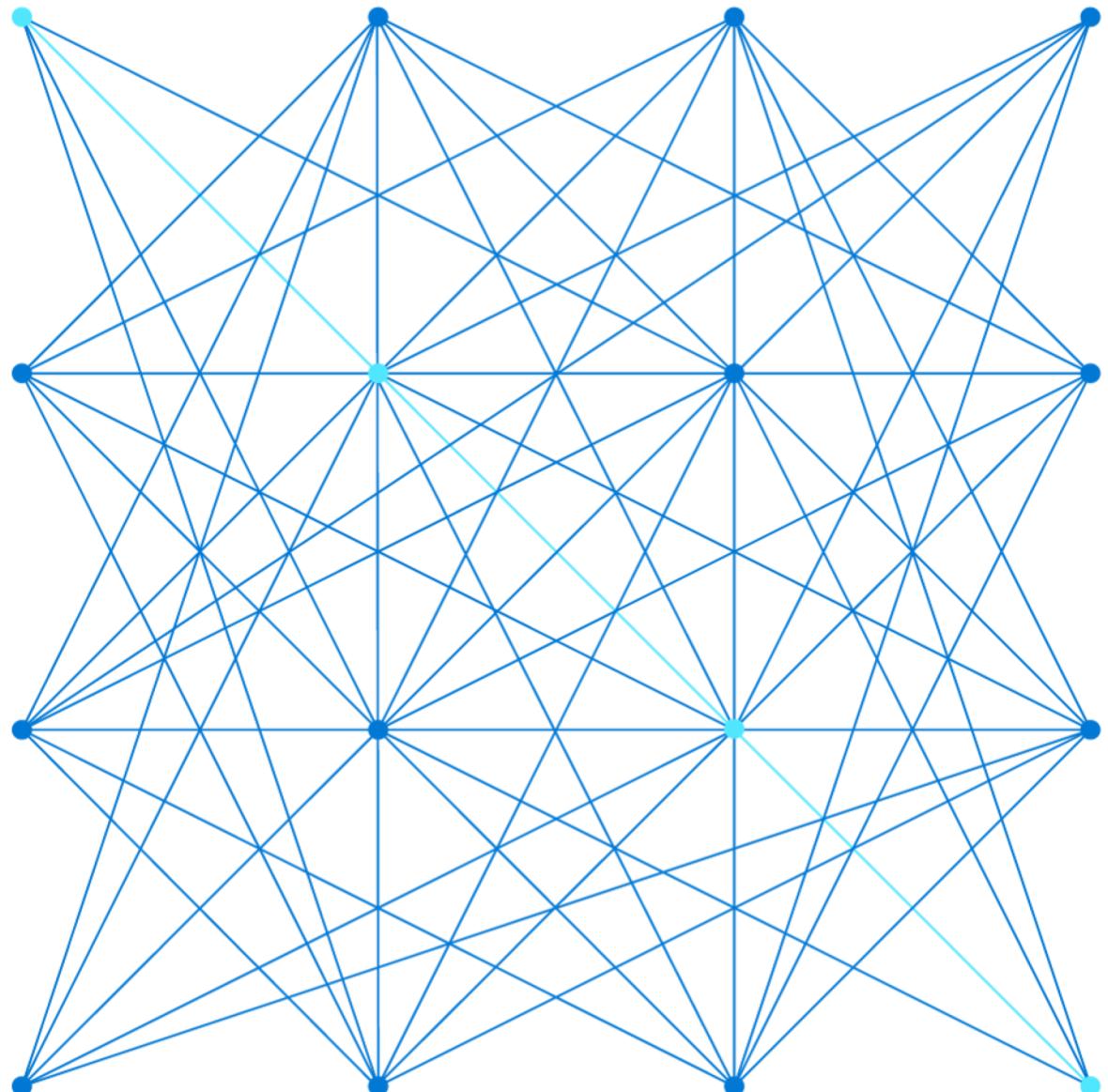


# AZ-104T00A

## Administer Data Protection



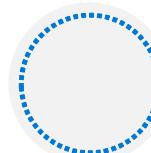
Administer  
Network  
Protection  
Introduction



Configure File and Folder Backups



Configure Virtual Machine Backups



Lab 10 – Implement Data Protection

# Configure File and Folder Backups



# Configure File and Folder Backups

## Introduction

-  Describe Azure Backup Benefits
-  Implement Azure Backup Center
-  Setup Recovery Service Vault Backup Options
-  Demonstration – Backup Azure File Shares
-  Configure On-premises File and Folder Backups
-  Manage the Microsoft Azure Recovery Services Agent
-  Demonstration – Backup Files and Folders
-  Summary and Resources

# Describe Azure Backup Benefits



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

# Implement Azure Backup Center

Single pane of glass to manage backups across a large and distributed Azure environment

Data source-centric management focused on what you are backing up

Connected experiences with native integrations that enables management at scale

The screenshot shows the Azure Backup center interface. The left sidebar includes links for Overview, Getting started, Community, Manage (Backup instances, Backup policies, Vaults), Monitoring + reporting (Backup jobs, Backup reports), Policy and compliance (Backup compliance, Azure policies for backup, Protectable datasources), Support + troubleshooting (New support request), and a search bar.

The main content area displays the following information:

- Datasource type: Azure Virtual machines**: Overview of Jobs and Backup instances.
- Jobs (last 24 Hours)**: A table showing the count of Failed, In progress, and Completed operations for Scheduled backup, On-demand backup, and Restore.
- Backup instances**: Summary for Azure Virtual machines, showing 2 protection configured, 0 protection stopped, and 0 soft deleted.
- Azure Virtual machines**: Details for 2 backup instances, showing Protection configured (2), Protection stopped (0), and Soft deleted (0).
- Support + troubleshooting**: Shows 0 out of 2 new support requests.

# Setup Recovery Services Vault Backup Options - Files

## Azure Workloads

Where is your workload running?

Azure

What do you want to backup?

Virtual machine

Virtual machine

Azure FileShare

SQL Server in Azure VM

SAP HANA in Azure VM

## On-Premises Workloads

vmbackuptest- Backup  
Recovery Services vault

Where is your workload running?

On-Premises

What do you want to backup?

Files and folders

Files and folders

Hyper-V Virtual Machines

VMware Virtual Machines

Microsoft SQL Server

Microsoft SharePoint

Microsoft Exchange

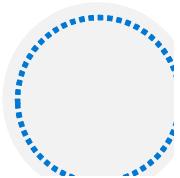
System State

Bare Metal Recovery

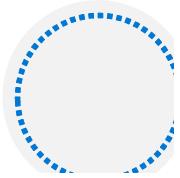
Step: Prepare Infrastructure

Prepare Infrastructure

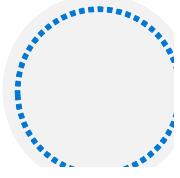
# Demonstration – Backup Azure File Shares



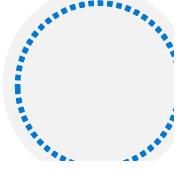
Configure a storage account with file share



Create a Recovery Services vault



Configure file share backup



Verify the file share backup

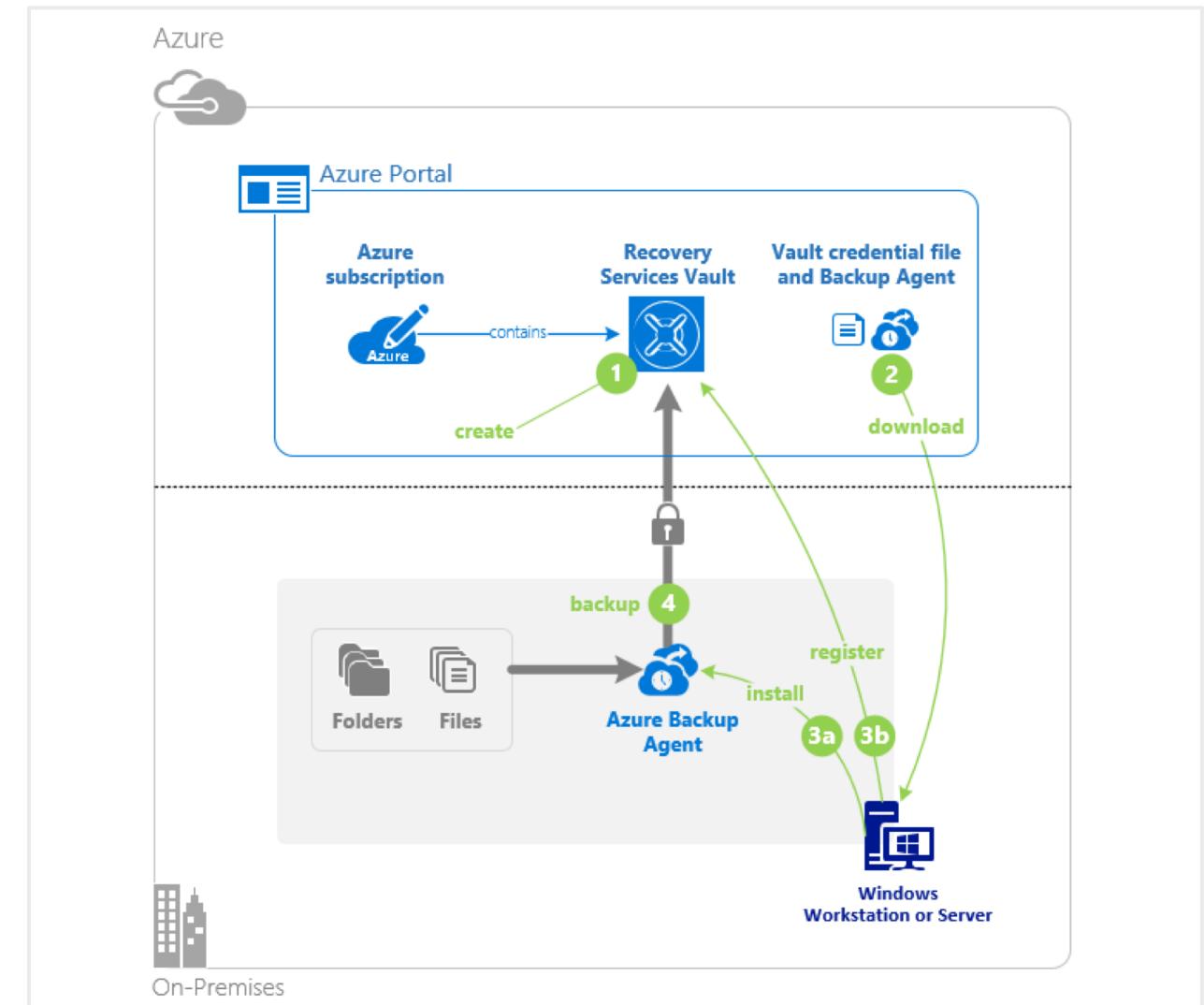
# Configure On-Premises File and Folder Backup

1. Create the recovery services vault

2. Download the agent and credential file

3. Install and register agent

4. Configure the backup



# Manage the Microsoft Azure Recovery Services Agent

The screenshot shows the Microsoft Azure Backup interface. On the left, there's a message about scheduled backups and a warning that backups have not been configured for the server. Below that is a table of recent jobs (Activity in the past 7 days). The table has columns for Status, Time, Message, and Description. There are three completed jobs listed:

Status	Time	Message	Description
✓	2/28/2019 6:48 AM	Recovery	Job completed.
✓	2/28/2019 6:45 AM	Recovery	Job completed.
✓	2/28/2019 6:41 AM	Backup	Job completed.

The right side features a vertical Actions pane with options like Backup, Register Server, Schedule Backup, Recover Data, Change Properties, Open Portal, Privacy & Cookies, View, and Help.

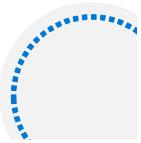
Backup or recover files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure)

No separate backup server required

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

No support for Linux

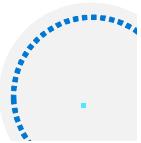
# Demonstration – Backup Files and Folders



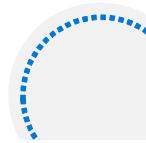
Create a Recovery Services vault



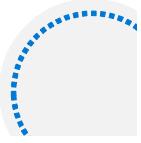
Backup files and folders



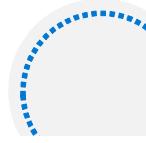
Configure the vault



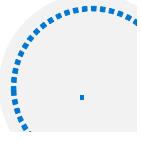
Explore the recover settings



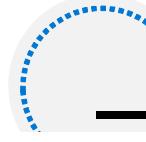
Install and register the agent



Explore the backup properties



Create the backup policy



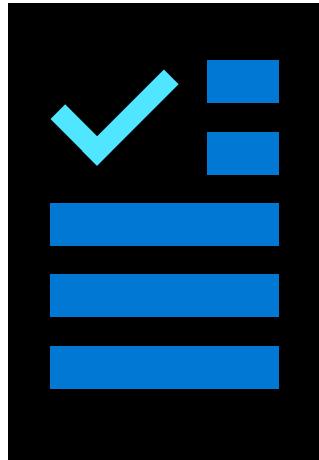
Delete your backup schedule

# Summary and Resources – Configure File and Folder Backups

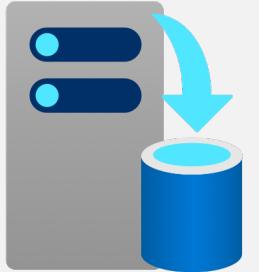
Knowledge Check Questions

Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))

[Introduction to Azure Backup](#)



# Configure Virtual Machine Backups



# Configure Virtual Machine Backups Introduction

-  Protect Virtual Machine Data
-  Create Virtual Machine Snapshots
-  Setup Recovery Services Vault Backup Options
-  Backup Virtual Machines
-  Restore Virtual Machines
-  Demonstration – Virtual Machine Backups
-  Implement Azure Backup Server
-  Compare Backup Options
-  Manage Soft Delete
-  Implement Azure Site Recovery
-  Summary and Resources

# Protect Virtual Machine Data

Snapshots

Azure backup

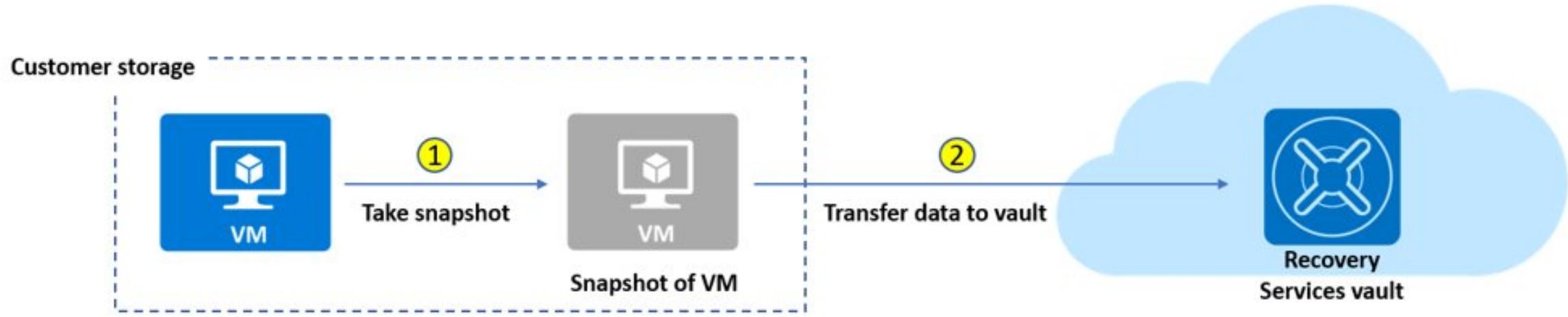
Azure Site Recovery

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

# Create Virtual Machine Snapshots



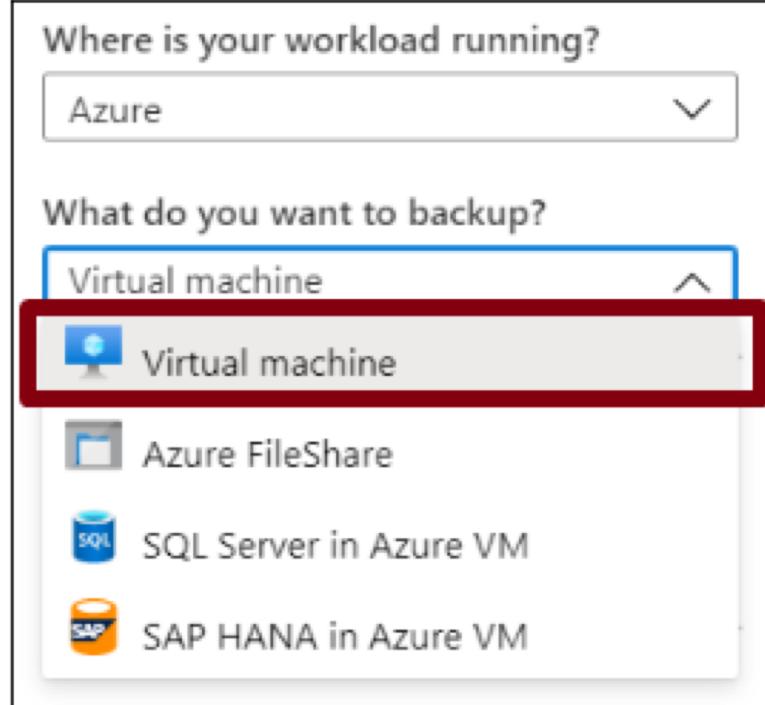
Use snapshots taken as part of a backup job

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

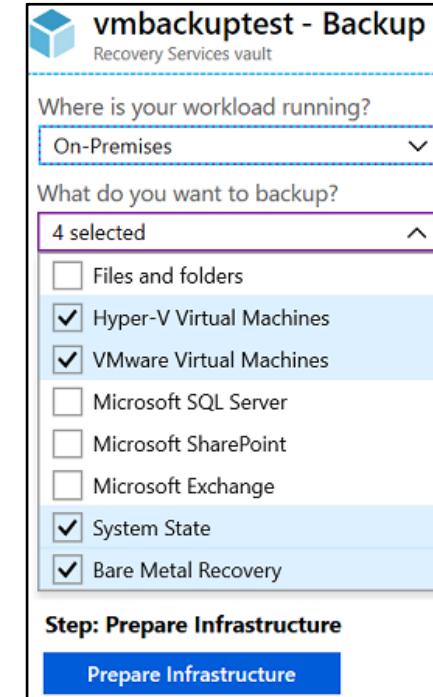
Configure Instant Restore retention  
(1 to 5 days)

# Setup Recovery Services Vault Backup Options - VMs

## Azure Workloads



## On-Premises Workloads



Multiple servers can be protected using the same Recovery Services vault

# Backup Virtual Machines

Create a recovery services vault

1

Use the Portal to define the backup

2

Backup the virtual machine

3

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

# Restore Virtual Machines

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

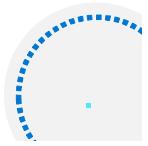
The screenshot shows the Azure Backup service interface for a backup item named 'ContosoWebFE1'. At the top, there are several action buttons: 'Backup now', 'Restore VM', 'File Recovery', 'Stop backup', and 'Resume backup'. Below these are two main sections: 'Alerts and Jobs' and 'Backup status'. Under 'Alerts and Jobs', there are links to 'View all Alerts' (last 24 hours) and 'View all Jobs' (last 24 hours). Under 'Backup status', it shows 'Backup Pre-Check' as 'Passed' and 'Last backup status' as 'Success 3/12/2020, 12:20:38 AM'. A horizontal line separates this from the 'Restore points (30)' section. This section includes three summary counts: 'CRASH CONSISTENT' (30), 'APPLICATION CONSISTENT' (0), and 'FILE-SYSTEM CONSISTENT' (0). It also includes a 'Time' column (with entries '3/12/2020, 12:20:42 AM' and '3/11/2020, 12:20:59 AM') and a 'Consistency' column (both entries are 'Crash Consistent').

# Demonstration – Virtual Machine Backups



Enable a backup on a virtual machine

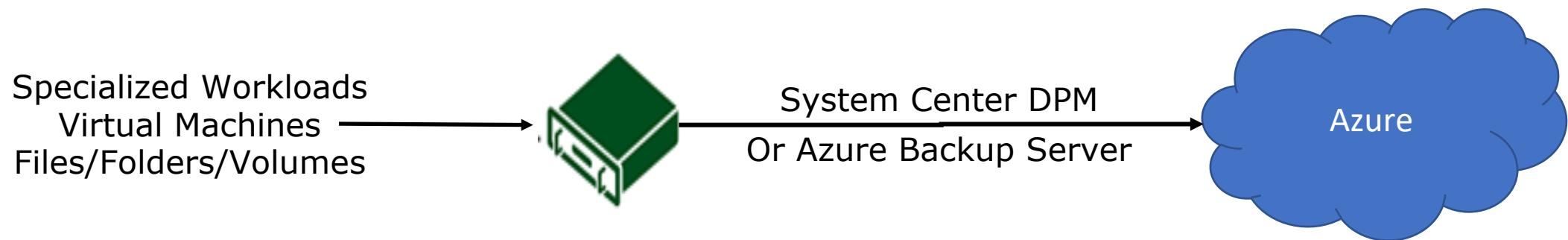
---



Start a backup job and monitor the progress

---

# Implement 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

# Compare Backup Options

Component	Benefits	Limits	Protects	Backup Storage
Azure Backup (MARS) agent	<ul style="list-style-type: none"><li>Backup files and folders on physical or virtual Windows OS</li><li>No separate backup server required</li></ul>	<ul style="list-style-type: none"><li>Backup 3x per day</li><li>Not application aware</li><li>File, folder, and volume-level restore only</li><li>No support for Linux</li></ul>	<ul style="list-style-type: none"><li>Files</li><li>Folders</li></ul>	<ul style="list-style-type: none"><li>Recovery services vault</li></ul>
Azure Backup Server (MABS)	<ul style="list-style-type: none"><li>App aware snapshots</li><li>Full flex for when to backups</li><li>Recovery granularity</li><li>Linux support on Hyper-V and VMware VMs</li><li>Backup and restore VMware VMs</li><li>Doesn't require a System Center license</li></ul>	<ul style="list-style-type: none"><li>Cannot backup Oracle workloads</li><li>Always requires live Azure subscription</li><li>No support for tape backup</li></ul>	<ul style="list-style-type: none"><li>Files</li><li>Folders</li><li>Volumes</li><li>VMs</li><li>Applications</li><li>Workloads</li></ul>	<ul style="list-style-type: none"><li>Recovery services vault</li><li>Locally attached disk</li></ul>

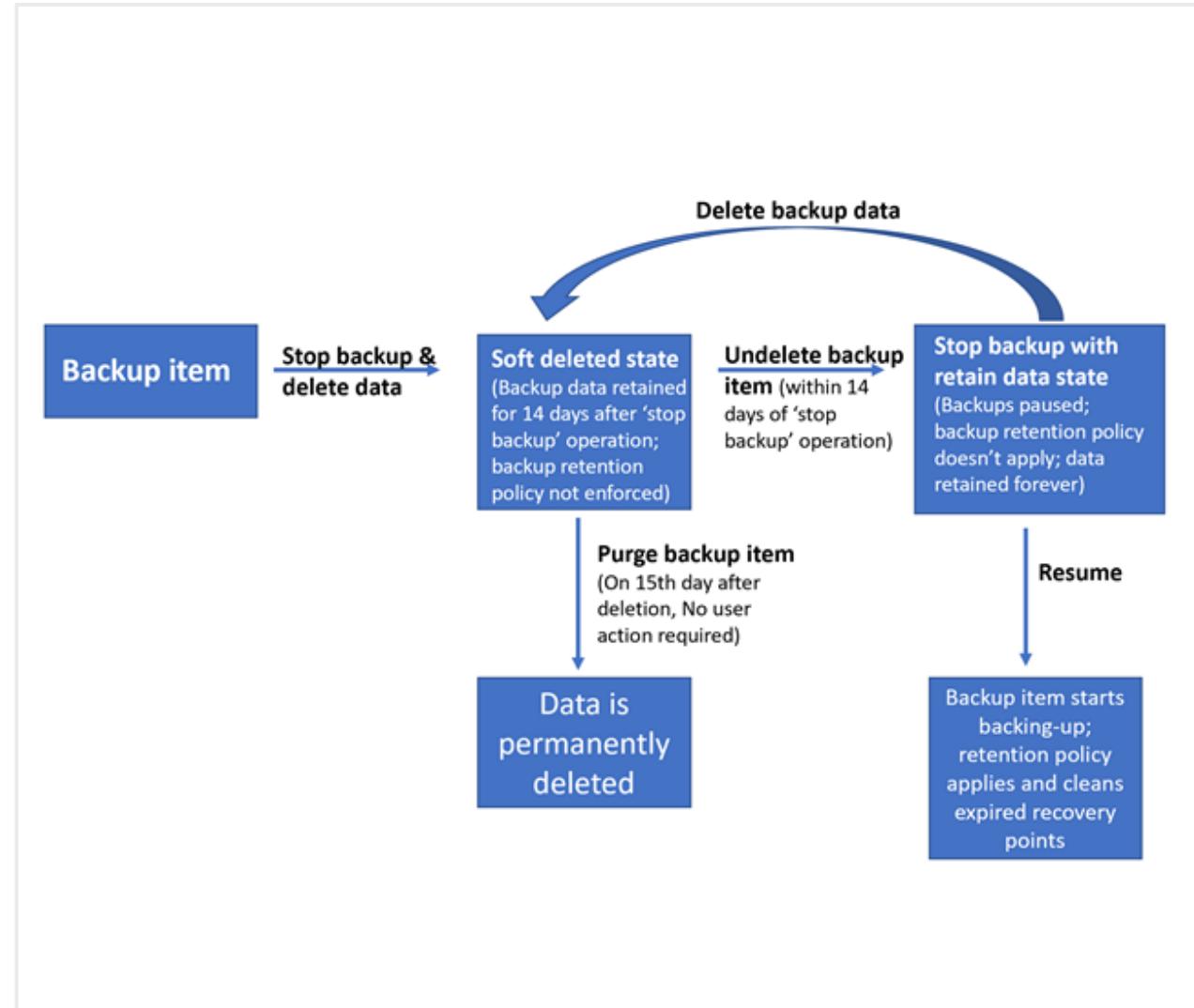
# Manage Soft Delete

Backup data is retained for 14 additional days

Recover soft deleted backup items using an 'Undelete' operation

Also available for storage account containers and file shares

Natively built-in for all the recovery services vaults



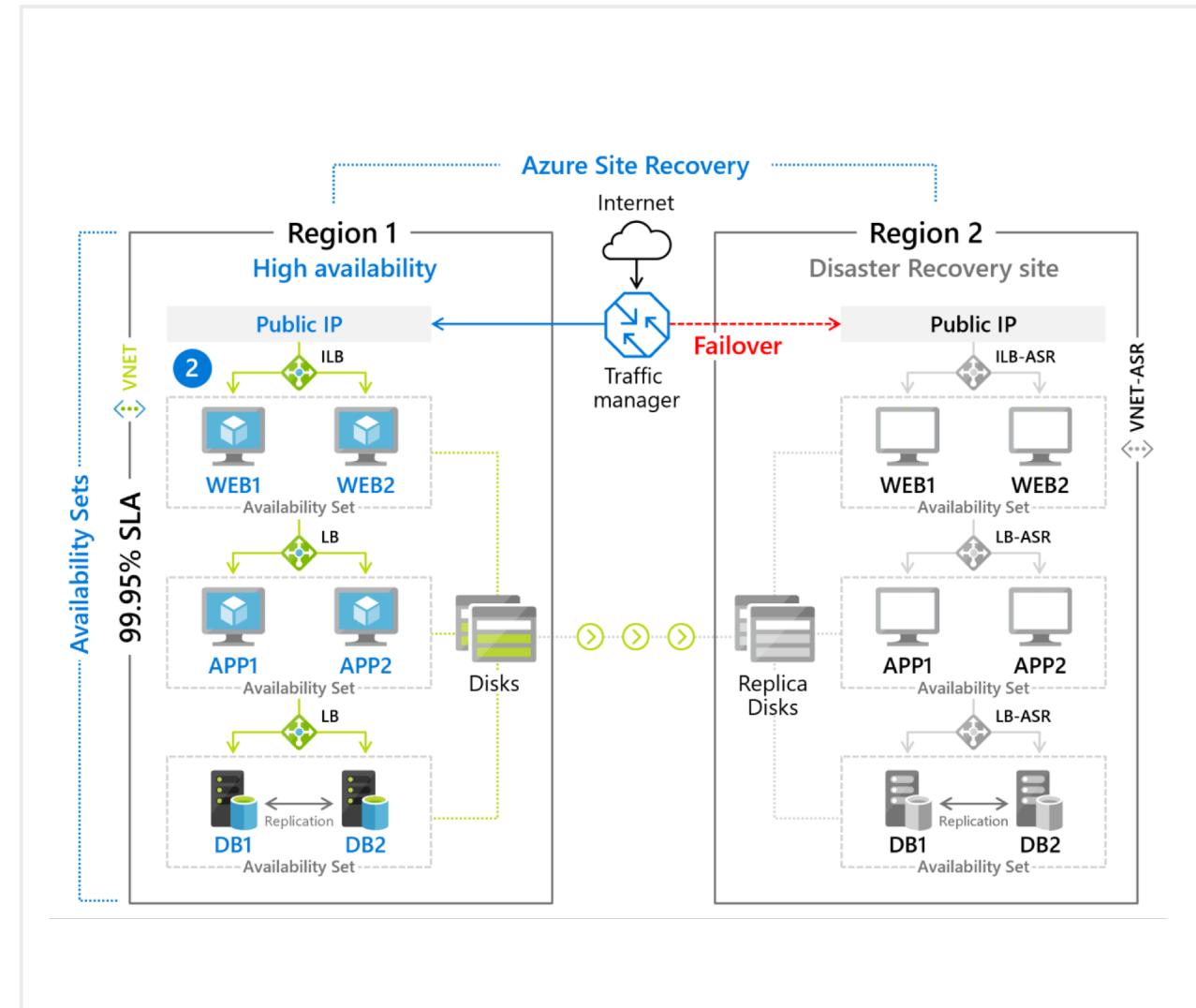
# Implement Azure Site Recovery

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

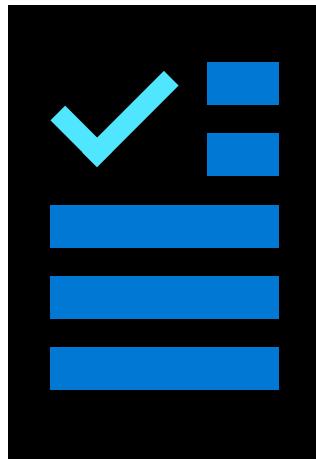
Replicate AWS Windows instances to Azure

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



# Summary and Resources – Configure Virtual Machine Backups

## Knowledge Check Questions



## Microsoft Learn Modules ([docs.microsoft.com/Learn](https://docs.microsoft.com/Learn))

[Introduction to Azure Backup](#)

---

[Protect your virtual machines by using Azure Backup](#)

---

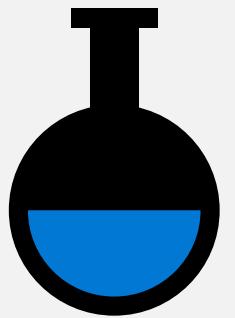
[Implement hybrid backup and recovery with Windows Server IaaS](#)

---

[Protect your Azure infrastructure with Azure Site Recovery](#)

---

# Lab 10 – Implement Data Protection



# 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

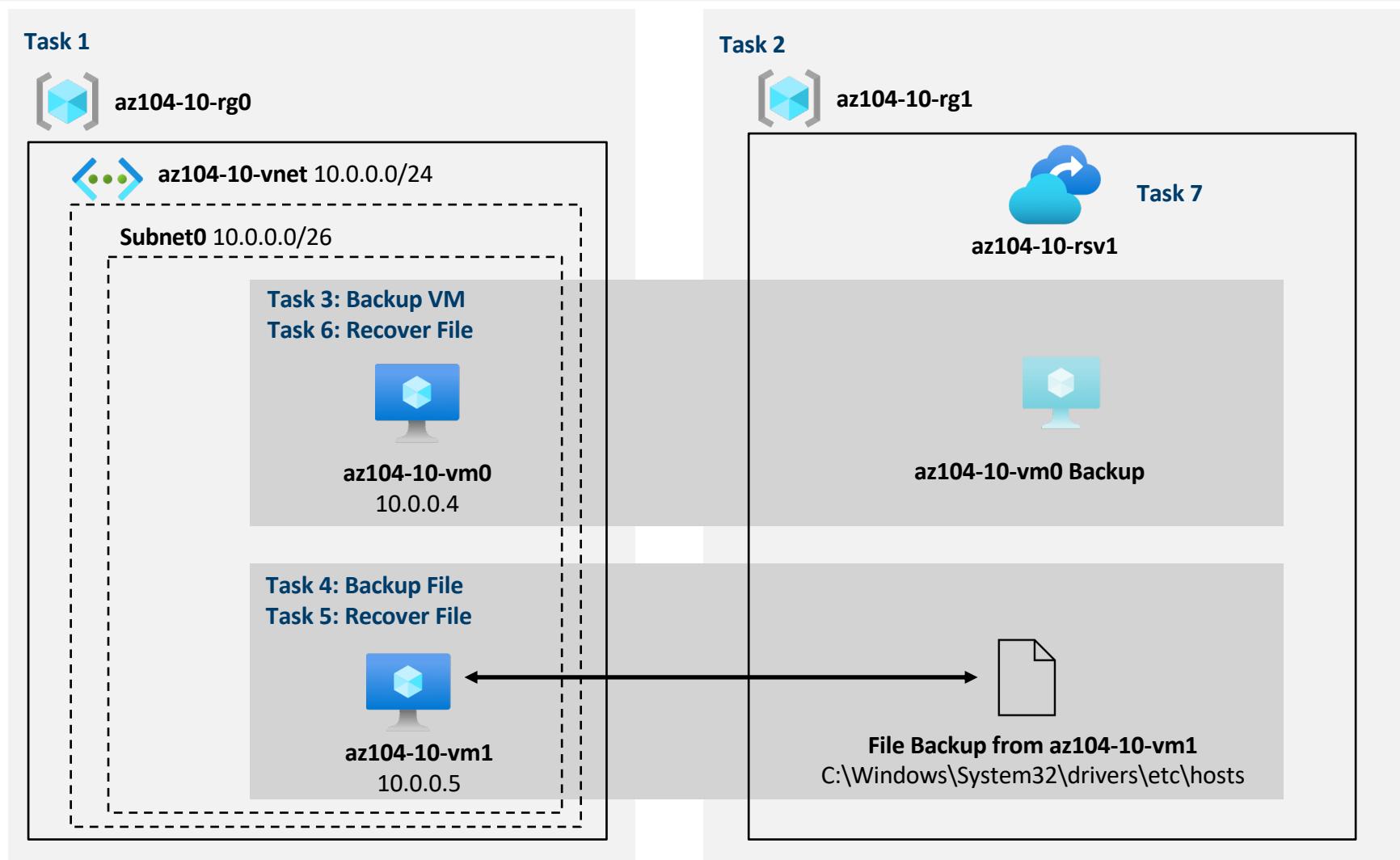
**Task 6:**  
Perform file recovery by using Azure virtual machine snapshots

**Task 7:**  
Review the Azure Recovery Services soft delete functionality

Next slide for an architecture diagram



# Lab 10 – Architecture diagram



End of presentation

