Protecting Virtualization Infrastructure by Using DPM

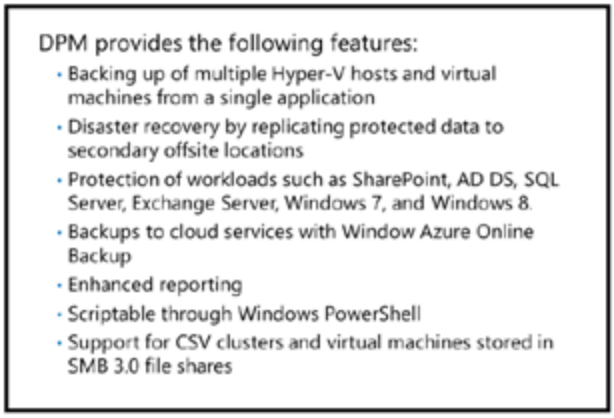
Building a robust protection solution for your virtualization infrastructure is as import ant as building the solution itself. This lesson provides insight into the capabilities of System Center 2012 R2 Data Protection Manager
(DPM), specifically in relation to server virtualization. DPM along with server virtualization provides a framework on which you can build a protection solution. This lesson provides details on both core and optional DPM components, their usage, and requirements.

Lesson Objectives

After completing this lesson, you will be able to:

- Describe the benefits of using DPM.
- Describe the DPM components and protection process.
- Explain the considerations for using DPM to back up virtual machines.
- Describe how to deploy DPM protection agents.
- Explain how to configure protection groups.
- Describe the options for protecting virtualization infrastructure.
- Describe how to perform a virtual machine recovery.
- Explain how to deploy Windows Azure Online Backup for DPM.

Benefits of Using DPM



DPM is an enterprise backup solution. DPM is classified as Enterprise for its features and functionality, although it is also an optimal solution for small to medium size organizations.
While DPM is available as an independent platform, for optimal usage, it is best to int egrate it with other System Center components.
You use DPM to back up virtualized data centers.

It offers application-aware backups and full Hyper-
V host backups. Unlike Windows Backup, DPM supports multiple backup schedules and has advanced features and functionality that you can use to create a fully automated protection solution.
You should use DPM to:

- Back up multiple Hyper-V hosts and virtual machine servers at the same time, and use one or more schedules.
- Enhance disaster recovery by replicating protected data to a secondary offsite location.
- Protect workloads such as Microsoft Office SharePoint, AD DS, SQL Server, Microsoft Exchange Server, Linux and Windows client operating systems such Windows 7 and Windows 8.
- Protect data using disk-to-disk, disk-to-tape, or Window Azure Online Backup.
- Received detail reports on data churn, growth, forecasting and the Data Protections Manager Health status.

DPM offers the following feature and or benefits:

- Uses SQL Server, and includes support for clustered servers that are running SQL Server. This allows for scalability and availability of your backup solution.
- Supports full and incremental backups. After a full synchronization has occurred, you can optionally back up only the block changes, thereby providing faster backups.
- Can be deployed to a virtual machine; this enhances its own protection and flexibility.
- Provides self-service for workloads such as SQL Server databases. For example, a developer could restore a database to the same location, to a folder, or to an alternate server that is running SQL Server. An end user also could recover files they have deleted from within a protected share.
- Integration with System Center 2012 Orchestrator. This enables you to build automation into your virtualization or cloud computing environment.
- Integration with System Center 2012 Service Manager. This enables you to offer backup as part of a service catalogue, and align with business processes.
- Integration with Operations Manager. You can administer DPM from within the Operation console. This provides a single console to administer multiple DPM servers, and allows granular delegation of tasks to operators and administrators, such as bulk restart of failed backup jobs.
- Supports item-level Recovery. Item-level recovery allows you to back up a virtual disk of a virtual machine on the Hyper-V host server. You can then recover individual items from within the protected virtual machine's virtual disk.
- Supports automation. Supports automation using either the DPM Management Shell,

which is built on Windows PowerShell, or by using the System Center Integration Pack that integrates Orchestrator and DPM.

- Supports bare-metal restores. This enables you to restore an entire server using the Repair your computer option located on the Windows Server setup media.
- Online backup. DPM makes use of VSS on the Hyper-V host and on a virtual machine. If a virtual machine is running Windows 2003 or newer, and if the virtual machine receives a backup request from the Hyper-V host, it uses VSS and places the guest operating system in a suitable state for backup.
- Provides several disaster recovery options. For disaster recovery you can back up all the DPM-protected data to a secondary site, or back up to Windows Azure Online Backup.

DPM protects several workloads and their associated components as follows:

- SQL Server
- Hyper-V
- AD DS
- SharePoint Server
- Exchange Server
- Virtual Machine Manager database
- Linux virtual machines

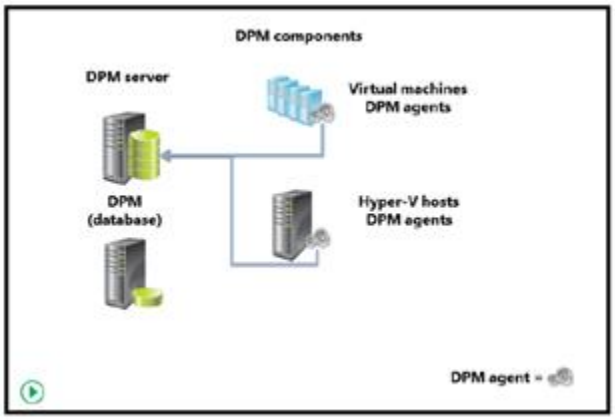
For a comprehensive list of protected workloads and their recoverable data types, refer to the following link:

Protecting workloads with DPM

http://go.microsoft.com/fwlink/?LinkID=386744

Other DPM benefits include support for the protection of virtual machines that are run ning on CSV, and for virtual machines that are running from Server Message Block (SMB) 3.0 file shares. To improve backup performance, DPM can exclude virtual ma chine page files from incremental backups. DPM also supports backups for machines during live migration.

DPM Components and the Protection Process



DPM is made up of the following architectural components:

- DPM server. The DPM server is the main server component that processes the backup and recovery jobs. It manages the storage volumes and tape hardware, and provides the reporting features. The DPM server also manages agent configuration and deployment.
  The DPM server requires a server that is running SQL Server. The DPM installation includes an instance of SQL Server 2008 R2, which DPM setup installs on the DPM server. You can choose to use an alternate SQL Server for DPM.
- DPM database. The DPM database stores the DPM configuration and reporting data. When using a remote SQL Server, DPM requires that the SQL Server database engine and SQL Server Reporting Services components are installed. DPM supports SQL Server 2008 R2 and SQL Server 2012.
- DPM protection agents. A protection agent is the software that you install on the target servers or computers that you intend to protect. Protection agents allow the DPM server to identify and transfer the data for backup and restore. DPM has only a single agent type. Whether you are protecting SQL Server, Hyper-V, Exchange Server, or AD DS, you only need to deploy a single agent type.
- Protection groups. Protection groups define storage pools, retention settings, and data sources that need protecting. All data sources in the same protection group share storage allocation, replication creation methods, and compression settings.
- Central console. The central console allows monitoring of multiple DPM servers including differing versions from a single console. You must install the central console on an Operations Manager server. The console provides remote administration, role-based access, remote remediation, service level agreement (SLA) alerts, scripting support, and alert consolidation.
- Storage pool. The storage pool consists of disks that attach to the DPM server, and that DPM uses to store its data replicas and recovery points. DPM can use direct-attached storage (DAS), Fibre Channel, and Internet small

computer system interface (iSCSI). However, it cannot use USB storage or the Storage Spaces feature in Windows Server.

- Tape libraries. You can attach tape drives and tape libraries to the DPM server either directly, or through your SAN. (Refer to TechNet DPM documentation to search for compatible tape devices.)
  You can also use a virtual tape library. A virtual tape library emulates a physical tape library but stores data on disk.
- Secondary DPM server. The secondary DPM server is the same as the primary DPM server with the exception that you use it to provide protection for you primary DPM servers.
- Windows Azure Backup Agent. When using the Windows Azure Backup feature, you must download and install a Windows Azure Backup Agent on to each DPM server (both primary and secondary).

Overview of DPM Features
http://go.microsoft.com/fwlink/?LinkId=253435

How DPM Works

After you have installed a primary DPM server and configured its storage and tape co mponents, you are now ready to create a protection group. Within the DPM console, s elect the desired protection type
(Servers or Clients), add at least one member to the group, and then define if you will use disk, tape, or Windows Azure Backup Agent. You then set a schedule and retentio n range, and then configure the disk allocation and the initial replication method.
After you create the protection group, DPM creates a volume in the storage pool in wh ich to store a replica of each server or client that is part of the protection group. When the DPM protection agent on the protected server or client tracks data changes, DPM s ynchronizes the protected data to the replica, and transfers the changed data to the DP M server.

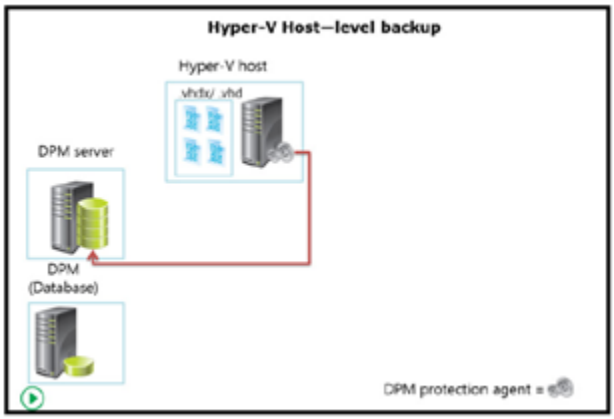
The Synchronization Process

During synchronization, the DPM protection agent uses a volume filter and change jo urnal to track file changes, and then performs a checksum process to synchronize only the changed blocks. A data replica has can become inconsistent due to various reason s. However, you can schedule to run a consistency check that allows DPM to verify re plica data with its source, and then synchronize required changes that return the replic a to a consistent state. When creating or modifying a protection group, you can define what are known as recovery points. *Recovery points* are points in time from which yo u can restore data.
DPM uses VSS writers for backing up remote workloads. It also uses VSS locally to create express full backups. Express full backups update the replica data with the

incremental changes.

- For file data, DPM can store a maximum of 64 recovery points, which is the limit for VSS. For example, if you schedule two recovery points per day, the maximum retention will be 32 days.
- For application data, DPM can store a maximum of 512 available recovery points. However, DPM reserves 64 recovery points for VSS, so you can only select up to 448 recovery points for your applications.
- For longer term recovery options, you should consider using tapes or virtual tapes.

Considerations for Using DPM to Back Up Virtual Machines

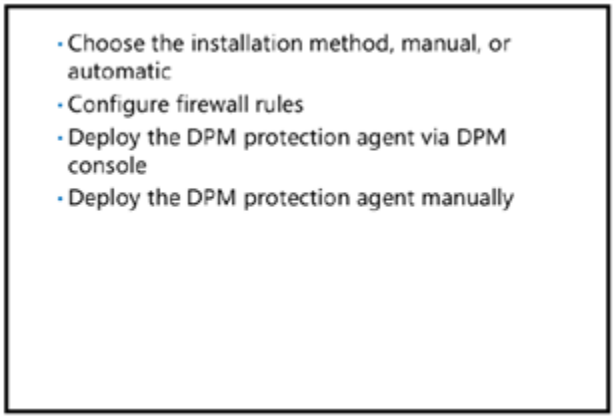


When planning your backup strategy for virtual machines, you should consider your backup options with respect to specific services or product that are running on your virtual machines. Moreover, you should follow the technical documentation and supported backup options for each service or product that runs on your virtual machines, such as AD DS, files and folders, Exchange Server, and SQL Server. Consider the following options for implementing virtual machine backups in your organization:

- Perform backups on the physical server where virtual machines are located. In this scenario, you back up all virtual machine files. This type of backup is thorough, because all of your virtual machine configuration and data is backed up. However, you must ensure that this type of backup is supported for the services or products that are running on your virtual machines. For example, we do not recommend this type of backup for Exchange Server when it is running in a virtual environment.
- Perform data backups on the virtualized server. This option performs data backup in the same manner as if a server was installed on a physical machine, which means that only the data inside the virtual machine is backed up. We recommend this type of backup when Microsoft Exchange Server is running in a virtual environment.

- Perform an online backup. This type of backup ensures that data has been backed up without interrupting a production environment. If the product installed in your virtualized environment supports this type of backup, we recommend that organizations utilize online backup so that their servers can continue to work during the backup process.
- Perform an offline backup. This type of backup requires that you stop the virtual machine until the backup is complete. The virtual machines then can resume working. We do not recommend this type of backup because it will cause a downtime of services that are running on the virtual machine. Instead, consider performing an offline backup if no other type of backup is supported or is possible in your organization.

Deploying DPM Protection Agents



You must install DPM protection agents on each server or client that you want to prot ect. The DPM protection agent is the software that DPM uses to identify and track cha nges to data that the DPM server can protect. You can use several methods to deploy protection agents, and several scenarios in which you can deploy them.

Note: This course reviews how to install DPM protection agents in the same Windows domain as the DPM server. Installing D PM in untrusted domains and work groups is supported, but it is beyond the scope of t his course.

Firewall Settings

Before you deploy DPM protection agents, you should ensure that the DPM server ca n communicate with the protected computer through any firewalls. On the DPM serve r, you should ensure that port 135 is open for TCP traffic, and that the DPM service (Msdpm.exe) and the DPM protection agent (DPmra.exe) can communicate through the firewall.

Automated Installation Process for No Firewall, Same Domain

1. On the DPM server, launch the DPM Administrator Console. On the ribbon, click the **Management** workspace, and then click **Install**.

2. In the Protection Agent Installation Wizard, on the **Select Agent Deployment Method** page, click **Install agents**, and then click **Next**.
3. On the **Select Computers** page, in the **Computer name** section, click to highlight one or more computers that you want to protect, and thenclick **Add**. You can install earlier versions of the agent by clicking **Advanced**, and then selecting the version from the drop-down list box. When you have finished selecting computers, click **Next**.
4. On the **Enter Credentials** page, enter credentials with administrative rights for the server or client you will be protecting. You domain will be listed as default. After entering your credentials, click **Next**, and wait for the cluster-checking phase to complete.
5. On the **Choose Restart Method** page, click **Restart the protected computer manually or automatically**, and then click **Next**.
6. On the **Summary** page, review the note about computers possibly losing network connectivity during installation, and then click **Install**.

Manual Installation Process for Windows Firewall, Same Domain

1. Copy the DPM protection agent setup files, or map a drive to the DPM protection agent installation directory on the DPM server.
2. Run the installer from a command prompt, and specify the fully qualified domain name (FQDN) for the DPM server. For example, to install the DPM protection agent on a 64-bit computer with a DPM server named LON-DPM1.adatum.com, you would type the following at a command prompt:
```
DPMAgentInstaller_x64.exe LON-DPM1.adatum.com
```
3. On the server you wish to protect, sign in, open a command prompt, and type the following command:
```
netsh advfirewall firewall add rule name="Allow DPM Remote Agent Push" dir=in
action=allow service=any enable=yes profile=any remoteip=<IPAddress>
```
4. On the DPM server, launch the DPM Administrator Console. Click the **Management** workspace and then on the ribbon click **Install**.
5. In the Protection Agent Installation Wizard, on the **Select Agent Deployment Method** page, click **Attach agents**, click **Computers on trusted domain**, and then click **Next**.
6. On the **Select Computers** page, in the **Computer name** section, click to highlight one or more computers that you want to protect. Alternatively, you either can type the FQDN of the DPM server, or you can select to import from a text file, and then click **Add**. When you have finished selecting computers to protect, click **Next**.
7. On the **Enter Credentials** page, enter credentials with administrative rights for the server or client you will be protecting. Your domain will be listed as the default. After entering your credentials, click **Next**, and wait for the cluster checking phase to complete.

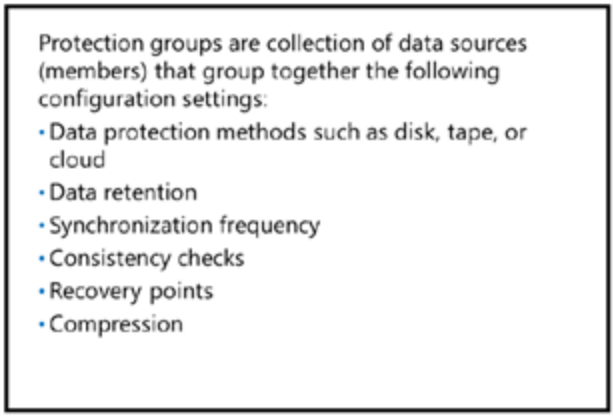
8. On the **Summary** page, review the note about computers possibly losing network connectivity during installation, and then click **Attach**.

DPM performs an automatic discovery to identify new computers that have been added to the Active Directory domain of which the DPM server is a member. By default, auto discovery runs at 01:00 A.M daily, but you can modify this schedule. Discovered servers and clients are listed in the Protection Agent Installation Wizard, or in the Create New Protection Group Wizard.

For a list of ports and agent network troubleshooting steps, use the following article as a guide:

Data Protection Manager Agent Network Troubleshooting
http://go.microsoft.com/fwlink/?LinkID=386741

Configuring Protection Groups



What Are Protection Groups?

Protection groups are a collection of data sources that share protection configurations, such as storage pools, retention settings, schedules, recovery points, and compression settings. Data sources are referred to as *members*. Individual servers can have multiple members. For example, system state and each volume are classified as members.

A member can be protected by multiple protection groups, but only one primary DPM server can protect any one data source. Protection groups can include more than one server or client, and you should use them to create logical groups that support your backup strategy. Some examples of protection groups that you could implement are:

- A group of Hyper-V hosts whose virtual machines you protect using the online backup method.
- A group for specific virtual machines and physical servers such as SQL Server databases or domain controllers.

- A group of file servers.
- An Exchange Server group
- A group of non-production servers.

To create a protection group, perform the following steps:

1. On the DPM server, launch the DPM Administrator Console, and then click the **Protection** workspace. On the ribbon, click **New**.
2. In the New Protection Group Wizard, on the **Welcome** page, click **Next**.
3. On the **Select protection group type** page, click **Next**.
4. On the **Select group members** page, in the **Available members** section, select the data sources. For example, if your Hyper-V host server is named LON-HOST1, expand LON-HOST1, and then click to select each virtual machine that you want to protect. When you are finished selecting data sources, click **Next**.
5. On the **Select Data Protection Method** page, in the **Protection group name** text box, type a descriptive name for the protection group name. Click to select the protection method or methods. For example, click **I want to short-term protection using: Disk**. If you have configured online protection with Windows Azure Backup or if you have configured a tape library, you can select these now. When you are finished selecting the protection methods, click **Next**.
6. On the **Select Short-term Goals** page, select the number of retention days for the protection group, and then click **Modify**.
7. On the **Express Full Backup** page, you can optimize the number of recovery points by amending the express full backup schedule. When done, click **Next**.
8. On the **Review Disk Allocation** page, click **Modify**. Here you can review and change the replica and recovery point volumes. Click **Cancel**, and note that **Automatically grow the volumes** is selected by default. Click **Next**.
9. On the **Choose Replica Creation Method** page, for the data that you select, you can choose either to replicate now, or to replicate later. Alternatively you can perform a manual data transfer using removable media. Leave the default settings, and then click **Next**.
10. On the **Consistency check options** page, you can choose to run consistency checks when replicas become inconsistent (this is the default). Additionally, you can create a scheduled daily check. Leave the default settings, and then click **Next**.
11. On the **Summary** page, review your protection group settings, then click **Create Group**.
12. On the **Status** page, review the results of the tasks, and then click **Close**.

Within protection groups, you can configure recovery points separately for application members and file members. For example, you can schedule daily express full backup s for a file server, and multiple daily backups for SQL databases in the same group. Where separate applications such as Exchange Server and SQL Server are within the same group, they will be grouped on the same schedule. Therefore, if this option is not suitable, you should create a separate protection group for another application type .

You can enable compression for each protection group. Compression reduces the amount of data that transmits over the network for replica creation, synchronization, consistency checks, and recovery operations. By enabling compression, you incur a slight additional CPU overhead for both the DPM server and the protected server or client.

You can enable compression by using the following steps:

1. Sign in to the DPM server and launch the DPM Administrator Console. Click the **Protection** workspace. In the central section under **Protection Group Member**, click the **Protection** group, and then on the ribbon, click **Optimize**.
2. In the **Optimize Performance** dialog box, click the **Network** tab. In the **Network** section, click **Enable on-the-wire compression**.

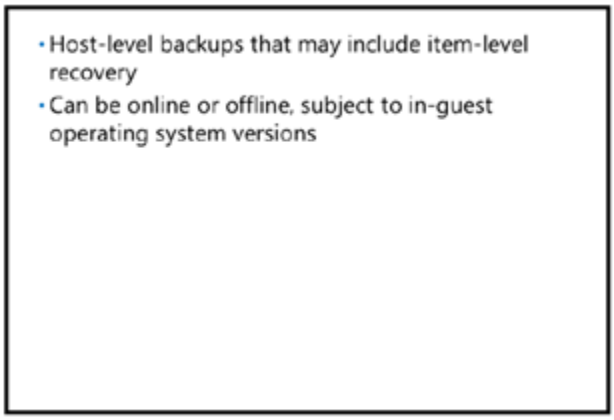
You can add and remove members from a protection group, and you can modify group settings by using the Modify Group Wizard. Use the following steps to access the Modify Group Wizard:

1. Sign in to the DPM server, and launch the DPM Administrator Console. Click the **Protection** workspace, then in the central section under **Protection Group Member**, click the **Protection** group. On the ribbon, click **Modify**.
2. In the Modify Group Wizard, on the **Select Group** page, you can add and remove members.
3. Complete each step of the wizard, making any required changes.

A consistency check verifies that replica data is valid. Consistency check settings are shared with all data members in a protection group. Running consistency checks can create a slight overhead on the DPM server and the protected computer, and consume network bandwidth.

You cannot throttle bandwidth at the protection group level. Bandwidth throttling is set in the DPM protection agent settings for each protected server or client.

Options for Protecting Virtualization Infrastructure



You can use DPM to build your virtualization infrastructure protection strategy by utilizing the following virtualization-specific functionalities:

- Protection for both running and stopped virtual machines, from a DPM agent that you install on a Hyper-V host
- Protection for running virtual machines using a traditional backup, including system state and all files
- Protection of specific guest application workloads, namely Microsoft workloads such as the SQL databases used to run the System Center 2012 components
- Item-level recovery, which allows you to restore a single file from within a virtual hard disk that was backed up at host level
- Protection for virtual machines that reside on CSVs
- Protection for virtual machines that reside on SMB storage
- Protection for virtual machines during live migration
- Protection for both clustered and non-clustered VMM servers
- Scale-out protection. In some scenarios, you can have multiple DPM servers to provide protection to a large Hyper-V cluster. The host must be running a clean installation of Hyper-V on Windows 2012, and System Center 2012 SP1 DPM or System Center 2012 R2 DPM
- Select to back up Hyper-V as a host-level workload in a protection group. This ensures that all future virtual machines that you create on that host or cluster will also be backed up

When designing a backup solution, you will need to consider options such as the following:

- How and when will initial replication take place?
- How many hosts and virtual machines can be backed up at the same time without causing performance issues?
- How much load will there be, and is compression and or

bandwidth throttling required?

Remember that you can use DPM in conjunction with other technologies such as Hyper-V Replica, and that DPM can help form part of an overall solution. While it is imperative that you implement a good data protection strategy, it is also important that you not overcomplicate protection and recovery. The following topics are protection options for different Hyper-V host scenarios.

Stand-Alone Hyper-V Hosts

To provide host-level protection to a virtual machine that is running on a stand-alone Hyper-V host, you must first install an agent on the Hyper-V host. You can protect virtual machines that are running on local storage, such as DAS, SAN, and network-attached storage (NAS). If your Hyper-V host uses SMB 3.x, you must also install a DPM protection agent on the file server that is hosting the SMB share.

CSVs

DPM can provide protection for virtual machines that reside in CSV by using a hardware VSS provider, or an integrated software provider. There is a significant difference between Windows Server 2008 R2 Hyper-V CSVs and Windows Server 2012 R2 CSVs. Without a hardware-based VSS provider, you can only run one backup job at a time per CSV volume. In addition, the backup job places the cluster into a redirected I/O mode, which significantly reduces overall cluster performance. With CSV 2.0, this is no longer the case. By default, you can run three parallel backups or more with a registry key update. I/O redirection no longer occurs during backup. To perform CSV backups, you must install the DPM protection agent on each node in the Hyper-V host cluster.

SMB 3.x Shares

As with stand-alone Hyper-V hosts, you can back up Hyper-V host clusters that use SMB 3.x storage. The storage is represented by either a stand-alone file server or a clustered file server. You must install the DPM protection agent on each Hyper-V host and on each file server, to protect the virtual machines by using host-level backups.

Live Migration Protection

During live migrations, DPM protects virtual machines within a cluster without

requiring any administrator intervention. DPM detects the migration and continues to protect the virtual machine from the new hosting node of the cluster. DPM can also protect live migrations that you perform outside of a cluster. However, this method has some requirements, such as the protected virtual machine must be part of cloud configuredon System Center 2012 Service Pack 1
(SP1) VMM or newer, and the DPM servers must be connected to the VMM manage ment server on which the cloud service is located.

Item-Level Recovery

Item-
level recovery allows you to protect virtual machines at the host level. It also allows you to recover individual files and folders from within the virtual hard disk of the virtual machines. Unfortunately, you cannot restore these items directly to their original location. However, you can restore them locally to the DPM server or to a net work location, and then copy them to their original location. Item-
level recovery is very useful in many situations. However, you may want to use the in -guest backup method for a file server, which will enable end-user self-
service recovery.
You can use each of these to protect an entire virtual machine at the host level. When you build your protection solution, ensure that you take into consideration the workloads that you need to protect. Where appropriate, you should schedule virtual machine–level backups.
Using both item-level recovery and virtual machine–
level backup provides the best solution. For example, you may have a critical database server that requires hourly backups. However, you could schedule the virtual machine that is hosting the database to be backed up daily. In this scenario, you would configure two scheduled backups, and then set the start times.

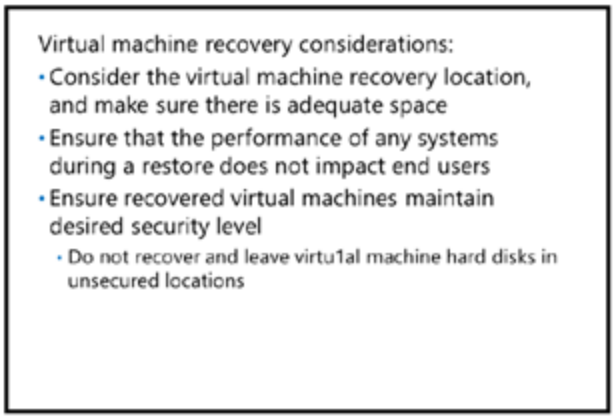
Best Practices

As a best practice, you should:

- Document the options pertaining to your specific virtualization infrastructure, including:
  - Hyper-V host versions.
  - Storage technology.
  - Virtual machine workloads.
  - Operating systems versions.
- Where possible, use a proof of concept on hardware that is as similar as possible to the end solution.

- Determine the following:
  - Backup volumes
  - Network throughput
  - Document recovery points
  - Recovery times and locations
- Be sure to test recovery from backups, and where possible, randomize the recovery testing.
- Define who will receive the backup reports, and make sure that they receive them.
- Have an action plan that is subject to the content of the backup reports, such as increasing storage space, modifying schedules, or throttling bandwidth.

Performing Virtual Machine Recovery



When performing a virtual machine recovery, there are typically three scenarios:

- Recovering a virtual machine to its original location
- Recovering a virtual machine to an alternate location
- Recovering an item such as a file, folder, volume, or disk, from within a virtual machine

You can use the DPM Administrator Console to recover a virtual machine to its origin al location.
Use the following high-level steps, where:

- DomainName is the name of the domain in which the server was backed up.
- ServerName is the name of the server you are recovering.
- xyz is the state of the server when it was backed up, for example: Saved State, or Online.

1. Launch the DPM Administrator Console.
2. Click the **Recovery** workspace.
3. In the navigation pane, expand **Recoverable Data*DomainName**ServerName***, and then click **All Protected HyperV Data**.

4. In the results pane, under **Recoverable Item**, select and right-click **Backup Using *xyz* State *ServerName***, and then click **Recover**.
5. In the Recovery Wizard, on the **Review Recovery Selection** page, click **Next**.
6. On the **Select Recovery Type** page, click **Recover to original instance**, and then click **Next**.
7. On the **Specify Recovery Options** page, c**lick Next**.
8. On the **Summary** page, click **Recover**.
9. On the **Recovery Status** page, verify that the **Recovery status is Successful**, and then click **Close**.

As a best practice, you should always test recovery scenarios as part of your overall backup strategy. When testing, note the amount of time it takes to recover the data, and the integrity of data. Consider that as the backup sizes grow, the recovery time will also grow. While an incremental backup may take 10 minutes, a full server restore may take an hour or longer.

Note: Be aware of any performance impact from recovering virtual machines to production Hyper-V hosts. During the proof of concept phase of a virtualization deployment, you should determine whether recovering full virtual machines is acceptable during business hours. To determine this, review network, storage, and processor performance.