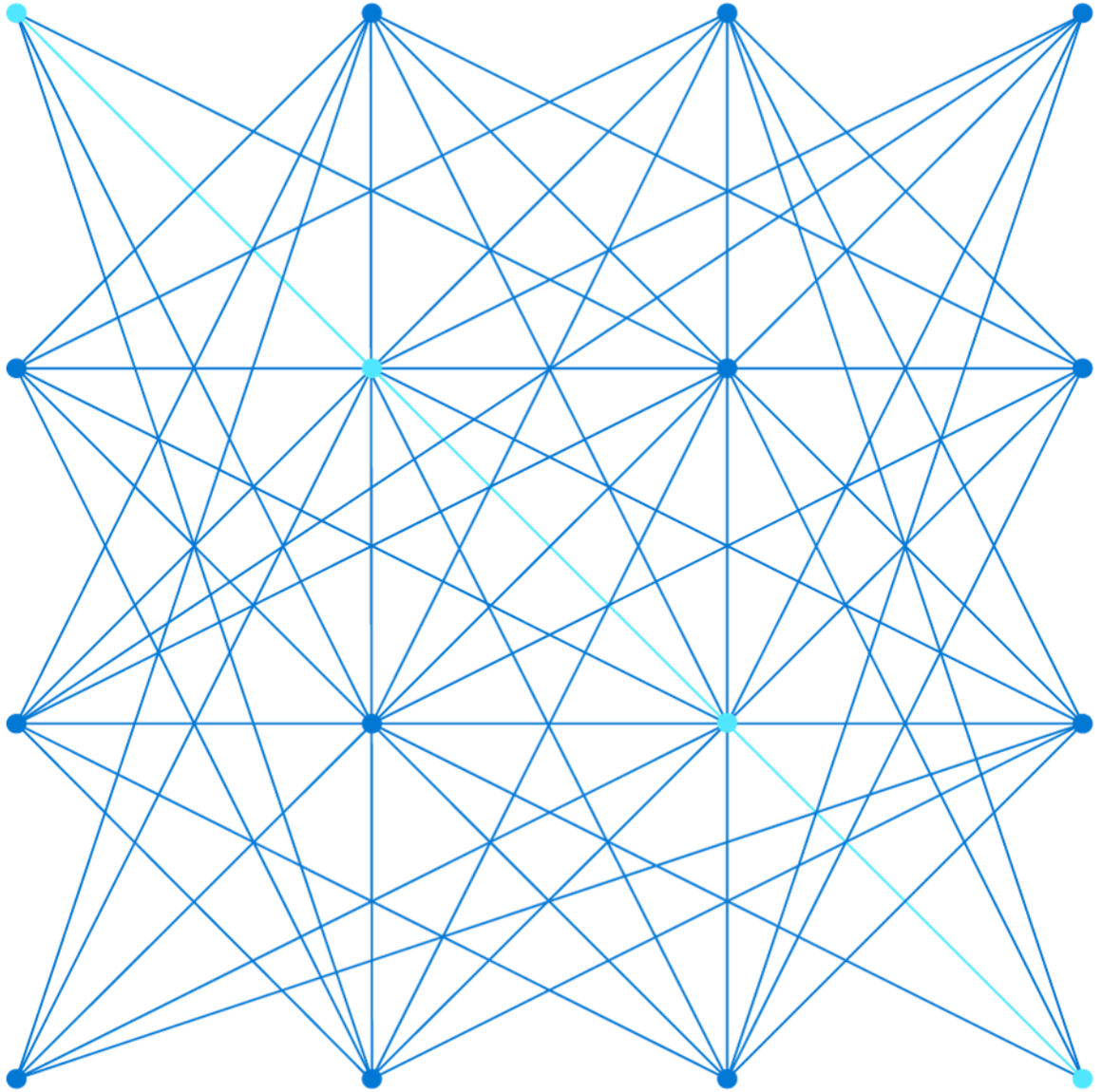
Microsoft Azure

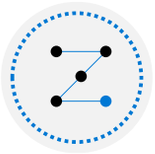
# AZ-104

# Administer Data Protection



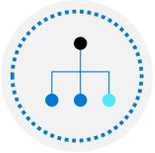
# About this course: Course Outline

01: Administer Identity



02: Administer Governance and Compliance

03: Administer Azure Resources

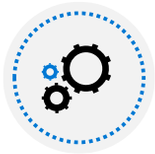


04: Administer Virtual Networking

05: Administer Intersite Connectivity

06: Administer Network Traffic Management

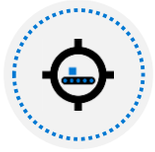
07: Administer Azure Storage



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

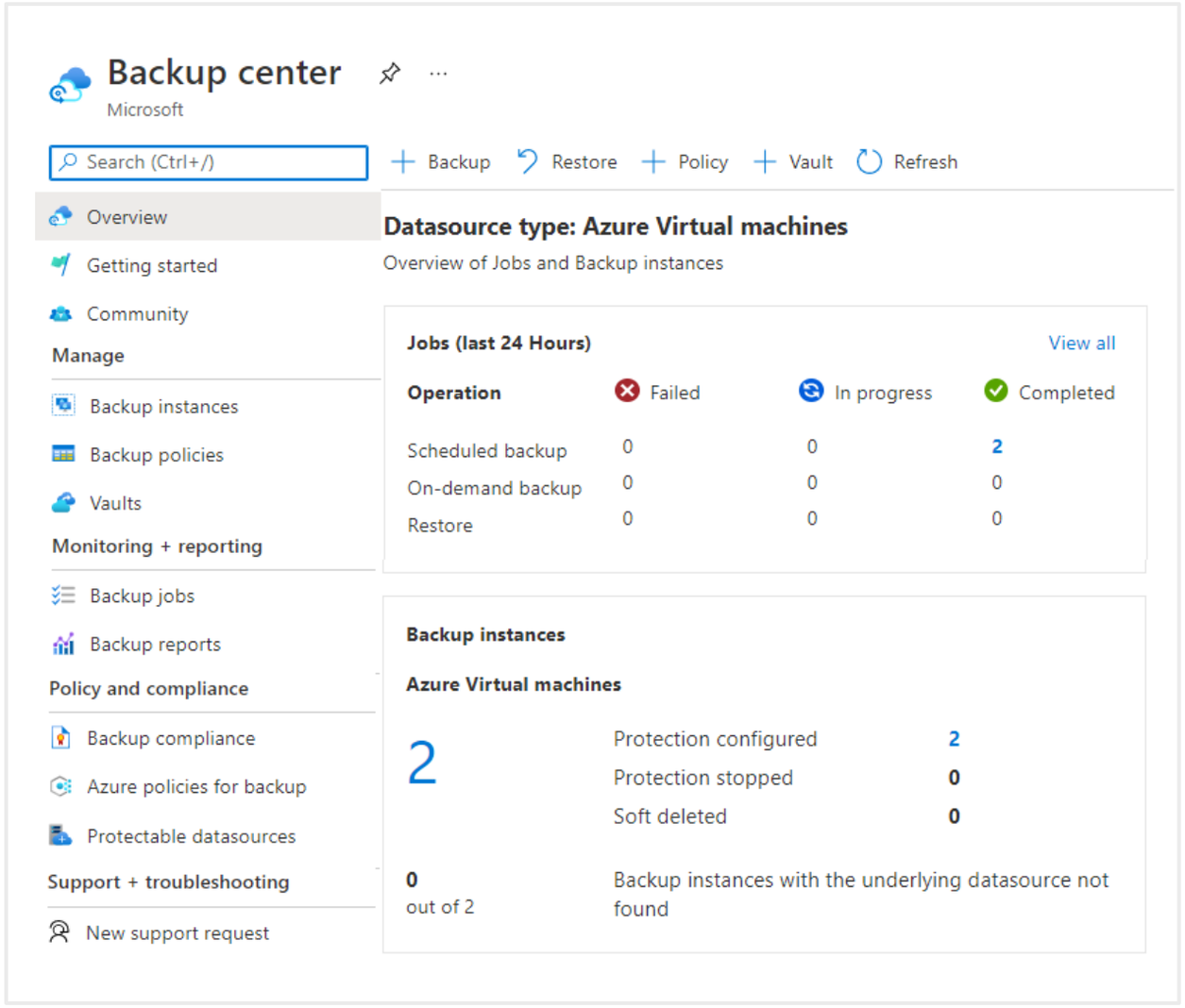
Long-term retention

# Implement Azure Backup Center

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

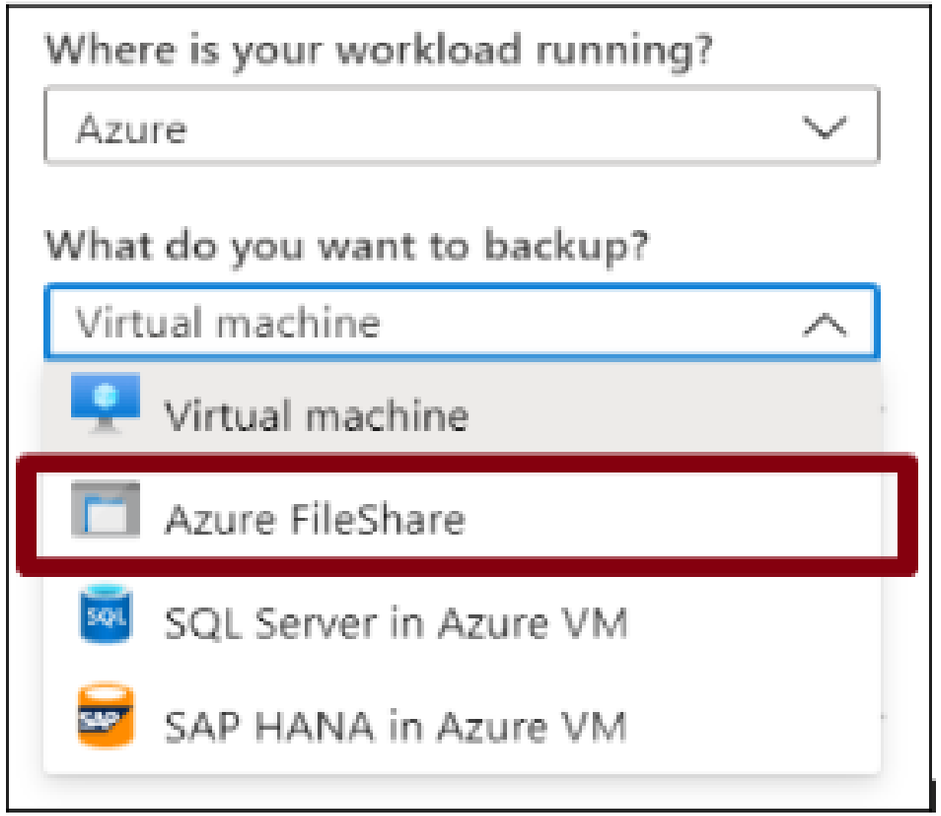
Datasource-centric management focused on what you are backing up

Connected experiences with native integrations that enables management at scale

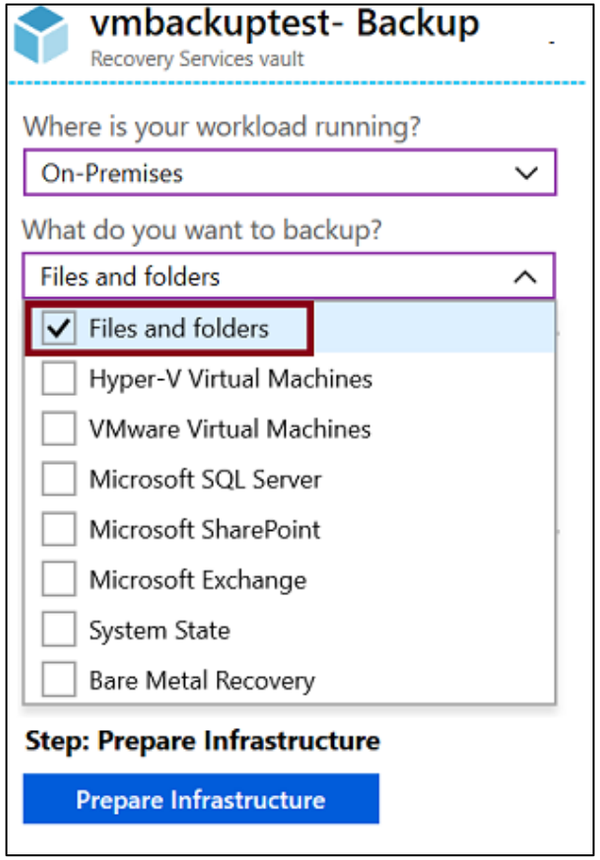


# Setup Recovery Services Vault Backup Options - Files

## Azure Workloads




## On-Premises Workloads



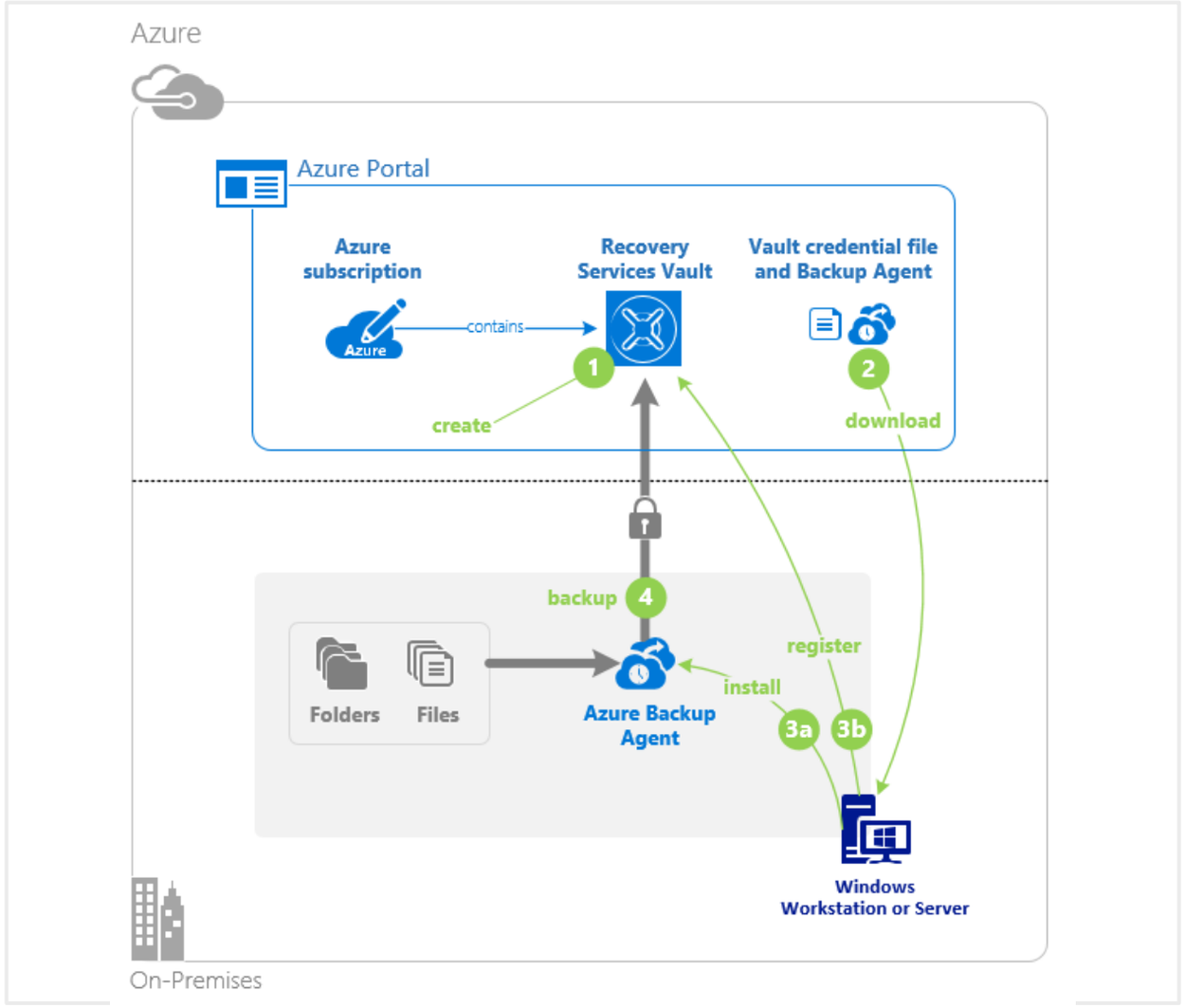
# Configure On-Premises File and Folder Backup

1. Create the recovery services vault

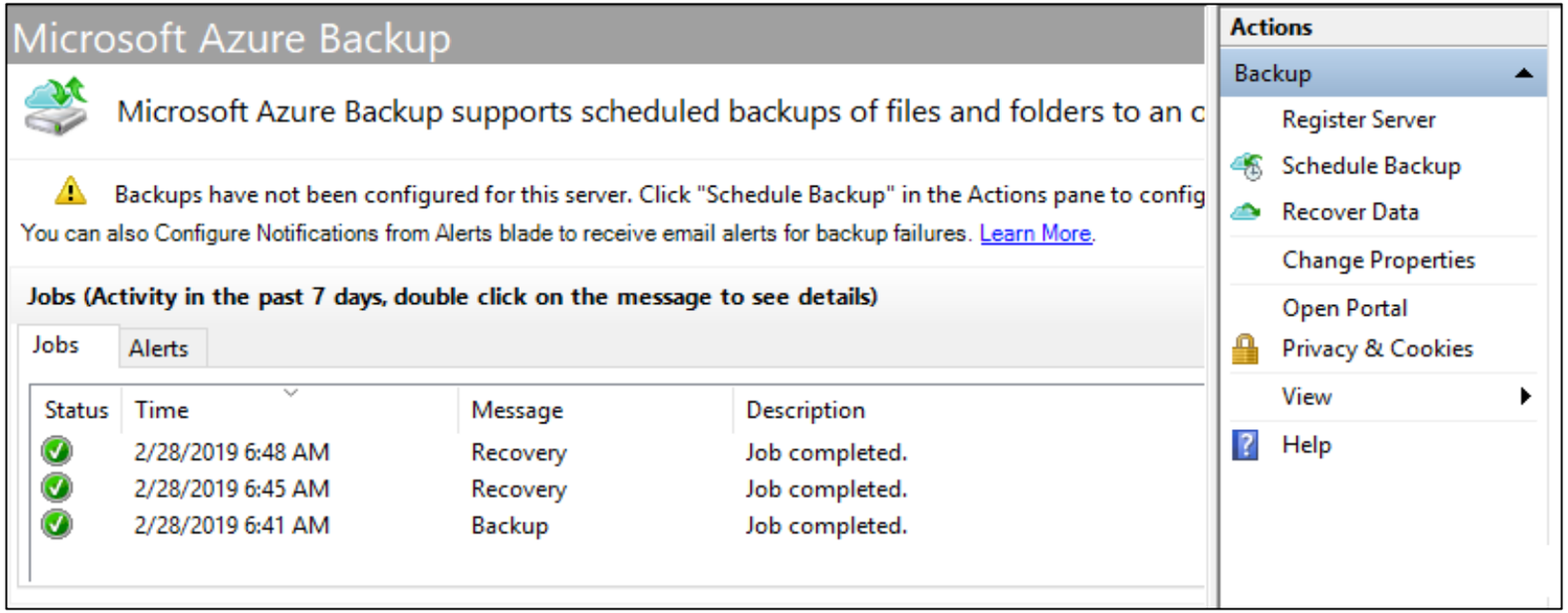
2. Download the agent and credential file

3. Install and register agent

4. Configure the backup



# Manage the Microsoft Azure Recovery Services Agent




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

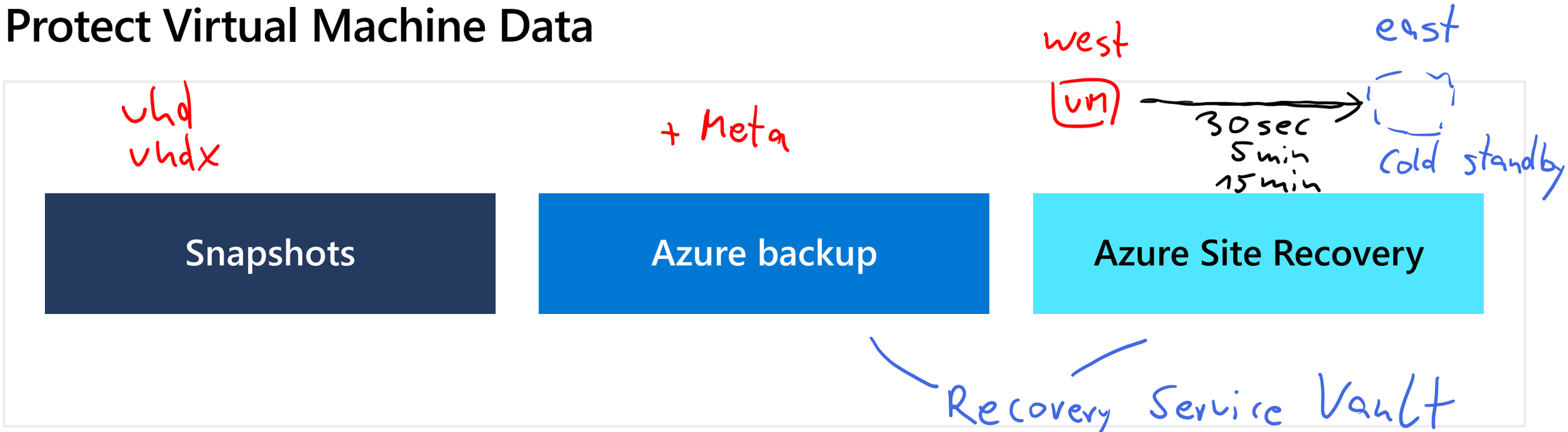
No separate backup server required

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

No support for Linux

# Configure Virtual Machine Backups

# Protect Virtual Machine Data



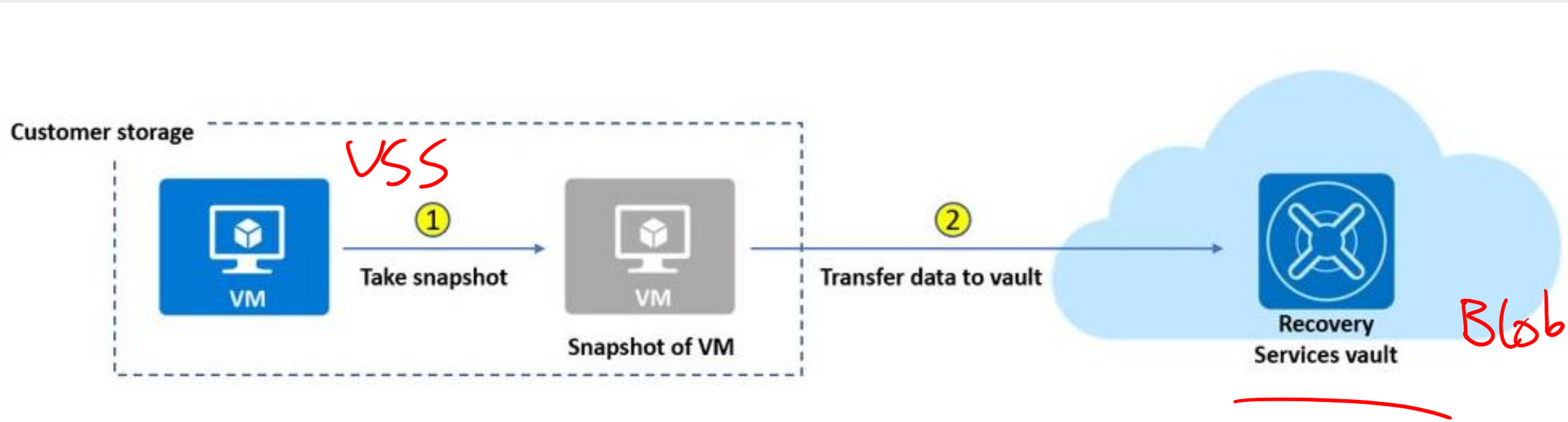

Managed snapshots provide a quick and simple option for backing up VMs that use Managed Disks

Key Vault

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



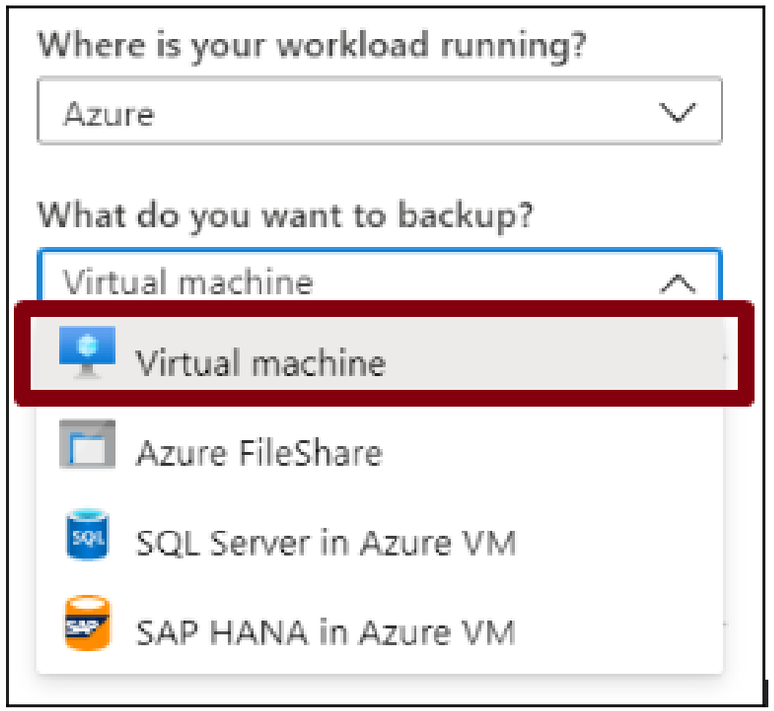

Use snapshots taken as part of a backup job

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

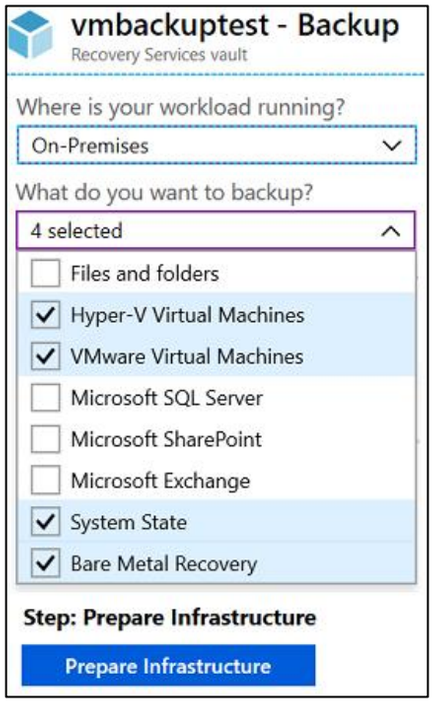
Configure Instant Restore retention (1 to 5 days)

# Setup Recovery Services Vault Backup Options - VMs

## Azure Workloads

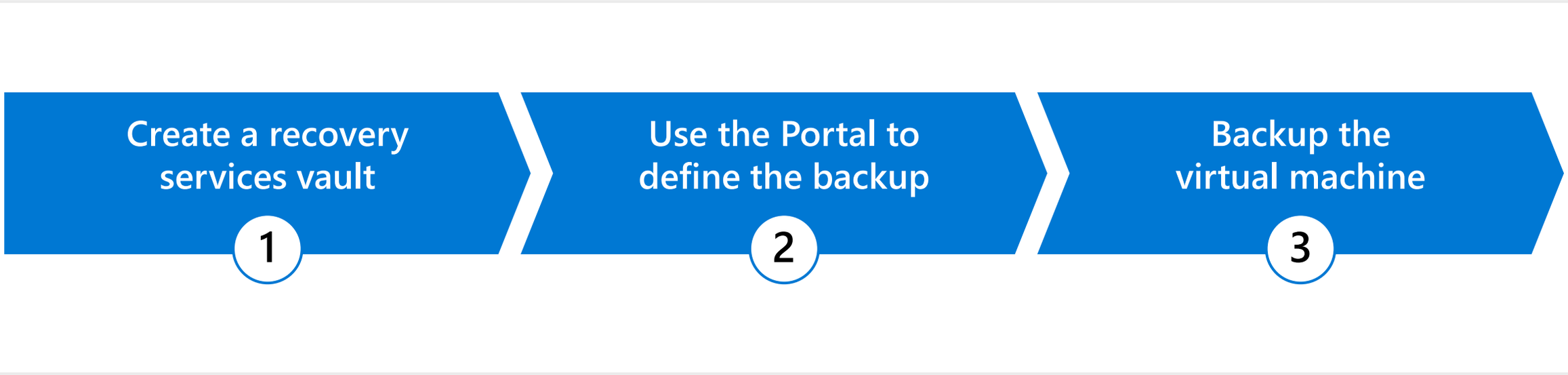



## On-Premises Workloads




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

# Backup Virtual Machines




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

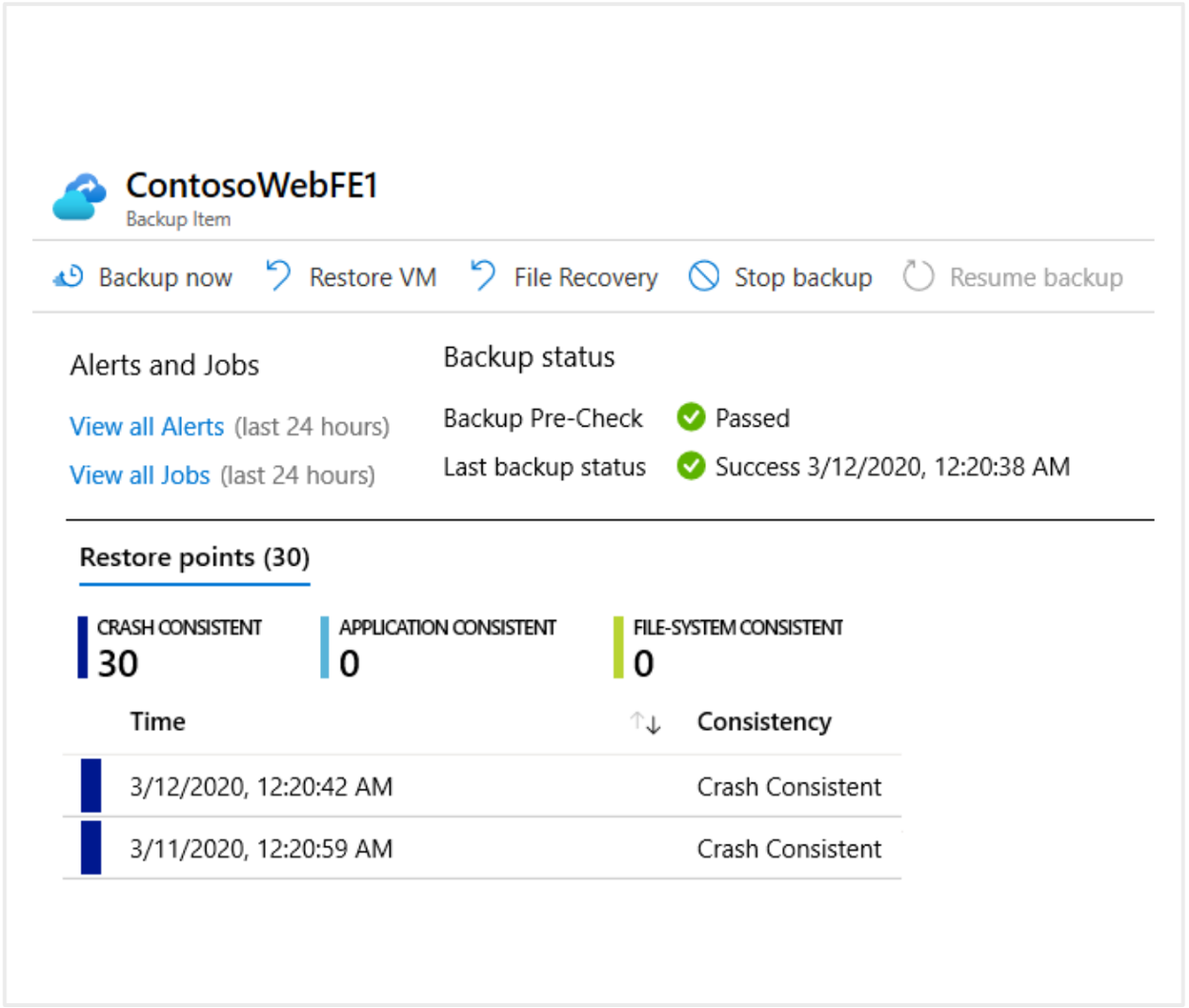
2. Take snapshots (recovery points) of your data at defined intervals. These snapshots are stored in recovery services vaults

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



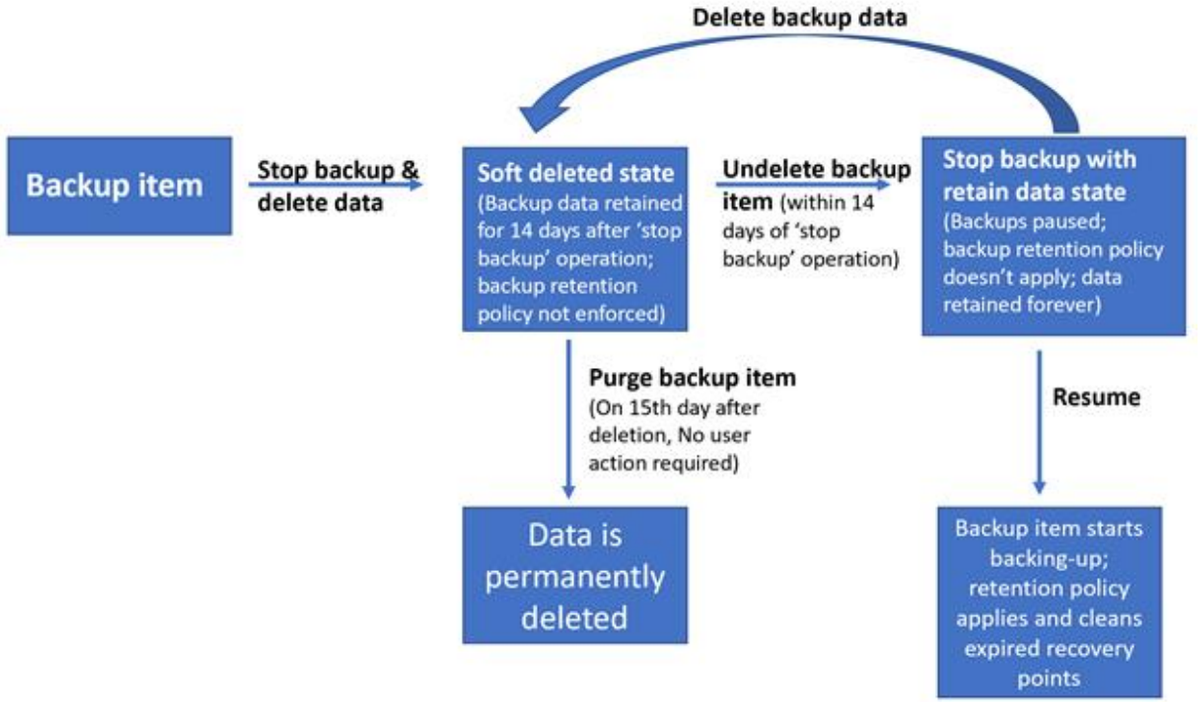
# Manage Soft Delete

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



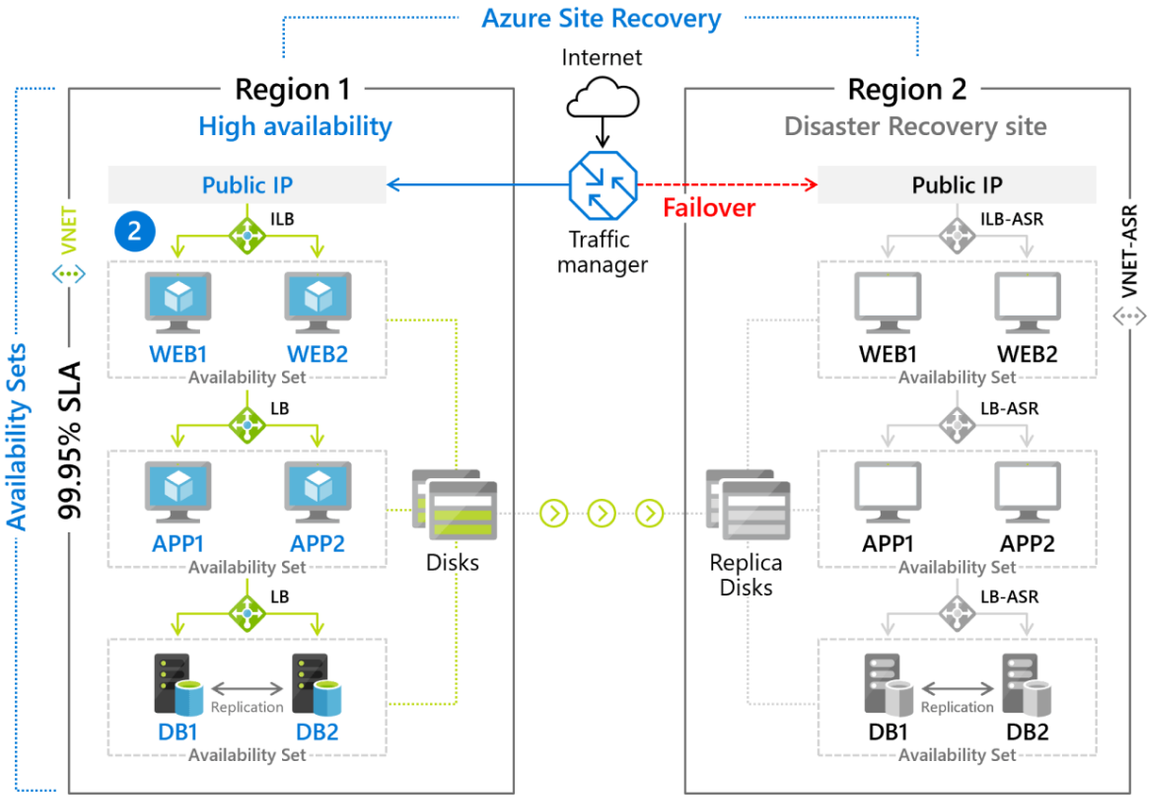
# Implement Azure Site Recovery

Replicate Azure VMs from one Azure region to another

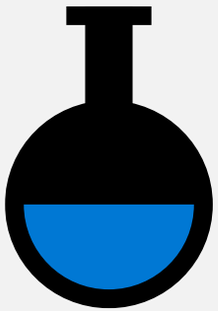
Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure

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

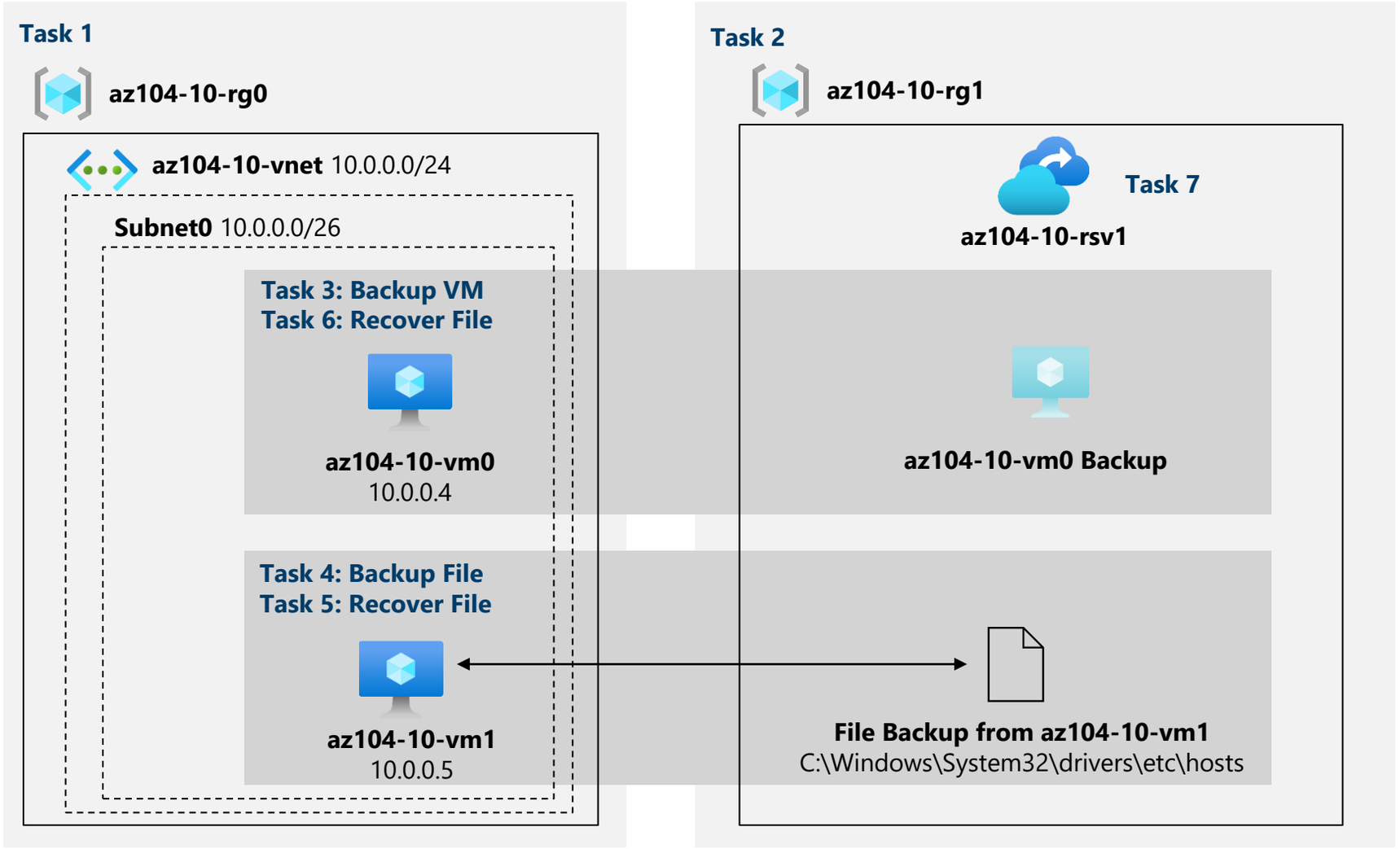
**Task 5:**
Perform file recovery by using Azure Recovery Services agent

**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