Microsoft

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 ← github.com/www42/az-104

11: Administer Monitoring

Learning Objectives - Administer Network Protection

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

Recovery Service Vault
Backup
Site Recovery (ASR)

Key Vault

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

Handwritten annotations:

Soft Delete LRS GRS

Free

Cost
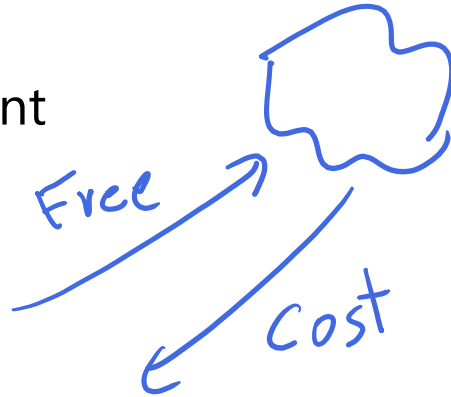
RSA QC

max 99 Jahr

Crash consistent

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

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
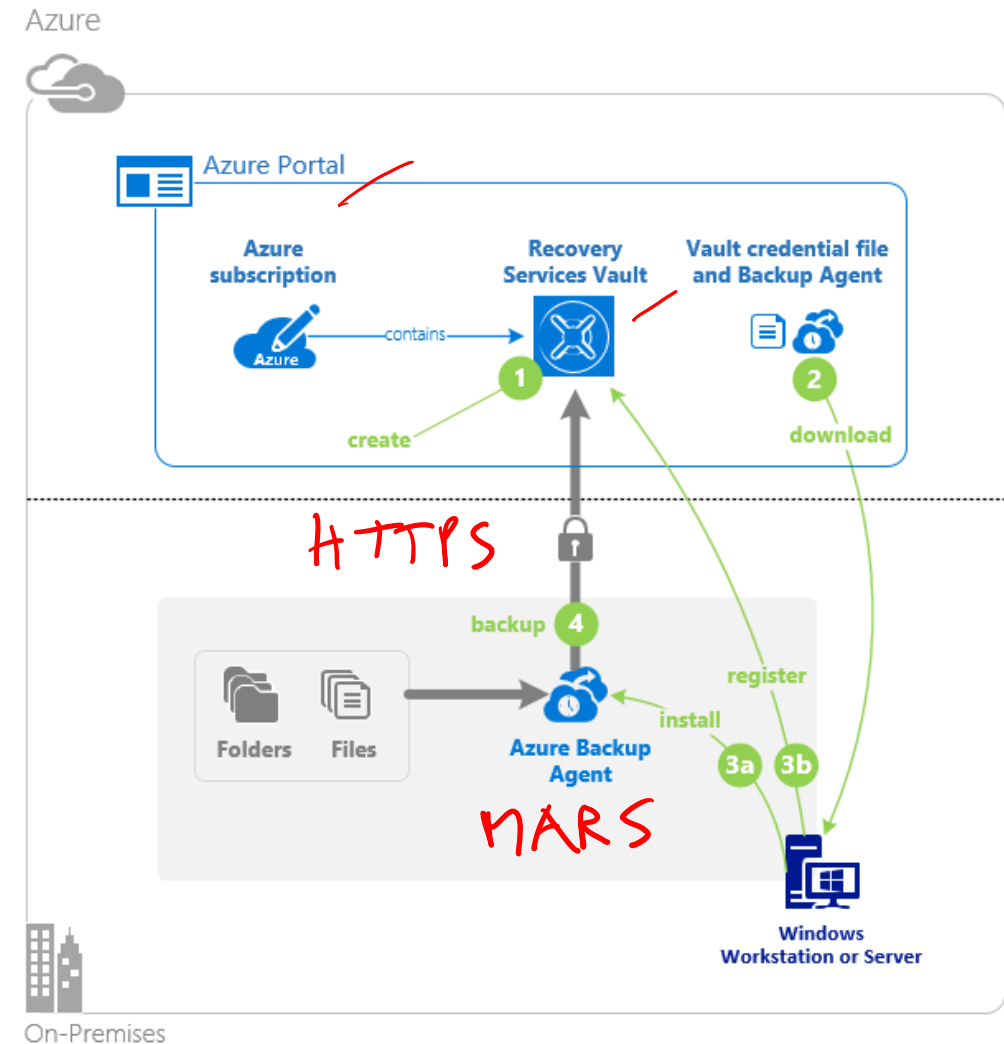
Manage the Microsoft Azure Recovery Services Agent

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

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
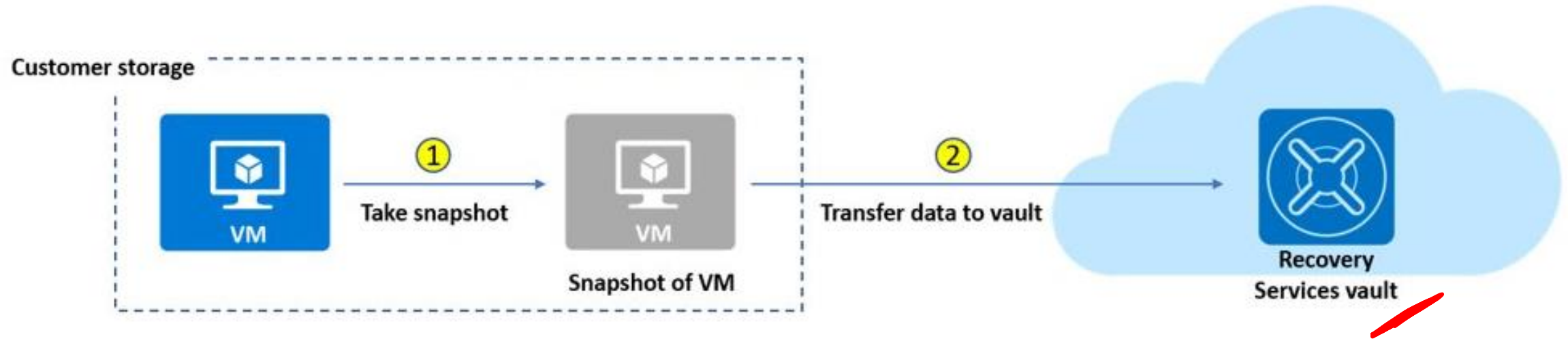
Use snapshots taken as part of a backup job	Reduces recovery wait times – don't wait for data transfer to the vault to finish	Configure Instant Restore retention (1 to 5 days)

Setup Recovery Services Vault Backup Options - VMs

Multiple servers can be protected using the same Recovery Services vault

Azure Workloads	On-Premises Workloads

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

vhd
vhdx

Download
mount
E:
E:\.....

robocopy

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)

CRASH CONSISTENT   APPLICATION CONSISTENT   FILE-SYSTEM CONSISTENT
30   0   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

Delete backup data

Backup item → Stop backup & delete data → **Soft deleted state** (Backup data retained for 14 days after 'stop backup' operation; backup retention policy not enforced) → Undelete backup item (within 14 days of 'stop backup' operation) → **Stop backup with retain data state** (Backups paused; backup retention policy doesn't apply; data retained forever)

Purge backup item (On 15th day after deletion, No user action required)

Resume

Data is permanently deleted

Backup item starts backing-up; retention policy applies and cleans expired recovery points

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

Recovery Service Vault
Region 1 ✗
Region 2 ✓   30 sec
Region 3 ✓   5 min
              15 min
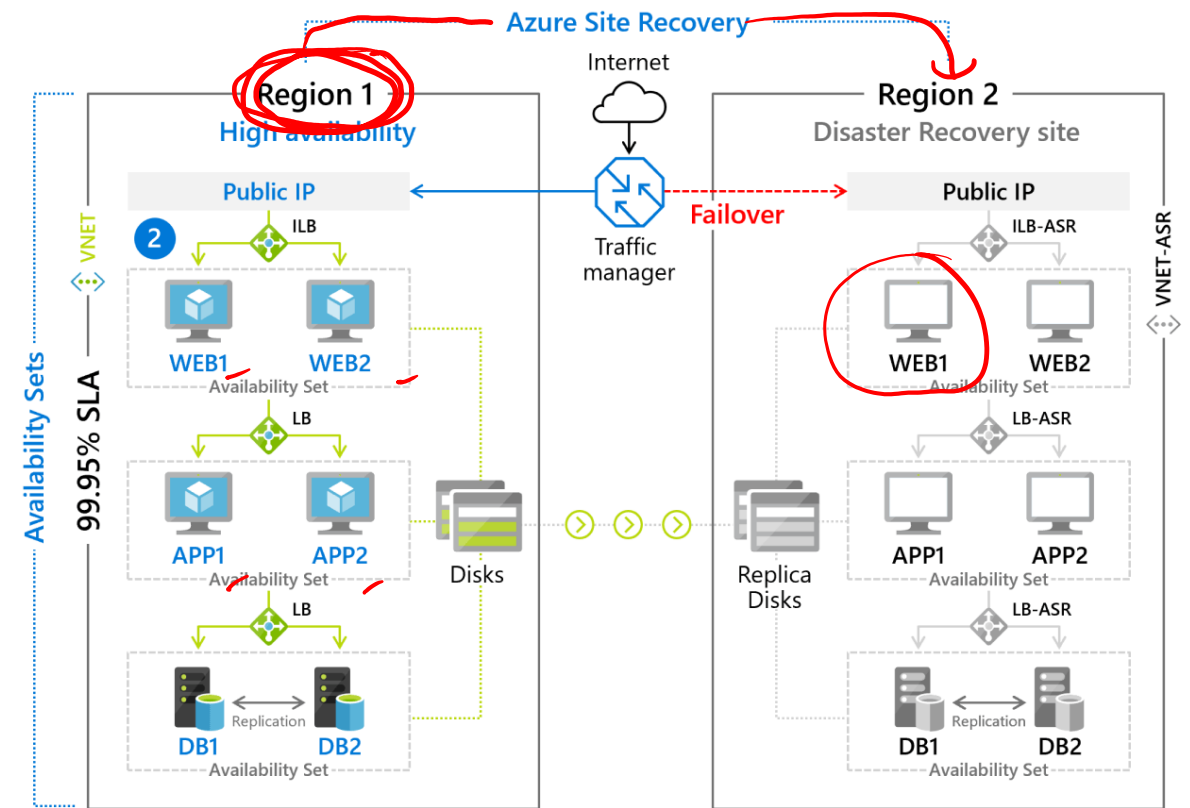
cold standy

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

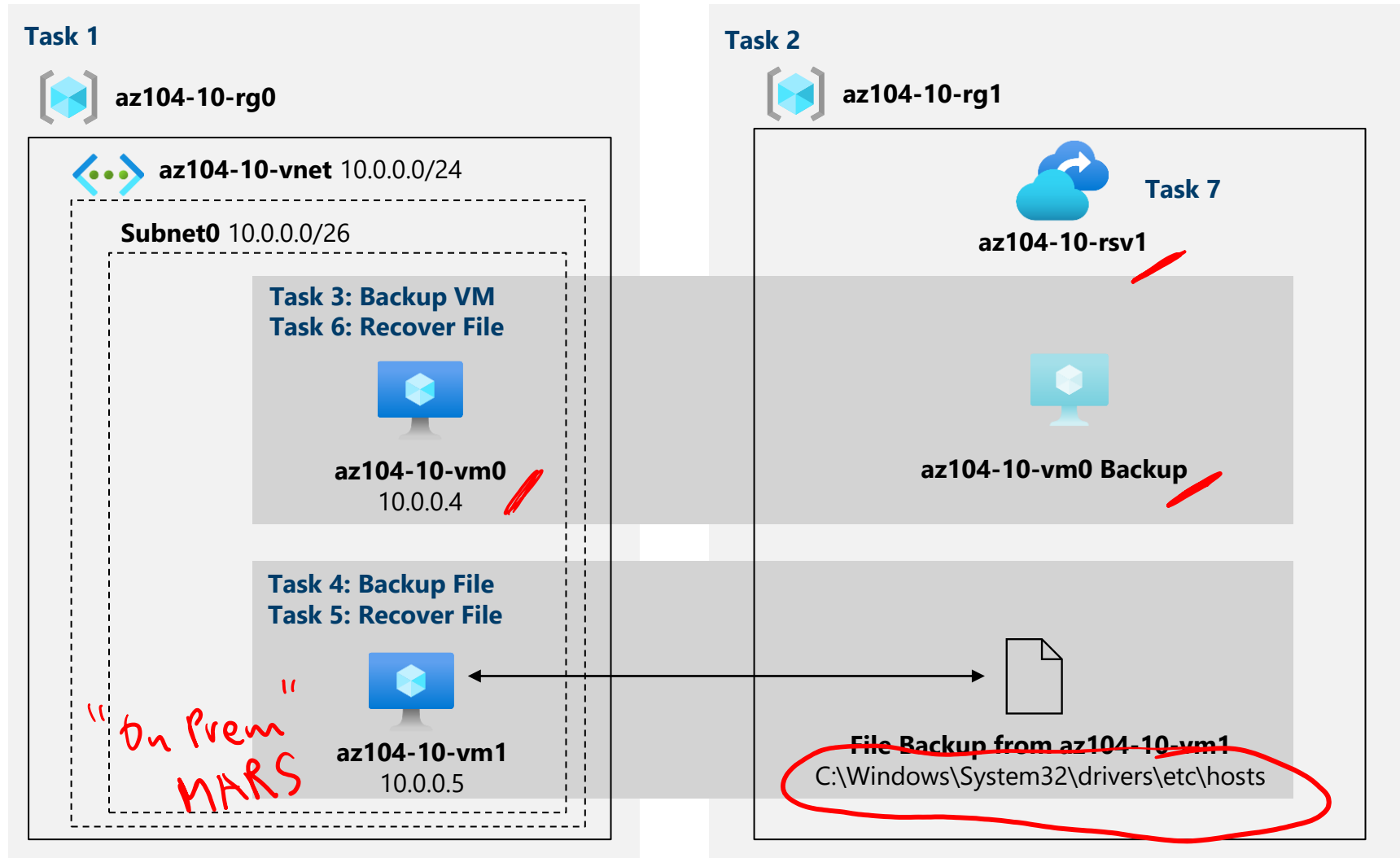**Task 4:** Implement File and Folder backup

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

Task 1

az104-10-rg0

az104-10-vnet 10.0.0.0/24

Subnet0 10.0.0.0/26

Task 3: Backup VM
Task 6: Recover File

az104-10-vm0
10.0.0.4

Task 4: Backup File
Task 5: Recover File

az104-10-vm1
10.0.0.5

"On Prem"
MARS

Task 2

az104-10-rg1

Task 7

az104-10-rsv1

az104-10-vm0 Backup

File Backup from az104-10-vm1
C:\Windows\System32\drivers\etc\hosts

End of presentation