

This is one of the great improvements in IBM Spectrum Protect for VMware 7.1.3: File recovery has become very easy. After the mount proxy has been configured, and file-level recovery options enabled through the IBM Spectrum Protect User Interface wizard, the only thing that you have to do is to connect to the web interface and provide your credentials. You no longer require any IBM Spectrum Protect, system, or VMware knowledge, you just need to know what file and what date you are looking for.

IBM Spectrum Protect for Virtual Environment - DP for VMWare version 7.1.3 provides a “self-service” model through a web interface, enabling users to recover their own files onto their own virtual machines. When installed, it is accessible through the following website (Figure 7-20):

<https://<IBM Spectrum Protect for VE host>:9081/FileRestoreUI/>



Figure 7-20 Login screen for IBM Spectrum Protect File Restore

Figure 7-21 shows the File Restore pane, which you use to view backups in a date range.

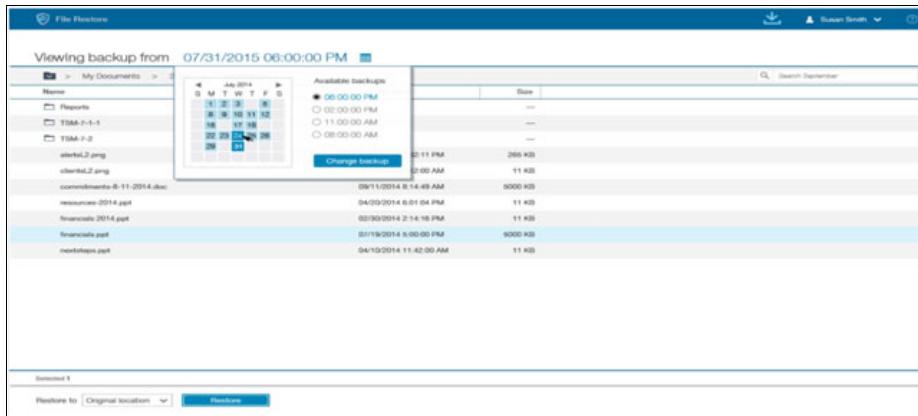


Figure 7-21 Viewing backup for particular date

Here are the key advantages of this new file recovery approach:

- ▶ “Self Service”: No administrator assistance required
- ▶ User does not need to know IBM Spectrum Protect
- ▶ Browser-based: No software required on end user system

The steps required to recover the data are:

1. Point web browser to IBM Spectrum Protect File Recovery Service URL.
2. Enter credentials for VM.
3. Choose recovery point and files directly from browser.
4. Click **Restore**.
5. Done.

There are some [file restore known issues and limitations](#) that you must be aware of. Review the linked IBM Technote.

7.1.7 Microsoft SQL Server object recovery

When you enable the Self Contained Application Data protection (using the option INCLUDE.VMTSMVSS in datamover option file), Microsoft SQL databases are also protected by the full virtual machine block level based backup done by IBM Spectrum Protect Virtual Environment - Data protection for VMware.

By activating this option, you take advantage of the single ingest backup method, allowing you to recover the whole Virtual machine or only portion of databases, to your needs.

Here is an example of how to configure self-contained application protection for MS SQL.

The steps are similar for MS Exchange.

Configuring the data mover node for the VM backups of the MS SQL server VM guest

Complete the following steps:

1. Specify the following **include** in the data mover client option file (dsm.opt in Windows, /dsm.sys in Linux):

```
INCLUDE.VMTSMVSS <vmname> <if needed, management class name> <if needed to keep the MS SQL logs, OPTions=KEEPSqllog>
```

For example: **INCLUDE.VMTSMVSS vm_mssql**

2. Ensure that the VMDKs hosting the Microsoft SQL database or log files are not being excluded from the VM backups.
3. On the data mover vBS, store the guest VM credentials to Data Protection for VMware by executing the following command:

```
dsmc set password -optfile=<dsm.opt of the data mover node, for example DM_1> -type=vmguest vm_mssql <guest admin ID> <guest admin pw>
```

See here which permissions that guest user needs:

- For MS Exchange: <http://www.ibm.com/support/docview.wss?uid=swg21647986>
- For MS SQL: <http://www.ibm.com/support/docview.wss?uid=swg21647995>

4. Use the data mover command-line client with the 'preview' option to verify that application protection is set correctly:

```
dsmc backup vm vm_mssql -preview -asnode=<datacenter node for example 'DC_1'>
```

5. Let the backups run.

6. Before you can restore individual Microsoft SQL databases from a Data Protection for VMware VM backup, at least one successful VM backup must contain the necessary Microsoft SQL database metadata.

To verify that, run the data mover client command:

```
dsmc query vm vm_mssql -detail -asnode=DC_1
```

In the output, you need to see the following results, as shown in Example 7-2:

- a. 'Application(s) protected: (database-level recovery)'
- b. No 'VMDK Status' fields for the disks hosting the MS SQL databases and logs that indicate 'Excluded'.

Example 7-2 Output from the data mover client command

#	Backup Date	Mgmt Class	Size	Type	A/I	Virtual Machine
1	<timestamp>	MSSQLMGMT	65 GB	IFFULL	A	vm_mssql
Size of this incremental backup: n/a						
Number of incremental backups since last full: 0						
Amount of extra data: 0						
TSM object fragmentation: 0						
Backup is represented by: 417 TSM objects						
Application protection type: TSM VSS						
Application(s) protected: MS SQL 2012 (database-level recovery)						
VMDK[1]Label: Hard Disk 1						
VMDK[1]Name: [datastore_1] vm_mssql/vm_mssql.vmdk						
VMDK[1]Status: Protected						
...						

```
VMDK[4]Label: Hard Disk 4  
VMDK[4]Name: [datastore_1] vm_mssql/vm_mssql_3.vmdk  
VMDK[4]Status: Protected  
...
```

Configuring Data Protection for Microsoft SQL in the guest

Complete the following steps:

1. Verify the following software packages are installed:
 - Data Protection for VMware Recovery Agent and Data mover client from the Data Protection for VMware product package
 - Data Protection for Microsoft SQL
2. Using the Data Protection for Microsoft SQL Configuration Wizard, make sure to enter the datacenter node name, for example, DC_1, in the 'DataCenter Node' field on the IBM Spectrum Protect Node Names wizard page.
3. After Data Protection for Microsoft SQL is configured, verify that the 'Configuring Recovery Agent rule' status is Passed.
4. Go to the data mover vBS and do the following:
 - a. Give to the data mover node configured within the guest (also called the VSS requestor node, for example 'sqlnode') to the VM backup data owned by the datacenter node DC_1.

This command needs to be run from the datacenter node DC_1 directly.
Because there is no dsm.opt file for the datacenter node, we need to create it temporarily only for this purpose, and it can be deleted afterwards.
 - b. Copy the dsm.opt of DM_1 to dsm.setaccess.opt file
 - c. Edit the dsm.setaccess.opt file to set the NODENAME option to the following:
`NODENAME <datacenter node>, for example <DC_1>`

5. Now run the '**set access**' command, as shown in Example 7-3:

```
dsmc set access backup -type=VM <vm guest name> <vss_requestor_node>  
-optfile=dsm.setaccess.opt
```

Example 7-3 The set access command

```
dsmc set access backup -type=VM vm_mssql sqlnode -optfile=dsm.setaccess.opt  
ANS1148I 'Set Access' command successfully completed.  
dsmc query access  
Node name: DC_1  
Type   Node   User Path  
-----  
Backup sqlnode *  \VMFULL-vm_mssql\*/*  
ANS1148I 'Query Access' command completed successfully
```

Note: If the datacenter node name is not known, the IBM Spectrum Protect server administrator must reset the password to run the **set access** command. To recover SQL data from virtual machine backup, log on to the system where you want to restore the SQL Server database. The Data Protection for VMware Datamover, DP for VMware Recovery Agent, and Data Protection for SQL Server must be installed on the system where you will restore the data.

6. In order to connect to the IBM Spectrum Protect Server and backup data, run the DP for SQL wizard as you would do to protect local SQL databases.
7. In the Data Protection for SQL Server wizard, for the Configuring Recovery Agent rule, verify that the status is Passed. If the status is not Passed, rerun the configuration wizard.
8. On the IBM Spectrum Protect Server Node Names wizard page, enter the data center node name. The data center node is the virtual node that maps to a data center.
9. Before starting to restore SQL data from within the virtual machine backup, ensure that all access between datamover, data owner and data worker are properly set. Run the set access command on the datamover machine that was used to perform the backup giving access to the in guest dsmagent node that was used during the configuration process. Using your datacenter node, issue the following command:

```
# dsmc set access backup -type=vm <vmName> <dsmagentNode>
```

In the command, *vmName* is the name of the Virtual machine where the database resides, and *dsmagentNode* is the VSS requestor node specified in the DP for SQL setup.

Figure 7-22 shows the access and relationship configured for our setup, and Table 7-2 describes the details.

```
C:\Program Files\Tivoli\TSM\baclient>dsmc query access -optfile=temp.opt
IBM Tivoli Storage Manager
Command Line Backup-Archive Client Interface
  Client Version 7, Release 1, Level 4.0
  Client date/time: 01/19/2016 04:34:54
  <c> Copyright by IBM Corporation and other(s) 1990, 2015. All Rights Reserved.

Node Name: DEMODC
Please enter your user id <DEMODC>:

Please enter password for user id "DEMODC": *****

Session established with server TSMSRV01: Linux/x86_64
  Server Version 7, Release 1, Level 4.0
  Server date/time: 01/19/2016 04:34:54 Last access: 01/19/2016 04:20:38

Type      Node        User        Path
-----    ---        ---        ---
Backup    WIN2008_DEMO  *          \VMFULL-Win2008-x64-demo-client\**\*
ANS1148I 'Query Access' command successfully completed

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

Figure 7-22 Access and relationship configured

Table 7-2 Node name details

Node name	Role	Access required
DEMODC	Node name holding virtual machine backups	Target proxynode of VE datamover, as part of IBM Spectrum Protect for VE setup
WIN2008_DEMO	Node name configured as VSS requestor on DP for SQL installation (within MS-SQL server virtual machine)	Access granted to the MS-SQL virtual machine backups managed by DEMODC Dsmc set access backup -type=vm Win2008-x64-demo-client WIN2008_DEMO
WIN2008_DEMO_SQL	Node name configured as DP for SQL node	Target proxynode of WIN2008_DEMO. GRANT PROXYNODE agent=win2008_demo target=win2008_demo_sql

10. The last step that you could do before attempting to recover an SQL object from a single ingest backup, is to ensure that IBM Spectrum Protect has all of the required metadata associated to that SQL object (Figure 7-23).

```
C:\Program Files\Tivoli\TSM\baclient>dsnc query vm win2008-x64-demo-client -detail -optfile=dsn.BASE-WIN2K8X64_datamover
.opt -asnode name=demo
IBM Tivoli Storage Manager
Command Line Backup-Archive Client Interface
Client Version 7, Release 1, Level 4.0
Client date/time: 01/15/2016 10:26:01
(c) Copyright by IBM Corporation and other(s) 1990, 2015. All Rights Reserved.

Node Name: BASE-WIN2K8X64_DATAMOVER
Session established with server TSMSRV01: Linux/x86_64
Server Version 7, Release 1, Level 4.0
Server date/time: 01/15/2016 10:26:01 Last access: 01/15/2016 10:25:18

Accessing as node: DEMODC
Query Virtual Machine for Full VM backup

# Backup Date Mgmt Class Size Type A/I Virtual Machine
1 01/15/2016 09:59:07 BACKUP_DISK_MIRROR30DAYS 51.76 GB IFINCR A Win2008-x64-demo-client
Size of this incremental backup: 149.81 MB
Number of incremental backups since last full: 3
Amount of extra data: 0
TSM object fragmentation: 3
Backup is represented by: 686 TSM objects
Application protection type: TSM USS
Application(s) protected: MS SQL 2012 (database-level recovery)
Snapshot type: Tivoli Storage Manager USS
Disk1Label: Hard Disk 1
Disk1Name: [DataStore1] Win2008-x64-demo-client/Win2008-x64-demo-client-000005.udnk
Disk1Status: Protected
Disk2Label: Hard Disk 2
Disk2Name: [DataStore1] Win2008-x64-demo-client/Win2008-x64-demo-client_1-000004.udnk
Disk2Status: Protected

All averages are calculated only for incremental forever backups displayed above.
The average size of incremental backup: 149.81 MB
The average number of incremental backups since last full: 3
The average overhead of extra data: 0
The average TSM objects fragmentation: 3
The average number of TSM objects per backup: 686

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

Figure 7-23 Query backup

11. When the system is configured and ready, open the FlashCopy Manager Management console and go to the “Protect and Recover data” (left pane) menu, select the **Recover** tab, and let the wizard guide you through the recovery steps (Figure 7-24).

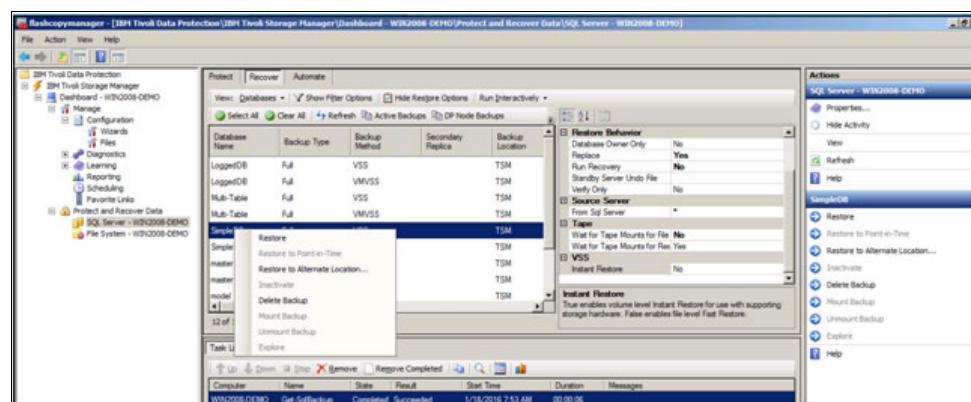


Figure 7-24 Recovery steps

12. When you click **Restore**, all of the recovery steps are done automatically. Ensure that you have these two recovery options properly set (Figure 7-25):

- Autoselect = no
- Run recovery = no

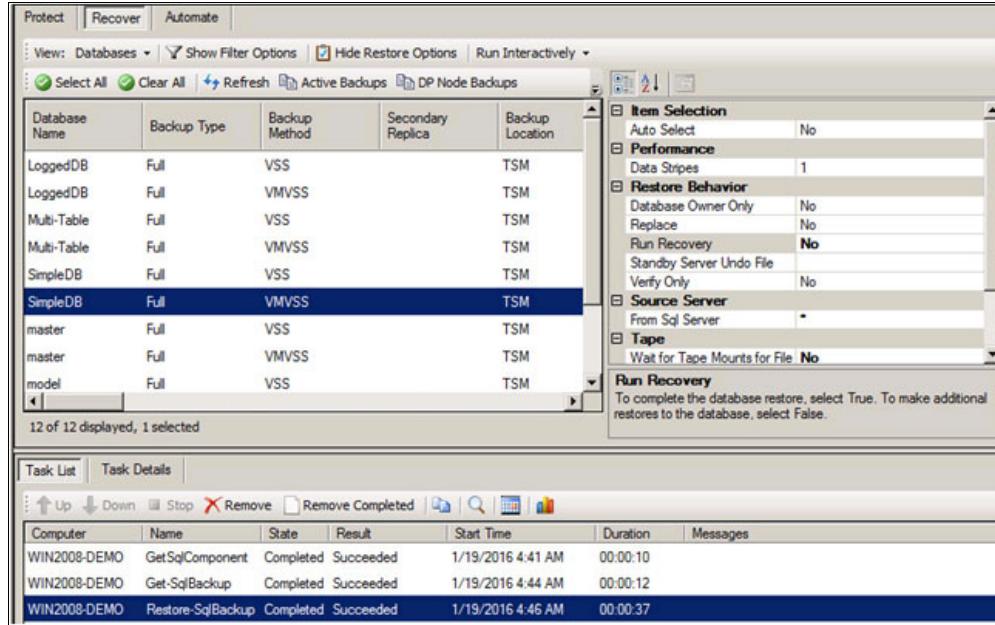


Figure 7-25 Recovery settings

Figure 7-26 shows the log entry associated to recovery activity.

```
tdpsql - Notepad
File Edit Format View Help
01/19/2016 04:44:32 -----
01/19/2016 04:44:34 Request : QUERY TSM DBNAME
01/19/2016 04:44:34 SQL Server Name Override : =
01/19/2016 04:44:34 Database Input List : =
01/19/2016 04:44:34 Include Inactive Files? : No
01/19/2016 04:44:34 Include Compatibility Info? : Yes
01/19/2016 04:44:34 Include File Info? : No
01/19/2016 04:44:34 FileInfo Mount wait : Yes
01/19/2016 04:46:06 -----
01/19/2016 04:46:06 Request : QUERY SQL
01/19/2016 04:46:06 -----
01/19/2016 04:46:12 Request : VSS RESTORE
01/19/2016 04:46:12 Component List : 'SimpleDB'(Full, TSM)
01/19/2016 04:46:12 Local DSMAGENT Node : WIN2008_DEMO
01/19/2016 04:46:12 Mount wait : Yes
01/19/2016 04:46:12 -----
01/19/2016 04:46:15 Backup(s) to be restored:
01/19/2016 04:46:15 <SimpleDB>VSS Full 01/19/2016 01:01:28>
01/19/2016 04:46:36 Restoring 'SimpleDB' via file-level copy from snapshot(s). This process may take some time. Please wait.
01/19/2016 04:46:41 VSS Restore operation completed with rc = 0
01/19/2016 04:46:41 Files Examined : 2
01/19/2016 04:46:41 Files Completed : 2
01/19/2016 04:46:41 Files Failed : 0
01/19/2016 04:46:41 Total Bytes : 5243230
01/19/2016 04:46:41 Total LanFree Bytes : 0
01/19/2016 04:51:26 -----
```

Figure 7-26 Recovery log

Another way to restore is to use the command-line interface (Figure 7-27):

```
Tdpsqlc restore SimpleDB /backupmethod=vmvss /recover=no
```

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window contains the following text output:

```
C:\>Program Files\Tivoli\TSM\TDPSql>Tdpsqlc restore SimpleDB /recover=no /backupmethod=vmvss
IBM Tivoli Storage Manager for Databases:
Data Protection for Microsoft SQL Server
Version 7, Release 1, Level 4.0
(C) Copyright IBM Corporation 1997, 2015. All rights reserved.

Connecting to SQL Server, please wait...
Querying TSM Server for Backups ....
Connecting to TSM Server as node 'WIN2008_DEMO_SQL'...
Connecting to Local DSM Agent 'WIN2008_DEMO'...
Using backup node 'WIN2008_DEMO_SQL'...
Starting Sql database restore...

Beginning USS restore of 'SimpleDB'...

Restoring 'SimpleDB' via file-level copy from snapshot(s). This process may take
some time. Please wait.
    Files Examined/Completed/Failed: [ 2 / 2 / 0 ]   Total Bytes: 5243230

USS Restore operation completed with rc = 0
    Files Examined      : 2
    Files Completed    : 2
    Files Failed       : 0
    Total Bytes        : 5243230
    Total LanFree Bytes : 0

The operation completed successfully. <rc = 0>

C:\>Program Files\Tivoli\TSM\TDPSql>
C:\>Program Files\Tivoli\TSM\TDPSql>
C:\>Program Files\Tivoli\TSM\TDPSql>
C:\>Program Files\Tivoli\TSM\TDPSql>
```

Figure 7-27 Command line based recovery

In case you have database logs available and you want to recover these logs after the full restore, use the below command. This approach implies that you have done log backup using DP for SQL in combination with the virtual machine snapshot data protection:

```
# Tdpsqlc restore SimpleDB log=* /recover=yes
```

Figure 7-28 provides detailed information about what is happening under the cover when doing an SQL database recovery from a virtual machine backup.

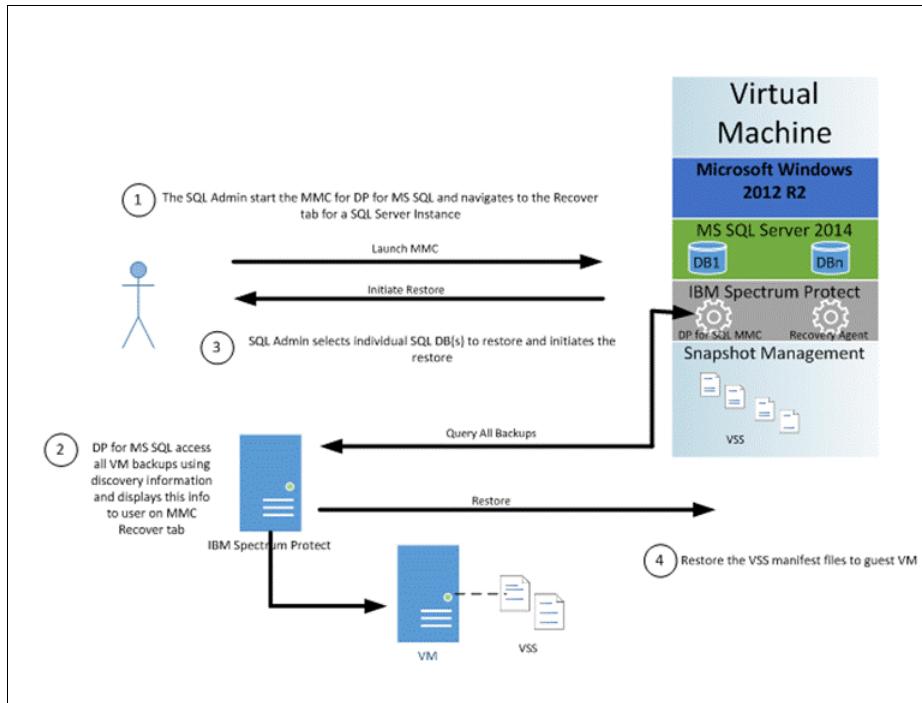


Figure 7-28 SQL database recovery from a virtual machine backup Part A

Figure 7-29 shows the rest of the SQL database recovery from a virtual machine backup.

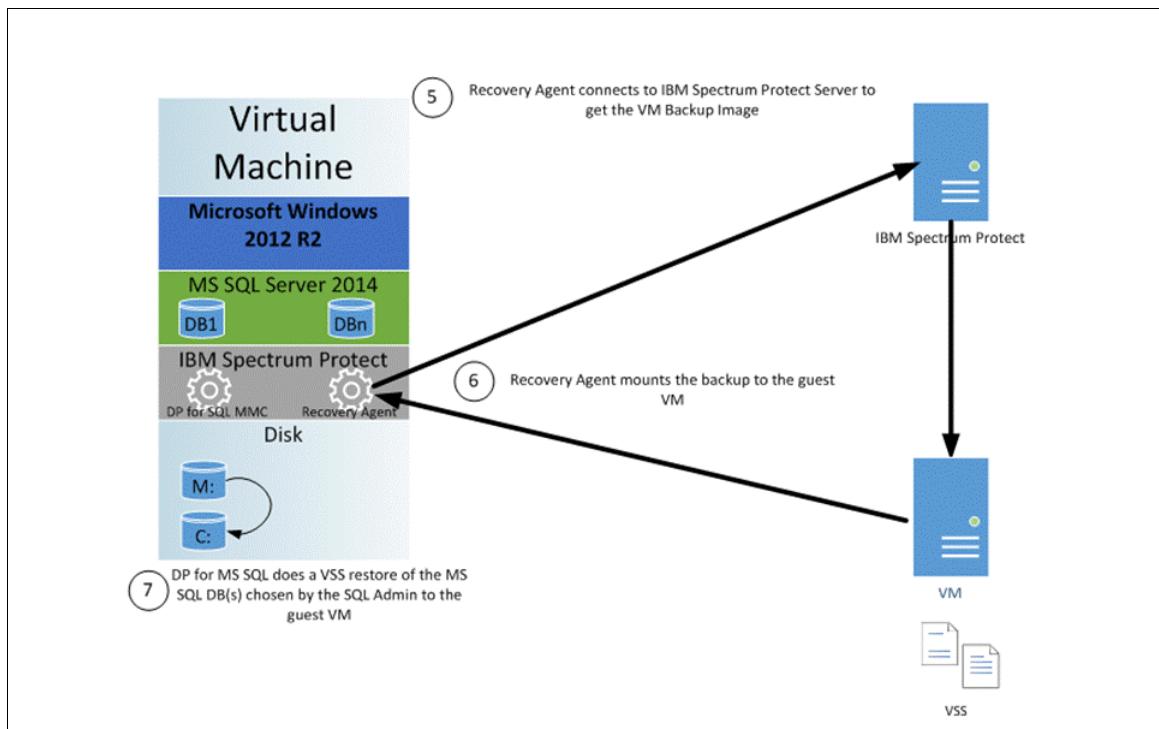


Figure 7-29 SQL database recovery from a virtual machine backup Part B

7.2 Overview of recovery procedures using the IBM Spectrum Protect Snapshot for VMware GUI

The use of IBM Spectrum Protect for Snapshot is very easy, all the steps can be done through the graphical user interface.

As for the Data protection for VMware graphical interface, the IBM Spectrum Protect Snapshot for VMware interface is accessible through a supported web browser from any machine having access to the same net-work where the IBM Spectrum Protect Snapshot for VMware engine is running.

As an example <https://myproxy:9081/TSMVMwareUI> (case sensitive), where <myproxy> is the Linux machine where the IBM Spectrum Protect Snapshot for VMware components are installed.

Although two modes of recovery are available using IBM Spectrum Protect for Snapshot, which are Virtual Machine and Datastore, you can also recover your data in the following ways:

- ▶ Virtual machine individual file
- ▶ Virtual machine vmdk
- ▶ Virtual machine
- ▶ Datastore

7.2.1 Virtual machine recovery

You can restore a single virtual machine or virtual disk to its original location or to an alternative location.

IBM Spectrum Protect Snapshot for VMware enables you to recover a virtual machine in a very limited amount of time. This recovery operation overwrites the virtual machine that you ask to be recovered, even if the virtual machine is powered on. The recovery process powers off, unregister the virtual machine and register a new virtual machine once restored onto the specified datastore. The background copy is basically a file-level copy from the datastore that was mounted from the snapshot, to the datastore that you asked the virtual machine to be restored into. When the file copy is done and the virtual machine registered back to vCenter, the mounted datastore is removed.

To perform virtual machine recovery operation, complete these steps:

1. Connect to the IBM Spectrum Protect Snapshot for VMware UI and go to the Restore tab.
2. Select the virtual machine and click **Restore** to start the wizard.

Figure 7-30 shows the virtual machine recovery wizard.

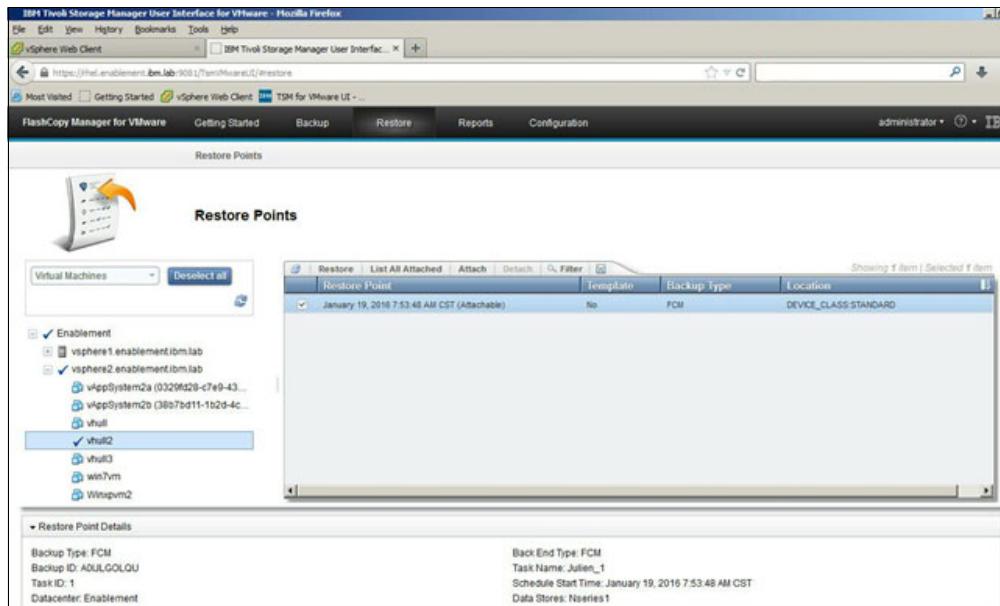


Figure 7-30 Virtual machine recovery wizard

- When you click **Restore**, the Wizard window opens and guides you through the steps to recover the virtual machine. In case the virtual machine still exists, the wizard prompts you a confirmation whether you want to overwrite existing virtual machine or abort the operation.

To track the task's progress, go to the Report tab, the Recent Task menu, or monitor the virtual machine availability on VSphere client side. You can also track each step and detailed information in the Vsphere client task console. IBM Spectrum Protect Snapshot for VMware creates entries for each step that it is making on the VMware side.

7.2.2 Virtual machine virtual disk recovery

Virtual machine virtual disk (VMDK) recovery follows almost the same steps as for the virtual machine recovery. The only thing you have to change is the granularity option from full restore to virtual disk restore (Figure 7-31 on page 115).

To perform the virtual machine disk recovery operation, complete the following steps:

1. Connect to the IBM Spectrum Protect Snapshot for VMware UI and go to the Restore tab.
 2. Select the virtual machine and click **Restore** to start the wizard, as shown in Figure 7-31 on page 115.

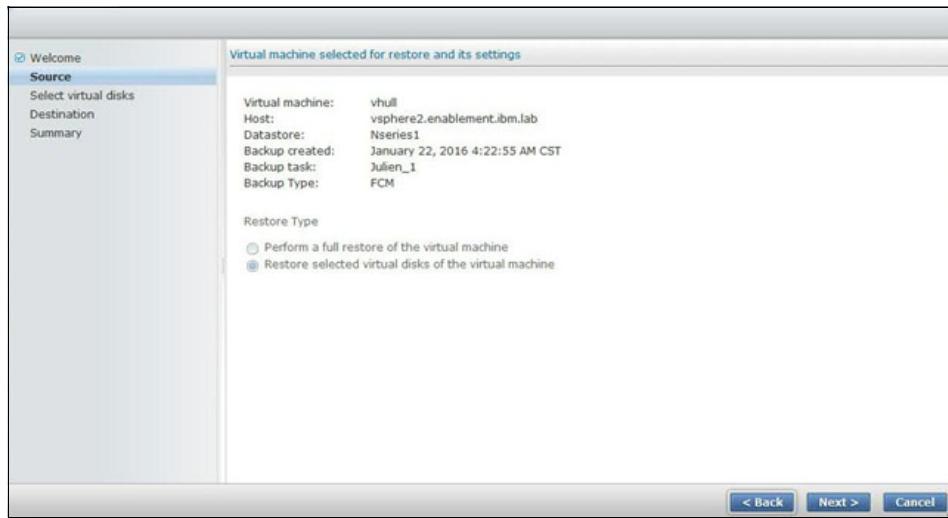


Figure 7-31 Virtual disk restore

3. After you select this option, you are prompted to select the virtual disk that you want to restore. This action provides you with detailed information about the disk as of its backup, including label, size, and its full path (Figure 7-32).

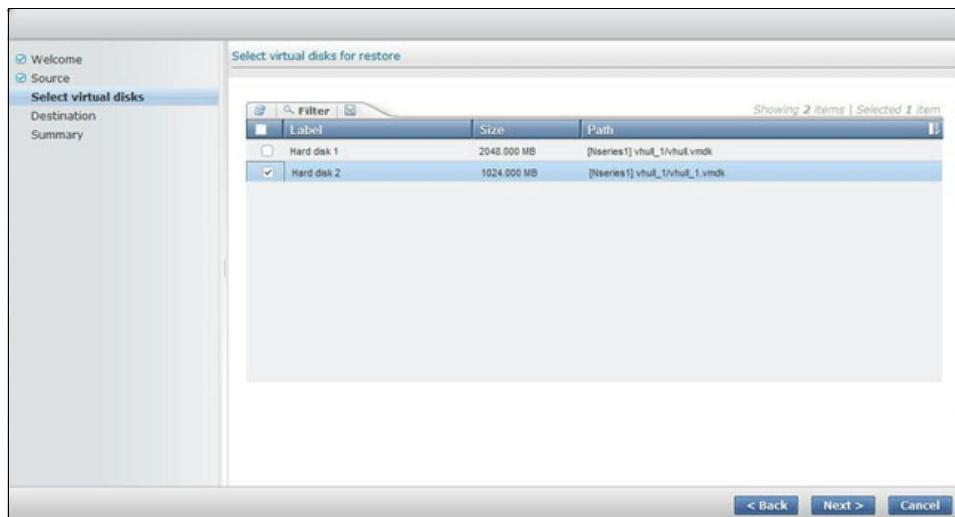


Figure 7-32 Virtual disk prompts

4. Select the virtual disk that you need to restore, and then select the destination virtual machine that you want this virtual disk to be attached to.

Here are the steps done automatically for this virtual disk recovery process:

1. Mount the datastore from the snapshot.
2. Copy the .vmx file from the mounted datastore to the restore location datastore.
3. Register the VM and then unregister the VM.
4. Delete the original VMDK from the original machine (the one to be restored).
5. Copy the VMDK file from the mounted datastore to the restore location datastore.
6. Unmount the previously mounted datastore.
7. Operation done.

Note: When you decide to restore in the same location, the existing virtual disk is overwritten by the recovered one. If you decide to restore the virtual disk onto another virtual machine, it becomes a new device assigned to that target virtual machine.

To track the task's progress, select the Report tab, the Recent Task menu, or monitor the virtual machine availability on the vSphere client side. You can also track each step and detailed information in the vSphere client task console. IBM Spectrum Protect Snapshot for VMware creates entries for each step that it is making on the VMware side.

7.2.3 Virtual machine individual file recovery

IBM Spectrum Protect Snapshot for VMware allows you to recover a single file. It basically mounts and shows you the backup image content onto the virtual machine of your choice. Usually this location is where you need the file, and you browse and pick the file you need to copy back to your machine. This section describes the steps to achieve that.

To recover a file, IBM Spectrum Protect Snapshot for VMware attaches a mounted image of the datastore where the virtual machine is, and prompts you to enter the name of a virtual machine where you want the virtual machine disk to be attached to.

Because IBM Spectrum Protect Snapshot for VMware is able to attach multiple virtual disks for individual file recovery at the same time, check if there are already attached operations in progress before starting an individual file recovery operation. In this way, you will be able to identify your attach operation afterwards.

To do so, complete the following steps:

1. Go to Restore tab, and use the “List Attached” menu to list all attached snapshots (Figure 7-33).

The screenshot shows a dialog box titled "All Attached Restore Points". It contains a message "Select the datacenter that contains the restore points you want to detach" and a dropdown menu set to "Enablement". Below this is a table with the following data:

Restore Point	Source Host	Source VM	Target Host	Target VM
January 19, 2016 7:53:48 AM CST	vsphere2.enablement.ibm.lab	wm7vm	vsphere2.enablement.ibm.lab	vhul0
January 22, 2016 4:22:55 AM CST	vsphere2.enablement.ibm.lab	vhul	vsphere2.enablement.ibm.lab	vhul0

At the bottom right of the dialog box is a "Close" button.

Figure 7-33 All attached restore points

Tip: When a virtual machine contains an attached snapshot, you can see it as a highlighted blue line in the Restore tab with the “(Attached)” comment (Figure 7-34 on page 117).

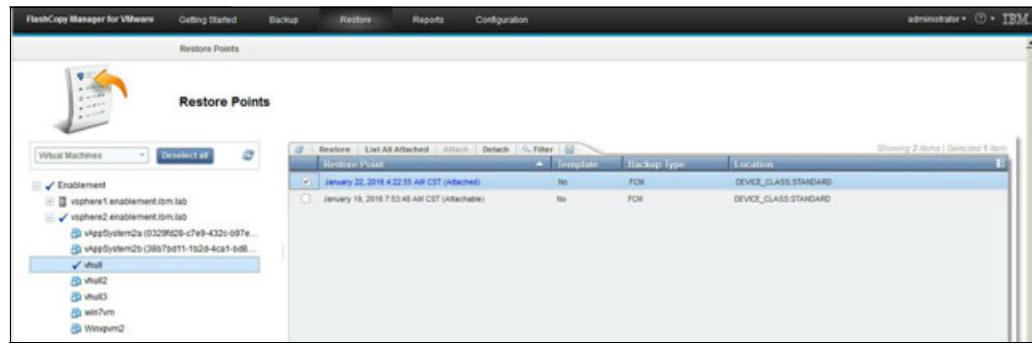


Figure 7-34 Attached snapshot

- Now, to perform virtual machine individual file recovery operation, connect to the IBM Spectrum Protect Snapshot for VMware UI and go to Restore tab, select the virtual machine and click on “Attach” to start the wizard.

Figure 7-35 shows the virtual machine file recovery attach wizard.

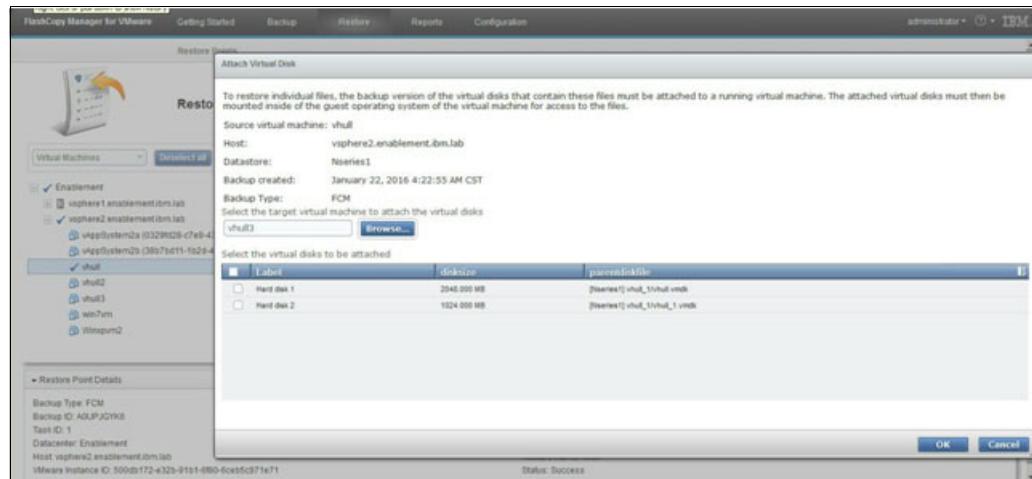


Figure 7-35 Virtual machine file recovery attach wizard

- Select the following items:
 - The virtual machine that you want to extract data from
 - The snapshot date
 - The virtual disk containing the file that you want to restore
 - The virtual machine where you want to assign the virtual disk, so that you have access to that volume content
- Here are the steps done by IBM Spectrum Protect Snapshot for VMWare in this individual file recovery scenario:
 - Mount datastore from snapshot.
 - Attach the virtual disk to the chosen virtual machine (as an independent, non-persistent VMDK).
 - At this point, the virtual disk is accessible from inside the virtual machine and you can perform the file copy at operating system level.

- After you complete the copy/paste operation, go back to the Restore tab in the IBM Spectrum Protect Snapshot for VMware UI menu. Click **List Attached** to retrieve information regarding which mount point are attached. Then close this menu and find the mount point you want to detach, and click **Detach**.

Tip: The detach button is disabled when there is not an associated target attached. It becomes available only if an attached operation is ongoing for the selected snapshot.

Detach operation consists on removing the virtual disk from the virtual machine used for file copy operation, and then unmount the datastore previously mounted for that individual file recovery.

7.2.4 Complete datastore recovery

To perform an entire datastore recovery operation, complete the following steps:

- Connect to the IBM Spectrum Protect Snapshot for VMware UI.
- Go to Restore tab, select the Datastore in the menu below the **Restore points**.

Figure 7-36 shows the Datastore recovery wizard.

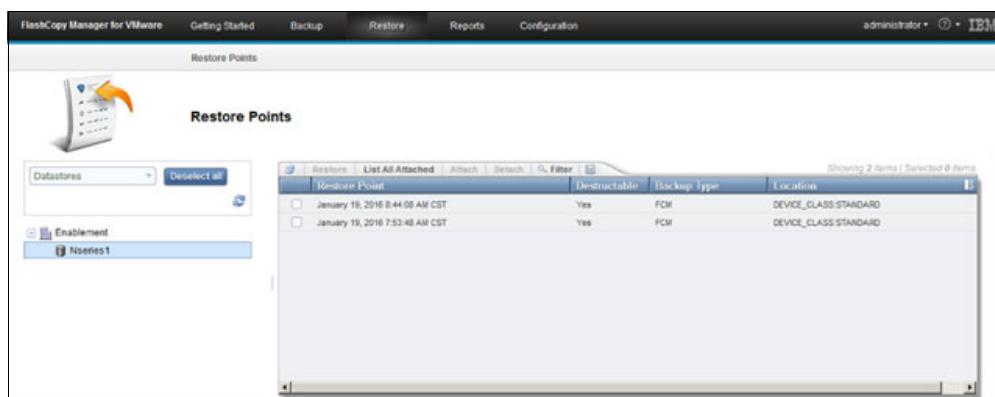


Figure 7-36 Database recovery wizard

- The first choice to make is the snapshot date, then select what virtual machine from within the datastore backup that you want to be restored (and then activated after recovery completes). The wizard will tell you if there is any risk of overwriting an existing virtual machine (Figure 7-37 on page 119).

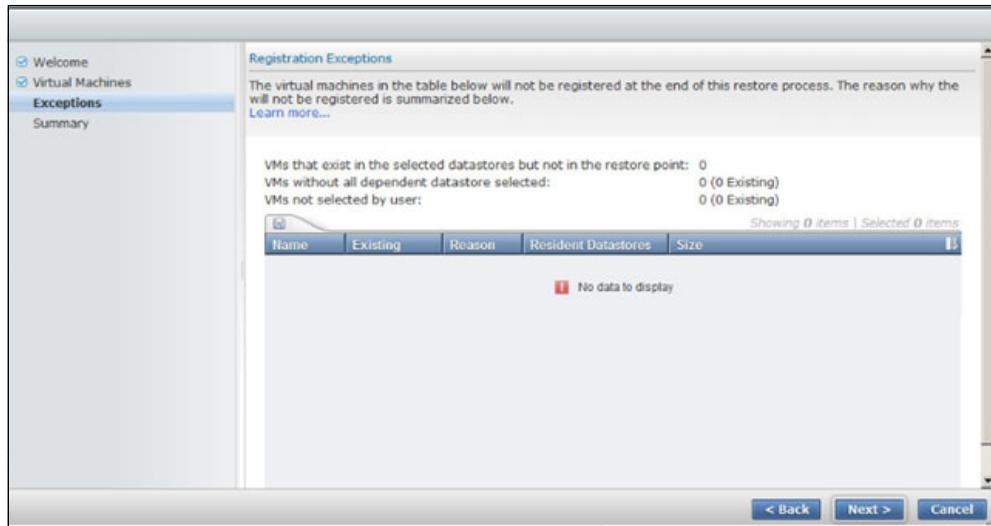


Figure 7-37 Risk of overwriting an existing virtual machine

Figure 7-38 shows any virtual machine recovery contention.

- Indeed, a datastore recovery operation overwrite then entire datastore, even if you want to recovery only few virtual machine available at the backup time. The wizard informs you a last time before proceeding with the snapshot's restoration (Figure 7-38).

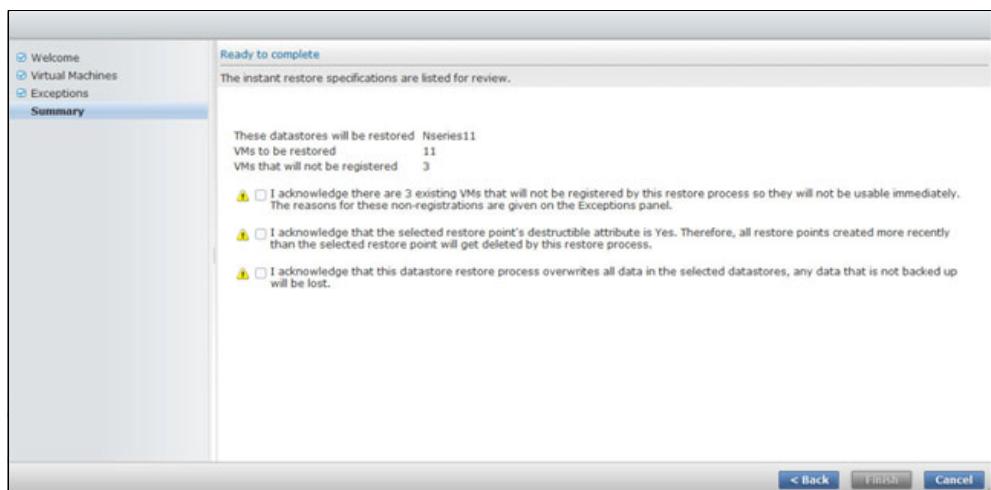


Figure 7-38 VM recovery content

Notice that before recovering a datastore, there must be a datastore existing and accessible in the VSphere infrastructure.

Note: Renaming the datastore has no effect. For example, if the datastore was named Nserie1 at backup time, but now you need to recover the datastore and you name the datastore Nserie_recovery1, IBM Spectrum Protect is still able to find the associated backup.

Tip: if a datastore has been deleted, any of its backups will be kept as per the backup policy. Therefore, you can still see the datastore as an available recovery point within the interface.

The following steps are performed by IBM Spectrum Protect Snapshot for VMWare in this full datastore recovery scenario:

1. Unmount the VMFS datastore that will be recovered.
2. Remove the datastore from the VMware configuration.
3. Ask the backend storage to revert back to a previous snapshot (based on your snapshot date selection).
4. Rescan the attached storage on the VSphere side.
5. Mount the VMFS datastore.
6. Register the virtual machines as per the selected virtual machine to be recovered. Notice that there could be some virtual machines stored on that datastore. However, they are not “seen” by the vCenter server because you specified to not register those machines. Obviously, you can register them afterwards.



Reporting

Several types of reports are available when you use IBM Spectrum Protect Data Protection for VMware solutions:

- ▶ Reports that can be displayed natively in the IBM Spectrum Protect software
- ▶ Reports that can be created by mining information in the IBM Spectrum Protect server database by using SQL SELECT statements

This chapter includes the following topics:

- ▶ Native reports
- ▶ SQL reports
- ▶ VMware vSphere Web Client

8.1 Native reports

Native reports are available from the Data Protection for VMware vSphere web graphical user interface (GUI). This GUI is accessible as an extension to the VMware vSphere Web Client or directly through a web browser.

In order to run the VMware vSphere Web GUI from the vSphere Web Client extension, it must be installed and configured. Verify the configuration from the main screen of the vSphere Web Client extension click **Home** → **IBM Data Protection** and select the **Connections** tab. The vCenter Connection Status field indicates a Verified Connection after the GUI is configured (Figure 8-1).

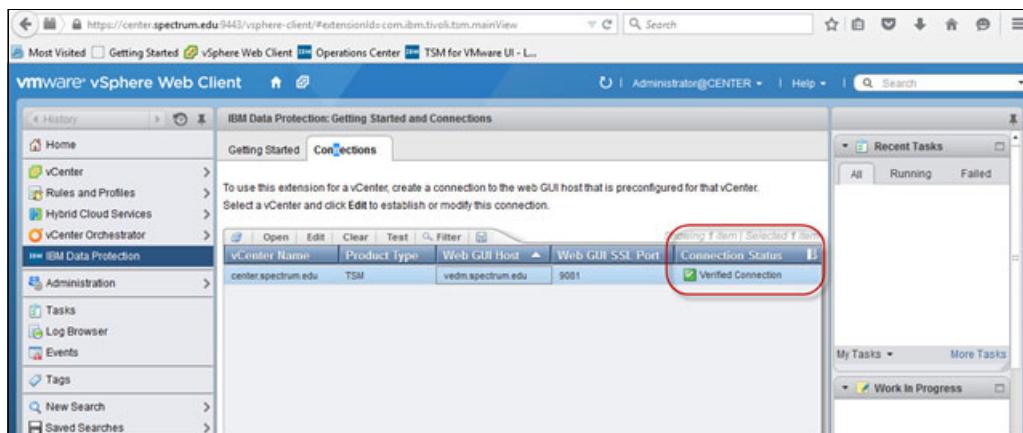


Figure 8-1 Web Client verified connection

Select the vCenter that you want to report on, and click **Open** to start the Data Protection for VMware vSphere Web GUI. You can find the native reports by clicking **Reports** from the menu at the top of the page (Figure 8-2).

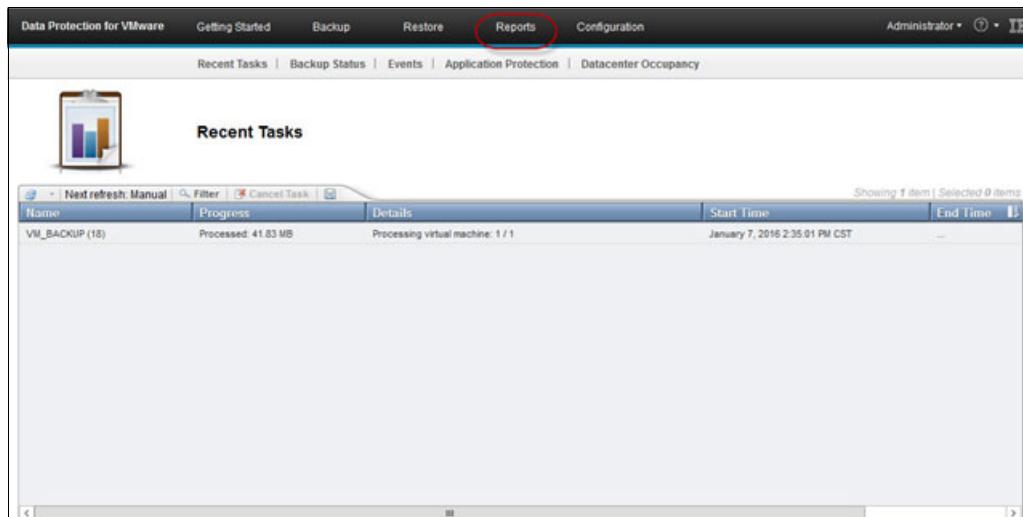
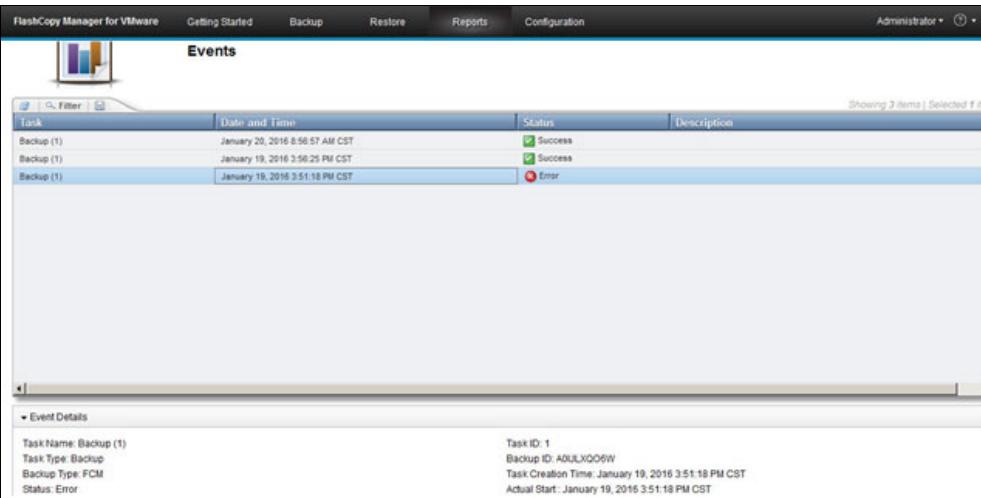


Figure 8-2 Native reports for vCenter

Tip: Although similar in many respects, the GUI for IBM Spectrum Protect for Virtual Environments and IBM Spectrum Protect Snapshot provide different reports.

8.1.1 Events

Use the Events page to view the status of the events that completed within the last three days. An event is a message that provides status on an operation. Event information is determined by the backup or restore method. When you click an event, detailed information is shown in the pane at the bottom of the window (Figure 8-3).



The screenshot shows the 'Events' page of the FlashCopy Manager for VMware interface. At the top, there are tabs for 'Getting Started', 'Backup', 'Restore', 'Reports', and 'Configuration'. On the right, it says 'Administrator'. Below the tabs, there's a title 'Events' with a small icon. Underneath is a table with columns: 'Task', 'Date and Time', 'Status', and 'Description'. Three rows are listed:

Task	Date and Time	Status	Description
Backup (1)	January 20, 2016 8:58:57 AM CST	Success	
Backup (1)	January 19, 2016 3:56:25 PM CST	Success	
Backup (1)	January 19, 2016 3:51:18 PM CST	Error	

At the bottom of the table, there's a section titled 'Event Details' with the following information:

Task Name: Backup (1)	Task ID: 1
Task Type: Backup	Backup ID: A0ULXQO6W
Backup Type: FCM	Task Creation Time: January 19, 2016 3:51:18 PM CST
Status: Error	Actual Start: January 19, 2016 3:51:18 PM CST

Figure 8-3 Events completed in the last 3 days

8.1.2 Recent tasks

Use the Recent Tasks page to verify the progress of a backup, restore, or mount operation that started or completed in the last hour. The information identifies tasks in real-time and includes tasks that are already completed (Figure 8-4).

To stop a backup, restore, instant restore, or instant access operation, select the operation and click **Cancel Task** in the toolbar. This action stops the operation without leaving VMs or data movers in an unstable state.



The screenshot shows the 'Recent Tasks' page of the FlashCopy Manager for VMware interface. At the top, there are tabs for 'Getting Started', 'Backup', 'Restore', 'Reports', and 'Configuration'. On the right, it says 'Administrator'. Below the tabs, there's a title 'Recent Tasks' with a small icon. Underneath is a table with columns: 'Name', 'Progress', 'Details', 'Start Time', and 'End Time'. One row is listed:

Name	Progress	Details	Start Time	End Time
Backup (1)	Success		January 20, 2016 8:58:57 AM CST	January 20, 2016 8:58:27 AM CST

Figure 8-4 Recent task status

8.1.3 Backup Status

Use the Backup Status page to generate reports about the backup status of the VMs that are managed in the specified VMware datacenter domain. Backup status reports provide information that assists with periodic validation of your VM backups. These reports show activity only for Data Protection for VMware backups; the reports do not show activity for in-guest backup operations.

After you select the datacenter, select one of the reports and click **Generate Report**. Use the report to verify the backup status, determine whether a problem exists, or identify other issues that require additional investigation.

The following reports are available in IBM Spectrum Protect for Virtual Environments or IBM Spectrum Protect Snapshot:

- ▶ Coverage status for all virtual machines (VMs)

This report displays all information regardless of status, without any filtering (Figure 8-5).

VM Name	Status	Last Backup End	Backup Duration	Backup Currency
linux-box1	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
vAppSystem1a (6c3bea44-d748-4...	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
vappSystem1b (bd79a493-19cc-4...	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
vAppSystem2a (0229fd28-7e9-4...	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
vAppSystem2b (3eb7bd11-1b2d-4...	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
vhull	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
vhull2	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
vhull3	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
win7vm	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
winxpvm1	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour
Winxpvm2	Current	January 20, 2016 8:58:27 AM CST	1 minute	1 hour

Figure 8-5 Coverage status for all VMs

- ▶ VMs with a backup

This report displays the status of backed up VMs and includes the location (the vSphere Hypervisor (ESX) host name) of each VM.

- ▶ VMs without backups

This report displays VMs for which the Data Protection for VMware vSphere GUI does not contain any data.

- ▶ VMs with a completion date more than 7 days in the past

This report displays the VMs that are not included in a weekly backup or that might have a backup issue.

- ▶ VMs with a backup status other than current

This report displays the VMs that might have a backup issue. Use this report to determine whether a problem exists or whether further investigation is necessary.

- ▶ VMs that have backups but the VM does not exist in the vCenter

This report identifies VMs that were deleted from the vCenter and still have backups on the IBM Spectrum Protect server.

The following reports are available only when both IBM Spectrum Protect for Virtual Environments and IBM Spectrum Protect Snapshot are installed:

- ▶ VMs without a IBM Spectrum Protect copy of the backup

This report displays whether the VM has an offload backup on the IBM Spectrum Protect server.

- ▶ VMs that have a IBM Spectrum Protect backup but not a IBM Spectrum Protect Snapshot for VMware hardware snapshot

This report displays VMs that have an offload backup on the IBM Spectrum Protect server but does not have a IBM Spectrum Protect Snapshot hardware snapshot.

8.1.4 Application Protection page

Use the Application Protection page to generate reports about how applications are backed up by multiple IBM Spectrum Protect data protection agents. These reports show backup activity for the Data Protection for VMware backups that are owned by the VMware datacenter node and in-guest backups.

These reports are only available with IBM Spectrum Protect for Virtual Environments.

All the event data shown in these reports is generated from the IBM Spectrum Protect server used for Data Protection for VMware backup operations. This server is the IBM Spectrum Protect server that is defined on the Server Credentials page of the configuration wizard.

The value that is shown in the Total VMs field represents the number of VMs that existed in the vCenter when the most recent scan started. The value that is shown in the VMs scanned successfully field represents the number of VMs that were scanned successfully. The report identifies VMs that were not scanned successfully and includes the reason why they were not scanned (Figure 8-6).

The screenshot shows the 'Application Protection' section of the IBM Spectrum Protect interface. At the top, there are dropdown menus for 'Select a datacenter' (set to 'Enablement') and 'Select a report' (set to 'Unified Component Backup Status'), with a 'Generate Report' button. Below this, a message states 'Last Scan Attempted: No scan status | Refresh status.. Overall Scan Status: No scan status Total VMs: 0, VMs scanned successfully: 0 | Scan settings...'. A table below lists VM details: VM Name (specm), Application Instance (N/A), Database / Storage (Image Level Backup), Application (Data Protection VMware), Backup Agent (TSM API L...), Agent Level (7.1.2), TSM API L... (N/A), Node Name (APP_ENABLEMENT), and Last Backup End (January 20, 2018 3:51:42 PM). The table has columns for VM Name, Application Instance, Database / Storage, Application, Backup Agent, Agent Level, TSM API L..., Node Name, and Last Backup End.

Figure 8-6 Application Protection page

Managed Capacity

Use the Managed Capacity page to identify information about the space that is managed by IBM Spectrum Protect backups (Figure 8-7). This page is only available in IBM Spectrum Protect Snapshot.

The screenshot shows the 'Managed Capacity' section of the IBM Spectrum Protect interface. At the top, there are dropdown menus for 'Recent Tasks', 'Backup Status', 'Events', and 'Managed Capacity'. Below this, a message states 'Total Managed Capacity: 0 GB'. A table below lists volume details: Volume ID (BffwirSEMHS) and Capacity (GB) (0). The table has columns for Volume ID and Capacity (GB).

Figure 8-7 Managed Capacity

Data Center Occupancy

Use the Data Center Occupancy page to display details about the amount of space that is occupied by backups of IBM Spectrum Protect client nodes that are on the IBM Spectrum Protect server. The client nodes represent the VMware datacenter objects from which data is backed up to an IBM Spectrum Protect server. This view is only available if IBM Spectrum Protect for Virtual Environments is installed and if an IBM Spectrum Protect server is defined.

8.2 SQL reports

You can run your own reports by querying the IBM Spectrum Protect server tables. Here we provide several examples of what you can do to report your VM backup activity.

8.2.1 Successful backup in a specified time frame

The first scenario we provide (“Successful Backup in Last 24 hours”) is a report to list all of the virtual machines protected in the last 24 hours, including backup type and number of bytes processed:

```
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 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 report to show “What Failed Last 24 hours”. The report shows which virtual machine backups failed in the last 24 hours, including information about its datacenter node and the reason of the failure:

```
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 report to show “Not Backed up since” . The report allows you to determine which virtual machines have not been backed up since a given amount of time, including the last backup date:

```
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 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 filesystem_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 Additional reporting information

The [IBM Support document](#) discloses some common IBM Spectrum Protect Snapshot for VMware failures.

8.3 VMware vSphere Web Client

Reporting information is also available to the administrator via the VMware vSphere Web Client, as shown in Figure 8-8.

The screenshot shows the VMware vSphere Web Client interface. On the left, the Navigator pane is open, showing categories like Hosts and Clusters, VMs and Templates, Storage, Networking, Content Libraries, Global Inventory Lists, Policies and Profiles, and IBM Spectrum Protect. The IBM Spectrum Protect category is selected. In the main content area, the title is "IBM Spectrum Protect: Getting Started and Connections". The "Monitor" tab is highlighted with a red circle. Below the tabs, there are two sections: "Schedules" and "Maintenance". The "Schedules" section contains a table with columns: Schedule Start Time, Schedule Name, Status, VMs Succeeded, VMs Failed, and Duration. The table lists several scheduled backups. The "Maintenance" section is currently inactive. At the bottom, there is a table titled "Backup" with columns: Virtual Machine Name, Status, Backup Type, Start Time, Error Code, and Data Mover. It lists several virtual machines and their backup status.

Schedule Start Time	Schedule Name	Status	VMs Succeeded	VMs Failed	Duration
June 19, 2017 5:59:36 AM PDT	KHA-VUX-HOURLY	In progress	0	0	—
June 19, 2017 5:58:49 AM PDT	KHA-TAG-HOURLY	Missed	0	—	—
June 19, 2017 5:58:44 AM PDT	KHA-VUX-HOURLY_DUP	Succeeded	16	17	11 minutes
June 19, 2017 5:44:21 AM PDT	KHA-TAG-HOURLY1	Failed	0	—	42 minutes
June 19, 2017 5:27:58 AM PDT	KHA-DC-HOURLY	In progress	1	1	—
June 19, 2017 5:19:34 AM PDT	KHA-TAG-HOURLY2	Failed	0	—	42 minutes
June 19, 2017 5:13:33 AM PDT	KHA-HOURLY	Failed	0	—	43 minutes
June 19, 2017 4:58:49 AM PDT	KHA-TAG-HOURLY	Missed	0	—	—

Virtual Machine Name	Status	Backup Type	Start Time	Error Code	Data Mover
vm1	Succeeded	Incremental	June 19, 2017 5:57:32 AM PDT	-	WIN12_LOCAL_DATACENT
Kha_vm1	Succeeded	Incremental	June 19, 2017 5:57:35 AM PDT	-	WIN12_LOCAL_DATACENT
kha_vm5	Succeeded	Incremental	June 19, 2017 5:57:39 AM PDT	-	WIN12_LOCAL_DATACENT
Kha_vm1_Restored_M...	Failed	Incremental	June 19, 2017 5:57:43 AM PDT	-1	WIN12_LOCAL_DATACENT
YongThinDummy	Succeeded	Incremental	June 19, 2017 5:57:48 AM PDT	-	WIN12_LOCAL_DATACENT

Figure 8-8 Reporting information available in the client



Disaster recovery

Disaster recovery is a large topic with various aspects. A common theme in the world of data protection is the confusion of business continuity with disaster recovery. It is important to understand that these are two different concepts. The misunderstanding of the two terms could result in the organization and the business being left at significant risk due to inadequate planning.

The purpose of this chapter is to define what a disaster recovery is, how it matters, and how IBM Spectrum Protect products help to keep data safe and available in every circumstance. The chapter covers from a machine to an entire site disaster and explains:

- ▶ How you can easily and quickly recover a virtual machine (VM) using IBM Spectrum Protect for Virtual Environment - Data Protection for VMware, for an isolated disaster
- ▶ How IBM Spectrum Protect for Snapshot for VMware can easily and quickly restore an entire datastore following, for instance, a disk failure
- ▶ How to recover from an entire site disaster by leveraging IBM Spectrum Protect for Virtual Environment or IBM Spectrum Protect for Snapshot for VMware in combination with IBM Spectrum Protect Server and its built-in Node Replication feature, enabling you to literally clone your backup environment to an alternate location

Remember, there is not a one-size-fits-all disaster recovery plan. Probability and impact rankings vary widely by industry, geography, and company size. The assessment approach recommends development of “use cases” that are representative of the core business functions. For more details, see the [Site Recovery Manager and Stretched Storage Tech Preview](#) video.

The business continuity modes are:

- ▶ Bunker mode
- ▶ Production and DR site
- ▶ Bi-directional failover sites
- ▶ Active-active datacenter

This chapter includes the following topics:

- ▶ Disaster recovery key point indicators
- ▶ Disaster recovery requirements
- ▶ Disaster recovery use cases

9.1 Disaster recovery key point indicators

Disaster recovery is a subset of overall business continuity. It is the process of protecting the data in order of being able to recover it in the event of a disaster. Disaster in IT ranges from minor (loss of a subset of data) to major (loss of entire data center).

Disaster recovery strategies is driven by and built on two major principles which are RPO (Recovery Point Objectives) and RTO (Recovery Time Objectives):

- ▶ Recovery time objective (RTO) answers the question:

If a disaster renders a system unavailable, how much time do you have to make it available again?

In other words, RTO is the maximum wanted length of time that is allowed between a disaster and the resumption of normal operations and service levels. A business might define and measure its RTO in days or hours for non-critical business systems, but in minutes or seconds for mission critical systems.

- ▶ Recovery point objective (RPO) answers a different question:

If a disaster renders a system unavailable, what is the time frame in which data might be lost?

RPO addresses the maximum acceptable amount of data loss measured in time due to a disaster.

Whereas business continuity requires very low RPO and RTO (millisecond to second), disaster recovery RPO and RTO are usually hours or even days.

There is no exact formula to determine RTO and RPO. Each organization has different expectations that contribute to RTO and RPO requirements. The challenge in this area is balancing those expectations against the technical complexity of enabling disaster recovery.

9.2 Disaster recovery requirements

This section discusses the actions necessary to build a relevant disaster recovery plan.

9.2.1 Assess the recovery needs

It is extremely important to accurately assess the business requirements of every business service to determine which architectural pattern to apply to each specific service based on business requirements.

It is critical to determine how much time you can afford to recover your data and how many points in time you want to keep so you can resume operation.

9.2.2 Disaster recovery level definitions

The four levels of disaster recovery (DR) are as follows:

- ▶ Bunker mode

Bunker mode allows for cold recovery, most likely it might take multiple days to recover all the data.

- ▶ Production and DR site

Production and DR site approach allows for faster recovery as bunker mode, as the DR site includes the infrastructure required to recover the data, and possibly the client's machines as well.

- ▶ Bi-directional failover sites

Bi-directional failover sites making high availability and other cluster mechanism to run, across the two sites, thus making the protected data available asynchronously, with a delay depending on replication mechanisms involved.

- ▶ Active-Active datacenter

Active-Active datacenter is the basis of "Always On" infrastructure. This mode is not part of Data protection world, but rather based on disk-based replication mechanism or other high available disk systems, such as IBM Spectrum virtualize Enhanced Stretch cluster.

To determine which of the four would fit your business, you must identify, and assess your requirement (that are scope and type of data, RPO and RTO) and build and list of most probable disaster cause, based on your infrastructure, business, geography, all of these requirement and other meaningful information should be detailed in a disaster recovery plan.

Table 9-1 suggests key items you can find in a disaster recovery plan and specifies different levels of requirements. This table is discussing data recovery and not application availability. Application availability must be handled by appropriate teams. Obviously it is highly recommended that all the teams work together with the data protection team when they are building their availability plans.

Table 9-1 Disaster recovery plan

Scope	Time of recovery (RTO) from a disaster ^a	Recovery Point Objectives (RPO)	Where IBM Spectrum Protect features fit	Associated DR description
Production database	Hours ^b	No data loss	IBM Spectrum Protect Data Protection for databases agent running within VM together with IBM Spectrum Protect Data protection for VMware and IBM Spectrum Protect server enabled for Node replication. IBM Spectrum Protect Snapshot would also fit if the database consistency is managed	Bi-directional failover site
Non production databases	One day	1 day	IBM Spectrum Protect Data Protection for databases agent running within VM together with IBM Spectrum Protect Data Protection for VMware and IBM Spectrum Protect server enabled for Node replication. In this case, backup frequency would be different than for the above line (Production Database)	Bi-directional failover site
Production data (non DB)	24 hours	24 hours	Spectrum Snapshot for VMware together with IBM Spectrum Protect for VMware to offload data onto IBM Spectrum Protect server enabled for node replication.	Bi-directional failover site
Non production data (non DB)	Days	24 hours	Spectrum Snapshot for VMware together with IBM Spectrum Protect for VMware to offload data onto IBM Spectrum Protect server enabled for node replication.	Production and DR site

Scope	Time of recovery (RTO) from a disaster ^a	Recovery Point Objectives (RPO)	Where IBM Spectrum Protect features fit	Associated DR description
Enterprise mails	Hours ^c	No data loss	IBM Spectrum Data Protection for Databases agent running within VM together with IBM Spectrum Protect Data Protection for VMware and IBM Spectrum Protect server enabled for node replication. IBM Spectrum Snapshot would also fit if the database consistency is managed.	Bi-directional failover site
Archived Data (long-term archive purpose)	Weeks	No data loss	IBM Spectrum Protect for VMware together with IBM Spectrum Protect server. For vaulting purpose, choose physical tape-based solution managed by IBM Spectrum Protect server Disaster Recovery Manager (included feature)	Bunker mode

a. Understand that this table assume the production site is no longer available, we are not talking about "in-place" recovery that could occur on a daily basis.

b. This value should be carefully defined as it directly linked to the amount of data to be recovered.

c. See footnote b.

9.3 Disaster recovery use cases

The disaster recovery use cases are discussed in this section.

9.3.1 Business requirements

As demonstrated in Table 9-1, IBM Spectrum Protect suite allows you to protect your virtual environment very well, using different ways based on your business requirements. All of the below cases are covered, whatever the type of data experiencing a disaster:

- ▶ Data deletion
- ▶ Data corruption
- ▶ System failure (isolated virtual machine failure)
- ▶ Isolated storage failure (VMware datastore loss of access)
- ▶ Global storage failure resulting from issue with underlying storage system
- ▶ Server room disaster

9.3.2 Active data including versioning

IBM Spectrum Protect disaster recovery capabilities brings value not only for protecting active active data, also all the previous backup versions of your environment. This is something very critical in the big data era.

To illustrate this concept, lets look at about VMware vSphere Site Recovery Manager.

First of all, VMware vSphere Site Recovery Manager requires underlying disk replication, most likely to use SAN, where IBM Spectrum Protect based solution only requires LAN to replicate the data between the two sites. Moreover, VMware vSphere Site Recovery Manager does not cover the case where there is an unexpected data deletion.

One more difference is that VMware vSphere Site Recovery Manager cannot restart a virtual machine in a specified point in time. Two things that would drive you to IBM Spectrum Protect:

- ▶ Disaster recovery using Data Protection for VMWare
- ▶ Disaster recovery using IBM Spectrum Protect Snapshot for VMware



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 errors
- ▶ How to open a call with IBM Support
- ▶ Frequently asked questions

10.1 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.

10.1.1 Common error messages

This link describes [common error messages](#) returned by VMware vStorage API for Data Protection (VDAP).

10.1.2 Restoration by using SAN transport method

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 about [SAN Best Practices](#).

The virtual machine template backups cannot be restored by using SAN transport because they cannot be backed up over the SAN.

10.1.3 Plug-in management

You might need to manually remove or unregister the Data Protection for VMware plug-in from the vSphere vCenter server.

To perform these tasks follow this guidance:

In C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin, use the commands shown in Example 10-1.

Example 10-1 Manually remove the plug-in

```
register_vcenter_extension.cmd
usage:
=====
"usage: register_vcenter_extension.cmd <vCenter Address> <vCenter UserID> <vCenter
Password> <GUI Web Server Port>"
"usage: register_vcenter_extension.cmd <vCenter Address> <vCenter UserID> <vCenter
Password> <GUI Web Server Port> <Local Host Fully Qualified Domain Name or IP
Address>"
=====

unregister_vcenter_extension.cmd
usage:
=====
"usage: unregister_vcenter_extension.cmd <vCenter Address> <vCenter UserID>
<vCenter Password>"
=====
```

The logging for the command is recorded in the file regtool.log (in the same directory as above) and overwritten each time a registration command is run.

10.2 Analyzing errors

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.

10.2.1 Web resources

The following resources provide useful information:

- ▶ If you are experiencing problems with your Data Protection for VMware installation, see the following IBM Spectrum Protect Support web site and search [IBM Knowledge Center](#).
- ▶ General IBM Spectrum Protect information can be found in [IBM Knowledge Center](#).
- ▶ Information about the IBM Tivoli Storage Manager for [VMware 7.1.6](#).
- ▶ Information about [IBM Spectrum Protect Snapshot](#).
- ▶ Various Technotes are available that might give you some hints to solve the issue on your own. A good starting point to have a view of the existing technotes is this technote, “[Links to IBM Spectrum Protect Family Featured Documents](#).”

The links provided in this document hold a wealth of information because tech docs are grouped in subjects, including the following :

- ▶ Hardware & Software Requirements
- ▶ Downloads and Fixes
- ▶ Flashes
- ▶ Known Issues and Limitations
- ▶ Update History
- ▶ Compatibility Information
- ▶ Documentation
- ▶ End of Support Information
- ▶ Announcement Letters

Before opening a call, it might also be useful to consult the known issues and limitations documents:

- ▶ “Known Issues and Limitations: [Data Protection for VMware V8.1](#)”
- ▶ “IBM Spectrum Protect V8.1 Windows Backup-Archive Client [known problems and limitations](#)”

The following resources are available for troubleshooting and tuning performance issues:

- ▶ “Resolving common performance problems with [virtual machine backup operations](#)”
- ▶ “[Tuning virtual machine backup operations](#)”

If you do not find a solution and you are entitled to support, collect the information by using the processes that are described at these websites:

- ▶ Collecting data for [Linux](#).
- ▶ Collecting data for [Windows](#).
- ▶ IBM Spectrum Protect [Snapshot for VMware](#).

10.3 How to open a call with IBM Support

In this section, we direct you to resources for more information and help in resolving errors.

10.3.1 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:

- a. 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 Spectrum Protect, 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 [Passport Advantage](#).
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](#).

Click **Contacts**.

- b. 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.

- c. 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 139.

Submitting the problem to IBM Software Support

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

Online

Go to [IBM Software Support](#).

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](#).

Click **Contacts**.

10.4 Frequently asked questions

An up-to-date frequently asked questions (FAQ) section is available in the [IBM Wiki](#).

Related publications

The publications 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 publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- ▶ *Tivoli Storage Manager as a Data Protection Solution*, SG24-8134

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Other publications

These 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

These 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.ibm.com/support/docview.wss?uid=swg21611903>

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services



REDP-5252-00

ISBN 0738456411

Printed in U.S.A.

Get connected

