IBM Spectrum Protect for Virtual Environments
Version 8.1.0

Data Protection for Microsoft Hyper-V Installation and User's Guide

IBM Spectrum Protect for Virtual Environments
Version 8.1.0

Data Protection for Microsoft Hyper-V Installation and User's Guide

Note:
Before you use this information and the product it supports, read the information in “Notices” on page 81.

First edition (December 2016)

This edition applies to version 8, release 1, modification 0 of IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V (product number 5725-X00) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2011, 2016.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2011, 2016

About this publication

This publication provides overview, planning, and user instructions for IBM Spectrum Protect™ for Virtual Environments: Data Protection for Microsoft Hyper-V.

Who should read this publication

This publication is intended for administrators and users who are responsible for implementing a backup solution with IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V in one of the supported environments.

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

- Microsoft Hyper-V Server 2012 or Microsoft Hyper-V Server 2012 R2
- The IBM® backup-archive client
- The IBM Spectrum Protect server

Publications

The IBM Spectrum Protect product family includes IBM Spectrum Protect Snapshot, IBM Spectrum Protect for Space Management, IBM Spectrum Protect for Databases, and several other storage management products from IBM.

To view IBM product documentation, see IBM Knowledge Center.

© Copyright IBM Corp. 2011, 2016

What's new in Version 8.1

Data Protection for Microsoft Hyper-V Version 8.1 introduces new features and updates.

For a list of new features and updates in this release, see Data Protection for Microsoft Hyper-V updates.

New and changed information in this product documentation is indicated by a vertical bar (|) to the left of the change.

© Copyright IBM Corp. 2011, 2016

Chapter 1. Protection for Microsoft Hyper-V virtual machines

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V is a licensed product that provides storage management services for virtual machines in a Microsoft Hyper-V environment.

Data Protection for Microsoft Hyper-V integrates IBM Spectrum Protect for Virtual Environments virtualization protection with the IBM backup-archive client to protect Microsoft Hyper-V virtual machines on Microsoft Windows Server 2012 or 2012 R2 systems.

Back up Hyper-V virtual machines

Data Protection for Microsoft Hyper-V creates an incremental forever full or incremental forever incremental backup of Hyper-V virtual machines in VHDX disk format. The virtual machine is backed up to the IBM Spectrum Protect server. Microsoft Volume Shadow Copy Service (VSS) is used to take a consistent snapshot of the virtual machine.

You can back up Hyper-V virtual machines that exist on a local disk, a SAN-attached disk, or cluster shared volume. For example, you can back up virtual machines that are stored on Cluster Shared Volumes (CSV) in a Hyper-V cluster environment or on Server Message Block (SMB) file shares that are on a remote system. You can back up any guest operating systems that are hosted by the Hyper-V server on remote shares, regardless of whether the guest operating system is supported by IBM Spectrum Protect.

The following backup types are supported for Microsoft Hyper-V virtual machines in VHDX disk format:

Incremental forever full backup
Creates a backup of snapshot disk data to the IBM Spectrum Protect server.

Incremental forever incremental backup
Creates a snapshot of the blocks that changed since the last incremental forever full backup.

For more information, see "Hyper-V backup support limitations" on page 6.

Restore an entire Hyper-V virtual machine

Each Hyper-V virtual machine backup is restored from the IBM Spectrum Protect server as a single entity. You can restore any guest operating systems that are hosted by the Hyper-V server regardless of whether the guest operating system is supported by IBM Spectrum Protect.

A Data Protection for Microsoft Hyper-V restore operation ensures that the same block on the production disk is only restored once. Older backup versions expire according to the IBM Spectrum Protect server management class policy that is associated with the virtual machine.

© Copyright IBM Corp. 2011, 2016

Restore an entire Hyper-V virtual machine to an alternative location

You can restore a Hyper-V virtual machine to an alternate virtual machine name, to an alternate location on the Hyper-V host, or both. You can also restore a Hyper-V virtual machine to a different Hyper-V host. However, to restore the virtual machine to a different host, you must run the restore operation from the Hyper-V host where the virtual machine is being restored to.

Restore a file from a Hyper-V virtual machine

Use this restore method when only one or more files must be restored. The files are manually copied from a mounted virtual machine disk that is accessed through an iSCSI target or partition. This method requires the IBM Spectrum Protect recovery agent to be installed.

Policy management at the virtual machine level

Storage requirements for Hyper-V virtual machine backups are determined by IBM Spectrum Protect server management classes. You can set different policies for different virtual machines. Although the default management class determines storage characteristics for all Hyper-V backups, you can override the default management class or specify a management class to use for the Hyper-V control files.

User interfaces

Complete all Data Protection for Microsoft Hyper-V backup, restore, and query tasks with the backup-archive client Java GUI or backup-archive command-line client. To restore one or more files from a Hyper-V virtual machine, use the IBM Spectrum Protect recovery agent GUI.

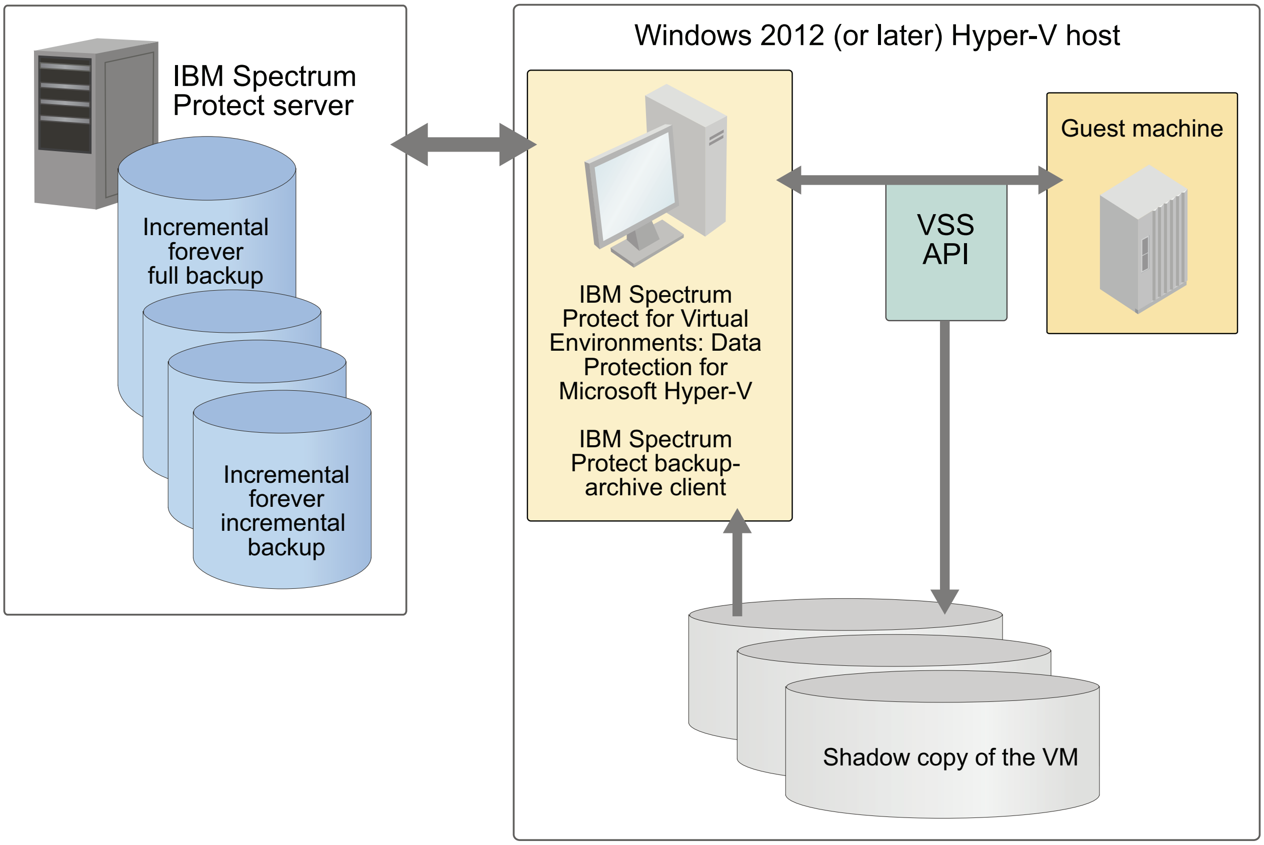

IBM Spectrum Protect server
Incremental forever full backup
Incremental forever incremental backup
Windows 2012 (or later) Hyper-V host
IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
IBM Spectrum Protect backup-archive client
VSS API
Guest machine
Shadow copy of the VM

Figure 1. High-level overview of IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V environment

Incremental forever backup strategy

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

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V provides a backup strategy called incremental forever. This backup solution requires only one initial full backup. Afterward, an ongoing (forever) sequence of incremental backups occurs. The incremental forever backup solution provides these advantages:

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

In addition, the restore process is optimized, as only the latest versions of blocks that belong to a restored backup are restored. Since the same area on the production disk is recovered only one time, the same block is not written to multiple times. As a result of these advantages, incremental forever is the preferred backup strategy.

Snapshot management with Windows PowerShell

On a Microsoft Hyper-V system, you can use Windows PowerShell “cmdlets” to remove (undo) snapshots that were created by IBM for a Hyper-V virtual machine.

You can use these cmdlets only on the Hyper-V system; you cannot remove snapshots from the Microsoft System Center Virtual Machine Manager.

Hyper-V systems issue cautionary messages to discourage you from editing virtual hard disks that contain snapshots, or virtual hard disks that are associated with a chain of differencing (incremental-forever) snapshots. Instead, use the cmdlets to manage snapshots to minimize the risk of data loss.

For a list of cmdlets that are available for Hyper-V, go to http://technet.microsoft.com/en-us/library/hh848559.aspx and read the information for the available cmdlets. Use the **`Get-VMSnapshot`** cmdlet with the **`-SnapshotType Recovery`** parameter to retrieve snapshots for a virtual machine. Use the **`Remove-VMSnapshot`** cmdlet to remove a snapshot. Removing a snapshot merges the information that the snapshot wrote to the snapshot differences file (the AVHDX file) back to the virtual machine hard disk (the VHDX file).

Documentation resources

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V software provides several components to assist with protecting your virtual machines. As a result, multiple documentation resources are provided to assist with specific tasks.

Table 1. Data Protection for Microsoft Hyper-V documentation resources

Documentation	Contents	Location
IBM Spectrum Protect for Virtual Environments Data Protection for Microsoft Hyper-V Installation and User's Guide	Overview information, strategy planning, installation, configuration, back up and restore scenarios, and command-line reference.	IBM Knowledge Center at https://www.ibm.com/support/knowledgecenter/SSERB6_8.1.0/ve.user/r_pdf_ve.html

Table 1. Data Protection for Microsoft Hyper-V documentation resources (continued)

Documentation	**Contents**	**Location**
Online help for the IBM Spectrum Protect backup-archive command-line client	Back up and restore tasks related to Hyper-V guests virtual machines.	Start the IBM Spectrum Protect backup-archive command line client by using either of the following methods: • On the Windows system, go to **Start** > **Apps by name** > **IBM** > **Backup-Archive Command Line**. • Open an Administrator command prompt window and change to the backup-archive client installation directory (**cd** `"C:\Program Files\tivoli\tsm\baclient"`). Run **`dsmc.exe`**. Access the help by using either of the following methods: • After you start the command line client, at the "tsm" prompt, enter **`help`** to display the table of contents for the help. • To display the help in its own window, open an Administrator command prompt window and change to the backup-archive client installation directory (**cd** `"C:\Program Files\tivoli\tsm\baclient"`). Run **`dsmc.exe help`** to display the help table of contents. You can also append a topic title to the command to display help for a topic. For example, `dsmc help options` displays the help topic that describes how to use client options; `dsmc help backup vm` displays the help for the **`backup vm`** command.
Online help for the IBM Spectrum Protect backup-archive GUI	Back up and restore tasks related to Hyper-V guests virtual machines.	Start the IBM Spectrum Protect backup-archive GUI client using either of the following methods: • On the Windows system, go to **Start** > **Apps by name** > **IBM** > **Backup-Archive GUI**. • Open an Administrator command prompt window and change to the backup-archive client installation directory (**cd** `"C:\Program Files\tivoli\tsm\baclient"`). Run **`dsm.exe`**. Access the help using either of the following methods: • Select the help icon and click **Help Topics** or Getting started. • You can also press the F1 key to open the **Help Topics** help.

Hyper-V backup support limitations

Before you attempt a backup operation, be aware that certain limitations apply.

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V does not back up Hyper-V virtual machines that use physical disks. The entire virtual machine (including virtual disks) is skipped and the backup operation fails.

Data Protection for Microsoft Hyper-V also does not back up Hyper-V virtual machines with attached iSCSI disks. This is because Data Protection for Microsoft Hyper-V uses Volume Shadow Copy Service (VSS) for backup operations and VSS cannot create a snapshot of the iSCSI disks. If you try to back up a virtual machine with attached iSCSI disks, the operation fails.

Data Protection for Microsoft Hyper-V supports incremental forever full backup and incremental forever incremental backup of Microsoft Hyper-V virtual machines in VHDX disk format only. To create an image backup of the full virtual machine in VHD or VHDX disk format, use the IBM backup-archive client without IBM Spectrum Protect - Data Protection for Microsoft Hyper-V installed on the system. Issue the backup-archive client **`dsmc backup vm`** *vmname* `-vmbackuptype=`**`hypervfull`** `-mode=`**`full`** command to create an image backup of all objects on a Microsoft Hyper-V virtual machine VHD or VHDX disk. Optionally, convert .vhd files to .vhdx format according to instructions available in Microsoft documentation.

The Microsoft Windows Management Instrumentation (WMI) Service (winmgmt) must be running on the systems where Data Protection for Microsoft Hyper-V, IBM Spectrum Protect backup-archive client, and IBM Spectrum Protect recovery agent are installed. Operations fail if the WMI Service is not running. Therefore, do not turn off the WMI Service.

Hyper-V configurations from Windows Server 2012 R2 are not compatible with Windows Server 2012. As a result, a restore operation from Windows Server 2012 R2 to Windows Server 2012 fails. However, a restore operation from Windows Server 2012 to Windows Server 2012 R2 succeeds. For more information, see the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/2868279.

Verify that no Exchange Server database is hosted on raw device mapped (RDM) disks in physical compatibility mode, independent disks, or on disks that are attached directly to the guest through in-guest iSCSI.

Chapter 2. Installing Data Protection for Microsoft Hyper-V

Determine system requirements

IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V requires 500 MB of disk space for installation and a supported operating system.

Data Protection for Microsoft Hyper-V requires the Hyper-V role to be installed on the Microsoft Windows Server 2012 or 2012 R2 system.

For detailed Data Protection for Microsoft Hyper-V software and hardware requirements, see *Data Protection for Microsoft Hyper-V Requirements* at http://www.ibm.com/support/docview.wss?uid=swg21993754.

Determine which features to install

Review the features that are available for you to install.

The following features are available for you to install with the IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V product download image:

- The Data Protection for Microsoft Hyper-V product code

  Provides virtualization protection for Microsoft Hyper-V virtual machines.

  Tip: The Data Protection for Microsoft Hyper-V product code is installed with every feature.

  To install the Data Protection for Microsoft Hyper-V product code, follow the steps in "Install Data Protection for Microsoft Hyper-V features with default settings" on page 8.
- The IBM backup-archive client

  When you offload backup workloads, the backup-archive client runs the operation on the backup server and "moves" the data to the IBM Spectrum Protect server. This client is referred to as the data mover.

  To install the backup-archive client, follow the steps in "Install the backup-archive client (data mover)" on page 8.
- The IBM Spectrum Protect recovery agent

  Provides virtual mount and file restore capability.

  To install the IBM Spectrum Protect recovery agent, follow the steps in "Install the IBM Spectrum Protect recovery agent" on page 10.

© Copyright IBM Corp. 2011, 2016

Install Data Protection for Microsoft Hyper-V features with default settings

Install the IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V software and the backup-archive client (data mover) without modifying features or installation directories.

About this task

To install Data Protection for Microsoft Hyper-V with default settings, complete the following steps:

Procedure

1. Download the Data Protection for Microsoft Hyper-V product image from IBM Passport Advantage®.
2. To start the installation program, double-click the `Setup.exe` file. Choose the language for the installation process, then click **Next**.
3. On the Welcome to the InstallShield Wizard for IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V suite page, click **Next**.
4. On the License Agreement page, read the terms of the license agreement. Click **I accept the terms in the license agreement**. If you do not accept the terms of the license agreement, the installation ends. Click **Next**
5. On the Installation Type page, the installation process begins immediately after you click **Typical Installation**. You cannot change your selection once the installation process begins. If you are sure that you want to install Data Protection for Microsoft Hyper-V and the backup-archive client (data mover) without modifying features or installation directories, click **Typical Installation**.

   Tip: The installation process might take several minutes to complete.
6. On the Install Wizard Completed page, click **Finish** to exit the wizard.

Results

Data Protection for Microsoft Hyper-V and the backup-archive client (data mover) are installed.

What to do next

Before you attempt a backup or restore operation, complete the tasks described in "Creating and modifying the client options file" on page 15.

Install the backup-archive client (data mover)

Install the backup-archive client and modify features or installation directories.

Before you begin

- The backup-archive client runs the operation on the backup server and "moves" the data to the IBM server. This client is referred to as the data mover.
- The IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V product code is also installed with this feature.

About this task

To install the backup-archive client (data mover), complete the following steps:

Procedure

1. Download the Data Protection for Microsoft Hyper-V product image from IBM Passport Advantage.
2. To start the installation program, double-click the `Setup.exe` file. Choose the language for the installation process, then click **Next**.
3. On the Welcome to the InstallShield Wizard for IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V suite page, click **Next**.
4. On the License Agreement page, read the terms of the license agreement. Click **I accept the terms in the license agreement**. If you do not accept the terms of the license agreement, the installation ends. Click **Next**
5. On the Installation Type page, click **Advanced Installation**.

   On the Advanced Installation page, the installation process begins immediately after you click **Install the IBM Spectrum Protect backup-archive client (data mover)**. You cannot change your selection after the installation process begins.
6. If you are sure that you want to install the backup-archive client (data mover), click **Install the IBM Spectrum Protect backup-archive client (data mover)**.
7. On the Welcome to the InstallShield Wizard for IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V suite page, click **Next**.
8. On the Destination Folder page, specify where to install Data Protection for Microsoft Hyper-V. You can accept the default location that is shown in the **Destination Folder** field or click **Change** to specify another location. Click **Next** after you make your selection.
9. On the Ready to Install the Program page, click **Install** to begin installing your selected components.
10. On the Install Wizard Completed page, click **Finish** to exit the wizard. The InstallShield Wizard begins installing the data mover.
11. On the Location to Save Files page, specify where to save the data mover files. You can accept the default location that is shown in the **Save files in folder** field or click **Change** to specify another location. Click **Next** after you make your selection.
12. On the Welcome to the InstallShield Wizard for IBM Spectrum Protect Client page, click **Next**.
13. On the Destination Folder page, specify where to install the software. You can accept the default location that is shown in the **Install IBM Client to** field or click **Change** to specify another location. Click **Next** after you make your selection.
14. On the Setup Type page, select one of the following the types: **Typical** or **Custom**.
    - **Typical**

      A typical installation installs the following features:
      - The backup-archive client GUI files (needed to use the Java™ GUI)
      - The backup-archive client web files (needed to use the web client)
      - The client API files (as needed by your client and operating system)
    - **Custom**

      A custom installation selects the same files as a typical installation. However, you can accept the default location that is shown in the **Install to** field or click **Change** to specify another location. Click **Space** to view required disk space.

    Click **Next** after you make your selection.

15. On the Ready to Install the Program page, click **Install** to begin installing your selected backup-archive client (data mover) features.

    Tip: After you click **Install**, the installation process might take several minutes to complete.
16. On the Install Wizard Completed page, click **Finish** to exit the wizard.

Results

The backup-archive client (and Data Protection for Microsoft Hyper-V) are installed.

What to do next

Before you attempt to back up a Hyper-V virtual machine, complete the tasks described in "Creating and modifying the client options file" on page 15.

Install the IBM Spectrum Protect recovery agent

Install the IBM Spectrum Protect recovery agent for virtual mount and file restore operations.

Before you begin

- The IBM Spectrum Protect recovery agent installation requires the system to be restarted. Therefore, to avoid possible issues that are related to restarting the Hyper-V host system, do not install the recovery agent on the Hyper-V host system.
- TCP ports `22` (SSH default port) and `3260` (iSCSI default port) must be open and available before you install the IBM Spectrum Protect recovery agent. To check the port status, opening a command prompt and issue the following commands:

  ```
  netstat -np TCP | find "22"
  ```

  ```
  netstat -np TCP | find "3260"
  ```
- The IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V product code is also installed with this feature.

About this task

To install the IBM Spectrum Protect recovery agent, complete the following steps on a virtual machine or other system that is not the Hyper-V host system:

Procedure

1. Download the Data Protection for Microsoft Hyper-V product image from IBM Passport Advantage.
2. To start the installation program, double-click the `Setup.exe` file. Choose the language for the installation process, then click **Next**.
   If you already completed a Typical Installation, the Program Maintenance page displays after you double-click the `Setup.exe` file:
   a. On the Program Maintenance page, click **Modify**.
   b. On the Custom Setup page, click **IBM Spectrum Protect recovery agent**, then click **Install**.
   c. Go to Step 11 on page 11 and follow the remaining installation steps.
3. On the Welcome to the InstallShield Wizard for IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V suite page, click **Next**.

4. On the License Agreement page, read the terms of the license agreement. Click **I accept the terms in the license agreement**. If you do not accept the terms of the license agreement, the installation ends. Click **Next**.
5. On the Installation Type page, click **Advanced Installation**.

   On the Advanced Installation page, the installation process begins immediately after you click **Install the IBM Spectrum Protect recovery agent**. You cannot change your selection once the installation process begins.
6. If you are sure that you want to install the recovery agent, click **Install the IBM Spectrum Protect recovery agent**.

   Tip: The installation process might take several minutes to complete.
7. On the Welcome to the InstallShield Wizard for IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V suite page, click **Next**.
8. On the Destination Folder page, specify where to install the software. You can accept the default location that is shown in the **Destination Folder** field or click **Change** to specify another location. Click **Next** after you make your selection.
9. On the Ready to Install the Program page, click **Install** to begin installing your selected components
10. On the Install Wizard Completed page, click **Finish** to exit the wizard.
11. On the Welcome to the InstallShield Wizard for IBM Spectrum Protect for Virtual Environments: Data Protection for Hyper-V suite page, click **Next**.
12. On the Software License Agreement page, read the terms of the license agreement. Click **I accept the terms in the license agreement**. If you do not accept the terms of the license agreement, the installation ends. Click **Next**.
13. On the Custom Setup page, you can click **Space** to view required disk space. Click **Change** to specify where to install this feature. The following user interfaces are installed:
    - The IBM Spectrum Protect recovery agent GUI
    - The IBM Spectrum Protect recovery agent command-line interface (`RecoveryAgentShell.exe`)

    Click **Next** after you make your selection.
14. On the Ready to Install the Program page, click **Install** to begin installing your selected components.
    - You are prompted to install the IBM Virtual Volume driver. This driver is used for mount operations. Click **Install** to install the driver. If you do not install the driver now, you are prompted again to install it when you attempt to mount a volume.
    - TCP ports `22` (SSH default port) and `3260` (iSCSI default port) must be open and available to complete the installation process. Click **OK**.
15. On the IBM Spectrum Protect for Virtual Environments InstallShield Wizard Completed page, click **Finish** to exit the wizard. You must restart your system after installation completes.

Results

The IBM Spectrum Protect recovery agent (and Data Protection for Microsoft Hyper-V) are installed.

What to do next

Before you attempt to mount a backed up Hyper-V virtual machine disk to restore a file, complete the tasks described in "Configuring the IBM Spectrum Protect recovery agent GUI" on page 19.

Installing in silent mode

Install all IBM Spectrum Protect for Virtual Environments and data mover features silently on a single system.

About this task

Restriction: All features are installed to their default location. You cannot silently install IBM Spectrum Protect for Virtual Environments and data mover features to a non-default location.

Procedure

1. Download the image from IBM Passport Advantage.
2. From a command prompt window, use the **cd** command to change to `<extract folder>TSM4VE_WIN`.
3. Enter the following command:

```
setup.exe /silent
```

4. Restart the system after installation completes.

   The following message is displayed the first time that you mount a volume:

```
The Virtual Volume Driver is not yet registered. Recovery Agent can register
the driver now. During registration, a Microsoft Windows Logo warning may be displayed.
Accept this warning to allow the registration to complete.
Do you want to register the Virtual Volume Driver now?
```

   You must register the Virtual Volume Driver to proceed with the IBM Spectrum Protect recovery agent operations.

Uninstalling Data Protection for Microsoft Hyper-V

The process for uninstalling IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V is the same for a new installation and for an upgraded version.

Before you begin

Restriction: You must unmount all virtual volumes before uninstalling the IBM Spectrum Protect recovery agent. Otherwise, these mounted virtual volumes cannot be unmounted after the IBM Spectrum Protect recovery agent is reinstalled.

Procedure

1. Go to **Start** > **Control Panel** > **Programs - Uninstall a program**.
2. On the Uninstall or change a program page, select **IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V** and click **Uninstall**.
3. On the Uninstall or change a program page, select **IBM client** and click **Uninstall**.

4. On the Uninstall or change a program page, select **IBM Spectrum Protect recovery agent** and click **Uninstall**.

Uninstalling Data Protection for Microsoft Hyper-V with the Microsoft Windows Installer Tool

Uninstall IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V from a Microsoft Windows Server Core with the Microsoft Windows Installer Tool.

Procedure

1. Locate the Data Protection for Microsoft Hyper-V **`UninstallString`** in the `Wow6432Node` registry path. For example:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\
   Uninstall\{060612C6-E661-4502-ADD0-AF912CDB02C9}]
   ```

2. Run the following command:

   ```
   C:\"C:\Program Files (x86)\InstallShield Installation Information\
   {060612C6-E661-4502-ADD0-AF912CDB02C9}\Setup.exe" -remove -runfromtemp
   ```

Chapter 3. Configuring Data Protection for Microsoft Hyper-V

After successfully installing the IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V software, you must configure the client before performing any backup and restore operations. You must also configure the IBM Spectrum Protect recovery agent to restore individual files.

Creating and modifying the client options file

The client options file is an editable text file that contains configuration information for the backup-archive client options that are used for IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V operations.

About this task

The first time that you start the Windows backup-archive client GUI, the installation program searches for an existing client options file, called `dsm.opt`. If this file is not detected, a client options file configuration wizard starts and prompts you to specify initial client configuration settings. When the wizard completes, it saves the information that you specified in the `dsm.opt` file. By default, the `dsm.opt` file is saved to `C:\Program Files\Tivoli\TSM\baclient`.

The options file must contain the following information to communicate with the server:

- The `VMBACKUPType HYPERVFULL` option must be specified.
- The host name or IP address of the IBM server.
- The port number that the server listens on for client communications. A default port number is configured by the client options file configuration wizard. You do not need to override this default port number unless your server is configured to listen on a different port.
- Your client node name. The node name is a name that uniquely identifies your client node. The node name defaults to the short host name of the computer that the client is installed on.

Additional client options can be specified, as needed.

Tip: Client options can also be set on the server in a *client option set*. Client options that are defined on the server in a client option set override client options that are set in the client options file.

A sample options file is copied to your disk when you install the backup-archive client. The file is called `dsm.smp`. By default, the `dsm.smp` file is copied to `C:\Program Files\Tivoli\TSM\config\`. You can view the contents of this file to see examples of different options and how they are specified. The file also contains comments that explain syntax conventions for include lists, exclude lists, and wildcard use. You can also use this file as a template for your client options file by editing it and saving it as `dsm.opt` in the `C:\Program Files\Tivoli\TSM\baclient` directory.

© Copyright IBM Corp. 2011, 2016

After the initial client options file is created, you can modify the client options by adding or changing the options as needed. You can modify the `dsm.opt` file in any of the following ways:

- By running the client options file configuration setup wizard
- By using the client preferences editor
- By editing the `dsm.opt` file with a text editor program, such as Notepad

Perform the following steps to modify the client options:

Procedure

1. Select a method to modify the file.

Method	Steps
Setup wizard	The configure wizard opens automatically when the backup-archive client is installed for the first time. If the wizard does not open automatically, complete the following steps: 1. Click **Start** > **All Programs** > **IBM Spectrum Protect** > **Backup-Archive GUI**. 2. Select **Utilities** > **Setup Wizard** > **Help me configure the Client Options File**. On-screen text and online help is available to provide guidance as you navigate through the wizard panels. This client options file configuration wizard offers limited choices and configures only the most basic options.
Preferences editor	1. Click **Start** > **All Programs** > **IBM Spectrum Protect** > **Backup-Archive GUI**. 2. Select **Edit** > **Client Preferences**. Select the tabs in the preferences editor to set client options. Specify the options in the dialog boxes, drop down lists, and other controls. Online help is provided. Click the question mark (?) icon to display the help topics for the online help for the tab that you are editing. You can set more options in the preferences editor than you can set in the setup wizard.
Edit the dsm.opt file	1. Edit the `dsm.opt` file by using a plain text editor. Each of the options is described in detail in the documentation in Chapter 5, “Options reference,” on page 43. This method is the most versatile way to set client options because not all options can be set in the client options file configuration wizard or in the preferences editor. 2. To comment out a setting, insert an asterisk (*) as the first character on the line that you want to comment out. Remove the asterisk to make the commented option active.

2. Save the changes.
   1. Changes made in the client options file configuration wizard and in the preferences editor are saved and recognized by the client when the wizard completes, or when you exit the preferences editor.
   2. If you edit the client options file with a text editor while the client is running, you must save the file and restart the client so the changes are detected.
3. Verify that your configuration is complete by making sure that you can view the virtual machines in your environment:
   - To verify your configuration with the IBM Spectrum Protect backup-archive command line client, issue the **`dsmc show vm`** command. A list of virtual machines that are available for backup displays.
   - To verify your configuration with the IBM Spectrum Protect backup-archive GUI, click **Actions** > **Backup VM**. In the Backup Virtual Machine window, expand the **Hyper-V VMs** node to show the virtual machines that are available for backup.

   If you can view the virtual machines in your environment, you are ready to back up your virtual machines as described in "**`Backup VM`**" on page 31.

What to do next

If you plan to run backup and restore operations in a cluster, complete the tasks described in "Configuring Data Protection for Microsoft Hyper-V in a cluster environment" before you attempt a backup or restore operation.

Configuring Data Protection for Microsoft Hyper-V in a cluster environment

Configuration consists of updating the dsm.opt files and registering the nodes for each physical server in the cluster.

Before you begin

You can use the Hyper-V failover clustering feature to allow Hyper-V virtual machines to fail over from one cluster node to another cluster node when an outage occurs. For information about installing this feature, and for information that describes how to set up a cluster configuration for Hyper-V virtual machines, see the Microsoft documentation for Hyper-V and your operating system.

In a failover cluster configuration, you can ensure that the Hyper-V virtual machines are backed up to (and restorable from) a single IBM Spectrum Protect server container, regardless of which cluster node is backing them up. You implement this configuration by creating a proxy relationship, on the IBM Spectrum Protect server, to allow each physical server node (`NODENAME` option) to perform operations on behalf of a node that serves as a container on the IBM Spectrum Protect server (`ASNODENAME` option). You can move virtual machines within the cluster and still back up data to the same container.

About this task

Before you begin, assign a unique node name for each physical server in the cluster (for example, Host1, Host2). Next, assign a node name that is the IBM Spectrum Protect server container for all the virtual machine backups in the cluster (for example, clusternode).

Procedure

Complete Step 1 through Step 3 on the IBM Spectrum Protect server:

1. Log on to the server and start an administrative client session in command line mode:

   ```
   dsmadmc -id=admin -password=admin
   ```

2. Issue the **REGISTER NODE** command to register each physical server node in the cluster, and the cluster node, to the server.
   For this example, you register the following nodes:

   ```
   REGISTER NODE HOST1 <password for HOST1>
   ```

   ```
   REGISTER NODE HOST2 <password for HOST2>
   ```

   ```
   REGISTER NODE CLUSTERNODE <password for CLUSTERNODE>
   ```

   The `ASNODENAME` value (`CLUSTERNODE`) identifies a container on the server where files are stored that were backed up by the physical server nodes in the cluster.

3. Issue the **GRANT PROXYNODE** command to grant proxy authority to each physical server node in the cluster. This proxy authority allows each physical server node in the cluster to back up files to the `CLUSTERNODE`.
   For this example, you register the following proxy authority:
   a. This command allows HOST1 to perform operations on behalf of CLUSTERNODE:

      ```
      GRANT PROXYNODE TARGET=CLUSTERNODE AGENT=HOST1
      ```

   b. This command allows HOST2 to perform operations on behalf of CLUSTERNODE:

      ```
      GRANT PROXYNODE TARGET=CLUSTERNODE AGENT=HOST2
      ```

Complete Step 4 through Step 6 on each physical server node in the cluster:

4. Install and configure the IBM Spectrum Protect backup-archive client on each physical server node in the cluster.
   For detailed instructions, see the following contents:
   - "Install the backup-archive client (data mover)" on page 8
   - "Creating and modifying the client options file" on page 15
5. Identify each physical server node with a unique nodename, and set the `NODENAME` option in the dsm.opt file on each physical server node in the cluster.
   For this example, assume that you specified the following values for the `NODENAME` option:
   - In the dsm.opt file on Host1, you specified `NODENAME HOST1`
   - In the dsm.opt file on Host2, you specified `NODENAME HOST2`
6. Set the `ASNODENAME` option in the dsm.opt file on each physical server node in the cluster.
   - The `ASNODENAME` value must be the same in all dsm.opt files in the cluster.
   - The `ASNODENAME` value must not match any `NODENAME` value in any dsm.opt files in the cluster.

   For this example, assume that you specified the following values for the `ASNODENAME` option:
   - In the dsm.opt file on Host1, you specified `ASNODENAME CLUSTERNODE`
   - In the dsm.opt file on Host2, you specified `ASNODENAME CLUSTERNODE`

Results

When either of the nodes (HOST1, HOST2) backs up data to the IBM Spectrum Protect server, the backups are stored in the container named `CLUSTERNODE`. Both nodes (HOST1, HOST2) can back up or restore data from that IBM Spectrum Protect server container.

Example

For example, when this command is issued on HOST2, it performs an incremental forever full backup of virtual machine VM1 (owned by HOST2) to the IBM Spectrum Protect server container identified by CLUSTERNODE:

```
dsmc backup vm VM1 -vmbackuptype=hypervfull -mode=iffull -asnode=clusternode
```

Configuring the IBM Spectrum Protect recovery agent GUI

You must set up the IBM Spectrum Protect recovery agent GUI for mount and file restore operations.

Before you begin

These configuration tasks must be completed before you use the IBM Spectrum Protect recovery agent GUI.

Procedure

1. Log on to the system where you want to restore files. The IBM Spectrum Protect recovery agent must be installed on the system.
2. Click **Select IBM Spectrum Protect server** in the IBM Spectrum Protect recovery agent GUI to connect to the IBM Spectrum Protect server.

   Specify the following options:

   Server address
   Enter the IP address or host name of the IBM Spectrum Protectserver.

   Server port
   Enter the port number that is used for TCP/IP communication with the server. The default port number is 1500.

   Node access method:

   Asnodename
   Select this option to use a proxy node to access the virtual machine backups that are in the target node. The proxy node is a node that is granted "proxy" authority to perform operations on behalf of the target node.

   Typically, you use the `grant proxynode` command to create the proxy relationship between two existing nodes.

   If you select this option, complete the following steps:

   a. Enter the name of the target node (the node where the virtual machine backups are located) in the **Target Node** field.
   b. Enter the name of the proxy node in the **Authentication node** field.
   c. Enter the password for the proxy node in the **Password** field.
   d. Click **OK** to save these settings and exit the IBM Spectrum Protectpage.

When you use this method, the IBM Spectrum Protect recovery agent user knows only the proxy node password, and the target node password is protected.

Fromnode

Select this option to use a node with access limited only to the snapshot data of specific virtual machines in the target node.

Typically, this node is given access from the target node that owns the virtual machine backups by using the `set access` command:

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

For example, this command gives the node named `myMountNode` the authority to restore files from the virtual machine named `myTestVM`:

```
set access backup -TYPE=VM myTestVM myMountNode
```

If you select this option, complete the following steps:

a. Enter the name of the target node (the node where the virtual machine backups are located) in the **Target Node** field.
b. Enter the name of the node that is given limited access in the **Authentication node** field.
c. Enter the password for the node that is given limited access in the **Password** field.
d. Click **OK** to save these settings and exit the IBM Spectrum Protect page.

When you use this method, you can see a complete list of backed-up virtual machines. However, you can restore only those virtual machine backups to which the node was granted access. In addition, the snapshot data is not protected from expiration on the server.

Direct Select this option to authenticate directly to the target node (the node where the virtual machine backups are located).

If you select this option, complete the following steps:

a. Enter the name of the target node (the node where the virtual machine backups are located) in the **Authentication node** field.
b. Enter the password for the target node in the **Password** field.
c. Click **OK** to save these settings and exit the IBM Spectrum Protectpage.

Use Password access generate

When this option is selected and the password field is empty, the IBM Spectrum Protect recovery agent authenticates with an existing password that is stored in the registry. If not selected, you must manually enter the password.

To use this option, you must first manually set an initial password for the node to which the option applies. You must specify the initial password when you connect to the IBM Spectrum Protect node for the first time by entering the password in the **Password** field and selecting the **Use Password access generate** check box.

However, when you use the local data mover node as the **Authentication node**, the password might already be stored in the registry. As a result, select the **Use Password access generate** check box and do not enter a password.

The IBM Spectrum Protect recovery agent queries the specified server for a list of protected virtual machines, and shows the list.

3. Set the following mount, backup, and restore options by clicking **Settings**:

Virtual Volume write cache
The IBM Spectrum Protect recovery agent that is running on the backup proxy host saves data changes on a virtual volume in the write cache. By default, the write cache is enabled and the maximum cache size is 90% of the available space for the selected folder. To prevent the system volume from becoming full, change the write cache to a path on a volume other than the system volume.

Folder for temporary files
Specify the path where data changes are saved. The write cache must be on a local drive and cannot be set to a path on a shared folder.

Cache size
Specify the size of the write cache. The maximum allowed cache size is 90% of the available space for the selected folder.

Restriction: To prevent any interruption during restore processing, exclude the write cache path from all antivirus software protection settings.

Data Access
Specify the type of data to be accessed. If you are using an offline device (such as tape or virtual tape library), you must specify the applicable data type.

Storage type
Specify one of the following storage devices from which to mount the snapshot:

Disk/File
The snapshot is mounted from a disk or file. This device is the default.

Tape The snapshot is mounted from a tape storage pool. When this option is selected, it is not possible to mount multiple snapshots.

VTL The snapshot is mounted from an offline virtual tape library. Concurrent mount sessions on the same virtual tape library are supported.

Requirement: When the storage type is changed, you must restart the service for the changes to take effect.

Disable expiration protection
During a mount operation, the snapshot on the IBM Spectrum Protect server is locked to prevent it from expiring during the operation. Expiration might occur because another snapshot is added to the mounted snapshot sequence. This value specifies whether to disable expiration protection during the mount operation.

- To protect the snapshot from expiration, do not select this option. This option is cleared by default. The snapshot on the IBM Spectrum Protect server is locked and the snapshot is protected from expiration during the mount operation.

- To disable expiration protection, select this option. The snapshot on the IBM Spectrum Protect server is not locked and the snapshot is not protected from expiration during the mount operation. As a result, the snapshot might expire during the mount operation. This expiration can produce unexpected results and negatively impact the mount point. For example, the mount point can become unusable or contain errors. However, expiration does not affect the current active copy. The active copy cannot expire during an operation.

  When the snapshot is on a target replication server, the snapshot cannot be locked because it is in read-only mode. A lock attempt by the server causes the mount operation to fail. To avoid the lock attempt and prevent such a failure, disable expiration protection by selecting this option.

Read Ahead size (in 16-KB blocks)
Specify the number of extra data blocks that are retrieved from the storage device after a read request is sent to a single block. The default values are as follows:

- Disk or file: 64
- Tape: 1024
- VTL: 64

The maximum value for any device is 1024.

Read Ahead cache size (in blocks)
Specify the size of the cache where the extra data blocks are stored. The default values are as follows:

- Disk or file: 10000
- Tape: 75000
- VTL: 10000

Since each snapshot has its own cache, make sure to plan how many snapshots are mounted or restored simultaneously. The cumulative cache size cannot exceed 75000 blocks.

Driver timeout (seconds)
This value specifies the amount of time to process data requests from the file system driver. If processing is not completed in time, the request is canceled and an error is returned to the file system driver. Consider increasing this value when you experience timeouts. For example, timeouts might occur when the network is slow, the storage device is busy, or multiple mount sessions are being processed. The default values are as follows:

- Disk or file: 60
- Tape: 180
- VTL: 60

Click **OK** to save your changes and exit the **Settings**.

4. Verify that each IBM Spectrum Protect server node (that was specified with the `Asnodename` and `Fromnode` options) allows backups to be deleted. The IBM Spectrum Protect recovery agent creates unused temporary objects during operations. The `BACKDELete=Yes` server option allows these objects to be removed so that they do not accumulate in the node.

a. Log on to the IBM Spectrum Protect server and start an administrative client session in command-line mode:

```
dsmadmc -id=admin -password=admin -dataonly=yes
```

b. Enter this command:

```
Query Node <nodename> Format=Detailed
```

Make sure the command output for each node includes the following statement:

```
Backup Delete Allowed?: Yes
```

If this statement is not included, update each node with this command:

```
UPDate Node <nodename> BACKDELete=Yes
```

Run the `Query Node` command again for each node to verify that each node allows backups to be deleted.

Enabling secure communication from the recovery agent to the IBM Spectrum Protect server

If the IBM Spectrum Protect server is configured to use the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol, you can enable the recovery agent to communicate with the server by using the protocol.

Before you begin

Consider the following requirements before you begin configuration for secure communication to the server:

- Each server that is enabled for SSL must have a unique certificate. The certificate can be one of the following types:
  - A certificate that is self-signed by the server.
  - A certificate that is issued by a third-party certificate authority (CA) certificate. The CA certificate can be from a company such as Symantec or Thawte, or an internal certifcate that is maintained within your company.
- For performance reasons, use SSL or TLS only for sessions where security is required. Consider adding more processor resources on the server system to manage the increased requirements.
- For a client to connect to a server that is using TLS Version 1.2, the certificate signature algorithm must be Secure Hash Algorithm 1 (SHA-1) or later. If you are using a self-signed certificate to a server that is using TSL V1.2, you must use the `cert256.arm` certificate. Your IBM Spectrum Protect administrator might need to change the default certificate on the server.
- To disable security protocols that are less secure than TLS 1.2, add the **`SSLDISABLELEGACYtls yes`** option to the `C:\windows\system32\fb.opt` or `C:\Windows\SysWOW64\fb.opt` file. TLS 1.2 or later helps to prevent attacks by malicious programs.

Enabling secure communication by using an IBM Spectrum Protect server self-signed certificate

If the IBM Spectrum Protect server is using a self-signed certificate, you must obtain a copy of that certificate from the server administrator and configure the recovery agent to communicate with the server by using the SSL or TLS protocol.

About this task

Each server generates its own certificate. Version 6.3 and later servers generate files that are named `cert256.arm` if the server is using TLS 1.2 or later or `cert.arm` if the server is using an earlier version of SSL or TLS. Server versions earlier than V6.3 generate files that are named `cert.arm` regardless of the protocol. You must choose the certificate that is set as the default on the server.

The certificate file is stored on the server workstation in the server instance directory. For example, `C:\IBM\tivoli\tsm\server\bin\cert256.arm`. If the certificate file does not exist, the certificate file is created when you restart the server with these options set.

Procedure

To enable SSL or TLS communication from the recovery agent to the server by using a self-signed certificate:

1. Append the GSKit binary path and library path to the PATH environment variable on the client. For example:

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. If you are configuring SSL or TLS on the client for the first time, you must create the client local key database dsmcert.kdb. From the `C:\Windows\SysWOW64` directory, run the **`gsk8capicmd_64`** command as shown in the following example:

   ```
   gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
   ```

   The password that you provide is used to encrypt the key database. The password is automatically stored encrypted in the stash file (dsmcert.sth). The stash file is used by the client to retrieve the key database password.
3. Obtain the server self-signed certificate.
4. Import the certificate in to the dsmcert.kdb database. You must import the certificate for each client in to the dsmcert.kdb. From the `C:\Windows\SysWOW64` directory, run the **`gsk8capicmd_64`** command as shown in the following example:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Server server_name self-signed key"
   -file path_to_certificate -format ascii -trust enable
   ```

   Multiple server certificates can be added to the dsmcert.kdb database so that the client can connect to different servers. Different certificates must have different labels. Use meaningful names for the labels.

   Important: For a disaster recovery of the server, if the certificate has been lost, the server automatically generates a new certificate. Each client must then import the new certificate.
5. After the server certificate is added to the dsmcert.kdb database, add the `ssl yes` option to the `C:\Windows\SysWOW64\fb.opt` file and update the value of the `tcpport` option.

Important:

The server is normally set up for SSL and TLS connections on a different port than non-SSL and TLS connections. Do not specify a non-SSL or TLS port number for the `tcpport` value. If the value of `tcpport` is incorrect, the recovery agent cannot connect to the server.

You cannot connect to a non-SSL or TLS port with a recovery agent that is enabled for SSL or TLS or connect a SSL or TLS port to a recovery agent that is not enabled for SSL or TLS.

6. Set the correct SSL or TLS ports in the following recovery agent configuration files:
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Enabling secure communication by using a third-party certificate

If the IBM Spectrum Protect server is using a third-party certificate authority (CA), you must obtain the CA root certificate.

About this task

If the certificate was issued by a CA such as Symantec or Thawte, the client is ready for SSL or TLS and you can skip the following configuration steps. For the list of preinstalled CA root certificates, see Certificate Authorities root certificates.

If the certificate was not issued by a preinstalled root certificate or is an internal CA certificate that is maintained within your company, you must configure the recovery agent to communicate with the server by using the SSL or TLS protocol.

Procedure

To enable SSL or TLS communication from the recovery agent to the server by using a CA certificate:

1. Append the GSKit binary path and library path to the PATH environment variable. For example:

```
set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
    C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```

2. If you are configuring SSL or TLS on the client for the first time, you must create the client local key database dsmcert.kdb. For clients, from the `C:\Windows\SysWOW64` directory, run the **`gsk8capicmd_64`** command as shown in the following example:

```
gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw password -stash
```

   The password that you provide is used to encrypt the key database. The password is automatically stored encrypted in the stash file (dsmcert.sth). The stash file is used by the client to retrieve the key database password.

3. Obtain the CA certificate.
4. Import the certificate in to the dsmcert.kdb database. You must import the certificate for each client in to the dsmcert.kdb. For clients, from the `C:\Windows\SysWOW64` directory, run the **`gsk8capicmd_64`** command as shown in the following example:

```
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "XYZ Certificate Authority"
-file path_to_CA_root_certificate -format ascii -trust enable
```

Multiple server certificates can be added to the dsmcert.kdb database so that the client can connect to different servers. Different certificates must have different labels. Use meaningful names for the labels.

Important: For a disaster recovery of the server, if the certificate has been lost, the server automatically generates a new certificate. Each client must import the new certificate.

5. After the server certificate is added to the dsmcert.kdb database, add the `ssl yes` option to the `C:\Windows\SysWOW64\fb.opt` file and update the value of the `tcpport` option.

   Important:

   The server is normally set up for SSL and TLS connections on a different port than non-SSL and TLS connections. Do not specify a non-SSL or TLS port number for the `tcpport` value. If the value of `tcpport` is incorrect, the recovery agent cannot connect to the server.

   You cannot connect to a non-SSL or TLS port with a recovery agent that is enabled for SSL or TLS or connect a SSL or TLS port to a recovery agent that is not enabled for SSL or TLS.
6. Set the correct SSL or TLS ports in the following recovery agent configuration files:
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Manually configuring an iSCSI device

You must configure the Windows system that is used during an iSCSI mount operation. The snapshot is mounted from IBM server storage.

Before you begin

Review the following iSCSI requirements before you proceed with this task:

- During an iSCSI mount, an iSCSI target is created on the IBM Spectrum Protect recovery agent system. You can connect to the iSCSI target from any system to create a volume that contains the backup data. Also, you can then mount this volume from another system.
- iSCSI initiator is required on any system that must connect to the iSCSI target.
- Make sure that an iSCSI initiator is installed on the system where the data is to be restored.
- Microsoft iSCSI Initiator is not required on the IBM Spectrum Protect recovery agent system.

Review the following disk and volume requirements before you proceed with this task:

- If a volume spans several disks, you must mount all the required disks. When mirrored volumes are used, mount only one of the mirrored disks. Mounting one disk prevents a time-consuming synchronization operation.
- If multiple dynamic disks were used on the backup system, these disks are assigned to the same group. As a result, Windows Disk Manager might consider some disks as missing and issue an error message when you mount only one

disk. Ignore this message. The data on the backed up disk is still accessible, unless some of the data is on the other disk. This issue can be solved by mounting all the dynamic disks.

About this task

Complete these tasks to configure the Windows system that is used during an iSCSI mount operation:

Procedure

1. On the IBM Spectrum Protect recovery agent system, open port `3260` in the LAN firewall and the Windows client firewall. Record the iSCSI initiator name on the system where data is to be restored.

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

   ```
   iqn.1991-05.com.microsoft:hostname
   ```
2. Complete these tasks on the system where the IBM Spectrum Protect recovery agent (or iSCSI target) is installed:
   a. Start the IBM Spectrum Protect recovery agent GUI. Complete the Select IBM Spectrum Protect server and Select snapshot dialogs and click **Mount**.
   b. In the Choose mount destination dialog, select **Mount an iSCSI target**.
   c. Create a target name. Make sure that it is unique and that you can identify it from the system that runs the iSCSI initiator. For example:

      ```
      iscsi-mount-tsm4ve
      ```
   d. Enter the iSCSI Initiator name that was recorded in Step 1 and click **OK**.
   e. Verify that the volume you just mounted is displayed in the Mounted Volumes field.
3. Locate and start the iSCSI Initiator program on the initiator system that was selected in Step 1:
   a. Connect to the iSCSI target:
      1) In the Targets tab, enter the TCP/IP address of the IBM Spectrum Protect recovery agent (iSCSI target) used in Step 2 in the Target: dialog. Click **Quick Connect**.
      2) The Quick Connect dialog shows a target that matches the target name that was specified in Step 2c. If it is not already connected, select this target and click **Connect**.
   b. On the initiator system, go to **Control Panel** > **Administrative Tools** > **Computer Management** > **Storage** > **Disk Management**.
      1) If the mounted iSCSI target is listed as Type=Foreign, right-click **Foreign Disk** and select **Import Foreign Disks**. The Foreign Disk Group is selected. Click **OK**.
      2) The next screen shows the type, condition, and size of the Foreign Disk. Click **OK** and wait for the disk to be imported.
      3) When the disk import completes, press **F5** (refresh). The mounted iSCSI snapshot is visible and contains an assigned drive letter. If drive letters are not automatically assigned, right-click the required partition and select **Change Drive Letters or Paths**. Click **Add** and select a drive letter.
4. Open Windows Explorer (or other utility) and browse the mounted snapshot for a file restore operation.
5. After the file is restored, complete these tasks:

a. Disconnect each iSCSI target by using the iSCSI Initiator Properties dialog.
b. Dismount the volume from Step 2 by selecting the volume in the IBM Spectrum Protect recovery agent GUI and clicking **Dismount**.

Chapter 4. Command reference

The following sections contain detailed information about each of the client commands that are used for IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V operations.

Issue these commands from the IBM backup-archive command line client. Start the command line client using either of the following methods on the Windows system:

- Go to **Start** > **Apps by name** > **IBM** > **Backup-Archive Command Line**.
- Open an Administrator command prompt window and change to the backup-archive client installation directory (`cd "C:\Program Files\tivoli\tsm\baclient"`). Run **`dsmc.exe`**.

To complete these tasks from the IBM Spectrum Protect backup-archive GUI, start the backup-archive GUI client using either of the following methods on the Windows system:

- Go to **Start** > **Apps by name** > **IBM** > **Backup-Archive GUI**.
- Open an Administrator command prompt window and change to the backup-archive client installation directory (`cd "C:\Program Files\tivoli\tsm\baclient"`). Run **`dsm.exe`**.

Access related GUI task help using either of the following methods:

- Select the help icon and click **Help Topics** or Getting started.
- You can also press the F1 key to open the **Help Topics** help.

Reading syntax diagrams

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

- The ►►─── symbol indicates the beginning of a syntax diagram.
- The ───► symbol at the end of a line indicates that the syntax diagram continues on the next line.
- The ►─── symbol at the beginning of a line indicates that a syntax diagram continues from the previous line.
- The ───►◄ symbol indicates the end of a syntax diagram.

Syntax items, such as a keyword or a variable, can be:

- On the line (required element)
- Above the line (default element)
- Below the line (optional element)

Symbols

Enter these symbols *exactly* as they appear in the syntax diagram.

- * Asterisk
- *{ }* Braces
- *:* Colon
- , Comma

© Copyright IBM Corp. 2011, 2016

- = Equal Sign
- - Hyphen
- () Parentheses
- . Period
- Space
- ″ quotation mark
- ′single quotation mark

Variables

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

```
►►──cmd_name──<var_name>──────────────────────────────────────────►◄
```

Repetition

An arrow returning to the left means that the item can be repeated. A character within the arrow means that you must separate repeated items with that character.

```
      ┌─,────┐
      ▼      │
►►────repeat─┴────────────────────────────────────────────────────►◄
```

A footnote (1) by the arrow refers to a limit that tells how many times the item can be repeated.

```
      ┌─,─────────────┐
      │ (1)           │
      ▼               │
►►────────────repeat──┴───────────────────────────────────────────►◄
```

Notes:

1 Specify *repeat* up to 5 times.

Required choices

When two or more items are in a stack and one of them is on the line, you *must* specify one item.

In this example, you must choose A, B, or C.

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

Optional choices

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

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

When two or more items are in a stack below the line, all of them are optional. In the second example, you can choose A, B, C, or nothing at all.

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

Repeatable choices

A stack of items followed by an arrow returning to the left indicates that you can select more than one item, or in some cases, repeat a single item.

In this example, you can select any combination of A, B, or C.

```
              ┌─,───┐
              ▼     │
►►──cmd_name───┬─A─┬┴────────────────────────────────────────────►◄
               ├─B─┤
               └─C─┘
```

Defaults

Defaults are above the line. The default is selected unless you override it, or you can select the default explicitly. To override the default, include an option from the stack below the line.

In this example, A is the default. Select either B or C to override A.

```
              ┌─A─┐
►►──cmd_name──┼───┼──────────────────────────────────────────────►◄
              ├─B─┤
              └─C─┘
```

Backup VM

Use the **Backup VM** command to back up Hyper-V virtual machines.

You can back up Hyper-V guests that exist on a local disk, a SAN-attached disk, a cluster shared volume, or guests that exist on a remote file server share. Remote file server shares must be on a Windows Server 2012 (or newer) system. In addition, remote file shares must be Server Message Block (SMB) 3.0 with the File Server VSS Agent Service installed on the server.

You must specify the backup mode to use when backing up a virtual machine by adding the **-mode** parameter on the command line. The following modes can be specified:

IFFull Incremental-forever-full mode. In this mode, a snapshot of all used blocks on a virtual machine's disks are backed up to the server. The backup includes configuration information, and all of the disks.

IFIncremental
Incremental-forever-incremental. In this mode, a snapshot is created of the blocks that have changed since the last incremental forever backup, whether full or incremental. The backup includes configuration information, and all of the disks.

Syntax

```
                                                          ┌─IFIncremental─┐
►►──Backup VM──vmname───VMBACKUPType =──HYPERVFULL───MODE =─┼───────────────┼──────────►
                                                          └─IFFull────────┘

►─┬─────────────────────┬──┬──────────┬──┬───────────────────┬────────────────────►◄
  └─-VMBACKUPUPDATEGUID─┘  └─-PREview─┘  └─-DETail── ─options─┘
```

Parameters

vmname
Specify the name of the virtual machine that you want to back up; the name is case-sensitive. To specify multiple virtual machines, use the `domain.vmfull` option.

Wildcards can be used in virtual machine names.

-VMBACKUPType
Optional parameter for backing up a Hyper-V virtual machine. The default is the value that is required for Hyper-V backups: `-VMBACKUPType=HYPERVFULL`.

-VMBACKUPUPDATEGUID
This option updates the globally unique identifier (GUID) for the virtual machine that you are backing up. This parameter is intended for use only in the following scenario:

You want to restore an already backed up virtual machine named ORION. But, before you shut down and replace the copy of ORION that is running in your production environment, you want to verify the configuration of the restored virtual machine before you use it to replace the existing ORION.

1. You restore the ORION virtual machine and give it a new name: `dsmc restore vm Orion -vmname=Orion2`
2. You update and verify the ORION2 virtual machine and determine that it is ready to replace the existing virtual machine that is named ORION.
3. You power down and delete ORION.
4. You rename ORION2 so it is now named ORION.
5. The next time that you backup ORION, by using either an incremental-forever full, or incremental-forever-incremental backup, you add the **`-VMBACKUPUPDATEGUID`** parameter to the **`backup vm`** command. This option updates the GUID, on the IBM server, so the new GUID is associated with the stored backups for the ORION virtual machine. The chain of incremental backups is preserved; there is no need to delete existing backups and replace them with new backups.

-PREView

This parameter displays additional information about a virtual machine, including the labels of the Hyper-V virtual hard disks (VHDX) that are in the virtual machine.

When you issue the `-preview` option, the backup operation does not start. You must issue the backup command without the `-preview` option to start the backup operation.

-DETail

This parameter displays detailed information about a virtual machine. Use this option with `-preview` to view more details about the disks that are involved in the backup operation.

When you issue the `-detail` option, the backup operation does not start. You must issue the backup command without the `-detail` option to start the backup operation.

Example commands

This command starts an incremental-forever-incremental backup of a Hyper-V virtual machine that is named "VM1":

```
dsmc backup vm VM1 -vmbackuptype=hypervfull -mode=ifincremental
```

This command starts an incremental-forever-incremental backup of a Hyper-V virtual machine that is named "VM3":

```
dsmc backup vm VM3 -vmbackuptype=hypervfull -mode=ifincremental -preview
```

In the command output, the `-preview` parameter displays the VHDX labels in the virtual machine:

```
VM Name: VM3

 Domain Keyword:       all-vm
 Mode:                 Incremental Forever - Incremental
 Target Node Name:     NODE1
 Data Mover Node Name: NODE1
 Cluster Resource:     Yes

 Disk[1]
 Name: c:\ClusterStorage\Volume1\Hyper-V\VM3\VM3.VHDX
 Capacity:             40.00 GB
 Size:                 9.09 GB
 Full Backup:          included
 Incremental Backup:   excluded
 Disk Type:            VHDX
 Number of Subdisk:    1

 Disk[2]
 Name: c:\ClusterStorage\Volume3\Hyper-V\VM3\VM3-DISK2.VHDX
 Capacity:             127.00 GB
 Size:                 4.00 MB
 Full Backup:          included
 Incremental Backup:   excluded
 Disk Type:            VHDX
 Number of Subdisk:    1
```

When the `-detail` parameter is specified with the `-preview` parameter, the VHDX labels and their subdisks are shown:

```
VM Name: VM3

 Domain Keyword:       all-vm
 Mode:                 Incremental Forever - Incremental
 Target Node Name:     NODE1
 Data Mover Node Name: NODE1
 Cluster Resource:     Yes

 Disk[1]
 Name: c:\ClusterStorage\Volume1\Hyper-V\VM3\VM3.VHDX
 Capacity:             40.00 GB
 Size:                 9.09 GB
 Full Backup:          included
 Incremental Backup:   excluded
 Disk Type:            VHDX
 Number of Subdisk:    1

 Subdisk[1]
 Name: c:\ClusterStorage\Volume1\Hyper-V\VM3\VM3_9B26166-9C3E.avhdx
 Capacity:             40.00 GB
 Size:                 1.25 GB
 Full Backup:          included
 Incremental Backup:   included
 Disk Type:            AVHDX

 Disk[2]
 Name: c:\ClusterStorage\Volume3\Hyper-V\VM3\VM3-DISK2.VHDX
 Capacity:             127.00 GB
 Size:                 4.00 MB
 Full Backup:          included
 Incremental Backup:   excluded
 Disk Type:            VHDX
 Number of Subdisk:    1

 Subdisk[1]
 Name: c:\ClusterStorage\Volume3\Hyper-V\VM3\VM3-Disk2_243D063-9CD9.avhdx
 Capacity:             127.00 GB
 Size:                 4.00 MB
 Full Backup:          included
 Incremental Backup:   included
 Disk Type:            AVHDX
```

Options file examples

In this example, the `domain.vmfull` option specifies these virtual machines:

```
domain.vmfull BigVM,myGentoox64,HPV2VM3-OLD,Local10
```

This command starts an incremental-forever-incremental backup of all Hyper-V virtual machines specified in the `domain.vmfull` option. It also displays preview information about each virtual machine:

```
dsmc backup vm -vmbackuptype=hypervfull -mode=iffull -preview
```

The following output is shown:

```
1. VM Name: BigVM

 Domain Keyword:       all-vm
 Mode:                 Incremental Forever - Full
 Target Node Name:     MSF
 Data Mover Node Name: MSF
 Cluster Resource:     No

 Disk[1]
 Name: \\lingonberry\c$\Users\michael\Documents\Storage\BigVM.vhdx
 Capacity:             5.85 TB
 Size:                 5.00 MB
 Full Backup:          included
 Incremental Backup:   excluded
 Disk Type:            VHDX
 Number of Subdisk:    0

2. VM Name: Gentoox64

 Domain Keyword:       all-vm
 Mode:                 Incremental Forever - Full
 Target Node Name:     MSF
 Data Mover Node Name: MSF
 Cluster Resource:     No

3. VM Name: HPV2VM3-OLD

 Domain Keyword:       all-vm
 Mode:                 Incremental Forever - Full
 Target Node Name:     MSF
 Data Mover Node Name: MSF
 Cluster Resource:     No

4. VM Name: Local10

 Domain Keyword:       all-vm
 Mode:                 Incremental Forever - Full
 Target Node Name:     MSF
 Data Mover Node Name: MSF
 Cluster Resource:     No

 Disk[1]
 Name: \\lingonberry\c$\Users\michael\Documents\Storage\Local10.vhdx
 Capacity:             127.00 GB
 Size:                 4.00 MB
 Full Backup:          included
 Incremental Backup:   excluded
 Disk Type:            VHDX
 Number of Subdisk:    0

Total number of virtual machines processed: 4
ANS1900I Return code is 0.
ANS1901I Highest return code was 0.
```

Related links for backing up Hyper-V virtual machines

- “`Detail`” on page 45
- “`Domain.vmfull`” on page 45
- “`Mbobjrefreshthresh`” on page 51
- “`Mbpctrefreshthresh`” on page 52
- “`Mode`” on page 50
- “**`Query VM`**” on page 37
- “**`Restore VM`**” on page 40
- “`Vmbackuptype`” on page 58

Expire

The **expire** command deactivates the backup objects that you specify in the file specification or with the `filelist` option. You can specify an individual file to expire, or a file that contains a list of files to expire. If `OBJTYPE=VM`, this command deactivates the current backup for a virtual machine.

When you are working in interactive mode, a prompt notifies you before files are expired.

The **expire** command does not remove workstation files. If you expire a file or directory that still exists on your workstation, the file or directory is backed up again during the next incremental backup, unless you exclude the object from backup processing.

If you expire a directory that contains active files, those files are not displayed in a subsequent query from the GUI. However, these files are displayed on the command line, if you specify the correct query with a wildcard character for the directory.

Note: Because the **expire** command changes the server picture of the client file system without changing the client file system, the **expire** command is not allowed on files that are on a file system that is monitored by the IBM journal service.

Syntax

```
                 ┌─OBJTYPE=FILE── ──filespec─┐
►►──EXPire── ────┴───────────────────────────┼──────────────────────────────►
                                             └─OBJTYPE=VM── ──vmname─┘

►──┬─────────┬─────────────────────────────────────────────────────────────►◄
   └─options─┘
```

Parameters

`OBJTYPE=FILE filespec`
Specifies a path and a file name that you want to expire. You can enter only one file specification on this command. However, you can use wildcards to select a group of files or all the files in a directory. If you specify the `filelist` option, the `filespec` designation is ignored.

`OBJTYPE=VM vmname`
`vmname` specifies the name of a virtual machine. The active backup for the specified virtual machine is expired. The virtual machine name cannot contain wildcard characters.

When `objtype=VM` is specified, the expire command expires only full virtual machine backups (`MODE=FULL` or `MODE=IFFULL`) for the virtual machine that is specified on the `vmname` parameter.

Table 2. Expire command: Related options

Option	**Where to use**
`dateformat` "Dateformat" on page 43	Client options file (dsm.opt) or command line.

Table 2. Expire command: Related options (continued)

Option	Where to use
`filelist` "Filelist" on page 47	Command line only.
`noprompt` "Noprompt" on page 53	Command line only.
`numberformat` "Numberformat" on page 53	Client options file (dsm.opt) or command line.
`pick` "Pick" on page 54	Command line only.
`timeformat` "Timeformat" on page 56	Client user-options file (dsm.opt) or command line.

Examples

Task Deactivate the `letter1.txt` file in the `home` directory.

Command: `dsmc expire c:\home\letter1.txt`

Task Deactivate all files in the `admin\mydir` directory.

Command: `dsmc expire c:\admin\mydir\*`

Task Deactivate all files that are named in the `c:\avi\filelist.txt` file.

Command: `dsmc expire -filelist=c:\avi\filelist.txt`

Task Deactivate the current backup of the virtual machine that is named vm_test.

Command: `dsmc expire –objtype=VM vm_test`

Query VM

Use the **`query vm`** command to determine which Hyper-V virtual machines were backed up.

Syntax

```
►►──Query VM── ──vmname──┬─────────┬──────────────────────────────────►◄
                         └─options─┘
```

Parameters

vmname

Specifies the virtual machine host name that you want to query. The virtual machine name is case-sensitive. If you specify a virtual machine name on the command, the name cannot contain wildcard characters.

If you omit the virtual machine name, the command displays all virtual machine backups on the IBM Spectrum Protect server.

Table 3. Query VM command: Related options for Hyper-V virtual machine queries.

Option	Where to use
`detail` "Detail" on page 45	Command line. Displays the details of each disk (label, name) and its status (protected or excluded), and incremental-forever backup performance statistics.
`inactive` "Inactive" on page 48 Valid for vmbackuptype=hypervfull	Command line.
`pitdate` "Pitdate" on page 55 Valid for vmbackuptype=hypervfull	Command line.
`pittime` "Pittime" on page 55 Valid for vmbackuptype=hypervfull	Command line.
`vmbackuptype=hypervfull` "Vmbackuptype" on page 58	Command line or client options file.

Examples

Task List all virtual machines that have been backed up by IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V on the Hyper-V host.

```
dsmc query vm -vmbackuptype=hypervfull
```

Query VM examples

The following is an example of **`query VM`** command that displays information about Hyper-V virtual machines that have been backed up.

```
dsmc query vm -vmbackuptype=hypervfull -detail

 #      Backup Date       Mgmt Class  Size         Type   A/I Virtual Machine
---  -------------------  ----------  -----------  ------ --- ---------------
  1  04/03/2014 15:07:16  STANDARD      127.00 GB  IFINCR  A  Win8.1
 The size of this incremental backup: 3.06 GB
 The number of incremental backups since last full: 2
 The amount of extra data: 1
 The objects fragmentation: 2
 Backup is represented by: 173 objects
 Application protection type: n/a
 Disk[1]Label:   Hard Disk 1
 Disk[1]Name:    na
 Disk[1]Status:  Protected
  2  04/08/2014 11:21:45  STANDARD        1.15 TB  IFFULL  A  Local4
 The size of this incremental backup: n/a
 The number of incremental backups since last full: 0
 The amount of extra data: 0
 The objects fragmentation: 0
 Backup is represented by: 0 objects
 Application protection type: n/a
 Disk[1]Label:   Hard Disk 1
 Disk[1]Name:    na
 Disk[1]Status:  Protected
-----------------------------------------------------------------------------
 All averages are calculated only for incremental forever backups displayed above.
 The average size of incremental backup: 3.06 GB
 The average number of incremental backups since last full: 1
 The average overhead of extra data: 0
 The average objects fragmentation: 1
 The average number of objects per backup: 86
ANS1900I Return code is 0.
ANS1901I Highest return code was 0.
```

The next example shows output from a **`query VM`** that includes the **`-detail`** option. This command includes a virtual machine name so the output is only displayed for the specified virtual machine. The detailed output includes the type of backup that was performed, the size of the virtual machine, information about its disks, and statistics.

```
dsmc query vm HPV2VM1 -detail

Periodic Full - Full

Query Virtual Machine for Full VM backup

 #      Backup Date       Mgmt Class  Size         Type   A/I Virtual Machine
---  -------------------  ----------  -----------  ------ --- ---------------
  1  03/14/2014 09:58:44  STANDARD       60.00 GB  IFINCR  A  HPV2VM1
        The size of this incremental backup: 8832 KB
        The number of incremental backups since last full: 4
        The amount of extra data: 0
        The objects fragmentation: 3
        Backup is represented by: 174 objects
        Application protection type: n/a
        Disk[1]Label:   Hard Disk 1
        Disk[1]Name:    na
        Disk[1]Status:  Protected
-----------------------------------------------------------------------------
        All averages are calculated only for incremental forever backups displayed above.
        The average size of incremental backup: 8832 KB
        The average number of incremental backups since last full: 4
        The average overhead of extra data: 0
        The average objects fragmentation: 3
        The average number of objects per backup: 174
```

The following example shows the syntax to use to list all Hyper-V virtual machines that have been backed up by this node:

```
dsmc query vm -vmbackuptype=hypervfull
```

Restore VM

The **restore vm** command can be used to restore a Microsoft Hyper-V virtual machine that was previously backed up by IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

If the virtual machine that you are restoring exists on the Hyper-V host server, it is shut down and deleted before it is restored from the image stored on the IBM Spectrum Protect server. The Restore VM operation then creates the virtual machine such that its content and configuration is identical to what it was when the backup occurred. Even though the client shuts down the virtual machine before deleting it, manually shutting down the virtual machine before running **Restore VM** is a good practice to bring any in-progress application activities to an orderly stop.

Syntax

```
►►──REStore VM── ──sourcevmspec──────────────────────────────────────────►

►──┬──────────────────────────────────────────────────┬──┬─────────────┬──────────►◄
   └─-vmname=──new_vm_name── ──-targetpath=──path─┘  └──options─┘
```

Parameters

Any parameter that contains spaces must be enclosed in quotation (" ") marks.

sourcevmspec
Specifies the name of the virtual machine that was backed up. The virtual machine name is case-sensitive.

-vmname=*new_vm_name*
Optional. Specifies a new name for the virtual machine. If this parameter is not specified, the virtual machine is restored and it has the same name it had when it was backed up. If you do specify a new name for a virtual machine, a target path is required.

-targetpath=*path*
Use this parameter to restore the virtual machine to an alterative location on the file system. This parameter is required when you specify the **vmname** parameter.

Table 4. Restore VM command: Related options when restoring Hyper-V virtual machines

Option	Where to use
`inactive`	Command line
`pick`	Command line
`pitdate`	Command line
`pittime`	Command line
`vmbackuptype`	Command line or client options file. To restore a Hyper-V virtual machine, this option must be set to **HYPERVFULL**.

Examples

Task Restore the most recent backup version of a virtual machine named myVM.

```
dsmc restore vm myvm
```

Chapter 5. Options reference

The following sections contain detailed information about each of the client options that are used for IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V operations.

Information for each option includes the following information:
- a description
- a syntax diagram
- detailed descriptions of the parameters
- examples of using the option in the client options file (if applicable)
- examples of using the option on the command line (if applicable)

Options with a command-line example of **Does not apply** cannot be used with command line or scheduled commands.

Dateformat

The `dateformat` option specifies the format you want to use to display or enter dates.

Use this option if you want to change the default date format for the language of the message repository you are using.

By default, the backup-archive and administrative clients obtain format information from the locale definition in effect at the time you start the client. Consult the documentation on your local system for details about setting up your locale definition.

You can use the `dateformat` option with the **`expire`** command.

When you include the `dateformat` option with a command, it must precede the `fromdate` and `pitdate` options.

Options File

Place this option in the client options file (dsm.opt). You can set this option on the **Regional Settings** tab, **Date Format** drop-down list of the Preferences editor.

Syntax

```
►►──DATEformat── ──format_number──────────────────────────────────────►◄
```

Parameters

`format_number`
Displays the date using one of the following formats. Select the number that corresponds to the date format you want to use:

1 MM/DD/YYYY

This is the default for the following available translations:

© Copyright IBM Corp. 2011, 2016

- US English
- Chinese (Traditional)
- Korean

2 DD-MM-YYYY

This is the default for the following available translations:
- Brazilian Portuguese
- Italian

3 YYYY-MM-DD

This is the default for the following available translations:
- Japanese
- Chinese (Simplified)
- Polish

4 DD.MM.YYYY

This is the default for the following available translations:
- German
- French
- Spanish
- Czech
- Russian

5 YYYY.MM.DD

This is the default for the following available translations:
- Hungarian

6 YYYY/MM/DD

7 DD/MM/YYYY

Examples

Options file:

```
dateformat 3
```

Command line:

```
-date=3
```

This option is valid on the initial command line and in interactive mode. If you use this option in interactive mode, it affects only the command with which it is specified. When that command completes, the value reverts to the value at the beginning of the interactive session. This is the value from the dsm.opt file unless overridden by the initial command line or by an option forced by the server.

Additional considerations for specifying time and date formats

The date or time format you specify with this option must be used when using options that take date and time as input. Examples are: `totime`, `fromtime`, `todate`, `fromdate`, and `pittime`.

For example, if you specify the `timeformat` option as `TIMEFORMAT 4`, the value that you provide on the `fromtime` or `totime` option must be specified as a time such as `12:24:00pm`. Specifying `13:24:00` would not be valid because `TIMEFORMAT 4` requires an hour integer that is 12 or less. If you want to specify up to 24 hour values on an option, and if you want to use commas as separators, you must specify `TIMEFORMAT 2`.

Detail

Use the `detail` option to display management class, file space, and backup information.

Use the `detail` with the **`query vm`** command to display the following statistics:
- The average number of IBM objects that are needed to describe a single megablock, across all megablocks in a backup.
- The average number of IBM objects that are needed to describe a single megablock, for all megablocks in a filespace.
- The number of backups that were created since the last full backup was created from the production disks.

The values returned on **`query vm`** can help you fine tune the heuristics (see the `Mbobjrefreshthresh` and `Mbpctrefreshthresh` options) to fine tune the values trigger for megablock refreshes.

Syntax

```
►►──DETail──────────────────────────────────────────────────────────►◄
```

Parameters

There are no parameters for this option.

Examples

Command line:

```
dsmc query vm -detail
```

Domain.vmfull

The `domain.vmfull` option specifies the virtual machines to include in your backup operations.

Use this option to specify which Hyper-V virtual machines are processed when you run a **`backup vm -vmbackuptype=hypervfull`** command, without specifying any Hyper-V virtual machine names.

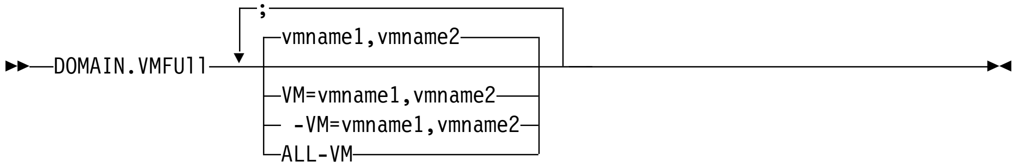
You can specify which virtual machines are to be processed by using any of the following techniques:
- Use the `VM=` option and specify the name of a virtual machine.
- Provide a comma-separated list of virtual machine names.
- Use wildcard syntax to process virtual machines that match the name pattern.
- Use the `all-vm` domain-level parameter. You can also include one or more virtual machines by using the `VM=` keyword, or exclude virtual machines by using the `-VM=` syntax.

The virtual machines that are specified on the `domain.vmfull` option are processed only when the **`backup vm`** command is entered without specifying a virtual machine or a list of virtual machines on the command line.

Options file

Set this option in the client options, by using the command line, or by using the **VM Backup** tab of the Preferences editor.

Syntax



Syntax rules: Multiple keywords must be separated by a semicolon. There cannot be any spaces after the semicolons. Multiple machine or domain names must be separated by commas, with no space characters. For examples, see `vm=`*`vmname`*.

Parameters

vmname

Defines the virtual machine name that you want to process. You can supply a list of virtual machine host names, by separating the names with commas (`vm1,VM2,Vm5`). The names are case-sensitive and must match the capitalization that is shown on the Hyper-V host in the **Hyper-V Manager** > **Virtual Machines** view.

vm=*vmname*

The `vm=` keyword specifies that the next set of values is a list of virtual machine names. The `vm=` keyword is the default and is not required.

In this example, `vm=` is not specified and commas are used to separate the machine names.

```
domain.vmfull my_vm1,my_vm2
```

If you specify multiple keywords, such as `vm=` and `-vm=`, the values that the keywords refer to must be separated by semicolons, with no intervening space characters:

```
domain.vmfull vm=my_vm1;vm=my_vm2
domain.vmfull -vm=my_vm3;-vm=my_vm4
```

Wildcard characters can be used to select virtual machine names that match a pattern. An asterisk (*) matches any sequence of characters. A question mark (?) matches any single character, for example:

- Exclude all files that have “test” in the host name: `-vm=*test*`
- Include all virtual machines with names such as: “test20”, “test25”, “test29”, “test2A”: `vm=test2?`

You can exclude a virtual machine from a backup operation by specifying the exclude operator (-) before the `vm=` keyword. For example, `-vm` is used to exclude a particular machine, or machines, from a domain level backup, such as, `ALL-VM`. You cannot use the exclude operator (-) to exclude a domain, such as `ALL-VM`. The exclude operator works only at the virtual machine name level.

all-vm

This option specifies that a **`backup vm`** operation processes all Hyper-V virtual machines that are known to the Hyper-V host.

Examples

Options file:

Include all virtual machines in full VM backup operations.

```
domain.vmfull all-vm
```

Include all virtual machines in full VM backup operations, except for the ones that have a name suffix of _test.

```
domain.vmfull all-vm;-vm=*_test
```

Include all virtual machines in full VM backup operations, but exclude virtual machines testvm1 and testmvm2.

```
domain.vmfull all-vm;-VM=testvm1,testvm2
```

Filelist

Use the `filelist` option to process a list of files.

You can use the `filelist` option with the **`expire`** command.

The IBM client opens the file you specify with this option and processes the list of files within according to the specific command. When you use the `filelist` option, IBM Spectrum Protect ignores all other file specifications on the command line.

The files (entries) listed in the filelist must adhere to the following rules:

- Each entry must be a fully-qualified or a relative path to a file or directory. Note that if you include a directory in a filelist entry, the directory is backed up, but the contents of the directory are not.
- Each path must be specified on a single line. A line can contain only one path.
- Paths must not contain control characters, such as 0x18 (CTRL-X), 0x19 (CTRL-Y) and 0x0A (newline).
- The filelist can be an MBCS file or a Unicode file with all Unicode entries.
- Any IBM Spectrum Protect filelist entry that does not comply with these rules is ignored.

The following are examples of valid paths in a filelist:

```
c:\myfiles\directory\file1
c:\tivoli\mydir\yourfile.doc
..\notes\avi\dir1
..\fs1\dir2\file3
"d:\fs2\Ha Ha Ha\file.txt"
"d:\fs3\file.txt"
```

You can use the `filelist` option during an open file support operation. In this case, IBM Spectrum Protect processes the entries in the filelist from the virtual volume instead of the real volume.

If an entry in the filelist indicates a directory, only that directory is processed and not the files within the directory.

If the file name (the `filelistspec`) you specify with the `filelist` option does not exist, the command fails. IBM Spectrum Protect skips any entries in the filelist that are not valid files or directories. IBM Spectrum Protect logs errors and processing continues to the next entry.

The entries in the list are processed in the order they appear in the filelist. For optimal processing performance, pre-sort the filelist by file space name and path.

Tip: IBM Spectrum Protect might back up a directory twice if the following conditions exist:
- The filelist contains an entry for the directory
- The filelist contains one or more entries for files within that directory
- No backup of the directory exists

For example, your filelist includes the entries `c:\dir0\myfile` and `c:\dir0`. If the `\dir0` directory does not exist on the server, the `c:\dir0` directory is sent to the server a second time.

Syntax

```
►►──FILEList =── ──filelistspec──────────────────────────────────────────►◄
```

Parameters

filelistspec
Specifies the location and name of the file that contains the list of files to process with the command.

Note: When you specify the `filelist` option on the command line, the `subdir` option is ignored.

Examples

Command line:
```
sel -filelist=c:\avi\filelist.txt
```

Inactive

Use the `inactive` option to display both active and inactive objects.

You can use the `inactive` option with the **`query vm`** and **`restore vm`** commands.

Important: When using the `inactive` option during a restore operation, also use the `pick` option because all versions are restored in an indeterminate order. This option is implicit when `pitdate` is used.

Syntax

```
►►──INActive─────────────────────────────────────────────────────────────►◄
```

Parameters

There are no parameters for this option.

Examples

Command line:
```
dsmc restore vm VM1 -inactive
```

`Include.vm`

This option overrides the management class that is specified on the `vmmc` option.

The management class specified on the `vmmc` option applies to all backups. You can use the `include.vm` option to override that management class, for one or more virtual machines. The `include.vm` option does not override or affect the management class that is specified by the `vmctlmc` option. The `vmctlmc` option binds backed-up virtual machine control files to a specific management class.

Options File

Set this option in the client options file.

Syntax

```
►►──INCLUDE.VM── ──vmname── ─┬──────────────┬──────────────────────►◄
                             └─mgmtclassname─┘
```

Parameters

vmname
: Required parameter. Specifies the name of a virtual machine that you want to bind to the specified management class. Only one virtual machine can be specified on each `include.vm` statement. However, you can specify as many `include.vm` statements as needed to bind each virtual machine to a specific management class.

You can include wildcards in the virtual machine name. An asterisk (*) matches any character string. A question mark (?) matches a single character. If the virtual machine name contains a space character, enclose the name in double quotation marks (").

Tip: If the virtual machine name contains special characters, type the question mark wildcard in place of the special characters when you specify the virtual machine name.

mgmtclassname
: Optional parameter. Specifies the management class to use when the specified virtual machine is backed up. If this parameter is not specified, the management class defaults to the global virtual machine management class that is specified by the `vmmc` option.

Examples

Assume that the following management classes exist and are active on the IBM Spectrum Protect server:

- MCFORTESTVMS
- MCFORPRODVMS
- MCUNIQUEVM

Example 1

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

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

Example 2

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

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

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

Example 3

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

```
include.vm VM1 MCUNIQUEVM
```

Related information

“`Vmmc`” on page 61

Mode

Use the mode option to specify the backup mode to use when performing specific backup operations.

You can use the `mode` option with the **`backup vm`** command. this parameter specifies whether to perform a full image backup, an incremental-forever full backup, or an incremental-forever-incremental backup of Hyper-V virtual machines.

The `mode` option has no effect on a when backing up a raw logical device.

Syntax

```
                .-IFIncremental-.
>>--MODE =------+---------------+-------------------------------------------><
                '-IFFull--------'
```

Parameters

`IFIncremental`

Specifies that you want to perform an incremental-forever-incremental backup of a Hyper-V virtual machine. An incremental-forever-incremental backup backs up only the disk blocks that have changed since the last backup. This is the default backup mode.

You cannot use this backup mode to back up a virtual machine if the client is configured to encrypt the backup data.

`IFFull`

Specifies that you want to perform an incremental-forever-full backup of a Hyper-V virtual machine. An incremental-forever-full backup backs up all used blocks on a virtual machine's disks. By default, the first backup of a Hyper-V virtual machine is an incremental-forever-full (`mode=iffull`) backup, even if you specify `mode=ifincremental` (or let the `mode` option default). Subsequent backups default to `mode=ifincremental`.

You cannot use this backup mode to back up a virtual machine if the client is configured to encrypt the backup data.

Examples

Task Perform an incremental-forever-full VM backup of a Windows Hyper-V VM named `msvm1`

```
dsmc backup vm msvm1 -mode=iffull
 -vmbackuptype=hypervfull
```

Task Perform an incremental-forever-incremental backup of a Windows Hyper-V VM named `msvm1`

```
dsmc backup vm msvm1 -mode=ifincremental
 -vmbackuptype=hypervfull
```

Related reference:

"**Backup VM**" on page 31

Mbobjrefreshthresh

The `mbobjrefreshthresh` (megablock object refresh threshold) option is a number defining a threshold. When the number of IBM Spectrum Protect objects that are needed to describe any 128 MB megablock exceeds this value, the entire megablock is refreshed and the objects that were used to represent this area, in previous backups, are expired.

When you backup a virtual machine, the data is stored on the IBM Spectrum Protect server in 128 MB units, called *megablocks*. If an area on the production disk changes and a new incremental backup is performed, a new megablock is created to represent the changes that were made to the previously backed up data. Because a new megablock can be created with each incremental backup, eventually the megablocks can adversely affect the performance of the IBM Spectrum Protect database, and therefore, adversely affect the performance of most IBM Spectrum Protect operations.

Use this option when estimating IBM Spectrum Protect objects that represent production data for each virtual machine backup. For example, when the number of IBM Spectrum Protect objects exceed this value, the megablock is refreshed. This action means that the entire 128-MB block is copied to the IBM Spectrum Protect server and is represented as a single IBM Spectrum Protect object. The minimum value is 2 and the maximum value is 8192. The default value is 50.

Options file

Specify this option in the client options file.

Syntax

```
                         ┌─50──────┐
►►──MBOBJREFRESHTHRESH──┼─────────┼──────────────────────────────────►◄
                         └─integer─┘
```

Parameters

The minimum value you can specify is 2 megablocks, the largest value is 8192 megablocks; the default is 50 megablocks.

Examples

Set this option to trigger a megablock refresh when the number of objects needed to represent an updated megablock exceeds 20 objects:

```
MBOBJREFRESHTHRESH 20
```

Mbpctrefreshthresh

The `mbpctrefreshthresh` (megablock percentage refresh threshold) option is a number defining a threshold. When the number of IBM Spectrum Protect percentage of objects that are needed to describe any 128 MB megablock exceeds this value, the entire megablock is refreshed and the objects that were used to represent this area, in previous backups, are expired.

When you backup a virtual machine, data is stored on the IBM Spectrum Protect server in 128 MB units, called *megablocks*. If an area on the production disk changes and a new incremental backup is performed, a new megablock is created to represent the changes that were made to the previously backed up data. Because a new megablock can be created with each incremental backup, eventually the megablocks can adversely affect the performance of the IBM Spectrum Protect database, and therefore, adversely affect the performance of most IBM Spectrum Protect operations.

Use this option when estimating the amount of additional data that is backed up for each virtual machine. For example, when a 128-MB block of a production disk changes more than the percentage specified, the entire 128-MB block is copied to the IBM Spectrum Protect server. The block is represented as a single IBM Spectrum Protect object.

Options file

Specify this option in the client options file.

Syntax

```
                       ┌─50──────┐
►►──MBPCTREFRESHTHRESH─┴─integer─┴──────────────────────────────────────►◄
```

Parameters

The minimum value you can specify is 1 percent, the largest value is 99 percent; the default is 50 percent.

Examples

Set this option to trigger a megablock refresh when 50 percent (or more) of the objects in a megablock on a production disk have changed:

```
MBPCTREFRESHTHRESHOLD 50
```

Noprompt

The `noprompt` option suppresses the confirmation prompt that is presented by the **`expire`** command.

Use the `noprompt` option with the **`expire`** command.

Syntax

```
►►──NOPrompt──────────────────────────────────────────────────────────►◄
```

Parameters

There are no parameters for this option.

Examples

Command line:

```
dsmc expire -noprompt c:\home\project\*
```

Numberformat

The `numberformat` option specifies the format you want to use to display numbers.

Use this option if you want to change the default number format for the language of the message repository you are using.

By default, format information is obtained from the locale definition in effect at the time the client is called. Consult the documentation on your local system for details about setting up your locale definition.

You can only use the `numberformat` option with the **`expire`** command.

Options File

Place this option in the client user-options file (dsm.opt). You can set this option on the **Regional Settings** tab, **Number Format** field of the Preferences editor.

Syntax

```
►►──NUMberformat── ──number───────────────────────────────────────────►◄
```

Parameters

`number`

Displays numbers using any one of the following formats. Specify the number (0–6) that corresponds to the number format you want to use.

0 Use the locale-specified date format. This is the default (does not apply to Mac OS X).

1 1,000.00

This is the default for the following available translations:

- US English
- Japanese

- Chinese (Traditional)
- Chinese (Simplified)
- Korean

2 1,000,00

3 1 000,00

This is the default for the following available translations:

- French
- Czech
- Hungarian
- Polish
- Russian

4 1 000.00

5 1.000,00

This is the default for the following available translations:

- Brazilian Portuguese
- German
- Italian
- Spanish

6 1'000,00

Examples

Options file:

```
num 4
```

Command line:

```
-numberformat=4
```

This option is valid on the initial command line and in interactive mode. If you use this option in interactive mode, it affects only the command with which it is specified. When that command completes, the value reverts to the value at the beginning of the interactive session. This is the value from the dsm.opt file unless overridden by the initial command line or by an option forced by the server.

Pick

The `pick` option creates a list of backup versions or archive copies that match the file specification you enter.

From the list, you can select the versions to process. Include the `inactive` option to view both active and inactive objects.

Use the `pick` option with the **`restore vm`** command.

Syntax

```
►►──PIck──────────────────────────────────────────────────────────►◄
```

Parameters

There are no parameters for this option.

Examples

Command line:

```
dsmc restore vm vmfin* -pick -inactive
```

Pitdate

Use the `pitdate` option with the `pittime` option to establish a point in time to display or restore the latest version of your backups.

Files that were backed up *on or before* the date and time you specify, and which were not deleted *before* the date and time you specify, are processed. Backup versions that you create after this date and time are ignored.

Use the `pitdate` option with the **`query vm`** and **`restore vm`** commands.

When `pitdate` is used, the `inactive` and `latest` options are implicit.

Syntax

```
►►──PITDate =── ──date──────────────────────────────────────────────►◄
```

Parameters

`date`
Specifies the appropriate date.

Examples

Command line:

```
dsmc restore vm vmfin3 -pitdate=02/21/2014
```

Pittime

Use the `pittime` option with the `pitdate` option to establish a point in time to display or restore the latest version of your backups.

Files that were backed up *on or before* the date and time you specify, and which were not deleted *before* the date and time you specify, are processed. Backup versions that you create after this date and time are ignored. This option is ignored if you do not specify `pitdate` option.

Use the `pittime` option with the **`query vm`** and **`restore vm`** commands.

Syntax

```
►►──PITTime =── ──time──────────────────────────────────────────────►◄
```

Parameters

time
Specifies a time on a specified date. If you do not specify a time, the time defaults to 23:59:59.

Examples

Command line:

```
dsmc query vm vmfin1 -pitt=06:00:00 -pitd=02/03/2014
```

Timeformat

The `timeformat` option specifies the format in which you want to display and enter system time.

Use this option if you want to change the default time format for the language of the message repository you are using.

By default, format information is obtained from the locale definition in effect at the time the client is called. Consult the documentation on your local system for details about setting up your locale definition.

You can only use the `timeformat` option with the **`expire`** command.

When you include the `timeformat` option with a command, it must precede the `fromtime`, `pittime`, and `totime` options.

Options File

Place this option in the client options file (dsm.opt). You can set this option on the **Regional Settings** tab, **Time Format** field of the Preferences editor.

Syntax

```
►►──TIMEformat── ──format_number──────────────────────────────────────────►◄
```

Parameters

format_number
Displays time in one of the formats listed here. Select the format number that corresponds to the format you want to use. When you include the `timeformat` option in a command, it must precede the `pittime` option.

1 23:00:00
2 23,00,00
3 23.00.00
4 12:00:00 A/P
5 A/P 12:00:00

Examples

Options file:

```
timeformat 4
```

Command line:

```
-time=3
```

This option is valid on the initial command line and in interactive mode. If you use this option in interactive mode, it affects only the command with which it is specified. When that command completes, the value reverts to the value at the beginning of the interactive session. This is the value from the dsm.opt file unless overridden by the initial command line or by an option forced by the server.

Additional considerations for specifying time and date formats

The date or time format you specify with this option must be used when using options that take date and time as input. Examples are: `totime`, `fromtime`, `todate`, `fromdate`, and `pittime`.

For example, if you specify the `timeformat` option as `TIMEFORMAT 4`, the value that you provide on the `fromtime` or `totime` option must be specified as a time such as `12:24:00pm`. Specifying `13:24:00` would not be valid because `TIMEFORMAT 4` requires an hour integer that is 12 or less. If you want to specify up to 24 hour values on an option, and if you want to use commas as separators, you must specify `TIMEFORMAT 2`.

Vmbackdir

The `vmbackdir` option specifies the temporary disk location where the client saves control files that are created during full VM backup and restore operations of Microsoft Hyper-V virtual machines.

When a client on a data mover node starts a full VM backup of a virtual machine, the client creates metadata in files that are associated with the backed up virtual machine and its data. The files that contain the metadata are referred to as *control files*.

During full VM backup operations, the metadata is saved on a disk in the data mover node until the backup completes and both the virtual machine data and the control files are saved to server storage. During a full VM restore operation, the control files are copied from the server and are temporarily stored on the data mover disk, where they are used to restore the virtual machine and its data. After a backup or a restore operation completes, the control files are no longer needed and the client deletes them from their temporary disk location.

The directory that is specified by this option must be on a drive that contains sufficient free space to contain the control information from a full VM backup.

Options File

Set this option in the client options file, or specify it on the command line as an option for the **backup vm** or **restore vm** commands.

Syntax

```
►►──VMBACKDir──directory──────────────────────────────────────────►◄
```

Parameters

directory

Specifies the path where the control files are stored on the backup server.

The default is `c:\mnt\tsmvmbackup\fullvm\`

Examples

Options file:

```
VMBACKD c:\mnt\tsmvmbackup\
```

Command line:

```
dsmc backup vm -VMBACKUPT=fullvm -VMBACKD=G:\virtual_machine\
control_files\
```

```
dsmc restore vm -VMBACKUPT=fullvm -VMBACKD=G:\san_temp\
```

Vmbackuptype

Use the `vmbackuptype` option with the **`backup VM`** or **`restore VM`** command to specify a Hyper-V full VM backup.

Options File

Place this option in the client options file (`dsm.opt`), or on the command line.

Syntax

```
►►──VMBACKUPType────HYPERVFULL───────────────────────────────────────────►◄
```

Parameters

HYPERVFULL
Specify this value when you perform a full VM backup of one or more Hyper-V virtual machines.

Examples

Options file:

```
VMBACKUPT hypervfull
```

Command line:

```
dsmc backup vm VM2 -VMBACKUPT=hypervfull -MODE=IFFULL
```

Performs a full virtual-machine backup of Hyper-V virtual machine named "VM2", to the IBM Spectrum Protect server.

Vmctlmc

This option specifies the management class to use when backing up virtual machine control files.

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

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

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

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

Options File

Place this option in the client options file `dsm.opt`.

Syntax

```
►►──VMCTLmc──class_name──────────────────────────────────────────────►◄
```

Parameters

`class_name`
Specifies a management class that applies to backing up virtual machine control files. If you do not set this option, the management class that is specified on the `vmmc` option is used. If you do not set this option and the `vmmc` option is not set, the default management class of the node is used.

Examples

Options file:
`vmctlmc diskonlymc`

Command line:
Does not apply.

Vmmaxparallel

This option is used to configure parallel backups of several virtual machines, using a single instance of the backup-archive client. The `vmmaxparallel` option specifies the maximum number of virtual machines that can be backed up to the server, at any one time.

Options file

This option is valid in the client options file (`dsm.opt`) or on the command line for **`Backup VM`**. It can also be included on the server in a client options set. It cannot be set in the Preferences Editor.

Syntax

```
                  ┌─1───────┐
►►──VMMAXParallel─┴─integer─┴────────────────────────────────────────►◄
```

Parameters

integer

Specifies the maximum number of virtual machines that can be backed up, at any one time, during a parallel backup operation. The default is 1. The maximum is 50.

Tip: When using client-side data deduplication, a deduplication session is started for each VM. This deduplication session is not counted as one of the `vmmaxparallel` sessions.

The `MAXNUMMP` server parameter specifies the maximum number of mount points a node is allowed to use on the server when the copy destination of the storage pool is FILE or TAPE. `MAXNUMMP` must be equal to or greater than the `VMMAXPARALLEL`setting. When multiple instances of the client are backing up files, or when a single client performs parallel backups, additional mount points might be needed. If the number of mount points requested exceeds the `MAXNUMMP` value, the server issues an error (ANS0266I). In response to the error, the client reduces `VMMAXPARALLEL` to match the number specified by `MAXNUMMP` and continues the backup with the reduced number of sessions. If additional ANS0266I errors are detected, the client reduces `VMMAXPARALLEL` by 1 and attempts to continue the backup. If `VMMAXPARALLEL` is decremented to 1 and the client receives more ANS0266I errors, the client ends the backup and issues the following error:

ANS5228E `A backup VM operation failed because VMMAXPARALLEL was reduced to 1 and the client still cannot obtain a server mount point.`

Contact your server administrator if you need the value that is currently set for `MAXNUMMP` increased, so your node can support additional parallel backup sessions.

During Hyper-V virtual machine backups, IBM creates VSS snapshots of all volumes that contain virtual machine data. Backup data is read from the VSS snapshots, and not from data that is on the live file system. In many cases, when IBM Spectrum Protect attempts to create several snapshots concurrently, the VSS software provider might fail to satisfy a snapshot request for several virtual machines. The failures occur because the VSS software snapshot provider can not handle the load that is created by several backups that are attempted in parallel. To avoid this issue, use a VSS hardware snapshot provider instead of a VSS software provider.

Examples

Options file

VMMAXP 10

Related reference:

"**`Backup VM`**" on page 31

"`Domain.vmfull`" on page 45

Vmmc

Use the `vmmc` option to store virtual machine backups by using a management class other than the default management class. The `vmmc` option is only valid when `vmbackuptype=hypervfull` option is set.

Options File

Place this option in the client options file (`dsm.opt`), or on the command line.

Syntax

```
►►──VMMC──management_class_name─────────────────────────────────────►◄
```

Parameters

management_class_name
Specifies a management class that applies to the backed up virtual machine data. If you do not set this option, the default management class of the node is used.

Examples

Task: Run a backup of the virtual machine that is named `myVirtualMachine` and save the backup according to the management class that is named `myManagmentClass`.

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

Chapter 6. Mount and file restore

IBM Spectrum Protect recovery agent configurations

The IBM Spectrum Protect recovery agent provides a variety of configurations for performing file restore and disk / block device exposure.

Off-host file restore

These configurations do not require the IBM Spectrum Protect recovery agent to be installed in each virtual machine guest. Instead, an off-host instance is responsible for file restore of multiple virtual machines. With this configuration, the mount process exposes a virtual volume from a selected disk partition. For GPT disks, the whole disk must be exposed to make the partitions available, and the disk must be iSCSI connected. Use the recovery agent GUI to accomplish this task.

You must register a node that is associated with the recovery agent. The recovery agent node must be granted proxy authority to access the data node (or nodes) where the snapshots are stored. When a snapshot is mounted to the off-host server, the virtual volume can be network-shared to make it accessible to the virtual machine guest. Or, you can copy the files from the mounted volume to the virtual machine guest by any file-sharing method.

- For step by step restore instructions, see "Restoring one or more files" on page 67

In-guest file restore

These configurations require IBM Spectrum Protect recovery agent to be installed in each virtual machine guest. The mount and restore process is performed for a single partition from the backed up disk.

The IBM Spectrum Protect recovery agent node name is typically granted access only to the virtual machine where it is running with the IBM Spectrum Protect backup-archive client **`dsmc set access`** command. The restore process is typically begun by a user who logs in to the guest machine of the virtual machine.

For these configurations, be sure to compare the specific virtual machine guest operating system requirements with the supported levels of IBM Spectrum Protect recovery agent. If a specific operating system is not supported, determine if the off-host disk / block device exposure configuration can also be used for file restore. Use the IBM Spectrum Protect recovery agent GUI to accomplish this task.

- For planning information and operating system-based guidelines, see Chapter 6, "Mount and file restore."
- For step-by-step restore instructions, see "Restoring one or more files" on page 67.

Off-host iSCSI target

This configuration exposes an iSCSI target from the instance of the off-host IBM Spectrum Protect recovery agent and manually uses an in-guest iSCSI initiator to access the disk snapshot. This configuration requires an iSCSI initiator to be installed within the virtual machine guest. This approach exposes an iSCSI LUN,

© Copyright IBM Corp. 2011, 2016

rather than the off-host file restore, which exposes an individual disk partition. Use the IBM Spectrum Protect recovery agent GUI to accomplish this task.

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

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

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

- For planning information and operating system-based guidelines, see Chapter 6, "Mount and file restore," on page 63.
- For step by step restore instructions, see "Restoring one or more files" on page 67.

Snapshot mount overview

You can use the IBM Spectrum Protect recovery agent to mount a snapshot and use the snapshot to complete data recovery.

Mount snapshots with the IBM Spectrum Protect recovery agent GUI. Install and run the recovery agent on a system that is connected to the IBM Spectrum Protect server through a LAN. You cannot use the recovery agent component operations in a LAN-free path.

Be aware of these situations when running mount operations:

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

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

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

As a result, avoid concurrent recovery agent sessions on the same tape volume.

Mount guidelines

Snapshots can be mounted in either read-only or read/write mode. In read/write mode, recovery agent saves changes to data in memory. If the service is restarted, the changes are lost.

The recovery agent operates in either of the following two modes:

No user is logged in
The recovery agent runs as a service.

User is logged in
The recovery agent continues to run as a service until you start the recovery agent and use the GUI. When you close the recovery agent and GUI, the service restarts. You can use only the recovery agent application and GUI when running with administrator login credentials. Only one copy of the recovery agent application can be active at any time.

When mounted volumes exist and you start Mount from the Start menu, this message is displayed:

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

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

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

File restore overview

Use the IBM Spectrum Protect recovery agent for efficient file restore operations and to minimize downtime by mounting snapshots to virtual volumes.

The IBM Spectrum Protect recovery agent can be used for the following tasks:

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

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

You can copy the changed files to another volume before you unmount the volume.

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

The IBM Spectrum Protect recovery agent mounts snapshots from the IBM Spectrum Protect server. In the IBM Spectrum Protect recovery agent GUI, click **Remove** to close an existing connection to the IBM Spectrum Protect server. You must remove any existing connection before you can establish a new connection to a different server or different node. Dismount all volumes before you click **Remove**. The remove operation fails if there are active mount and restore sessions in the mount machines. You cannot remove the connection to a server when you are running a file restore from that server. You must first dismount all virtual devices and stop all restore sessions before you disconnect from a server. If you do not do so, the connection is not removed.

You must unmount all virtual volumes before you uninstall the IBM Spectrum Protect recovery agent. Otherwise, these mounted virtual volumes cannot be unmounted after the IBM Spectrum Protect recovery agent is reinstalled.

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

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

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

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

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

Both volumes are now available.

Restriction: Do not change the IBM Spectrum Protect node password while running a file restore from snapshots stored in that node.

File restore guidelines

You can use the IBM Spectrum Protect recovery agent for efficient file restore and to minimize downtime by mounting snapshots to virtual volumes. File restore is supported from snapshots of NTFS, FAT, or FAT32 volumes.

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

If you are running a file restore of data on dynamic disks, the snapshot must be mounted to a server that has the same version of Windows, or a newer version of Windows, as the node that created the snapshot. Files on the dynamic disk can be accessed indirectly by nodes that have older versions of Windows, by mapping a drive on the older nodes to a CIFS share where the snapshot is mounted.

Important: The ACL values associated with the folders and files that are restored in a file restore operation are not transferred to the restored files. To maintain ACL values, use the **`XCOPY`** command when copying files from the target.

Restoring one or more files

You can restore one (or more) files from a virtual machine that was backed up to IBM server storage.

Before you begin

If your restore operation accesses the virtual machine disk snapshot with an in-guest iSCSI initiator, make sure the following conditions exist before proceeding:

- The iSCSI device is configured and the iSCSI Initiator program is running.
- Port `3260` is open in the LAN firewall between the system where the IBM Spectrum Protect recovery agent GUI is installed and the initiator system.

About this task

To mount a backed up virtual machine disk and export the mounted volume for a file restore operation, complete the following steps:

Procedure

1. Start the IBM Spectrum Protect recovery agent GUI.
   On the Windows system, go to **Start** > **Apps by name** > **IBM** > **IBM Spectrum Protect Recovery Agent**.
   The IBM Spectrum Protect recovery agent GUI can either be installed on the virtual machine guest or installed on a separate host.
2. Connect to the IBM Spectrum Protect server by clicking **Select IBM Spectrum Protect server**. The target node is where the backups are located. You can manage the level of access to the target node data by specifying a different node name in the `Node access method` section.
3. Select a virtual machine from the list.

Tip: You can find your virtual machine quickly by typing the first few letters of the machine name in the edit portion of the list box. The list shows only those machines that match the letters you entered. Machine names are case-sensitive.

A virtual machine might display in the list, but if you select it, the snapshots list might be empty. This situation occurs because of one of the following reasons:

- No snapshots completed successfully for that virtual machine.
- The **Fromnode** option was used and the specified node is not authorized to restore the selected virtual machine.

4. Mount the snapshot through an iSCSI connection:
   a. Click **Mount** in the IBM Spectrum Protect recovery agent GUI.
   b. In the Select mount destination dialog, click **Mount as an iSCSI target**.
   c. Enter the name of the target. This name must be unique for each mount.
   d. Enter the iSCSI initiator name.
      The iSCSI initiator name is shown in the Configuration tab in the iSCSI Initiator Properties dialog. For example:

      ```
      iqn.1991-05.com.microsoft:hostname
      ```
5. Complete these steps on the target system where the iSCSI initiator is installed:
   a. Click the Targets tab.
   b. In the Quick Connect section, enter the IP address or host name of the system where the IBM Spectrum Protect recovery agent GUI is installed.
   c. Click **Quick Connect**.
   d. In the Quick Connect dialog, select the IP address or host name in the Discovered targets field and click **Connect**.
   e. After Status - Connected is shown, click **Done**.
   f. Go to **Control Panel** > **Administrative Tools** > **Computer Management** > **Storage** > **Disk Management**.
      1) If the mounted iSCSI target is listed as Type=Foreign, right-click **Foreign Disk** and select **Import Foreign Disks**. The Foreign Disk Group is selected. Click **OK**.
      2) The next screen shows the type, condition, and size of the Foreign Disk. Click **OK** and wait for the disk to be imported.
      3) When the disk import completes, press **F5** (refresh). The mounted iSCSI snapshot is visible and contains an assigned drive letter. If drive letters are not automatically assigned, right-click the required partition and select **Change Drive Letters or Paths**. Click **Add** and select a drive letter.
6. Select the preferred snapshot date. A list of virtual machine disks that are backed up in the selected snapshot displays. Select a disk and click **Mount**.
7. In the `Select Mount Destination` dialog, check **Create virtual volume from selected partition**. A list of partitions available on the selected disk is shown. For each partition, its size, label, and file system type are displayed.
   - If the disk is not MBR-based, an error message is displayed.
   - By default, only partitions that can be used for file restore are displayed.
   - To display all partitions that existed on the original disk, clear the **Show only mountable partitions** check box.
8. Select the required partition. Partitions formatted using unsupported file systems cannot be selected.

9. Specify a drive letter or an empty folder as a mount point for the virtual volume.
10. Click **OK** to create a Virtual Volume that can be used to recover the files.
11. When the Virtual Volume is created, use Windows Explorer to copy the files to your preferred location.

    Tip: The ACL values associated with the folders and files that are restored in a file restore operation are not transferred to the restored files. To maintain ACL values, use the `XCOPY` command when copying files from the target.

Related tasks:

"Configuring the IBM Spectrum Protect recovery agent GUI" on page 19

"Manually configuring an iSCSI device" on page 26

Chapter 7. IBM Spectrum Protect recovery agent commands

The recovery agent CLI can be viewed as a command-line API to the IBM Spectrum Protect recovery agent. Changes completed with the recovery agent CLI to the IBM Spectrum Protect recovery agent take effect immediately.

You can use the recovery agent CLI to manage only one system running the IBM Spectrum Protect recovery agent.

On a Windows system, click **Start** > **Apps by name** > **IBM** > **Recovery Agent CLI**.

Mount

Use the `mount` command to complete various IBM Spectrum Protect recovery agent tasks.

The recovery agent CLI can be used to mount (`mount add`) and unmount (`mount del`) volumes and disks, and to view a list of mounted volumes (`mount view`).To use the `mount` command, the IBM Spectrum Protect recovery agent must be running. Use the `set_connection` command to connect a RecoveryAgentShell.exe to the mount application.

Snapshots are mounted or unmounted on the system where the IBM Spectrum Protect recovery agent is running.

Syntax for mounting a disk

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

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

►—pass—=—NodePassword"—-vmname—vmname—-type—disk—-disk———disk_number——————►

►—date—date_format————————————————————————————————————————————————————————►

►—-target—"ISCSI:—target—=—target_name—initiator—=—initiator_name"————————►◄
```

Syntax for mounting partition

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

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

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

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

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

Command types

add
Use this command type to mount a disk or volume of a snapshot to the system where IBM Spectrum Protect recovery agent is running.

The following list identifies the tags and parameters for the **add** command type:

-target
This tag is required. Use this tag to specify the following targets:

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

-rep
This tag is required. Use it to specify the IBM Spectrum Protect server that is storing the snapshots, and the IBM Spectrum Protect node that has access to the backups. For example:

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

You can also specify the `as_node` and `from_node` options. If the `password` field is empty, the IBM Spectrum Protect recovery agent attempts to use the password for the stored node.

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

-type disk

-type partition

-VMname
This tag is required. Use it to specify the machine name that is source of the snapshot. The specified value is case-sensitive.

-disk
This tag is required. Use it to specify the disk number of the source backed up machine to be mounted.

-date
This tag is required. Use it to specify the date of the snapshot that you want to mount. The date format is `yyyy-Mmm-dd hh:mm:ss`. For example:

```
-date "2013-Apr-12 22:42:52 AM"
```

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

-PartitionNumber
This tag is optional. If the -type is partition, enter the partition number to mount.

-ro|-fw
Use this tag to specify whether the mounted volume is read-only (**-ro**) or fake-write (**-fw**).

-disk
This tag is required. Use it to specify the disk number of the source backed up machine to be mounted.

-ExpireProtect
This tag is optional. During a mount operation, the snapshot on the IBM Spectrum Protect server is locked to prevent it from expiring during the operation. Expiration might occur because another snapshot is added to the mounted snapshot sequence. This value specifies whether to disable expiration protection during the mount operation. You can specify one of the following values:

Yes Specify `Yes` to protect the snapshot from expiration. This value is the default. The snapshot on the IBM Spectrum Protect server is locked and the snapshot is protected from expiration during the mount operation.

No Specify `No` to disable expiration protection. The snapshot on the IBM Spectrum Protect server is not locked and the snapshot is not protected from expiration during the mount operation. As a result, the snapshot might expire during the mount operation. This expiration can produce unexpected results and negatively impact the mount point. For example, the mount point can become unusable or contain errors. However, expiration does not affect the current active copy. The active copy cannot expire during an operation.

When the snapshot is on a target replication server, the snapshot cannot be locked because it is in read-only mode. A lock attempt by the server causes the mount operation to fail. To avoid the lock attempt and prevent such a failure, disable expiration protection by specifying `No`.

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

The following list identifies the tags and parameters for the **`dump`** command type:

`-rep` This tag is required. Use this tag to specify the IBM Spectrum Protect server storing the snapshots, and to specify the IBM Spectrum Protect node that has access to the backups. For example:

```
tsm: ip=<IP/host name> port=<PortNumber>
node=<NodeName> pass=<NodePassword>
```

`-file` This tag is optional. Use this tag to identify a file name to store the dump text. If this tag is not specified, the dump text is printed only to stdout.

remove

Use this type to remove the connection to the IBM Spectrum Protect server. A connection cannot be removed when it is in use, such as when mounted volumes exist.

The following list identifies the tag for the **`remove`** command type:

`-rep` - This tag is required. Use this tag to specify the IBM Spectrum Protect server connection to be removed.

view Use this type to view a list of all mounted snapshots. This type has no tags.

Example commands

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

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

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

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

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

- In the following example an iSCSI target is specified:

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

In this example, a snapshot of virtual machine named VM-03ent is located on the IBM Spectrum Protect server with IP 10.10.10.01. Disk number 1 of this snapshot is mounted to the system where the IBM Spectrum Protect recovery agent is running. The following command shows how to specify the **add** type to mount a disk:

```
mount add -rep "tsm: ip=10.10.10.01 port=1500 node=tsm-ba pass=password"
-target "iscsi: target=test1 initiator=initiator_name" -type disk
-vmname VM-03ENT -disk 1 -date "2014-Jan-21 10:46:57 AM -ExpireProtect=Yes"
```

The following examples show how to specify the dump type:

- List all the available backed up VMs.
  ```
  mount dump –type TSM –for TSMVE -rep P -request
  ListVM [–file <FileNameAndPath>]
  ```
- List all the available disk snapshots of a virtual machine.
  ```
  mount dump –type TSM –for TSMVE -rep P -request
  ListSnapshots -VMName P [-file <FileNameAndPath>]
  ```
- List all the available partitions of a disk snapshot.
  ```
  mount dump –type TSM –for TSMVE -rep P -request
  ListPartitions -VMName P -disk P -date P [-file <FileNameAndPath>]
  ```

In the following example, remove the connection to the IBM Spectrum Protect server (10.10.10.01) using node NodeName:

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

The following example uses the **view** type:

```
mount view
```

Related links for mounting a Hyper-V snapshot

- “**Set_connection**”
- “**Help**” on page 75

Set_connection

The **set_connection** command sets the Recovery Agent CLI to work with a specified IBM Spectrum Protect recovery agent.

Syntax

```
►►──RecoveryAgentShell.exe -c──set_connection──────────────────────────────►

►─mount_computer───IP address or host_name─────────────────────────────────►◄
```

Command type

mount_computer

Use this command type to set the connection from the recovery agent CLI to the system where the IBM Spectrum Protect recovery agent is installed.

The following list identifies the parameters for the **mount_computer** command type:

IP address or host_name

This variable is required. Specify the IP address or hostname of the system where the IBM Spectrum Protect recovery agent is installed.

Example commands

In the following example, the recovery agent CLI is set to work with the IBM Spectrum Protect recovery agent on the *ComputerName* host.

```
set_connection mount_computer ComputerName
```

Related links for setting a connection

- "**`Mount`**" on page 71
- "**`Help`**"

`Help`

The **`help`** command displays the help for all of the supported recovery agent CLI commands.

Syntax

```
►►──RecoveryAgentShell.exe -c──-h──command────────────────────────────────►◄
```

Command tag

`-h` Use this command tag to show help information.

The following list identifies the parameter for the **`mount_computer`** command type:

command

This variable is required. Specify the Recovery Agent command for which you want help information.

Example commands

In the following example, the recovery agent CLI is set to work with the IBM Spectrum Protect recovery agent on the *ComputerName* host.

```
set_connection mount_computer ComputerName
```

Related links for setting a connection

- "**`Mount`**" on page 71
- "**`Set_connection`**" on page 74

Recovery agent command-line interface return codes

Return codes help identify the results of the recovery agent CLI operations.

Use these return codes to check the status of your recovery agent CLI operations.

Table 5. Recovery Agent CLI return codes

Return Code	Value	Description
0	FBC_MSG_MOUNT_SUCCESS	Command submitted successfully to Data Protection for Microsoft Hyper-V mount.
0	FBC_MSG_DISMOUNT_SUCCESS	Successfully dismounted a snapshot.
0	FBC_MSG_VIEW_SUCCESS	View operation successful.

Table 5. Recovery Agent CLI return codes (continued)

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

Table 5. Recovery Agent CLI return codes (continued)

Return Code	Value	Description
41	FBC_MSG_RESOURCE_BUSY_IN_ TAPE_MODE	Data Protection for Microsoft Hyper-V is running in tape mode - media is busy.
42	FBC_MSG_DISK_TYPE_NOT_ SUPPORTED	Partition operation not supported for this type of disk.
43	FBC_MSG_MOUNT_INITIALIZING	The operation failed, Data Protection for Microsoft Hyper-V mount is currently initializing. Try again later.
44	FBC_MSG_CANNOT_LOCK_ SNAPSHOT	The snapshot cannot be protected against expiration during this operation. Refer to documentation for more details.

Appendix. Accessibility features for the IBM Spectrum Protect product family

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Overview

The IBM Spectrum Protect family of products includes the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader

The IBM Spectrum Protect family of products uses the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) and Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the product.

The product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described in the Accessibility section of the IBM Knowledge Center help (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Keyboard navigation

This product uses standard navigation keys.

Interface information

User interfaces do not have content that flashes 2 - 55 times per second.

Web user interfaces rely on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

Web user interfaces include WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Vendor software

The IBM Spectrum Protect product family includes certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for accessibility information about its products.

© Copyright IBM Corp. 2011, 2016

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility (www.ibm.com/able).

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 on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

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

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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

© Copyright IBM Corp. 2011, 2016

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

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

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

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

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

COPYRIGHT LICENSE:

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

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

Trademarks

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

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

Linear Tape-Open, LTO, and Ultrium are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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

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

Microsoft, Windows, and Windows NT 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.

SoftLayer® is a registered trademark of SoftLayer, Inc., an IBM Company.

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability
These terms and conditions are in addition to any terms of use for the IBM website.

Personal use
You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use
You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details in the section entitled “Cookies, Web Beacons and Other Technologies,” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

A glossary is available with terms and definitions for the IBM Spectrum Protect family of products.

See the IBM Spectrum Protect glossary.

To view glossaries for other IBM products, see IBM Terminology.

© Copyright IBM Corp. 2011, 2016

Index

Product Number: 5725-X00

Printed in USA