Microsoft

AZ-801

Configure Windows Server Hybrid Advanced Services

Agenda AZ-801

1 Security – Windows Server
2 Security – Hybrid

3 Failover Cluster

4 Disaster Recovery – Windows Server
5 Disaster Recovery – Hybrid

6 Upgrade and Migrate – Windows Server
7 Migrate Windows Server to the Cloud

8 Monitoring – Windows Server
9 Monitoring – Hybrid

Implement Disaster Recovery in Windows Server on-premises and Hybrid Environments

(Implementing Disaster Recovery Services in Hybrid Scenarios)

- Implement hybrid backup and recovery with Windows Server IaaS
- Protect your Azure infrastructure with Azure Site Recovery ✓
- Protect your virtual machines by using Azure Backup ✓
- Lab 05 – Implementing Azure-based recovery services

MARS - Agent
Windows only

Implement hybrid backup and recovery with Windows Server IaaS

Learning Objectives – Hybrid backup and recovery

- Describe Azure Backup
- Implement Recovery Service vaults
- Implement Azure Backup policies
- Recover Windows IaaS Virtual Machines
- Perform file and folder recovery
- Perform backup and restore of on-premises workloads
- Demonstration – Manage Azure virtual machine backups with Azure Backup service
- Learning recap

Describe Azure Backup

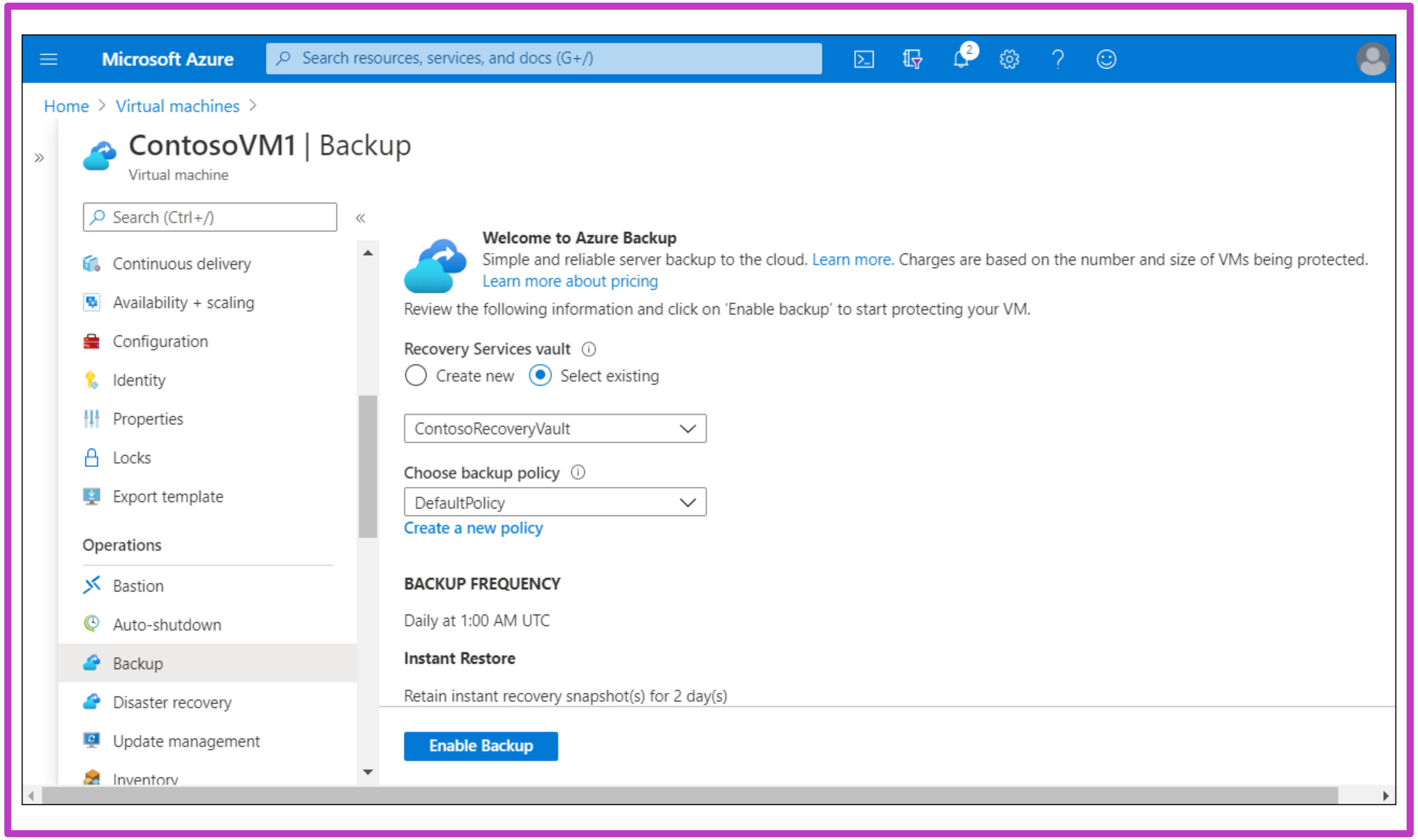
1. Uses Azure resources for short-term and long-term storage to minimize or even eliminate the need for maintaining physical backup media
2. Delivers benefits including: automatic storage management, unlimited scaling, unlimited data transfer, data encryption, and long-term retention
3. Includes the following backup types: on-premises, Azure VMs, Azure Files shares, Microsoft SQL Server, SAP HANA databases in Azure VMs and Microsoft cloud
4. Includes the following security features: Prevention, alerting and recovery

backup vault

Implement recovery service vaults for backup

A Recovery Services vault:

- Makes it easier to organize your backup data, while minimizing management overhead
- Supports DPM, Windows Server, Azure Backup Server, and others



Welcome to Azure Backup

Simple and reliable server backup to the cloud. Learn more. Charges are based on the number and size of VMs being protected.

Learn more about pricing

Review the following information and click on 'Enable backup' to start protecting your VM.

Recovery Services vault

○ Create new ● Select existing

ContosoRecoveryVault

Choose backup policy

DefaultPolicy

Create a new policy

BACKUP FREQUENCY

Daily at 1:00 AM UTC

Instant Restore

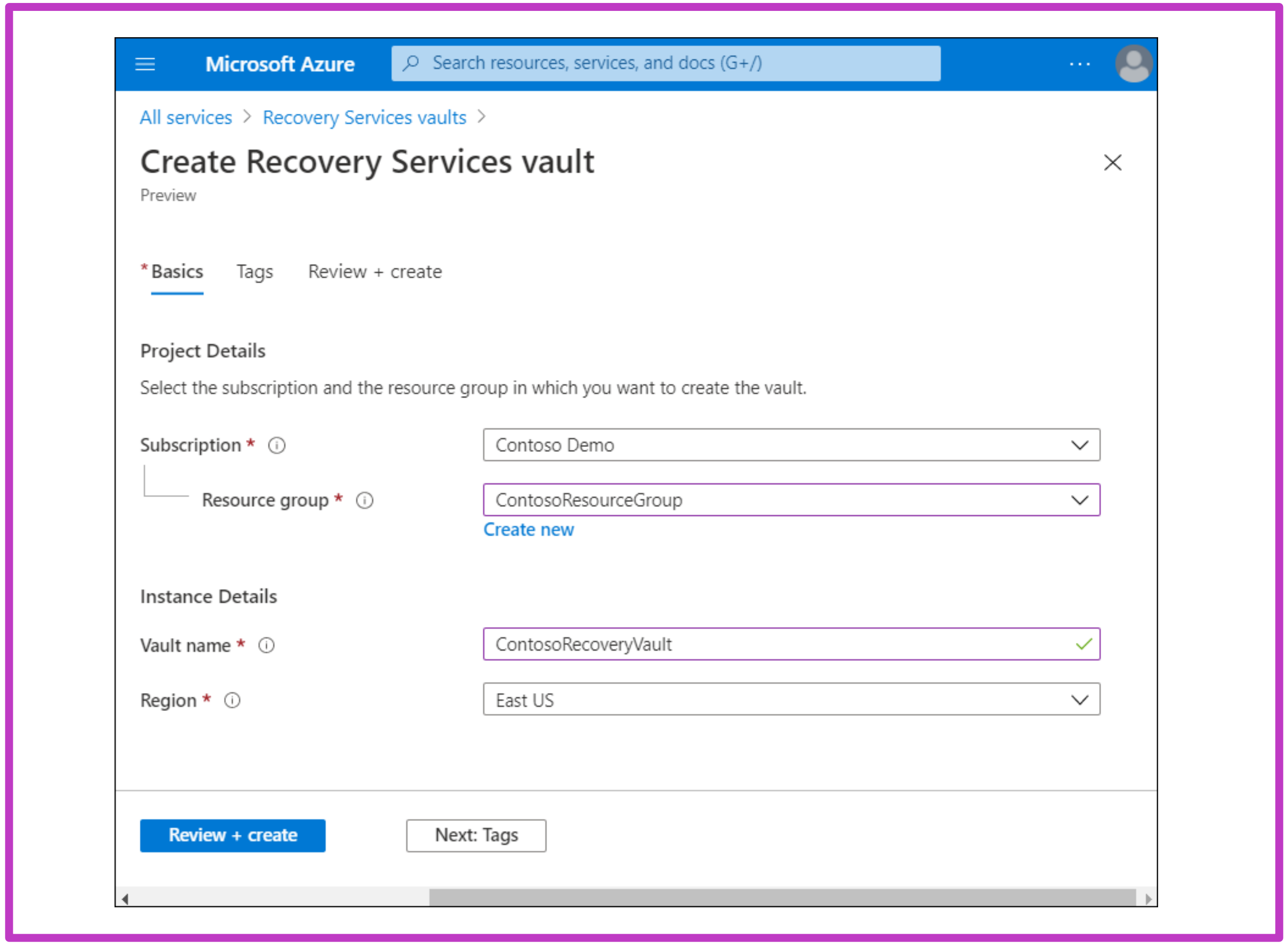
Retain instant recovery snapshot(s) for 2 day(s)

Enable Backup

Implement recovery vault for backup

To create a Recovery Services vault:

1. Sign in to your subscription in the Azure portal.
2. In the navigation pane, select **All services.**
3. In the All services dialog box, enter Recovery Services.
4. From the list of resources, select **Recovery Services vaults.**
5. On the Recovery Services vaults dashboard, select **Create**.
6. Define the subscription, resource group, specify a vault name, and choose the appropriate region, then select **Review + create.**


Microsoft Azure
Search resources, services, and docs (G+/)
All services > Recovery Services vaults >

Create Recovery Services vault

Preview

*Basics
Tags
Review + create

Project Details

Select the subscription and the resource group in which you want to create the vault.

Subscription * : Contoso Demo

Resource group * : ContosoResourceGroup

Instance Details

Vault name * : ContosoRecoveryVault

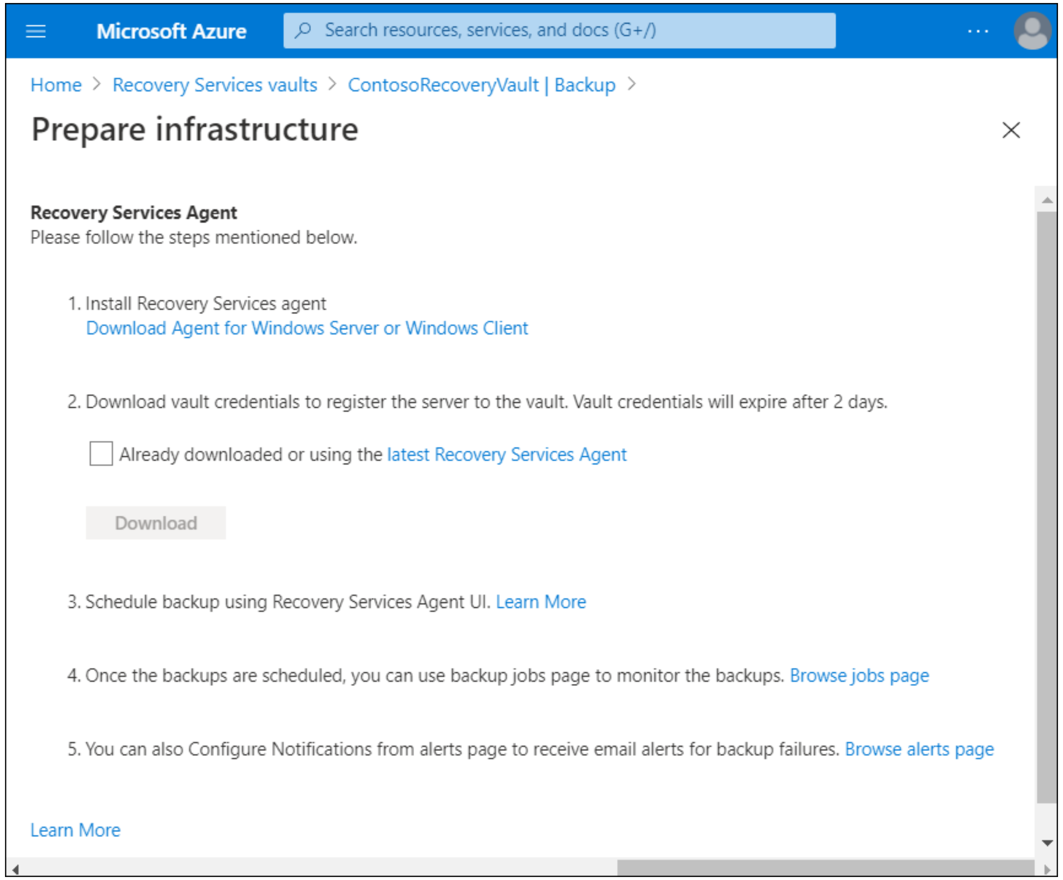
Region * : East US

Review + create
Next: Tags

Implement Azure Backup Policies

What is the MARS agent?

- Azure Backup uses the MARS agent to back up files, folders, and system state from on-premises machines and Azure VMs.
- These machines can back up directly to a Recovery Services vault in Azure.
- You can also back up Azure VMs that run Windows side by side with the Azure VM backup extension.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Recovery Services vaults > ContosoRecoveryVault | Backup >

Prepare infrastructure

Recovery Services Agent

Please follow the steps mentioned below.

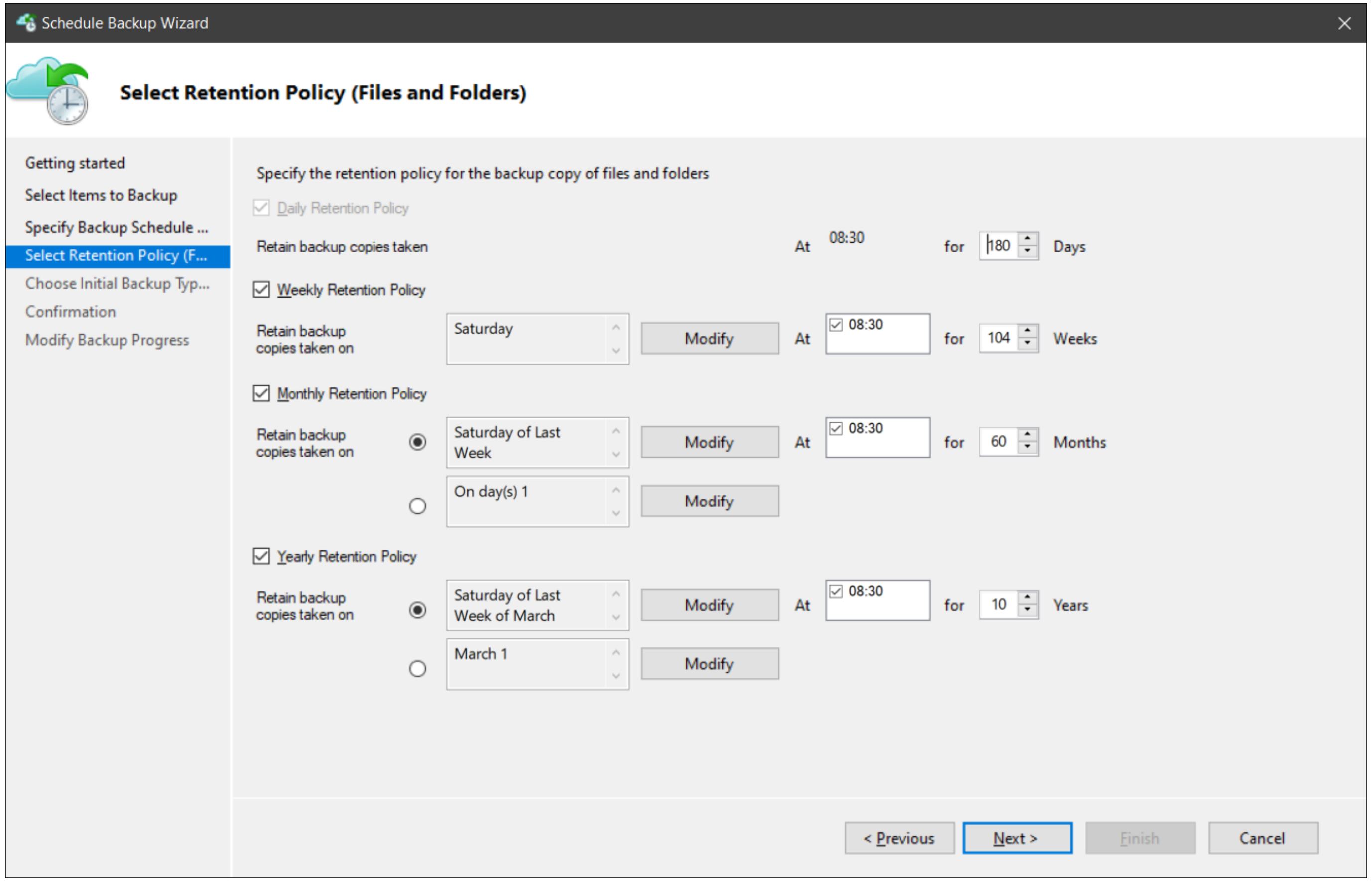
1. Install Recovery Services agent
   Download Agent for Windows Server or Windows Client
2. Download vault credentials to register the server to the vault. Vault credentials will expire after 2 days.
   □ Already downloaded or using the latest Recovery Services Agent
   Download
3. Schedule backup using Recovery Services Agent UI. Learn More
4. Once the backups are scheduled, you can use backup jobs page to monitor the backups. Browse jobs page
5. You can also Configure Notifications from alerts page to receive email alerts for backup failures. Browse alerts page

Learn More

Implement Azure Backup Policies

Create a backup policy:

- After you download and register the MARS agent, open the agent's console
- Choose Schedule Backup
- Complete the wizard by specifying the following settings:
  - Backup schedule
  - Retention settings
  - Initial backup type



Schedule Backup Wizard

Select Retention Policy (Files and Folders)

Getting started
Select Items to Backup
Specify Backup Schedule ...
Select Retention Policy (F...
Choose Initial Backup Typ...
Confirmation
Modify Backup Progress

Specify the retention policy for the backup copy of files and folders

☑ Daily Retention Policy

Retain backup copies taken At 08:30 for 180 Days

☑ Weekly Retention Policy

Retain backup copies taken on Saturday Modify At ☑ 08:30 for 104 Weeks

☑ Monthly Retention Policy

Retain backup copies taken on ● Saturday of Last Week Modify At ☑ 08:30 for 60 Months

○ On day(s) 1 Modify

☑ Yearly Retention Policy

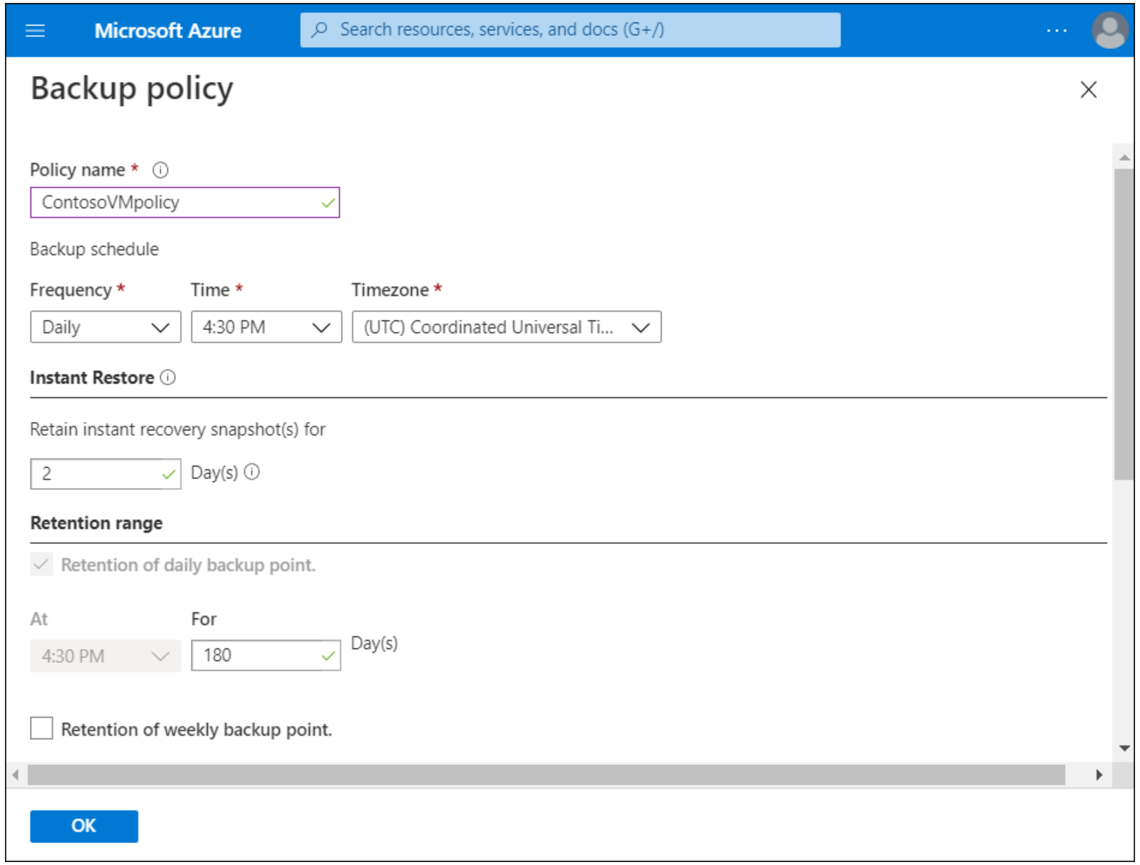
Retain backup copies taken on ● Saturday of Last Week of March Modify At ☑ 08:30 for 10 Years

○ March 1 Modify

Implement Azure Backup Policies

You can use the Azure portal to create a backup policy. Define the following information:

- Policy name
- Backup schedule
- Instant Restore settings
- Retention range



Backup policy

Policy name *: ContosoVMpolicy

Backup schedule

Frequency *: Daily
Time *: 4:30 PM
Timezone *: (UTC) Coordinated Universal Ti...

Instant Restore

Retain instant recovery snapshot(s) for: 2 Day(s)

Retention range

☑ Retention of daily backup point.

At: 4:30 PM
For: 180 Day(s)

□ Retention of weekly backup point.

Recover Windows IaaS Virtual Machines

There are several DR options available for VMs, depending on your use-case

Backup option	Description
VM backups	For backing up Azure VMs running production workloads, use Azure Backup. Azure Backup: • Supports application-consistent backups for both Windows and Linux VMs. • Creates recovery points that are stored in geo-redundant recovery vaults.
Azure Site Recovery	Protects your VMs from a major disaster scenario when an entire region experiences an outage. You can: • Configure Azure Site Recovery for your VMs so that you can recover your application in a matter of minutes. • Replicate to an Azure region of your choice.
Managed snapshots	Provide a quick and simple option for backing up VMs that use Managed Disks. A managed snapshot: • Is a read-only full copy of a managed disk. • Exist independent of the source disk and can be used to create new managed disks for rebuilding a VM. • Is billed based on the used portion of the disk.

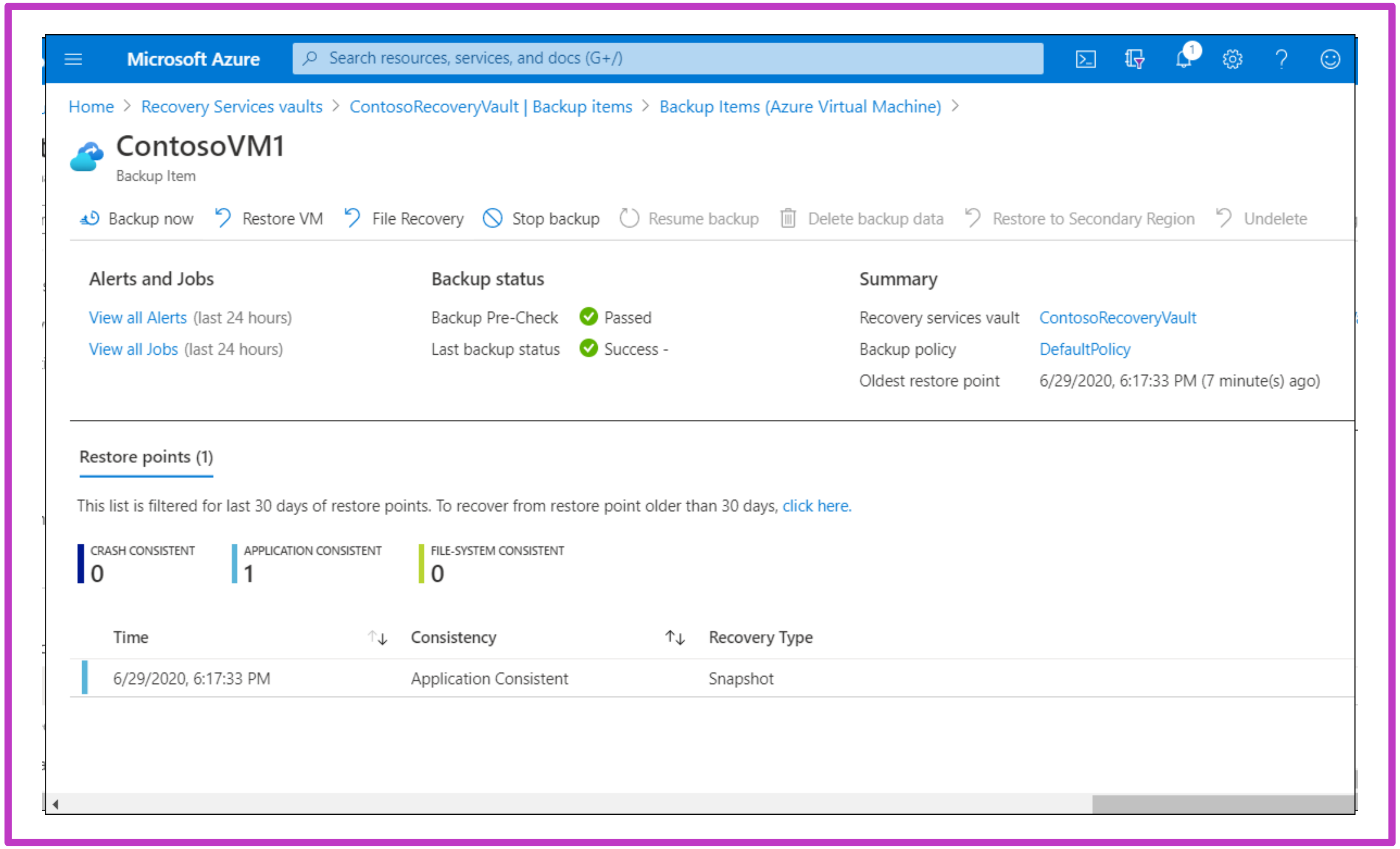
Recover Windows IaaS Virtual Machines

Backup your VM:

- Create a Recovery Services vault
- Use the Portal to define the backup
- Back up the VM

Restore your VM:

- Select the appropriate VM in the Azure portal, and then select Backup
- Select either File Recovery or Restore VM
- Follow the on-screen prompts to complete the process


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Recovery Services vaults > ContosoRecoveryVault | Backup items > Backup Items (Azure Virtual Machine) >
Backup now
Restore VM
File Recovery
Stop backup
Resume backup
Delete backup data
Restore to Secondary Region
Undelete

ContosoVM1

Backup Item

Alerts and Jobs

View all Alerts (last 24 hours)

View all Jobs (last 24 hours)

Backup status

Backup Pre-Check ✓ Passed

Last backup status ✓ Success -

Summary

Recovery services vault ContosoRecoveryVault

Backup policy DefaultPolicy

Oldest restore point 6/29/2020, 6:17:33 PM (7 minute(s) ago)

Restore points (1)

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, click here.

CRASH CONSISTENT 0

APPLICATION CONSISTENT 1

FILE-SYSTEM CONSISTENT 0

Time	Consistency	Recovery Type
6/29/2020, 6:17:33 PM	Application Consistent	Snapshot

Perform File and Folder Recovery

Backup files and folders

- Create a Recovery Services vault
- Download files
- Install and register the Backup Agent
- Back up your files and folders

Restore files and folders

- Select Recovery Mode
- Select Volume and Date
- Select Items to Recover
- Specify Recovery Options

Note: You can restore to the original location or to another location in the same machine.

Perform Backup and Restore of on-premises Workloads

The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Azure cloud.

Before you start

Make sure that you have an Azure account if you will need to back up a server or client to Azure…

Modify storage replication

You can use LRS to reduce Azure storage costs.

Download, install, and register the MARS agent

Run an on-demand backup

You can also run a backup at any time.

Restore files to Windows Server using the MARS Agent

Use Azure Instant Restore to recover data:

- To the same machine
- To a different machine

Perform Backup and Restore of on-premises Workloads

Restore files to Windows Server using the MARS Agent

If you accidentally delete a file and want to restore it to the same machine from which the backup was taken, use Azure Instant Restore, and recover to the same machine.

If your entire server is lost, you can still recover. Use Azure Instant Restore and recover to an alternate machine.

Demonstration – Manage Azure VM backups with Azure Backup Service

1. Create a Recovery Services vault

2. Manage a backup policy for a VM

Learning recap – Implement Hybrid Backup and Recovery with Windows Server IaaS

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Implement hybrid backup and recovery with Windows Server IaaS

Protect your Virtual Machines by Using Azure Backup

Learning Objectives – Azure Backup Introduction

- Azure Backup features and scenarios
- Back up an Azure virtual machine by using Azure Backup
- Demonstration – Back up an Azure virtual machine (optional)
- Restore virtual machine data
- Demonstration – Restore Azure virtual machine data (optional)
- Knowledge check and resources

Azure Backup Features and Scenarios

How Azure Backup works?

- Offers specialized backup solutions for Azure and on-premises virtual machines (VMs)
- Enables workloads running in Azure VMs to have enterprise-class backup and restore options.

Azure Backup versus Azure Site Recovery

- The primary goal of backup is to maintain copies of stateful data that allow you to go back in time
- Site-recovery replicates the data in almost real time and allows for a failover.

Why use Azure Backup?

Azure Backup has several benefits:

- Zero-infrastructure backup
- Long-term retention
- Security
- High availability
- Centralized monitoring and management

Azure Backup supported scenarios

- Azure VMs
- On-premises
- Azure Files shares
- SQL Server in Azure VMs and SAP HANA databases in Azure VMs

Back Up an Azure Virtual Machine by Using Azure Backup

Azure Backup consists of a number of components:

Recovery Services vault

Used to manage and store the backup data

Snapshots

A point-in-time backup of all disks on the VM

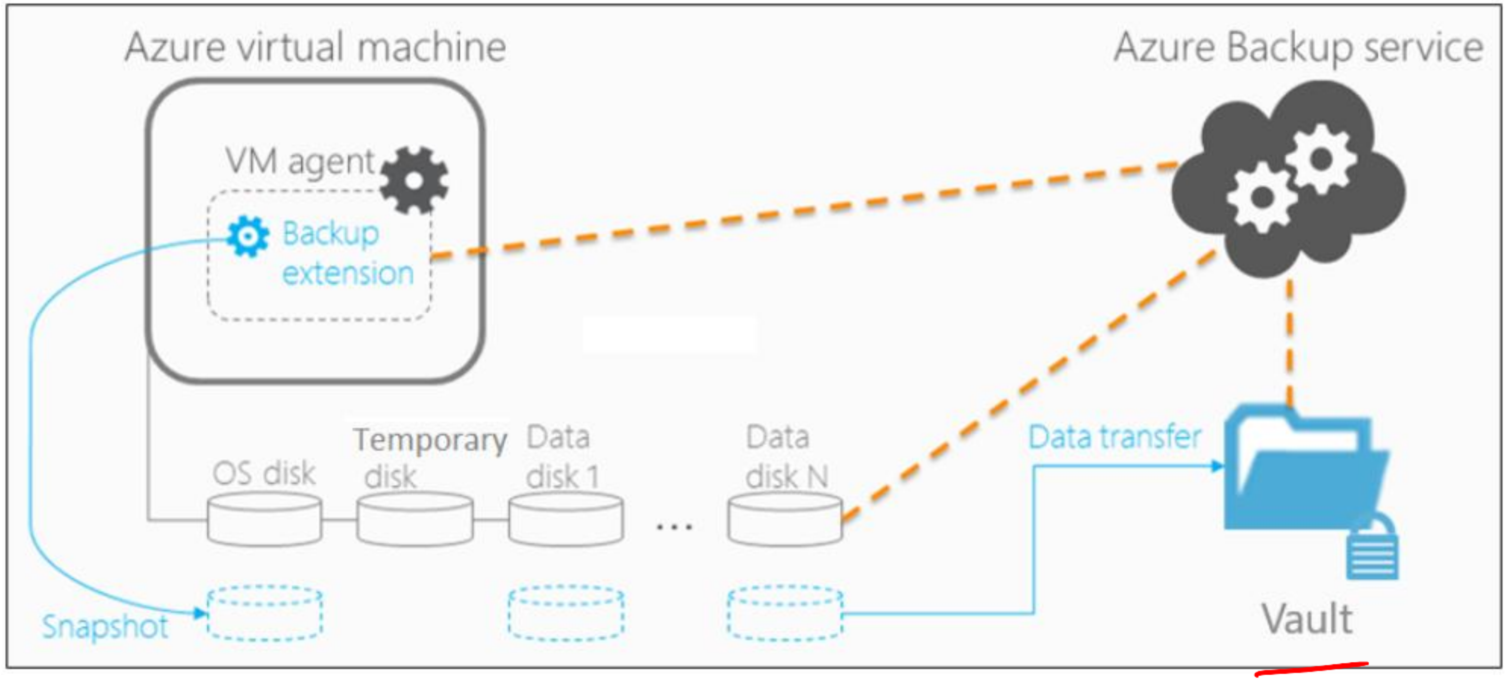
Backup policy

Defines the backup frequency and retention duration for your backups

Back Up an Azure Virtual Machine by Using Azure Backup

Backup process for an Azure virtual machine:

1. For Azure VMs that are selected for backup, Azure Backup starts a backup job according to the backup frequency you specify in the backup policy
2. During the first backup, a backup extension is installed on the VM
3. After the snapshot is taken, it's stored locally as well transferred to the vault



Demonstration – Back Up an Azure Virtual Machine (Optional)

1. Create a backup for Azure virtual machines
2. Enable backup for a virtual machine
3. Monitor backups

Restore Virtual Machine Data

Restore types

Restore option	Details
Create a new VM	Quickly creates and gets a basic VM up and running from a restore point. The new VM must be created in the same region as the source VM.
Restore disk	Restores a VM disk, which can be used to create a new VM. The disks are copied to the Resource Group you specify. Azure Backup provides a template to help you customize and create a VM. Alternatively, you can attach the disk to an existing VM, or create a new VM.
Replace existing	You can restore a disk and use it to replace a disk on the existing VM. Azure Backup takes a snapshot of the existing VM before replacing the disk and stores it in the staging location you specify. Existing disks connected to the VM are replaced with the selected restore point. The current VM must exist. If it's been deleted, this option can't be used.
Cross Region (secondary region)	Cross Region restore can be used to restore Azure VMs in the secondary region, which is an Azure paired region. This feature is available for the options below: • Create a VM • Restore Disks We don’t currently support the Replace existing disks option.

Demonstration – Restore Azure Virtual Machine Data (Optional)

1 Restore a virtual machine in the Azure portal

2 Track a restore

Learning recap – Protect your Virtual Machines by Using Azure Backup

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Protect your virtual machines by using Azure Backup

Protect your Azure Infrastructure with Azure Site Recovery

Learning Objectives – Azure Site Recovery Introduction

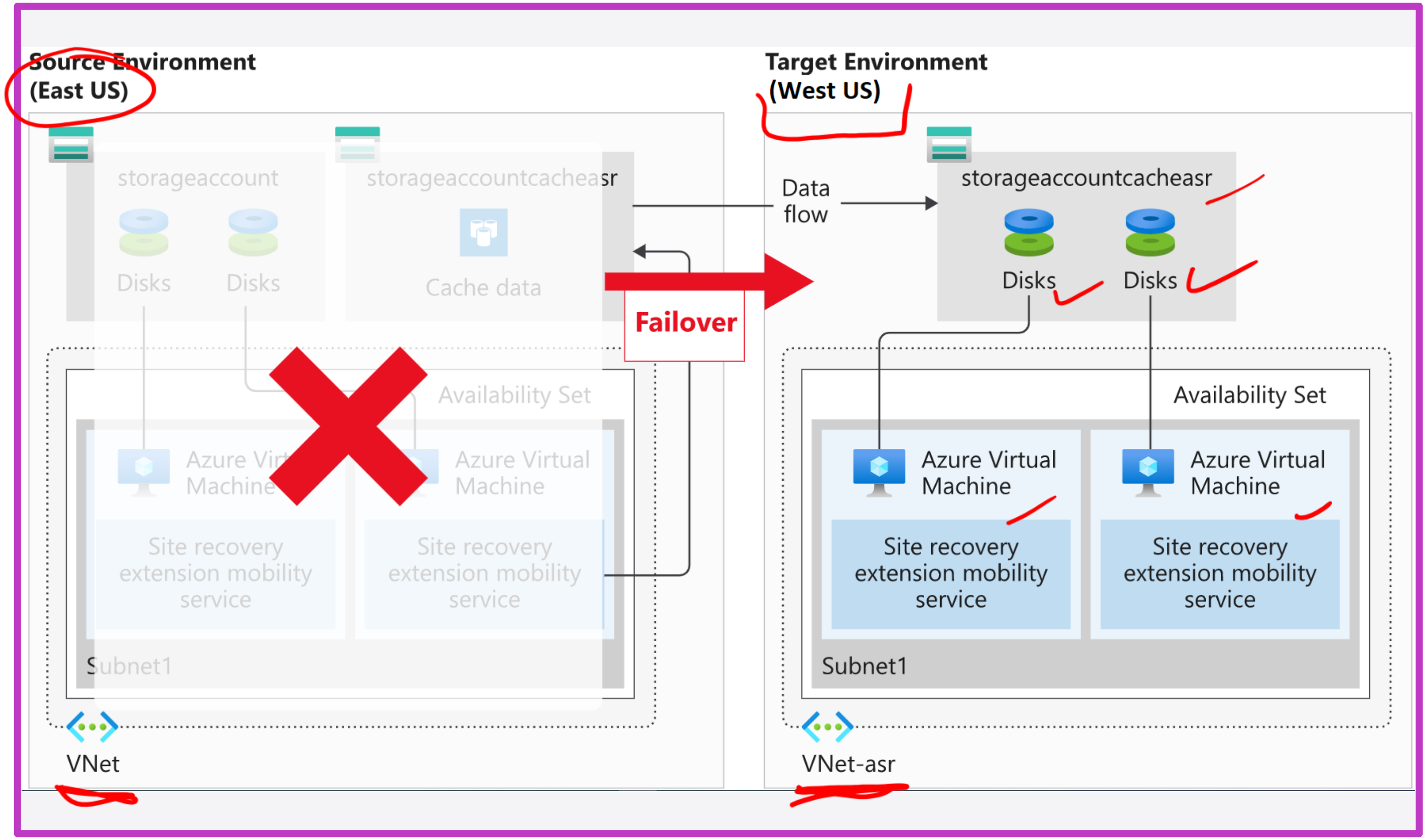
- What is Azure Site Recovery?
- Prepare for disaster recovery with Azure Site Recovery
- Demonstration – Set up disaster recovery with Azure Site Recovery (Optional)
- Run a disaster recovery drill
- Demonstration – Run a disaster recovery drill (Optional)
- Failover and failback using Azure Site Recovery
- Demonstration – Failover and failback using Azure Site Recovery(Optional)
- Learning recap

What is Azure Site Recovery

nur VMs
VMSS

Azure Site Recovery provides:

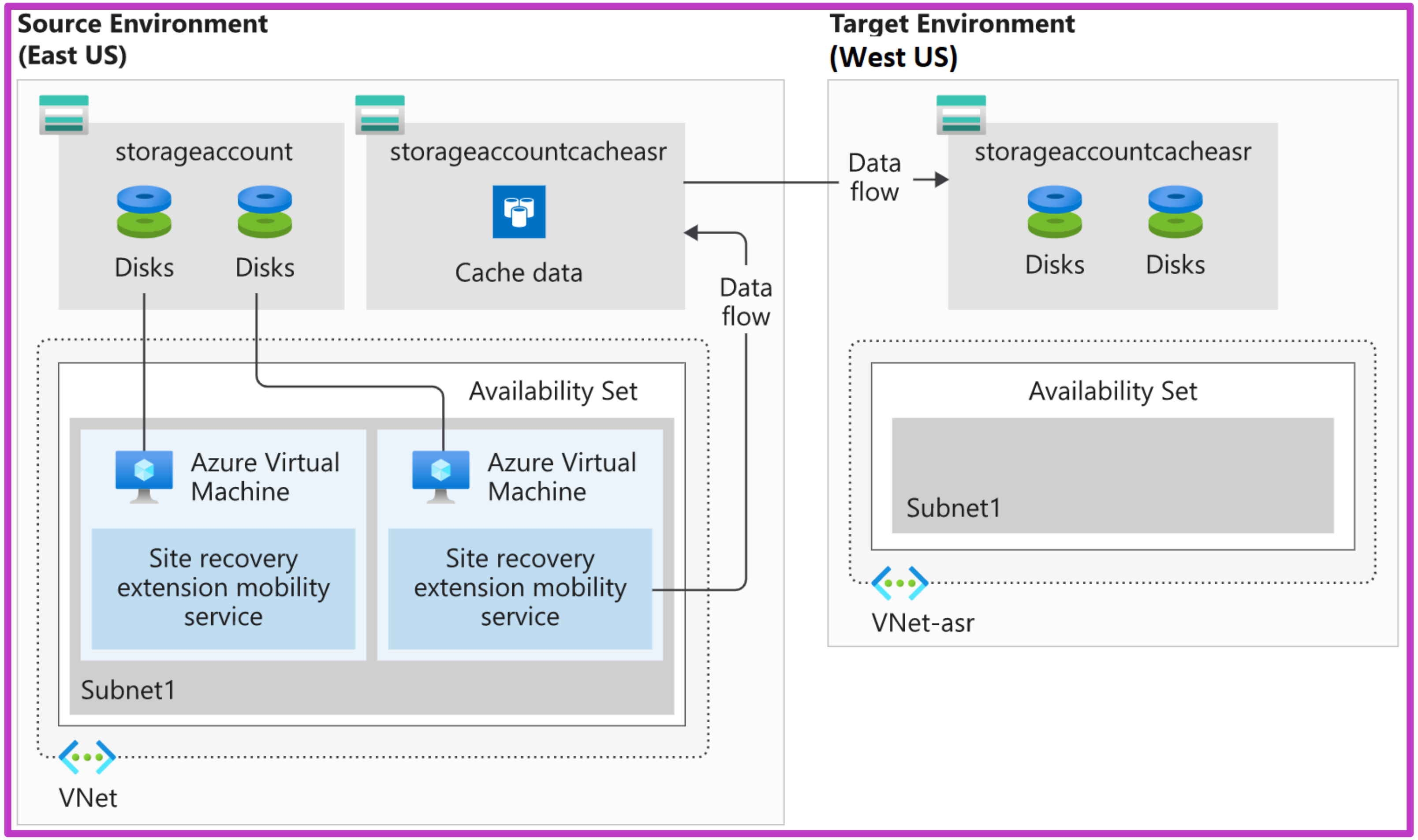
- Azure virtual machine protection
- Snapshots and recovery points
- Replication to a secondary region
- Disaster recovery drills
- Flexible failover and failback



Prepare for Disaster Recovery with Azure Site Recovery

Disaster recovery preparation:

- Add a Recovery Services vault
- Organize target resources
- Configure outbound network connectivity
- Set up replication on existing VMs



Demonstration – Set Up Disaster Recovery with Azure Site Recovery (Optional)

1. Create a recovery services vault
2. Enable replication
3. Monitor replication progress

Run a Disaster Recovery Drill

What is a disaster recovery drill?

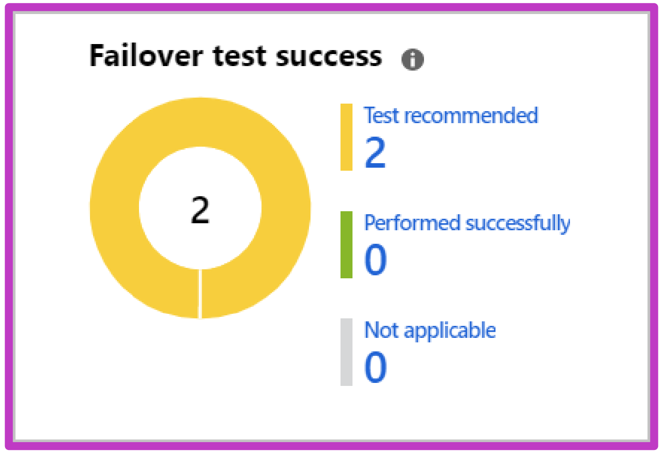
- A DR drill is a way to check if you configured your solution correctly.

Why should you run a DR drill?

- A DR drill is vital to ensure the solution implemented meets the BCDR requirements, and to ensure the replication works appropriately

Content of running a disaster recovery drill

- Test failover of individual machines
- Create a failover test
- Flexible failover of multiple machines
- Understand the difference between a drill and production failover



Failover test success

2

Test recommended
2

Performed successfully
0

Not applicable
0

Demonstration – Run a Disaster Recovery Drill (Optional)

1. Create a recovery plan
2. Run a test failover using a recovery plan
3. Monitor failover progress

Failover and Failback Using Azure Site Recovery

What is failover and failback?

A failover occurs when a decision is made to execute a DR plan for your organization:

- The existing production environment, protected by Site Recovery is replicated to a different region

Failback is the reverse of a failover:

- A completed failover to a secondary region has been committed, and is now the production environment
- Reprotection has completed for the failed-over environment, and the source environment is now its replica
- In a failback scenario, Site Recovery will fail over back to the source VMs

What is reprotection, and why is it important?

- When a VM is failed over, the replication performed by Site Recovery is no longer occurring.
- You must re-enable the protection to start protecting the failed-over VM.
- As you already have the infrastructure in a different region, you can start replication back to the source region.
- Reprotection enables Site Recovery to start replicating your new target environment back to the source environment where it started.

Failover and Failback Using Azure Site Recovery

Fix issues with a failover

Even though Site Recovery is automated, errors can still happen.

The following are the three most common issues observed:

- Azure resource quota issues
- One or more disk(s) are available for protection
- Trusted root certificates

Demonstration – Failover and Failback Using Azure Site Recovery (Optional)

1. Fail over a VM to a secondary region using PowerShell
2. Reprotect the VM using PowerShell
3. Monitor and test using PowerShell
4. Failback to the West US region using the portal

Learning recap – Protect your Azure Infrastructure with Azure Site Recovery

Knowledge Check

Microsoft Learn Modules (learn.microsoft.com/)

Protect your Azure infrastructure with Azure Site Recovery

Lab 05: Implementing Azure-based recovery services

Lab 05 – Implementing Azure-based recovery services

Lab scenario

To address concerns regarding the outdated operational model, the limited use of automation, and reliance on tape backups for restores and disaster recovery, you decide to use Azure-based recovery services. As the first step, you'll implement Azure Site Recovery and Azure Backup.

Objectives

- Create and configure an Azure Site Recovery vault
- Implement Hyper-V VM protection by using Azure Site Recovery vault
- Implement Azure Backup

End of presentation