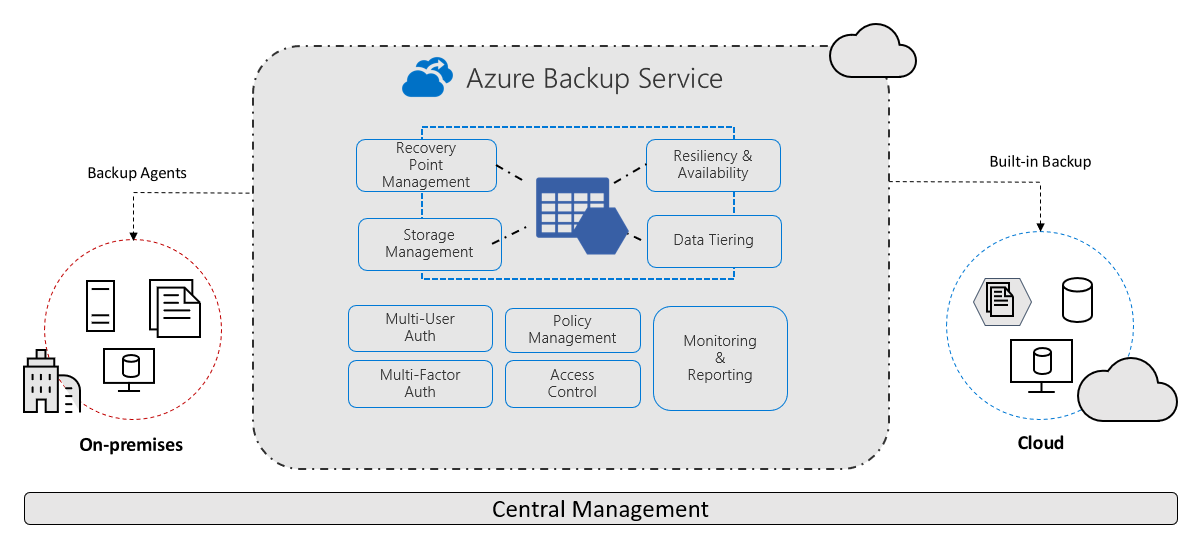
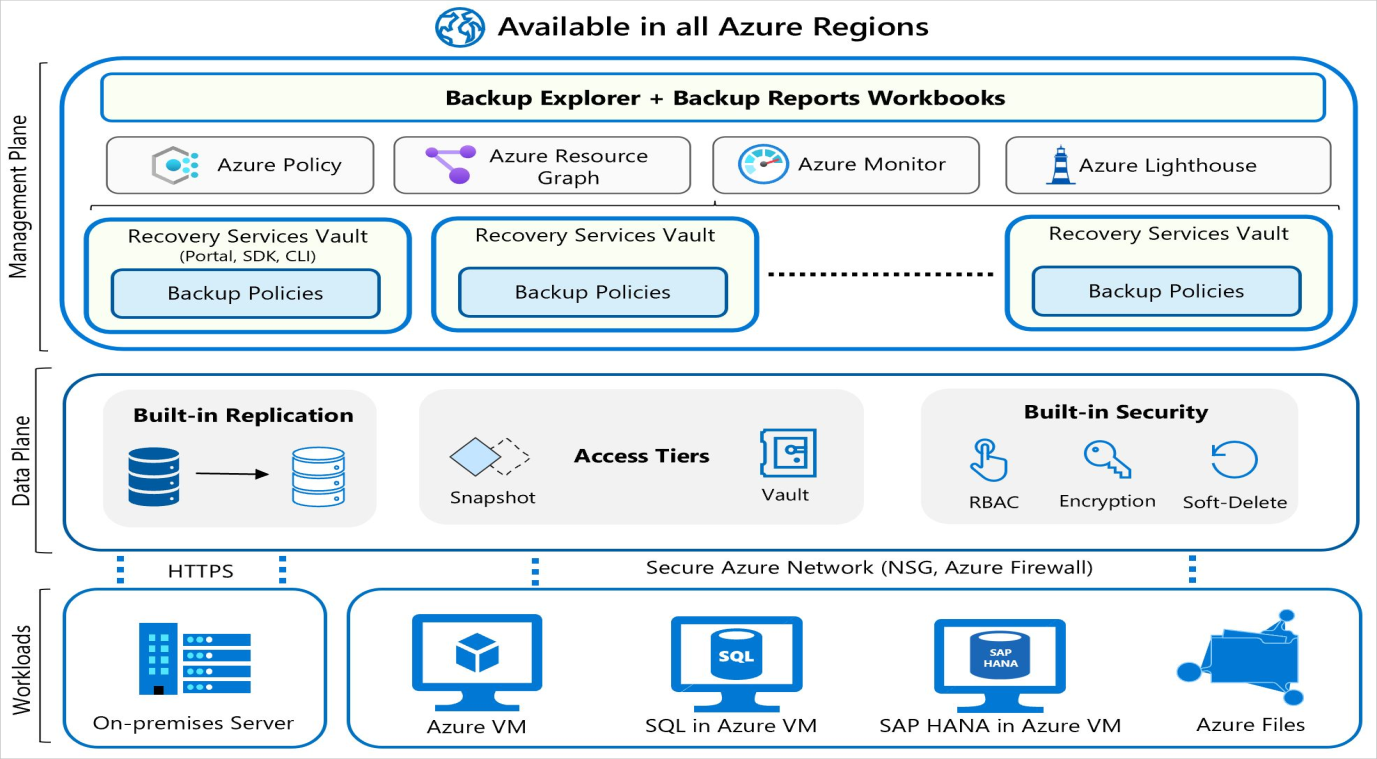
**6.1 - Introduction to Azure Backup**

**What is Azure Backup?**

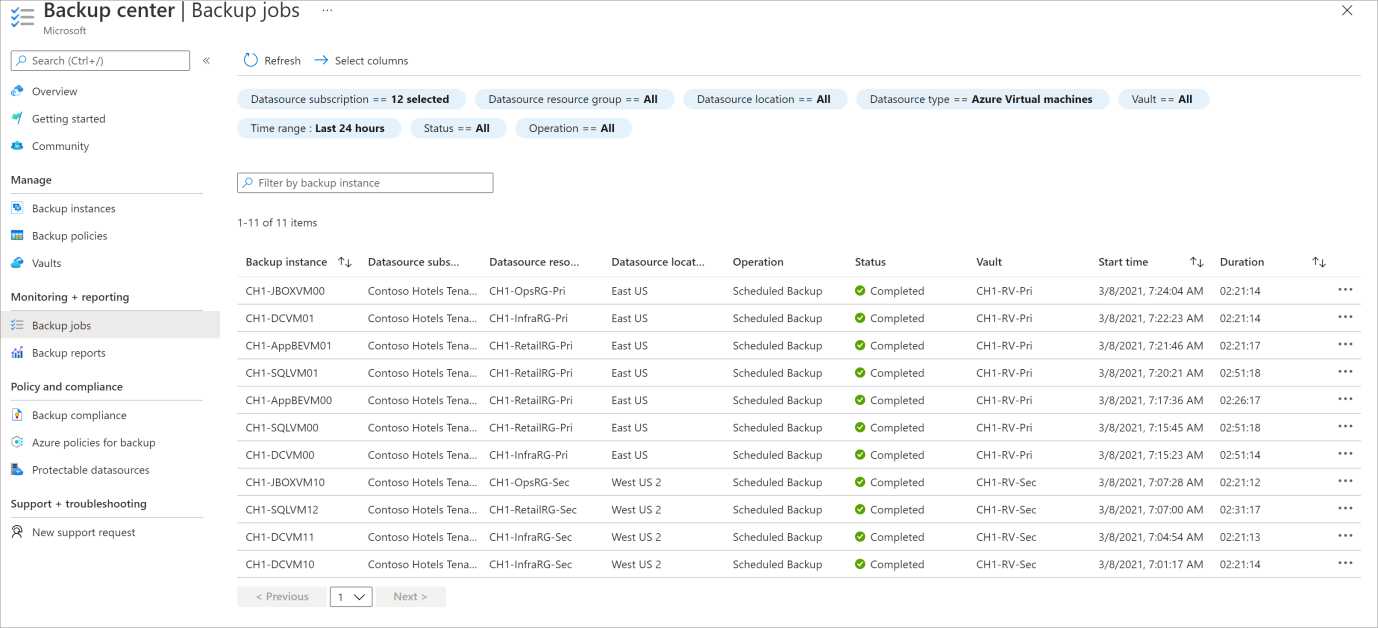
* The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.
* Azure Backup is an Azure service that provides cost effective, secure, and zero-infrastructure backup solutions for all Azure-managed data assets.
* The centralized management interface makes it easy to define backup policies and protect a wide range of enterprise workloads, including Azure Virtual Machines, Azure Disks, SQL and SAP databases, Azure file shares, and blobs.



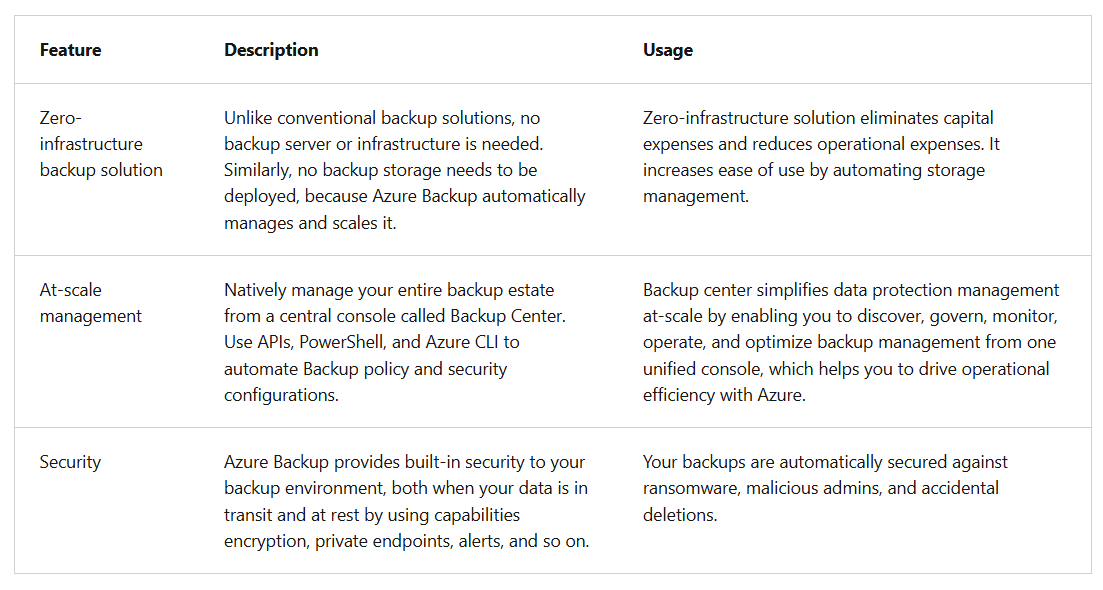


**When to use Azure Backup**

* As the IT admin of your organization, you're responsible for meeting the compliance needs for all the data assets of the firm, and backup is a critical aspect. There are also various application admins in your company who need to do self-service backup and restore to take care of issues like data corruption or rogue-admin scenarios. You're looking for an enterprise-class backup solution to protect all your workloads and manage them from a central place.
* Azure Backup can provide backup services for the following data assets:
  + On-premises files, folders, and system state
  + Azure Virtual Machines (VMs)
  + Azure Managed Disks
  + Azure Files Shares
  + SQL Server in Azure VMs
  + SAP HANA (High-performance Analytic Appliance) databases in Azure VMs
  + Azure Database for PostgreSQL servers
  + Azure Blobs
  + Azure Database for PostgreSQL - Flexible servers
  + Azure Database for MySQL - Flexible servers
  + Azure Kubernetes cluster



**Azure Backup key features**



**How do Recovery Time Objective and Recovery Point Objective work?**

* **Recovery Time Objective (RTO)** is the target time within which a business process must be restored after a disaster occurs to avoid unacceptable consequences. For instance, if a critical application goes down due to a server failure and the business can only tolerate a maximum of four hours of downtime, then the RTO is four hours.
* **Recovery Point Objective (RPO)** is the maximum amount of data loss, measured in time, that your organization can sustain during an event.
* The following example scenario describes both the RPO and RTO concepts:
  + Your organization has an RPO of one hour for your customer database, which means you perform backups every hour. If a data-loss incident occurs, you lose not more than one hour of data. When you set RTO to three hours, then if a system failure occurs, you aim to restore access to the database within three hours to minimize the impact on operations.

**How Azure Backup works**

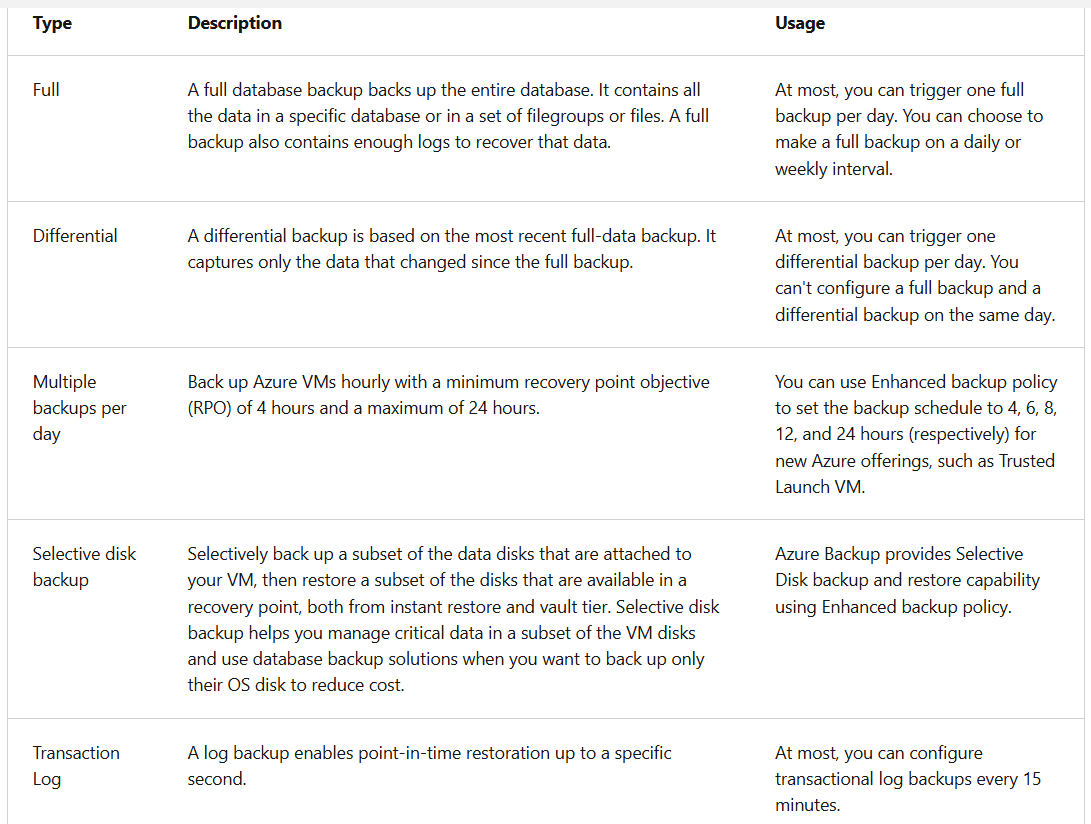
* **Workload integration layer** **- Backup Extension**: Integration with the actual workload, such as Azure virtual machines (VMs) or Azure Blobs, happens at this layer.
* **Data Plane - Access Tiers**: There are three access tiers where the backups could be stored:
  + Snapshot tier
  + Standard tier
  + Archive tier
* **Data Plane - Availability and Security**: The backup data is replicated across zones or regions, based on the redundancy the user specifies.
* **Management Plane – Recovery Services vault/Backup vault and Backup center:** The vault provides an interface for the user to interact with the backup service.

**What data is backed up and how?**

* The simplest explanation of Azure Backup is that it backs up data, machine state, and workloads running on on-premises machines and VM instances to the Azure cloud. Azure Backup stores the backed-up data in Recovery Services vaults and Backup vaults.
* For on-premises Windows machines, you can back up directly to Azure with the Azure Backup Microsoft Azure Recovery Services (MARS) agent. Alternatively, you can back up these Windows machines to a backup server, perhaps a System Center Data Protection Manager (DPM) or Microsoft Azure Backup Server (MABS). You can then back that server up to a Recovery Services vault in Azure.
* If you're using Azure VMs, you can back them up directly. Azure Backup installs a backup extension to the Azure VM agent that's running on the VM, which allows you to back up the entire VM. If you only want to back up the files and folders on the VM, you can do so by running the MARS agent.
* Azure Backup stores backed-up data in vaults: Recovery Services vaults and Backup vaults. A vault is an online-storage entity in Azure that's used to hold data such as backup copies, recovery points, and backup policies.

**Supported backup types**

* Azure Backup supports full backups and incremental backups. Your initial backup is a full backup. DPM/MABS use the incremental backup for disk backups, and all backups to Azure also use incremental backups. As the name suggests, incremental backups only focus on the blocks of data that changed since the previous backup.
* Azure Backup also supports SQL Server backup types. The following table outlines the support for SQL Server type backups:



**Workload integration layer - Backup Extension**

* A backup extension specific to each workload is installed on the source VM or a worker VM. At the time of backup (as defined by the user in the Backup Policy) the backup extension generates the backup, which could be:
  + **Storage**: Snapshots when using an Azure VM or Azure Files.
  + **Stream backup**: For databases like SQL or High-performance Analytic Appliance (HANA) running in VMs.
* The backup data is eventually transferred to Azure Backup managed storage in the data plane by using secure Azure networks Network Security Groups (NSG), Firewalls, or more sophisticated private endpoints.

**Data Plane - Access Tiers**

* **Snapshot tier:** (Workload-specific term) In the first phase of a virtual machine backup, the snapshot is taken and stored along with the disk. This form of storage is referred to as a snapshot tier. Restoring a snapshot tier is faster than restoring from a vault, because it eliminates the wait time for snapshots to be copied from the vault before triggering the restore operation. The snapshots of the VM/Azure Files/Azure Blobs/and so on are retained in the customer's subscription in a specified resource group. This container ensures that restores are quick, because the backup/snapshot is available locally to the customer.
* **Vault-standard tier:** Backup data for all workloads supported by Azure Backup is stored in vaults, which hold backup storage, an autoscaling set of storage accounts managed by Azure Backup. The Vault-standard tier is an online storage tier that allows you to store an isolated copy of backup data in a Microsoft-managed tenant, thus creating an extra layer of protection. For workloads where snapshot tier is supported, there's a copy of the backup data in both the snapshot tier and the Vault-standard tier. The Vault-standard tier ensures that backup data is available even if the data source being backed up is deleted or compromised.
* **Archive tier:** Customers rely on Azure Backup for storing backup data, including their Long-Term Retention (LTR) backup data, with retention needs defined in the organization's compliance rules. In most cases, the older backup data is rarely accessed and is only stored for compliance needs.
* **Azure Backup supports backup of long-term retention points in the archive tier**.

**Data Plane - Availability and Security**

* The backup data is replicated across zones or regions, based on the redundancy you specify. You can choose from locally redundant storage (LRS), Geo-redundant storage (GRS), or zone-redundant storage (ZRS). These options provide you with highly available data storage capabilities.
* The data is kept safe by encrypting it and implementing Azure role-based access control (RBAC). You choose who can perform backup and restore operations. Azure Backup also provides protection against malicious deletion of your backup by using soft-delete operations. A deleted backup is stored for 14 days, free of charge, which allows you to recover the backup if needed.
* Azure Backup also supports a backup data lifecycle-management scenario that allows you to comply with retention policies.

**Management Plane – Recovery Services vault/Backup vault and Backup center**

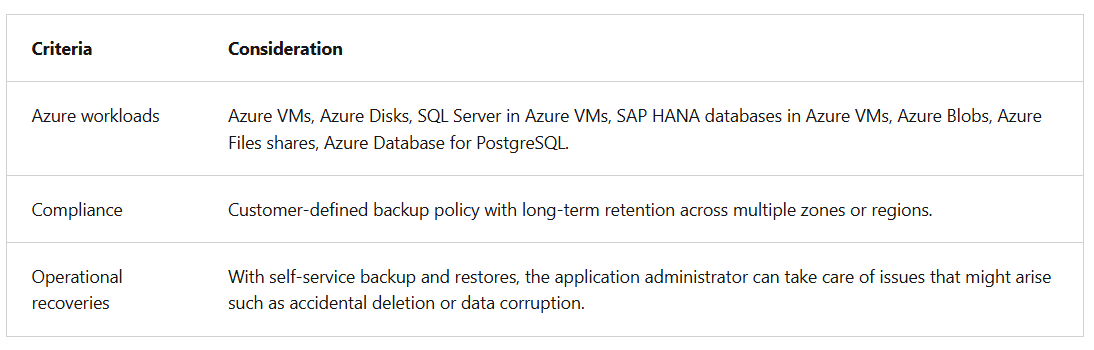
* Azure Backup uses Recovery Services vaults and Backup vaults to orchestrate and manage backups. It also uses vaults to store backed-up data. The vault provides an interface for the user to interact with the backup service. Azure Backup Policies within each vault define when the backups should get triggered and how long they need to be retained.
* You can use a single vault or multiple vaults to organize and manage your backup. If you manage your workloads with a single subscription and single resource, you can use a single vault to monitor and manage your backup estate. If your workloads are spread across multiple subscriptions, you can create multiple vaults with one or more vaults per subscription.
* Backup center allows you to have a single pane of glass to manage all tasks related to backups. Backup center is designed to function well across a large and distributed Azure environment. You can use Backup center to efficiently manage backups spanning multiple workload types, vaults, subscriptions, regions, and Azure Lighthouse tenants.

**When to use Azure Backup**

* Common backup scenarios where Azure Backup provides benefits, such as:
  + Ensuring availability of your data.
  + Protecting your Azure workloads.
  + Securing your data.

**Decision criteria**

* Azure Backup is an Azure service that provides secure and zero-infrastructure backup solutions for all Azure-managed data assets. It protects a wide range of enterprise workloads. Including, Azure Virtual Machines (VMs), Azure Disks, SQL and SAP databases, and Azure file shares and blobs.
* The main criteria that we're evaluating are outlined in the following table. The table contains some key areas where Azure Backup can provide services to you for data protection.

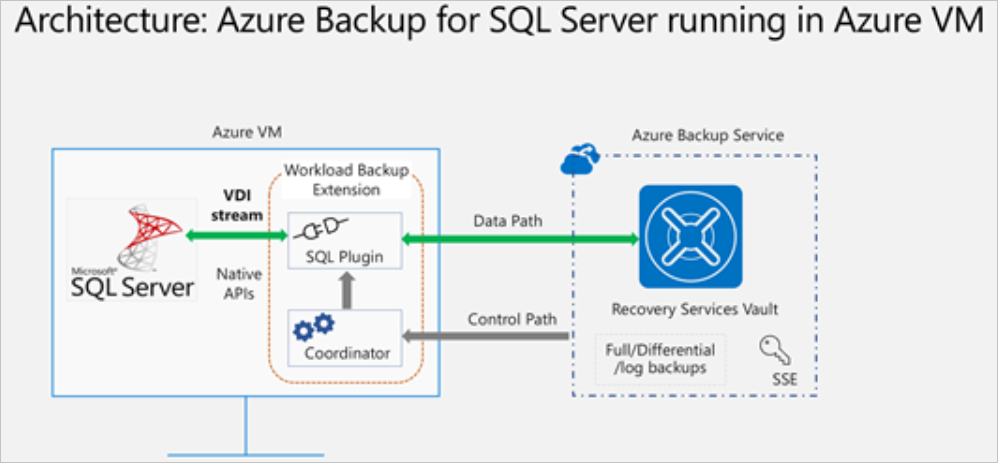


**Apply the criteria**

* Before we dive into how Azure Backup can help meet these needs, it's important to understand what isn't currently supported. If your three Azure VMs are deployed across multiple subscriptions or regions, you should note that Azure Backup doesn’t support cross-region backup for most workloads. However, it does support cross-region restore in a paired secondary region.

**Can Azure Backup protect the Azure VMs hosting the SQL Server instances?**

* Azure Backup is able to back up entire Windows and Linux VMs using backup extensions. As a result, you can back up the entire VM that hosts SQL Server. If you only want to back up the files, folders, and system state on the Azure VMs, you can use the Microsoft Azure Recovery Services (MARS) agent.
* If your main concern is to only back up the SQL Server data, Azure Backup provides support for that as well. Azure Backup offers a stream-based, specialized solution to back up SQL Servers running in Azure VMs. This solution aligns with Azure Backup's benefits of zero-infrastructure backup, long-term retention, and central management.
* Additionally, Azure Backup provides the following advantages specifically for SQL Server:
  + Workload aware backups that support all backup types: full, differential, and log
  + 15-minute recovery point objective (RPO) with frequent log backups
  + Point-in-time recovery up to a second
  + Individual database-level backup and restore



**Does Azure Backup help with compliance?**

* You can implement required access-control mechanisms for your backups. Vaults (Recovery Services and Backup vaults) provide the management capabilities and are accessible via the Azure portal, Backup Center, Vault dashboards, SDK, CLI, and even REST APIs. It's also an Azure role-based access control (Azure RBAC) boundary, providing you with the option to restrict access to backups only to authorized Backup Admins.
* **Short-term retention** can be minutes or daily. Retention for weekly, monthly, or yearly backup points is referred to as Long-term retention.
* **Long-term retention** can be:
  + **Planned (compliance requirements)**: If you know in advance that data is required years from the current time, use Long-term retention.
  + **Unplanned (on-demand requirement)**: If you don't know in advance, then you can use on-demand backup with specific custom retention settings. Your policy settings don't impact these custom retention settings.
  + **On-demand backup with custom retention**: If you need to take a backup not scheduled via backup policy, then you can use an on-demand backup. It can be useful for taking backups that don’t fit your scheduled backup or for taking granular backup (for example, multiple IaaS VM backups per day since scheduled backup permits only one backup per day). It's important to note that the retention policy defined in scheduled policy doesn't apply to on-demand backups.
* You can also implement policy management to help with compliance. Azure Backup Policies within each vault define when the backups should be triggered and how long they need to be retained. You can also manage these policies and apply them across multiple items.

**Does Azure Backup simplify monitoring and administration?**

* Azure Backup integrates with Log Analytics for monitoring and reporting and provides reports via Workbooks.
* Azure Backup provides in-built job monitoring for operations such as configuring backup, backing up, restoring, deleting backups, and so on. Azure Backup is scoped to the vault, making it ideal for monitoring a single vault.
* If you need to monitor operational activities at scale, Backup Explorer provides an aggregated view of your entire backup estate, enabling detailed drill-down analysis and troubleshooting. It's a built-in Azure Monitor workbook that provides a single, central location to help you monitor operational activities across the entire backup estate on Azure, spanning tenants, locations, subscriptions, resource groups, and vaults.

**6.2 - Protect your virtual machines by using Azure Backup**

**What is Azure Backup?**

* Azure Backup is a built-in Azure service that provides secure backup for all Azure-managed data assets. It uses zero-infrastructure solutions to enable self-service backups and restores, with at-scale management at a lower and predictable cost. Azure Backup currently offers specialized backup solutions for Azure and on-premises virtual machines (VMs). Azure Backup also gives workloads like SQL Server or SAP HANA (High-performance Analytic Appliance) running in Azure VMs enterprise-class backup and restore options.
* In contrast to traditional backup solutions that can take considerable effort to set up, Azure Backup is easily managed through the Azure portal.

**Azure Backup versus Azure Site Recovery**

* Both Azure Backup and Azure Site Recovery aim to make the system more resilient to faults and failures, but they use two different approaches. The primary goal of Backup is to maintain copies of stateful data that allow you to go back in time. Site Recovery, however, replicates the data in almost real time and allows for a failover.
* In that sense, if there are issues like network or power outages, you can use availability zones. For a region-wide disaster (such as natural disasters), Site Recovery is used. Backups are used in cases of accidental data loss, data corruption, or ransomware attacks.

**Azure Backup supported scenarios**

* **Azure VMs** - Back up Windows or Linux Azure VMs
* **On-premises** - Back up files, folders, and system state using the Microsoft Azure Recovery Services (MARS) agent. Or use Microsoft Azure Backup Server (MABS) or Data Protection Manager (DPM) server to protect on-premises VMs (Hyper-V and VMware) and other on-premises workloads.
* **Azure Files shares** - Azure Files provides snapshot management by Azure Backup.
* **SQL Server in Azure VMs and SAP HANA databases in Azure VMs** - Azure Backup offers stream-based, specialized solutions to back up SQL Server, or SAP HANA running in Azure VMs. These solutions take workload-aware backups that support different backup types such as full, differential and log, 15-minute RPO, and point-in-time recovery.

**Why use Azure Backup?**

* **Zero-infrastructure backup**: Azure Backup eliminates the need to deploy and manage any backup infrastructure or storage. There's no overhead in maintaining backup servers or scaling the storage up or down as the needs vary.
* **Long-term retention**: Meet rigorous compliance and audit needs by retaining backups for many years, after which the built-in lifecycle management capability prunes the recovery points automatically.
* **Security**: Azure Backup provides security to your backup environment, both when your data is in transit and at rest:
  + **Azure role-based access control**: Role-based access control allows you to segregate duties within your team and grant only the amount of access to users necessary to do their jobs.
  + **Encryption of backups**: Backup data is automatically encrypted using Microsoft-managed keys. Alternatively, you can encrypt your backed-up data using customer-managed keys stored in the Azure Key Vault.
  + **No internet connectivity required**: When you use Azure VMs, all the data transfer happens only on the Azure backbone network without needing to access your virtual network. So no access to any IPs or fully qualified domain names (FQDNs) is required.
  + **Soft delete**: With soft delete, the backup data is retained for 14 more days even after the deletion of the backup item. This retention protects against accidental deletion or malicious deletion scenarios, allowing the recovery of those backups with no data loss. Azure Backup also provides Enhanced soft delete that enables you to retain a deleted item in the soft deleted state for a longer duration.
* **High availability**: Azure Backup offers three types of replication:
  + **Locally redundant storage (LRS)**: The lowest-cost option with basic protection against server rack and drive failures. We recommend it for noncritical scenarios.
  + **Geo-redundant storage (GRS)**: The intermediate option has failover capabilities in a secondary region. We recommend it for backup scenarios.
  + **Zone-redundant storage (ZRS)**: This option protects against datacenter-level failures by replicating your storage account synchronously across three Azure availability zones. We recommend it for high-availability scenarios.
* **Centralized monitoring and management**: Azure Backup provides built-in monitoring and alerting capabilities in a Recovery Services vault. These capabilities are available without any other management infrastructure.

**Recovery Services vault**

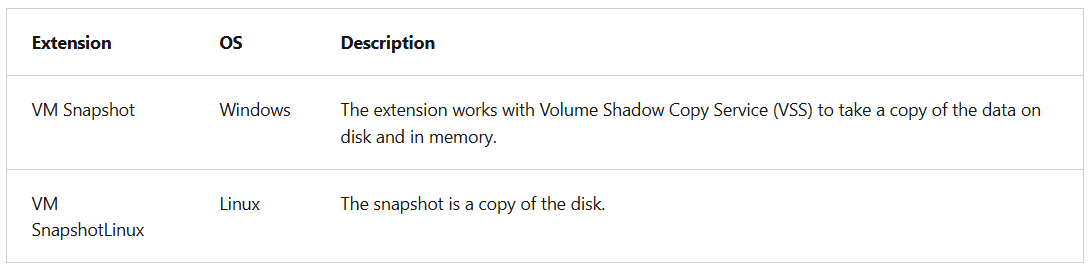
* Azure Backup uses a Recovery Services vault to manage and store the backup data. A vault is a storage-management entity, which provides a simple experience to carry out and monitor backup and restore operations. With Azure Backup, you don't need to worry about deploying or managing storage accounts. In fact, all you need to specify is the vault that you want to back up the virtual machine (VM) to. The backup data is transferred to the Azure Backup storage accounts (in a separate fault domain) in the background. The vault also acts as a role-based access control boundary to allow secure access to the data.

**Backup policy**

* You can define the backup frequency and retention duration for your backups. Currently, the VM backup can be triggered daily or weekly, and can be stored for multiple years. The backup policy supports two access tiers: snapshot tier and the vault tier. By using the Enhanced policy, you can trigger hourly backups.
* **Selective disk backup**: Azure Backup provides Selective Disk backup and restore capability using Enhanced policy. By using this capability, you can selectively back up a subset of the data disks that are attached to your VM. Then, you can restore a subset of the disks that are available in a recovery point, both from instant restore and vault tier. It helps you manage critical data in a subset of the VM disks and use database backup solutions when you want to back up only their OS disk to reduce cost.
* **Snapshot tier**: All the snapshots are stored locally for a maximum period of five days, in what is called the snapshot tier. For all types of operation recoveries, we recommended that you restore from the snapshots because it's faster to do so. This capability is called instant restore.
* **Vault tier**: All snapshots are additionally transferred to the vault for more security and longer retention. At this point, the recovery point type changes to "snapshot and vault."

**Snapshots**

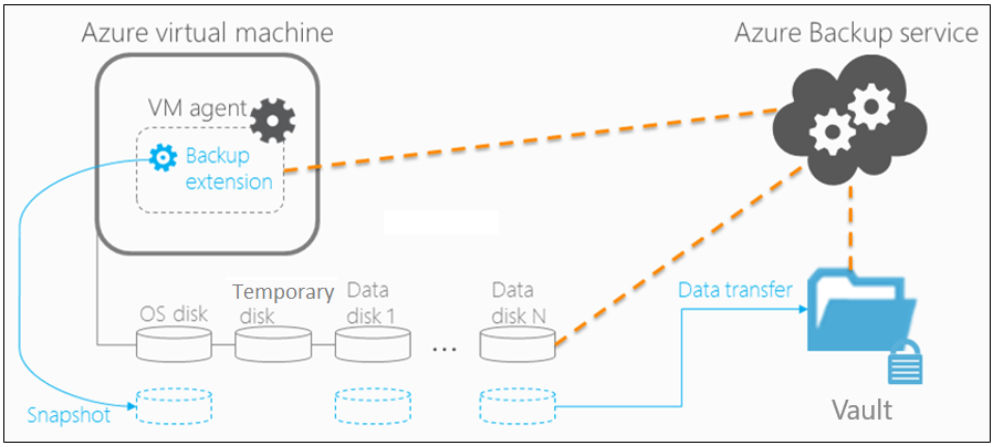
* A snapshot is a point-in-time backup of all disks on the VM. For Azure VMs, Azure Backup uses different extensions for each supporting operating system:



* Depending on how the snapshot is taken and what it includes, you can achieve different levels of consistency:
  + **Application consistent**
    - The snapshot captures the VM as a whole. It uses VSS writers to capture the content of the machine memory and any pending I/O operations.
    - For Linux machines, you need to write custom pre or post scripts per app to capture the application state.
    - You can get complete consistency for the VM and all running applications.
  + **File system consistent**
    - If VSS fails on Windows, or the pre and post scripts fail on Linux, Azure Backup still creates a file-system-consistent snapshot.
    - During a recovery, no corruption occurs within the machine. But installed applications need to do their own cleanup during startup to become consistent.
  + **Crash consistent**
    - This level of consistency typically occurs if the VM is shut down at the time of the backup.
    - No I/O operations or memory contents are captured during this type of backup. This method doesn't guarantee data consistency for the OS or app.

**Backup process for an Azure virtual machine**

* For Azure VMs that are selected for backup, Azure Backup starts a backup job according to the backup frequency you specify in the backup policy.
* During the first backup, a backup extension is installed on the VM, if the VM is running:
  + For Windows VMs, the VM Snapshot extension is installed.
  + For Linux VMs, the VM SnapshotLinux extension is installed.
* After the snapshot is taken, the data is stored locally and transferred to the vault.
  + The backup is optimized by backing up each VM disk in parallel.
  + For each disk that's being backed up, Azure Backup reads the blocks on the disk and identifies and transfers only the data blocks that changed (the delta) since the previous backup.
  + Snapshot data might not be immediately copied to the vault. It might take several hours at peak times. Total backup time for a VM is less than 24 hours for daily backup policies.



You can additionally enable vault encryption with customer-managed keys (CMK). By using Enhanced soft delete for a Recovery Services vault, you can protect backups from deletion. You can also keep Enhanced soft delete always on to prevent turning it off, thus protecting your backups from accidental deletion or from malware attacks.

**Restore virtual machine data**

* Companies that have a business continuity and disaster recovery (BCDR) plan typically schedule test runs to ensure that the business can successfully recover from disasters. Now that you successfully backed up your virtual machines, you want to explore the options available for restoring them as part of your BCDR testing.

**Restore types**

* Azure Backup provides many ways to restore a VM. You can either instantly restore from the snapshot tier (optimal for operational recoveries) or from the vault tier.

**Recover files from a backup**

You can also recover individual files from a recovery point by mounting the snapshot on the target machine using the iSCSI initiator in the machine.

**Restore an encrypted virtual machine**

* Azure Backup supports the backup and restore of machines encrypted through Azure Disk Encryption. Disk Encryption works with Azure Key Vault to manage the relevant secrets that are associated with the encrypted disk. For an extra layer of security, you can use key vault encryption keys (KEKs) to encrypt the secrets before they're written to the key vault.
* Certain limitations apply when you restore encrypted VMs:
  + Azure Backup supports only standalone key encryption. Any key that's part of a certificate isn't currently supported.
  + File-level or folder-level restores aren't supported with encrypted VMs. To restore to that level of granularity, the entire VM has to be restored. You can then manually copy the file or folders.
  + The Replace existing VM option isn't available for encrypted VMs.