Module Overview

• Data Protection Overview
• Implementing Windows Server Backup
• Implementing Server and Data Recovery
Lesson 1: Data Protection Overview

• Identifying Recovery Requirements
• What Are Service Level Agreements?
• Overview of Enterprise Data Protection Strategies
• Mitigation Strategies
• Best Practices When Implementing a Data Protection Strategy
Identifying Recovery Requirements

Identify your data protection options by:

1. Defining organization critical resources
2. Identifying risks associated with those critical resources
3. Identifying the time needed to complete the recovery
4. Developing a protection strategy
What Are Service Level Agreements?

SLAs define responsibilities of the service provider

SLA components include:

- Hours of operation
- Service availability
- RPO and RTO
- Retention objectives
- System performance
You need strategies for recovering:

- Data
- Services
- Servers
- Sites
- Offsite backups
## Mitigation Strategies

<table>
<thead>
<tr>
<th>Problem</th>
<th>Mitigation strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>The media where a copy of the backup data is stored becomes corrupted</td>
<td>Have at least two copies of your backup data</td>
</tr>
<tr>
<td>An administrator has accidentally deleted an OU that contains many user and computer objects</td>
<td>Protect OUs from accidental deletion, especially after migrations</td>
</tr>
<tr>
<td>A server in a branch office where important files are located has failed</td>
<td>Use DFS Replication to replicate files from branch offices to central data centers</td>
</tr>
<tr>
<td>The virtualization infrastructure where business servers are located is unavailable</td>
<td>Avoid deploying all critical servers, such as domain controllers, on the same virtual infrastructure</td>
</tr>
<tr>
<td>A major outage in a data center has occurred</td>
<td>Deploy a secondary data center that will contain replicas of most of the critical servers in your primary data center</td>
</tr>
</tbody>
</table>
Best Practices When Implementing a Data Protection Strategy

To implement a data protection strategy, you should:

• Perform a risk assessment plan

• Discuss the risks you evaluated with your business managers, and create a data protection strategy and disaster mitigation strategy

• Ensure that each organization has its own data protection plan

• Document all steps that should be performed in a recovery scenario

• Test your recovery plan on regular basis, in an isolated, non-production environment.

• Evaluate your data protection strategy on a regular basis, and update your data protection strategy depending on your evaluation outcome
Lesson 2: Implementing Windows Server Backup

- Planning a Backup Strategy
- What Is Windows Server Backup?
- Backup Types
- Backup Technologies
- Planning Backup Capacity
- Planning Backup Security
- Demonstration: Configuring a Scheduled Backup
- What Is Windows Azure Backup?
- Considerations for an Enterprise Backup Solution
- What Is Data Protection Manager?
Planning a Backup Strategy

When planning your backup strategy, ensure that you:

- Determine the critical resources
- Verify your backups
- Confirm that backups are secure
- Ensure that compliance and regulatory responsibilities are met
What Is Windows Server Backup?

You can use Windows Server Backup to:

- Back up full server (all volumes)
- Back up selected volumes
- Back up selected items
- Perform a bare-metal recovery
- Perform a system state
- Back up individual files and folders
- Exclude selected files or file types during backup
- Select from more storage locations for the backup
Backup Types

• A full backup is a block-level replica of all blocks on all the server’s volumes.

• An incremental backup is a copy of only those blocks that have changed since the last full or incremental backup.
Backup Technologies

• The VSS backup technology solves data consistency issues by creating shadow copies.

• You can also use streaming backups for older applications that are not VSS-aware.

• Hyper-V replica provides you with a disaster recovery option by replicating a consistent copy of a virtual machine to another server or site.
Planning Backup Capacity

When planning for backup capacity, consider the following:

• Space requirements for a full backup
• Space requirements for an incremental backup
• Amount of time required to back up
• Backup frequency
• Backup retention
Planning Backup Security

When planning your backup security, consider the following:

• Backups contain all organizational data
• Access to backup media means access to all data
• Windows Server Backup does not encrypt backups
• Keep backup media in a secure location
Demonstration: Configuring a Scheduled Backup

In this demonstration, you will see how to configure Windows Server Backup to perform a scheduled backup of specific folders that includes a filter to exclude specific file types.
What Is Windows Azure Backup?

Windows Azure Backup features include:

- Simple configuration and management
- Block-level incremental backups
- Data compression, encryption, and throttling
- Data integrity verified in the cloud
- Configurable retention policies for storing data in the cloud
Considerations for an enterprise backup solution are:

- What is the theoretical RPO of the product?
- How quick is RTO recovery?
- Does the solution provide centralized backup?
- Is the solution supported by vendors?
- What is the recovery point capacity?
What Is Data Protection Manager?

DPM:

- Allows you to centralize backups
- Offers 15-minute snapshots of servers and clients
- Can store backup data on SANs and export to tape
- Can back up remote sites
- Can be used as part of a backup-to-cloud strategy
- Supports Microsoft products
Lesson 3: Implementing Server and Data Recovery

- Options for Server Recovery
- Options for Server Restore with Windows RE
- Options for Data Recovery
- Demonstration: Using Windows Server Backup to Restore a Folder
- Restoring with Windows Azure Backup
Options for Server Recovery

The options for server recovery include:

- Files and folders
- Applications and data
- Volumes
- Operating system
- Full server
- System state
- BCDEdit allows you to edit the BCD Store to modify boot options
- Safe mode boots computer with minimal services and drivers
- Last Known Good configuration is the most recent set of driver and registry settings from a successful startup
Options for Server Restore with Windows RE

- Windows RE allows you to recover server images or volumes from local disk or network share

You can enter Windows RE when:

- You boot from install media
- You press F8
- Successive boot failures or unexpected shutdowns occur
Options for Data Recovery

The four options for recovering data include:

- Allowing users to recover their own data
- Recovering data to an alternate location
- Recovering data to the original location
- Performing a full volume recovery
Demonstration: Using Windows Server Backup to Restore a Folder

In this demonstration, you will see how to use the Recovery Wizard to restore a folder.
When restoring files by using Windows Azure Online Backup, perform the following steps:

1. Select the server
2. Locate the files you want to recover from backup
3. Choose the restore location
4. Select an option for copy creation
Lab: Implementing Windows Server Backup and Restore

• Exercise 1: Backing Up Data on a Windows Server 2012 R2 Server
• Exercise 2: Restoring Files Using Windows Server Backup

Logon Information
Virtual machines: 20412D-LON-DC1, 20412D-LON-SVR1
User name: Adatum\Administrator
Password: Pa$$w0rd

Estimated Time: 60 minutes
Much of the data that is stored on the A. Datum Corporation’s network is extremely valuable to the organization. Losing this data would be a significant loss to the organization. Additionally, many of the servers that are running on the network provide extremely valuable services for the organization, which means that losing these servers for a significant time would also result in losses to the organization. Because of the significance of the data and services, it is critical that they can be restored in the event of disaster.
Lab Scenario

A. Datum is considering backing up critical data to a cloud-based service. A. Datum also is considering this as an option for small branch offices that do not have a full datacenter infrastructure.

As one of the senior network administrators at A. Datum, you are responsible for planning and implementing a data-protection solution that will ensure that critical data and services can be recovered in the event of any type of failure. You need to implement a backup-and-restore process that can recover lost data and services.
• You are concerned about business-critical data that is located on your company's servers. You want to perform backups every day, but not during business hours. What should you do?
• Users report that they can no longer access data that is located on the server. You connect to the server, and you realize that the shared folder where users were accessing data is missing. What should you do?
Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips