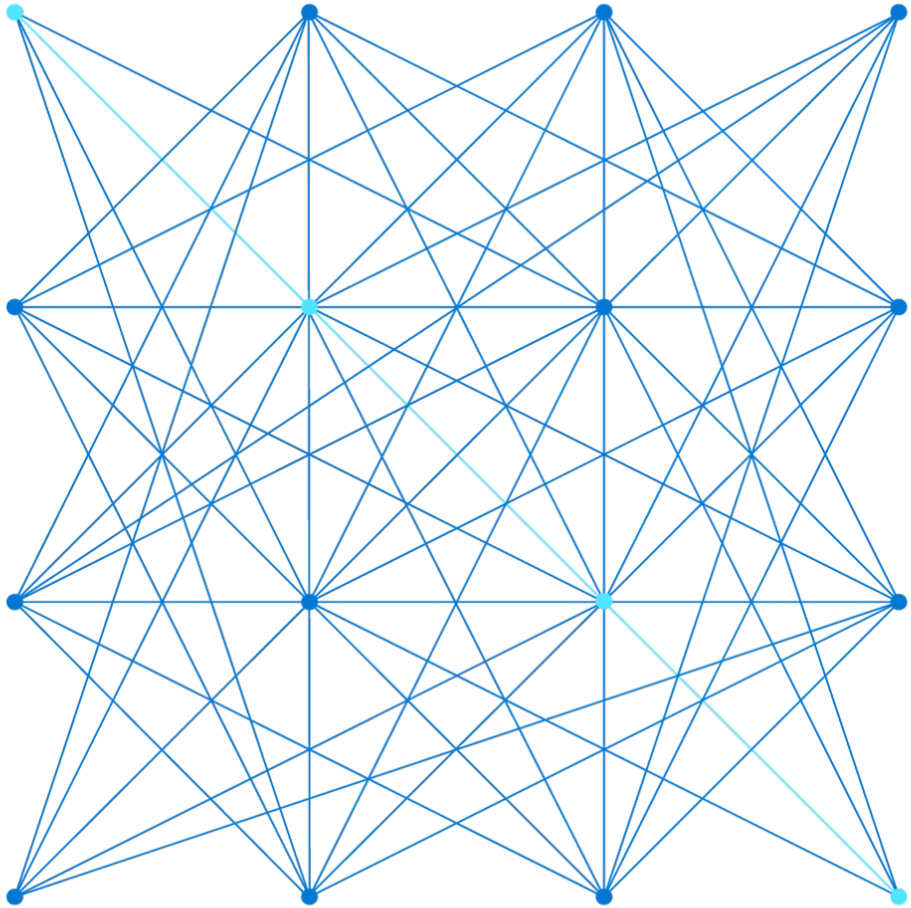
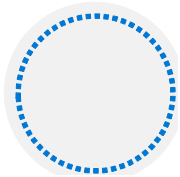
Microsoft Azure

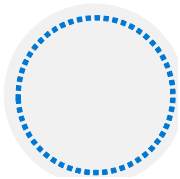
AZ-104T00A Module 10: Data Protection



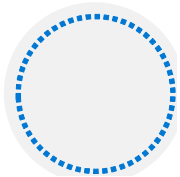
Module Overview



Lesson 01: File and Folder Backups

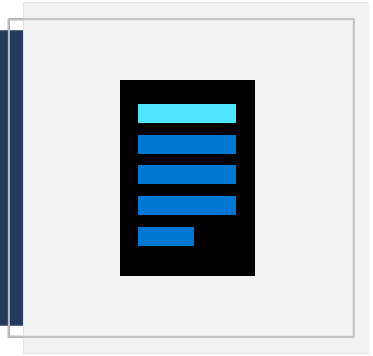


Lesson 02: Virtual Machine Backups



Lesson 03: Module 10 Lab and Review

Lesson 01: File and Folder Backups



File and Folder Backups Overview

- Azure Backup
- Recovery Service Vault Backup Options
- Demonstration – Backup Azure File Shares
- Implementing On-premises File and Folder Backups
- Microsoft Azure Recovery Services Agent
- Demonstration – Backup Files and Folders

Azure Backup

Azure-based service used to back up and restore data in Microsoft cloud

Automatic Storage Management

Multiple storage options

Unlimited data transfer

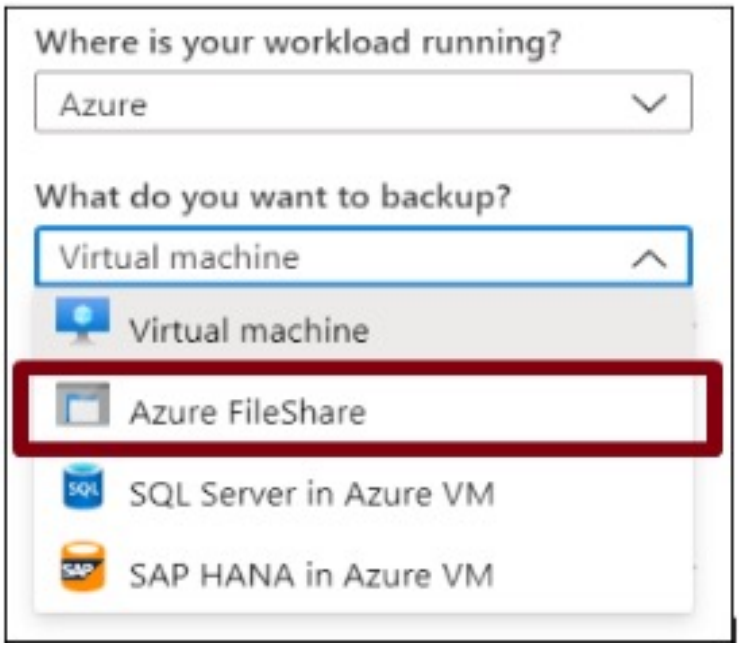
Data encryption

Application consistent backup

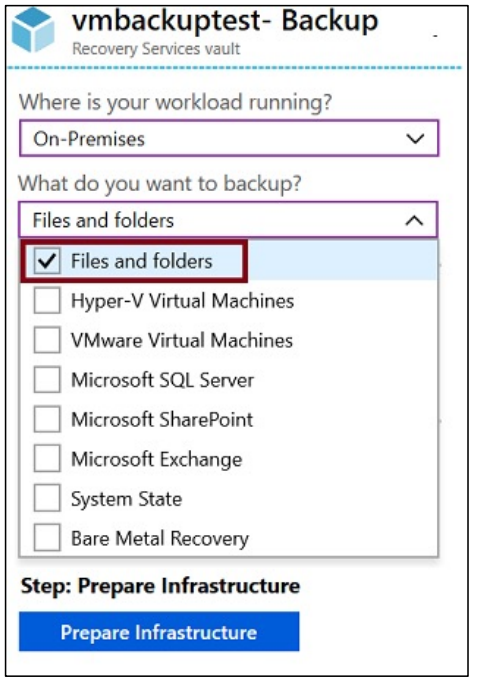
Long-term retention

Recovery Services Vault Backup Options

Azure Workloads



On-Premises Workloads



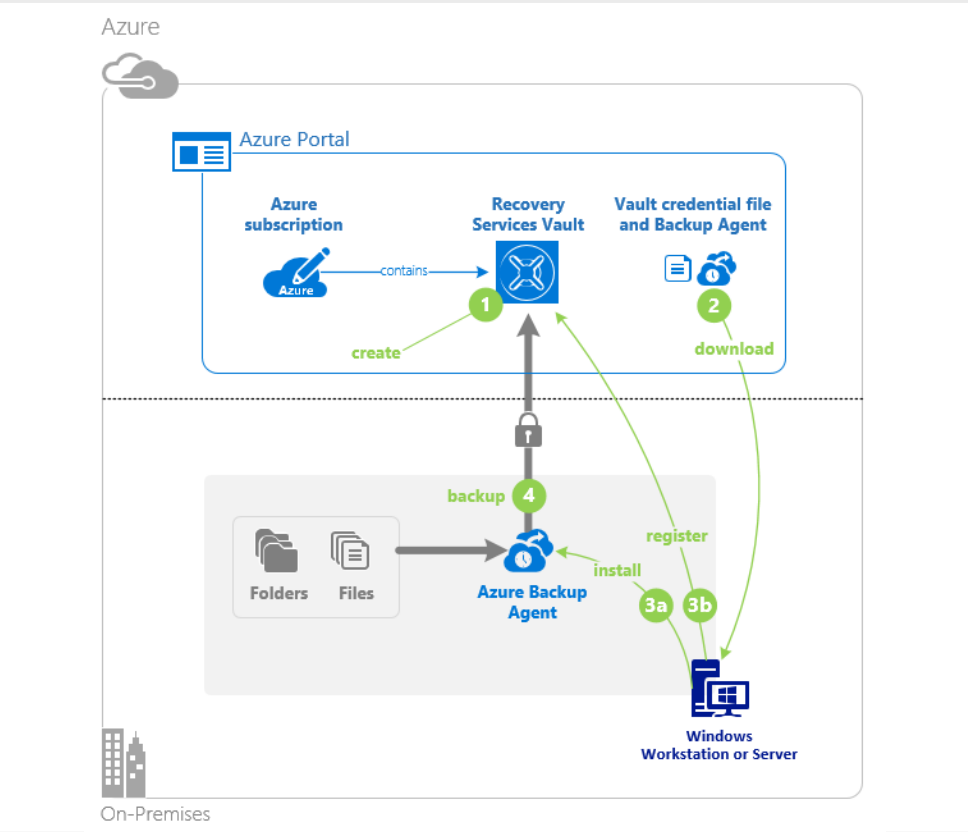
Implementing On-premises File and Folder Backup

1. Create the recovery services vault

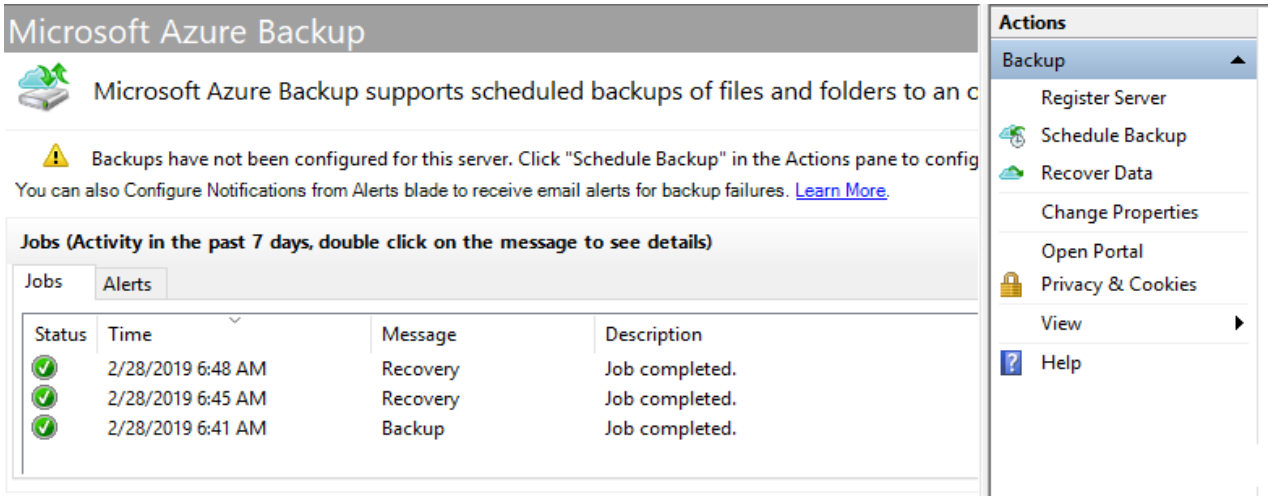
2. Download the agent and credential file

3. Install and register agent

4. Configure the backup



Microsoft Azure Recovery Services Agent (MARS)



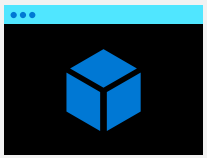
Backup or recover files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure)

No separate backup server required

Not application aware; file, folder, and volume-level restore only

No support for Linux

Lesson 02: Virtual Machine Backups



Virtual machine backups overview

Virtual Machine Data Protection

Workload Protection Needs

Virtual Machine Snapshots

Recovery Services Vault VM Backup Options

Implementing VM Backups

Implementing VM Restore

Azure Backup Server

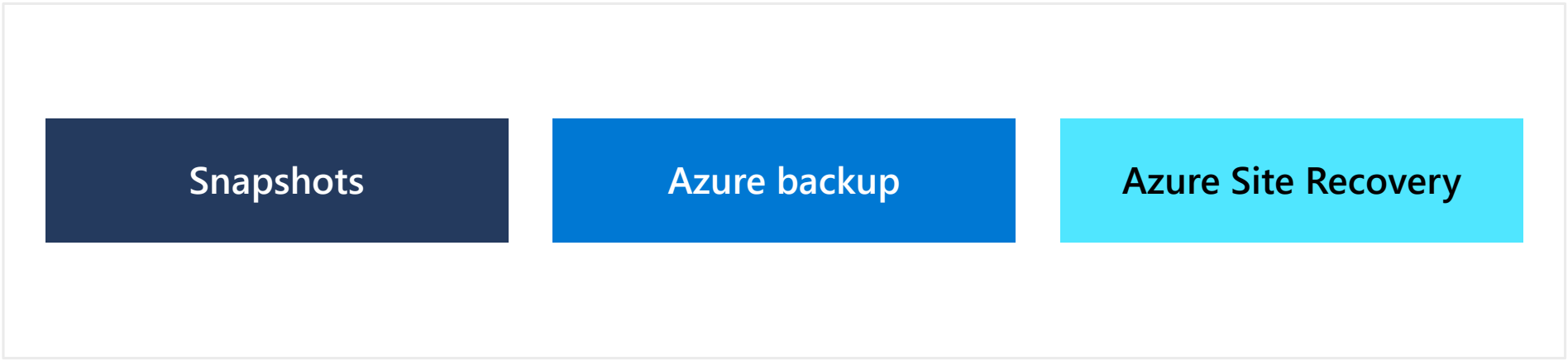
Backup Component Comparison

Soft Delete

Azure Site Recovery

Azure to Azure Architecture

Virtual Machine Data Protection



Managed snapshots provide a quick and simple option for backing up VMs that use Managed Disks

Azure Backup supports application-consistent backups for both Windows and Linux VMs

Azure Site Recovery protects your VMs from a major disaster scenario when a whole region experiences an outage

Workload Protection Needs

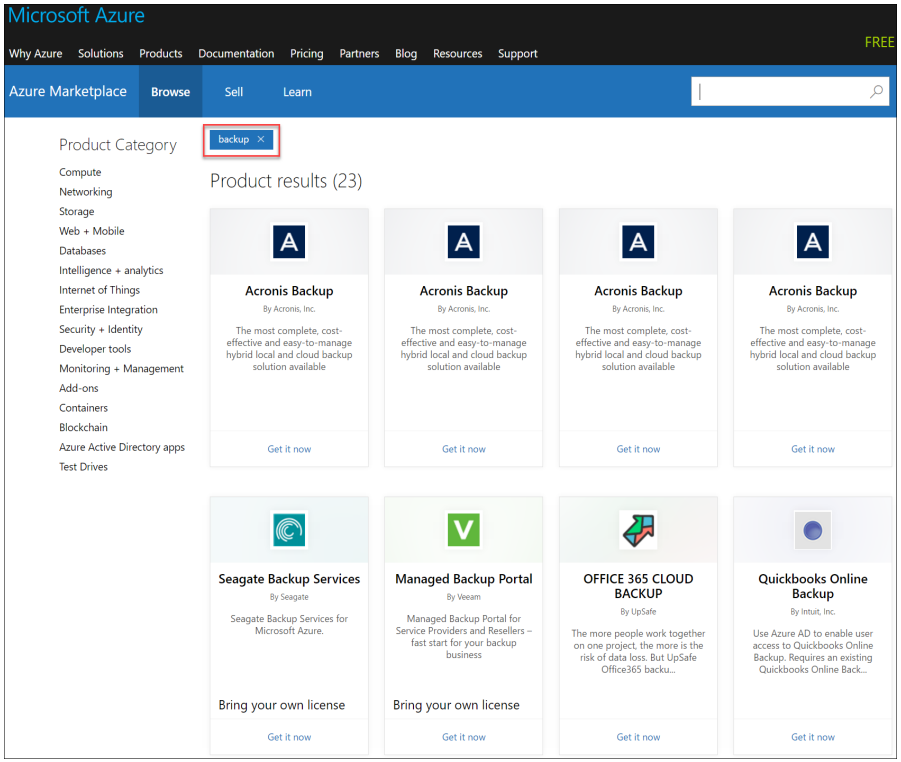
Many backup options are available

How the workload is being protected today?

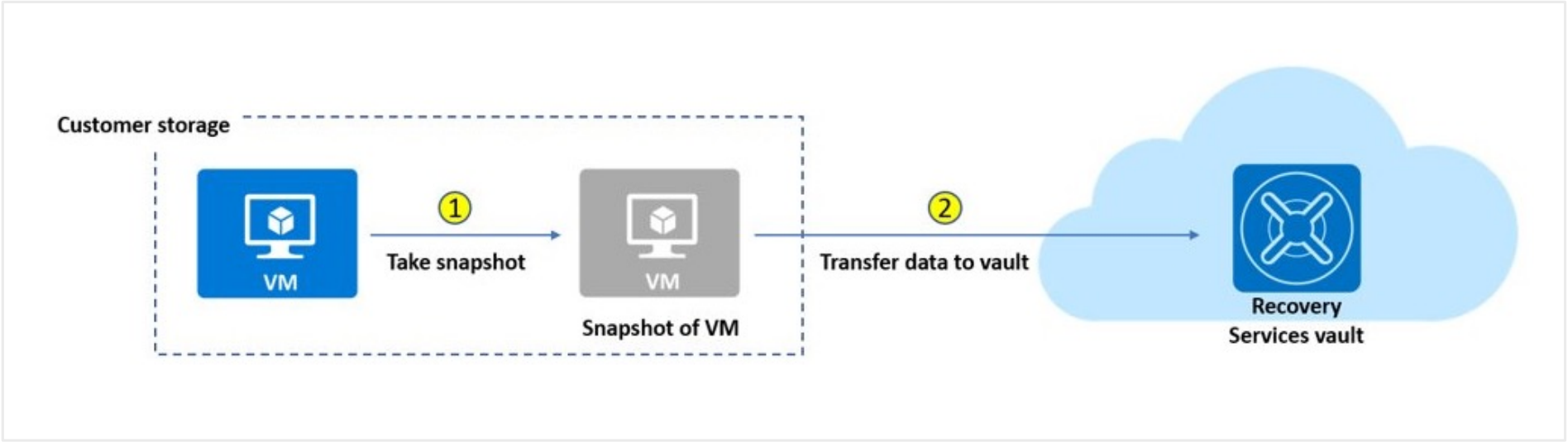
How often is the workload is backed up?

What types of backups are being done?

Is disaster recovery protection in place?



Virtual Machine Snapshots



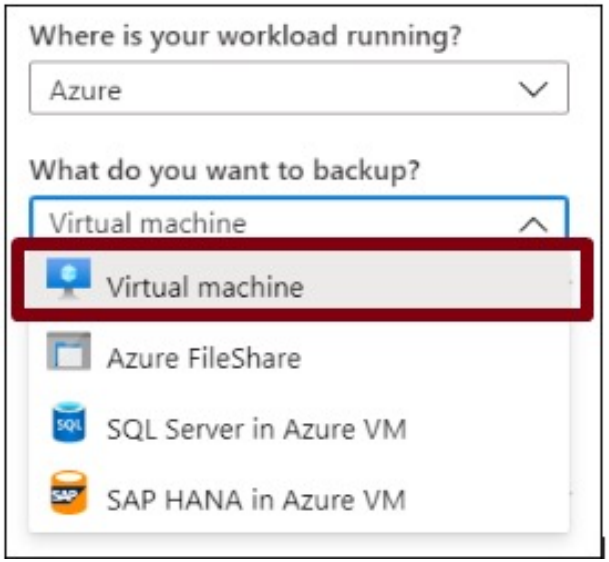
Use snapshots taken as part of a backup job

Reduces recovery wait times – don't wait for data transfer to the vault to finish

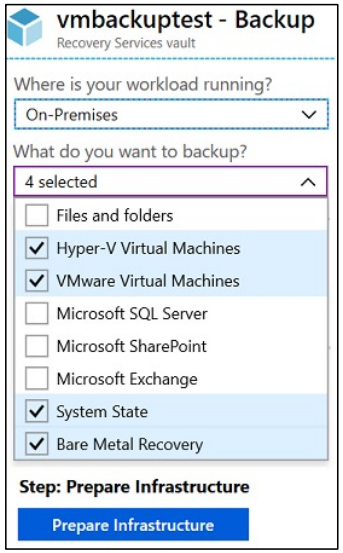
Configure Instant Restore retention (1 to 5 days)

Recovery Services Vault VM Backup Options

Azure Workloads

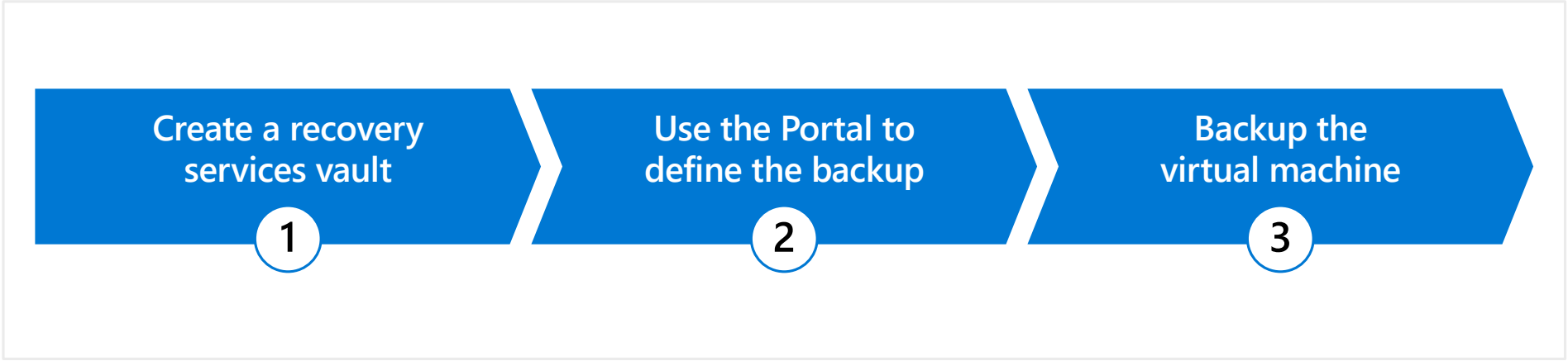


On-Premises Workloads



✓ Multiple servers can be protected using the same Recovery Services vault

Implementing VM Backups



1. Use a Recovery Services Vault in the region where you are performing your Virtual Machine backups and choose a replication strategy for Vault

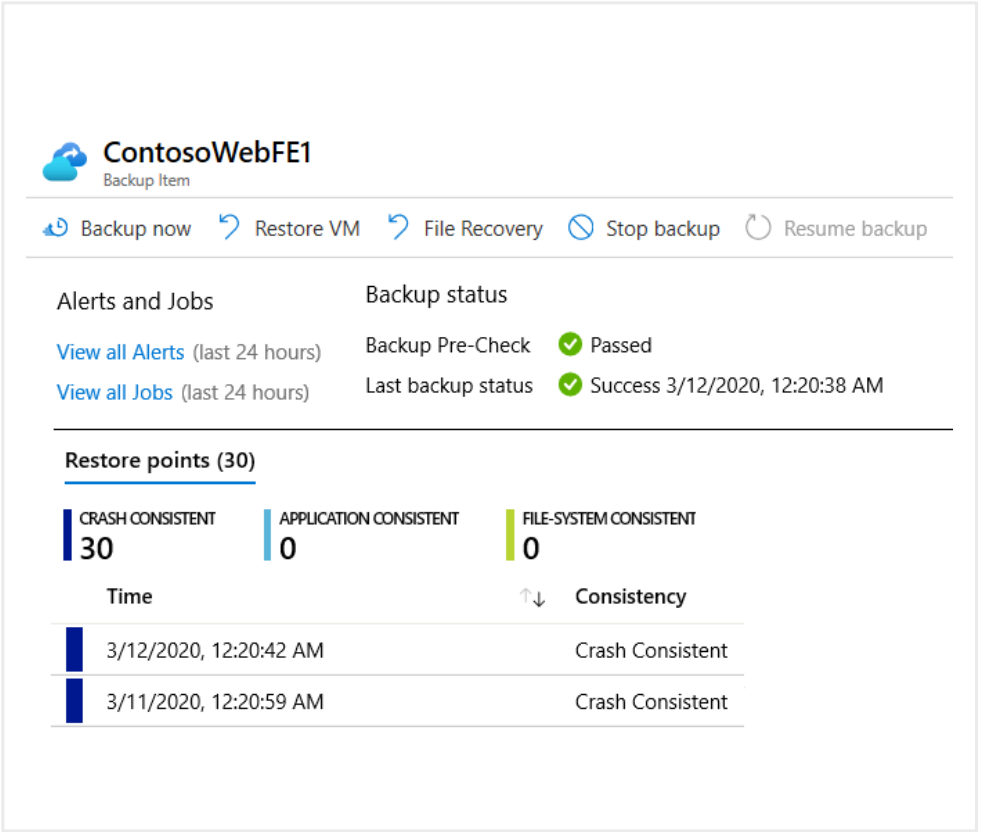
2. Take snapshots (recovery points) of your data at defined intervals. These snapshots are stored in recovery services vaults

3. For the Backup extension to work, the Azure VM Agent must be installed on the Azure virtual machine

Implementing VM Restore

Once you trigger the restore operation, the Backup service creates a job for tracking the restore operation

The Backup service also creates and temporarily displays notifications, so you monitor how the backup is proceeding



Azure Backup Server

App-aware backups, file/folder/volume backups, and machine state backups (bare-metal, system state)

Each machine runs the DPM/MABS protection agent, and the MARS agent runs on the MABS/DPM

Flexibility and granular scheduling options

Manage backups for multiple machines in a protection group

Backup Component Comparison

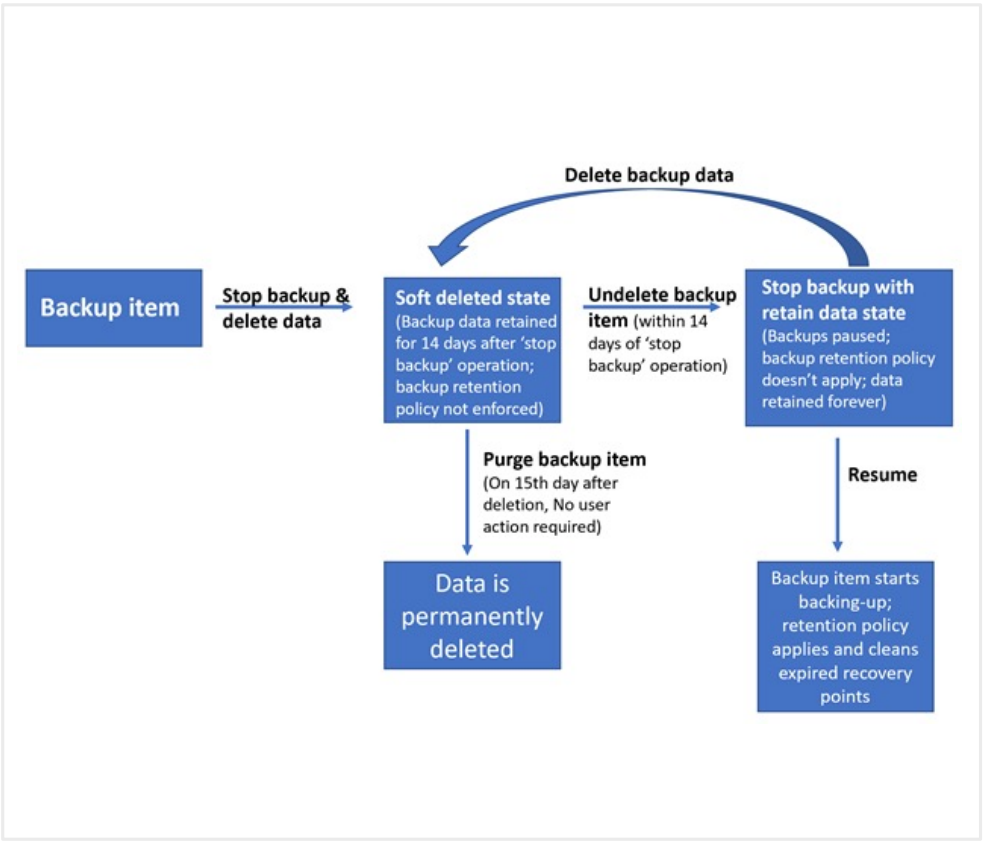
Component	Benefits	Limits	Protects	Backup Storage
Azure Backup (MARS) agent	• Backup files and folders on physical or virtual Windows OS • No separate backup server required	• Backup 3x per day • Not application aware • File, folder, and volume-level restore only • No support for Linux	• Files • Folders	• Recovery services vault
Azure Backup Server (MABS)	• App aware snapshots • Full flex for when to backups • Recovery granularity • Linux support on Hyper-V and VMware VMs • Backup and restore VMware VMs • Doesn't require a System Center license	• Cannot backup Oracle workloads • Always requires live Azure subscription • No support for tape backup	• Files • Folders • Volumes • VMs • Applications • Workloads	• Recovery services vault • Locally attached disk

Soft Delete

Backup data is retained for 14 additional days

Recover soft deleted backup items using an 'Undelete' operation

Natively built-in for all the recovery services vaults



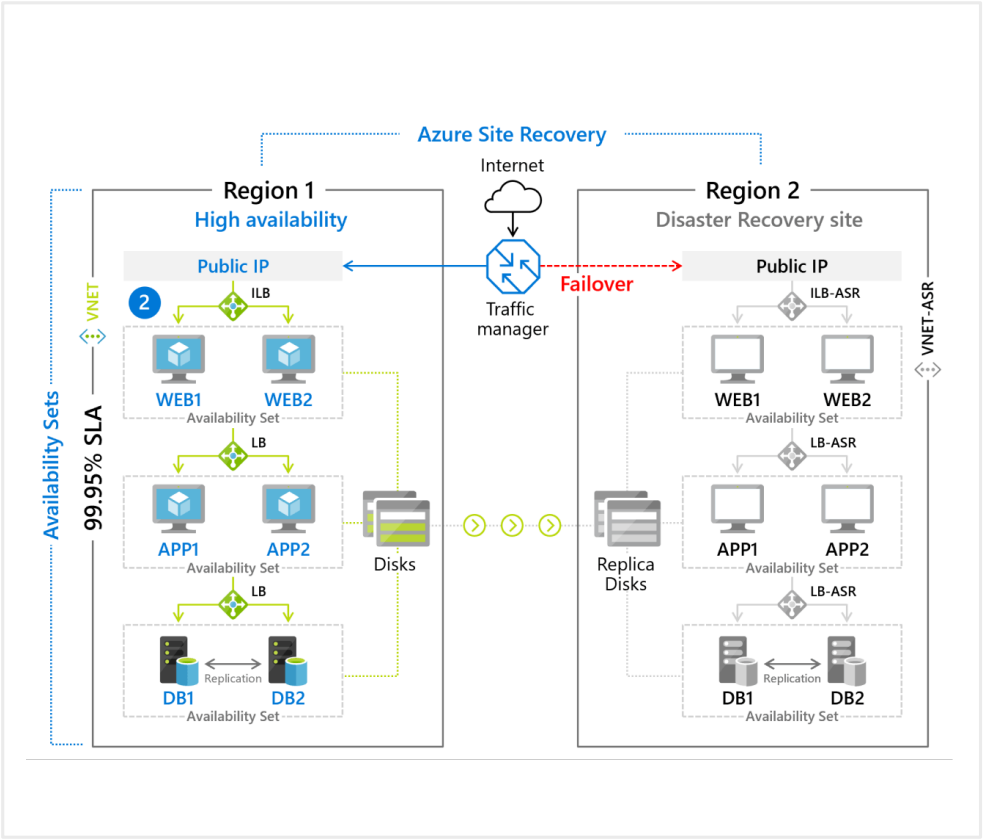
Azure Site Recovery

Replicate Azure VMs from one Azure region to another

Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure

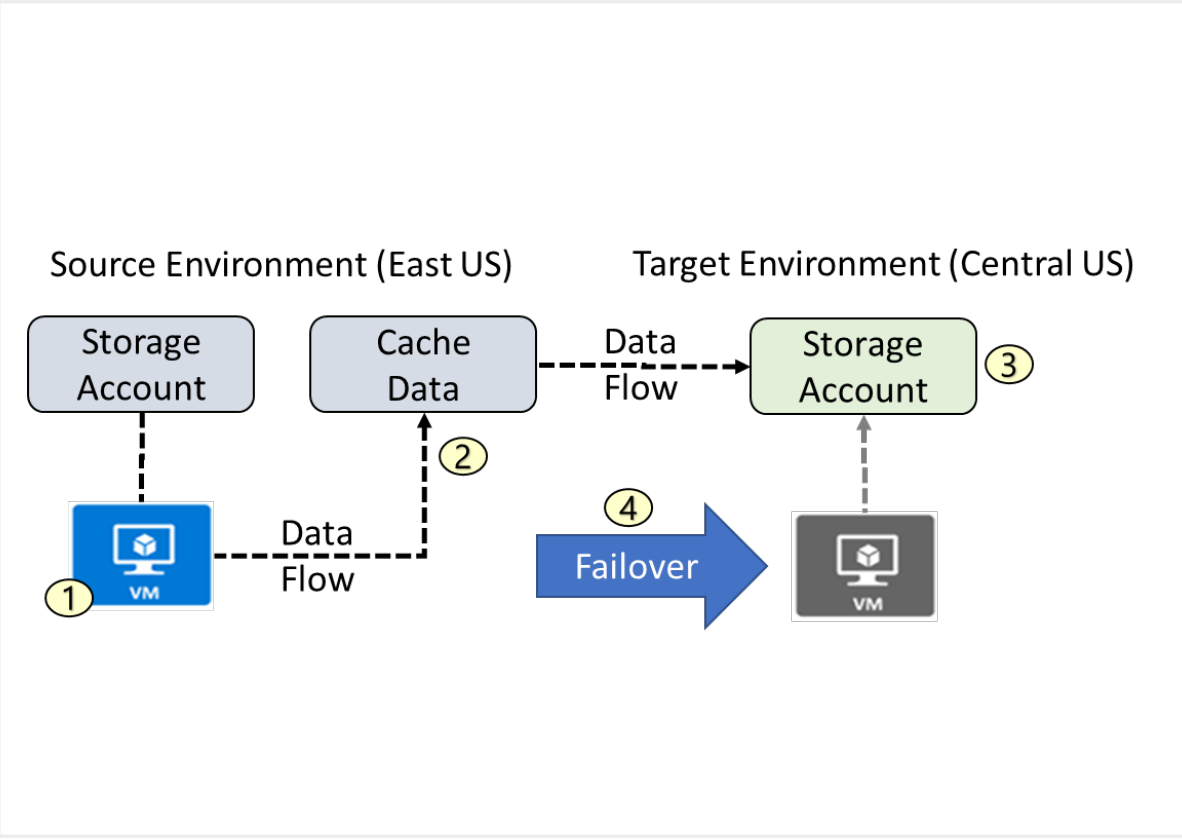
Replicate AWS Windows instances to Azure

Replicate on-premises VMware VMs, Hyper-V VMs managed by System Center VMM, and physical servers to a secondary site

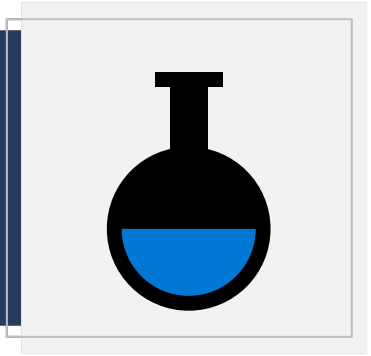


Azure to Azure Architecture

1. VM is registered with Azure Site Recovery
2. Data is continuously replicated to cache
3. Cache is replicated to the target storage account
4. During failover the virtual machine is added to the target environment



Lesson 03: Module 10 Lab and Review



Lab 10 – Backup virtual machines

Lab scenario

You have been tasked with evaluating the use of Azure Recovery Services for backup and restore of files hosted on Azure virtual machines and on-premises computers. In addition, you want to identify methods of protecting data stored in the Recovery Services vault from accidental or malicious data loss

Objectives

Task 1:
Provision the lab environment

Task 2:
Create a Recovery Services vault

Task 3:
Implement Azure virtual machine-level backup

Task 4:
Implement File and Folder backup

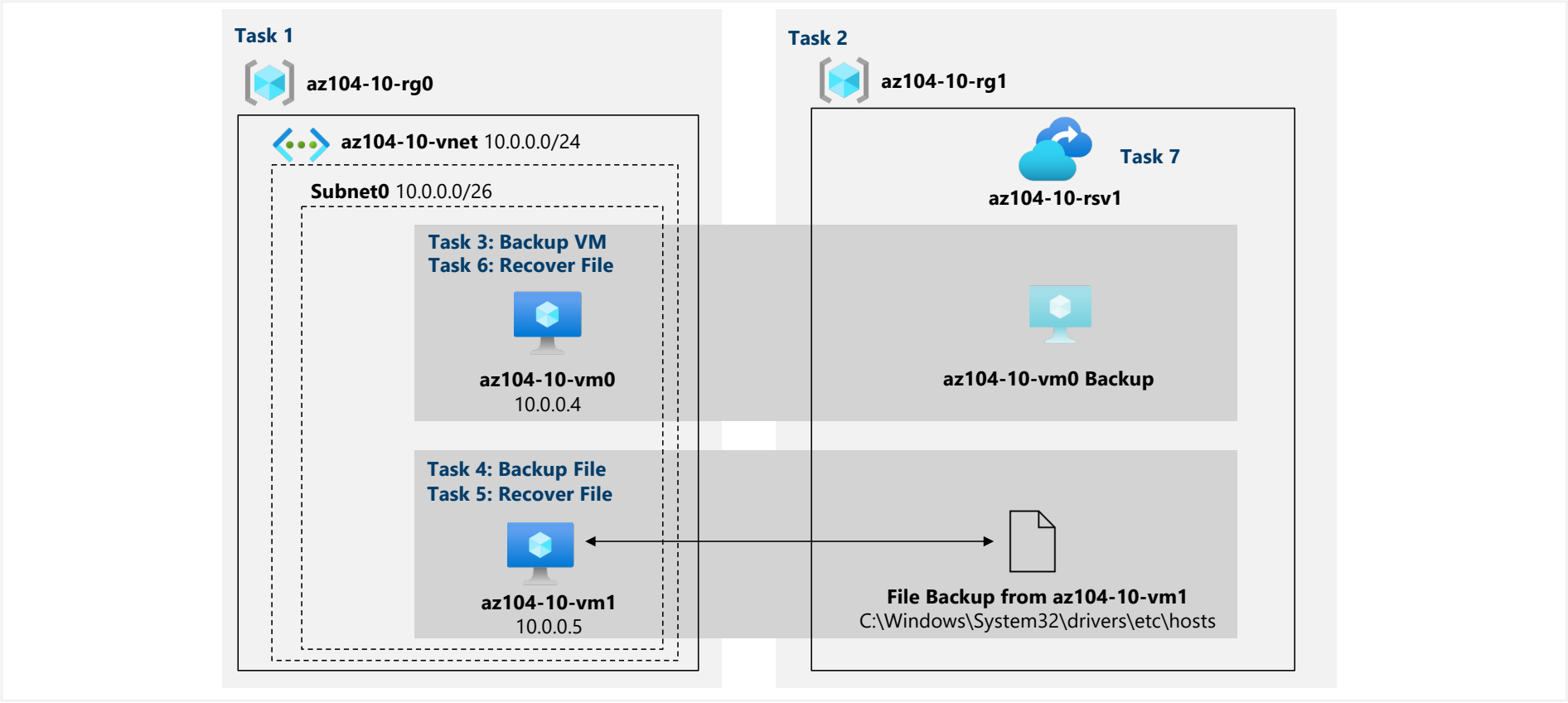
Task 5:
Perform file recovery by using Azure Recovery Services agent

Task 6:
Perform file recovery by using Azure virtual machine snapshots

Task 7:
Review the Azure Recovery Services soft delete functionality

Next slide for an architecture diagram

Lab 10 – Architecture diagram



Module Review

Module Review Questions	Microsoft Learn Modules (docs.microsoft.com/Learn)
	Protect your virtual machines by using Azure Backup
	Back up and restore your Azure SQL database
	Protect your Azure infrastructure with Azure Site Recovery
	Protect your on-premises infrastructure from disasters with Azure Site Recovery

End of presentation