Module 10
Configuring High Availability, Disaster Recovery and Protection for a Cloud

Module Overview

• Planning for Azure Site Recovery
• Planning DPM Deployment
• DPM Architecture and Components
• Upgrading DPM
• Configuring DPM for the Private Cloud
• Configuring Application Protection for a Cloud
• Restoring Applications to the Cloud
Lesson 1: Planning for Azure Site Recovery

- Considerations for Hyper-V Replica
- Managing Replica Health with Virtual Machine Manager
- Overview of Azure Site Recovery
- Orchestrated Recovery

Considerations for Hyper-V Replica

- Considerations for Hyper-V Replica include:
  - Planning
    - Establish the most important applications and services, and
    - How much downtime and data loss is acceptable.
  - Disaster Recovery Scenarios
  - Data Replication Timescale
  - Capacity Planning
  - Hosting and Network
  - Monitoring
  - Financial
Managing Replica Health with Virtual Machine Manager

- The Primary Server checks and maintains the status of the Virtual Machine's replication health.
  - This status is maintained in memory and refreshed periodically - 5 minutes is the default interval.
  - It provides a summary of the Hyper-V replication, for example, for a particular virtual machine, the time of its last replication and the size of the replicated data onto the Replica Server.
  - A health status can take one of the following values: Normal, Warning or Critical.
  - Other statuses are - Not Replicating and Not Applicable.

Overview of Azure Site Recovery

- Azure Site Recovery is used to:
  - Manage the failover of VMs sited on VMM clouds.
  - Co-ordinate and monitor the asynchronous replication of VMs between sites.
  - Continually monitor service availability.
  - Test the recovery.
  - Enabling automatic orchestrated site recovery.
  - Handle virtual networks that failover by mapping them at the primary and secondary sites to one another.
Orchestrated Recovery

- Orchestrated Recovery includes:
  - Creating a Recovery Plan
  - Customizing a Recovery Plan by:
    - Adding virtual machines and groups
    - Adding manual actions and scripts
  - Testing the Recovery Plan
  - Performing a planned failover
  - Performing an unplanned failover
  - Monitoring Azure Site Recovery job status

Lesson 2: Planning DPM Deployment

- Considerations for DPM Deployment
- Selecting a Backup Method
- Defining Storage Requirements
- Defining Security Requirements
- Defining Software Requirements
- Defining Hardware, Network, and Scaling Requirements
Considerations for DPM Deployment

**Consider the following:**
- What is your budget?
- Which applications and operating systems will DPM protect?
- Where and how long will DPM retain data?
- What is the RPO for each application?
- What is the RTO for each application?
- How much data will DPM protect for each application?
- How many agents are domain-joined to AD DS, how are non-domain-joined, and where will they be located?
- Will you perform all recovery operations, or will you delegate this task to others?

Selecting a Backup Method
Defining Storage Requirements

**DPM requires block storage:**

- Direct attached storage
- Storage area network

**To estimate storage requirements, you can use:**

- DPM storage calculators
- Incremental backup calculations

---

Defining Security Requirements

<table>
<thead>
<tr>
<th>User Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPM Read-Only Operator</td>
<td>Can view all items, but cannot modify or run any items</td>
</tr>
<tr>
<td>DPM Recovery Operator</td>
<td>Can only perform recoveries</td>
</tr>
<tr>
<td>DPM Reporting Operator</td>
<td>Can only run and manage reports</td>
</tr>
<tr>
<td>DPM Tier-1 Support</td>
<td>Can run backups and perform basic troubleshooting</td>
</tr>
<tr>
<td>DPM Tier-2 Support</td>
<td>Can run backups and perform corrective actions such as enabling/disabling agents</td>
</tr>
<tr>
<td>DPM Tape Operator</td>
<td>Can rerun backups or perform tape drive tasks</td>
</tr>
<tr>
<td>DPM Tape Admin</td>
<td>Can perform all tape-related actions</td>
</tr>
<tr>
<td>DPM Admin</td>
<td>Can perform all actions</td>
</tr>
</tbody>
</table>
Defining Software Requirements

**DPM requires:**

- .NET Framework 4.0
- Visual C++ 2008 Redistributable
- Windows PowerShell 2.0
- Windows Single Instance Store
- Microsoft Application Error Reporting

Defining Hardware, Network, and Scaling Requirements

**In addition to the software requirements, DPM requires:**

- Windows Server 2008 R2 (SP1) or later
- SQL Server 2008 R2 (SP1) or later
- At least 1 GHz dual-core CPU
- Pagefile that is 0.2 percent of the total size of all recovery point volumes
- At least 4 GB RAM
- At least 5 GB of free storage space and one additional drive for backup storage
- Membership in an Active Directory domain
Lesson 3: DPM Architecture and Components

• DPM Components
• DPM Protection Process
• Protecting Files and Applications
• End-User File Recovery
DPM Protection Process

- Volume D: Replica
- Volume D: Recovery Points
- Storage Group Replica
- Storage Group Recovery Points
- Database Replica
- Database Recovery Points
- Storage Pool

Transfer Changes
Update Replica
Volume D Replica

Protecting Files and Applications

Requestor

- DPM Agent
- Requestor

Writers

- Hyper-V
- SQL Server
- File servers
- AD DS
- Failover clusters
- Exchange Server
- SharePoint Server
- VMM
- System State
- Bare metal recovery

Provider

1 2 3 4 5 6 7
End-User File Recovery

To configure AD DS to support end-user recovery, do the following:

1. Extend the AD DS schema
2. Create the MS-ShareMapConfiguration container
3. Grant the DPM server permissions to change the container’s contents
4. Map source shares to shares on the replicas

Lesson 4: Upgrading DPM

- Prerequisites for Upgrading to DPM 2012 R2
- Performing an In-Place Upgrade
- Performing a Side-By-Side Upgrade
Prerequisites for Upgrading to DPM 2012 R2

To upgrade to DPM 2012 R2, you must have:

- Windows Server 2008 R2 (SP1) or later
- SQL Server 2008 R2 (SP1) or later
- DPM 2012 SP1 already deployed
- At least 1 GHz dual-core CPU
- Pagefile that is 0.2 percent of the total size of all recovery point volumes
- At least 4 GB RAM
- At least 5 GB of free storage space and one additional drive for backup storage

Performing an In-Place Upgrade

To perform an in-place upgrade with a local SQL Server instance, complete the following steps:

1. Back up the DPM 2012 SP1 DPMDB database
2. Verify that Microsoft$DPM$Acct has full permissions to the DPM 2012 DPMDB directory
3. Start DPM 2012 R2 Setup from the installation media
4. In the Setup Wizard, select the Use the dedicated instance SQL Server option
5. Complete the Setup Wizard
6. Upgrade the DPM protection agents
Performing a Side-By-Side Upgrade

Lesson 5: Configuring DPM for the Private Cloud

- Managing Storage Pools
- Deploying DPM Protection Agents on Trusted Domain-Joined Computers
- Using DPM Protection Agents on Untrusted and Workgroup Computers
- Deploying DPM Protection Agents on Untrusted and Workgroup Computers
- Using DPM Protection Agents with Certificate-Based Authentication
- Deploying DPM Protection Agents Using Certificate-Based Authentication
- Demonstration: Deploying DPM Protection Agents
### Managing Storage Pools

**The DPM storage pool can store various types of storage disks:**

- SAN
- DAS (SAS, SATA, IDE, SCSI)

### Deploying DPM Protection Agents on Trusted Domain-Joined Computers

**To manually install a protection agent, complete the following steps:**

1. Install the DPM protection agent
2. Configure the DPM protection agent for the DPM server
3. Attach the DPM protection agent on the DPM server

**To automatically install a DPM protection agent, use the Protection Agent Installation Wizard:**

1. Select the computers to use to install and configure the agents
2. Specify credentials of an account with permissions to install and configure the DPM protection agent
3. Choose whether to allow DPM to restart the computer
Using DPM Protection Agents on Untrusted and Workgroup Computers

Before deploying DPM protection agents on untrusted and workgroup computers, you must authenticate the computers.

NTLM Authentication

Untrusted or Workgroup Computer

Deploying DPM Protection Agents on Untrusted and Workgroup Computers

To deploy DPM protection agents on untrusted and workgroup computers, complete the following steps:

1. Copy setup files or map a drive to the installation directory
2. Run the DPM protection agent installer on the target computer
3. Set-DPMServer.exe -InNonDomainServer -UserName
4. Run the DPM Protection Agent Installation Wizard
Using DPM Protection Agents with Certificate-Based Authentication

Certificates must meet the following requirements:

- X.509 V3 certificates
- Certificates cannot be self-signed, and the root must be trusted
- Certificates must be enabled for both client authentication and server authentication
- Key length must be at least 1,024 bits
- Key type must be Exchange
- Certificates be installed for DPM server and protected computers

Deploying DPM Protection Agents Using Certificate-Based Authentication

1. Create and install a certificate
2. Set-DPMCredentials
   - Type Certificate
   - Action Configure
   - Thumbprint
   - OutputFilePath
3. Copy metadata file output
4. Install DPM protection agent on protected server, and use SetDPMServer.exe to associate agent with DPM server
5. Run AttachProductionServer With Certificate.ps1
Demonstration: Deploying DPM Protection Agents

In this demonstration you will see how to deploy the DPM protection agent.
Lesson 6: Configuring Application Protection for a Cloud

- Considerations for Configuring Protection Groups
- Configuring SQL Server Protection
- Options for Protecting the Cloud
- Configuring Item-Level Recovery for Cloud-Based Hosts
- Understanding Cluster Shared Volume Protection
- Configuring Self-Service Recovery for End Users

Considerations for Configuring Protection Groups

Consider the following when configuring your protection groups:

- You can include more than one computer in a protection group
- All protection group members of the same type share the same recovery point settings
- A protection group that includes application and file data sources has separate recovery settings for each
- The retention range is configured for all data sources in a protection group
- On-the-wire compression is set for each protection group
- You cannot move data sources between protection groups
- Consistency check settings are shared for all data sources in a protection group
**Configuring SQL Server Protection**

**To protect SQL Server you must:**

1. Choose the SQL Server instances or databases to protect
2. Configure the length of time to retain backup data
3. Configure the synchronization frequency
4. Set the schedule for creating express full backups

---

**Options for Protecting the Cloud**

**In guest protection**
- Windows Server 2008 R2 and newer

**Hyper-V Online Backup**
- Windows Server 2008 R2 and newer

**Cluster Backup**
- Servers in a cluster such as Hyper-V servers with CSV
Configuring Item-Level Recovery for Cloud-Based Hosts

Understanding Cluster Shared Volume Protection

**Standard CSV backup:**
1. The virtual machine backup that is stored on a CSV sets the CSV to redirected I/O mode until the backup completes
2. All storage I/O for the CSV disk then transfers over the network to the server that owns the CSV disk

**Hardware-based snapshots:**
1. The virtual machine backup that is stored on a CSV sets the CSV to redirected I/O mode, while the storage hardware creates the snapshot
2. CSV returns to normal I/O mode
3. Hardware-based snapshot is used to create a DPM replica DPM releases hardware snapshot
Configuring Self-Service Recovery for End Users

To configure self-service recovery, do the following:

1. Create a recovery role and assign Active Directory groups to the role
2. Specify the SQL Server instance from which users can recover data
3. Specify to where the users in the role can recover data

Lesson 7: Restoring Applications to the Cloud

- Recovering SQL Server Data
- Performing Self-Service SQL Server Data Recovery
- Performing Virtual Machine Recovery
- Performing Item-Level Recovery on Hyper-V Virtual Machines
Recovering SQL Server Data

With DPM, you can:

- Recover data to the original location
- Recover data to the original location with a different name
- Recover data to a different SQL Server instance
- Recover data to a network folder
- Recover data to tape media
- Recover data and apply additional log backups

Performing Self-Service SQL Server Data Recovery

To configure self-service recovery, do the following:

1. Start the DPM Self Service Recovery tool
2. Connect to the DPM server
3. Create a new recovery job
4. Select the SQL Server and database you want to recover
5. Select the recovery point
6. Select to recover to SQL Server database or to a network folder
7. Select the recovery location
Performing Virtual Machine Recovery

**When performing a VHD recovery, you can:**

- Recover data to the original location
- Recover data as a virtual machine to any host
- Copy the data to a network folder

Performing Item-Level Recovery on Hyper-V Virtual Machines

**To perform ILR, do the following:**

1. Select the recovery point
2. Select the virtual machine from which you want to restore an item
3. Select the VHD that contains the item that you want to recover
4. Select the folders or files that you want to recover
5. Start the Recovery Wizard
6. Select the network location
Lab: Protecting the Private Cloud Infrastructure

- Exercise 1: Configuring the Storage Pool
- Exercise 2: Deploying DPM Protection Agents
- Exercise 3: Creating and Configuring Protection Groups
- Exercise 4: Configuring SQL Server Self-Service Recovery
- Exercise 5: Restoring Data from a SQL Server Protection Group
- Exercise 6: Performing Self-Service Recovery of SQL Server Data

Logon Information

Virtual Machines: 20247D-LON-DC1, 20247D-LON-SQ1, 20247D-LON-DM1, 20247D-LON-AP1, 20247D-LON-AP2, 20247D-LON-OR1
User Name: Contoso\Administrator
Password: Pa$$w0rd

Estimated Time: 45 minutes
Lab Scenario

You are the administrator at Contoso, Ltd. You have just deployed DPM, and now you want to perform basic configuration and testing. Critical to the success of your private cloud initiative is the ability to recover quickly from data loss. Furthermore, management has mandated that all data must be restored to within 15 minutes of the last transaction. Additionally, the SQL Server teams must be able to recover SQL Server databases themselves from any SQL Server, and without having to interact with the data center management team.

Lab Review

• Are you required to create two separate protection groups to protect both the Hyper-V and SQL Server computers?
• What is an RPO?
<table>
<thead>
<tr>
<th>Module Review and Takeaways</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Review Question(s)</td>
</tr>
<tr>
<td>• Real-world Issues and Scenarios</td>
</tr>
<tr>
<td>• Common Issues and Troubleshooting Tips</td>
</tr>
</tbody>
</table>