

AZ-104

Administer Data Protection



AZ-104 Agenda

- 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 Data Protection

- Introduction to Azure Backup
- Protect your virtual machines by using Azure Backup
- Lab 10 – Implement Data Protection

Introduction to Azure Backup

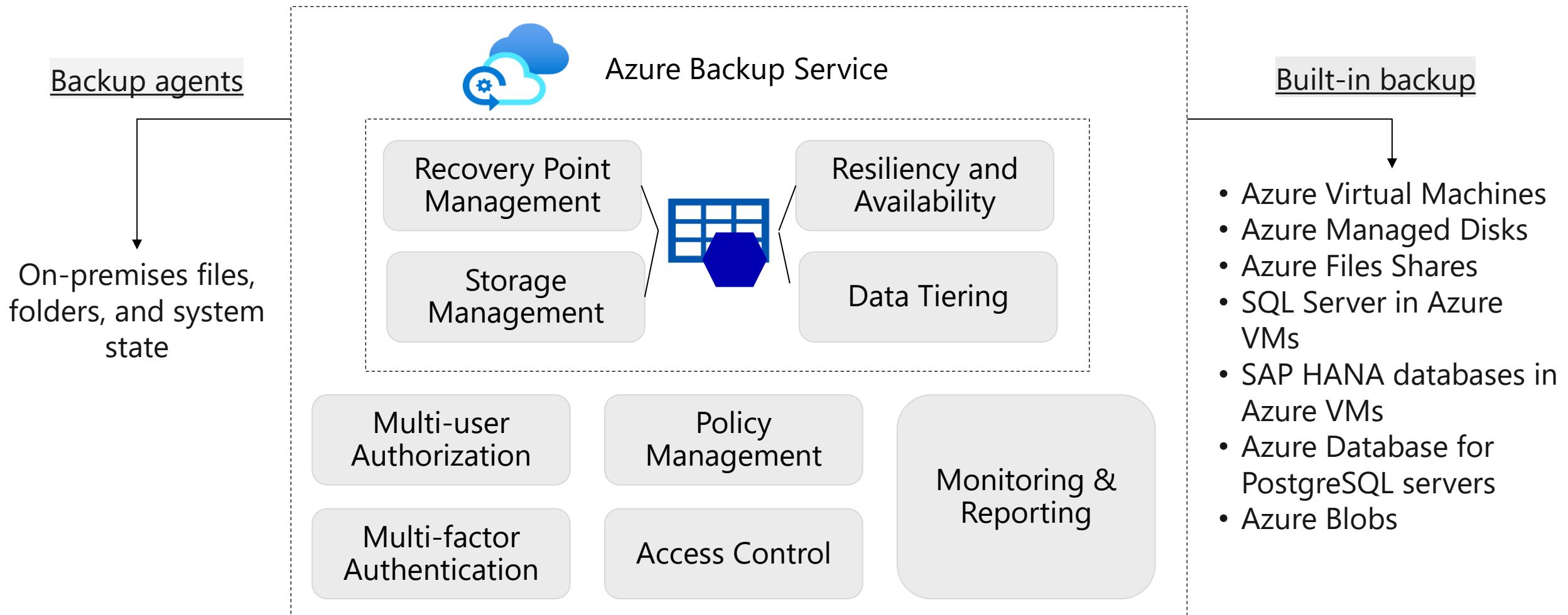
Learning Objectives – Introduction to Azure Backup

- What is Azure Backup?
- How Azure Backup works
- Use the Azure Business Continuity Center
- Demonstration – Backup Azure File Shares
- Learning Recap

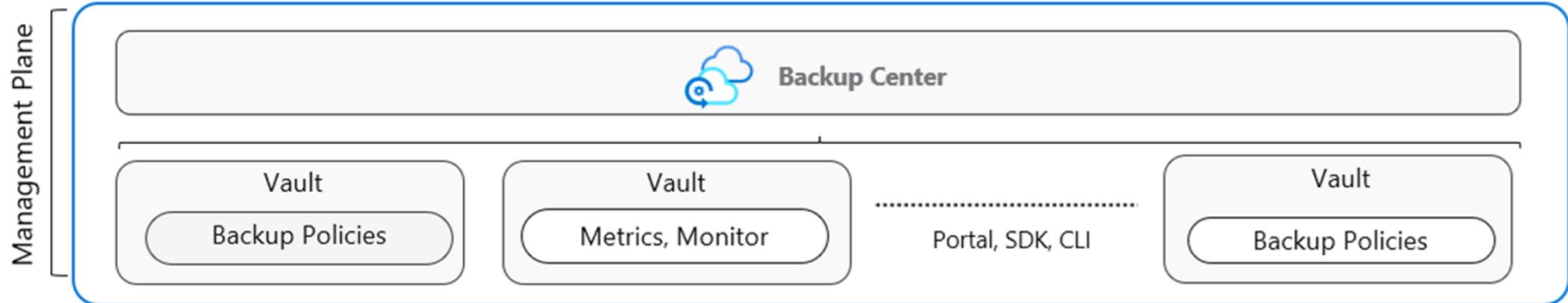
Monitor and maintain Azure resources (10–15%): Implement backup and recovery

- Create a Recovery Services vault
- Create an Azure Backup vault
- Create and configure a backup policy
- Configure and interpret reports and alerts for backups

What is Azure Backup?



How Azure Backup works (vaults and policies)



- Vaults store backup copies, recovery points, and backup policies
- Two types of vaults: Backup vault and Recovery Service vault
- Backup Policies define the data source, storage vault, and backup schedule
- The Business Continuity Center provides a single unified management experience (next slide)

Use the Azure Business Continuity Center

- Single pane of glass to manage BCDR protection
- Action center to protect Azure, Hybrid, and Edge environments
- At-scale unified monitoring capabilities across the solutions
- Evaluates your current configuration and proactively notifies you of any gaps
- View compliance against the applied policies

The screenshot shows the Azure Business Continuity Center (BCC) interface. The left sidebar contains navigation links: Overview, Getting started, Protection inventory (with sub-links for Protectable resources and Protected items), Monitoring + Reporting (with sub-links for Alerts, Metrics, Jobs, and Reports), Security + Threat management (with sub-links for Security posture), Governance (with sub-links for Azure Policies for protection and Protection compliance), Manage (with sub-links for Protection policies and Vaults), and Help.

Protection

Protection status	Count
Protected in both primary and secondary regions	0
Protected in primary region only	0
Protected in secondary region only	0
Not protected currently	0

Security

BCDR security coverage	Count
Excellent security	0
Good security	0
Fair security	0
Poor security	0
Not available	0

Learning Recap – Introduction to Azure Backup



Reference modules

- [Introduction to Azure Backup](#)

Check your knowledge questions and additional study

Protect your virtual machines by using Azure Backup

Learning Objectives – Protect your virtual machines with Azure Backup

- Explore options to protect virtual machine data
- Create virtual machine snapshots in Azure Backup
- Setup Recovery Services Vault backup options
- Backup Virtual Machines
- Restore Virtual Machines
- Demonstration – Virtual Machine Backups
- Manage soft delete (optional)
- Implement Azure Site Recovery
- Learning Recap

Monitor and maintain Azure resources (10–15%): Implement backup and recovery

- Perform backup and restore operations by using Azure Backup
- Configure Azure Site Recovery for Azure resources
- Perform a failover to a secondary region by using Site Recovery

Explore options to protect virtual machine data

Snapshots

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

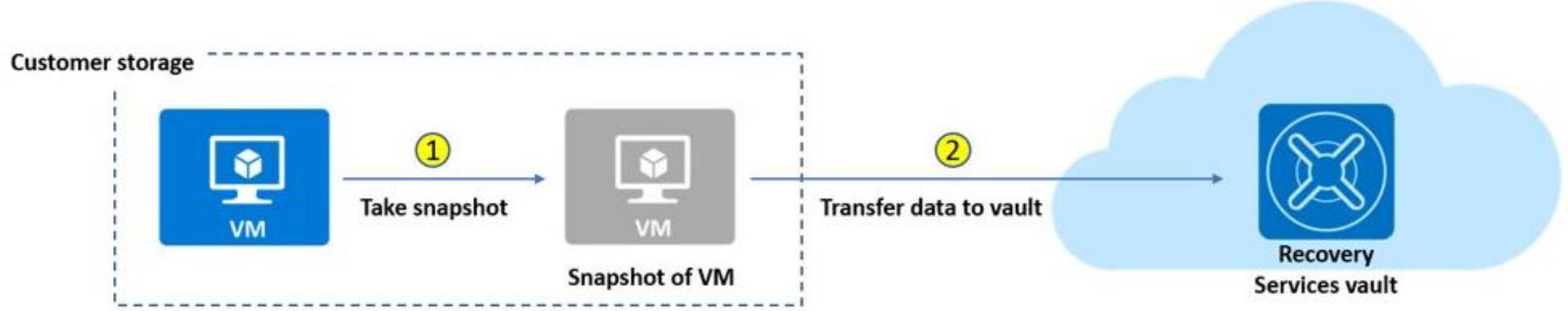
Azure Backup

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 in Azure Backup



Use snapshots taken as part of a backup job

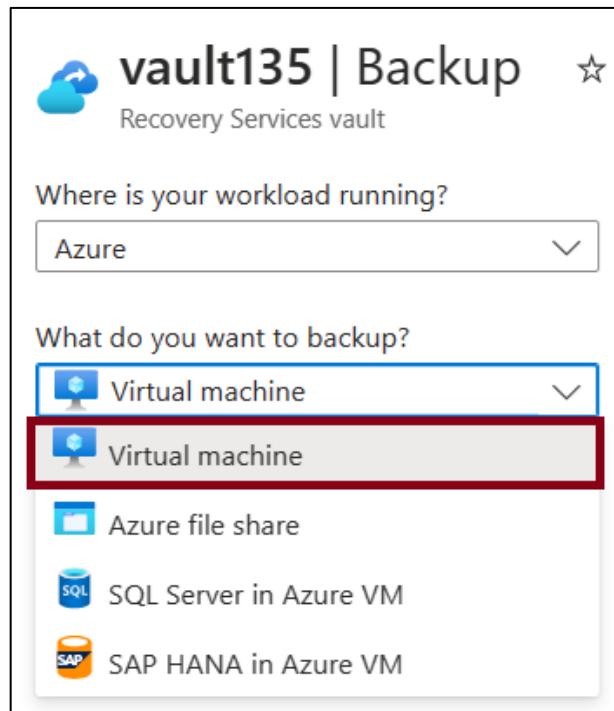
Reduces recovery wait times – don't wait for data transfer to the vault to finish

Configure Instant Restore retention (standard or enhanced)

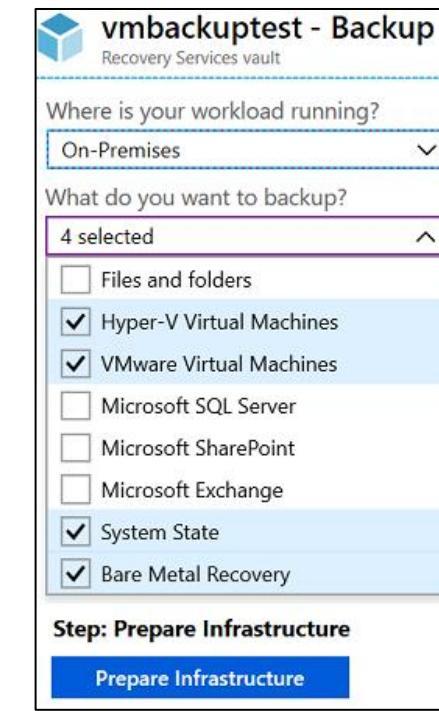
Set up Azure Recovery Services vault backup options

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

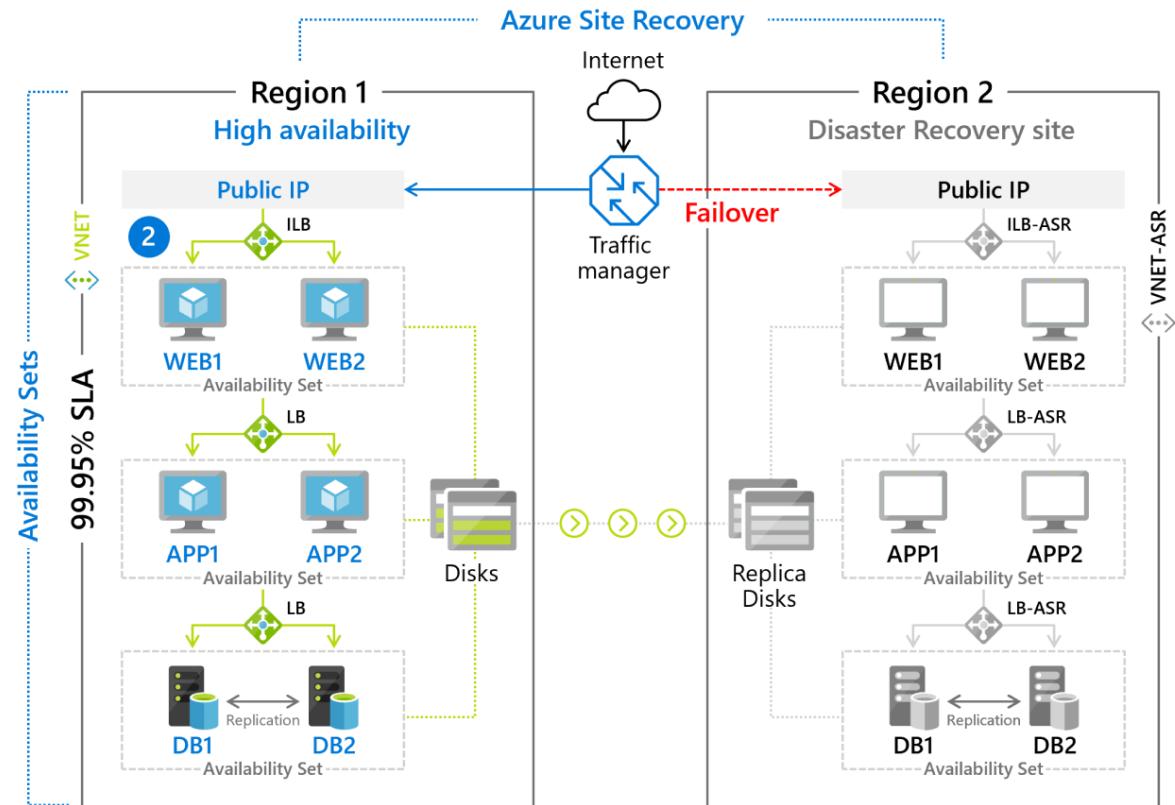
Once you trigger the restore operation, the Backup service creates a job for tracking the restore operation

The Backup service also creates and temporarily displays notifications, so you monitor how the backup is proceeding

The screenshot shows the Azure Backup service interface for a backup item named "ContosoWebFE1". At the top, there are five action buttons: "Backup now", "Restore VM", "File Recovery", "Stop backup", and "Resume backup". Below these are two sections: "Alerts and Jobs" and "Backup status". Under "Alerts and Jobs", there are links to "View all Alerts (last 24 hours)" and "View all Jobs (last 24 hours)". Under "Backup status", it shows "Backup Pre-Check" as "Passed" and "Last backup status" as "Success 3/12/2020, 12:20:38 AM". A horizontal line separates this from the "Restore points (30)" section. This section includes three summary counts: "CRASH CONSISTENT 30", "APPLICATION CONSISTENT 0", and "FILE-SYSTEM CONSISTENT 0". It also has two sorting headers: "Time" and "Consistency". Two restore points are listed: "3/12/2020, 12:20:42 AM" under "Crash Consistent" and "3/11/2020, 12:20:59 AM" under "Crash Consistent".

Implement Azure Site Recovery

- Manages the orchestration of disaster recovery
- Replicates workloads continuously from a primary location or region to a secondary location
- Failover to shift to the secondary location; fallback to return to the primary location



Learning Recap – Protect your virtual machines by using Azure Backup



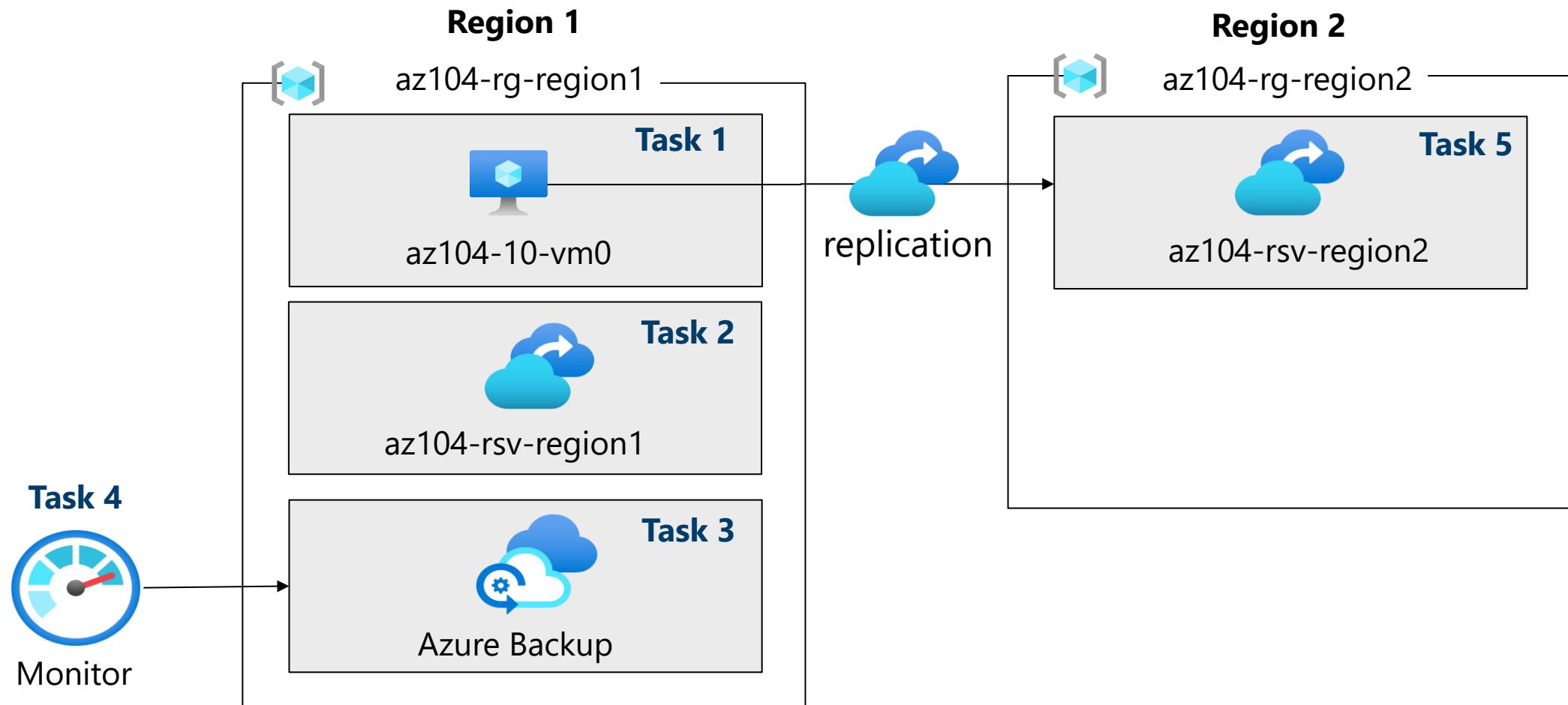
Check your knowledge questions and additional study

Reference modules

- [Protect your virtual machines by using Azure Backup](#)
- [Monitor workload protection in Azure Backup](#)
- [Implement hybrid backup and recovery with Windows Server IaaS](#)

Lab – Implement Data Protection

Lab 10 – Architecture diagram



End of presentation