



# AZ-305T00A

## Microsoft

### Azure Infrastructure

### Architect



# Design a business continuity solution



# Learning Objectives

- Design for backup and recovery
- Design for Azure Backup
- Design for Azure blob backup and recovery
- Design for Azure Files backup and recovery
- Design for Azure virtual machine backup and recovery
- Design for Azure SQL backup and recovery
- Design for Azure Site Recovery
- Learning recap

## AZ-305: Design Business Continuity Solutions (15-20%)

### Design a Solution for Backup and Disaster Recovery

- Recommend a recovery solution for Azure and hybrid workloads that meets recovery objectives
- Recommend a backup and recovery solution for compute
- Recommend a backup and recovery solution for databases
- Recommend a backup and recovery solution for unstructured data

# Design for backup and recovery



# Plan for backup and recovery

Identify your business needs and create a plan to address those needs

- What are your workloads and their usage?
- What are the usage patterns for your workloads?
- What are the availability metrics (MTTR and MTBF)?
- What are the recovery metrics (RTO and RPO)?
- What are the workload availability targets?
- What are your SLAs?



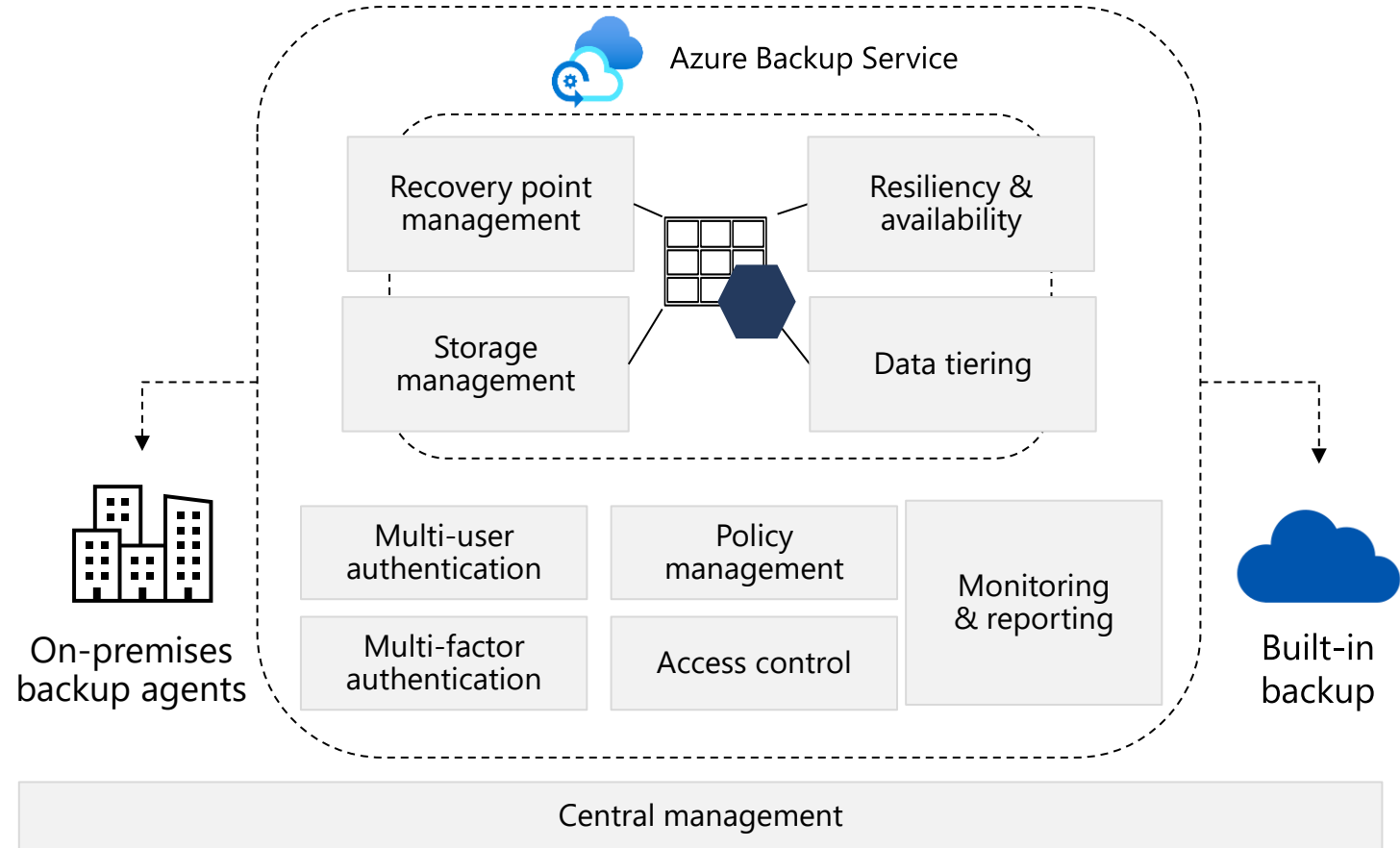
# Design for Azure Backup



# When to use Azure Backup

Azure Backup is a full-service backup and recovery solution.

- Unlimited scaling with high availability and unlimited data transfer
- Automatic replication of locally redundant storage and geo-redundant storage using a pay-as-you-use model
- Application-consistent backups with secure transmission and storage of your data in Azure
- No limits on the length of time you can keep the backup data



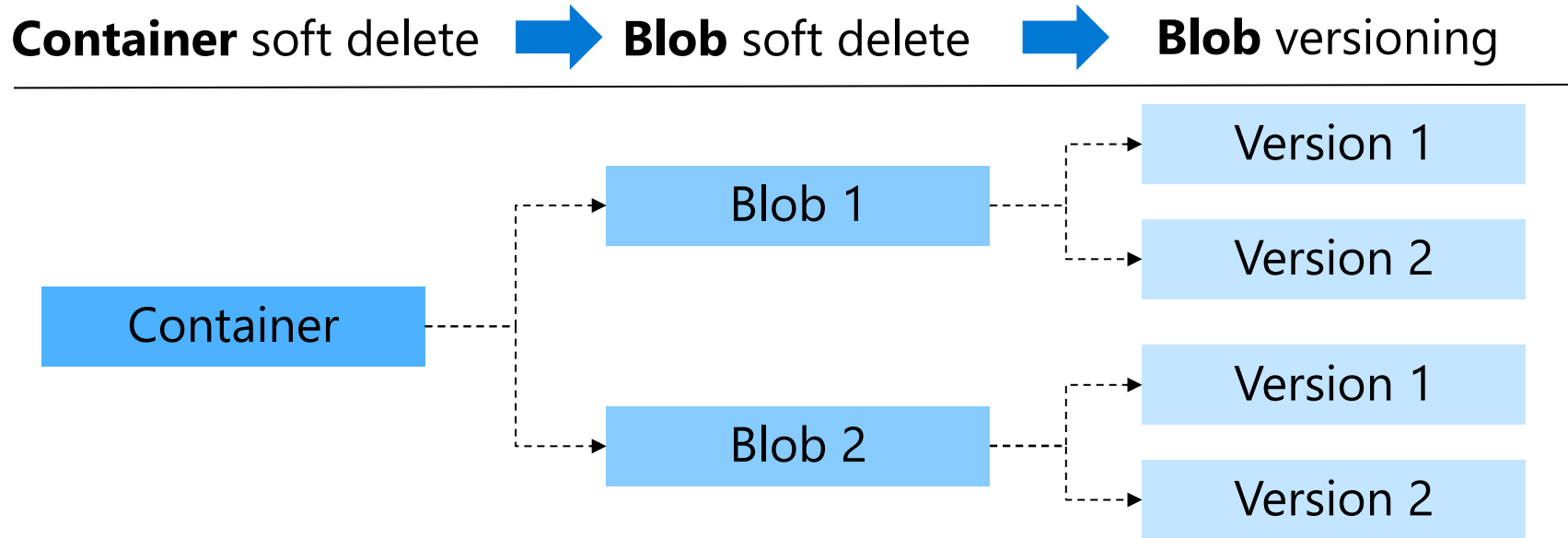
# Design for blob backup and recovery





# Considerations for soft delete

Consider soft delete with recovery times from 1 to 365 days

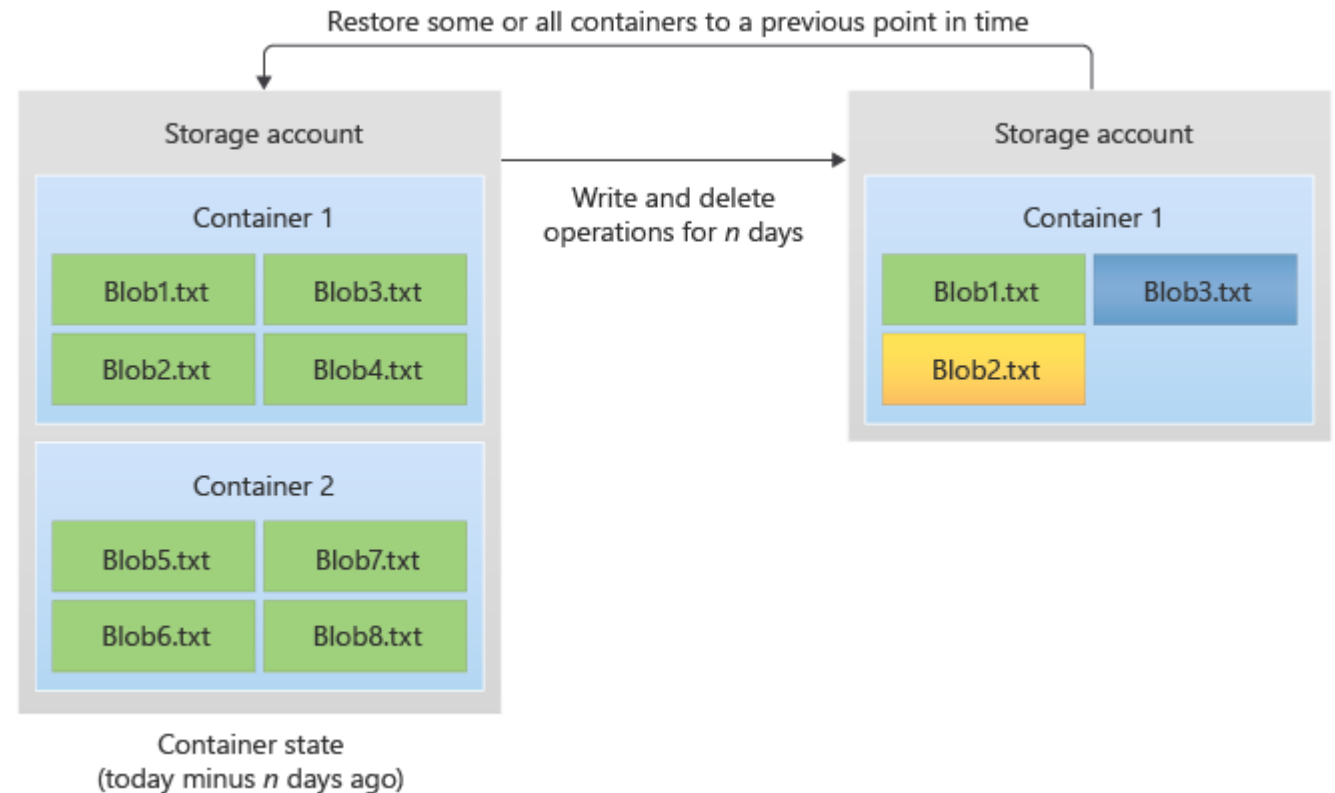


- Maintains the deleted data in the system for a specified retention period
- Soft delete protects blobs, snapshot, containers, or versions from accidental deletes or overwrites

# Considerations for point-in-time restore

## Consider point-in-time restore for block blobs

- Useful in scenarios where a user or application accidentally deletes data or where an application error corrupts data
- Use policy to specify the retention period



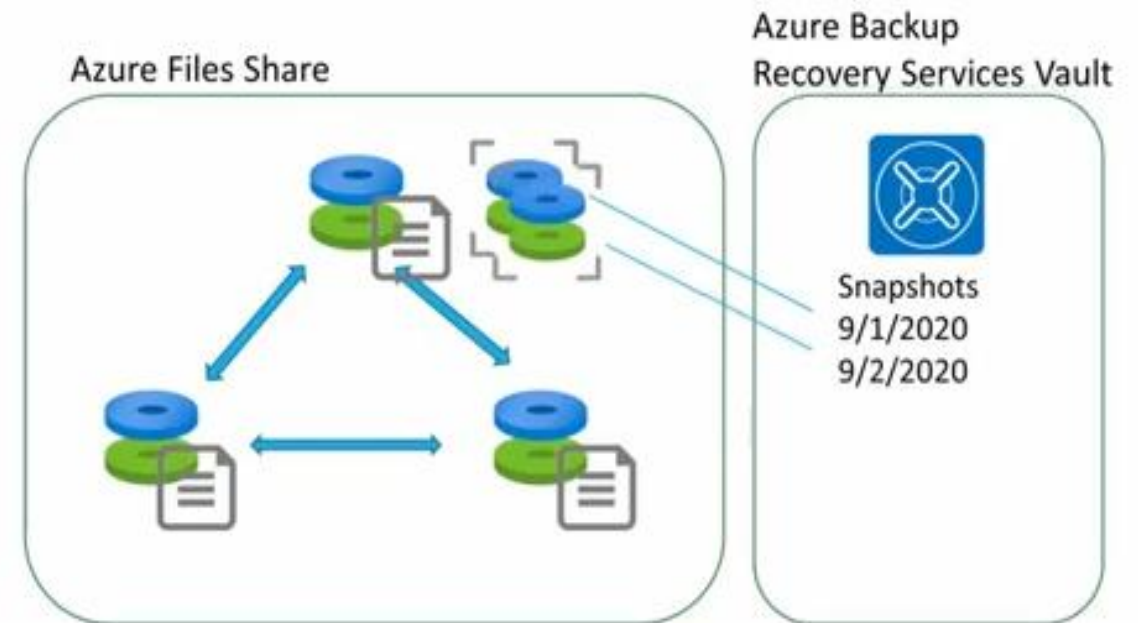
# Design for Azure Files backup and recovery



# Considerations for Azure Files backup and recovery

## Consider snapshots for both blobs and Azure Files

- Organize file shares with backup in mind
- Snapshots can be on-demand or scheduled using Azure Backup and backup policies.
- Snapshots are at the file share root – retrieval is at the file
- Use snapshots to cover the time between daily backups
- Use instant restore – consider self service restore
- Snapshots are incremental - snapshot before code deployments.



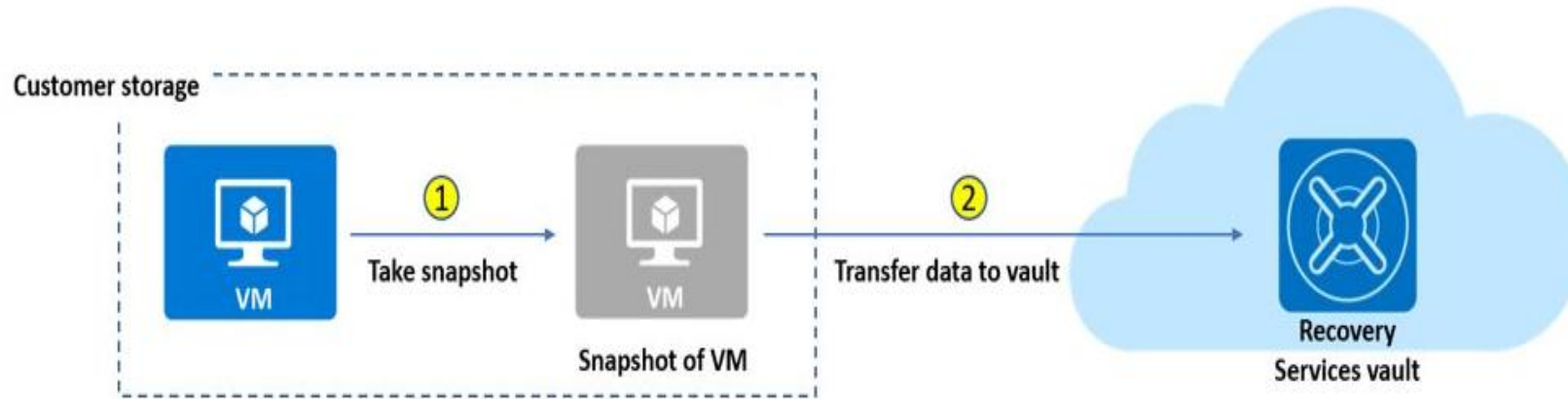
# Design for virtual machine backup and recovery





# Considerations for Azure virtual machines

Guard against unintended destruction of the data on your VMs.



- Group VMs into customized backup policies
- Combine short-term (daily), long-term (weekly), and on-demand backups
- Identify needs for app, crash, and file backups – practice the restore
- Consider Cross Region Restore (CRR) for VMs in the paired region
- Periodically review your policies – add monitor and alert

# Design for Azure SQL backup and recovery

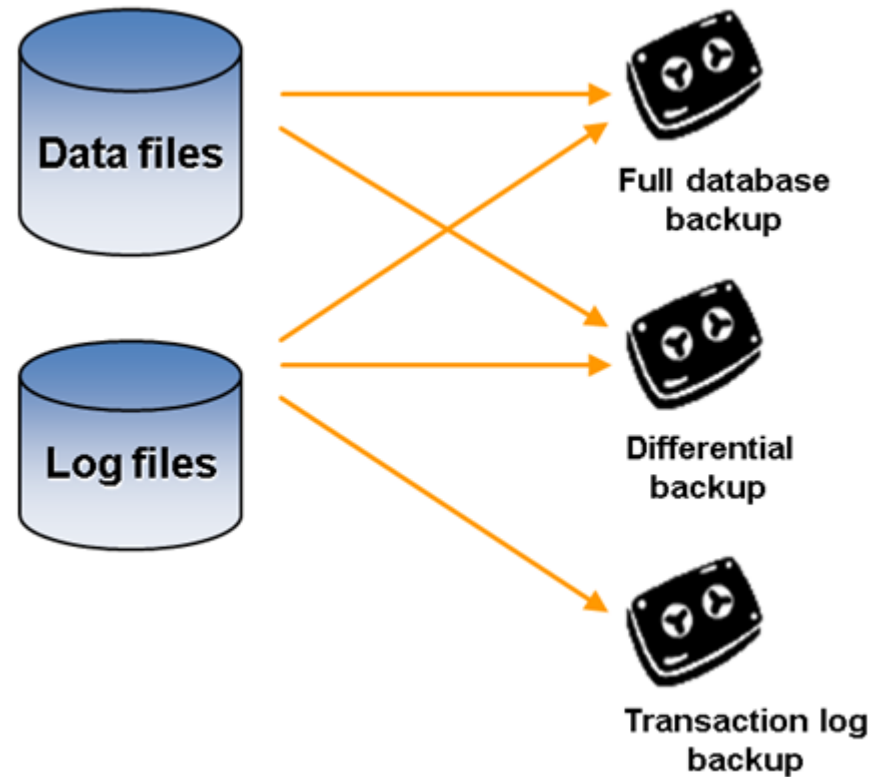


# How Azure SQL backup works

SQL Database and SQL Managed Instances automatically backup.

For fully consistent backups, the following are taken:

- Full backups once a week
- Differential backups every 12-24 hours
- Transactional log backups every 5-10 minutes



# Considerations for Azure SQL backup

## Restore in the retention period or use a long-term retention policy

- Restore an existing database to a point in time in the past within the retention period
- Restore a deleted database to the time of deletion or to any point in time within the retention period
- Restore a database to another geographic region
- Restore a database from a specific long-term backup of a single database or pooled database
- Long term retention uses read-access geo-redundant storage (RA-GRS)

Retention period	Long term retention
35 days	Up to 10 years

# Design for Azure Site Recovery

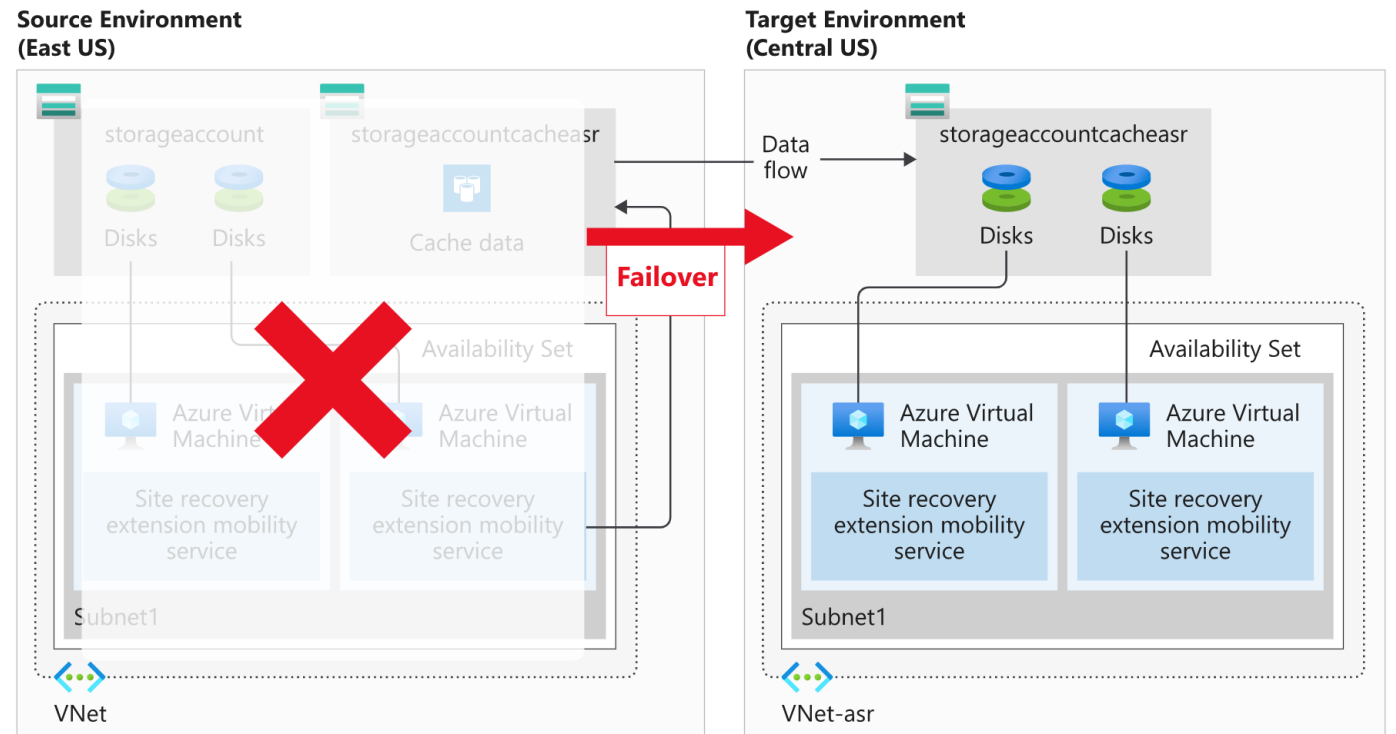




# When to use Azure Site Recovery

## Failover for Azure, on-premises, other cloud provider resources

- Perform disaster recovery and validate the replication strategy
- Migrate on-premises VMs and physical servers to Azure
- Replicate virtual machines between regions
- Define retention history and frequency of snapshots



# Combine Azure Site Recovery with Azure Backup

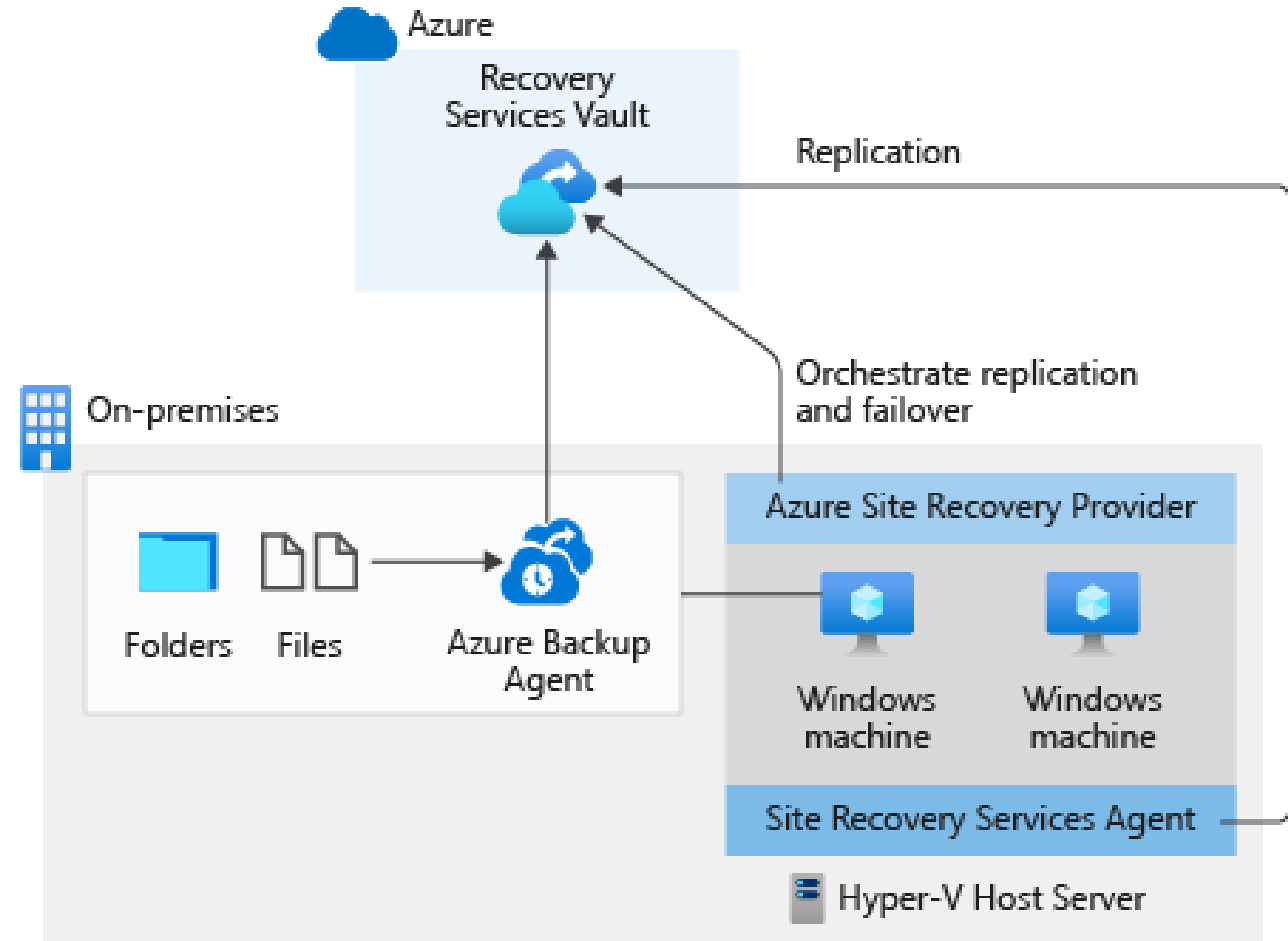
## Combine ASR with Azure Backup

### Requirement

- Backup all the files and folders in this virtual machine to Azure.
- Protect any workloads running on the virtual machine and keep running them even if the virtual machine fails.

### Azure Backup

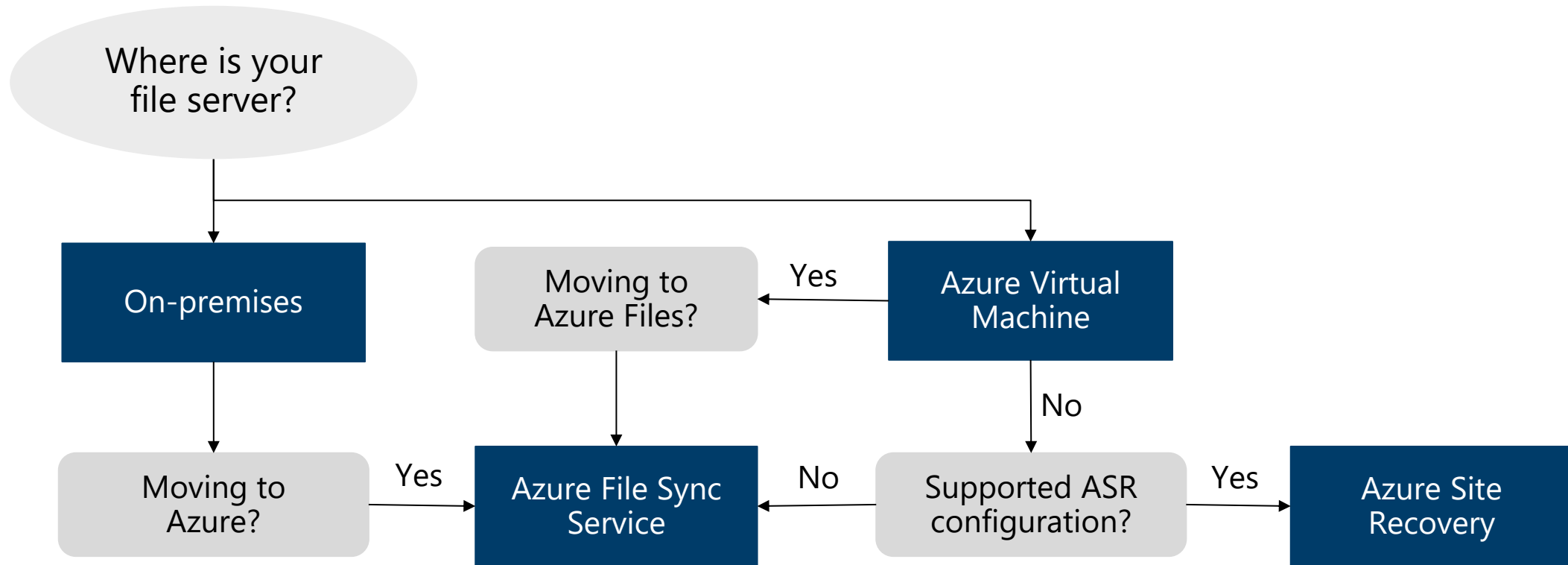
- Azure Backup periodically backs up the files and folders on the Windows machine to Azure.
- This process ensures they are secure and retrievable even if the whole on-premises environment stops functioning.



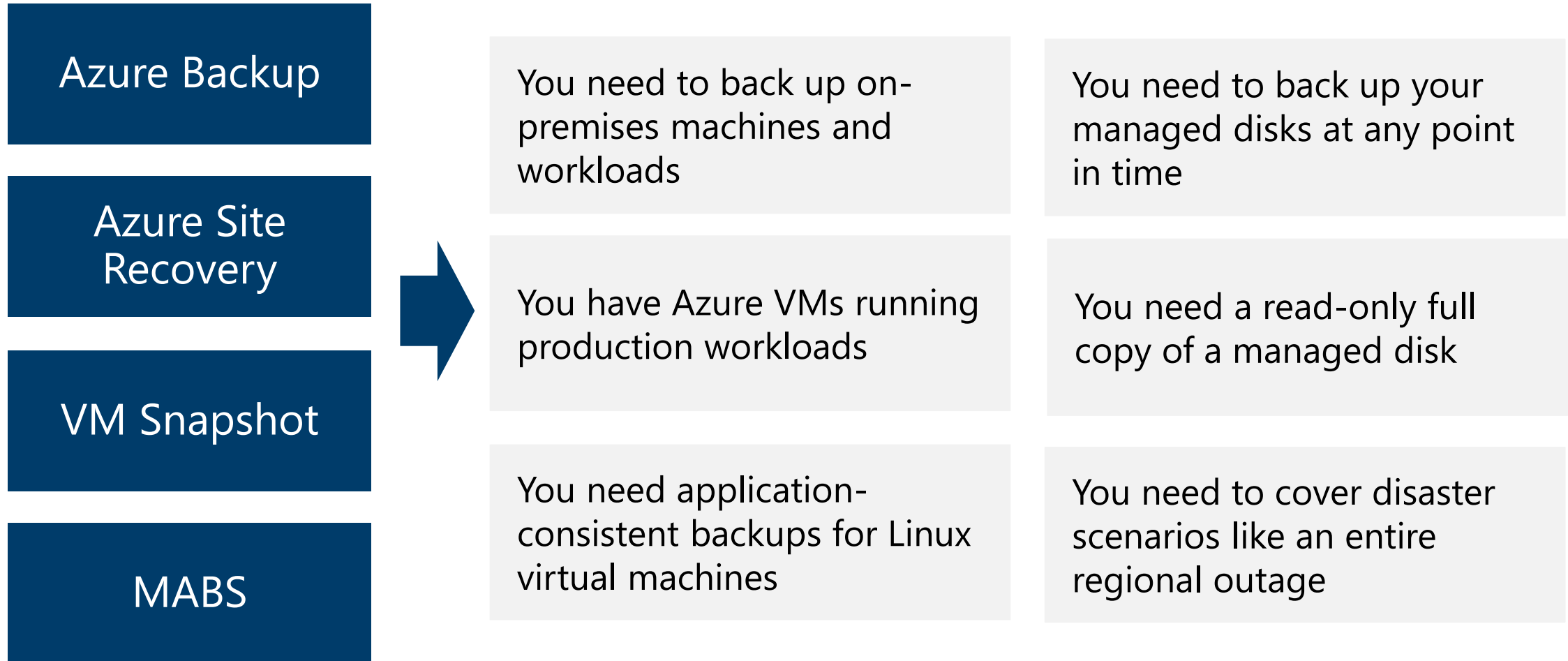
# Review



# Review file server backup and recovery options

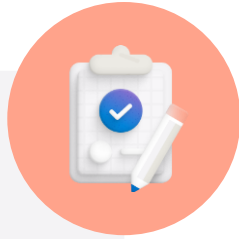


# Recommend a disaster recovery method (activity)





# Learning Recap – Business continuity solutions



Check your  
knowledge  
questions and  
review

## Reference modules

- [Protect your virtual machines by using Azure Backup](#)
- [Disaster recovery and backup](#)
- [Back up and restore your Azure SQL database](#)
- [Protect your Azure infrastructure with Azure Site Recovery](#)
- [Design your site recovery solution in Azure](#)

## Optional exercises:

- [Backup and restore your Azure SQL database](#)

# Instructor resources (hidden)



# End of presentation

