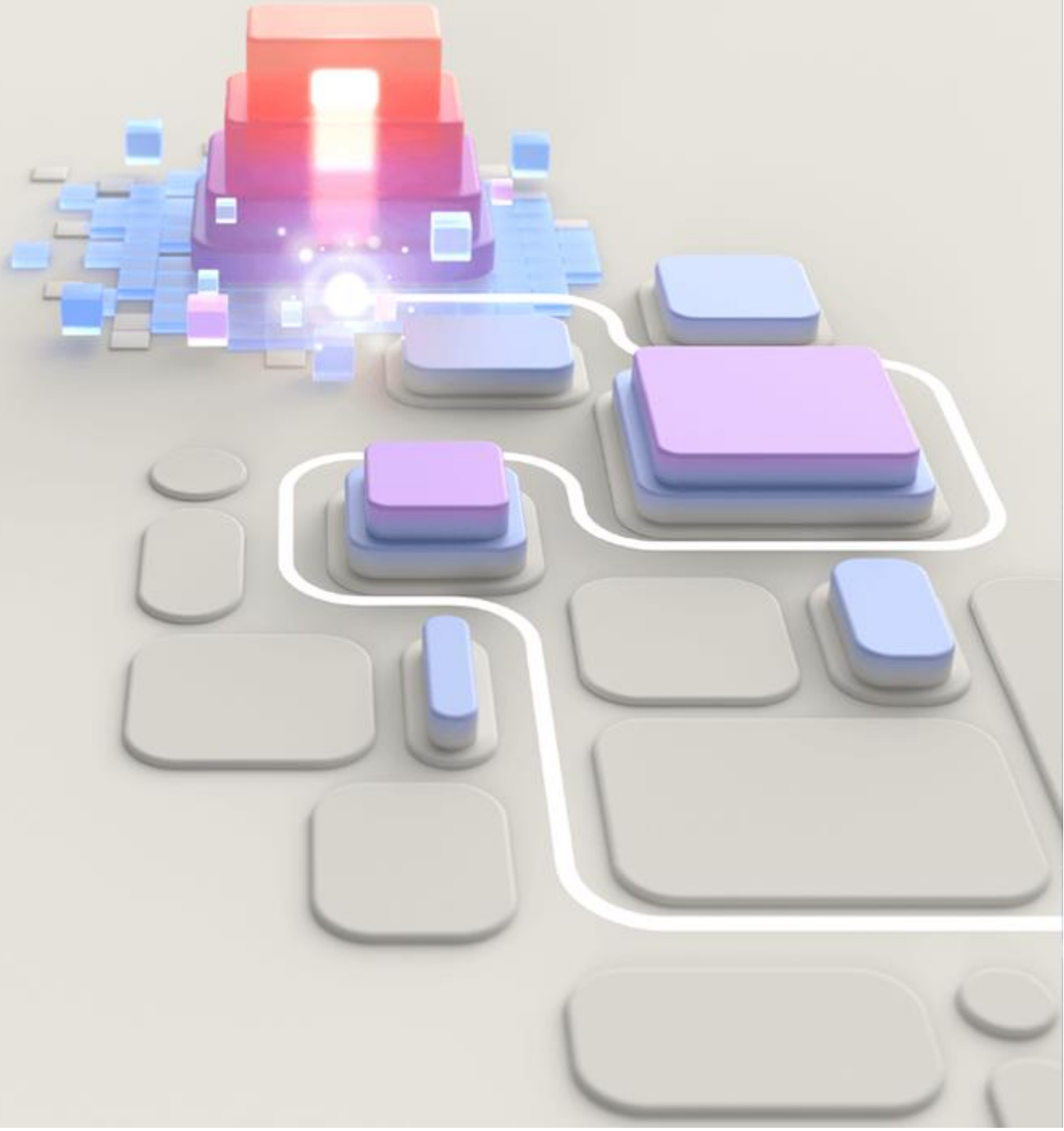
Microsoft

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

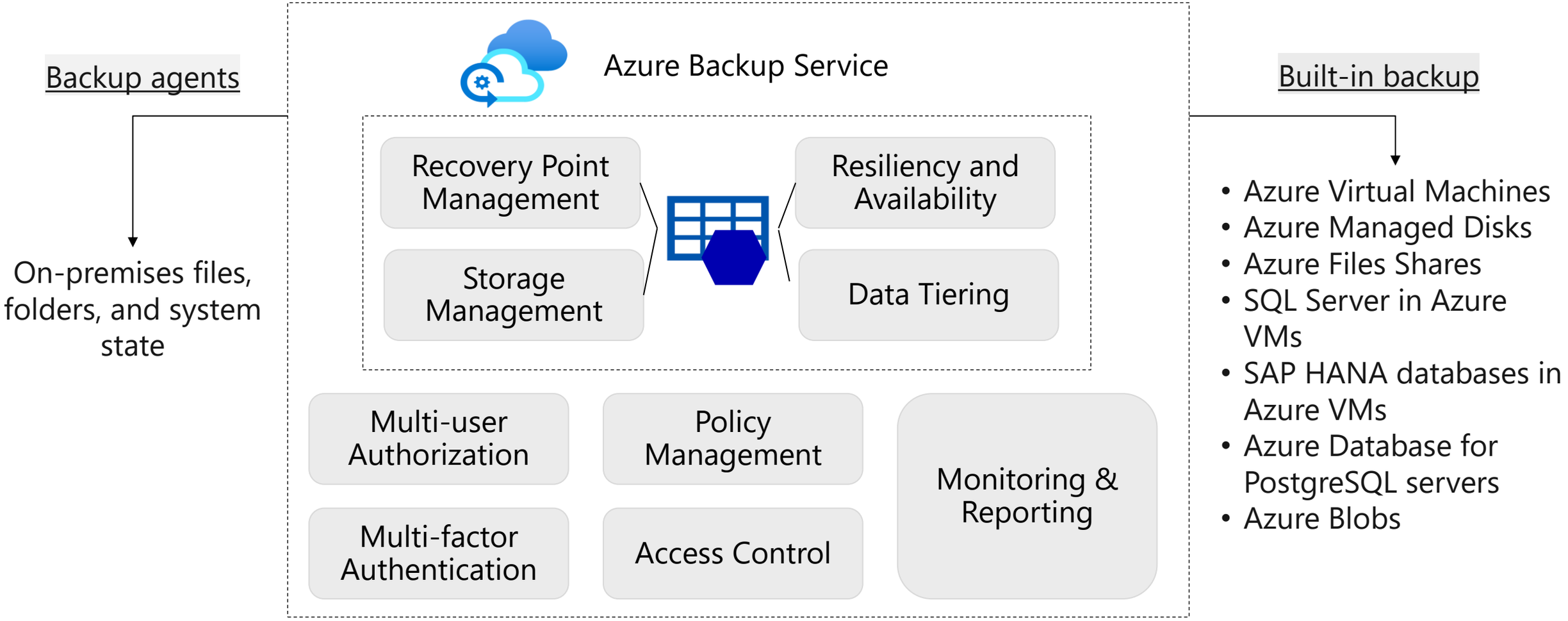
Learning Objectives – Introduction to Azure Backup

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

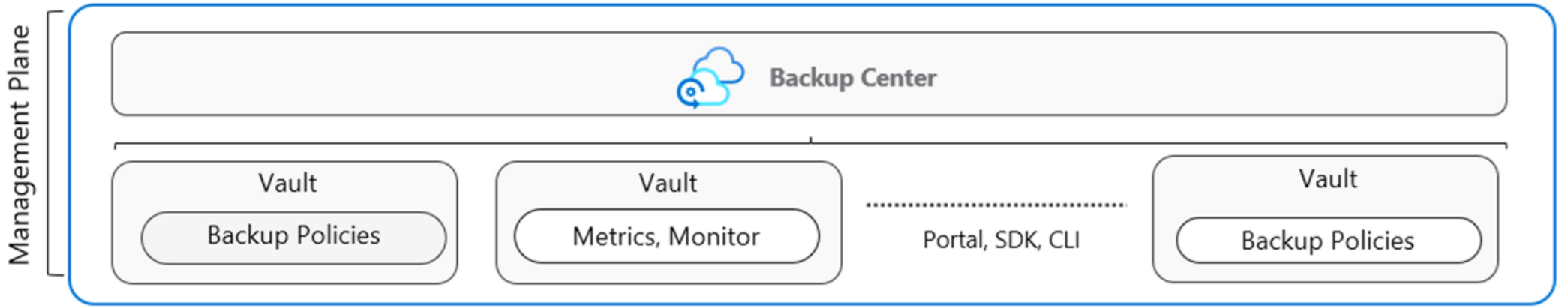
Monitor and maintain Azure resources (10–15%): Implement backup and recovery

- 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?



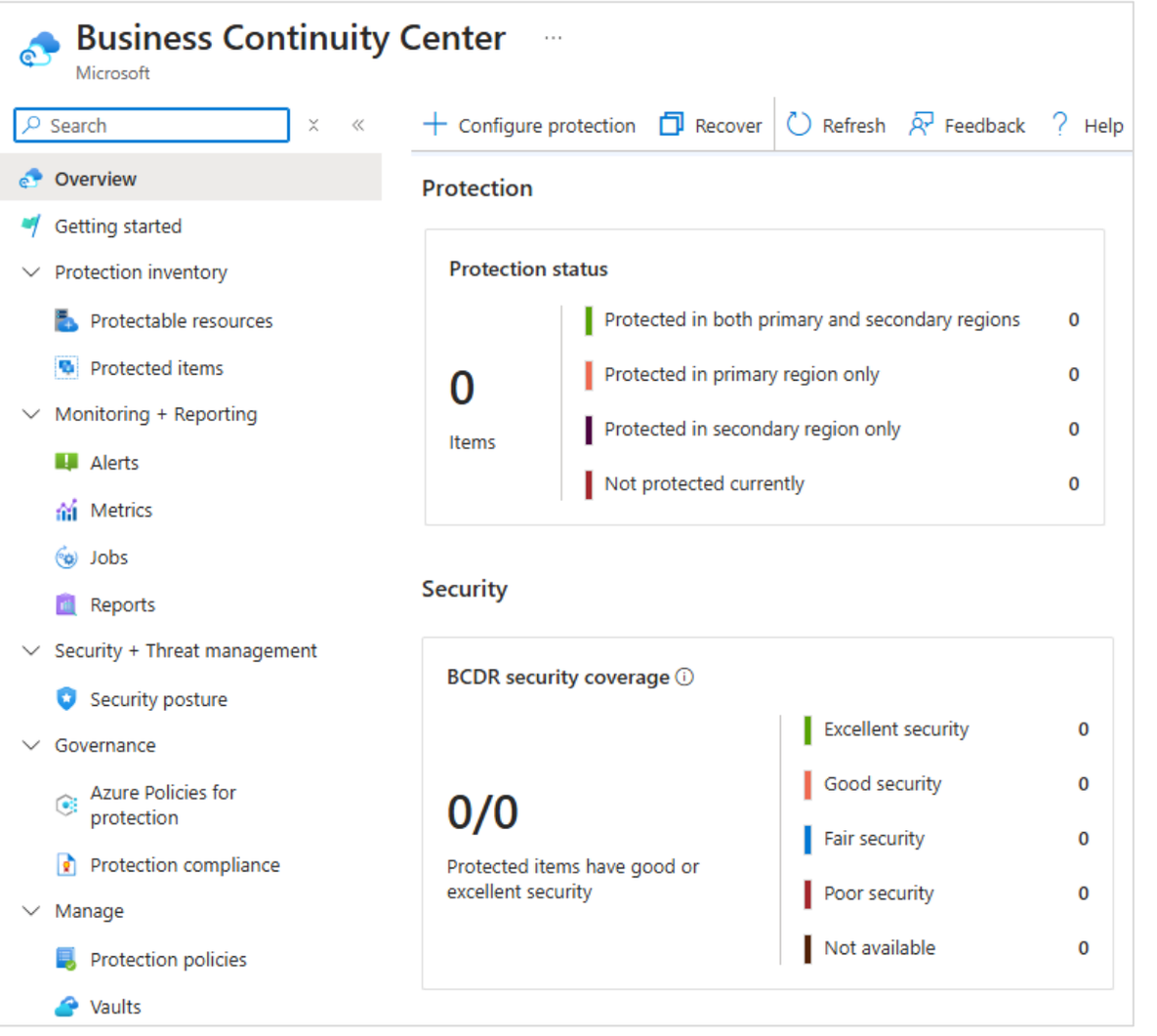
How Azure Backup works (vaults and policies)



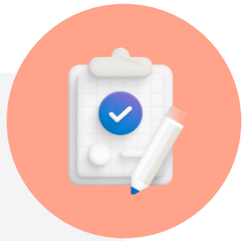
- Vaults store backup copies, recovery points, and backup policies
- Two types of vaults: Backup vault and Recovery Service vault
- Backup Policies define the data source, storage vault, and backup schedule
- The Business Continuity Center provides a single unified management experience (next slide)

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



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

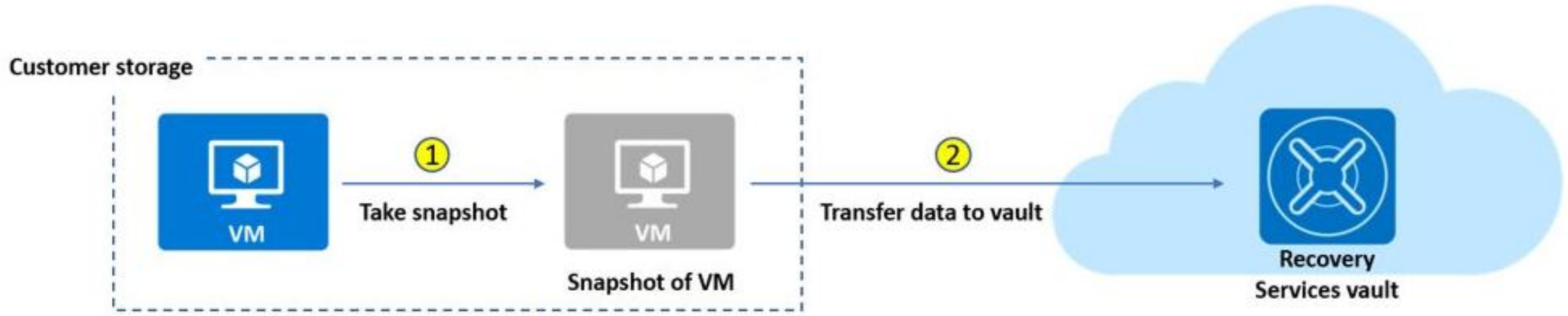
Monitor and maintain Azure resources (10–15%): Implement backup and recovery

- 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	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 in Azure Backup



Use snapshots taken as part of a backup job

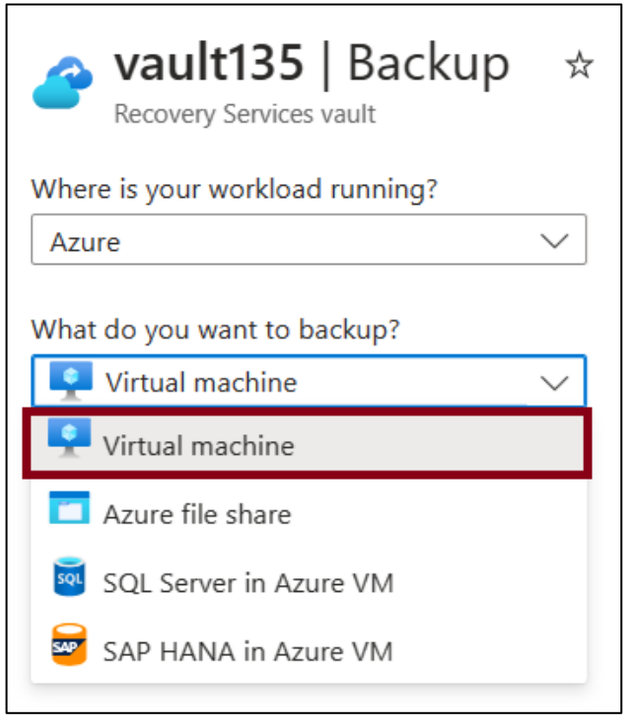
Reduces recovery wait times – don't wait for data transfer to the vault to finish

Configure Instant Restore retention (standard or enhanced)

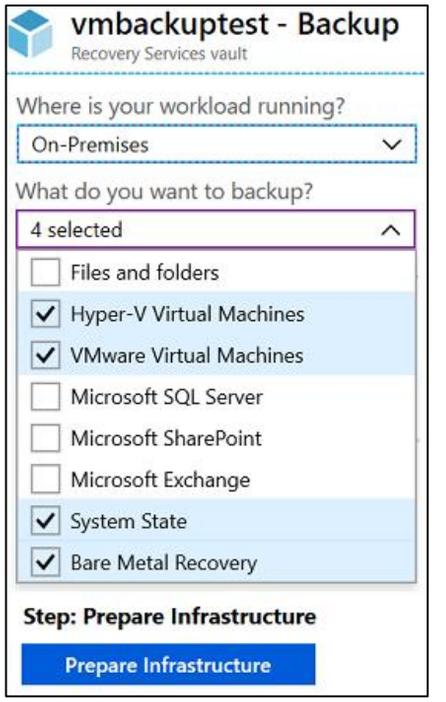
Set up Azure Recovery Services vault backup options

Multiple servers can be protected using the same Recovery Services vault

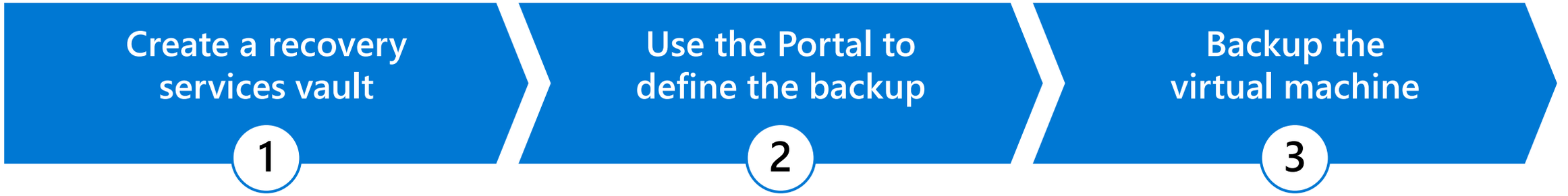
Azure Workloads



On-Premises Workloads



Backup Virtual Machines



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

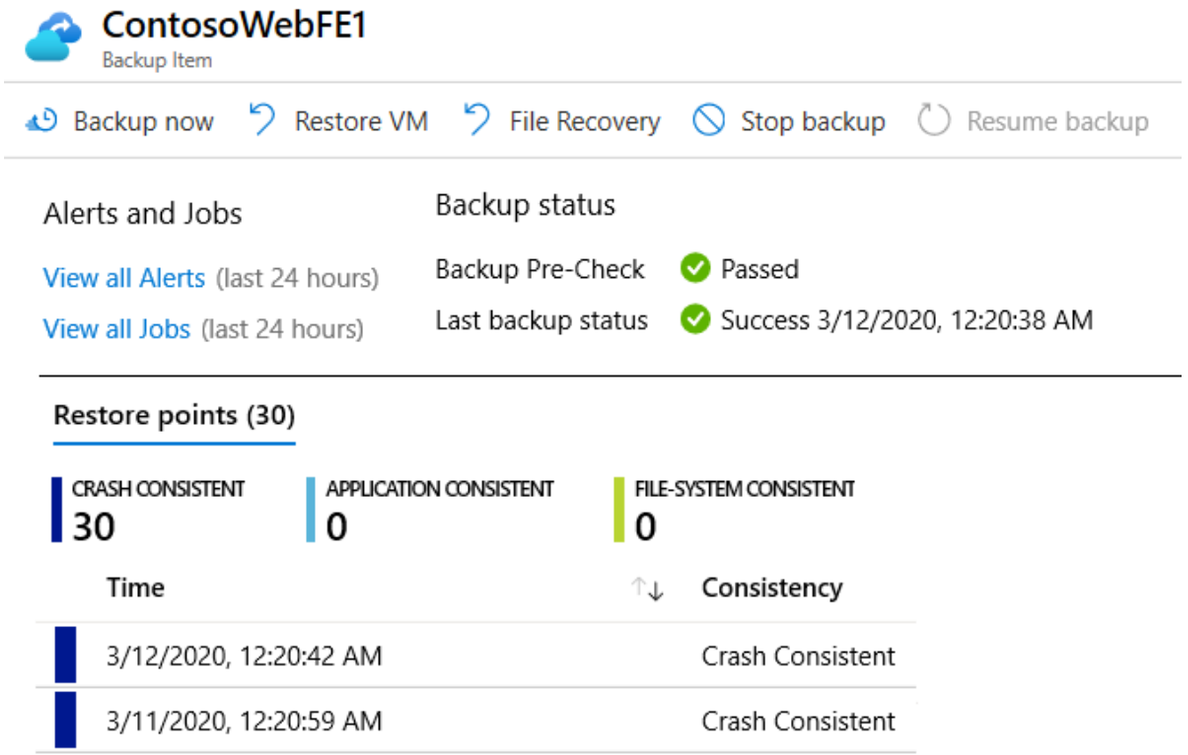
Take snapshots (recovery points) of your data at defined intervals. These snapshots are stored in recovery services vaults

For the Backup extension to work, the Azure VM Agent must be installed on the Azure virtual machine

Restore Virtual Machines

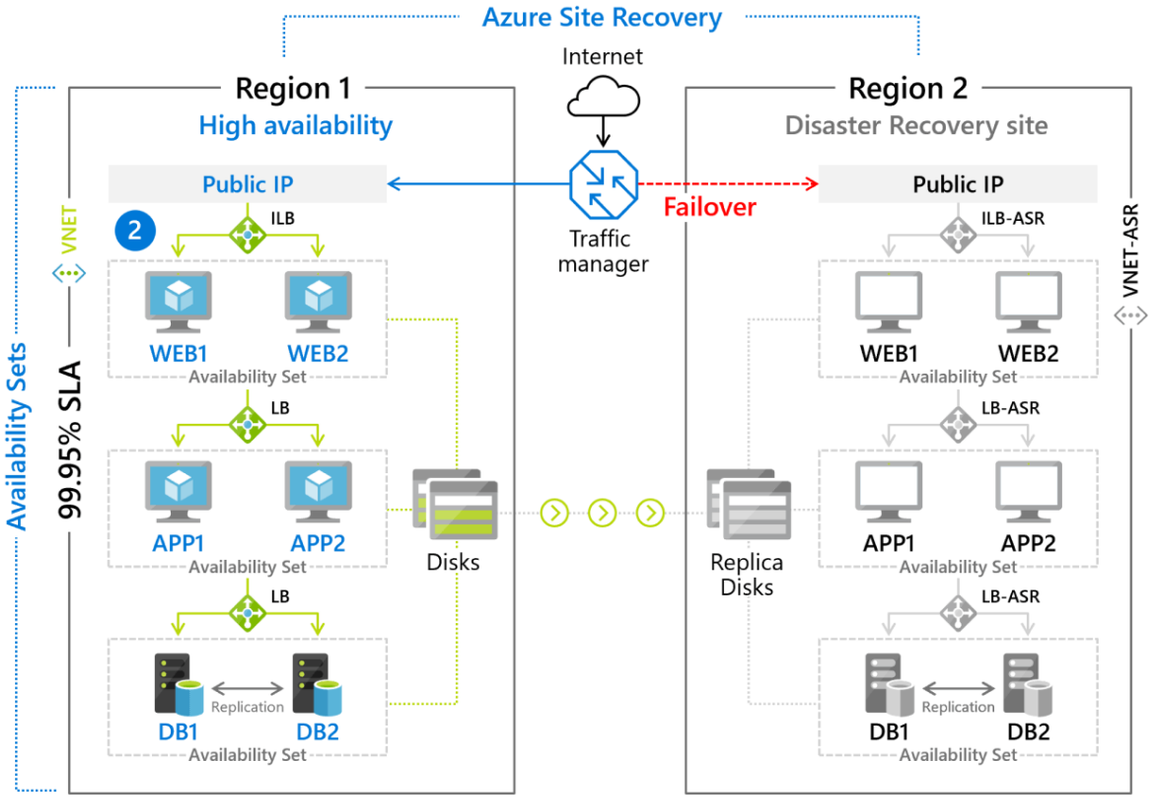
Once you trigger the restore operation, the Backup service creates a job for tracking the restore operation

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



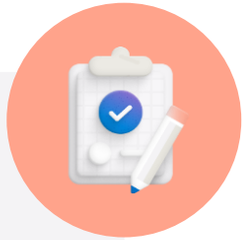
Implement Azure Site Recovery

- 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; failback to return to the primary location



Learning Recap – Protect your virtual machines by using Azure Backup

Check your knowledge questions and additional study

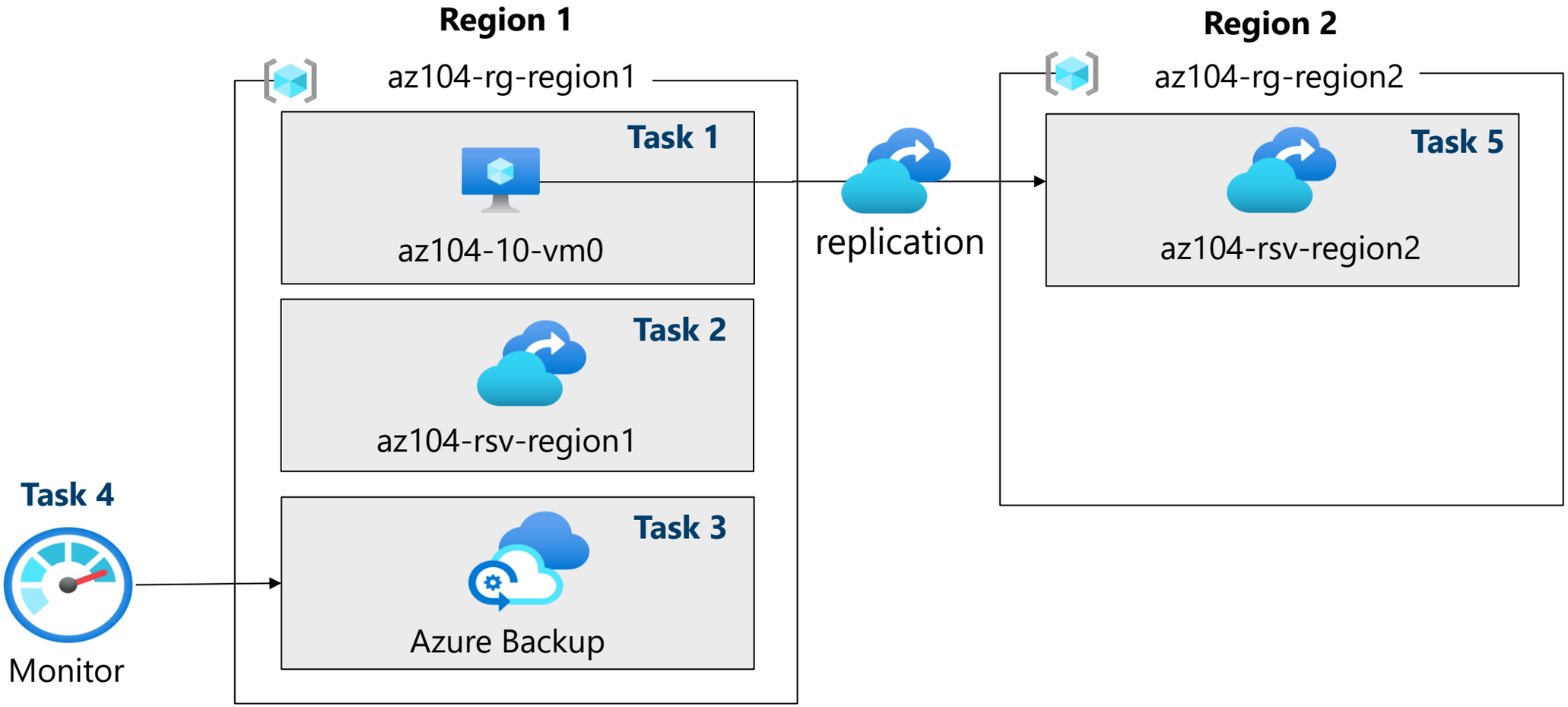


Reference modules

- 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