Cloud Computing

Caltech | Center for Technology & Management Education

Designing Infrastructure Solutions on Azure

Powerd by simplilearn

Design a Solution for Backup and Recovery

Learning Objectives

By the end of this lesson, you will be able to:

- Classify the architectural best practices for reliability into categories
- Recommend a solution for recovery in different regions
- Recommend a solution for Azure backup management
- Design a solution for data archiving and retention

A Day in the Life of an Azure Architect

You are working as a Cloud Architect in an automobile company. The company needs a business continuity solution for the deployment of an order processing system to Azure.

The order processing system would use Azure Linux and Windows Server VMs.

The system uses multiple Azure subscriptions and has a wide portfolio of products deployed across subscriptions. You need to design a solution keeping these requirements in mind:

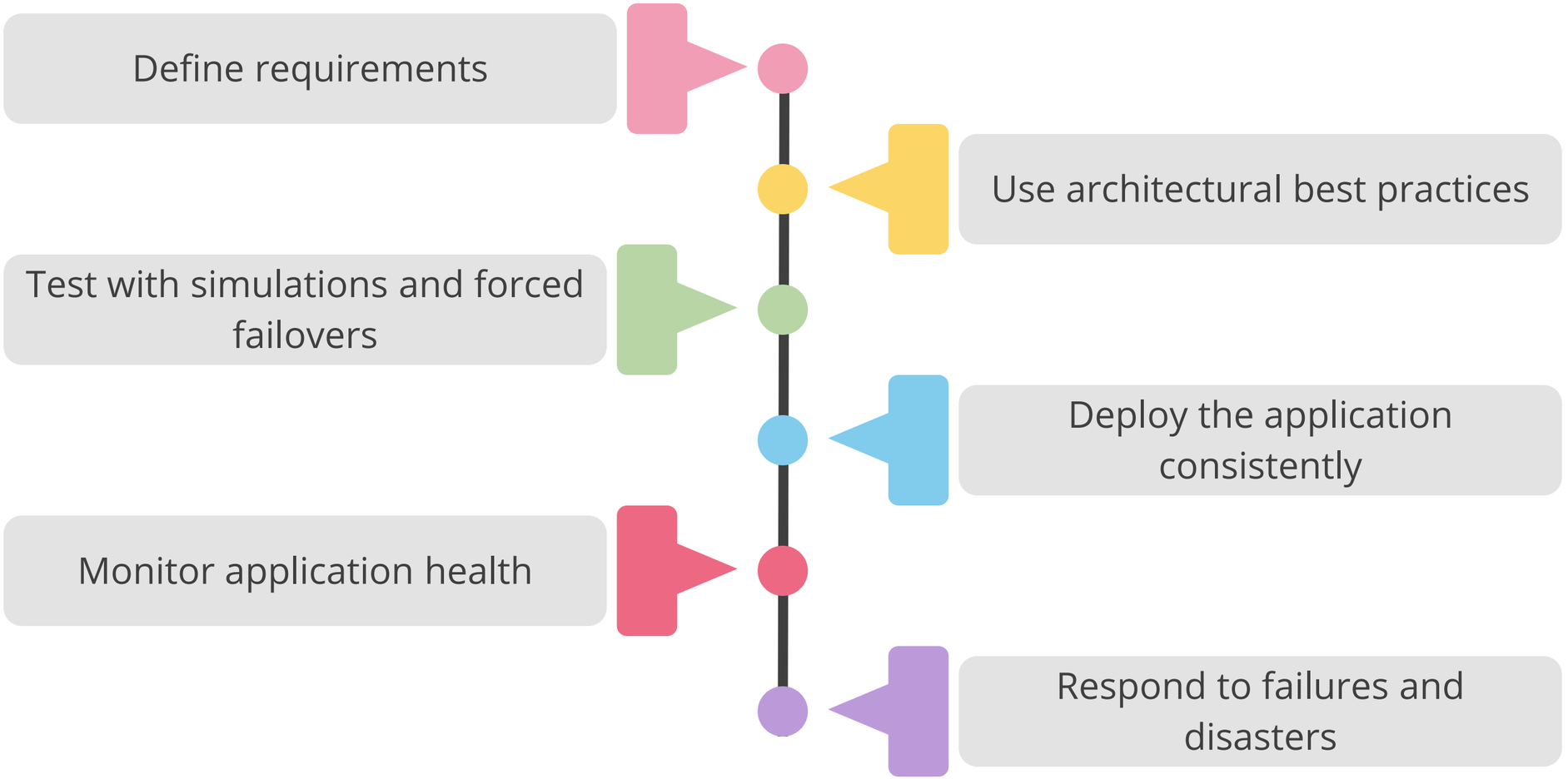
- There should be no business interruption if an Azure region fails.
- You need to keep the cost minimized.
- Your data should be safe and recoverable with this solution.

To achieve all of the above, along with some additional features, we would be learning a few concepts in this lesson that will help you find a solution for the above scenario.

Recommend a Recovery Solution for Azure Workloads

Architectural Best Practices for Reliability

The architectural best practices for reliability are:



Define Requirements

Define requirements using the criteria given:

1. Identify workloads and usage
2. Plan for usage patterns
3. Establish availability metrics (MTTR/MTBF)
4. Establish recovery metrics (RTO/RPO)
5. Determine workload availability targets
6. Understand service-level agreements

Recovery Time Objective

Recovery time objective (RTO) is the maximum acceptable time for which an application can be unavailable after an incident.

- If RTO is 90 minutes, the application must be restored to a running state within 90 minutes from the start of a disaster.
- If an application has a very low RTO, consider a second deployment running in standby mode.

Recovery Point Objective

Recovery point objective (RPO) is the maximum duration of data loss that is acceptable during a disaster.

Example:

Data stored in a single database with no replication to other databases and hourly backups could result in the loss of an hour's worth of data.

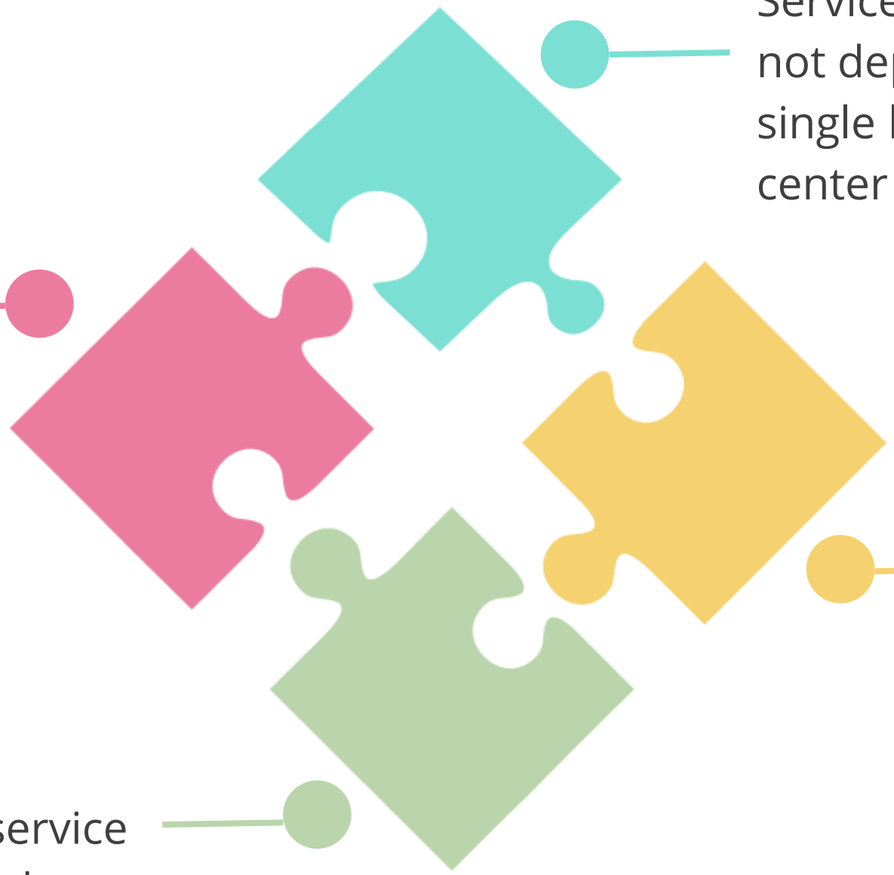
Use Architectural Best Practices

The following is a list of architectural best practices:

- Perform a failure mode analysis (FMA)
- Create a redundancy plan
- Design for scalability
- Plan for subscription and service requirements
- Use load-balancing to distribute requests
- Build availability requirements into the design
- Manage the data

Azure Service Dependencies

The following Azure services are dependent on one another:



Services that are not dependent on a single logical data center

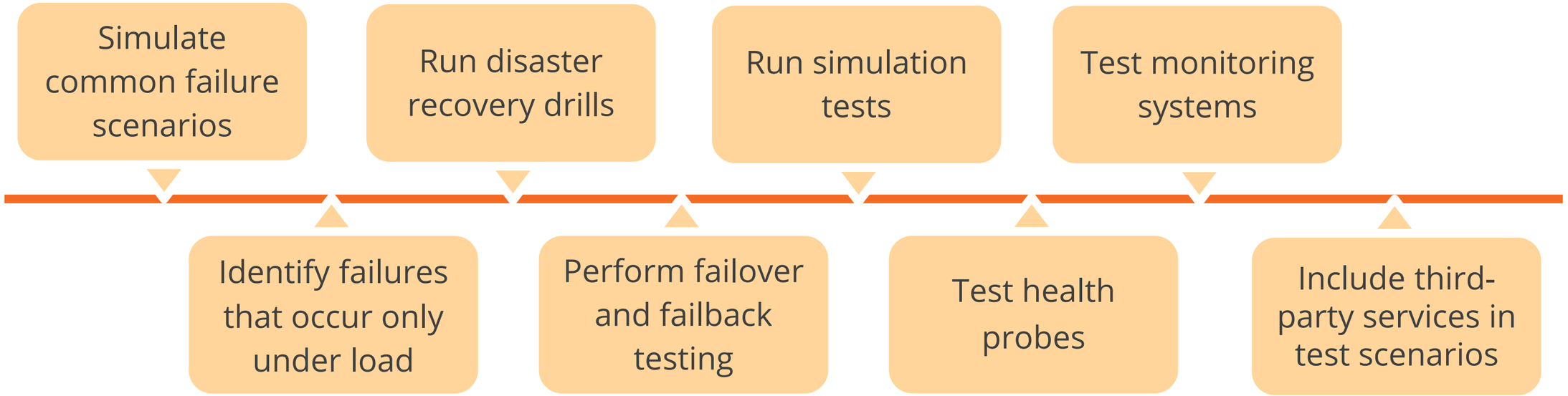
Customer-specific regions

Non-regional services deployed to two or more regions

Azure service dependency documentation

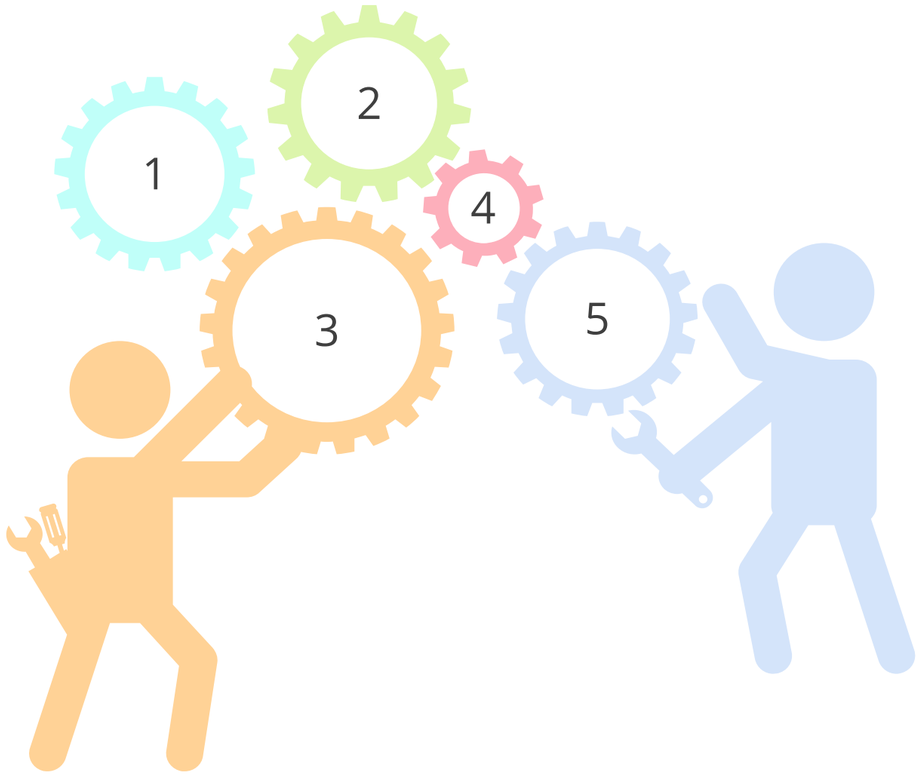
Test with Simulations and Forced Failovers

The steps involved in simulating a common failure scenario are as follows:



Deploy Applications Consistently

The stages in deploying a consistent application are as follows:



- Automate your application deployment process
- Design your release process to maximize availability
- Have a rollback plan for deployment
- Log and audit deployments
- Document the application release process

Monitor Application Health

The following factors are often used to take care of the application's health:

- Measure remote call statistics and share the data with the application team
- Track transient exceptions and retries over an appropriate time frame
- Implement health probes, check functions, and monitor third-party services
- Train multiple operators to monitor the application and to perform manual recovery steps

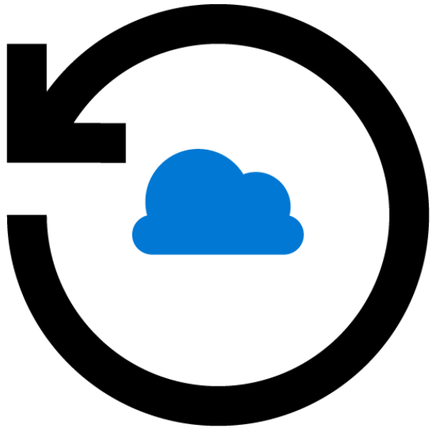
Monitor Application Health

The following factors are often used to take care of the application's health:

- Check long-running workflows
- Maintain application logs
- Set up an early warning system
- Operate within Azure subscription limits

Respond to Failures and Disasters

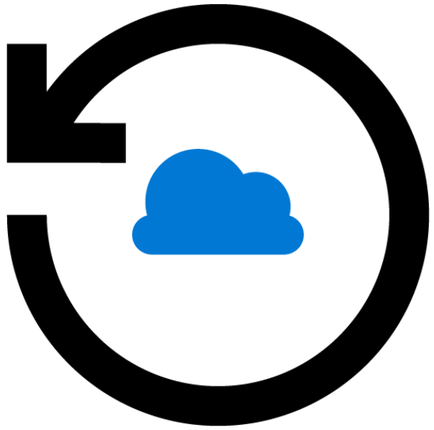
In case that the application fails, the following operations are carried out:



- Plan for Azure support interactions
- Document and test your disaster recovery plan
- Failover manually when required
- Prepare for application failure

Respond to Failures and Disasters

In the case that the application fails, the following operations are carried out:

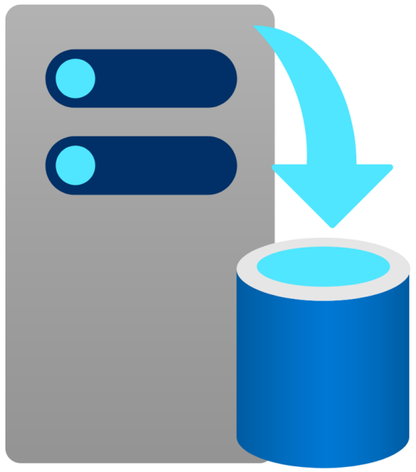


- Recover from data corruption
- Recover from a network outage
- Recover from a dependent service failure
- Recover from a region-wide service disruption

Recommend a Solution for Azure Backup Management

Microsoft Azure Backup Overview

Microsoft Azure Backup Service offers simple and reliable backup and protection for critical data in an easily recoverable way from any location.



Microsoft Azure Backup Benefits

Reliable offsite data protection

- Convenient offsite protection
- Safe data
- Encrypted backups

A simple and integrated solution

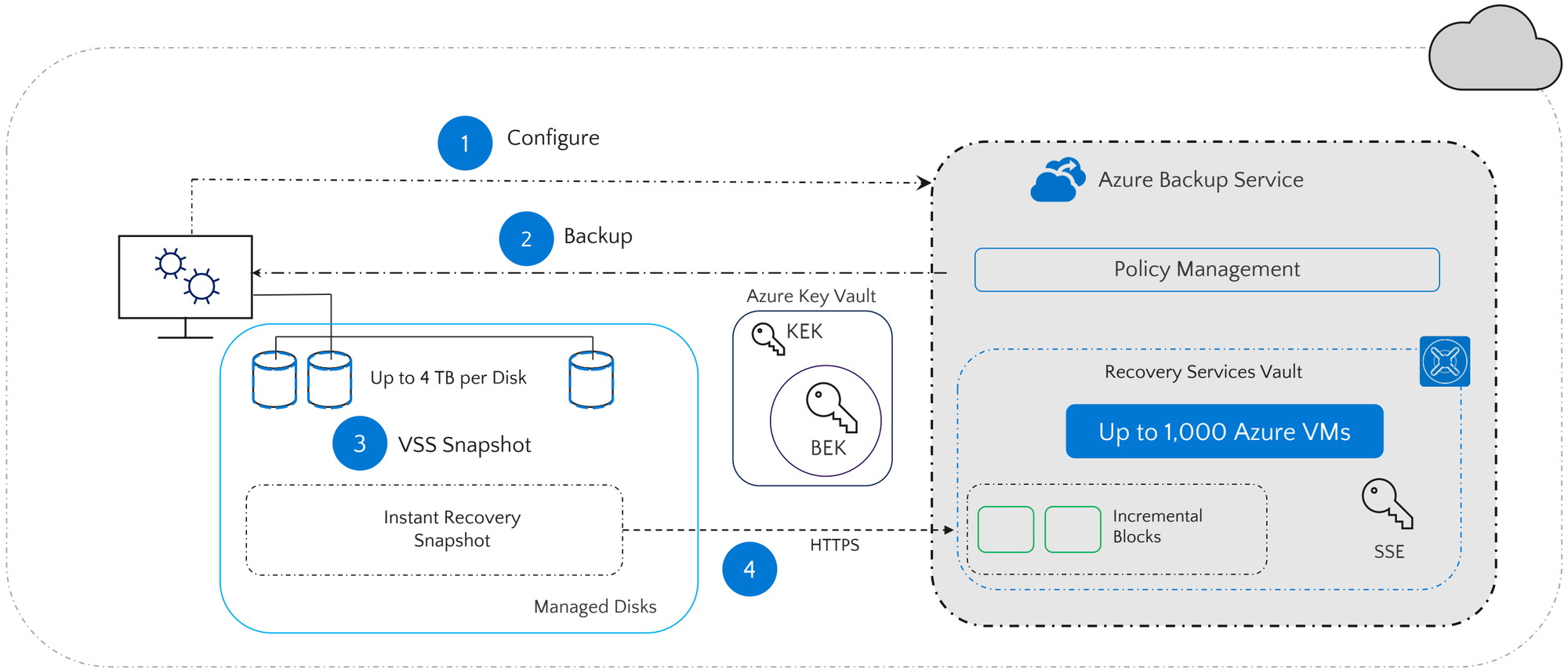
- Familiar interface
- Azure integration

Efficient backup and recovery

- Efficient use of bandwidth and storage
- Flexible configuration
- Flexible in recovery

Azure VM Backup Architecture

The following figure illustrates the architecture of Azure Backup Service:



Azure Backup Key Features

- Simple configuration and management
- Block-level incremental backups
- Data integrity verified in the cloud
- Configurable retention policies

Simple and familiar user interface to configure and monitor backups from Windows Server and System Center Data Protection Manager

Azure Backup Key Features

- Simple configuration and management
- Block-level incremental backups
- Data integrity verified in the cloud
- Configurable retention policies

Automatic incremental backup track file and block level changes, only transferring the changed blocks, hence reducing the storage and bandwidth utilization

Azure Backup Key Features

- Simple configuration and management
- Block-level incremental backups
- Data integrity verified in the cloud
- Configurable retention policies

Backed up data is also automatically checked for integrity once the backup is complete. As a result, any corruptions due to data transfer are automatically identified, and repair is attempted in the next backup.

Azure Backup Key Features

- Simple configuration and management
- Block-level incremental backups
- Data integrity verified in the cloud
- Configurable retention policies

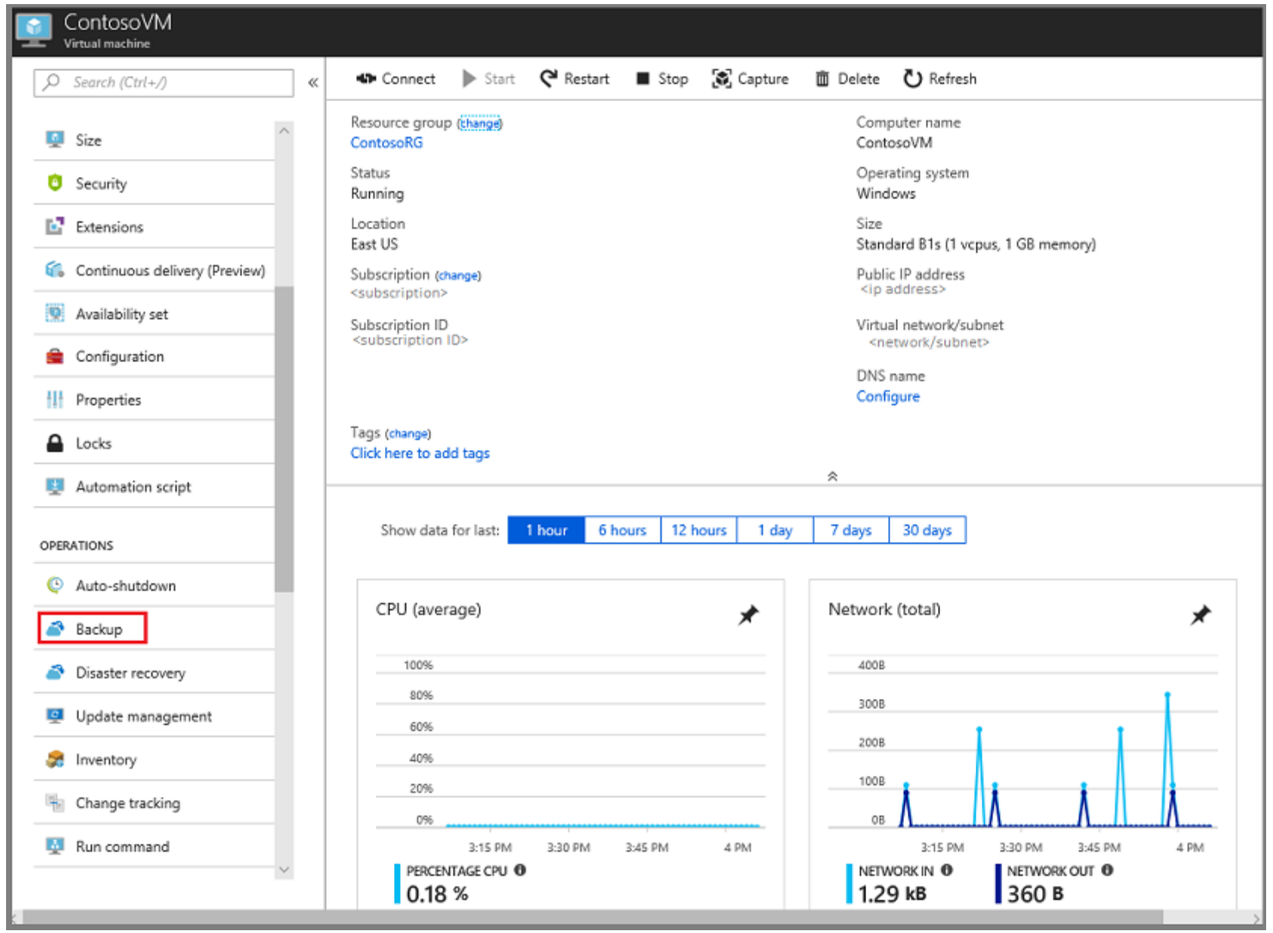
Retention policies are used to control how long a backup will be saved in Azure. This helps to meet business policies and manage backup costs.

Azure IaaS Backup Components

Component	Benefits	Limits	What is protected?	Where are backups stored?
Azure Backup Server (can be deployed in Azure and on-premises)	• App aware snapshots (VSS) • Full flexibility for when to take backups • Recovery granularity (all) • Can use Recovery Services vault • Linux support on Hyper-V and VMware VMs • Backup and restore VMware VMs • Does not require a System Center license	• Cannot backup Oracle workload • Always requires live Azure subscription • No support for tape backup	• Files • Folders • Volumes • VMs • Applications • Workloads • System State	• Recovery Services vault • Locally attached disk
Azure IaaS VM Backup	• Native backups for Windows/Linux • No specific agent installation required • Fabric-level backup with no backup infrastructure needed	• Backup VMs once-a-day • Restore VMs only at disk level • Cannot back up on-premises	• VMs • All disks (using PowerShell)	Recovery Services vault

Recovery Services Vault Overview

A Recovery Services vault is a storage entity in Azure that houses data.



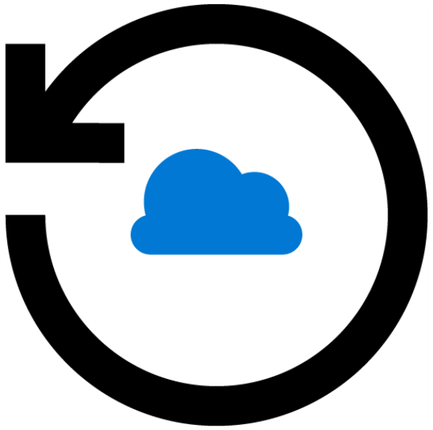
Azure Blob Backup

It is a managed, local data protection solution that will protect user block blobs from various data loss scenarios like corruptions, blob deletions, and accidental storage account deletion.

- Data is stored locally within the source storage account itself and can be recovered to a selected point in time whenever needed.
- The backup data is not transferred to the Backup vault but is stored in the source storage account itself.
- It is simple, secure, and cost-effective.

Data Protection in Blob Service

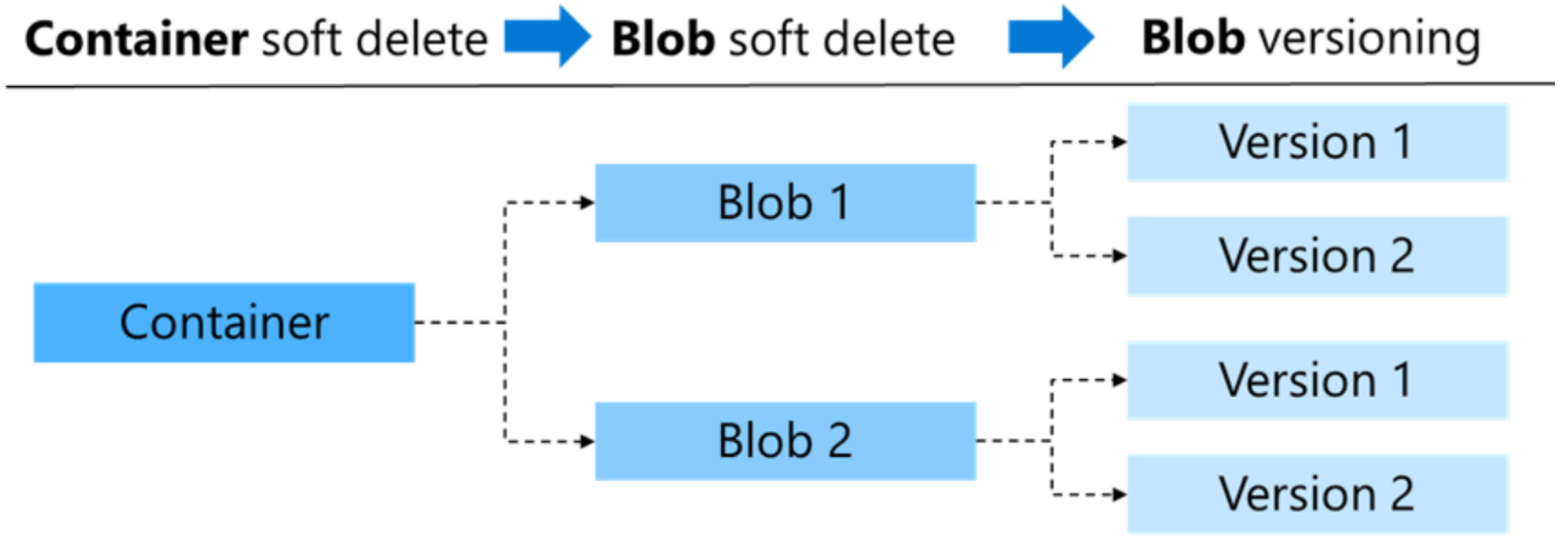
Properties in the Data protection tab of the blob service in the user storage account are:



- Point-in-time restore
- Soft delete
- Versioning for blobs and blob change feed
- Delete Lock

Design for Azure Blob Backup

Soft delete protects an individual blob, snapshot, container, or version from accidental deletes or overwrites.



Source: https://docs.microsoft.com/

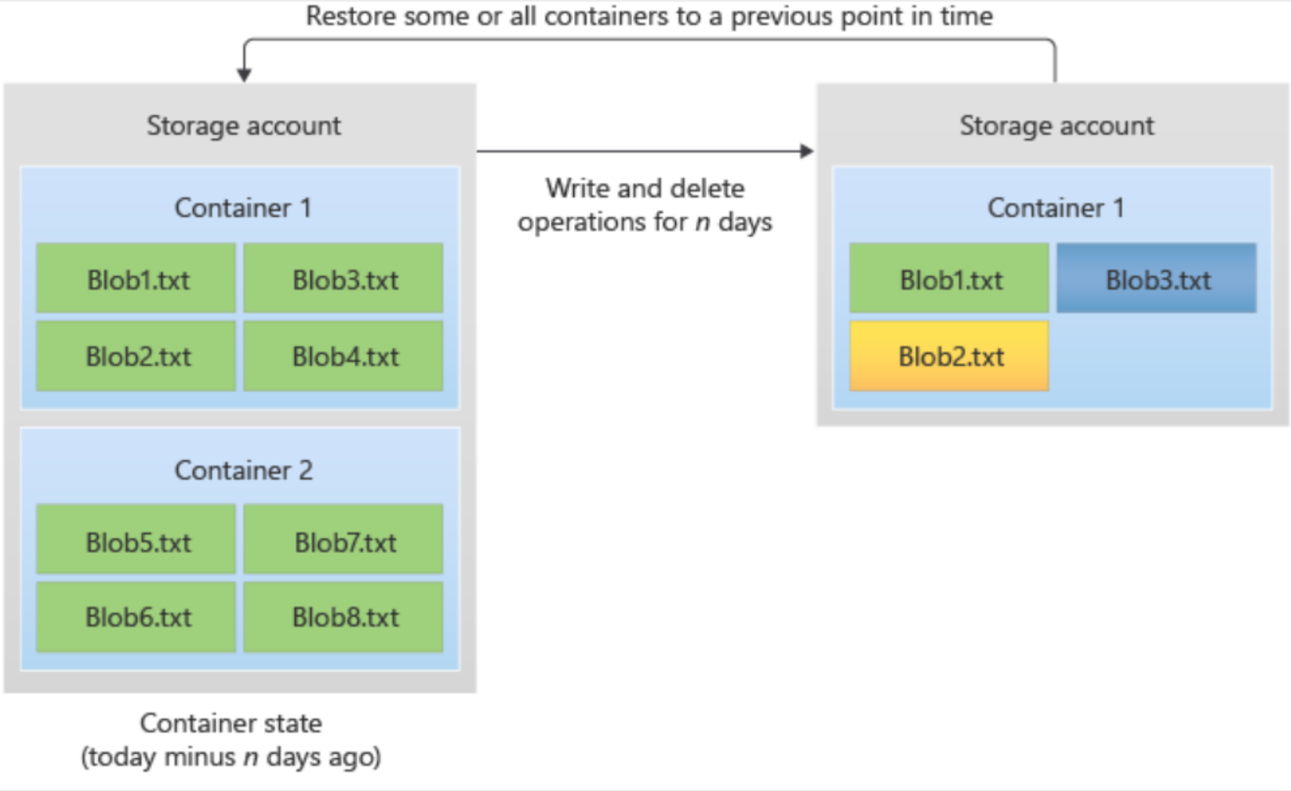
Advantages of Blob Soft Delete and Versioning

Soft delete maintains the deleted data in the system for a specified retention period. A user can restore a soft-deleted object to its previous state within the retention period.

Container soft delete	Restore a container and its contents at the time of deletion. Retention period : Between 1 and 365 days (for deleted containers)
Blob soft delete	Restore a blob, snapshot, or version that has been deleted. Retention period : Between 1 and 365 days (for deleted blobs)
Blob versioning	Restore an earlier version of a blob and recover the data if it is incorrectly modified or deleted.

Point-in-Time Restore for Block Blobs

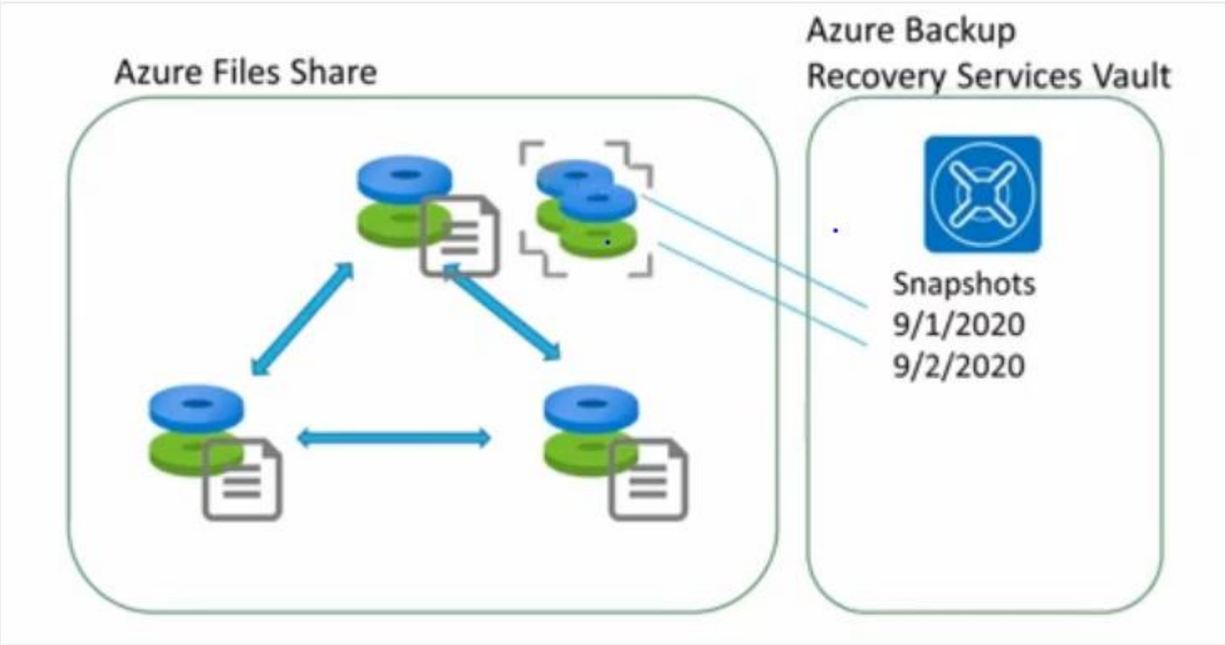
The diagram shows how point-in-time restore works:



The prior state of one or more containers or blob ranges is restored. As a result, write and delete actions that occurred during the retention period are reversed.

Azure Files Backup

Azure files are capable of taking share snapshots of file shares.



Share snapshots provide an added layer of security, lowering the danger of data corruption or deletion by accident.

Source: https://docs.microsoft.com/en-in/

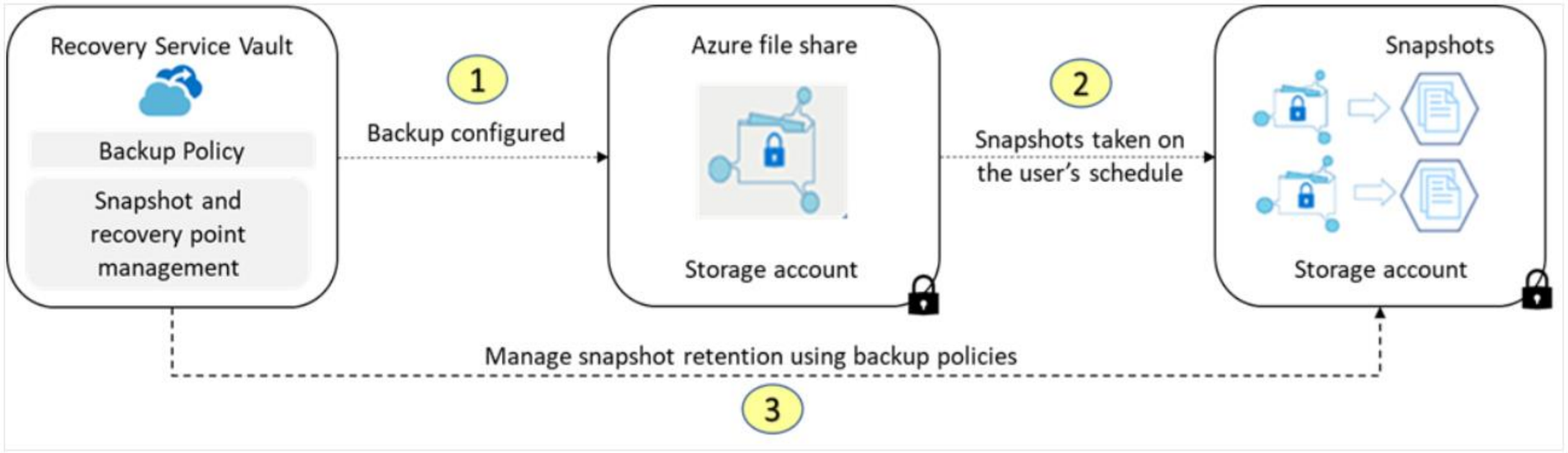
Snapshots Benefits

These are the benefits of Snapshots :

- Share snapshots capture the share state at that point in time.
- Snapshots can be automated using Azure Backup and backup policies.
- Snapshots can be created manually using the Azure portal, REST API, client libraries, the Azure CLI, and PowerShell.
- Snapshots are stored at the root level of a file sharing and applied to all its folders and files. Retrieval is done on a file-by-file basis.
- When a share snapshot is created, it can be read, copied, or deleted, but it cannot be modified.

Automating File Share Backups

The metadata of the backup is kept in the recovery services vault by Azure Backup, but no data is sent. This entails a quick backup solution with backup and built-in reporting.



Source: https://docs.microsoft.com/

Azure SQL Backup

Consider automated backups of a user's Azure SQL Database and Azure SQL Managed Instances

Full backups	Everything in the database and the transaction logs is backed up. Backup – every week
Differential backups	Everything that changed since the last full backup is backed up. Backup - every 12 - 24 hours
Transactional backups	The data is restored up to a specific time, which includes the moment before data was mistakenly deleted. Backup - every five to 10 minutes

Backup Usage Cases

Users can use automated backups in several ways

Uses	Explanation
Restore an existing database to a point in time in the past	To avoid overwriting the original database, this procedure generates a new database on the same server as the original database, but with a different name.
Restore a deleted database to the time of deletion	The deleted database can only be restored on the same server or managed instance where it was created in the first place.
Restore a database to another geographic region	When user can't access database or backups in user primary region due to a geographic disaster, user can use geo-restore to recover. It creates a new database in any Azure region on any existing server or managed instance.
Restore a database from a specific long-term backup	User can restore an older version of the database if the database has been setup with a long-term retention policy.

Long-Term Backup Retention Policies

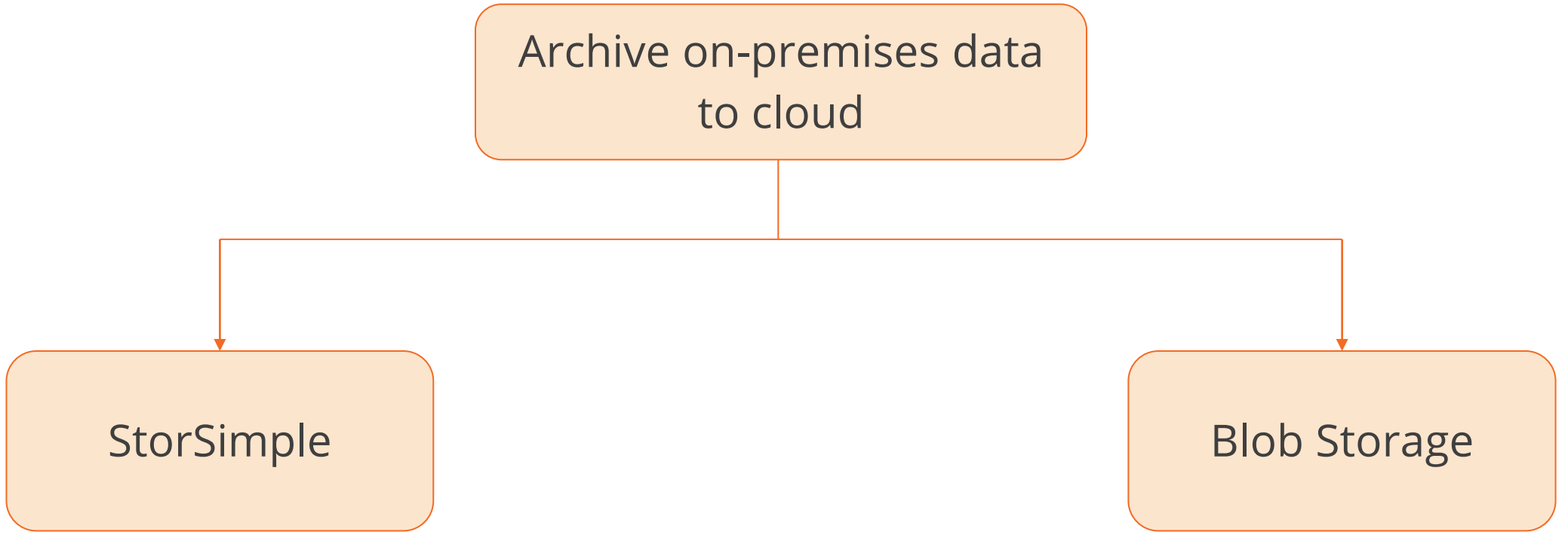
Recovery time objective (RTO) is the maximum acceptable time that an application can be unavailable after an incident.

- Backups of Azure SQL Database can be stored in read-access geo-redundant storage (RA-GRS) blobs for up to ten years.
- To access a backup in LTR, a user may use the Azure interface or PowerShell to restore it as a new database.

Design a Solution for Data Archiving and Retention

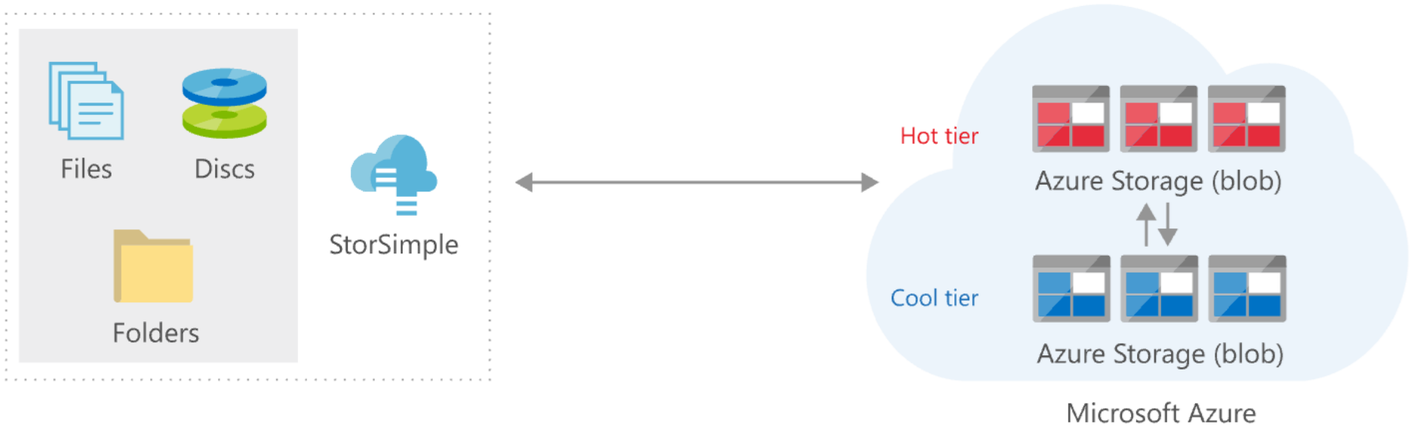
Archive On-Premises Data to Cloud

Azure Blob Storage can be used to archive on-premises data.



Archive On-Premises Data to Cloud

Azure StorSimple appliance running on-premises can tier data to Azure Blob storage (both hot and cool tier).

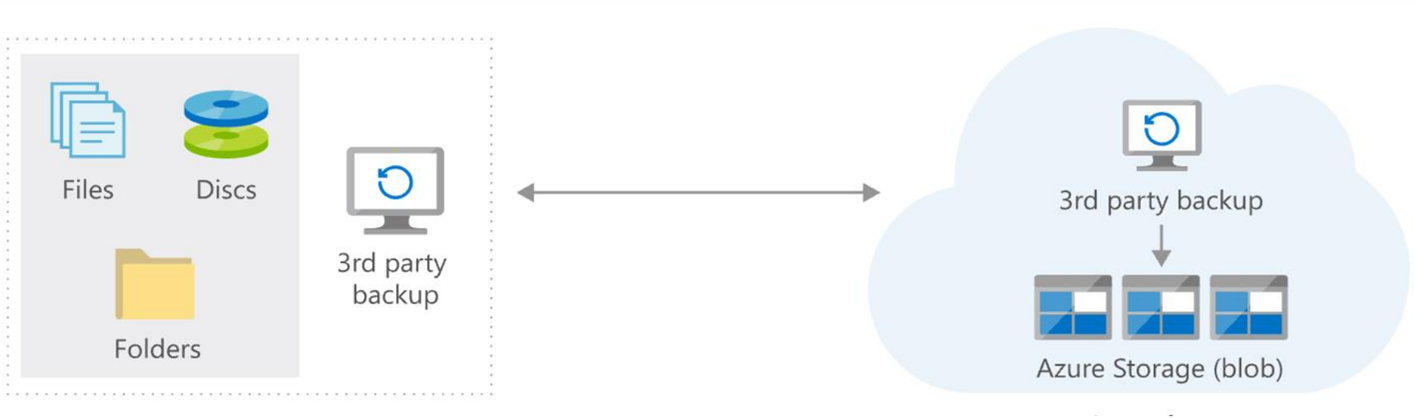


Azure StorSimple

StorSimple can be used to archive data from on-premises to Azure.

Archive On-Premises Data to Cloud

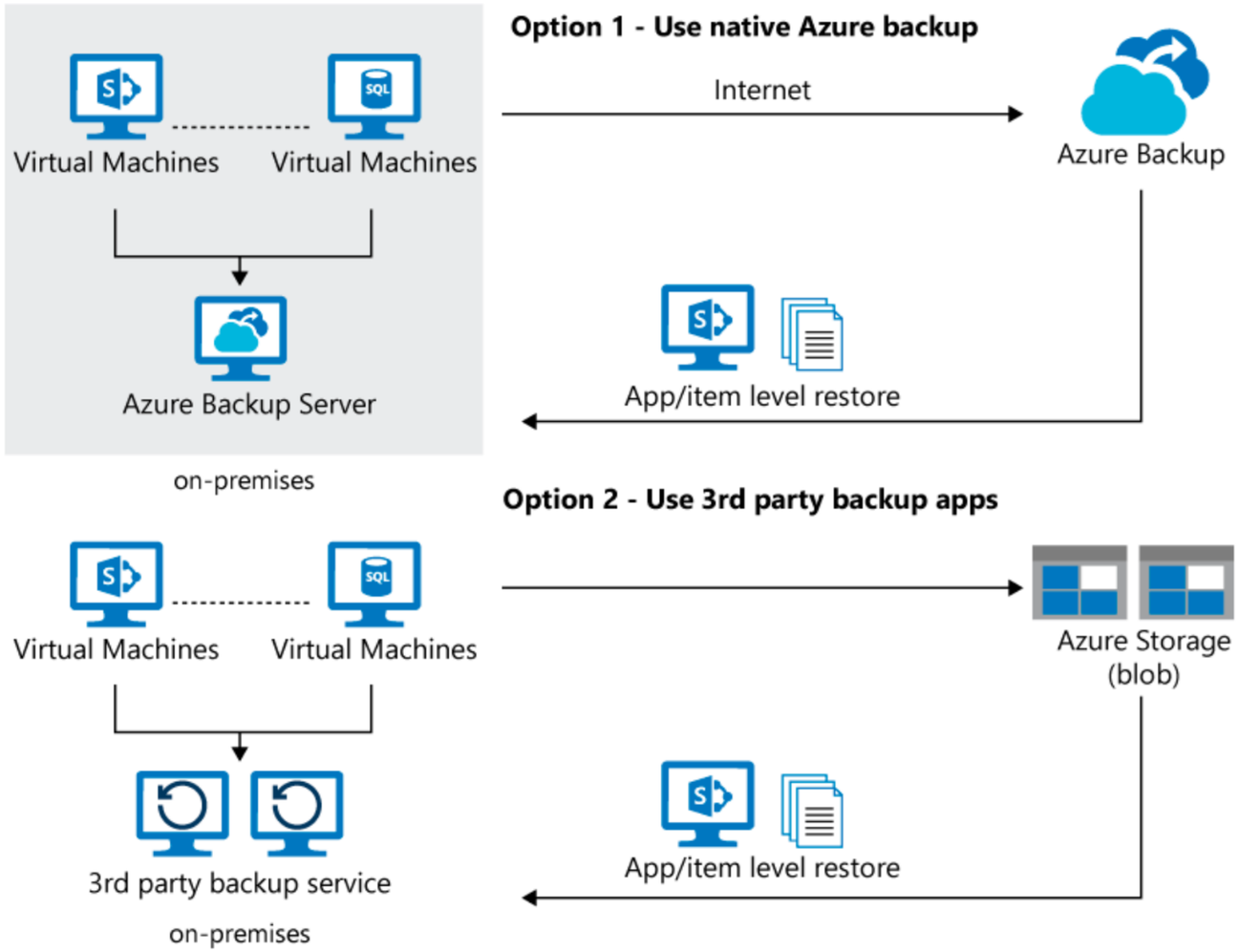
Blob Storage is a cool or archive tier on Azure Blob Storage, which is used to back up data that is less frequently accessed, while a hot tier is used to store data that is frequently accessed.



Azure Blob Storage

Backup On-Premises Applications and Data to the Cloud

Back up data and applications from an on-premises system to Azure using Azure Backup.

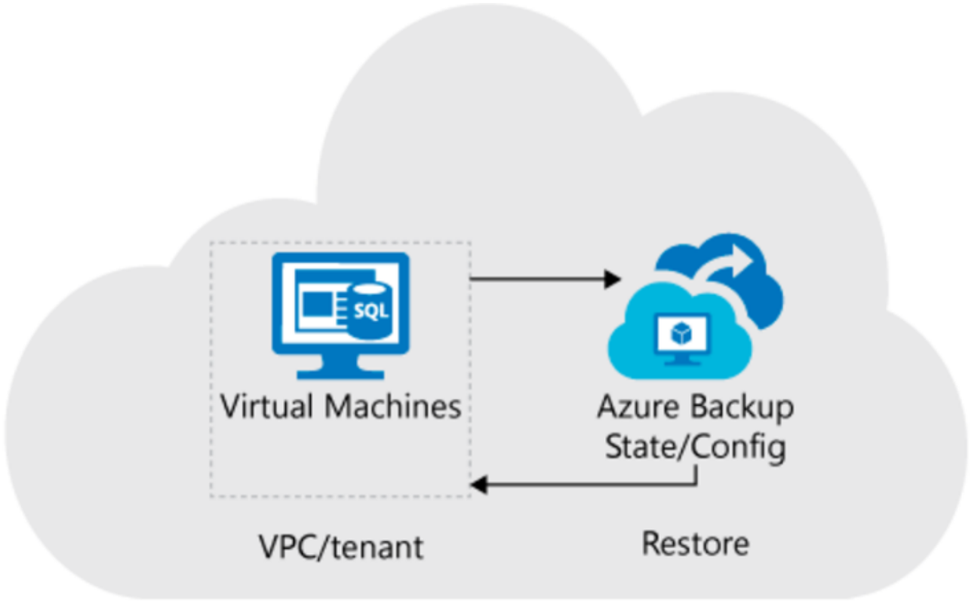


Backup On-Premises Applications and Data to the Cloud

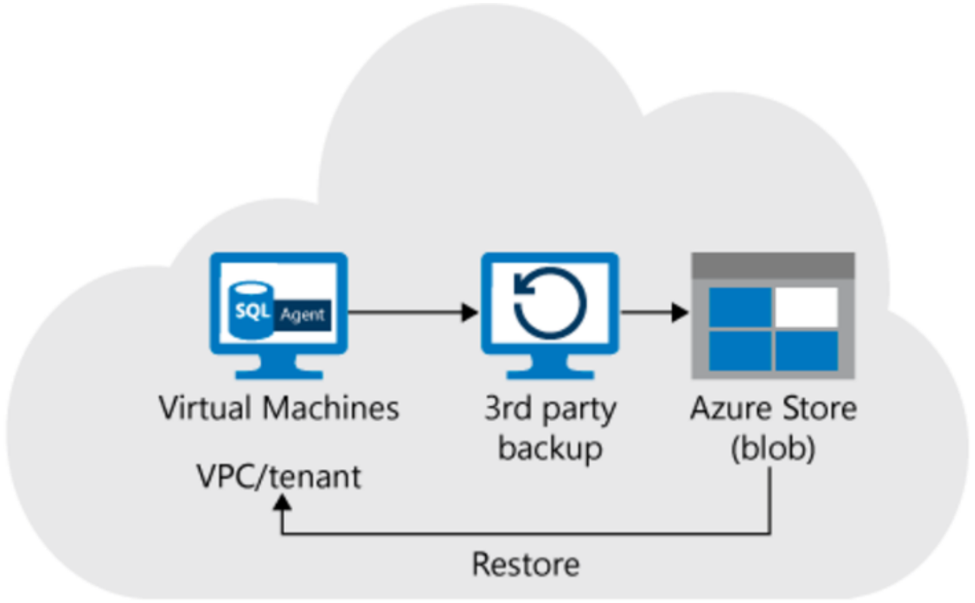
Azure Backup Server	Manages the configuration of restore procedures and orchestrates machine backups
Azure Backup Service	Runs on the cloud and holds the recovery points, enforce policies, and manages data and application protection
Blob Storage	Backs up data and applications for partner solutions such as Commvault

Backup Cloud Applications and Data to the Cloud

The two important components required to backup cloud applications and data to the cloud are Azure Backup Service and Blob Storage.



Option 1 - Use native Azure backup



Option 2 - Use 3rd party backup apps

Design and Azure Site Recovery Solution

Azure to Azure Site Recovery

Replicate Azure VMs to any other Azure location.

It automatically deploys ASR Mobility Service extension to protected machines.

Replicates:

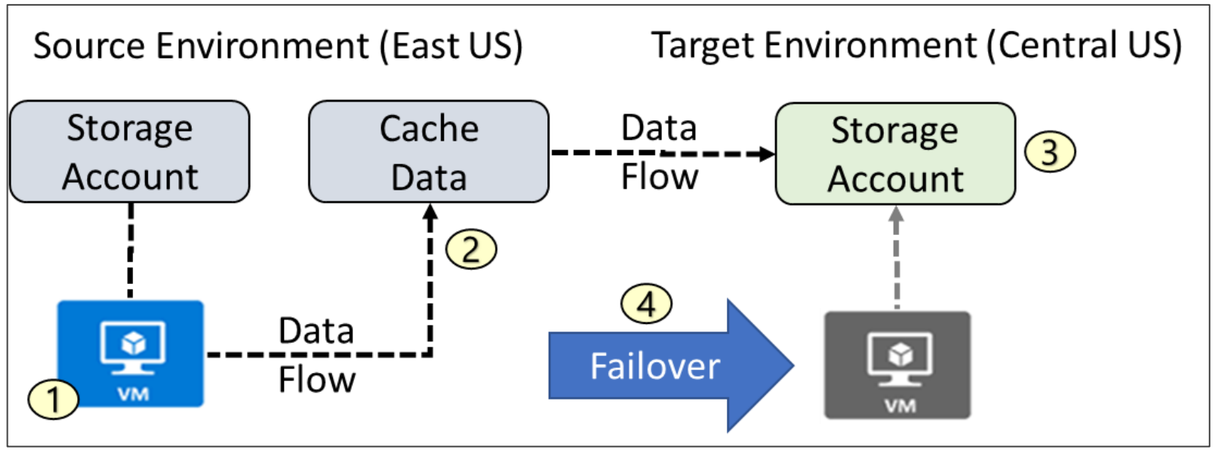
- VMs
- Virtual Networks
- Availability Sets
- Storage accounts
- Optionally – User can specify own VNets, Storage Accounts and Availability Sets

Replicates HTTPS channel on 443:

- Generates Azure egress cost for outbound traffic from primary region

Azure to Azure Architecture

These are steps of azure-to-azure architecture:



- VM is registered with Azure Site Recovery
- Data is continuously replicated to cache
- Cache is replicated to the target storage account
- During failover, the virtual machine is added to the target environment

Azure to Azure Site Recovery: Network Traffic

ASR traffic is only outbound from protected VMs.

Access to ASR URLs:

*.blob.core.windows.net	For naming storage writes
login.microsoftonline.com	Authorization and authentication to the ASR URLs
*.hypervrecoverymanager.windowsazure.com	ASR service communication channel
*.servicebus.windows.net	Monitoring and diagnostics

Azure to Azure Site Recovery: Network Traffic

ASR traffic is only outbound from protected VMs.

Outbound security rules for NSGs:

Site Recovery service and monitoring IP addresses (location specific)

Location	Site Recovery service IPs	Site Recovery monitoring IP
Central US	40.69.144.231	52.165.34.144

Snapshots and Recovery Points

Recovery points are created from snapshots.

Site Recovery snapshots:

Crash-consistent

Data that was on the disk when the snapshot was taken

App-consistent

All the information in a crash-consistent snapshot, plus all the data in memory and transactions in progress

Assisted Practice

Azure Site Recovery

Duration: 25 Min.

Problem Statement:

As an Azure Architect, you've been asked to assist your company with an Azure backup and recovery solution. Your data should be safe and recoverable with this Azure backup solution.

Assisted Practice: Guidelines

Steps to create Azure site recovery are:

1. Login the Azure portal
2. Search and select Recovery Service Vault
3. Configure Azure Site Recovery

Recommend a Solution for Recovery in Different Regions

Azure to Azure Disaster Recovery Architecture

The Azure to Azure disaster recovery architecture is shown below:

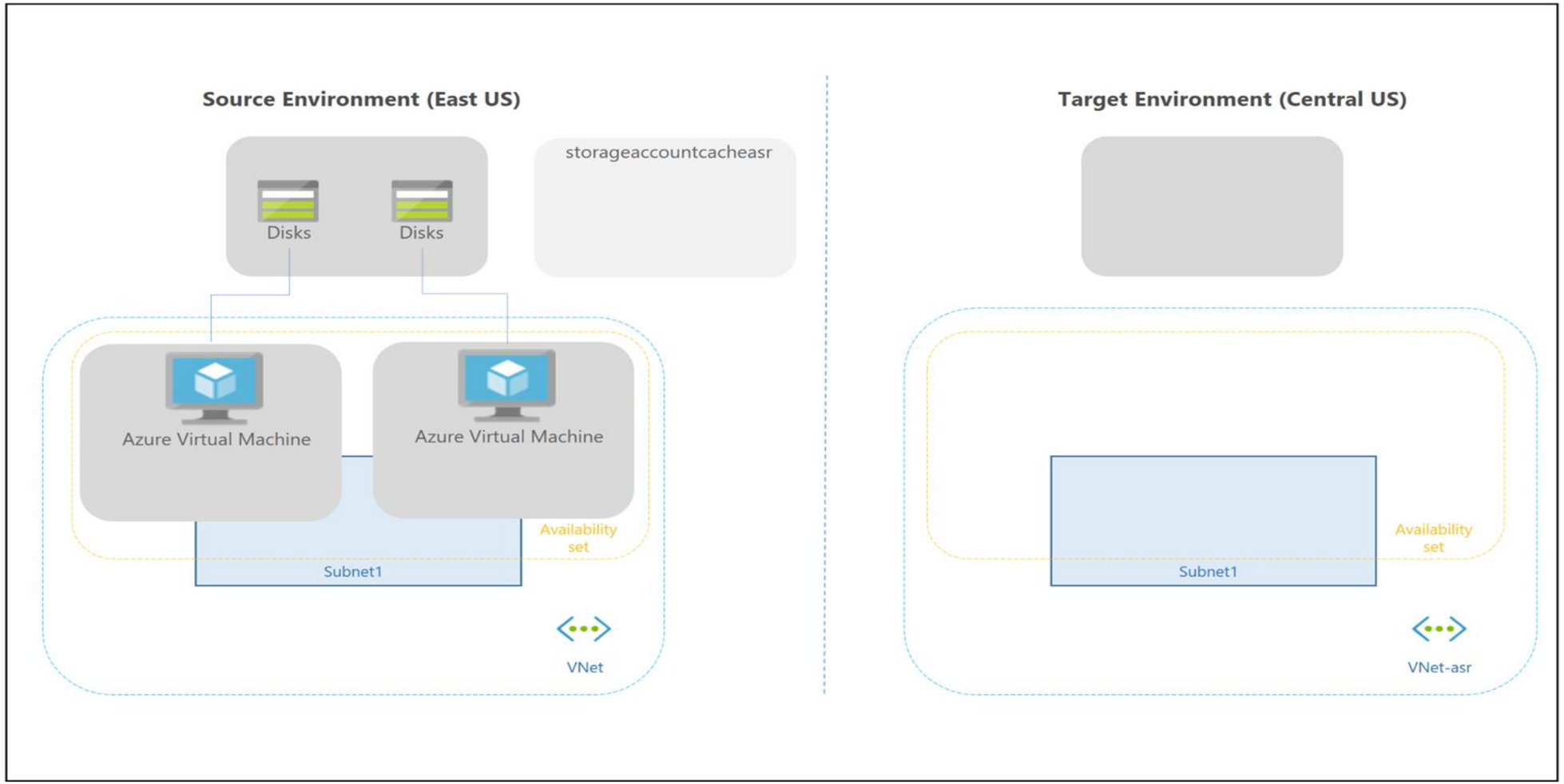


Image source: https://docs.microsoft.com/en-in/

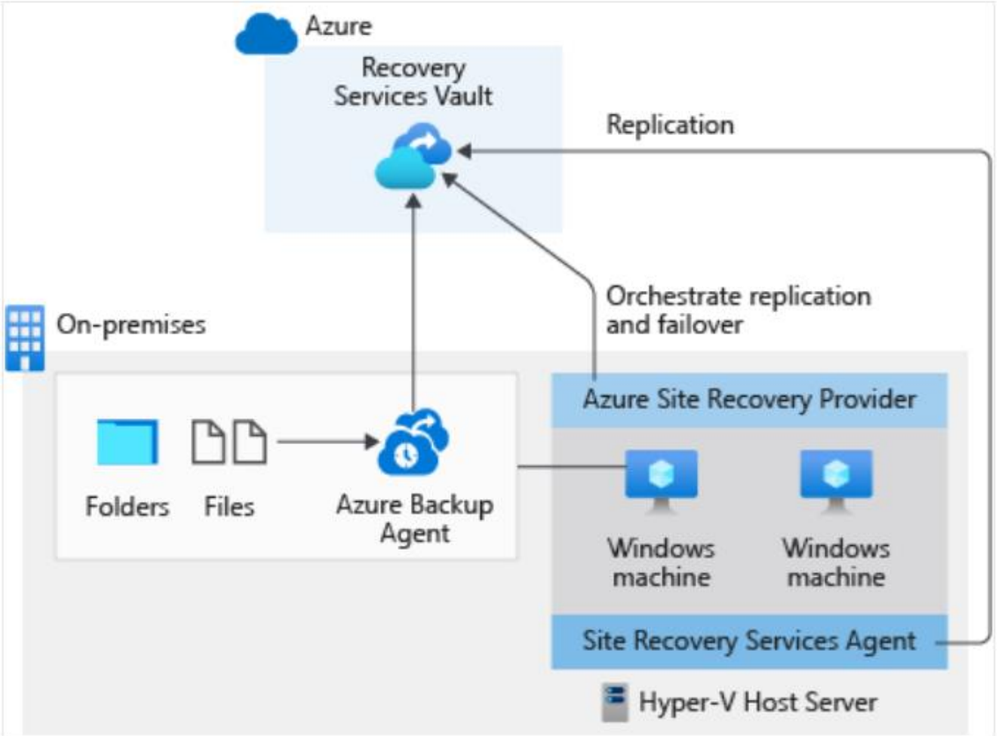
Azure Site Recovery Overview

Azure Site Recovery is a service that delivers BCDR capabilities for user Azure, on-premises, and other cloud-based applications.

It enables a user to automate disaster recovery by allowing them to define how machines restarted after they have been successfully failed over.

Azure Site Recover with Azure Backup

Azure Backup and Site Recovery can be used together as part of a single solution.



- Azure Backup backs up the files and folders on the Windows PC to Azure on a regular basis.
- Even if the entire on-premises environment fails, this method ensures that they are secure and retrievable.
- Separately, Site Recovery can be used to secure and maintain running workloads.

Architectural Components

These are the architectural components of disaster recovery:

- VMs in the source region
- Source VM storage
- Source VM networks
- Cache storage account
- Target resources

Architectural Components

The architectural components and requirements of disaster recovery are:

Components	Requirements
VMs in the source region	One or more Azure VMs must be in a supported source region.
Source VM storage	Non-managed disks can be distributed through storage accounts, whereas managed disks can be used in Azure VMs.
Source VM networks	In the source field, VMs can be found in one or more subnets of a virtual network.
Cache storage account	Using a cache means that production applications running on a VM have minimal effects.
Target resources	Target resources are used during replication and failover.

Replication Process

The replication process architecture is shown below:

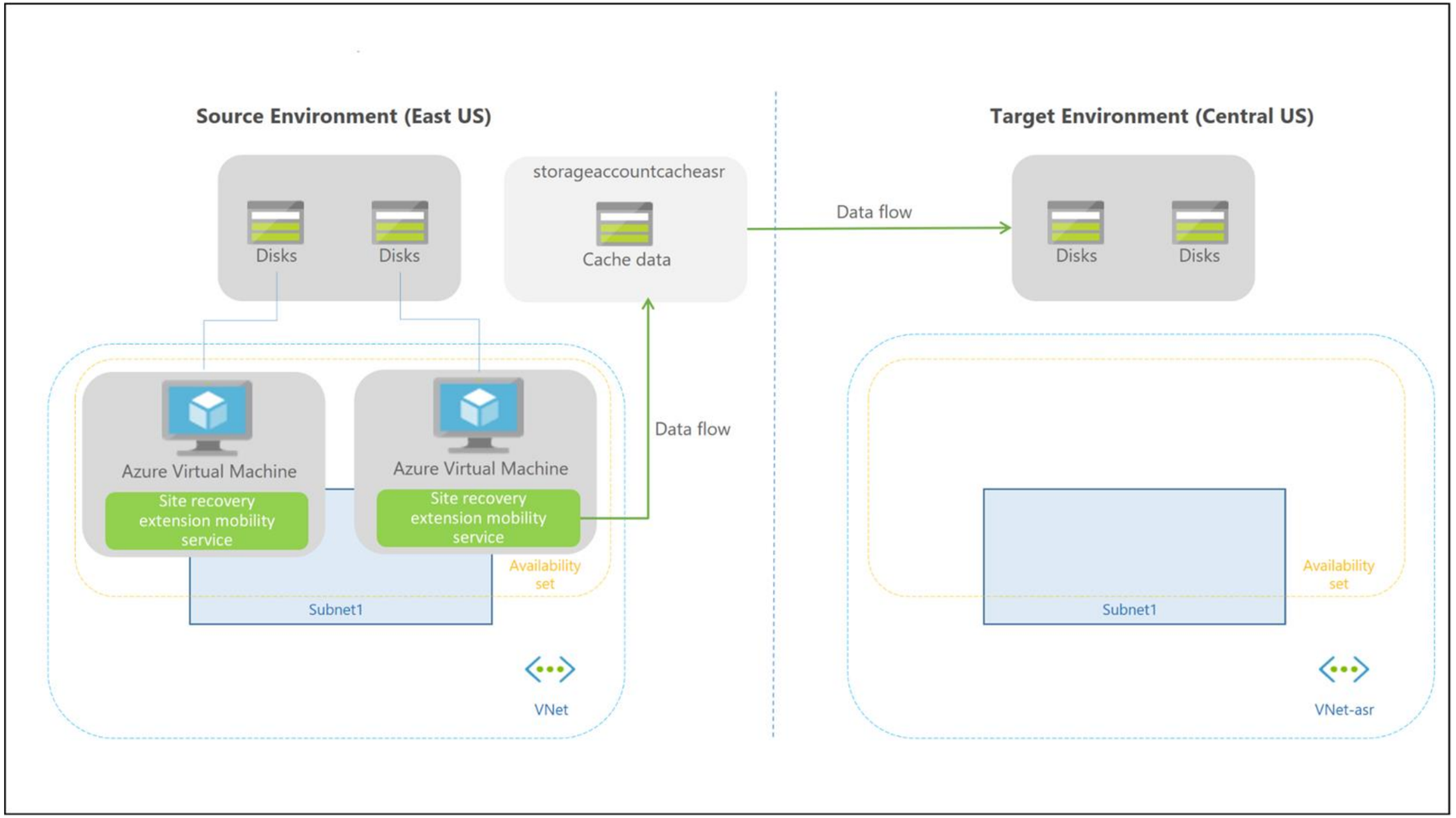


Image source: https://docs.microsoft.com/en-in/

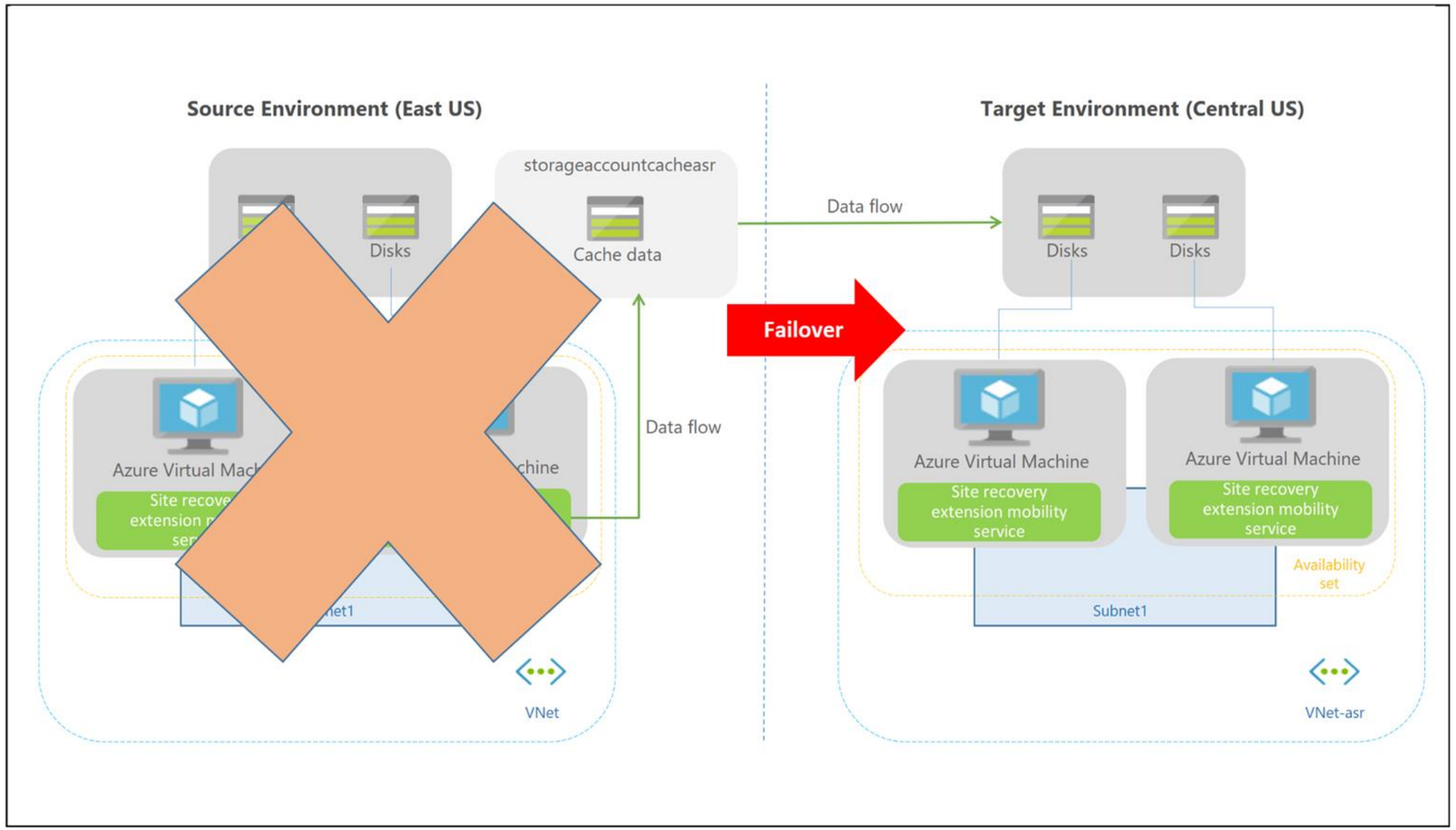
Replication Process

When replication is enabled for an Azure VM:

- The site recovery mobility service extension is installed on the VM.
- The extension registers the VM with site recovery.
- Continuous replication begins for the VM.
- Disk writes are transferred to the cache storage.
- Data is processed and sent to a target storage account or a replicated disk.
- Crash-consistent recovery points are generated every five minutes after data processing.

Failover Process

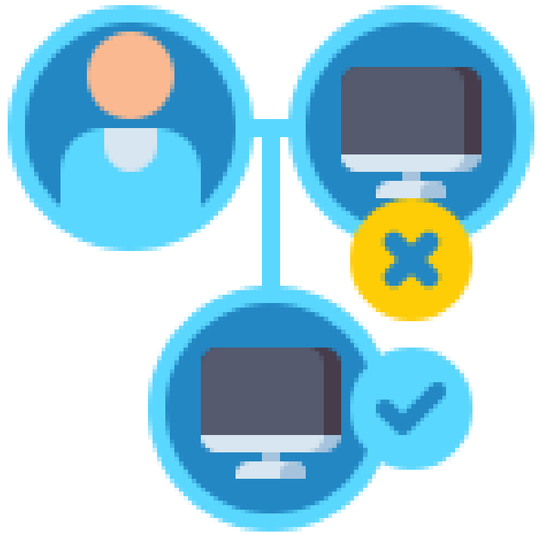
The failover process architecture is shown below:



Source: https://docs.microsoft.com/en-in/

Failover Process

When a user initiates a failover, the VMs are created in the target resource group, target virtual network, target subnet, and target availability set.



The user can use any recovery point during a failover.

Key Takeaways

- Defining the requirements, deploying the application regularly, and monitoring the health are all important facets in sustaining reliability.
- Recovery time objective (RTO) is the maximum acceptable time for which an application can be unavailable after an incident.
- The architectural components of disaster recovery are VMs in the source region, their storage and networks, cache storage account, and target resources.
- The two important components required to backup cloud applications and data to the cloud are Azure Backup Service and Blob Storage.

Azure Site Recovery between Azure region

Duration: 30 min

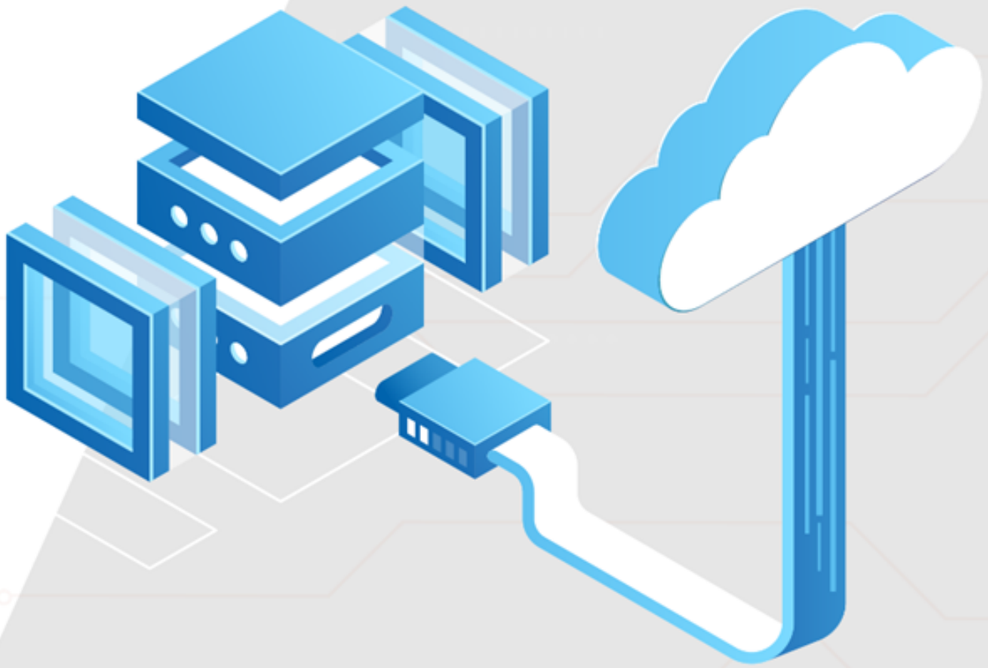
Project agenda: To implement Azure Site Recovery between Azure regions

Description: You need to implement Azure Site Recovery to facilitate migration and protection of Azure VMs between regions. To start, deploy an Azure VM to be migrated by using an Azure Resource Manager template and create an Azure Recovery Services vault. After that, you need to configure Azure VM replication and review Azure VM replication settings.

Perform the following:

1. Deploying an Azure VM to be migrated by using an Azure Resource Manager template
2. Creating an Azure Recovery Services vault
3. Configuring and reviewing Azure VM replication
4. Opening Cloud Shell and deleting resource groups

LESSON-END PROJECT



Thank you