

Module 8

Planning and implementing backup
and disaster recovery

Module Overview

- Planning for and implementing Azure Backup
- Overview of Azure Site Recovery
- Planning for Site Recovery
- Implementing Site Recovery with Azure as the disaster recovery site

Lesson 1: Planning for and implementing Azure Backup

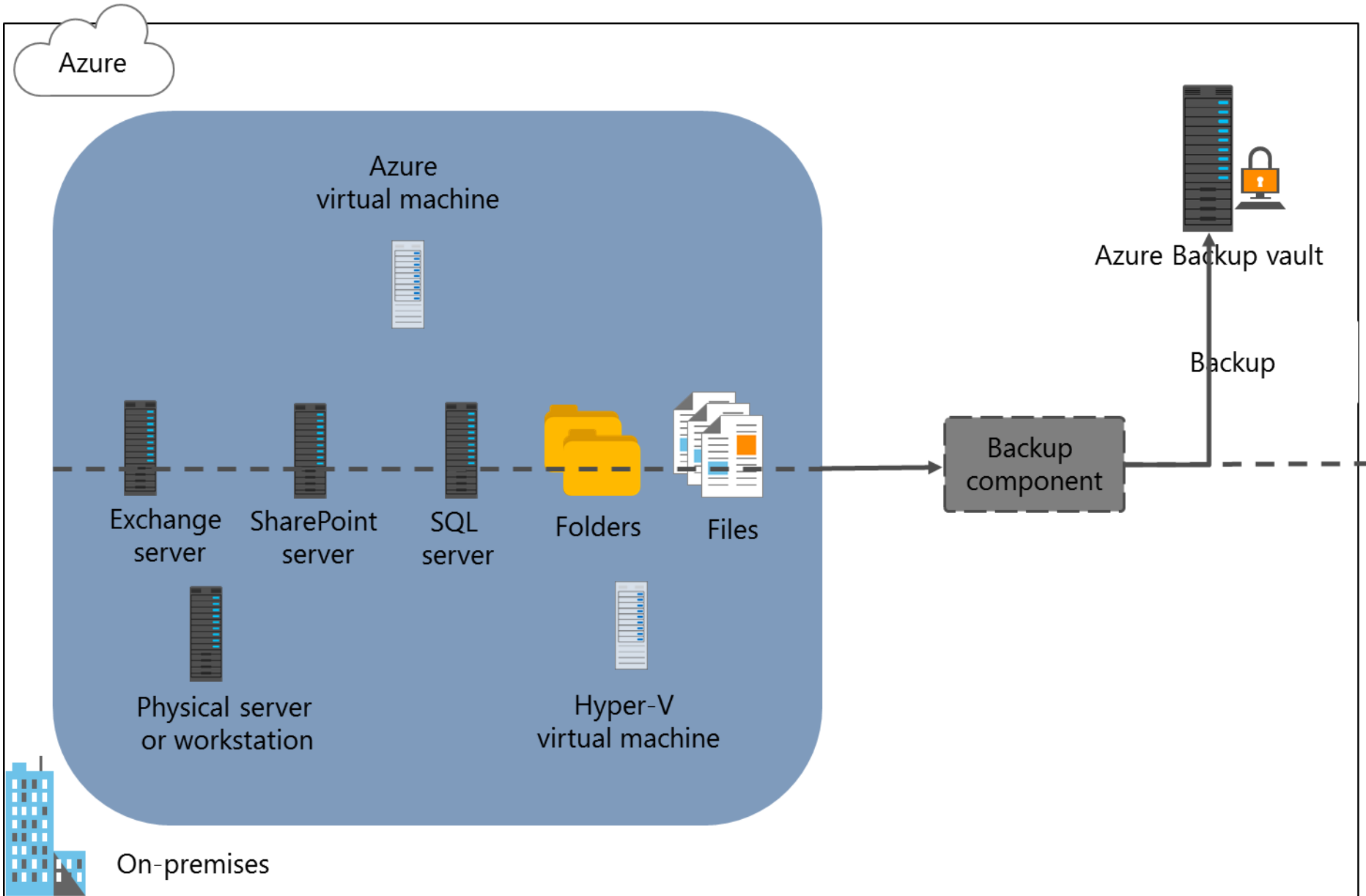
- Demonstration: Preparing the lab environment
- Overview of Azure Backup
- File, folder, and system state backups with the Recovery Services Agent
- Azure VM-level backup by using Azure VM extensions
- Integrating Azure Backup with Data Protection Manager and Microsoft Azure Backup Server
- Demonstration: Implementing and using Azure VM backups

Demonstration: Preparing the lab environment

In this demonstration, you will learn how to prepare the lab environment

Note: To prepare the lab environment for this module, you must complete this task

Overview of Azure Backup



File, folder, and system state backups with the Recovery Services Agent

1. Create an Azure Backup vault
2. Configure vault replication type
3. Specify the backup goal
 - Location of the workload: On-premises
 - The workload type: Files and folders or System state
4. Download the vault credentials
5. Download the Recovery Services Agent
6. Install the Recovery Services Agent
7. Register local computer with the vault and set a passphrase
8. Configure the initial backup type, choose files and folders to back up, and create a backup schedule

Azure VM-level backup by using Azure VM extensions

1. Create an Azure Backup vault
2. Configure vault replication type
3. Specify the backup goal
 - Location of the workload: Azure
 - The workload type: Virtual machine
4. Choose the backup policy
5. Specify the virtual machines to back up

Integrating Azure Backup with Data Protection Manager and Microsoft Azure Backup Server

Feature	System Center 2016 DPM	Azure Backup Server
Application workloads	Yes	Yes
Tape backup	Yes	No
Integration with System Center suite	Yes	No
System Center licensing required	Yes	No
Deduplication support	Yes	Yes

Demonstration: Implementing and using Azure VM backups

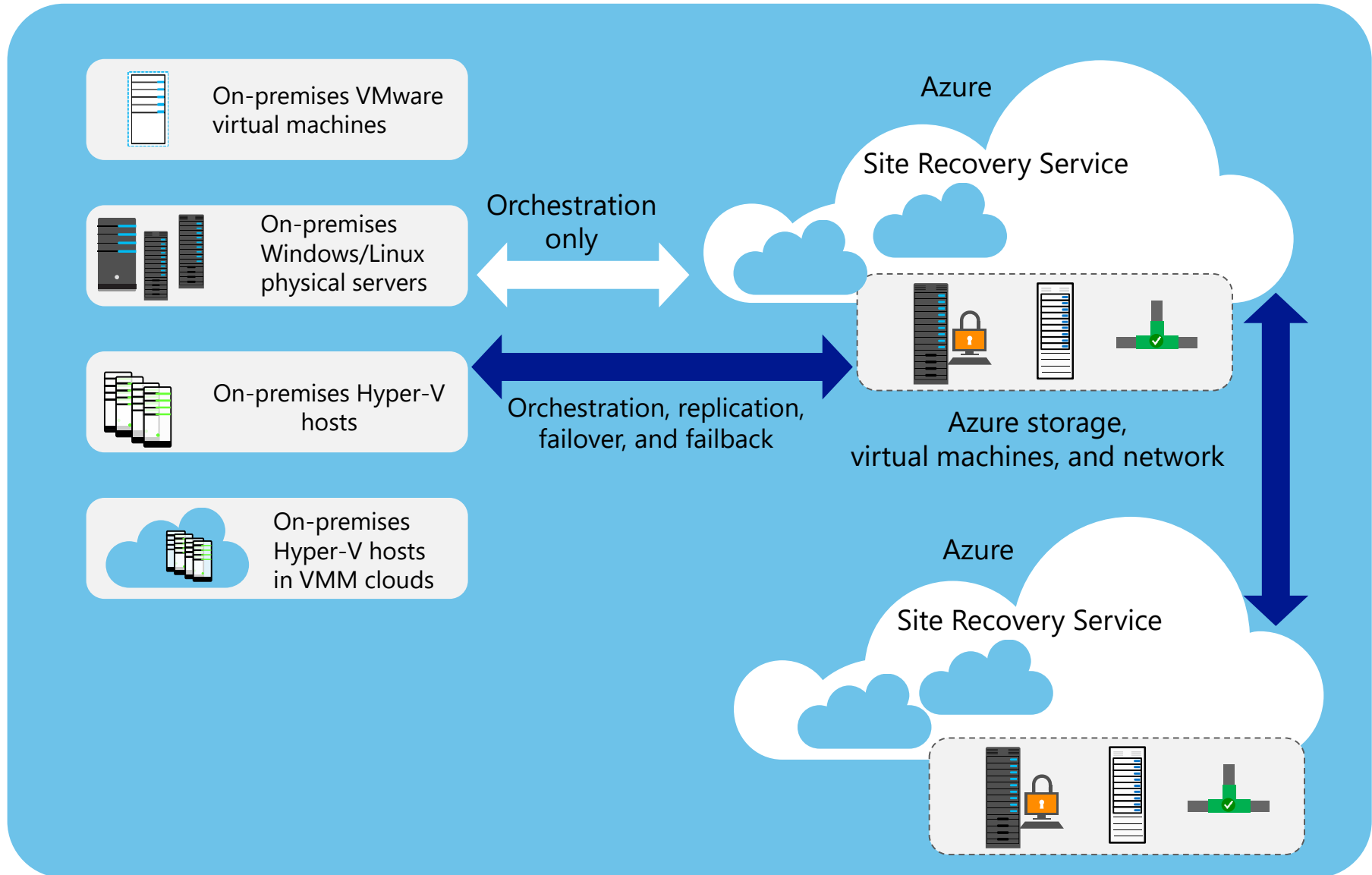
In this demonstration, you will see how to:

- Create an Azure Recovery Services vault
- Create a custom backup policy
- Register an Azure VM in the Recovery Services vault
- Restore an individual file

Lesson 2: Overview of Azure Site Recovery

- Overview of Site Recovery scenarios
- Site Recovery capabilities
- Site Recovery components: Hyper-V to Azure
- Site Recovery components: VMM to Azure
- Site Recovery components: VMware and physical servers to Azure
- Site Recovery components: Azure to Azure

Overview of Site Recovery scenarios

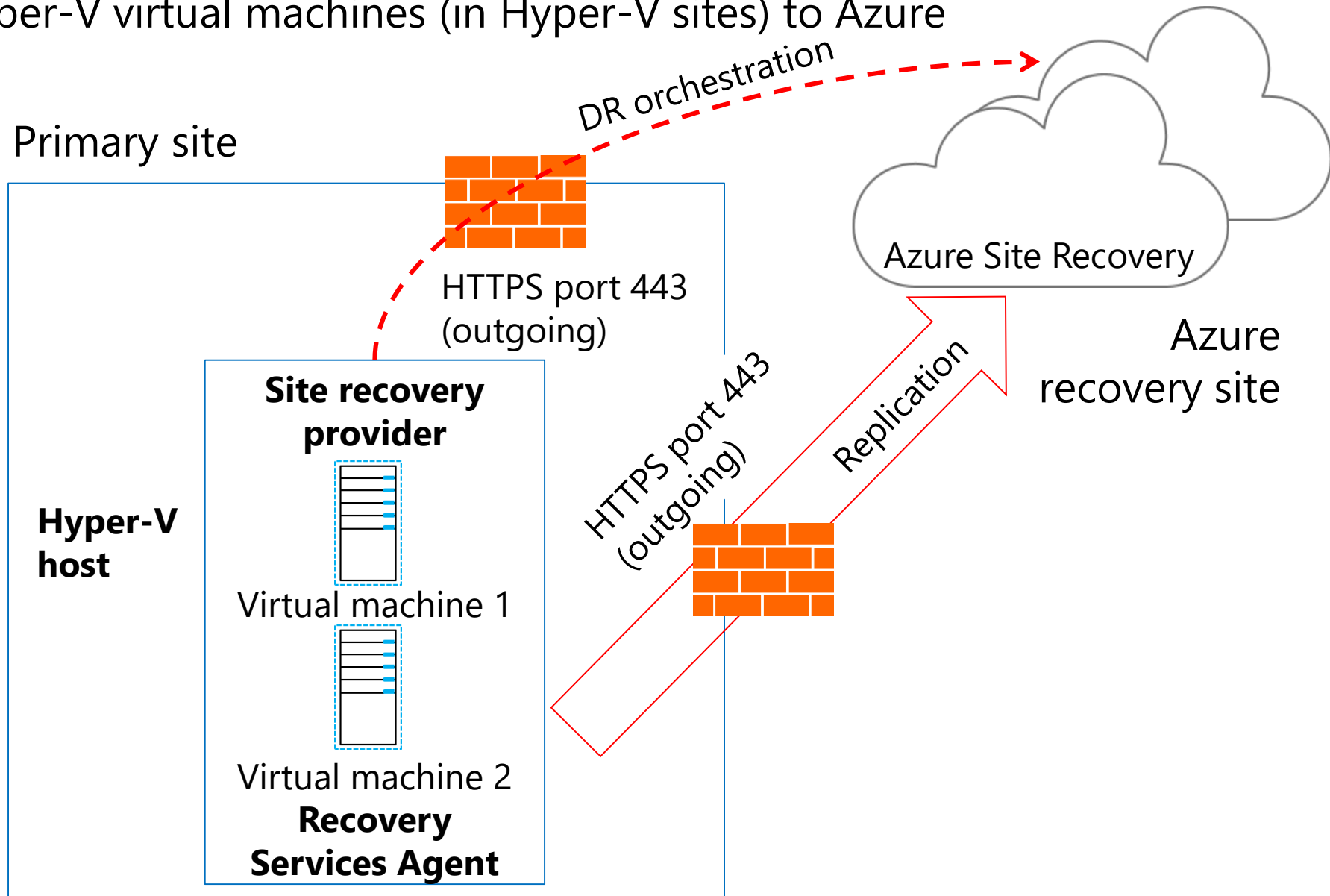


Site Recovery capabilities

- Storage or application-level replication
- Planned failover and failback
- Unplanned failover and failback
- Test failover
- Supported workloads include:
 - AD DS and DNS
 - IIS and SQL (including AlwaysOn and failover cluster instances)
 - System Center Operations Manager
 - SharePoint Server
 - SAP
 - Exchange Server
 - Remote Desktop (VDI)
 - Dynamics AX and CRM
 - Oracle

Site Recovery components: Hyper-V to Azure

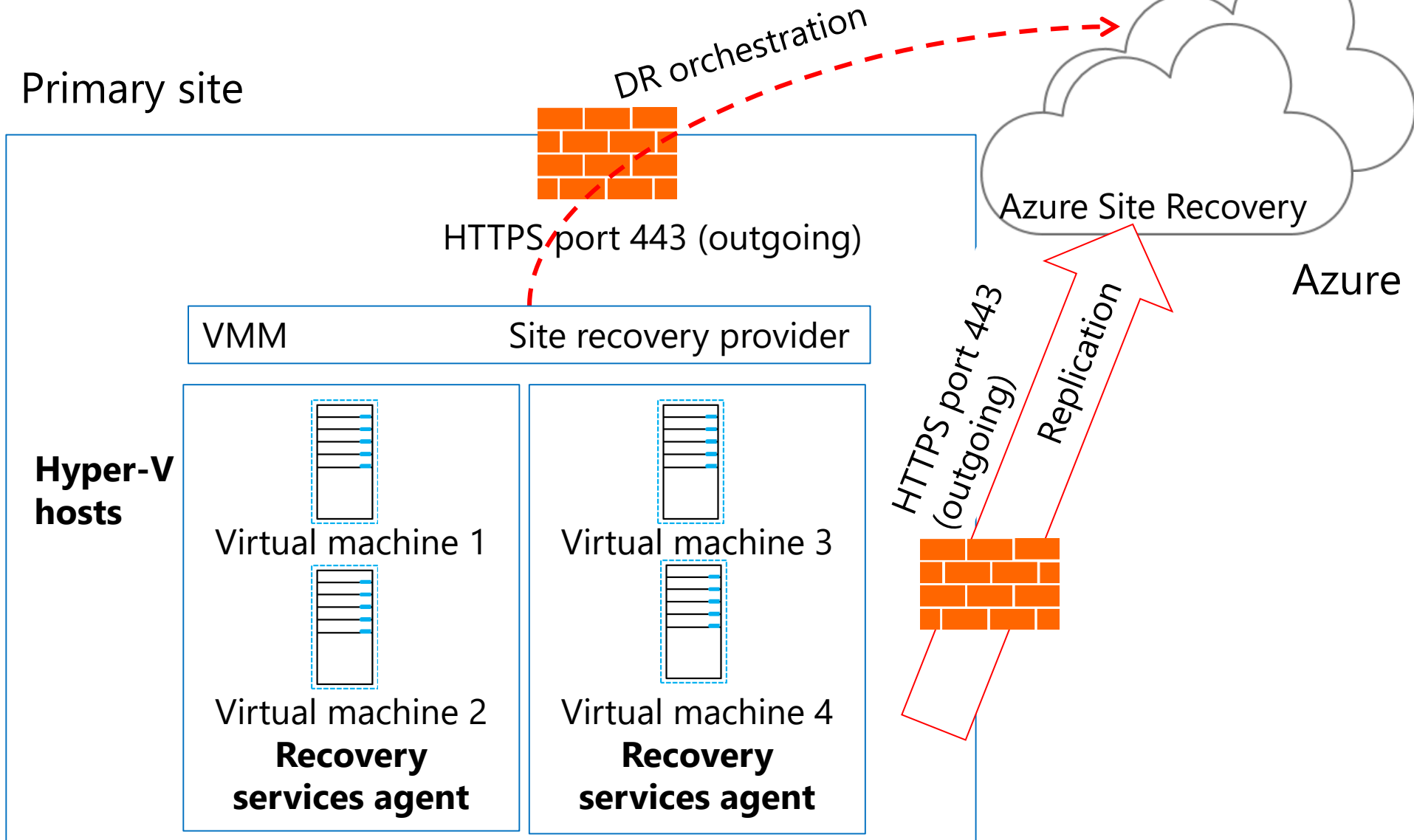
Hyper-V virtual machines (in Hyper-V sites) to Azure



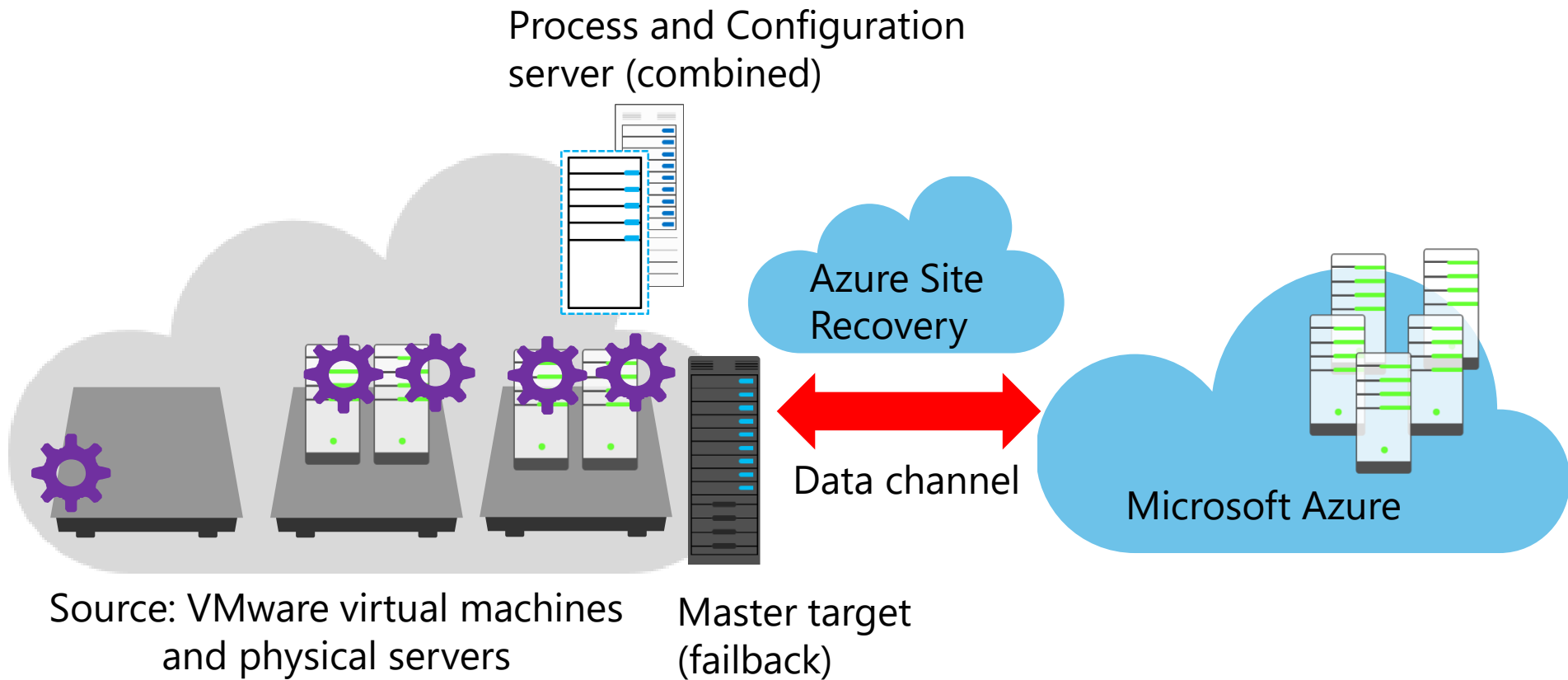
Site Recovery components: VMM to Azure


Hyper-V virtual machines (in VMM clouds) to Azure


Primary site





Site Recovery components: VMware and physical servers to Azure



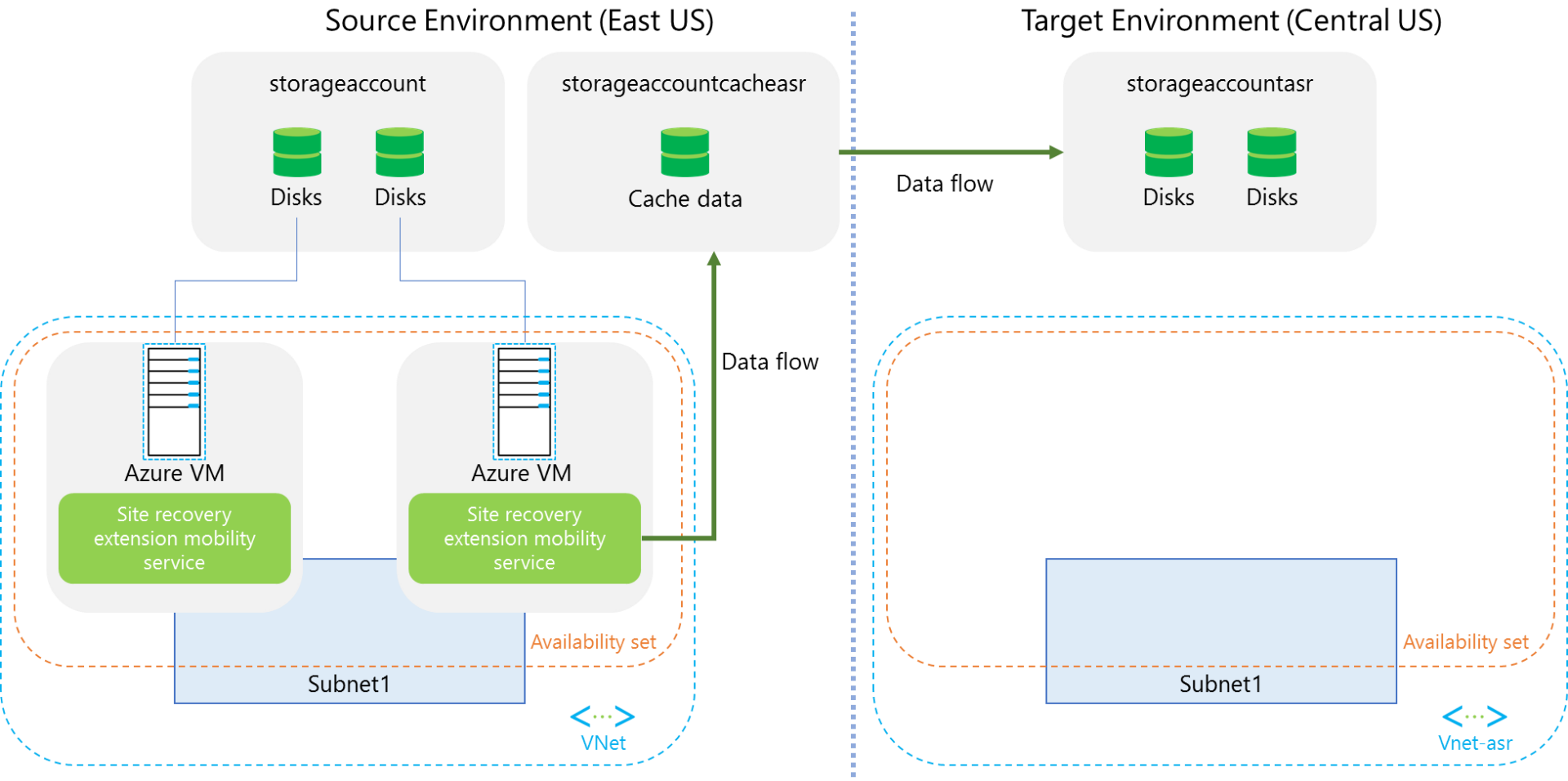
 Process server:
Used for caching,
compression, and
encryption

 Configuration
server: Used for
centralized
management

 Mobility service:
Captures all data
writes from
memory

 Master target:
Used for
failback only

Site Recovery components: Azure to Azure



Lesson 3: Planning for Site Recovery

- Primary considerations in planning for cross-premises Site Recovery deployments
- Additional considerations when configuring Azure-based protection of Hyper-V virtual machines
- Additional considerations when configuring Azure-based protection of Hyper-V VMs in VMM clouds
- Additional considerations when configuring Azure-based protection of VMware VMs and physical servers
- Additional considerations when configuring Azure-based protection of Azure VMs

Primary considerations in planning for cross-premises Site Recovery deployments

- Location of the recovery site:
 - On-premises
 - Azure
- Proximity to the primary site:
 - Not too close: Consider impact of a regional disaster
 - Not too far: Consider network latency
- On-premises servers:
 - Microsoft Hyper-V VMs (with or without VMM)
 - VMware VMs (vCenter 5.5, 6.0, or 6.5)
 - Physical servers (Windows and Linux)



Primary considerations in planning for cross-premises Site Recovery deployments

Deployment planner for Hyper-V and VMware replication to Azure:

- Functionality:
 - Compatibility assessment
 - Cross-premises network bandwidth assessment
 - Azure infrastructure requirements
 - On-premises infrastructure requirements
 - Initial replication guidance
 - Estimated infrastructure and licensing costs
- Modes of operation:
 - Profiling
 - Report generation
 - Bandwidth requirements analysis



Primary considerations in planning for cross-premises Site Recovery deployments

Azure virtual machine-related requirements:

- Operating system must be supported by Azure
- OS disk sizes:
 - Hyper-V Gen1 VMs, VMware VMs, physical servers – up to 2 TB
 - Hyper-V Gen2 VMs – up to 300 GB
- Data disk sizes:
 - Up to 4 TB
- Disk count:
 - Hyper-V VMs – up to 16
 - VMware VMs – up to 64
- Disk type cannot be:
 - iSCSI
 - Fibre Channel Shared virtual hard disks



Primary considerations in planning for cross-premises Site Recovery deployments

Network-related requirements:

- IP address space:
 - The same as on-premises:
 - Pro: No need for DNS changes following a failover
 - Con: No support for S2S VPN/ExpressRoute during normal operations
 - Different from on-premises:
 - Pro: Support for S2S VPN/ExpressRoute during normal operations
 - Con: DNS changes following a failover are required
 - Consider lowering DNS TTL
- Cross-premises connectivity:
 - P2S: Test failover only
 - S2S: Planned/unplanned failover
 - ExpressRoute: Planned/unplanned failover + replication traffic



Additional considerations when configuring Azure-based protection of Hyper-V virtual machines

- Outbound connectivity:
 - Must allow TCP 443 to access the following Azure URLs from Hyper-V hosts:
 - *.accesscontrol.windows.net
 - login.microsoftonline.com
 - *.backup.windowsazure.com
 - *.blob.core.windows.net
 - *.hypervrecoverymanager.windowsazure.com
 - time.nist.gov
 - time.windows.net
- Replication bandwidth of Hyper-V hosts:
 - Can be controlled via Azure Backup throttling
 - Can be controlled via registry (number of upload/download threads)

Additional considerations when configuring Azure-based protection of Hyper-V VMs in VMM clouds

- VMM configuration:
 - Include virtual machine networks (to map to Azure virtual networks)
- Outbound connectivity:
 - Allow TCP 443 to access the following Azure URLs from VMM server and Hyper-V hosts:
 - *.accesscontrol.windows.net
 - login.microsoftonline.com
 - *.backup.windowsazure.com
 - *.blob.core.windows.net
 - *.hypervrecoverymanager.windowsazure.com
 - time.nist.gov
 - time.windows.net
- Replication bandwidth of Hyper-V hosts:
 - Control via Azure Backup throttling
 - Control via registry (number of upload/download threads)

Additional considerations when configuring Azure-based protection of VMware VMs and physical servers

- VMware components:
 - Use vCenter 6.5, 6.0, or 5.5
- Outbound connectivity:
 - Must allow TCP 443/9443 to the following Azure URLs from the configuration server:
 - *.accesscontrol.windows.net
 - login.microsoftonline.com
 - *.backup.windowsazure.com
 - *.blob.core.windows.net
 - *.hypervrecoverymanager.windowsazure.com
 - time.nist.gov
 - time.windows.net
- Replication bandwidth of the process server:
 - Can be controlled via Azure Backup throttling
 - Can be controlled via registry (number of upload/download threads)

Additional considerations when configuring Azure-based protection of Azure VMs

- Outbound connectivity:
 - Allow TCP 443 to access the following Azure URLs from Azure VMs:
 - *.hypervrecoverymanager.windowsazure.com
 - *.blob.core.windows.net
 - login.microsoftonline.com
 - *.servicebus.windows.net
- The latest trusted root certificates
- Delegated permissions via RBAC:
 - Site Recovery Contributor
 - Site Recovery Operator
 - Site Recovery Reader

Lesson 4: Implementing Site Recovery with Azure as the disaster recovery site

- Implementing Azure-based protection of Hyper-V virtual machines without VMM
- Implementing Azure-based protection of Hyper-V virtual machines located in VMM clouds
- Implementing Azure-based protection of VMware virtual machines and physical servers
- Implementing Azure-based protection of Azure VMs
- Managing and automating Site Recovery
- Demonstration: Replicate an Azure VM to another Azure region

Implementing Azure-based protection of Hyper-V virtual machines without VMM

1. Create an Azure virtual network
2. Create one or more Azure storage accounts
3. Create a Recovery Services vault
4. Prepare mapping on-premises virtual machine networks to Azure virtual networks
5. Specify the protection goal
6. Set up the source environment
7. Set up the target environment
8. Set up replication settings
9. Select virtual machines to protect and enable their replication

Implementing Azure-based protection of Hyper-V virtual machines located in VMM clouds

1. Create one or more Azure virtual networks
2. Create one or more Azure storage accounts
3. Create a Recovery Services vault
4. Prepare for network mapping
5. Specify the protection goal
6. Set up the source environment
7. Set up the target environment
8. Set up replication settings
9. Select the VMM cloud and enable its replication

Implementing Azure-based protection of VMware virtual machines and physical servers

1. Create an Azure virtual network
2. Create one or more Azure storage accounts
3. Set up a user account on the vSphere host or vCenter server for automatic discovery of VMware VMs
4. Prepare the configuration server
5. Create a Recovery Services vault
6. Specify the protection goal
7. Set up the source environment
8. Set up the target environment
9. Set up replication settings
10. Select the VMware VMs to protect and enable their replication

Implementing Azure-based protection of Azure VMs

1. Create an Azure virtual network in the disaster recovery region
2. Create an Azure storage account in the disaster recovery region
3. Create an Azure storage account in the local region
4. Create a Recovery Services vault in the disaster recovery region
5. Specify the protection goal
6. Set up the source environment
7. Select Azure VMs to protect
8. Set up replication settings and enable replication

Managing and automating Site Recovery

- Failover
 - Test failover
 - Use an isolated Azure virtual network
 - Keep the protected virtual machine online—no production impact
 - Planned failover
 - Use an Azure virtual network mapped to the production network
 - Shut down the protected virtual machine—no data loss
 - Unplanned failover
 - Use an Azure virtual network mapped to the production network
 - Attempt to shut down the protected virtual machine—potential data loss
- Failback
 - Establish reverse replication
 - Use planned failover in the opposite direction



Managing and automating Site Recovery

- Recovery plans:
 - Orchestrate failover and failback
 - Can contain:
 - Recovery groups (collections for protected VMs)
 - Manual actions
 - Azure Automation runbooks
- Azure Automation runbooks:
 - Provision and configure additional Azure resources
 - Use the recovery context variable and its attributes:
 - *RecoveryPlanName*
 - *FailoverType*
 - *FailoverDirection*
 - *GroupID*
 - *VmMap*



Demonstration: Replicate an Azure VM to another Azure region

In this demonstration, you will see how to:

- Replicate an Azure VM to another Azure region
- Disable replication

Lab: Implementing Azure Backup and Azure Site Recovery

- Exercise 1: Protecting data with Azure Backup
- Exercise 2: Implementing protection of Azure VMs by using Site Recovery

Logon Information

Virtual machine: **20533E-MIA-CL1**

User name: **Student**

Password: **Pa55w.rd**

Estimated Time: 60 minutes

Lab Scenario

Adatum wants to evaluate the ability of Azure Backup to protect the content of on-premises computers and Azure IaaS virtual machines.

A. Datum Corporation also wants to evaluate Azure Site Recovery for protecting Azure VMs.

Lab Review

- Why did the lab not include failover and failback?
- If you wanted to protect Azure VMs that reside behind an Azure load balancer, how would you configure your Site Recovery solution?

Module Review and Takeaways

- Common Issues and Troubleshooting Tips
- Review Question