

# AZ-801

## Configuring Windows Server Hybrid Advanced Services

### 5 Disaster Recovery Cloud



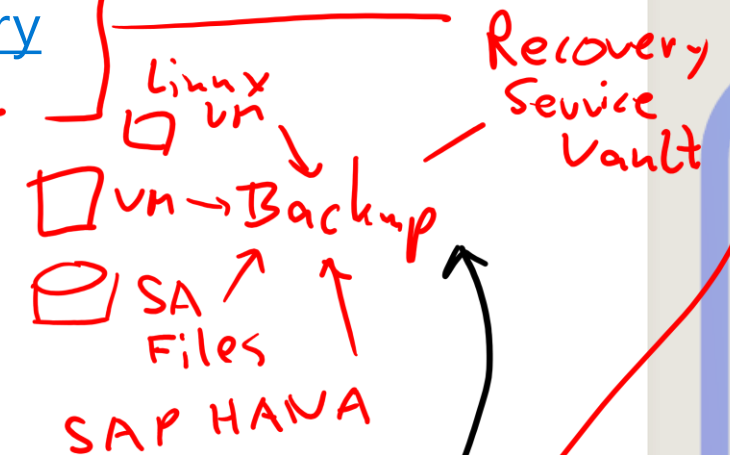
# AZ-801 Course Outline

- 1 Windows Server Security on Prem
- 2 Windows Server Security Cloud
- 3 Failover Cluster
- 4 Disaster Recovery on Prem
- 5 Disaster Recovery Cloud ← ASR
- 6 Windows Server Upgrade and Migrate
- 7 Migrate Windows Server to Cloud
- 8 Windows Server Monitoring
- 9 Monitoring in the Cloud

# 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](#)



# Implement hybrid backup and recovery with Windows Server IaaS



# Describe Azure Backup

Recovery Vault - LRS  
Locally Redundant Storage  
GRS

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

---

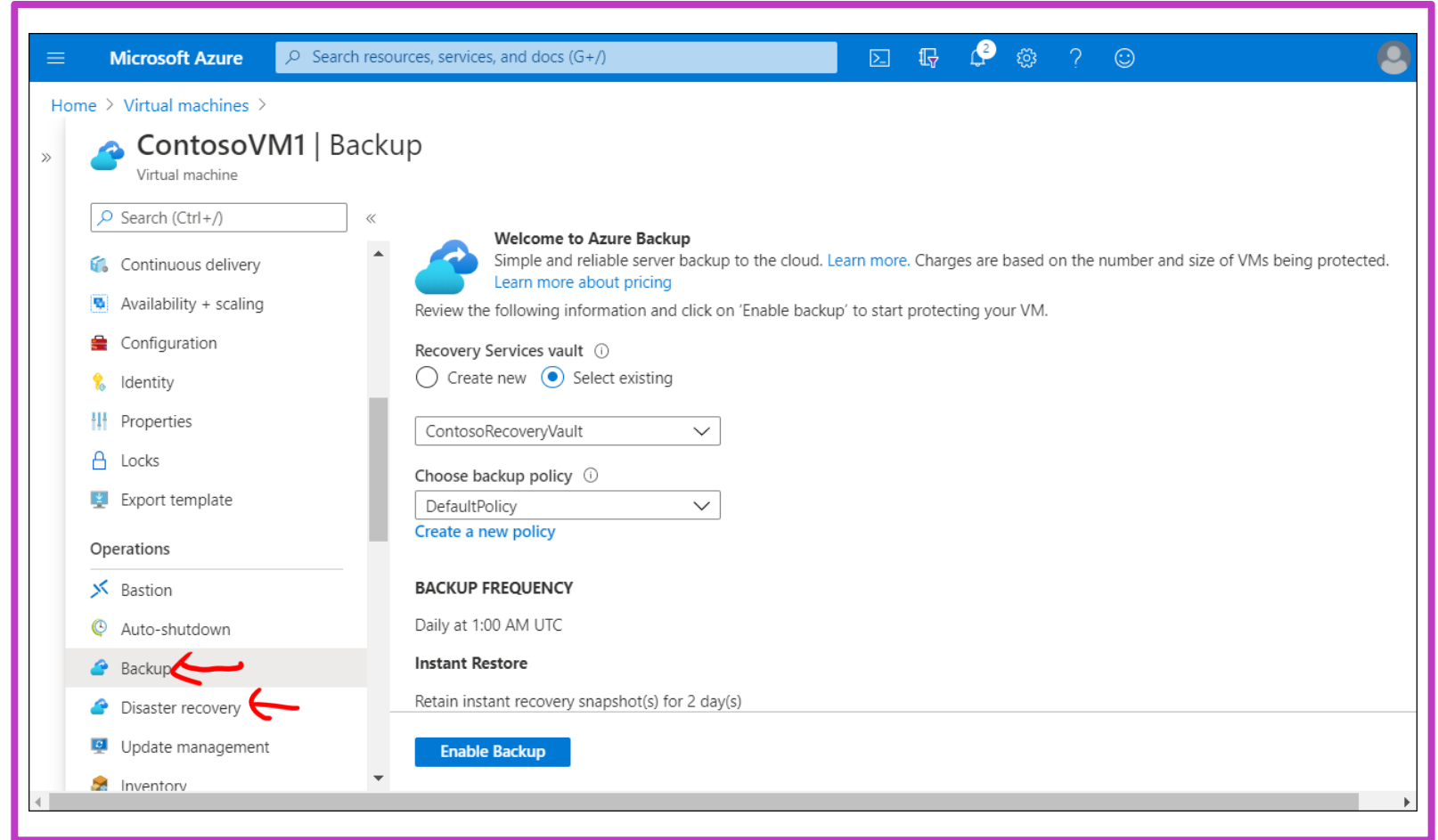
4

Includes the following security features: Prevention, alerting and recovery

# Implement recovery 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



# 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 **Add**.
6. Define the subscription, resource group, specify a vault name, and choose the appropriate region, then select **Create**.

The screenshot displays the 'Create Recovery Services vault' page in the Microsoft Azure portal. The page is titled 'Create Recovery Services vault' and includes a 'Preview' section. The 'Basics' tab is selected, showing the following details:

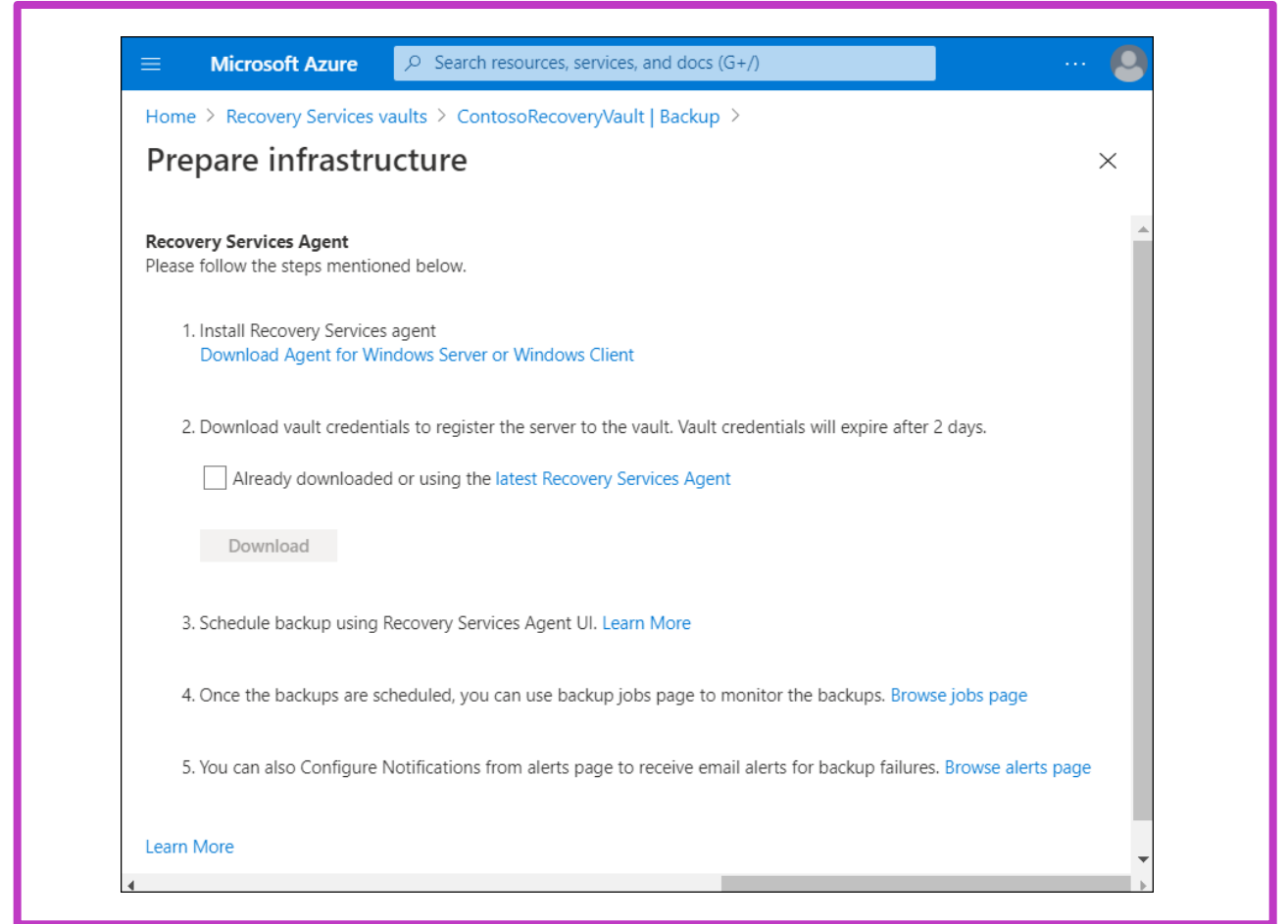
- Project Details:** Select the subscription and the resource group in which you want to create the vault.
  - Subscription:** Contoso Demo
  - Resource group:** ContosoResourceGroup (with a 'Create new' link below it)
- Instance Details:**
  - Vault name:** ContosoRecoveryVault (with a green checkmark)
  - Region:** East US (circled in red)

At the bottom of the form, there are two buttons: 'Review + create' and '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.





# Implement Azure Backup Policies

## Create a backup policy:

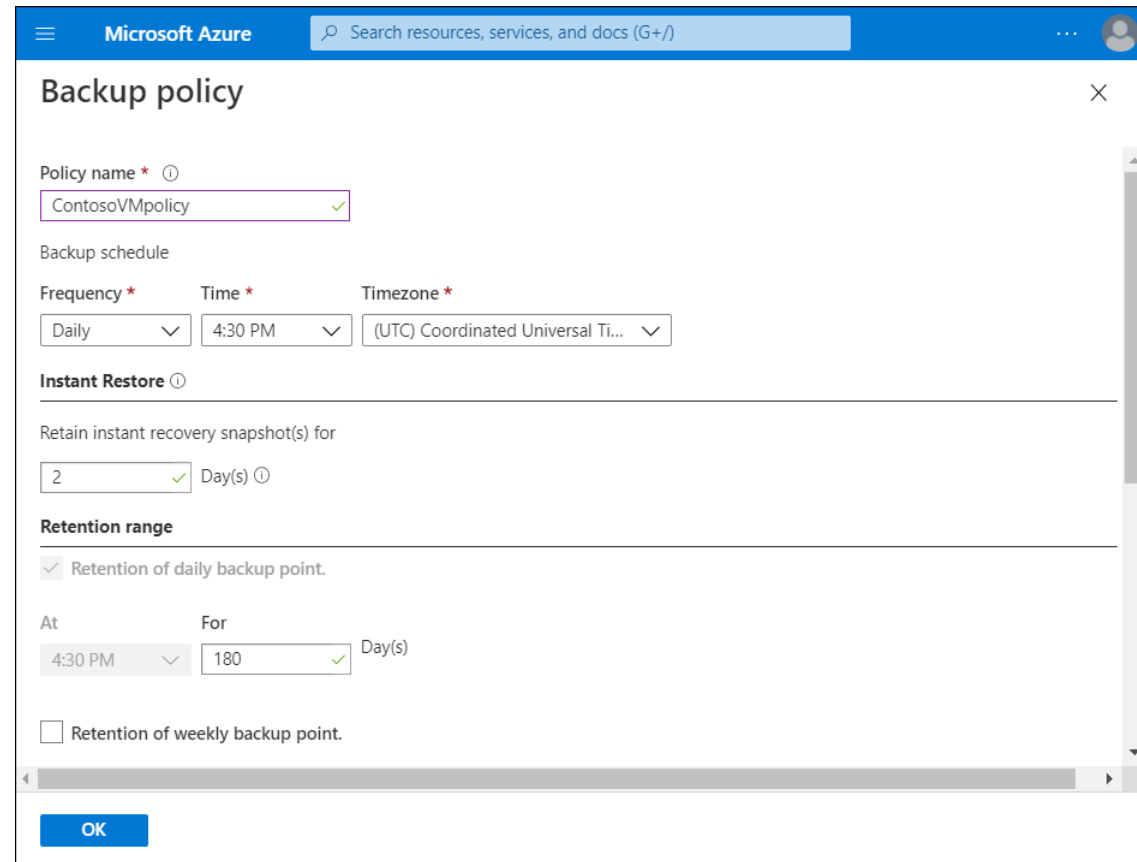
- After you download and register the MARS agent, open the agent's console
- Choose Schedule Backup
- Complete the wizard by specifying the following settings:
  - Backup schedule
  - Retention settings
  - Initial backup type

The screenshot shows the 'Schedule Backup Wizard' window with the title 'Select Retention Policy (Files and Folders)'. The left sidebar contains the following steps: 'Getting started', 'Select Items to Backup', 'Specify Backup Schedule ...', 'Select Retention Policy (F...)' (which is selected and highlighted in blue), 'Choose Initial Backup Typ...', 'Confirmation', and 'Modify Backup Progress'. The main area is titled 'Specify the retention policy for the backup copy of files and folders'. It contains four sections, each with a checked checkbox and a 'Retain backup copies taken' dropdown menu. The first section is 'Daily Retention Policy' with a retention of '180 Days'. The second is 'Weekly Retention Policy' with a retention of '104 Weeks'. The third is 'Monthly Retention Policy' with a retention of '60 Months'. The fourth is 'Yearly Retention Policy' with a retention of '10 Years'. Each section has a 'Modify' button next to the dropdown. At the bottom right, there are four buttons: '< Previous', 'Next >' (which is highlighted with a blue border), 'Finish', and 'Cancel'.

# 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



The screenshot shows the 'Backup policy' configuration window in the Microsoft Azure portal. The window has a blue header with the 'Microsoft Azure' logo and a search bar. The main content area is white and contains the following fields:

- Policy name \***: A text input field containing 'ContosoVMpolicy' with a green checkmark icon to its right.
- Backup schedule**: A section with three dropdown menus:
  - Frequency \***: Set to 'Daily'.
  - Time \***: Set to '4:30 PM'.
  - Timezone \***: Set to '(UTC) Coordinated Universal Ti...'.
- Instant Restore**: A section with a sub-label 'Retain instant recovery snapshot(s) for' and a text input field containing '2' with a green checkmark icon to its right, followed by 'Day(s)'.
- Retention range**: A section with a checked checkbox labeled 'Retention of daily backup point.' and a sub-label 'At' followed by a dropdown menu set to '4:30 PM' and a sub-label 'For' followed by a text input field containing '180' with a green checkmark icon to its right, followed by 'Day(s)'. There is also an unchecked checkbox labeled 'Retention of weekly backup point.'

At the bottom of the window is a blue 'OK' button.

# Recover Windows IaaS Virtual Machines

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

Backup option	Description
VM backups	<p>For backing up Azure VMs running production workloads, use Azure Backup. Azure Backup:</p> <ul style="list-style-type: none"><li>• Supports application-consistent backups for both Windows and Linux VMs.</li><li>• Creates recovery points that are stored in geo-redundant recovery vaults.</li></ul>
Azure Site Recovery	<p>Protects your VMs from a major disaster scenario when an entire region experiences an outage. You can:</p> <ul style="list-style-type: none"><li>• Configure Azure Site Recovery for your VMs so that you can recover your application in a matter of minutes.</li><li>• Replicate to an Azure region of your choice.</li></ul>
Managed snapshots	<p>Provide a quick and simple option for backing up VMs that use Managed Disks. A managed snapshot:</p> <ul style="list-style-type: none"><li>• Is a read-only full copy of a managed disk.</li><li>• Exist independent of the source disk and can be used to create new managed disks for rebuilding a VM.</li><li>• Is billed based on the used portion of the disk.</li></ul>

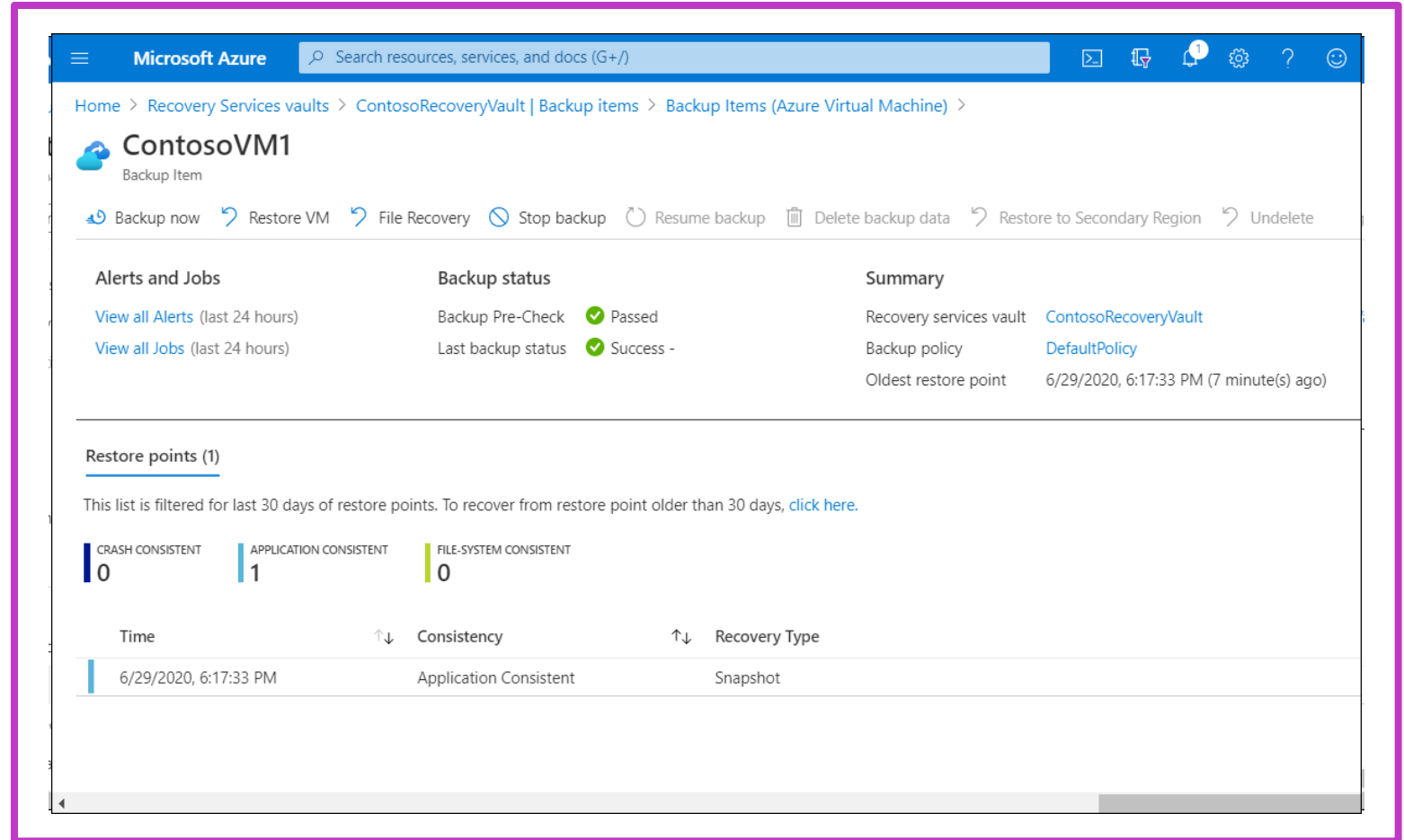
# Recover Windows IaaS Virtual Machines

## 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



# 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.

# Protect your Azure Infrastructure with Azure Site Recovery

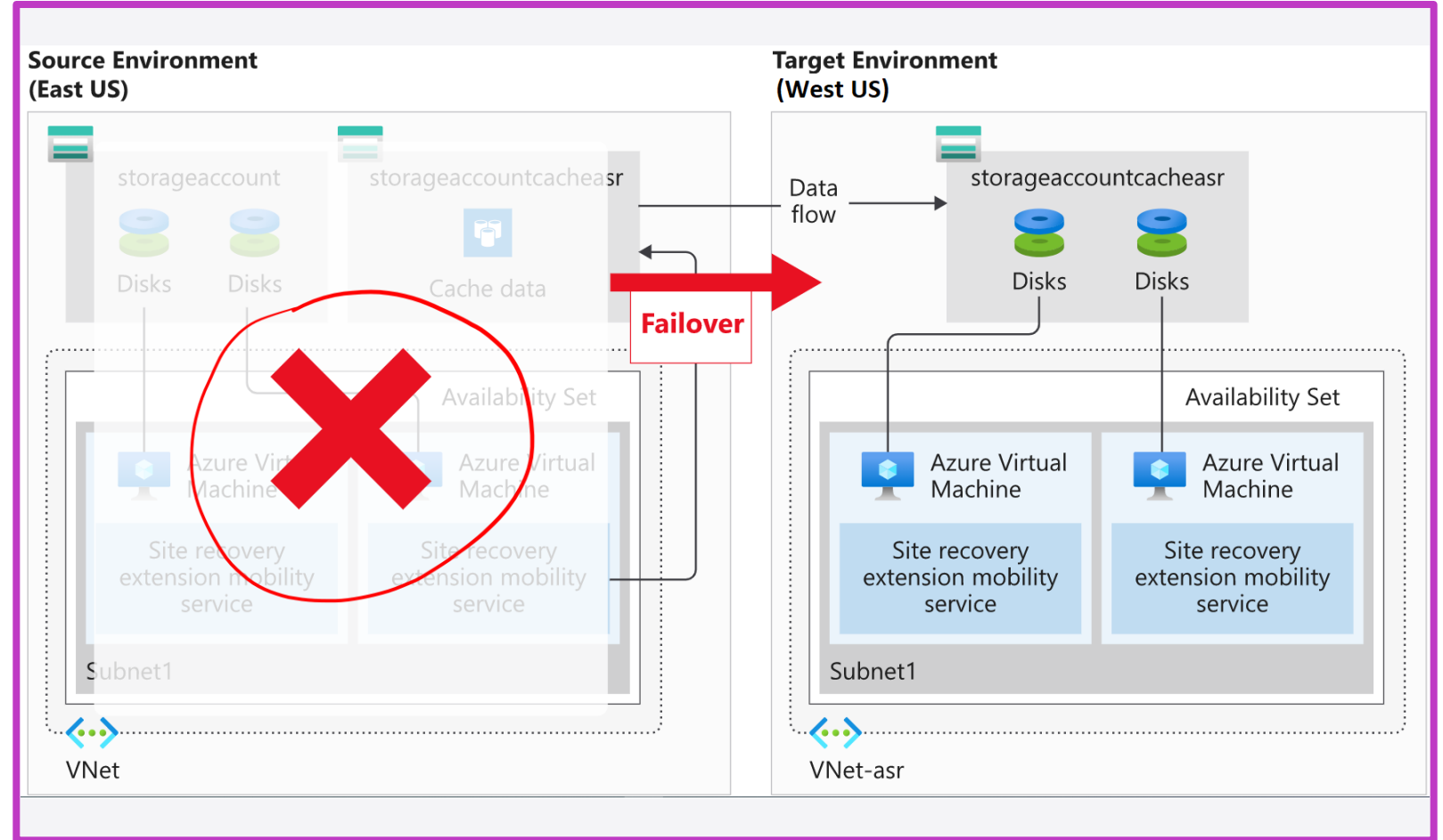




# What is Azure Site Recovery

## Azure Site Recovery provides:

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

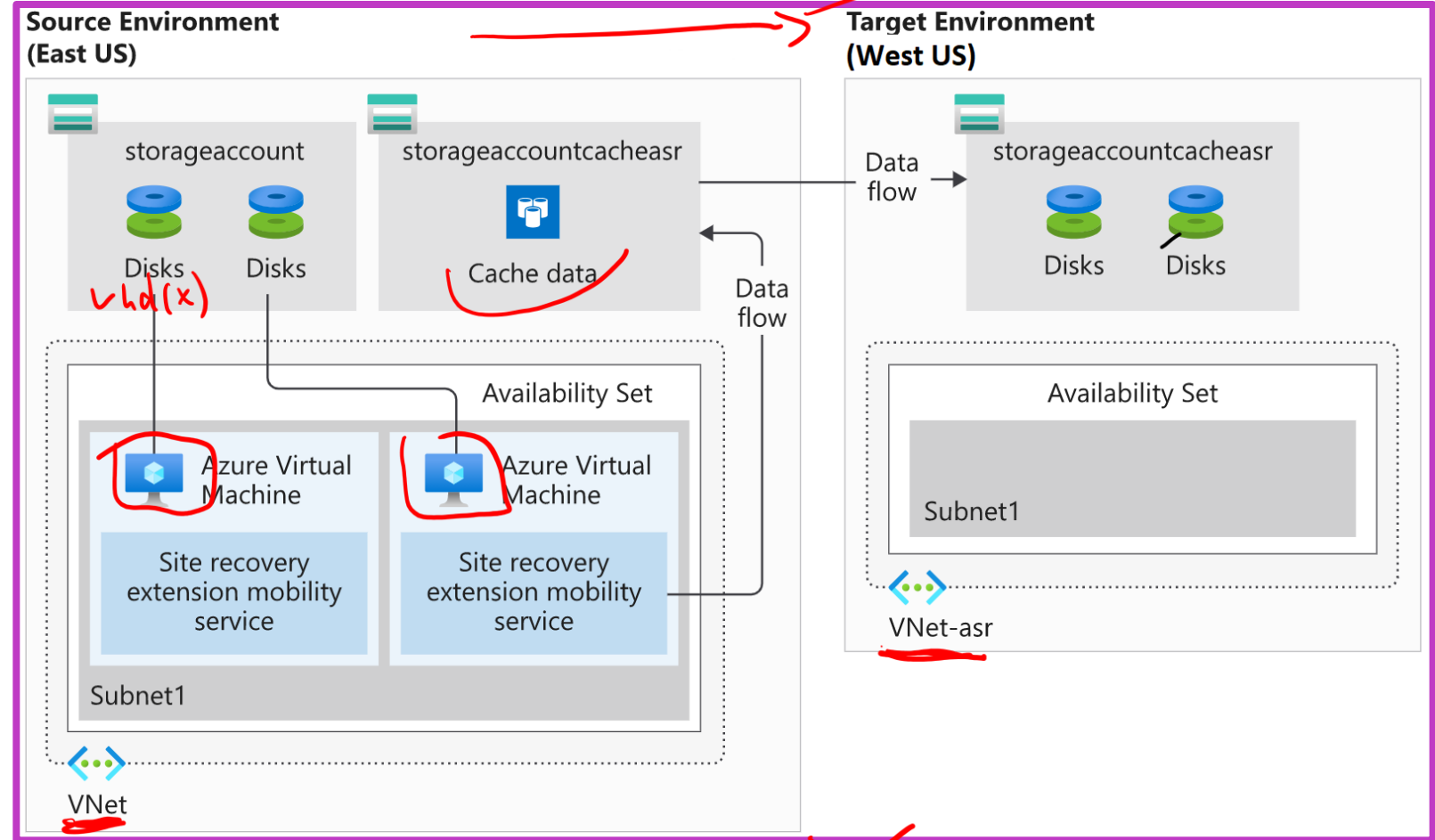


# Prepare for Disaster Recovery with Azure Site Recovery

Recovery Service Vault  
~~East US~~ West US ✓

## Disaster recovery preparation:

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



~~Peering~~  
10.0.0.0/24 10.0.0.0/24

# 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:

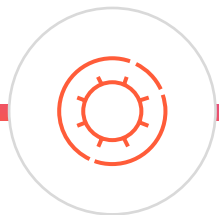
- Azure resource quota issues ← VCPU 10max / Region
- One or more disk(s) are available for protection
- Trusted root certificates

MARS

# Protect your Virtual Machines by Using Azure Backup



# Azure Backup Features and Scenarios



## How Azure Backup works?

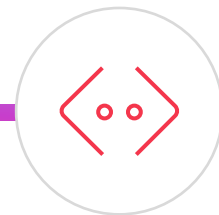
- Offers specialized backup solutions for Azure and on-premises virtual machines (VMs)
- Enables workloads running in Azure VMs to have enterprise-class backup and restore options.



## 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.

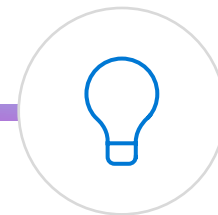
30 Sec



## 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

TB  
Blob Storage  
LRS  
soft delete

## Snapshots

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

VSS

App consistent  
Crash consistent

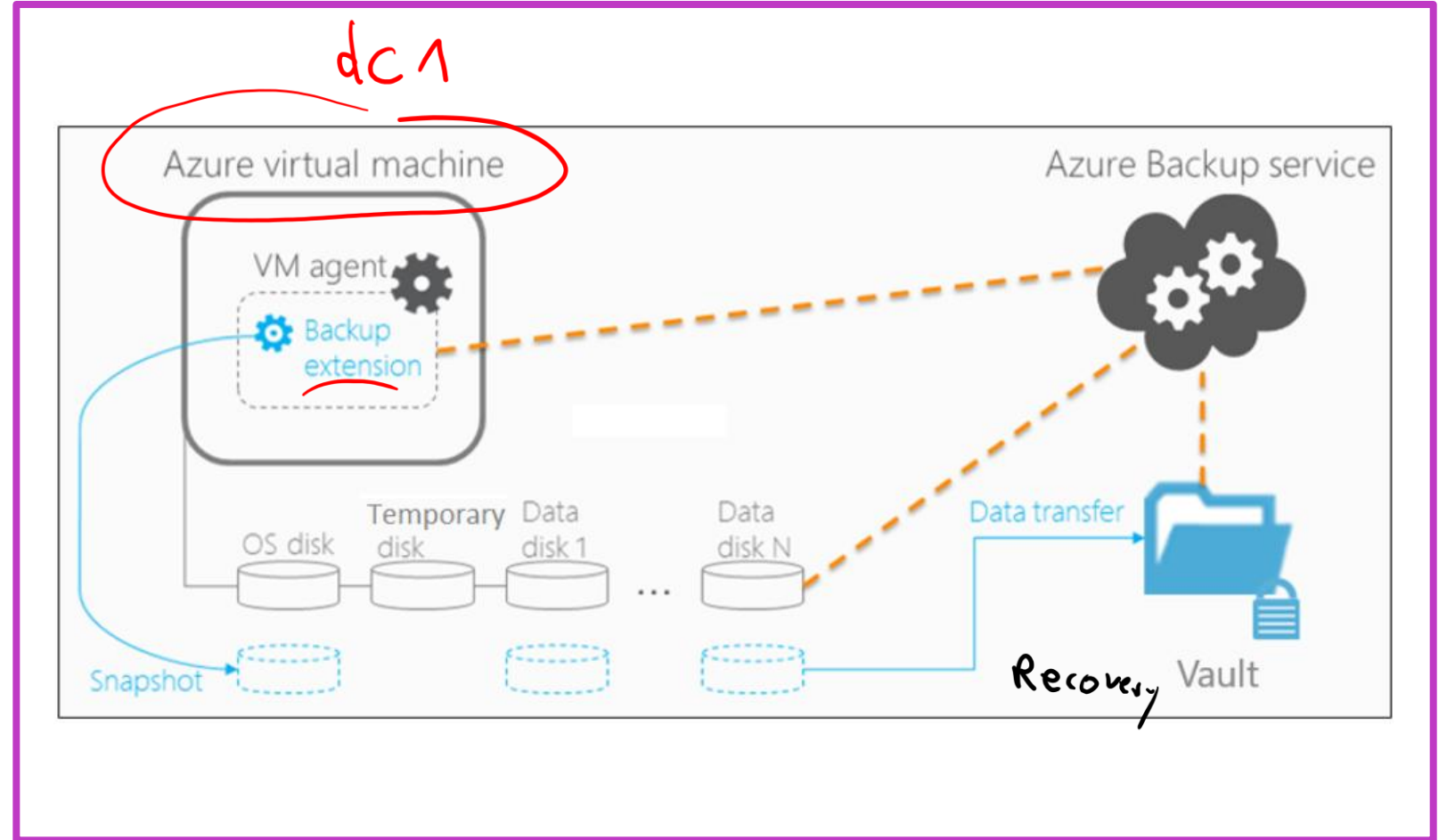
## Backup policy

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





# Restore Virtual Machine Data

Notebook  
PowerShell  
Azure Portal

Recovery Vault  
Backup  
VHD

D: vobocopy ← Download

## 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)	<p>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:</p> <ul style="list-style-type: none"><li>• Create a VM</li><li>• Restore Disks</li></ul> <p>We don't currently support the Replace existing disks option.</p>

# 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

