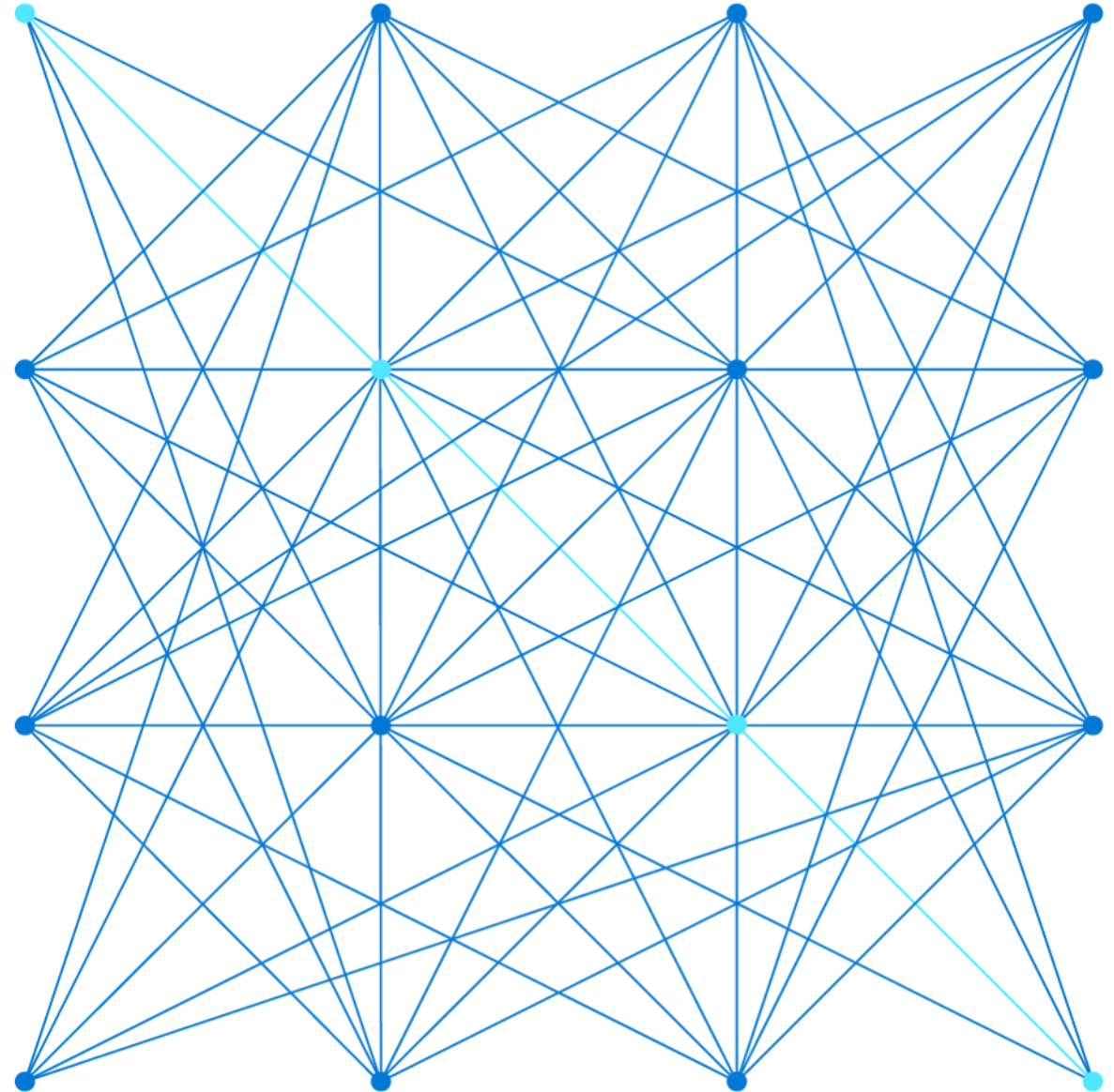


# AZ-104

## Administer Data Protection

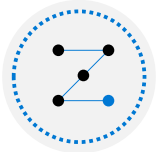


# About this course: Course Outline



01: Administer Identity

---



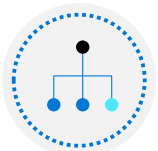
02: Administer Governance and Compliance

---



03: Administer Azure Resources

---



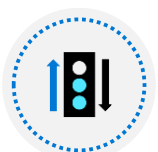
04: Administer Virtual Networking

---

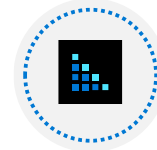


05: Administer Intersite Connectivity

---

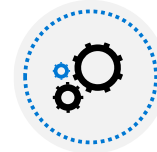


06: Administer Network Traffic Management



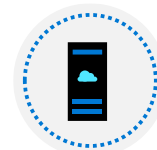
07: Administer Azure Storage

---



08: Administer Azure Virtual Machines

---



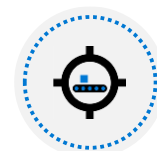
09: Administer PaaS Compute Options

---



10: Administer Data Protection

---



11: Administer Monitoring

# Administer Network Protection Introduction



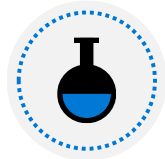
[Configure File and Folder Backups](#)

---



[Configure Virtual Machine Backups](#)

---



[Lab 10 – Implement Data Protection](#)

# Configure File and Folder Backups



# Describe Azure Backup Benefits



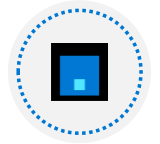
Azure-based service used to back up and restore data in Microsoft cloud

---



Automatic Storage Management

---



Multiple storage options

---



Unlimited data transfer

---



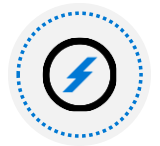
Data encryption

---



Application consistent backup

---



Long-term retention

---

# Implement Azure Backup Center

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

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 'Overview' page for 'Azure Virtual machines'. The interface includes a top navigation bar with 'Backup center' and 'Microsoft' branding, a search bar, and action buttons for '+ Backup', 'Restore', '+ Policy', '+ Vault', and 'Refresh'. A left-hand navigation pane lists various sections: Overview, Getting started, Community, Manage (with sub-items for Backup instances, Backup policies, and Vaults), Monitoring + reporting (with sub-items for Backup jobs and Backup reports), Policy and compliance (with sub-items for Backup compliance, Azure policies for backup, and Protectable datasources), and Support + troubleshooting (with a sub-item for New support request). The main content area is titled 'Datasource type: Azure Virtual machines' and 'Overview of Jobs and Backup instances'. It features two primary data sections. The first, 'Jobs (last 24 Hours)', includes a table with columns for 'Operation', 'Failed', 'In progress', and 'Completed'. The second, 'Backup instances', shows a summary for 'Azure Virtual machines' with a large '2' indicating the total count, and a breakdown of 'Protection configured' (2), 'Protection stopped' (0), and 'Soft deleted' (0). A note at the bottom states '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	Count
Azure Virtual machines	2
Protection configured	2
Protection stopped	0
Soft deleted	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

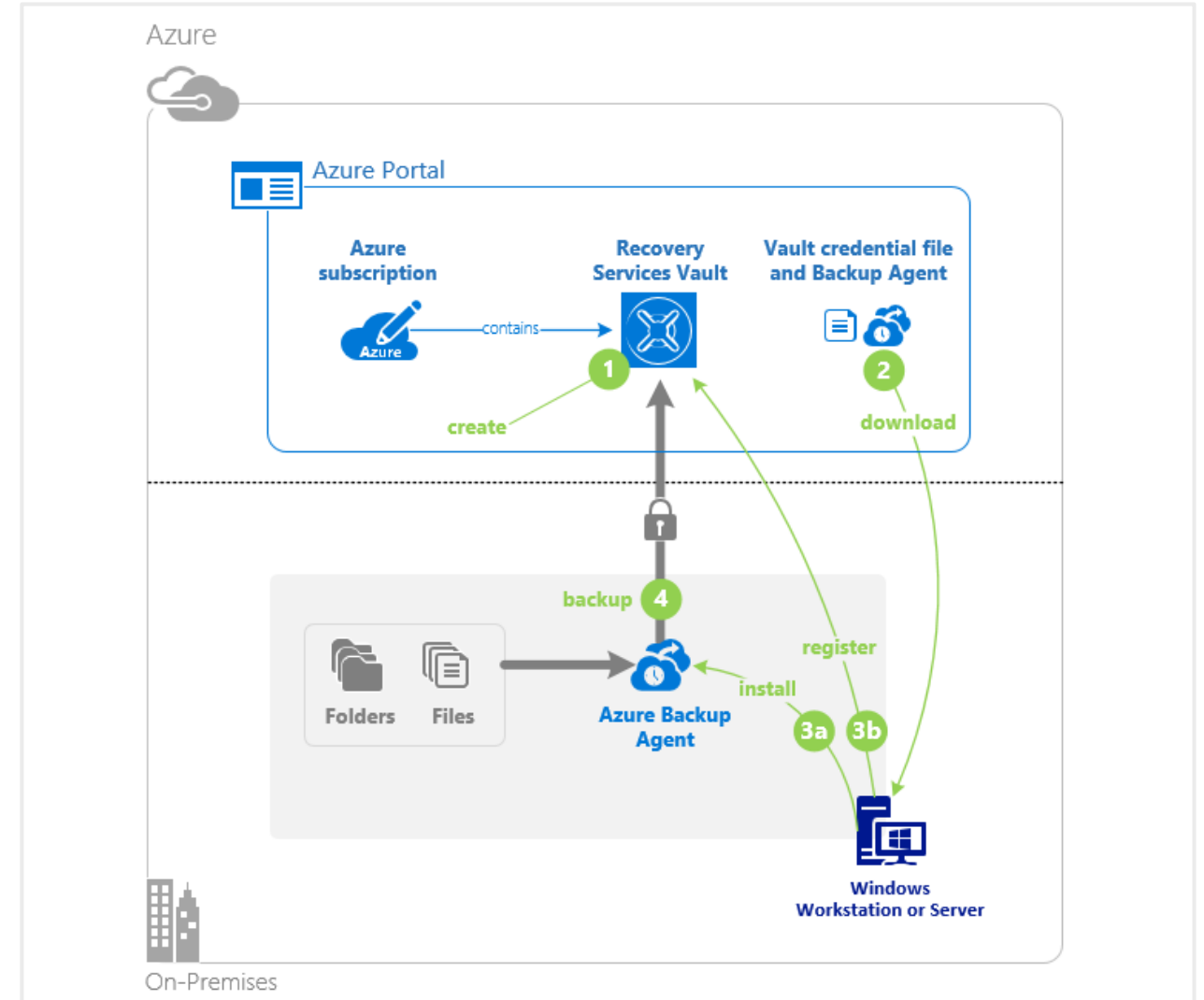
# Configure On-Premises File and Folder Backup

1. Create the recovery services vault

2. Download the agent and credential file

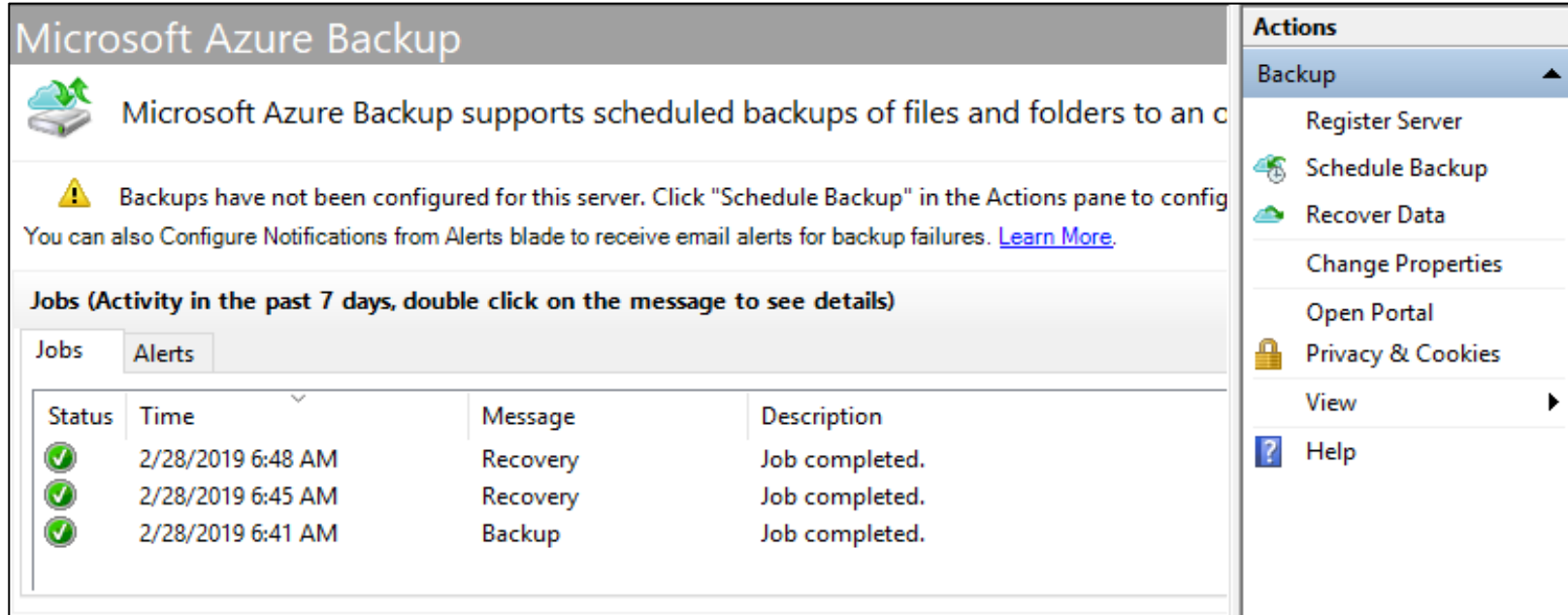
3. Install and register agent

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

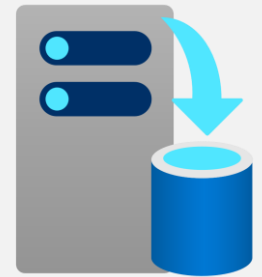
Backup or recover files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure)

No separate backup server required

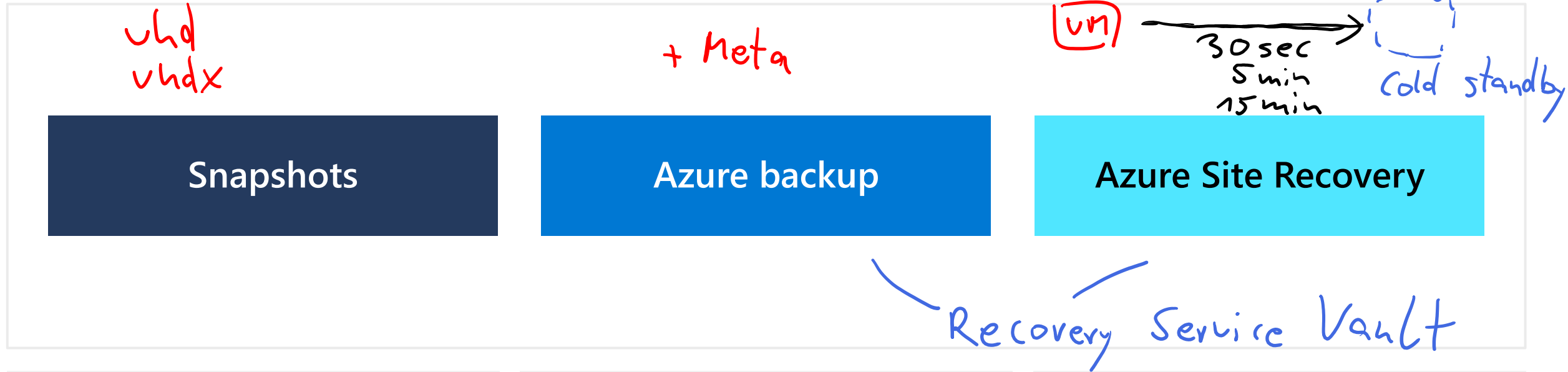
Not application aware; file, folder, and volume-level restore only

No support for Linux

# Configure Virtual Machine Backups



# Protect Virtual Machine Data



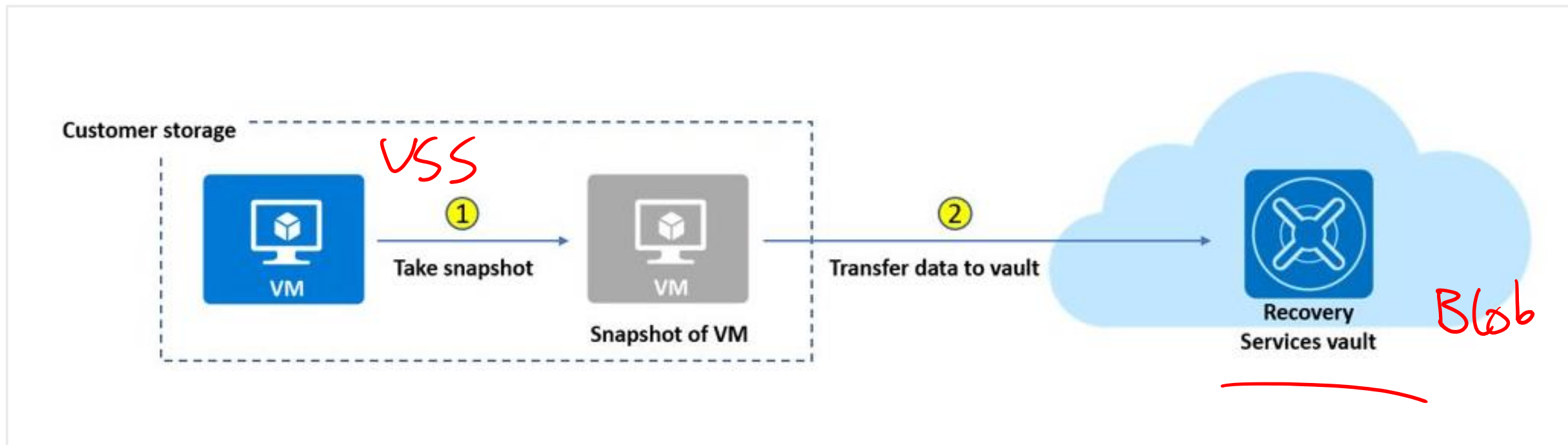
Managed snapshots provide a quick and simple option for backing up VMs that use Managed Disks

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

*Key Vault*

# 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

 **ContosoWebFE1**  
Backup Item

 Backup now  Restore VM  File Recovery  Stop backup  Resume backup

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 3/12/2020, 12:20:38 AM

**Restore points (30)**

CRASH CONSISTENT  
30

APPLICATION CONSISTENT  
0

FILE-SYSTEM CONSISTENT  
0

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

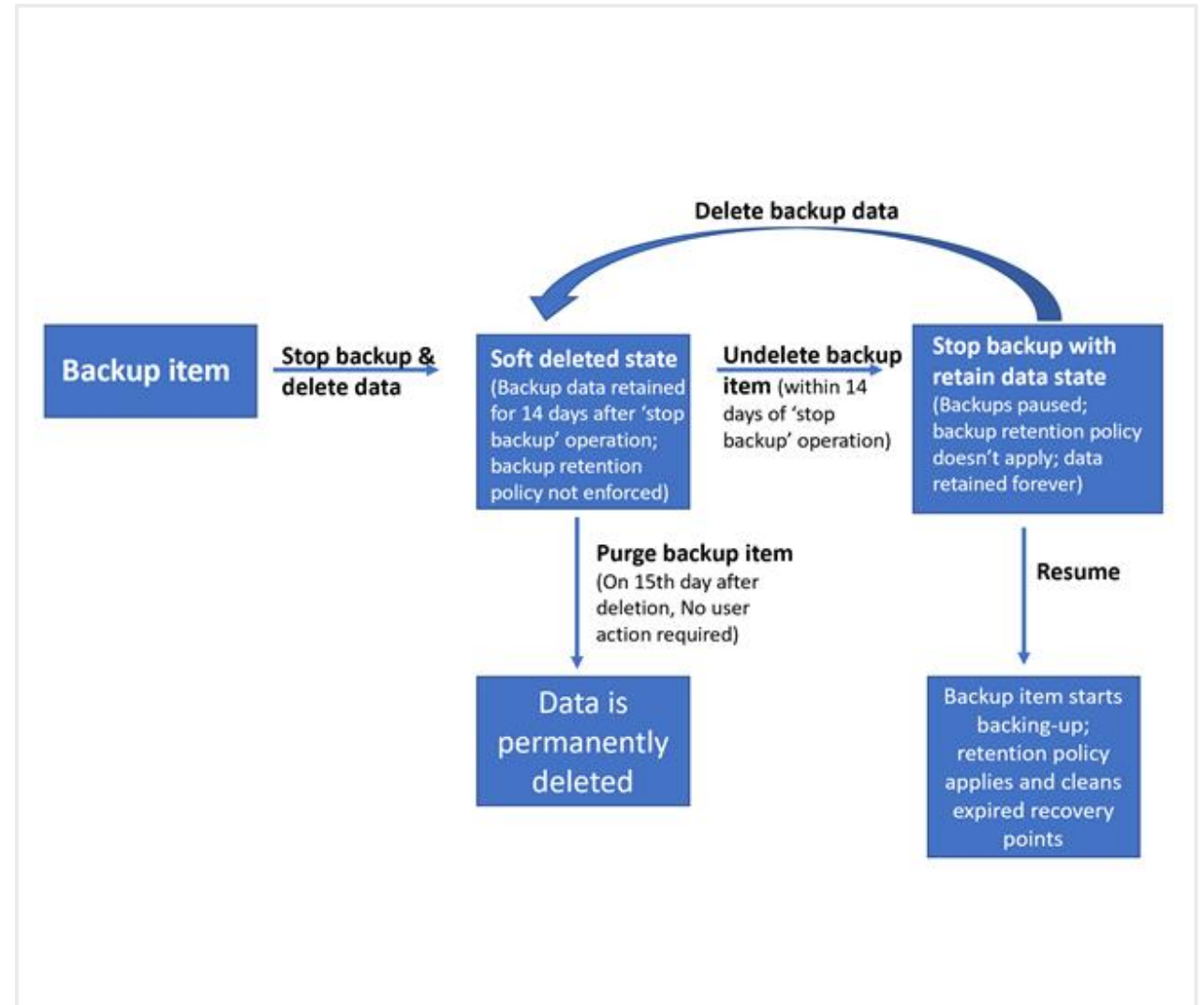
# Manage Soft Delete

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





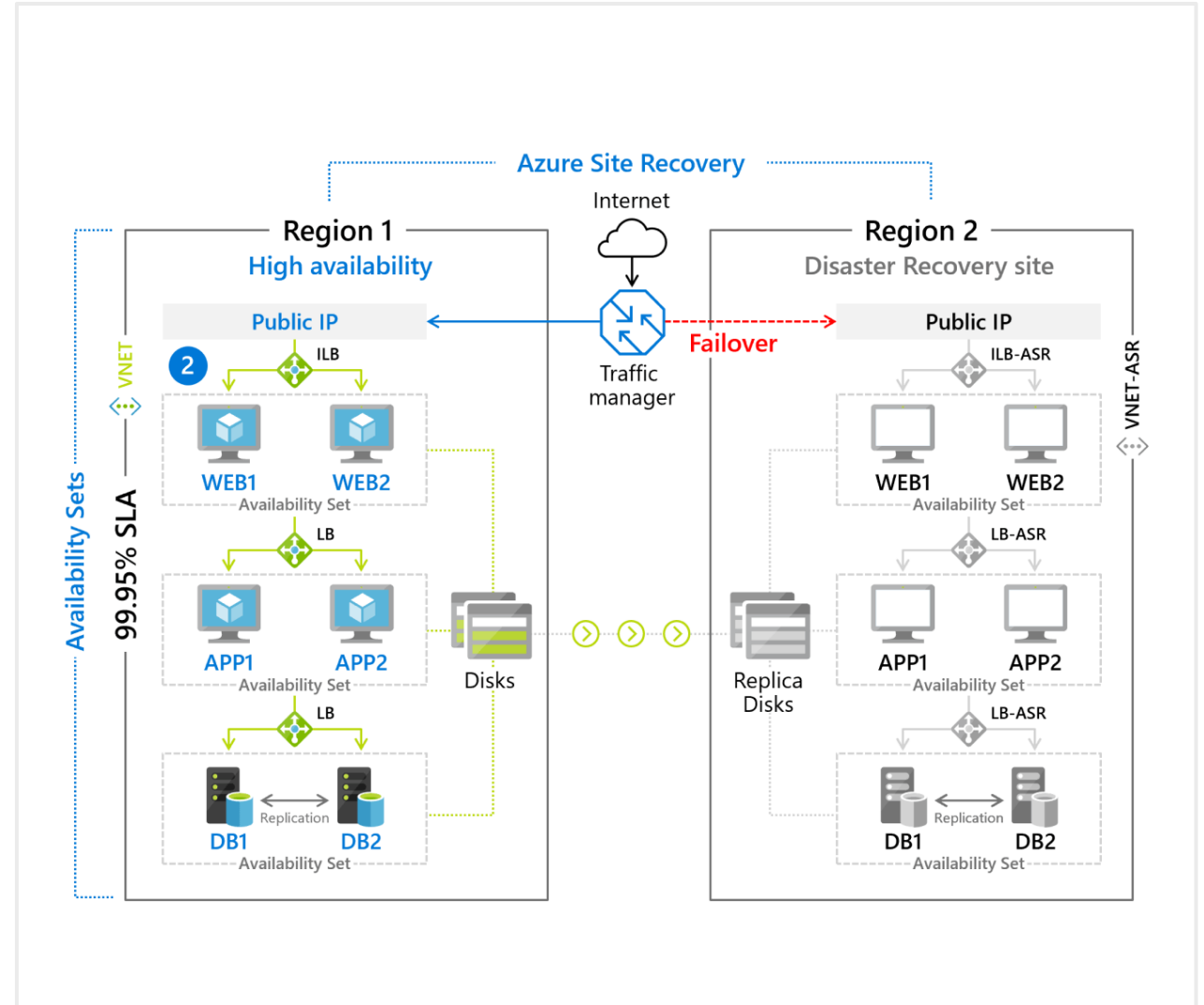
# Implement Azure Site Recovery

Replicate Azure VMs from one Azure region to another

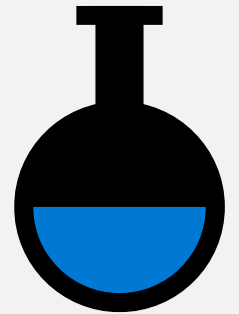
Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure

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



# 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:

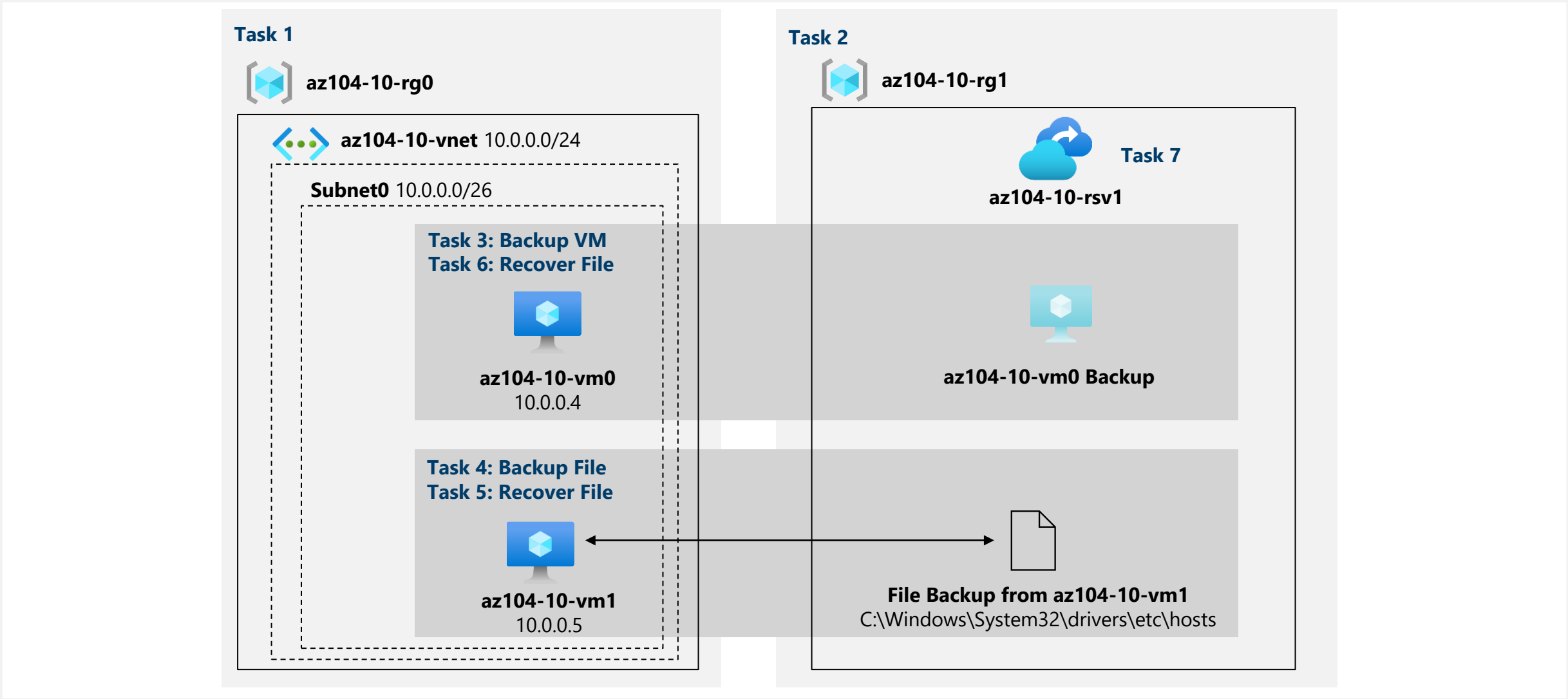
Perform file recovery by using Azure virtual machine snapshots

### Task 7:

Review the Azure Recovery Services soft delete functionality

Next slide for an architecture diagram 

# Lab 10 – Architecture diagram



# End of presentation

