Azure Backup provides secure and zero-infrastructure backup solutions for all Azure-managed data assets.

Azure Backup doesn't support cross-region backup for most workloads except cross-region restore in a paired secondary region.

Azure Backup is able to back up entire Windows and Linux VMs using backup extensions. we can back up the entire VM hosting SQL Server. If we only want to back up the files, folders, and system state on the Azure VMs, we can use the Microsoft Azure Recovery Services (MARS) agent.

Azure Backup provides support for SQL Server data back using stream-based, specialized solution with

1. full, differential, and log with 15-minute recovery point objective (RPO) ,
2. Point-in-time recovery up to a second,
3. Individual database-level backup and restore

Azure backup supports Azure role-based access control (Azure RBAC) boundary, providing you with the option to restrict access to backups only to authorized Backup Admins.

Backup Explorer provides an aggregated view of your entire backup estate, enabling detailed drill-down analysis and troubleshooting

Azure Backup *Back up Azure virtual machines running production workloads*

Azure Site Recovery *Azure Site Recovery is a service that helps ensure business continuity by replicating workloads from a primary site to a secondary location.*

Azure managed disks - image *Create an image from your custom virtual hard disk (VHD) in an Azure storage account or directly from a generalized (via Sysprep) virtual machine*

An Azure managed disks snapshot is a read-only full copy of a managed disk stored

We can set the default snapshot retention value from one to five days. Default is 2.

Recovery points for a virtual machine snapshot are available only after both phases (snapshot and save to vault) of the Azure Backup job are complete.

After a snapshot is first taken, the recovery points are identified with the **snapshot** recovery point type.

After the snapshot is transferred to an Azure Recovery Services vault, the recovery point type changes to **snapshot and vault**.

Azure Monitor is a comprehensive solution that collects, analyzes, and responds to telemetry data from both on-premises and cloud environments.

data collected by Azure Monitor fits into one of two fundamental types, metrics and logs:

Metrics are numerical values that describe some aspect of a system at a particular point in time. Metrics are lightweight and capable of supporting near real-time scenarios.

Logs contain different kinds of data organized into records with different sets of properties for each type. Data like events and traces are stored as logs along with performance data so all the data can be combined for analysis.

- Azure Monitor begins collecting data as soon as you create your Azure subscription and add resources.
- When you create or modify resources, this data is stored in Azure Monitor activity logs.
- Performance data about resources, along with the amount of resources consumed, is stored as Azure Monitor metrics.
- Extend the data you're collecting by enabling diagnostics and adding Azure Monitor Agent to compute resources. By extending your data sources, you can collect data for the internal operation of the resources.
- Azure Monitor Agent also lets you configure different data sources to collect logs and metrics from Windows and Linux guest operating systems.
- Azure Monitor can collect log data from any REST client by using the Data Collector API. The Data Collector API lets you create custom monitoring scenarios and extend monitoring to resources that don't expose data through other sources.

Activity logs are kept for 90 days.

Log Analytics is a tool in Azure Monitor that allows you to edit and run log queries for data collected in Azure Monitor Logs. It offers query features and tools, supports the Kusto Query Language (KQL), and allows for detailed analysis and problem-solving.

IP flow verify feature is ideal for helping to ensure correct application of your security rules.

next hop feature is ideal for identifying unresponsive virtual machines or broken routes in your network.

Azure Network Watcher provides a network monitoring **topology** tool to help administrators visualize and understand infrastructure.

Azure Monitor, Azure Service Health, and Azure Advisor use *action groups* to notify users about the alert, and to take an action when an alert is fired. An action group is a collection of notification preferences and actions that are executed when the alert is fired. You can run one or more actions for each triggered alert.

Azure Monitor can perform any of the following actions:

- Send an email
- Send a Short Message Service (SMS) message
- Create an Azure app push notification
- Make a voice call to a number
- Call an Azure function
- Trigger a logic app
- Send a notification to a webhook
- Create an IT Service Management (ITSM) ticket
- Use a runbook (to restart a virtual machine (VM) or scale a VM up or down)

Metrics are stored in a time-series database.

Azure Monitor Metrics automatically monitors a predefined set of metrics for every Azure VM, and retains the data for 93 days with some exceptions.