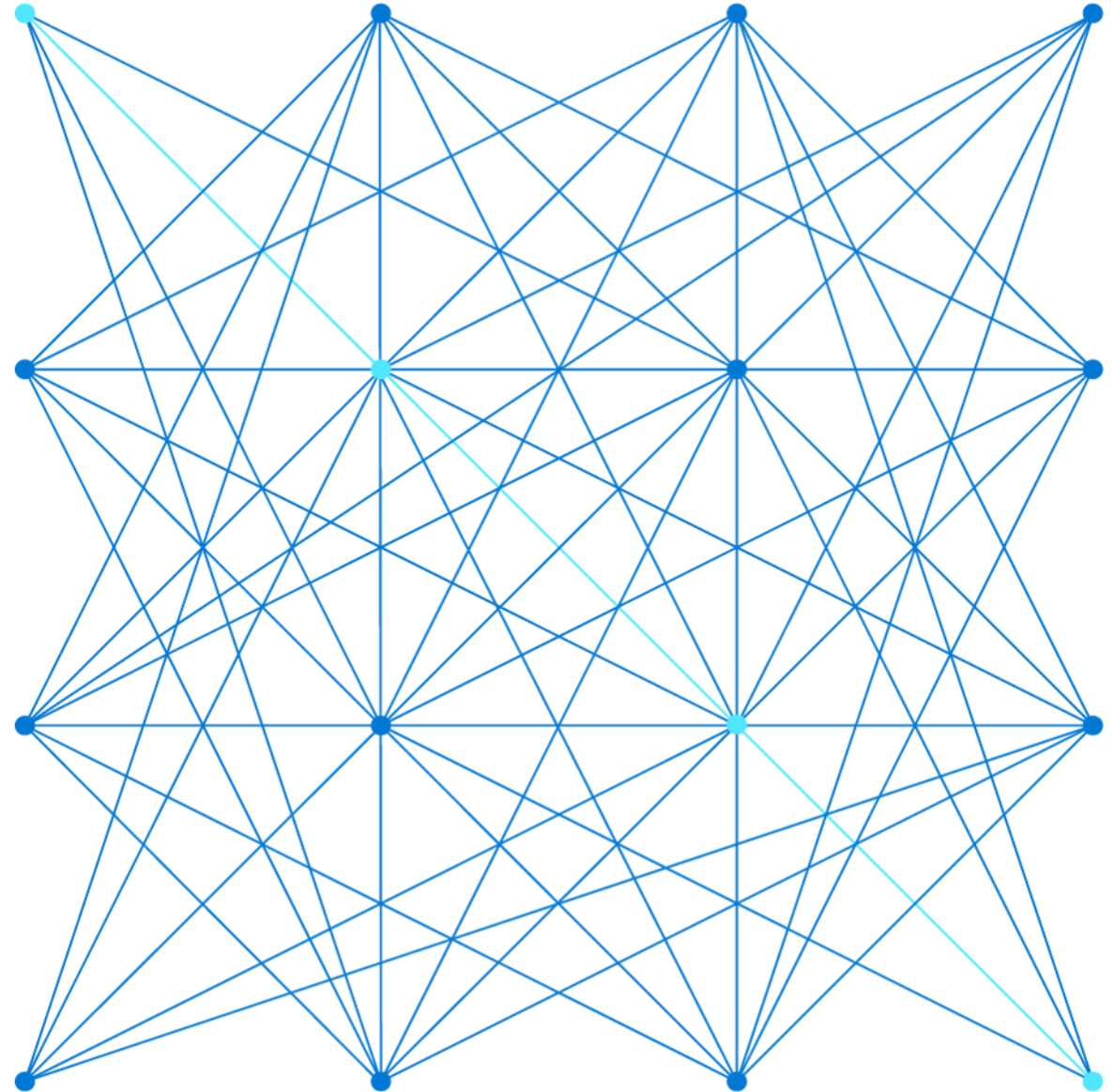


# AZ-104

## Administer Data Protection

10)



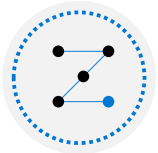
AZ-104

## About this course: Course Outline



01: Administer Identity

---



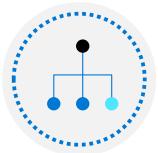
02: Administer Governance and Compliance

---



03: Administer Azure Resources

---



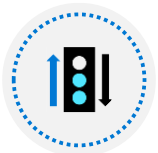
04: Administer Virtual Networking

---

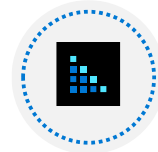


05: Administer Intersite Connectivity

---

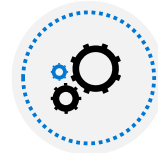


06: Administer Network Traffic Management



07: Administer Azure Storage

---



08: Administer Azure Virtual Machines

---



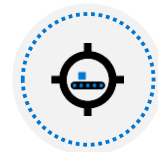
09: Administer PaaS Compute Options

---



10: Administer Data Protection

---



11: Administer Monitoring

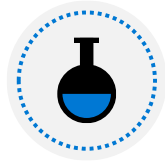
# Administer Network Protection Introduction



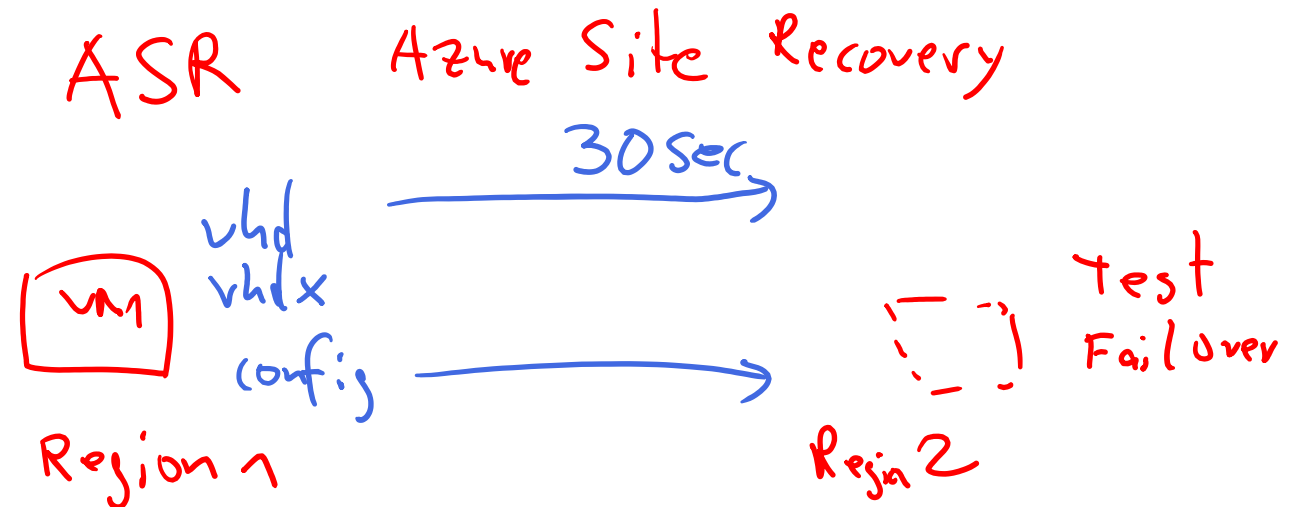
[Configure File and Folder Backups](#)



[Configure Virtual Machine Backups](#)







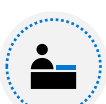
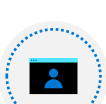


[Lab 10 – Implement Data Protection](#)



# 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



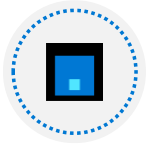
Azure-based service used to back up and restore data in Microsoft cloud

---



Automatic Storage Management

---



Multiple storage options *LRS*

---



Unlimited data transfer

---



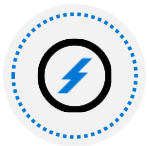
Data encryption *Bring your own key*

---



Application consistent backup

---



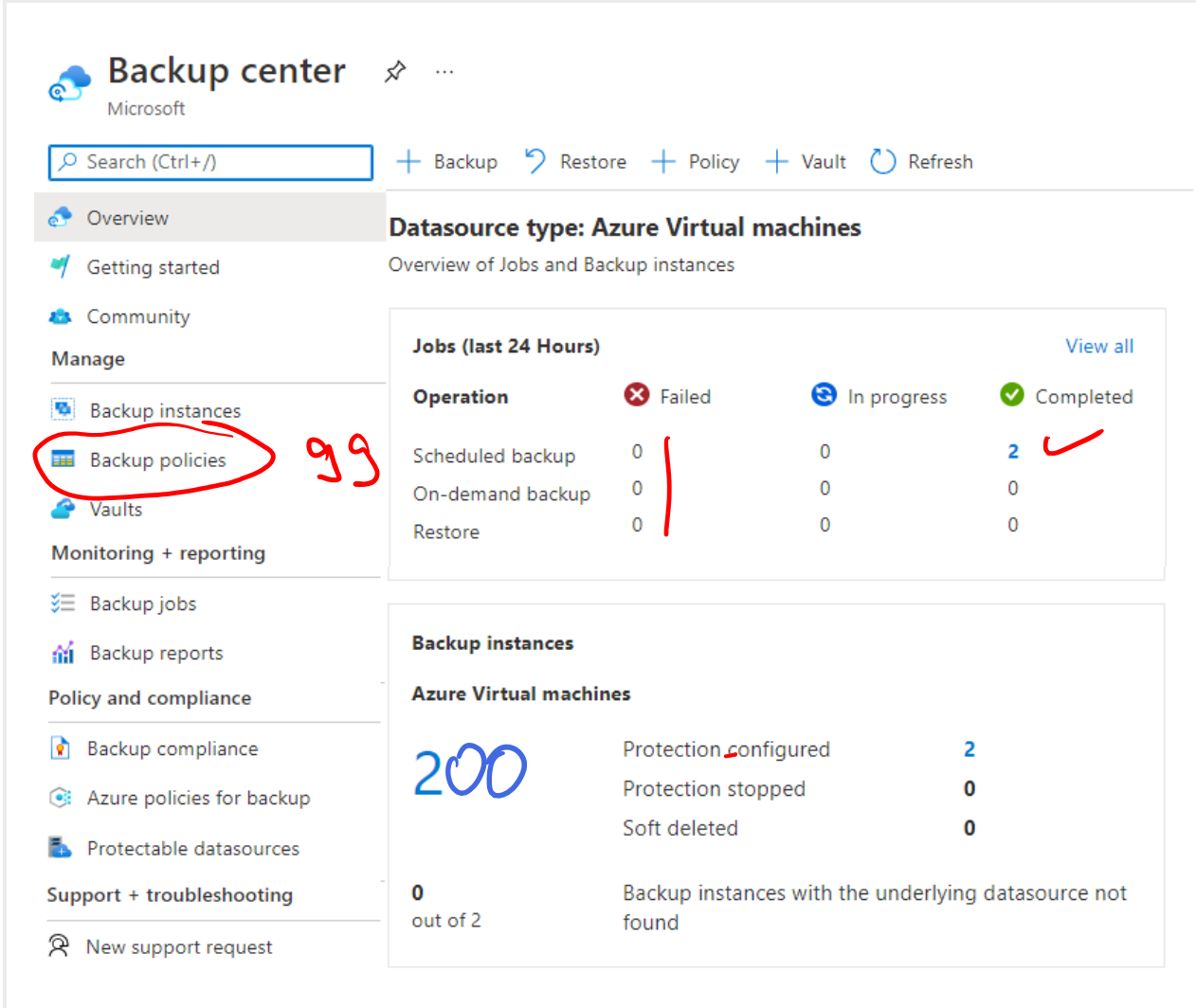
Long-term retention *1 Jahr  
2 5 10 20 99 Policy*

# Implement Azure Backup Center

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

Datasource-centric management focused on what you are backing up

Connected experiences with native integrations that enables management at scale



The screenshot displays the Azure Backup Center dashboard. The left-hand navigation pane includes sections for Overview, Getting started, Community, Manage (with sub-items: Backup instances, Backup policies, and Vaults), Monitoring + reporting (with sub-items: Backup jobs, Backup reports, and Policy and compliance), and Support + troubleshooting (with sub-item: New support request). The 'Backup policies' item is circled in red, with the handwritten number '99' next to it. The main content area is titled 'Backup center' and 'Microsoft'. It features a search bar and navigation links for Backup, Restore, Policy, Vault, and Refresh. The 'Datasource type: Azure Virtual machines' section provides an overview of jobs and backup instances. A table titled 'Jobs (last 24 Hours)' shows the status of various operations: Scheduled backup (0 Failed, 0 In progress, 2 Completed), On-demand backup (0 Failed, 0 In progress, 0 Completed), and Restore (0 Failed, 0 In progress, 0 Completed). The 'Backup instances' section for 'Azure Virtual machines' shows 200 instances with 2 protection configured, 0 protection stopped, and 0 soft deleted. A summary at the bottom indicates 0 out of 2 backup instances with the underlying datasource not found.

Operation	Failed	In progress	Completed
Scheduled backup	0	0	2
On-demand backup	0	0	0
Restore	0	0	0

Backup instances	Protection configured	Protection stopped	Soft deleted
200	2	0	0

0 out of 2 Backup instances with the underlying datasource not found

# 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

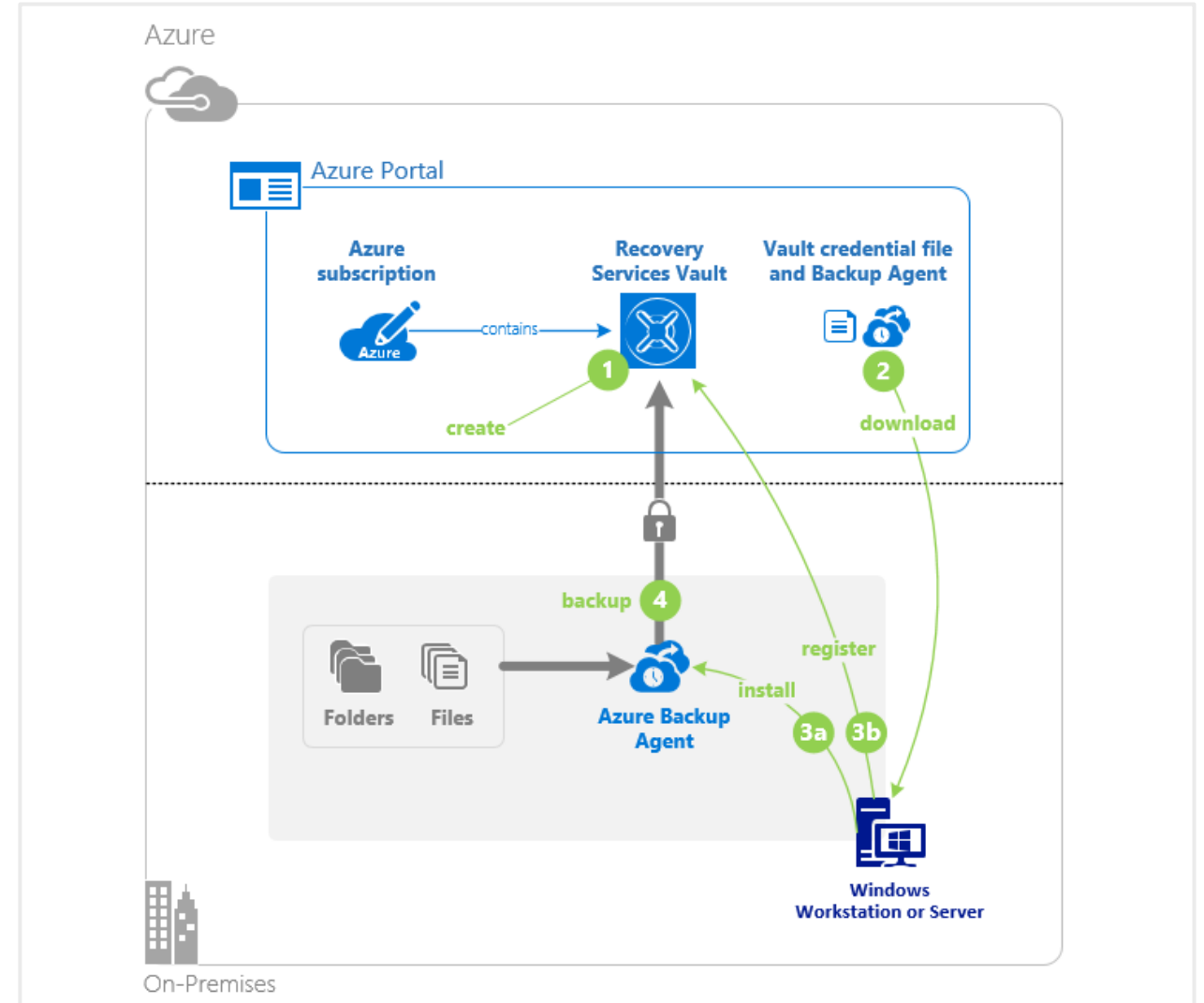
# Configure On-Premises File and Folder Backup

1. Create the recovery services vault

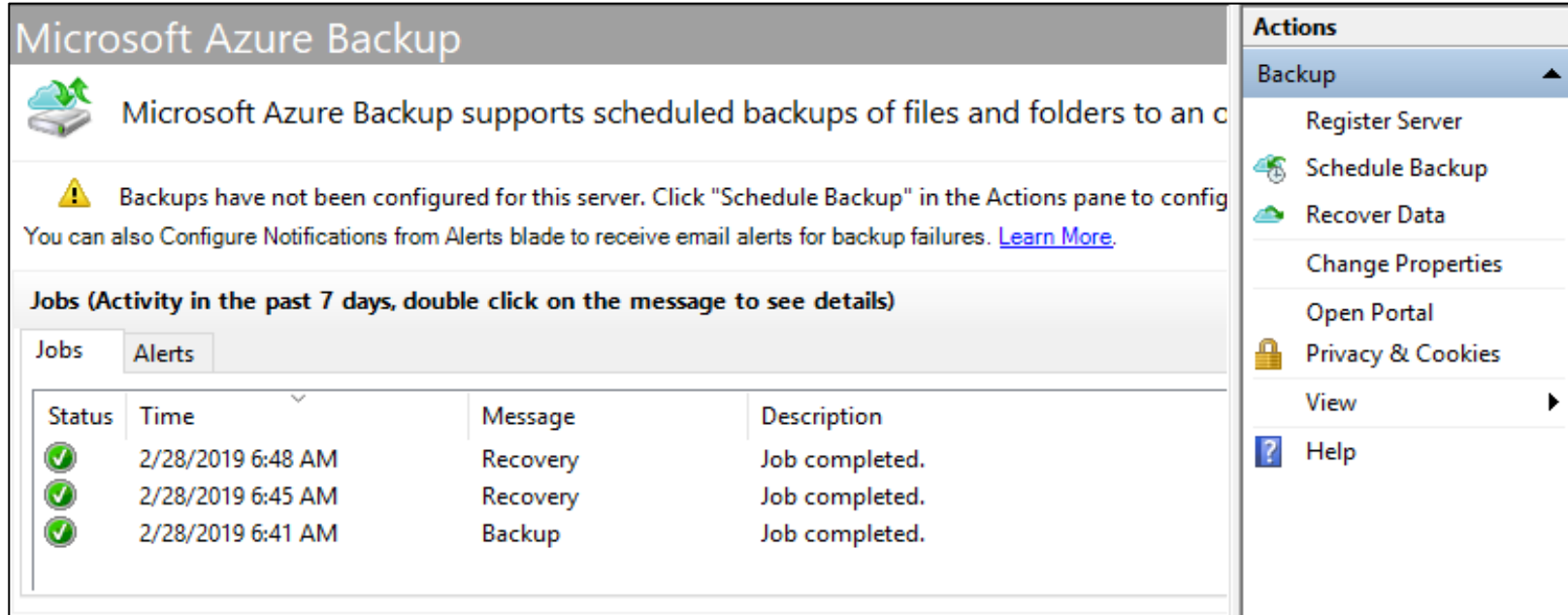
2. Download the agent and credential file

3. Install and register agent

4. Configure the backup



# Manage the Microsoft Azure Recovery Services Agent



**Microsoft Azure Backup**

Microsoft Azure Backup supports scheduled backups of files and folders to an cloud storage account.

**Warning:** Backups have not been configured for this server. Click "Schedule Backup" in the Actions pane to configure backups. You can also Configure Notifications from Alerts blade to receive email alerts for backup failures. [Learn More.](#)

**Jobs (Activity in the past 7 days, double click on the message to see details)**

Jobs Alerts

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.

**Actions**

- Backup
  - Register Server
  - Schedule Backup
  - Recover Data
  - Change Properties
  - Open Portal
  - Privacy & Cookies
  - View
- 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



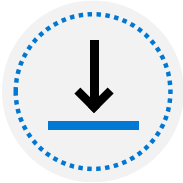
Create a Recovery Services vault

---



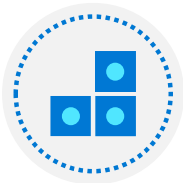
Configure the vault

---



Install and register the agent

---

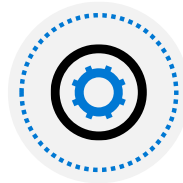


Create the backup policy



Backup files and folders

---



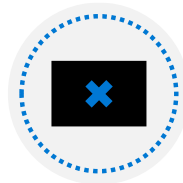
Explore the recover settings

---



Explore the backup properties

---



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](#)



Recovery Service Vault

Backup

Recovery

VM

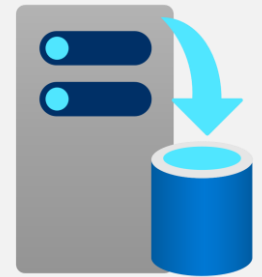
Azure Files

SAP HANA in VM

SQL in VM

ASR

# Configure Virtual Machine Backups









Backup Vault

VM

Blob

Postgre SQL

# 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**

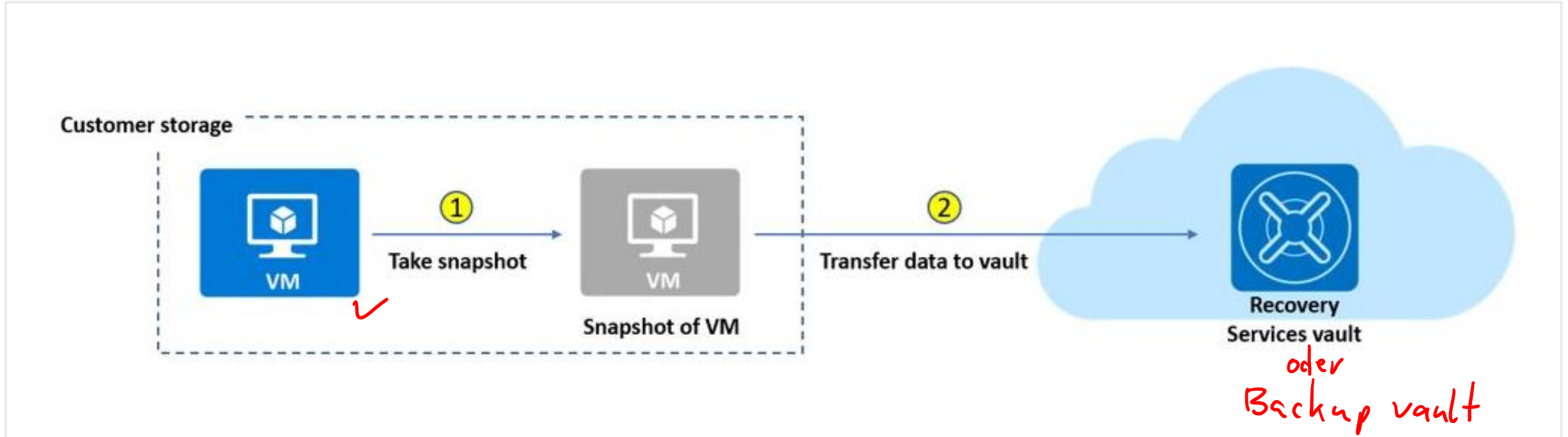
Managed snapshots provide a quick and simple option for backing up VMs that use Managed Disks

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

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?

4 selected

☐ 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



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

*Handwritten notes:* Vault Backup vhd Blob

**ContosoWebFE1**  
Backup Item

Backup now **Restore VM** File Recovery Stop backup Resume backup

Alerts and Jobs      Backup status

[View all Alerts](#) (last 24 hours)      Backup Pre-Check ✓ Passed

[View all Jobs](#) (last 24 hours)      Last backup status ✓ Success 3/12/2020, 12:20:38 AM

**Restore points (30)**

Time	Consistency
3/12/2020, 12:20:42 AM	Crash Consistent
3/11/2020, 12:20:59 AM	Crash Consistent

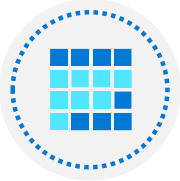
*Handwritten notes:* Notebook Z: download

# Demonstration – Virtual Machine Backups



Enable a backup on a virtual machine

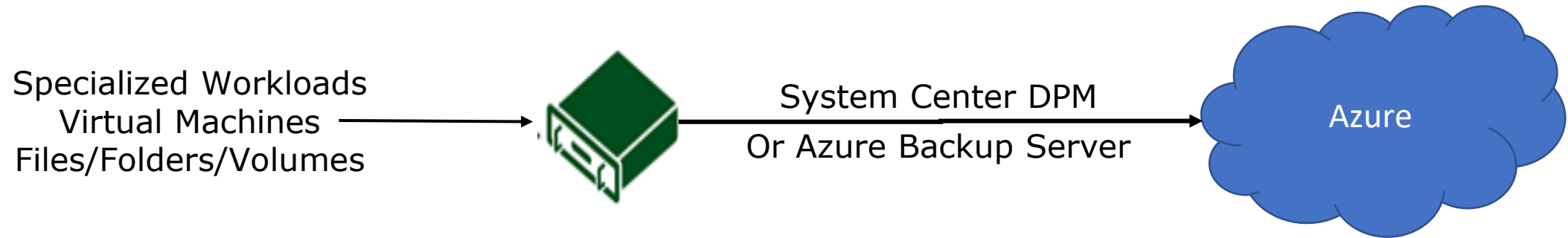
---



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
<u>Azure Backup (MARS) agent</u>	<ul style="list-style-type: none"> <li>Backup files and folders on physical or virtual <u>Windows OS</u> <i>on Prem</i></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>

*DPM*

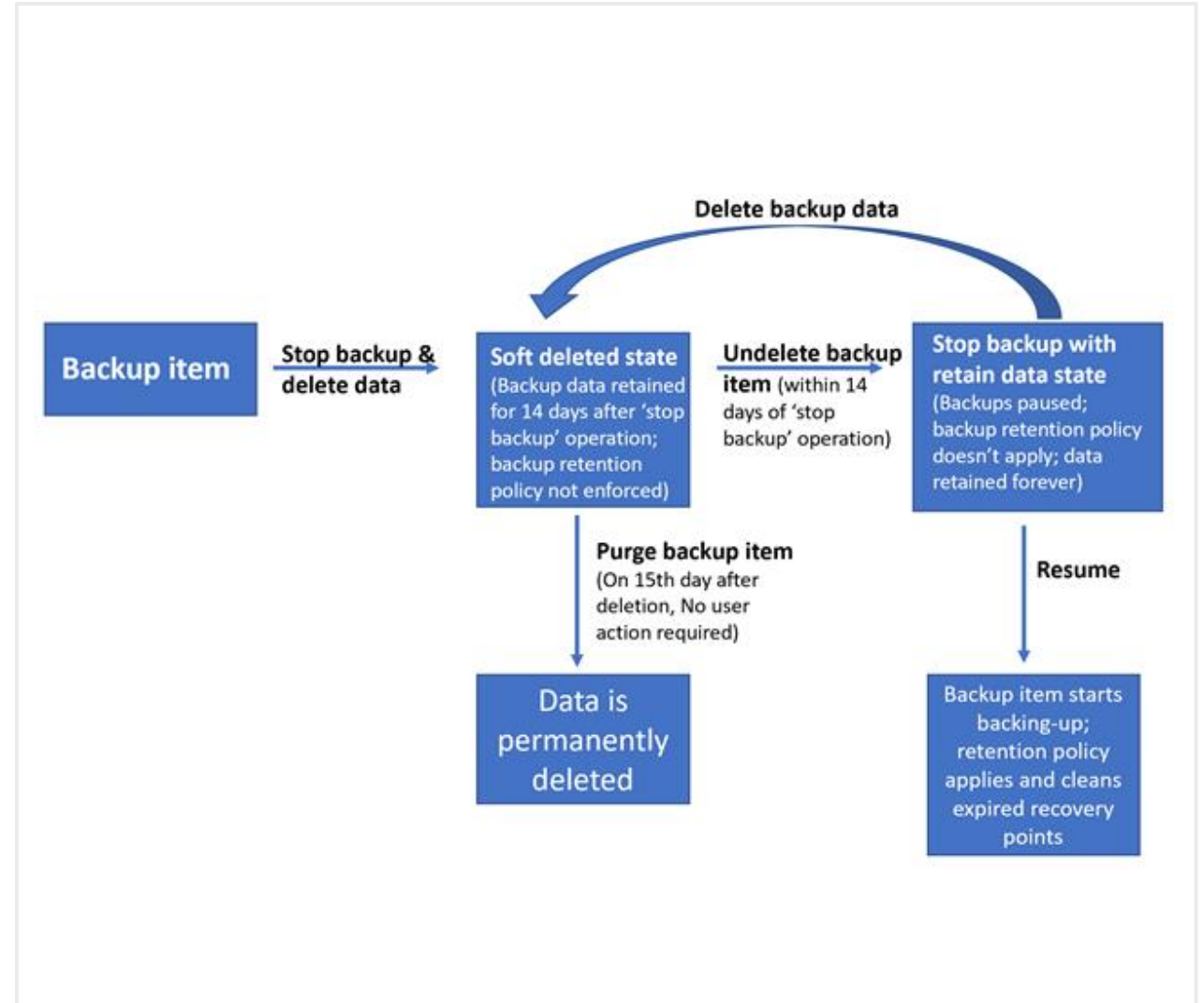
# Manage Soft Delete

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





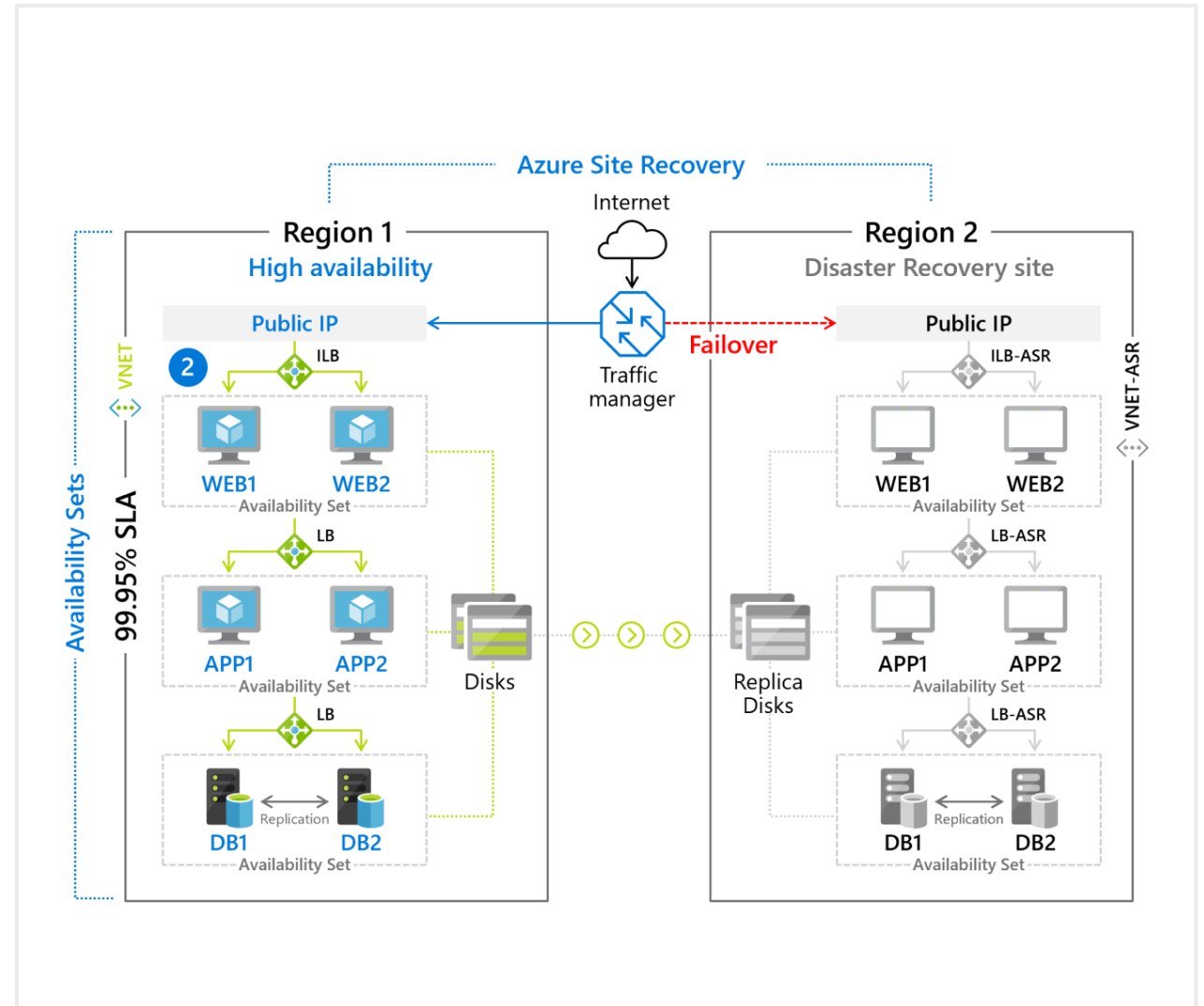
# Implement Azure Site Recovery

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](#)

---

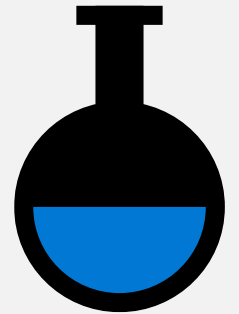
[Implement hybrid backup and recovery with Windows Server IaaS](#)

---

[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:

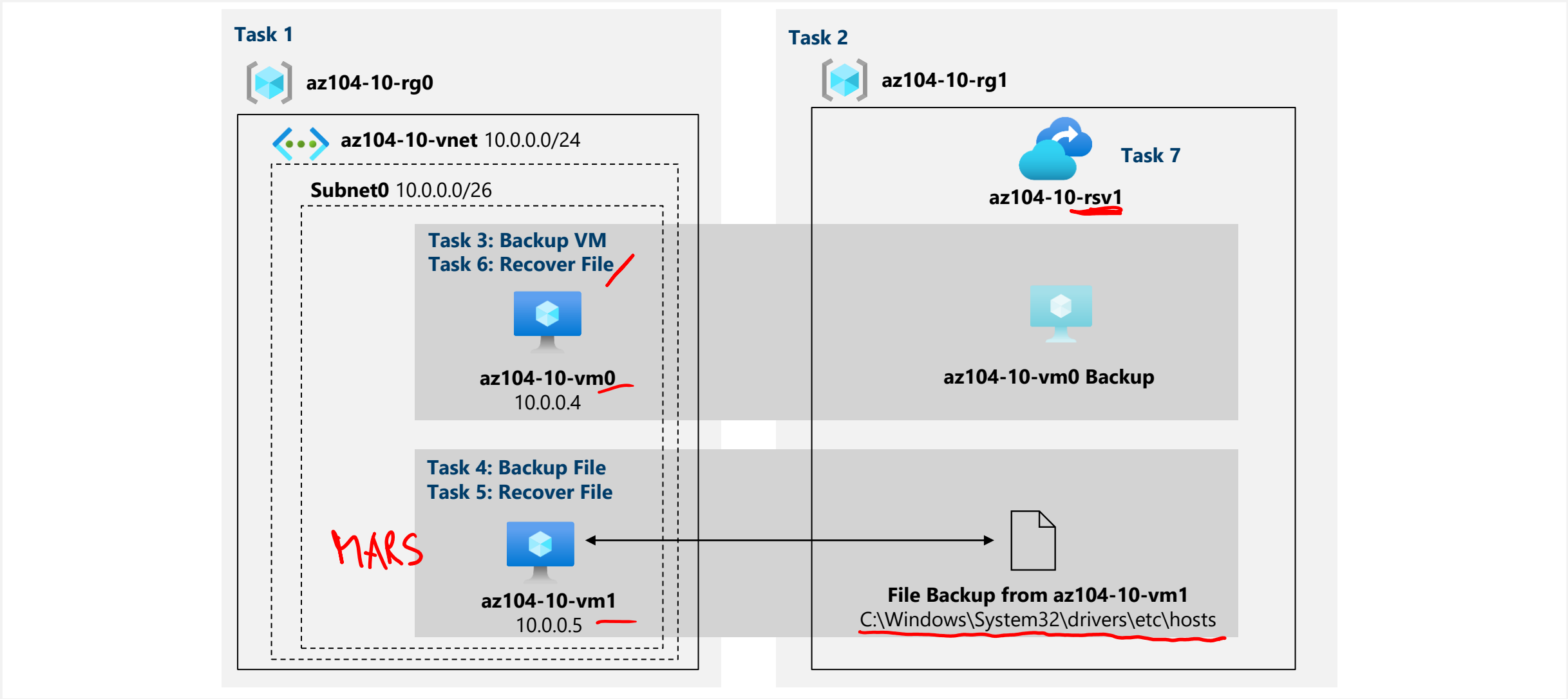
Perform file recovery by using Azure virtual machine snapshots

### Task 7:

Review the Azure Recovery Services soft delete functionality

Next slide for an architecture diagram 

# Lab 10 – Architecture diagram



# End of presentation

