


AZ-104

Administer Data Protection



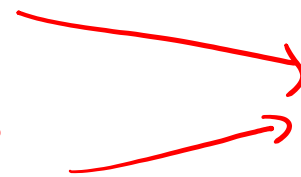
AZ-104 Course Outline

- 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

Learning Objectives - Administer Network Protection

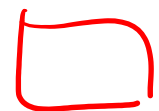
- [Configure File and Folder Backups](#)
- [Configure Virtual Machine Backups](#)
- [Lab 10 – Implement Data Protection](#)

vm



Azure Site Recovery
ASR

vm



Region 1



vm



vhdx

Region 2

cold standby

Veeam

Configure File and Folder Backups

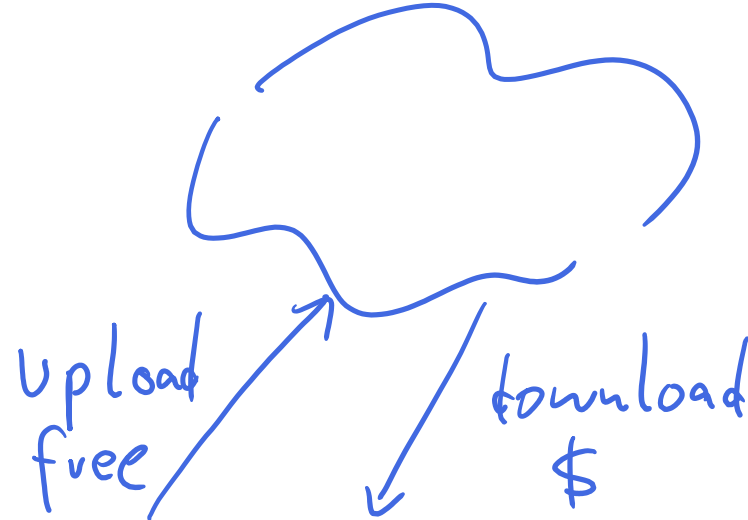


Describe Azure Backup Benefits

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

Bring your own key
VSS



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 shows the Azure Backup Center 'Overview' page. The left sidebar contains a navigation menu with sections: Overview (selected), Getting started, Community, Manage (with sub-items: Backup instances, Backup policies, Vaults), Monitoring + reporting (with sub-items: Backup jobs, Backup reports), Policy and compliance (with sub-items: Backup compliance, Azure policies for backup, Protectable datasources), and Support + troubleshooting (with sub-item: New support request). The main content area has a search bar and action buttons: Backup, Restore, Policy, Vault, and Refresh. Below these, it states 'Datasource type: Azure Virtual machines' and 'Overview of Jobs and Backup instances'. A 'Jobs (last 24 Hours)' table shows counts for Failed, In progress, and Completed operations. A 'Backup instances' section shows 2 instances for Azure Virtual machines, with a breakdown of protection status.

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

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

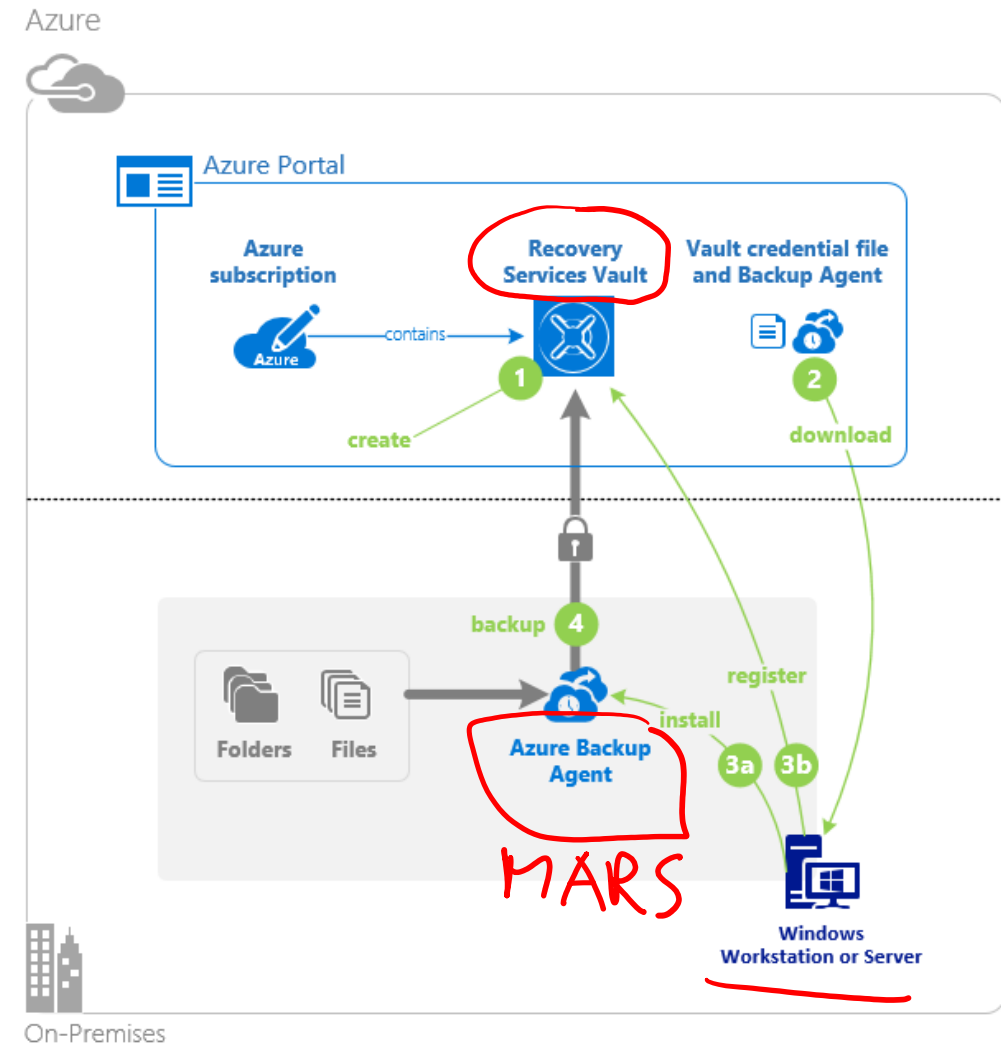
Configure On-Premises File and Folder Backup

1. Create the recovery services vault

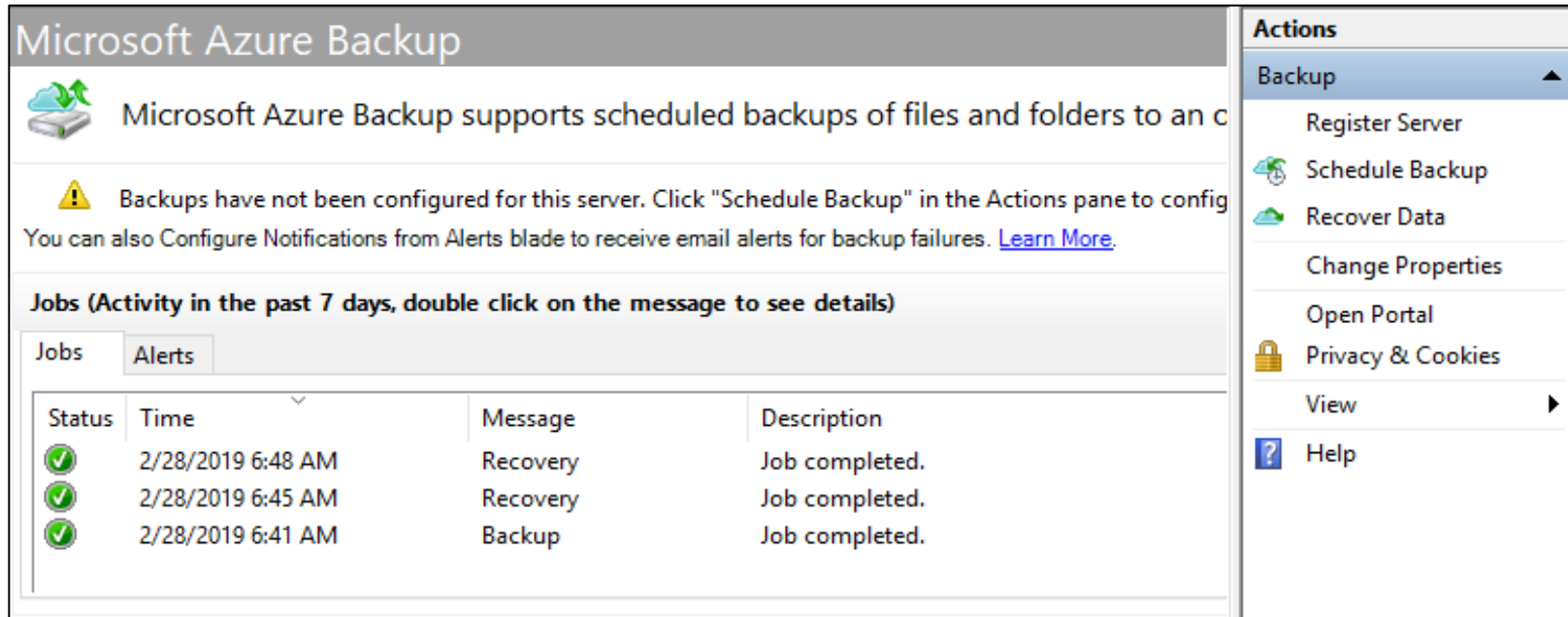
2. Download the agent and credential file

3. Install and register agent

4. Configure the backup



h A R S 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)

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

Snapshots

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

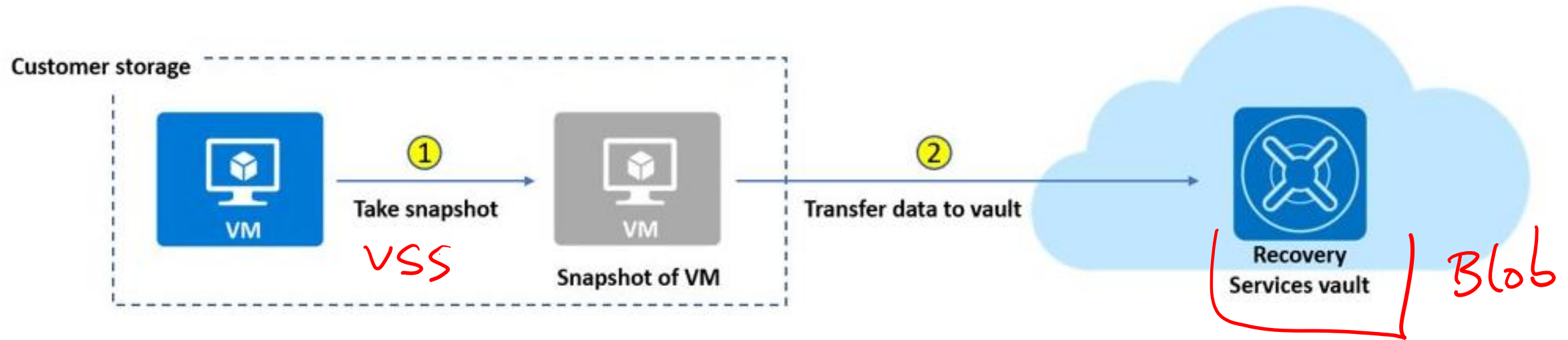
Azure backup

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

Azure Site Recovery

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

Multiple servers can be protected using the same Recovery Services vault

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

Backup Virtual Machines

Create a recovery services vault

1

Use the Portal to define the backup

2

Backup the virtual machine

3

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

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

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 and diagram illustrating the restore process:

- 4. azcopy (blue arrow from VN to NB)
- 1. download (red arrow from VN to I.vhd)
- 2. mount vhd (red arrow from I.vhd to C:\windows\system32\drivers\etc\hosts)
- 3. robocopy (blue arrow from NB to C:\windows\system32\drivers\etc\hosts)

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)

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

Manage Soft Delete ✓

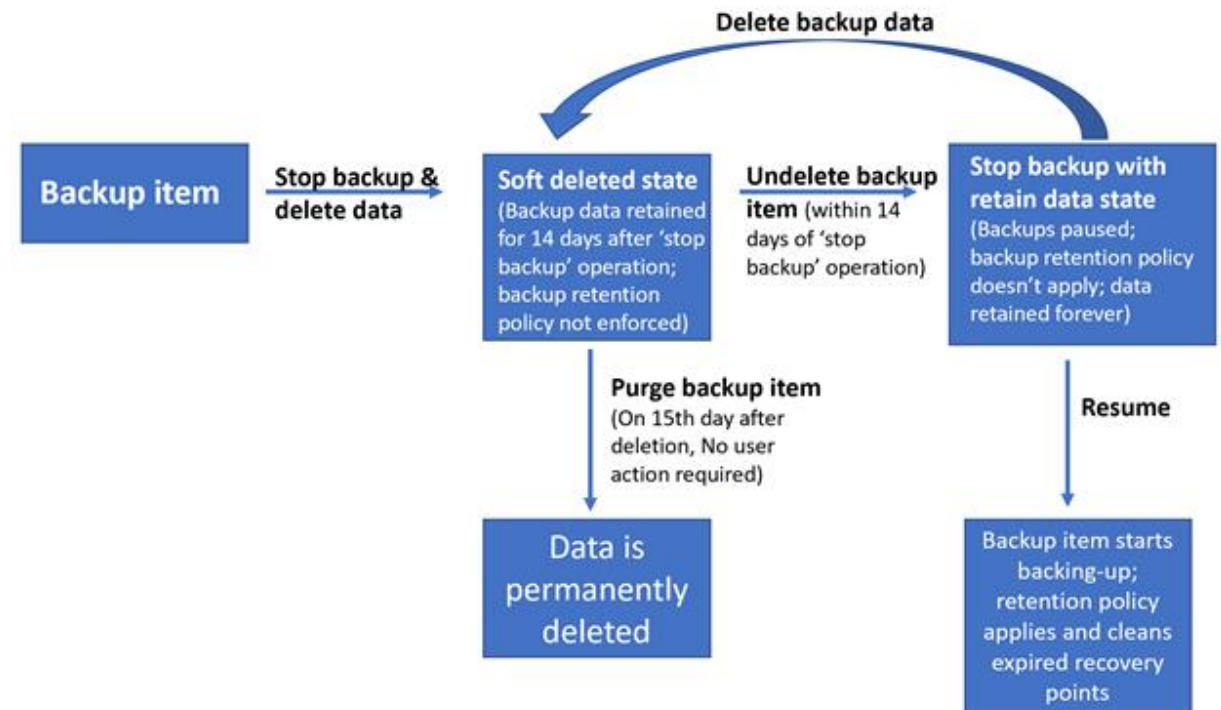
Backup data is retained for 14 additional days*

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

 ~~GRS~~
LRS



Implement Azure Site Recovery

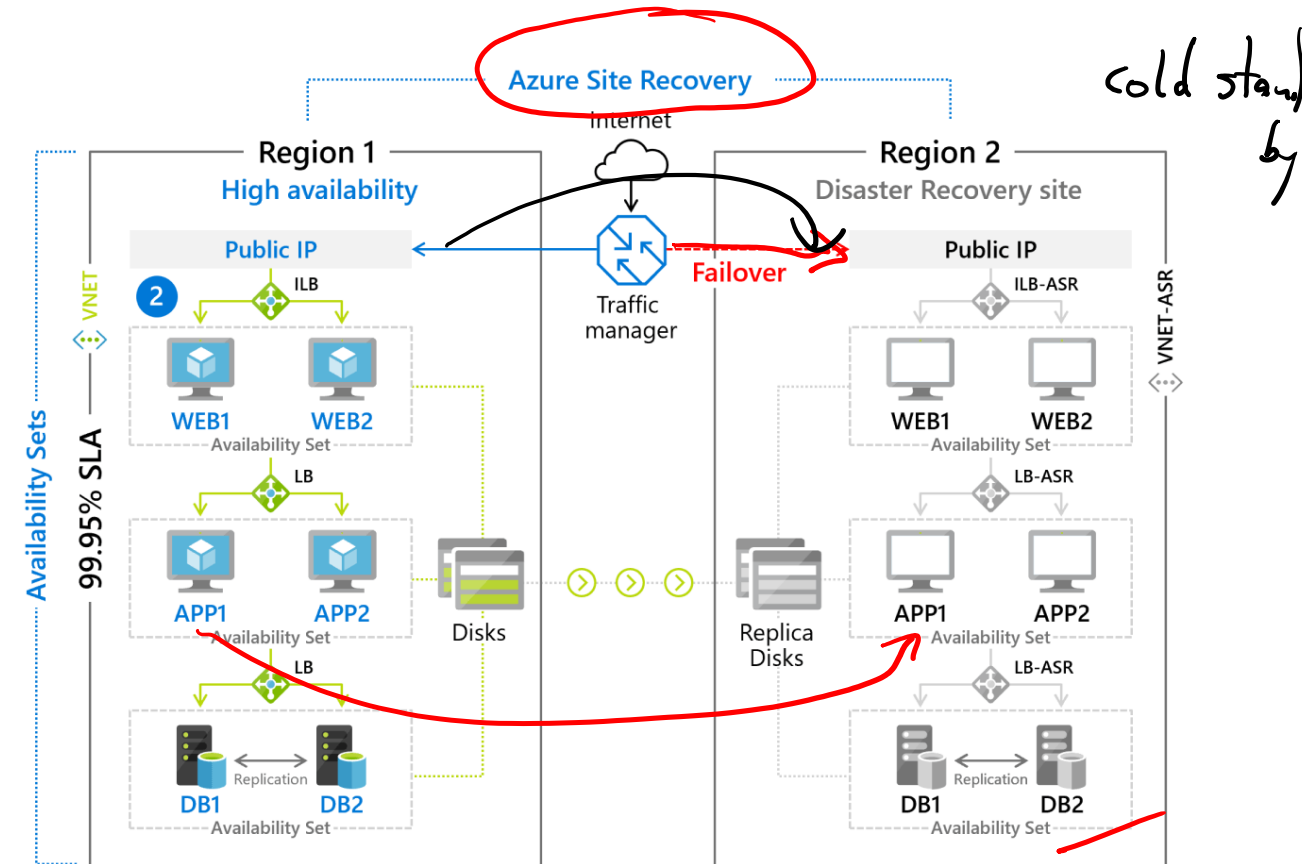
Replicate Azure VMs from one Azure region to another

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

Hyper-V Replica 15min
5min
30 sec



ASR

Primary
Region

D_{vm}

Vault
second. Region ✓
~~primary R.~~
third Region ✓

Secondary
Region

Lab 10 – Implement Data Protection



Lab 10 – Backup virtual machines



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

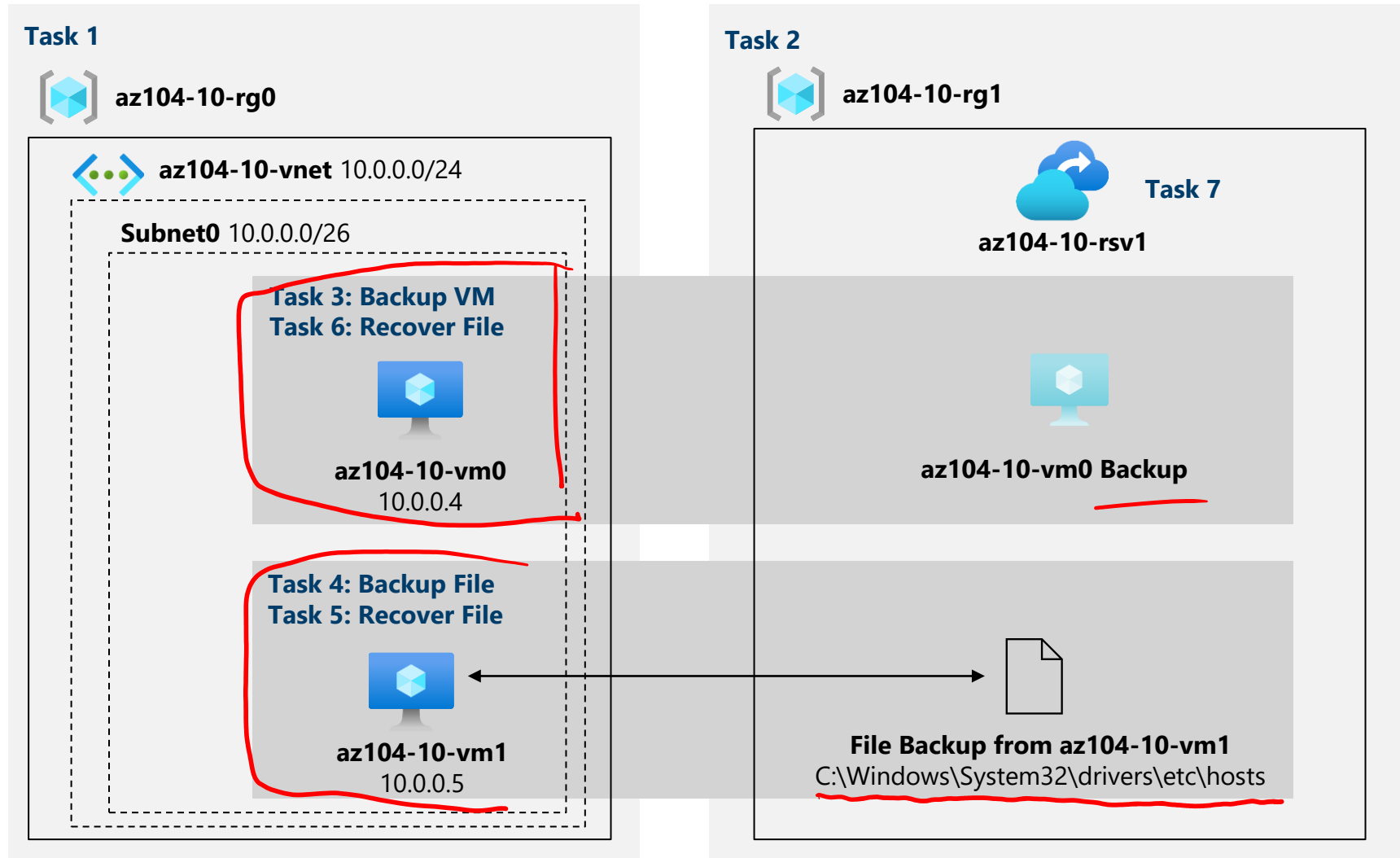
Task 5: Perform file recovery by using Azure Recovery Services agent

Task 6: Perform file recovery with 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

