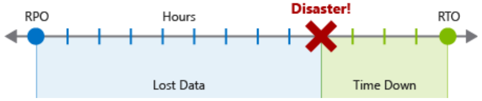
Threats at every security layer

Layer	Threat
Physical	Unauthorized access to facilities / badge theft.
Policies & access	Authentication happens here. Exposed credentials.
Perimeter	DoS attacks
Networking	Unnecessary open ports (SSH, RDP)
VM/Compute	Malware
Application	Code injection (SQL) / cross site scripting (XSS)
Data	Expose encryption key / weak encryption

Recoverability objectives

Objective	Description
Recovery Point Objective (RPO)	Max. duration of acceptable loss, measured in time, not volume, eg.: 30 minutes of data (= time between backups)
Recovery Time Objective (RTO)	Max, duration of acceptable downtime, eg. 8 hours



What is the Zero Trust model?

Never assume trust, continually validate trust, especially with BYOD.

Common security principles (CIA)

Principle	Description
Confidentiality	Principle of least privilege: explicitly grant access to individuals. Eg: passwords, certificates, biometric access control…
Integrity	Prevent unauthorized access to data at rest/in transit: hashing, encryption, digital fingerprinting, …
Availability	Ensure services are available to authorized users (DoS, natural disasters, …)

Azure encryption per service

Service	Encryption
Raw storage	SSE: Storage Service Encryption, for data at rest. Uses AES encryption keys to encrypt before storing and decrypt after retrieving. Blob and Files support Bring Your Own Key
VM's	ADE: Azure Disk Encryption. BitLocker on Windows, DM-Crypt on Linux
Database	TDE: Transparent Data Encryption
Secrets	Key vault
Backups	Uses AES256 to store data at rest

Scale kinds

Kind	Description
Scale up	Add more resources to the instance
Scale down	Remove resources from the instance
Scale out	Add more instances
Scale in	Remove instances

How can you group resources for billing?

- Assign resources to different subscriptions
- Assign resources to different resource groups
- Apply tags to resources

Difference between SLA and SLO

SLO are the Service Level Objectives within an SLA, eg.: the downtime per month.

High Availability (HA) concepts

Concept	Description
Availability set	Spread resources over update and fault domains, to protect against hardware failure and updates, WITHIN a datacenter
Availability zones	Spread resources over zones, in DIFFERENT datacenters, IN a region
Load balancing	Load balancer, application gateway, traffic manager

Azure Site Recovery (ASR) key characteristics

- A ‘process recovery’ service
- Replicates the following to alternate locations
  - VMs on Azure
  - VMs on physical servers
  - Workloads
    - Individual applications
    - VM OS + applications
- Does failover on outages

VPN Gateway high availability scenario’s

Scenario	Description
Active/standby	2 instances: active is live, standby takes over on maintenance/disruptions
Active/active	BGP, 2 instances, 2 public ip’s, 2 tunnels, 2 on-prem VPN’s
ExpressRoute failover	Use VPN gateway over the internet as fallback for ExpressRoute gateway
Zone redundant gateways	In supported regions

Which IP address ranges are for internal networks and won’t be routed over the internet?

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.1 to 192.168.255.255

ExpressRoute peering types

Peering	Description
Azure private peering	Connect to Azure VM’s and Cloud services on their private IP
Microsoft peering	Connect to Microsoft online services: Office 365, Dynamics 365, Azure PaaS. Needs public IP, owned by you or your connectivity provider

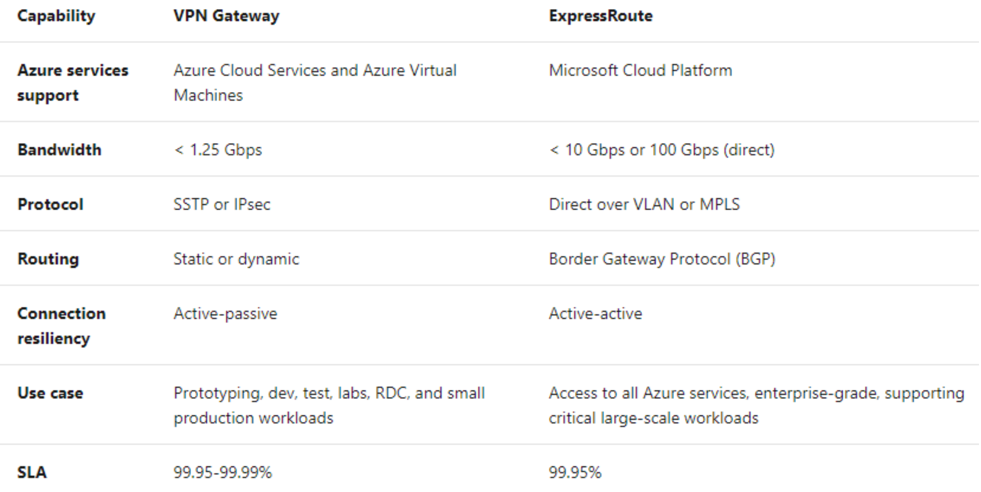
ExpressRoute components

Compontent	Description
On-premises network	Local AD-managed network
Local edge routers	Connect on premise network to the connectivity provider’s circuit
ExpressRoute circuit	Layer 3 circuit, supplied by connectivity provider. Links Azure edge routes and on premised edge router.
Microsoft edge routes	Cloud side connection between on premise network and the cloud. Always 2 (active-active)
Azure VNet	Segments your network, subnets and assets into tiers.

VNet peering

- You can peer over subscriptions
- You can peer over regions with Global VNet Peering

Hybrid networking comparison



Capability	VPN Gateway	ExpressRoute
Azure services support	Azure Cloud Services and Azure Virtual Machines	Microsoft Cloud Platform
Bandwidth	< 1.25 Gbps	< 10 Gbps or 100 Gbps (direct)
Protocol	SSTP or IPsec	Direct over VLAN or MPLS
Routing	Static or dynamic	Border Gateway Protocol (BGP)
Connection resiliency	Active-passive	Active-active
Use case	Prototyping, dev, test, labs, RDC, and small production workloads	Access to all Azure services, enterprise-grade, supporting critical large-scale workloads
SLA	99.95-99.99%	99.95%

Storage replication comparison

- LRS: single datacenter, 3 sync, copies
- ZRS: single zone, 3 sync. copies
- GRS: across zones, 3 sync. copies local + 3 in another region
- RA-GRS: same as GRS, but with read access in the other region

Network Watcher monitoring tools

Tool	Use to
Topology	Graphical display of the VNNet, resources, interconnections, …
Connection Monitor	Check that connections work between resources, eg: check if 2 VMs can communicate. Monitor communication between a VM and an endpoint
Network Performance Monitor	Track latency and packet drops.

Network Watcher diagnostic tools

Tool	Use to
IP flow verify	Tells if packets are allowed or denied for a specific VM (via NSG).
Next hop	Check the hops a packet travels by (from VM to destination).
Security group view	Show all effective NSG rules.
Packet capture	Record all packets from and to a VM.
Connection troubleshoot	Check TCP connectivity between source and destination VM.
VPN troubleshoot	Diagnose VPN gateway connection problems.

What would be a reason to use a Premium SSD instead of Standard SSD or Standard HDD?

Standard tiers don’t guarantee a minimum throughput.

What makes containers different from VMs?

- Doesn’t use virtualization
- Usually more lightweight
- Can run multiple isolated instances in a single container host
- Runs on top of a host OS, no OS in the container itself

Ways to manage containers?

- ACI: Azure Container Instances: PaaS, fast and simple, no VM management or additional configuration, just deploy

AKS: Azure Kubernetes Service: complete orchestration service for multiple containers with distributed architectures

Compute provisioning options

Option	Description
Custom scripts	Custom script extension downloads and runs script on VMs. Use for post deployment config, SW installation, tasks, …
DSC extensions	Desired State Configuration extensions. Run a script for more complex installation procedures, like reboots. DSC configurations are managed and deployed by Azure automation state configuration service.
Chef	A Chef server is hosted for you to run as a service, and can automate deployment of 10.000 machines at a time. Uses knife commands.
Terraform	Open source Infrastructure-as-code tool. Create infrastructures with HCL (Hashicorp Configuration Language) or JSON. Create script templates that work across providers (Azure, AWS, …)
Resource manager templates	JSON files that define resources to provision.

WebJobs vs Azure Functions

- WebJobs:
  - Can be part of App Service application
  - Provides control of JobHost
  - NuGet with WebJobs SDK
- Functions:
  - Auto scaling
  - Pay per use
  - Logic Apps integration
  - Test in browser
  - NuGet, NPM

HPC (High Performance Computing) options

Option	Description
Azure Batch	Managed service, automates tasks from storage across multiple auto-provisioned VMs to do parallel and intensive work. Supports rendering 3D packages and licenses. Visualize batch jobs with Batch Explorer. Doesn't support Basic A series VMs. Supports low priority nodes: VMs from a shared Azure pool, can become exhausted
VM series	HB: extreme memory HC: extreme computation NC: extreme graphics ND: extreme graphics, AI, deep learning
Microsoft HPC Pack	A series of Windows installers, for management and scheduling of on premise and cloud VM nodes and clusters. Hybrid: extends to the cloud when on prem resources don't suffice. Windows Server 20212 or later for the head node.

Resource governance options

Option	Description
Policy	A default-allow-and-explicity-deny system. Focuses on resource properties during deployment, like allowed SKU's and locations of resources.
Initiative	A set of policies.
Management Group	Containers for managing access, policies and compliance across MULTIPLE SUBSCRIPTIONS.
Blueprints	Defines a repeatable set of Azure resources that follows an organization's standards and patterns. To quickly set up new environments that comply with the organization. Handles: role assignments, policy assignments, resource manager templates, resource groups, … Can also fit in DevOps

Compliance and government sources

Source	Description
Microsoft Privacy Statement	What personal data Microsoft processes, how, and for what purpose.
Microsoft Trust Center	Details about how Microsoft implements and supports - Security - Privacy - Compliance - Transparency Trusted Cloud Initiative
Service Trust Portal (STP)	Contains audit reports. Guides to help your organization comply with standards and laws: - ISO - SOC - NIST - FedRAMP - GDPR Hosts Compliance Manager service: workflow based risk assessment dashboard to verify your organization's compliance.

Monitoring options

Option	Description
Azure Security Center	Manages infrastructure security from a centralized location. Monitors security of your workloads, on prem and in the cloud. Security threats. Security configuration.
Azure Application Insights	Monitor / manage application performance. Performance counters. Errors. Database query tracing.
Azure Monitor	Collecting, combining, analyzing data from different sources. Can see all Application Insights log data. Also used by Security Center, for VM security data etc.
Azure Sentinel	Collects data on devices, users, infra, apps, across your enterprise. Built in threat detection / investigation. Hunt for threats / anomalies. Connects to data sources like Office 365, Azure Advanced Threat Protection, AWS CloudTrail or on prem sources.

SQL Elastic Pool purchasing models

Model	Description
DTU-based	Simple. DTU = bundle of compute, storage, IO Tiers: Basic, Standard or Premium
vCore	Virtual Core. Choose between generations of hardware, number of cores, memory size, storage size, … Can be translated to your on premise workload Tiers: General Purpose, Business Critical.

What is a Cosmos DB Request Unit (RU)?

The approximate cost of 1 GET request on 1 1-KB document, using a document's ID.

Cosmos DB conflict resolution modes in multi-master

- Last-Writer-Wins (default)
- Custom: user defined function
- Custom: async: moved to conflicts feed for app to resolve asynchronously

Difference between event and message

Event	Message
Lightweight notification, contains reference to data (like an id).	Often contains the data itself.
Broadcast scenario: sender = publisher, receiver = subscriber	
No expectation of how it is handled	Expectation of what will happen with the message (eg: a user will be deleted)

Message deliver guarantees in queue systems

Guarantee	Description
At-Least-Once Delivery	- Each message delivered to at least one of the retrievers - If multiple retrieve instances, same message may be retrieved twice if processing takes a long time
At-Most-Once Delivery	- No chance for twice retrieval - Small chance that it doesn't arrive - Also called automatic duplicate detection
First-In-First-Out (FIFO)	- Guarantees ordered processing

Queue service comparison

Queue service	Description
Service Bus Topics	- Multiple receivers for each message
Service Bus Queues	- Supports At-Most-Once delivery guarantee - Supports FIFO guarantee - Supports transactions - Receive without polling - RBAC - Messages > 64 KB and < 256 KB - Queue size <= 80 GB - Batch publish/consume
Queue Storage	- Audit trail of all messages - Supports queues > 80 GB - Track progress for processing a message inside of the queue

API Management features

- (Auto generated) documentation
- Rate limiting
- Health monitoring
- Modern formats (JSON)
- Multiple API's in 1 management
- Analytics
- Security (OAuth 2.0, AD)
- Policies
  - Inbound (on request receive)
  - Backend (before forward to managed API)
  - Outbound (before response to client)
  - On-Error (on exception raise)

Difference between Site Recovery and Azure Backup

ASR	Azure Backup
Replicates VM workloads to secondary locations for failover on disaster that affects a whole site.	More granular recover, eg: VM disks or accidentally deleted files/folders.
Keep data in ASR vault as long as you like	Can backup to ASR vault for long retention
Low RPO	Longer/variable RPO
Shorter RTO	Longer RTO up to days

Why use MABS or DPM instead of MARS?

When backup of running apps is required

Why use Azure Front Door instead of Traffic Manager?

- Front Door is a global load balancer, like traffic manager, but works at layer 7
- Supports (only) HTTP(S) protocols to route and filter
    - Eg: filter on browser country code
    - Traffic manager uses DNS
- Supports TLS protocol termination
- Also uses health probes

Azure SQL Database multi-region implementations

Implementation	Description
Active geo-replication	- Auto replicates (ASYNC) db to another READ ONLY db in another region - DOESN'T SUPPORT by managed SQL Database instances
Auto failover groups	- Group of db's - Auto replicates (ASYNC) from primary to one or more secondary servers - Like geo-replication, but supports policies (region selection, make writable, …) - SUPPORTS managed SQL Database instances

AzCopy command line copy directions

From	To
Local	Azure Blob
Local	Azure Table
Local	Azure Files (share/directory)
Local	ADLS Gen 2
Azure Blob	Azure Blob
Azure Blob	Azure Files
Azure Files	Azure Files
Azure Files	Azure Blob
AWS S3	Azure Block Blob

What is Azure StorSimple?

- Hybrid cloud storage solution
- For large quantities of data
- Backups, snapshots, offsite storage, …
- SSD / HDD storage arrays -> better performance
- Needs Azure storage account

Difference between VM managed and unmanaged disk

Managed disk	Unmanaged disk
Storage is auto managed in ARM	You create storage account to hold the VHD
Must pick a size from list, can be resized.	Choose disk size during provisioning
Predictable performance	Performance can be impacted by storage account performance (except for premium disks)
If VM is in an availability set, disks are spread over fault domains	No guarantee of disk spreading
LRS	LRS, **GRS**
Availability zone support	
RBAC	

Azure AD identity providers

Provider	Description
B2C	- Allows sign-in with Microsoft, personal and social accounts, MFA - You are my customer and you may use my customer facing applications - Separate Azure AD B2C instance
B2B	- To share files/resources with other companies/partners, set up in Azure AD - I want to collaborate with you on my organization's applications and services - Uses the organization's Azure AD instance
v1.0 endpoint	- Sign in with work or school accounts, accounts managed in Azure AD
v2.0 endpoint	- Sign in with work, school and personal accounts, accounts managed in Azure AD

What is SQL Database LTR?

Long Term Retention for backups: stores full db backups in RA-GRS blob storage for up to 10 years. Auto db backups only support between 7-35 days retention.

Only for **Azure SQL Database (single or pooled instance)**, NOT for Managed Instance.

Use SQL Agents jobs to schedule backups beyond 35 days.

Which special service options can be enabled under Key Vault Access Policies?

- Enable access to **Azure Virtual Machines** for deployment
- Enable access to **Azure Resource Manager** for template deployment
- Enable access to **Azure Disk Encryption** for volume encryption

Different SQL type options

Option	**Description**
SQL database	- Fully managed, latest stable SQL Server features - Deployment options: - Single database - Elastic pool - Database server: group of databases and/or elastic pools
SQL managed instance	- Supports on prem migration with little or no change - Lift-and-shift ready - More capabilities than SQL database, like VNET and near 100% compatibility with on prem SQL Server
SQL virtual machines	- For migrations that require OS level access - Lift-and-shift ready - Full administrative control

Data migration options

Option	**Description**
AzCopy	Copy between storage accounts (also from local)
Data Migration Assistant	Migrate between different versions of SQL Server. Used by Azure Database Migration Service, supports stay-online migration to Premium plan Azure SQL database
Cosmos DB Data Migration Tool	Import from various sources (SQL Server, JSON, CSV, Mongo, Table Storage, Amazon, Cosmos SQL) to Cosmos DB
Azure Data Factory	To scale out a transfer operation. Orchestration and monitoring. To set up a cloud pipeline between on prem or on azure transfers.

Difference between Application Insights and Log Analytics

Application Insights	**Analytics**
- Data related to code-level - Application performance level - Page views - HTTP requests - Exceptions via **CodeLens** - Stack traces - Full app topology via **Composite Application Map** - **Retention analysis** for web applications: see how many users return to the web app, how often the perform tasks, …	- Data related to infrastructure - Network - Sys**log** - IIS log - Custom logs - Windows logs - **Performance** counters - **Resource** usage

Difference between Diagnostics agent (extension) and Log Analytics agent

Diagnostics agent	**Analytics agent**
- Collects diagnostics on a deployed application, **in Azure** - Perf counters, application logs, windows event logs, **IIS** logs, crash dumps, … - On Web / Worker roles, VMs, VM scale sets, Service Fabric - **Log to Azure storage**	- Monitors **Windows and Linux** VMs in any cloud, also **on prem** - Attached to Azure monitor - Indefinite retention - **Log to Analytics workspace**

AD membership types

- Assigned: principal directly added to group
- Dynamic: based on attribute queries (eg: jobtitle starts with…)
    - Evaluated periodically, not realtime

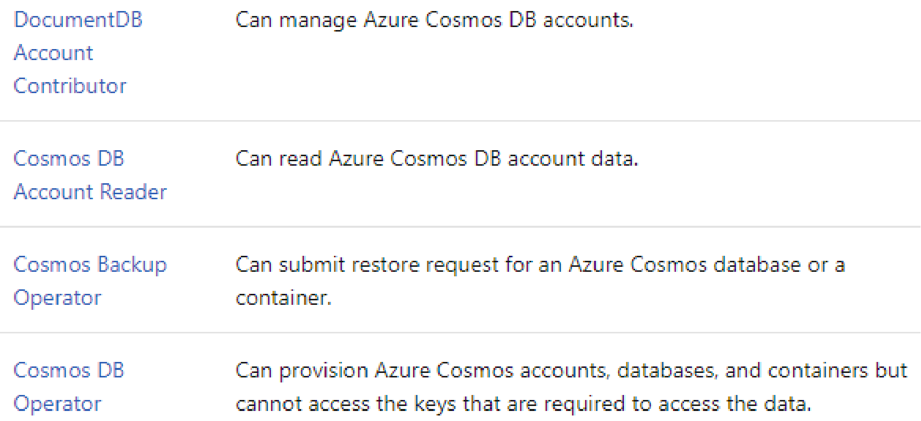
AD group types

- Security
    - Contains users and devices
    - Is a security principal
- Office 365
    - Contains only users
    - Is not a security principal
    - Can be mail-enabled, used in many ways in Office 365

Availability set SLA vs Availability zone SLA

- AS: 99.95%
- AZ: 99.99%

Cosmos DB built-in roles

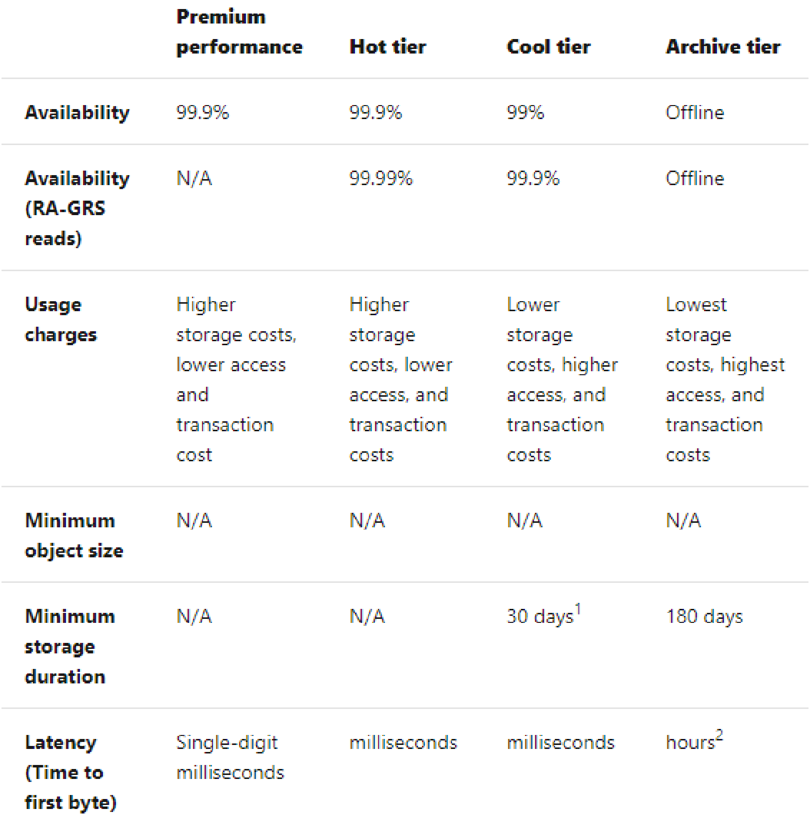


DocumentDB Account Contributor	Can manage Azure Cosmos DB accounts.
Cosmos DB Account Reader	Can read Azure Cosmos DB account data.
Cosmos Backup Operator	Can submit restore request for an Azure Cosmos database or a container.
Cosmos DB Operator	Can provision Azure Cosmos accounts, databases, and containers but cannot access the keys that are required to access the data.

Fault domain / update domain numbers for Availability Sets

- Fault domains: default 2, max 3
- Update domains: default 5, max 20

Block Storage options



	Premium performance	Hot tier	Cool tier	Archive tier
Availability	99.9%	99.9%	99%	Offline
Availability (RA-GRS reads)	N/A	99.99%	99.9%	Offline
Usage charges	Higher storage costs, lower access and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
Minimum object size	N/A	N/A	N/A	N/A
Minimum storage duration	N/A	N/A	30 days[1]	180 days
Latency (Time to first byte)	Single-digit milliseconds	milliseconds	milliseconds	hours[2]

Data Protection Options

Option	Use for
Data Protection Manager (DPM)	Backup from many sources to on prem storage or Azure. For bare metal recovery.
MARS agent	Data backup to Azure Backup Vault, NOT for bare metal recovery
Site Recovery Provider	Replicates VMs instead of making backups
Data Explorer	View telemetry data in Azure

Data Protection Manager (DPM)

You can deploy System Center Data Protection Manager (DPM) for:

- **Application-aware backup**: Application-aware back up of Microsoft workloads, including SQL Server, Exchange, and SharePoint.
- **File backup**: Back up files, folders and volumes for computers running Windows server and Windows client operating systems.
- **System backup**: Back up system state or run full, bare-metal backups of physical computers running Windows server or Windows client operating systems.
- **Hyper-V backup**: Back up Hyper-V virtual machines (VM) running Windows or Linux. You can back up an entire VM, or run application-aware backups of Microsoft workloads on Hyper-V VMs running Windows.
- Get a full list in What can DPM back up?

DPM can store backup data to:

- **Disk**: For short-term storage DPM backs up data to disk pools.
- **Azure**: For both short-term and long-term storage off-premises, DPM data stored in disk pools can be backed up to the Microsoft Azure cloud using the Azure Backup service.
- **Tape**: For long-term storage you can back up data to tape, which can then be stored offsite.

Burstable VM series

The VM B-series are burstable. Low-cost, can scale up on heavy workload and scale back down.

Azure AD Identity Protection

Identity Protection is a tool that allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

Identity Protection uses the learnings Microsoft has acquired from their position in organizations with Azure AD, the consumer space with Microsoft Accounts, and in gaming with Xbox to protect your users. Microsoft analyses 6.5 trillion signals per day to identify and protect customers from threats.

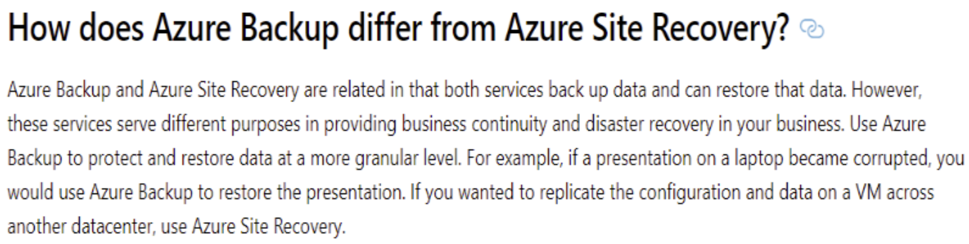
The signals generated by and fed to Identity Protection, can be further fed into tools like Conditional Access to make access decisions, or fed back to a security information and event management (SIEM) tool for further investigation based on your organization's enforced policies.

Elastic pool limits for DTU pricing model

- Basic: 1600 DTU
- Standard: 3000 DTU, columnstore indexes
- Premium: 4000 DTU, in memory OLTP, columnstore indexes

Data Factory setup

- Create a data factory
- Create an integration runtime for copying the data
- Create linked services to identify source and destination
- Create source and destination datasets
- Create a pipeline



How does Azure Backup differ from Azure Site Recovery?

Azure Backup and Azure Site Recovery are related in that both services back up data and can restore that data. However, these services serve different purposes in providing business continuity and disaster recovery in your business. Use Azure Backup to protect and restore data at a more granular level. For example, if a presentation on a laptop became corrupted, you would use Azure Backup to restore the presentation. If you wanted to replicate the configuration and data on a VM across another datacenter, use Azure Site Recovery.

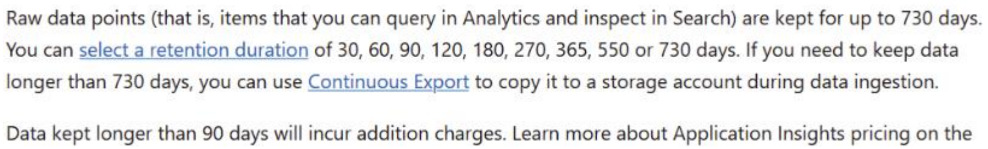
What can AD Connect Health monitor?f

- AD Connect
  - Sync errors
  - Sync services
- AD Federation Services
- AD Domain Services
- Also supports monitoring AD FS / web application proxy servers

API Management VNet access types

- Off: default, API Management not deployed into a VNet
- External: API Management gateway and dev portal accessible from the internet, via external load balancer
- Internal: API Management gateway and dev portal accessible from within the VNet only, via internal load balancer

How long can SQL metrics (SQLInsight, AutomaticTuning) data be kept in Log Analytics?



Raw data points (that is, items that you can query in Analytics and inspect in Search) are kept for up to 730 days. You can select a retention duration of 30, 60, 90, 120, 180, 270, 365, 550 or 730 days. If you need to keep data longer than 730 days, you can use Continuous Export to copy it to a storage account during data ingestion.

Data kept longer than 90 days will incur addition charges. Learn more about Application Insights pricing on the

Recommended caching policies for VMs hosting SQL Server

- Data disk: ReadOnly caching
- Log disk: None