

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?

Azure Architects design solutions to back up and recover their data to avoid costly business interruptions. Microsoft Azure provides an end-to-end backup and disaster recovery solution to support multiple scenarios. It's easy to implement, secure, scalable, and cost-effective.



Consideration	Description
What are your workloads and their usage?	A workload is a distinct capability or task that is logically separated from other tasks, in terms of business logic and data storage requirements. Each workload probably has different requirements for availability, scalability, data consistency, and disaster recovery.
What are the usage patterns for your workloads?	Usage patterns can determine your requirements. Identify differences in requirements during both critical and non-critical periods. To ensure uptime, plan redundancy across several regions in case one region fails. Conversely, to minimize costs during non-critical periods, you can run your application in a single region.
What are the availability metrics?	Mean time to recovery (MTTR) and mean time between failures (MTBF) are the typically used metrics. MTBF is how long a component can reasonably expect to last between outages. MTTR is the average time it takes to restore a component after a failure. Use these metrics to determine where you need to add redundancy, and to determine service-level agreements (SLAs) for customers.
What are the recovery metrics?	The recovery time objective (RTO) is the maximum acceptable time one of your apps can be unavailable following an incident. The recovery point objective (RPO) is the maximum duration of data loss that is acceptable during a disaster. Also consider the recovery level objective (RLO). This metric determines the granularity of recovery. In other words, whether you must be able to recover a server farm, a web app, a site, or just a specific item. To determine these values, conduct a risk assessment. Ensure that you understand the cost and risk of downtime or data loss in your organization.
What are the workload availability targets?	To help ensure that your app architecture meets your business requirements, define target SLAs for each workload. Account for the cost and complexity of meeting availability requirements, in addition to application dependencies.
What are your SLAs?	In Azure, the SLA describes the Microsoft commitments for uptime and connectivity. If the SLA for a particular service is 99.9 percent, you should expect the service to be available 99.9 percent of the time.

Tip

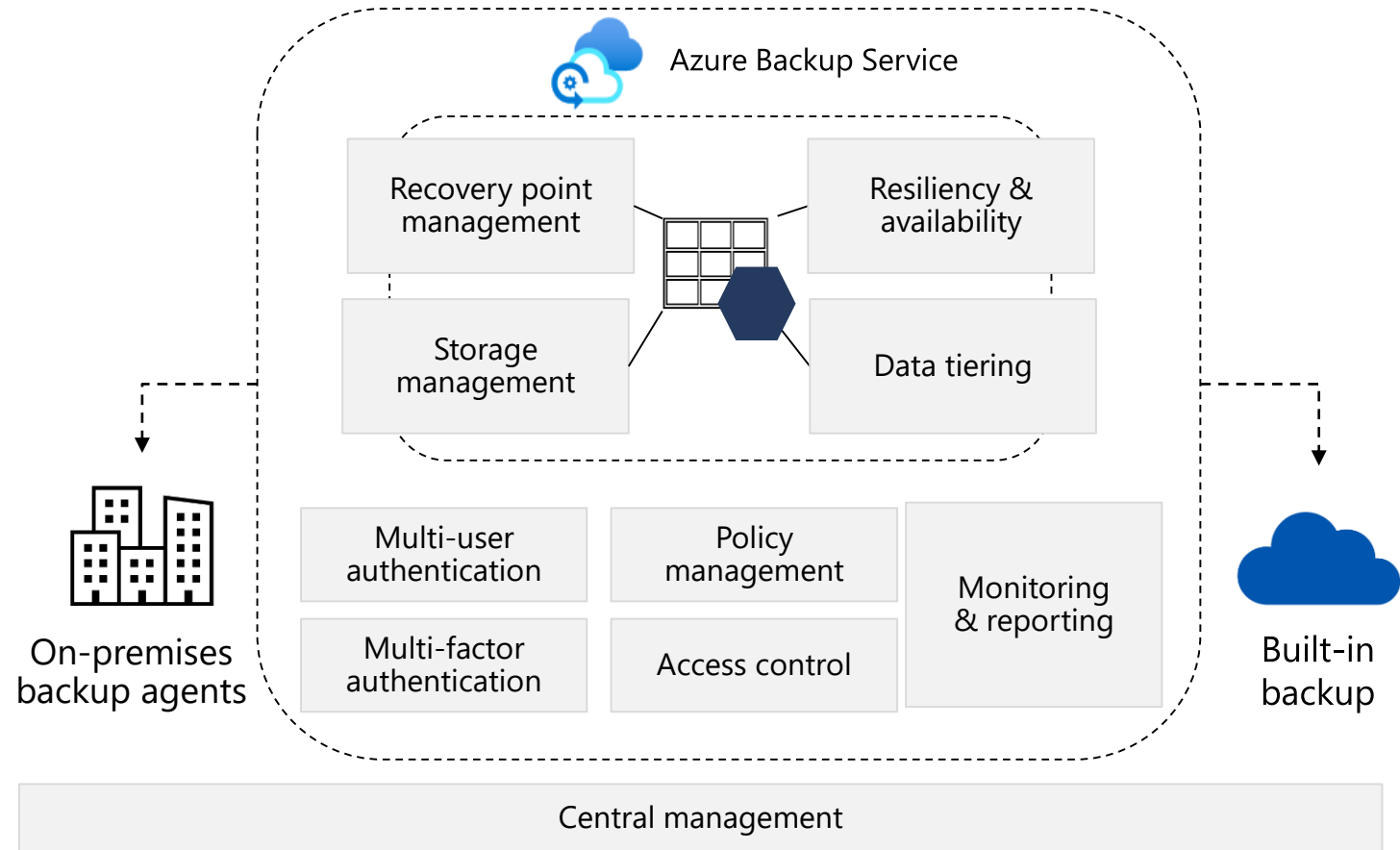
If the MTTR of any critical component in a highly available scenario exceeds the system RTO, then a failure in the system might cause an unacceptable business disruption. In other words, you can't restore the system within the defined RTO.

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



The types of backup you can perform with Azure Backup.

Backup type	Description
On-premises	Back up files, folders, and system state with the Microsoft Azure Recovery Services (MARS) agent. You can also use System Center Data Protection Manager (DPM) or the Microsoft Azure Backup Server (MABS) agent to protect on-premises virtual machines (both Hyper-V and VMware) and other on-premises workloads.
Azure Virtual Machines	Back up entire Windows or Linux virtual machines (by using backup extensions), or back up files, folders, and system state with the MARS agent.
Azure Files	Back up Azure file shares to a storage account.
SQL Server in Azure virtual machines	Back up SQL Server databases running on Azure virtual machines.
SAP HANA databases in Azure virtual machines	Back up SAP HANA databases running on Azure virtual machines.
Microsoft cloud	Azure Backup can replace your existing on-premises or off-site backup solution with a cloud-based solution that's reliable, secure, and cost-competitive.



Azure Backup storage vaults

Azure Backup organizes your backup data in a storage entity called a *vault*. A storage vault stores backup copies, recovery points, and backup policies. There are two types of vaults: Azure Backup and Azure Recovery Services. The primary differences are the types of supported data sources and Azure products.

- **Azure Backup vault:** Azure Backup vaults are used with Azure Backup only. Supported data sources include Azure Database for PostgreSQL servers, Azure blobs, and Azure disks.
- **Azure Recovery Services vault:** Azure Recovery Services vaults can be used with Azure Backup or Azure Site Recovery. Supported data sources include Azure virtual machines, SQL or SAP HANA in an Azure virtual machine, and Azure file shares. You can back up data to a Recovery Services vault from Azure Backup Server, Azure Backup Agent, and System Center Data Protection Manager.



Things to consider when using storage vaults

In your planning for Azure Backup and vault storage, consider the following points. Think about how you can use Azure Backup and storage vaults to support the Tailwind Traders BCDR requirements.

- **Consider vault organization.** Think about how you want to organize your storage vaults. If all your workloads are managed from a single subscription and single resource, you can use a single vault. If your workloads are spread across subscriptions, you can create multiple vaults. Use separate vaults for Azure Backup and Azure Site Recovery.
- **Consider Azure Policy.** For consistent policy settings across all your vaults, use Azure Policy to propagate your backup policy across multiple vaults. A backup policy is scoped to a vault.
- **Consider role-based protection.** Protect your vaults by using Azure role-based access control (RBAC). You can secure your vaults and manage access with role-based access.
- **Consider redundancy.** Specify how data in your vault is replicated for redundancy.
 - Use locally redundant storage (LRS) to protect against failure in a datacenter. LRS replicates data to a storage scale unit.
 - Use geo-redundant storage (GRS) to protect against region-wide outages. GRS replicates your data to a secondary region.

Design for blob backup and
recovery

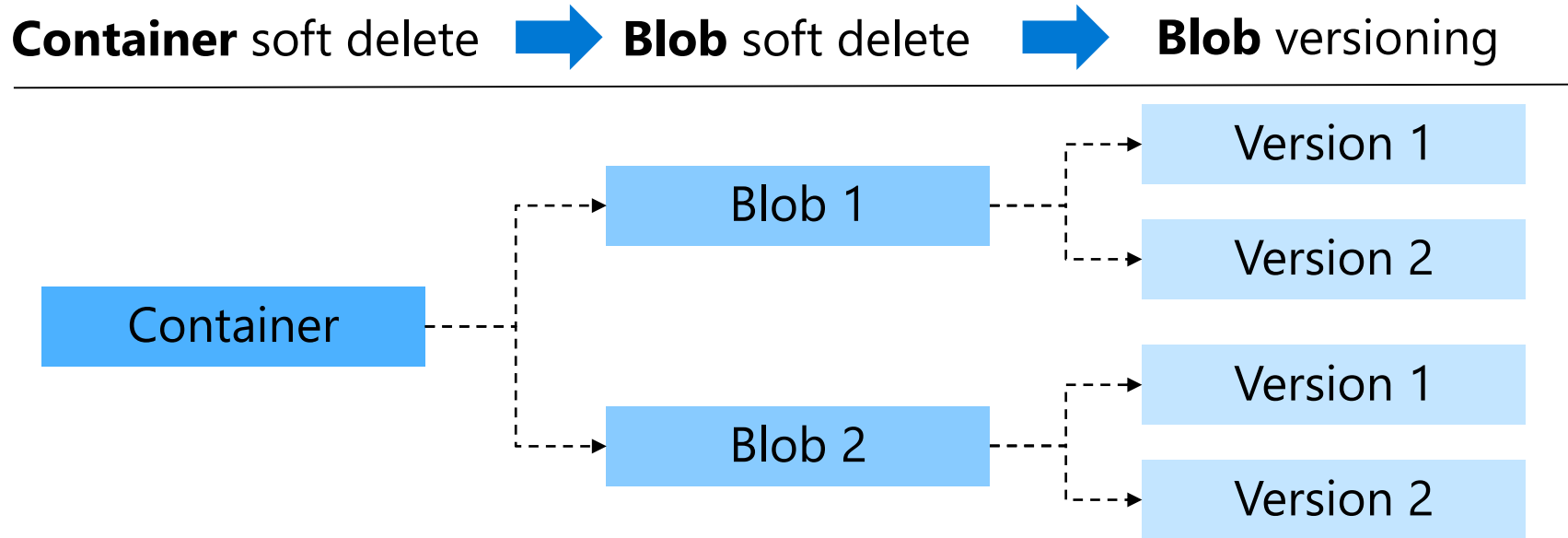
Things to know about Azure Blob Storage backup and recovery

Here are some of the prominent features available for backup and recovery of Azure Blob Storages.

- Operational backup for Azure blobs provides you with a *continuous backup* solution. You don't need to schedule any backups.
- All changes in an operational blob backup are retained for a specified period of time, and restorable from a selected point in time.
- The [soft delete feature](#) lets you protect your data from accidental deletion or corruption. During the retention period, you can restore a soft-deleted blob object to its state at the time it was deleted. Soft delete is available for blobs and containers.
- The retention period for deleted blobs or containers can be specified between 1 and 365 days. The default period is seven days.
- The operational backup solution supports [blob versioning](#). You can restore an earlier version of a blob, or recover your data after incorrect modification or deletion.
- The [point-in-time restore feature for block blobs](#) lets you protect against accidental deletion or corruption. During the retention period, you can restore block blobs from the present state to a state at a previous time.
- The [resource lock](#) feature prevents resources from being accidentally deleted or changed. You can set the resource lock to prohibit deletion or allow reading only.

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

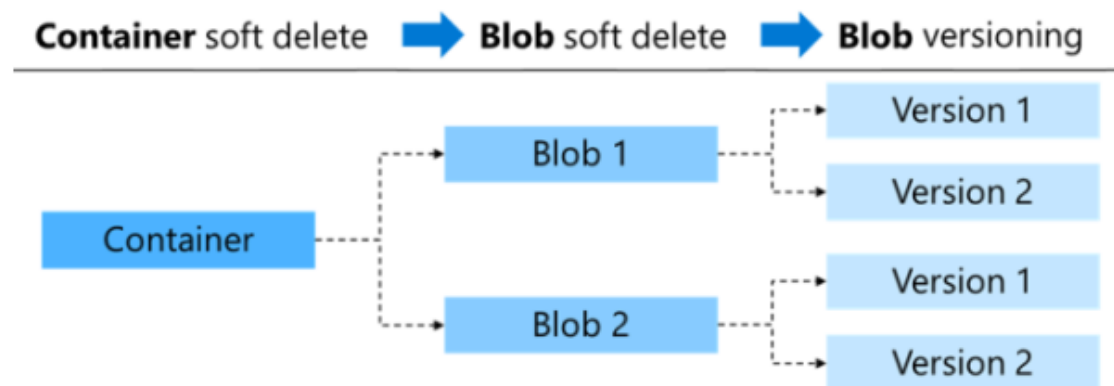
Azure Backup provides [operational backup for Azure blobs](#), which is a local backup solution for Azure Blob Storage. In this backup method, your backup data is stored in your source Azure storage account rather than being transferred to an Azure Backup storage vault.



Things to consider when using soft delete and versioning

You can implement the soft delete feature to protect an individual blob, snapshot, container, or blob version from accidental deletes or overwrites. Soft delete maintains the deleted data in the system for your specified retention period. During the retention period, you can restore a soft-deleted object to its state at the time it was deleted.

The following diagram shows a high-level view of the soft delete feature for containers and blobs, and blob versions.



There are different options for implementing soft delete and blob versioning:

- Implement [blob soft delete](#) to restore a specific deleted file, such as a blob, snapshot, or blob version.
- Use [container soft delete](#) to restore a container and its contents.

📌 Note

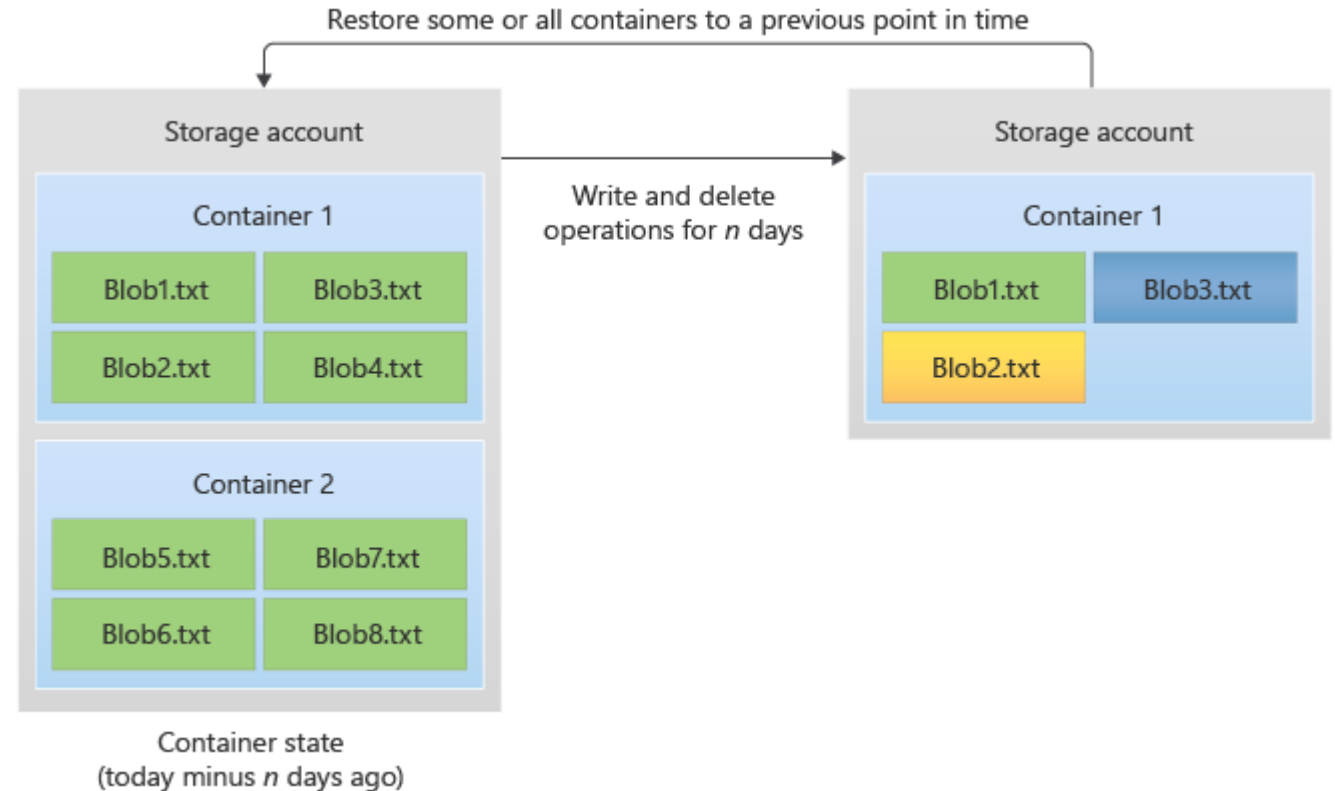
Container soft delete doesn't protect against the deletion of a storage account, but only against the deletion of containers in a storage account.

- Add [blob versioning](#) to automatically maintain previous versions of a blob. You can restore an earlier version of a blob, or use the feature to recover your data. Blob versioning is useful when you have multiple authors editing the same files. Implement blob versioning to maintain or restore individual changes from each author.

Considerations for point-in-time restore

Consider point-in-time restore for block blobs

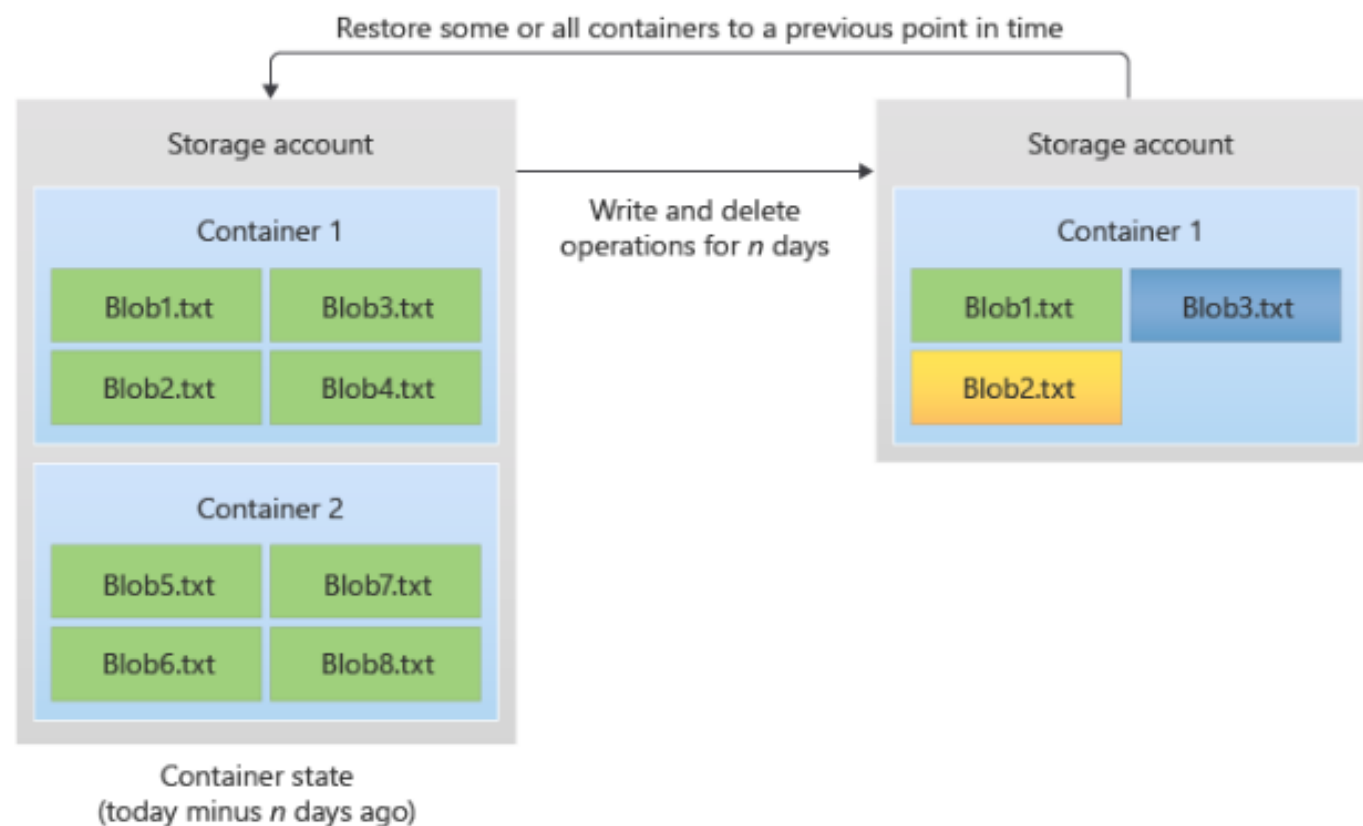
- Useful in scenarios where a user or application accidentally deletes data or where an application error corrupts data
- Use policy to specify the retention period



Things to consider when using point-in-time restore

Like soft delete, [point-in-time restore for block blobs](#) also protects against accidental deletion or corruption. Create a management policy for the source storage account and specify your retention period. During the retention period, you can restore block blobs from the present state to a state at a previous time. Point-in-time restore lets you test scenarios that require reverting a data set to a known state before you run further tests.

The following diagram shows how point-in-time restore works. One or more containers or blob ranges is restored to its previous state. The result of the process is to revert write and delete operations that occurred during the retention period.



Things to consider when using resource locks

You can protect your data and avoid accidental changes by using [resource locks](#). This feature prevents resources from being accidentally deleted or changed. There are two lock levels: `CanNotDelete` and `ReadOnly`.

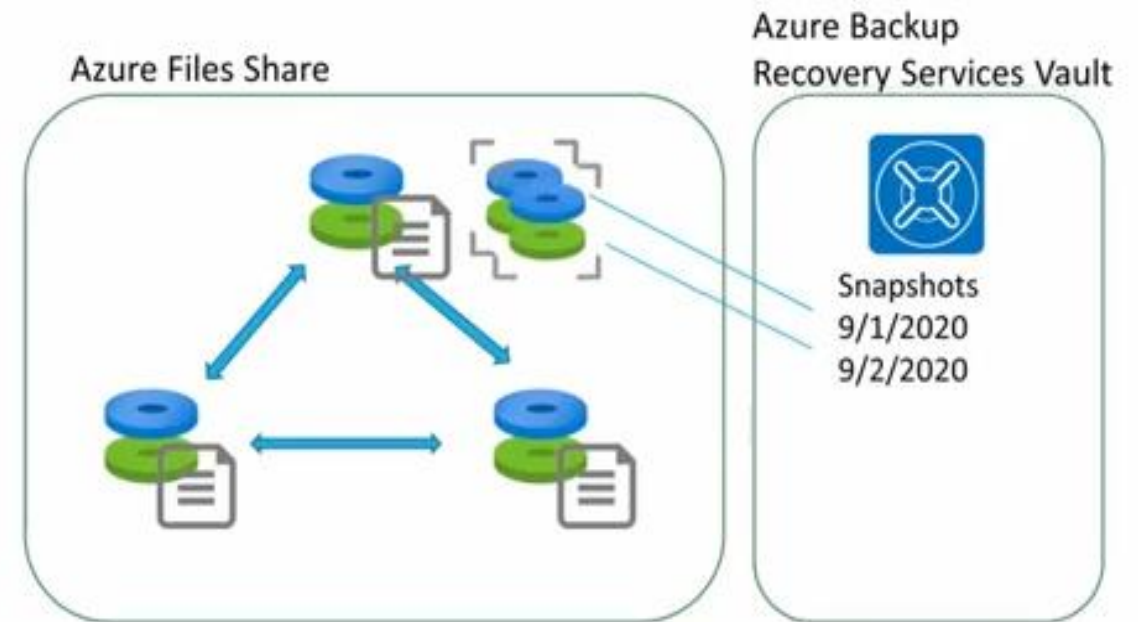
- `CanNotDelete` permits authorized users to read and modify a resource, but they can't delete the resource without first removing the lock.
- `ReadOnly` allows authorized users to read a resource, but they can't delete or change the resource. Applying this lock is like restricting all authorized users to the permissions granted by the *Reader* role in Azure RBAC.

Design for Azure Files backup and recovery

Considerations for Azure Files backup and recovery

Consider snapshots for both blobs and Azure Files

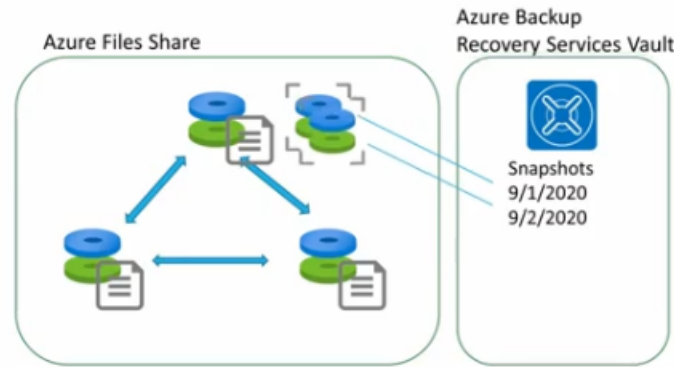
- Organize file shares with backup in mind
- Snapshots can be on-demand or scheduled using Azure Backup and backup policies.
- Snapshots are at the file share root – retrieval is at the file
- Use snapshots to cover the time between daily backups
- Use instant restore – consider self service restore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



Design for Azure files backup and recovery

3 minutes

Azure Files provides the capability to take [share snapshots of file shares](#). Share snapshots give you an extra level of security, and help reduce the risk of data corruption or accidental deletion. You can also use share snapshots as a general backup for disaster recovery.



Things to know about Azure File share backup and recovery

Let's review some of the characteristics regarding backup and recovery of Azure file shares.

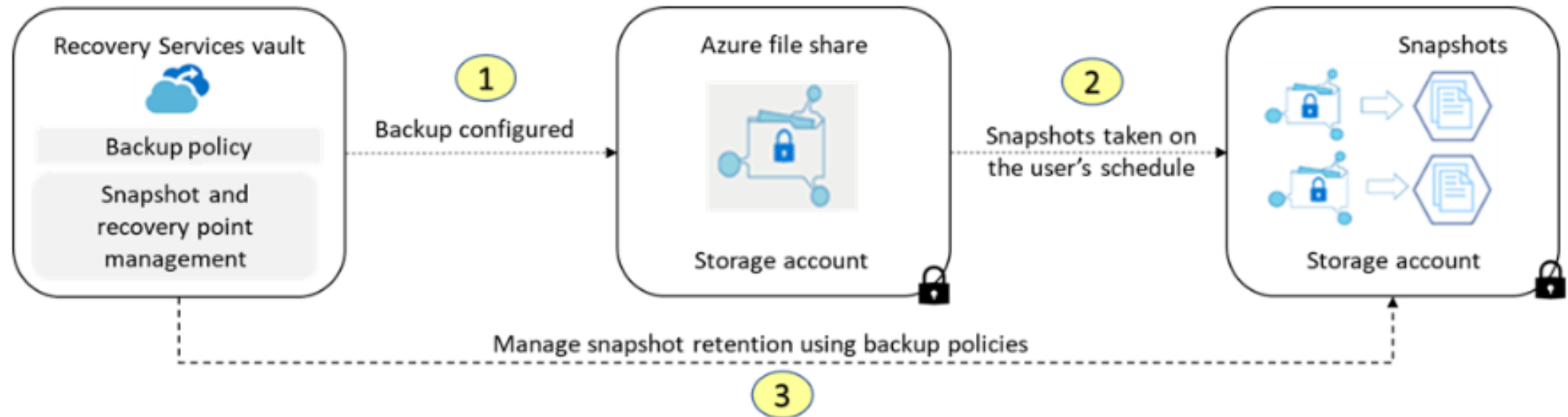
- Share snapshots capture the share state at that specific point in time.
- Snapshots can be created manually by using the Azure portal, REST API, client libraries, the Azure CLI, and PowerShell.
- Snapshots can be automated by using Azure Backup and backup policies.
- Snapshots are at the root level of a file share and apply to all the folders and files contained in the share. Retrieval is provided at the individual file level.
- Snapshots are incremental. Only the deltas between your snapshots are stored.
- After a share snapshot is created, it can be read, copied, or deleted, but it can't be modified.
- You can't delete a share that has share snapshots. To delete the share, you must delete all the share snapshots.

Important
Snapshots aren't a replacement for cloud-side backups.



Automated file share backups

You can automate and manage your Azure file shares snapshots. Automating snapshot backups with Azure Backup is the recommended approach. The following diagram shows how automatic backups of file shares can be restored from a Recovery Services vault.



- Azure Backup keeps the metadata about the snapshot backup in the Recovery Services vault, but no data is transferred. This method provides you with a fast backup solution that has built-in backup and reporting.
- When Azure Backup is enabled on the file share, the soft delete feature is also enabled.
- You can configure snapshot backups for daily, weekly, monthly or yearly retention, according to your requirements.



Things to consider when using file share backups

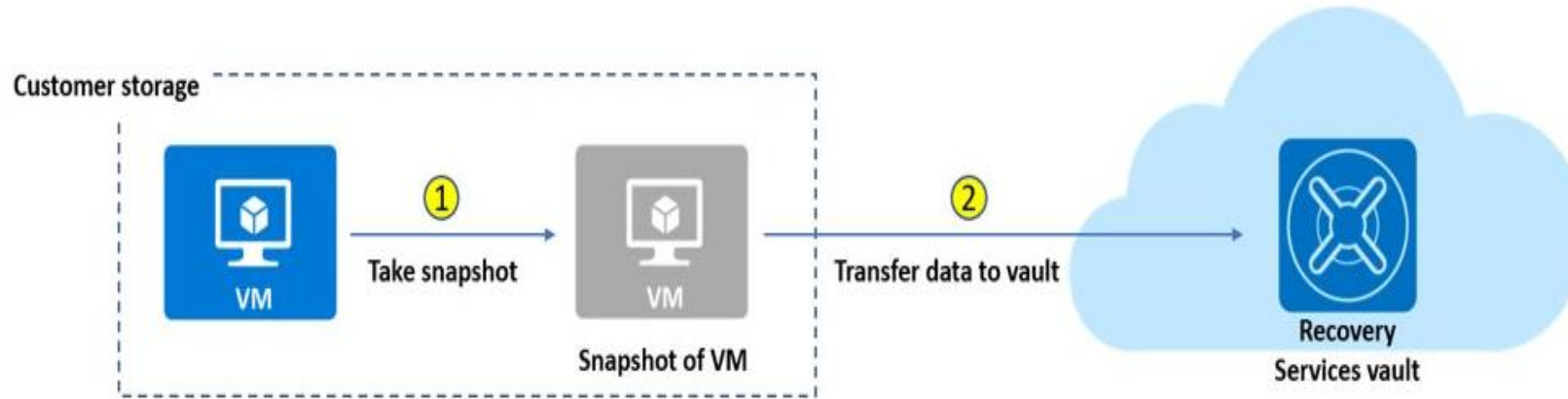
Take a moment to review some considerations for creating and recovering from file share backups. Think about how you can use this approach to support the Tailwind Traders BCDR requirements.

- **Consider instant restore.** Azure file share backup uses file share snapshots. You can select just the files you want to restore instantly.
- **Consider alerts and reporting.** You can configure alerts for backup and restore failures and use the reporting solution provided by Azure Backup. These reports provide insights on file share backups.
- **Consider self-service restore.** Azure Backup uses server endpoint Windows Volume Shadow Copy Service (VSS) snapshots. You might consider giving advanced users the ability to restore files themselves.
- **Consider on-demand backups.** Azure Backup policies are limited to scheduling a backup once a day. If a user creates a file in the morning and works on it all day, a nightly backup doesn't include the new file. For these reasons, consider on-demand backups for the most critical file shares.
- **Consider file share organization.** Organize your file shares according to how you intend to store the data in backups. You might separate your file shares for backup according to public facing data versus internal file shares.
- **Consider code deployments.** If a bug or application error is introduced with the new deployment, you can go back to a previous version of your data on that file share. To help protect against these scenarios, you can take a share snapshot before you deploy new application code.

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



Things to consider when using virtual machine backup and recovery

Here are some things to review when planning backup and recovery for your virtual machines. Consider how you can use Azure virtual machine backups in the Tailwind Traders BCDR solution.

- **Consider your backup schedule.** Identify the best backup schedule for your business needs. To distribute backup traffic, consider backing up different virtual machines at different times of the day, and make sure the backup times don't overlap. Ensure your backup scheduled start time is during non-peak production application times.
- **Consider backup frequency.** Determine how frequently you need to create fresh backups. Implement both short-term (daily) and long-term (weekly) backups. If you need to take a backup outside of your scheduled via backup policy, you can use an on-demand backup. You might do on-demand backups multiple times per day when scheduled backup permits only one backup per day.
- **Consider backup policies.** Create a single backup policy for a group of virtual machines that require the same schedule start time, frequency, and retention settings. You might establish a backup policy for critical virtual machines, and a separate policy for non-critical machines.
- **Consider plan changes.** After you implement your backup solution, continue to monitor and review your plan. As your business requirements change, make sure to review and change your backup policies. Enable monitoring and alerting features and review the results.



- **Consider practice restore runs.** Restoring backups for virtual machines can be time-consuming. It's a recommended practice to try restoring from your backups before you experience a critical scenario where recovery is essential.

The total restore time depends on the Input/Output operations per second (IOPS) and the throughput of the storage account. The total restore time can be affected if the target storage account is loaded with other application read and write operations. To improve restore operation, select a storage account that isn't loaded with other application data.

- **Consider throttling during restore.** If you're restoring virtual machines from a single Recovery Services vault, we highly recommend that you use different general-purpose v2 storage accounts. By using a v2 storage account, you can ensure your target storage account doesn't get throttled. Consider a scenario where each virtual machine must have a different storage account. If 10 virtual machines are being restored, plan to use 10 different storage accounts.
- **Consider Cross Region Restore (CRR).** CRR allows you to restore Azure virtual machines in a secondary region, which is an Azure paired region. This option lets you conduct drills to meet audit or compliance requirements. You can also restore the virtual machine or its disk if there's a disaster in the primary region. CRR is an opt-in feature for any Recovery Services vault. CRR also works for SQL databases and SAP HANA databases hosted on Azure virtual machines.

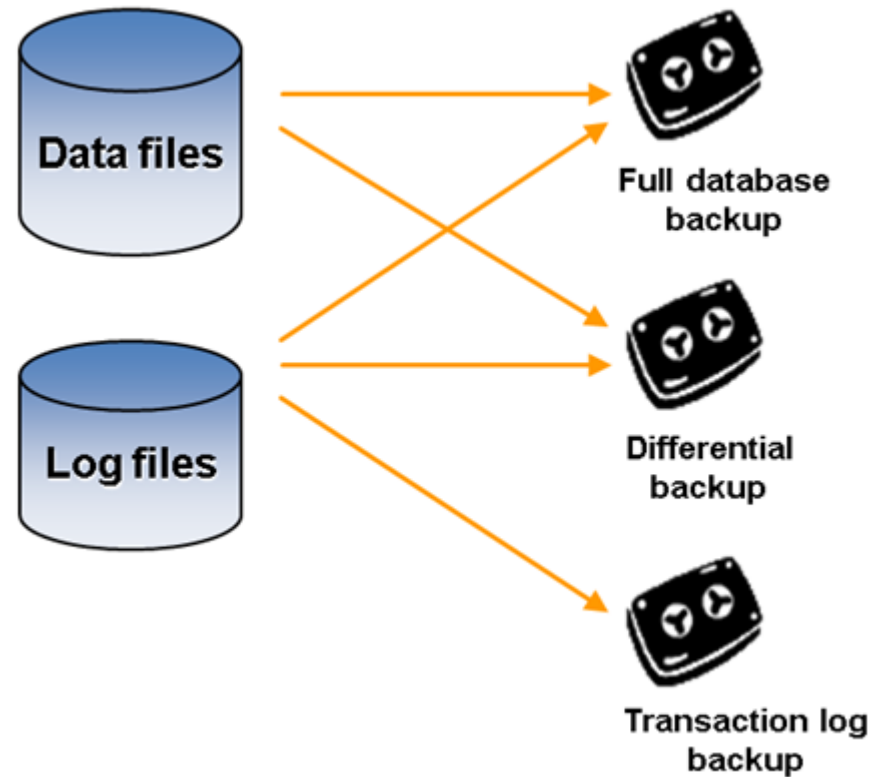
Design for Azure SQL backup and recovery

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



Design for Azure SQL backup and recovery

3 minutes

It's essential that you can recover your SQL database data. You should consider automated backups of your Azure SQL Database and Azure SQL Managed Instances. Database backups enable database restoration to a specified point in time and within a configured retention period.

Describe automated backups

Both SQL Database and SQL Managed Instance use SQL Server technology to create [full backups](#) every week, [differential backups](#) every 12-24 hours, and [transaction log backups](#) every 5 to 10 minutes. The frequency of transaction log backups is based on the compute size and the amount of database activity. When you restore a database, the service determines which full, differential, and transaction log backups need to be restored.

- **Full backups:** In a full backup, everything in the database and the transaction logs is backed up. SQL Database makes a full backup once a week.
- **Differential backups:** In a differential backup, everything that changed since the last full backup is backed up. SQL Database makes a differential backup every 12 - 24 hours.
- **Transactional backups:** In a transactional backup, the contents of the transaction logs are backed up. If the latest transaction log has failed or is corrupted, the option is to fall back to the previous transaction log backup. Transactional backups enable administrators to restore up to a specific time, which includes the moment before data was mistakenly deleted. Transaction log backups every five to 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



Describe backup usage cases

You can use the automated backups in several ways.

- [Restore an existing database to a point in time in the past](#) within the retention period. This operation creates a new database on the same server as the original database but uses a different name to avoid overwriting the original database. After the restore completes, you can delete the original database.
- [Restore a deleted database to the time of deletion](#) or to any point in time within the retention period. The deleted database can be restored only on the same server or managed instance where the original database was created.
- [Restore a database to another geographic region](#). Geo-restore allows you to recover from a geographic disaster when you cannot access your database or backups in the primary region. It creates a new database on any existing server or managed instance, in any Azure region.
- [Restore a database from a specific long-term backup](#) of a single database or pooled database. If the database has been configured with a long-term retention policy you can restore an old version of the database.

Long-term backup retention policies

Azure SQL Database automatic backups remain available to restore for up to 35 days. This period is enough for the purposes of day-to-day administration. But sometimes you might need to retain data for longer periods. For example, data protection regulations in your local jurisdiction might require you to keep backups for several years.

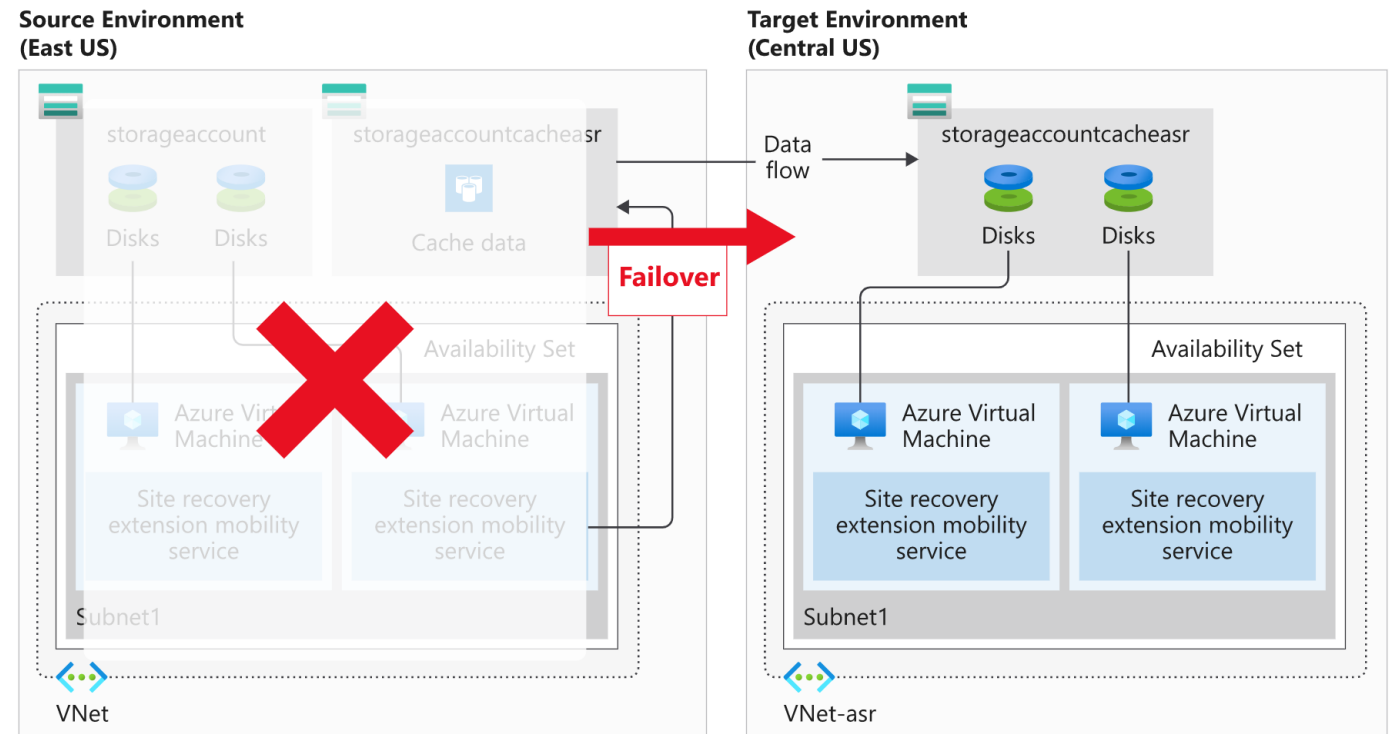
For these requirements, use the long-term retention (LTR) feature. This way, you can store Azure SQL Database backups in read-access geo-redundant storage (RA-GRS) blobs for up to 10 years. If you need access to any backup in LTR, you can restore it as a new database by using either the Azure portal or PowerShell.

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




Let's review some of the many capabilities of Azure Site Recovery.

Things to consider when using Site Recovery

Azure Site Recovery provides a simple BCDR solution with management support from the Azure portal. Set up and manage replication, fail over, and failback for your virtual machines from a single location.

Let's review some of the many capabilities of Azure Site Recovery.

 Expand table

Feature	Description
Replicate Azure virtual machines	Set up disaster recovery of your Azure virtual machines, and fail over from a primary region to a secondary region.
Replicate on-premises virtual machines	Replicate your on-premises virtual machines and physical servers to Azure, or to a secondary on-premises datacenter.
Replicate workloads	Replicate any workload running on supported Azure virtual machines, on-premises Hyper-V and VMware virtual machines, and Windows or Linux physical servers.
Automate BCDR tasks	Automate your BCDR tasks and further reduce your recovery time objective. You can use Azure Site Recovery to set up automatic periodic test failovers, and monitor the overall effectiveness of the recovery process.
Maintain data resilience	Orchestrate replication without intercepting app data by using Azure Site Recovery. When failover occurs, Azure virtual machines are created based on the replicated data. When you replicate to Azure, data is stored in Azure Storage, and you gain the resilience provided by that service.
Meet RTO and RPO targets	Keep the RTO and RPO goals within the defined organizational limits. Azure Site Recovery provides continuous replication for Azure virtual machines and VMware virtual machines, and replication frequency as low as 30 seconds for Hyper-V.



Feature	Description
Maintain consistent apps after failover	By using app-consistent snapshots, you can replicate from specific recovery points. These snapshots capture disk data, data in memory, and all in process transactions.
Test without disruption	Run disaster recovery tests without affecting ongoing replication.
Run flexible failovers	Execute planned failovers for expected outages with no data loss. Run unplanned failovers with minimal data loss, and fail back to your primary site when it's available again.
Customize recovery plans	Create recovery plans so you can customize and sequence the failover and recovery of your multi-tier apps running on multiple virtual machines. Group virtual machines together in a recovery plan, and add scripts and manual actions as needed. Integrate recovery plans with Azure Automation runbooks.
Integrate with BCDR technologies	Integrate Azure Site Recovery with other BCDR technologies. Use Site Recovery to protect the SQL Server backend of your corporate workloads. Because of its native support for SQL Server AlwaysOn, you can manage the failover of availability groups.
Access Azure Automation integration	Download from the Azure Automation library and integrate app-specific scripts with Azure Site Recovery.

Combine Azure Site Recovery with Azure Backup

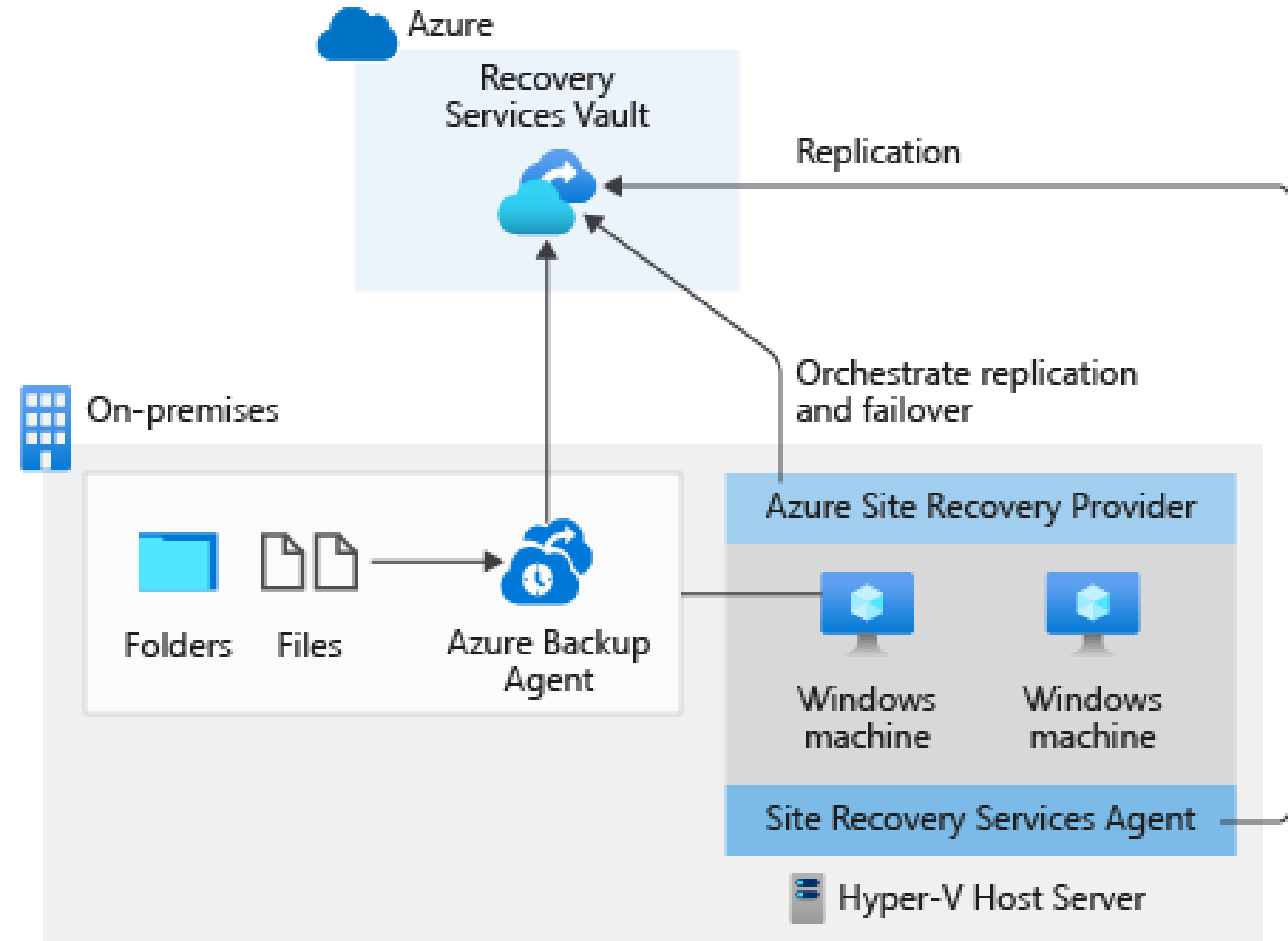
Combine ASR with Azure Backup

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

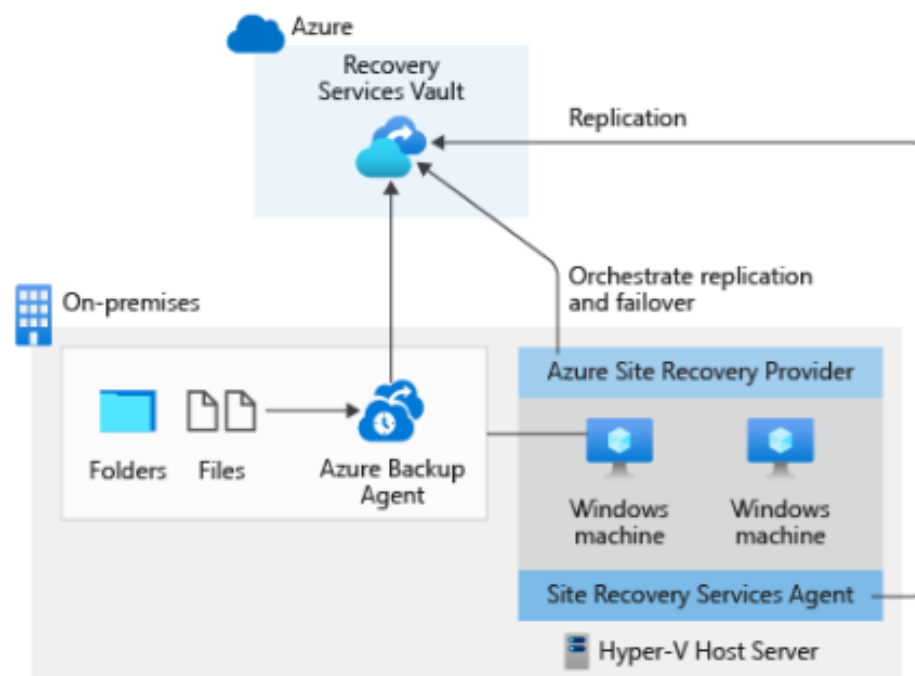
- Azure Backup periodically backs up the files and folders on the Windows machine to Azure.
- This process ensures they are secure and retrievable even if the whole on-premises environment stops functioning.



Use Azure Site Recovery with Azure Backup

Let's examine how you can implement Azure Site Recovery with Azure Backup for a BCDR solution.

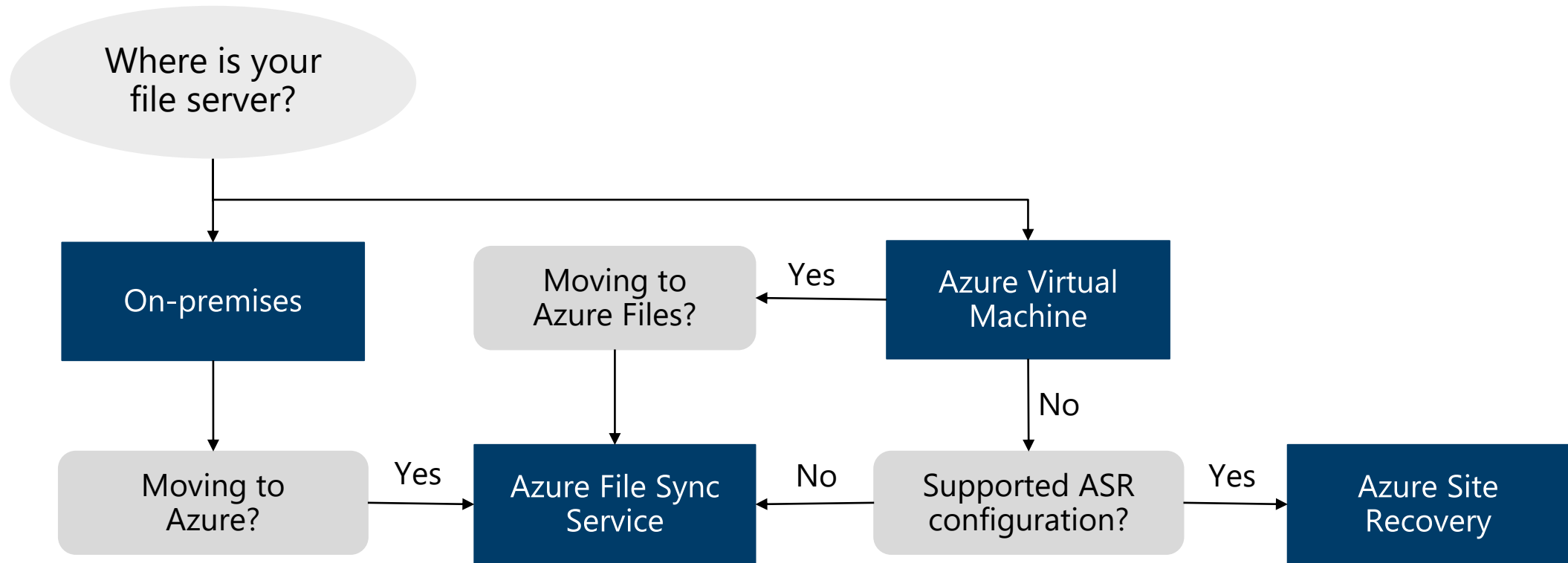
Suppose you have an on-premises environment with a Hyper-V host server for hosting virtual machines. You want to back up all the files and folders in your virtual machine to Azure. You also want to protect any workloads running on your virtual machine and keep them running if the virtual machine fails. Azure Backup and Site Recovery can be used together in a single solution.



In this scenario, Azure Backup periodically backs up the files and folders on your Windows machine to Azure. This process ensures they data is secure and retrievable even if the whole on-premises environment stops functioning. Separately, Azure Site Recovery is used to protect your running workloads and keep them running. Because Site Recovery can replicate frequently, the RTO for your workloads can be reduced.

Review

Review file server backup and recovery options



Recommend a disaster recovery method (activity)

