**Scalability and performance**

* Azure Load balancer will provide the same network layer 4 capabilities as the AWS Network Load Balancer and Classic Load Balancer, allowing you to distribute traffic for multiple VMs at the network level. It also provides a failover capability.
* [Application Gateway](https://learn.microsoft.com/en-us/azure/application-gateway/overview) Offers application-level rule-based routing comparable to the AWS Application Load Balancer.
* Azure virtual machine scale sets let you deploy and manage identical sets of VMs therefore letting you keep the VMs you need to improve performance and reduce traffic . The App Service autoscale lets you autoscale Azure App Service applications

**Reliability and Availability**

* To protect against localized hardware failures, such as a disk or network switch failing, deploy two or more VMs in an availability set. An availability set consists of two or more fault domains that share a common power source and network switch. VMs in an availability set are distributed across the fault domains, so if a hardware failure affects one fault domain, network traffic can still be routed to the VMs in the other fault domains.
* Each Azure Availability Zone has a distinct power source, network, and cooling system. Deploying VMs across availability zones helps to protect an application against datacenter-wide failures.

**Security and Compliance**

* The Service Bus avoid using the default access control and instead uses SAS tokens with limited permissions to increase security
* Due to limited access to Service Bus resources using Network Security Groups and Network Services endpoints enables network security
* Azure uses a combination of multi-factor authentication (MFA) and conditional access (CA) policies enable enhanced security for common authentication.
* To limit and control access for your highest privileged accounts in Microsoft Entra ID, [Privileged Identity Management (PIM)](https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management) can be enabled to provide just-in-time access to services for Azure cloud services. Once deployed, PIM can be used to control and limit access using the assignment model for roles, eliminate persistent access for these privileged accounts, and provide additional discover and monitoring of users with these account types.
* Azure uses role-based access to control(RBAC) to restrict permissions to authorized users.
* Azure Key Vault allows you to manage digital certificates and automate tasks related to the renewal and rollover of SSL/TLS certificates used in your applications.
* Azure Key Vault provides logging and auditing capabilities, allowing you to monitor access and actions taken on your keys and secrets. This is essential for compliance and security monitoring.

**Data Storage and Management**

* Azure uses subscription-bound [storage accounts](https://learn.microsoft.com/en-us/azure/storage/common/storage-quickstart-create-account) which allows you to create and manage the following storage services:
* [Blob storage](https://learn.microsoft.com/en-us/azure/storage/common/storage-quickstart-create-account) stores any type of text or binary data, such as a document, media file, or application installer. You can set Blob storage for private access or share contents publicly to the Internet. Blob storage serves the same purpose as both AWS S3 and EBS.
* [Table storage](https://learn.microsoft.com/en-us/azure/cosmos-db/table-storage-how-to-use-nodejs) stores structured datasets. Table storage is a NoSQL key-attribute data store that allows for rapid development and fast access to large quantities of data. Similar to AWS' SimpleDB and DynamoDB services.
* [Queue storage](https://learn.microsoft.com/en-us/azure/storage/queues/storage-quickstart-queues-nodejs?tabs=passwordless%2Croles-azure-portal%2Cenvironment-variable-windows%2Csign-in-azure-cli) provides messaging for workflow processing and for communication between components of cloud services.
* [File storage](https://learn.microsoft.com/en-us/azure/storage/files/storage-java-how-to-use-file-storage) offers shared storage for legacy applications using the standard server message block (SMB) protocol. File storage is used in a similar manner to EFS in the AWS platform.

**Integration Capabilities**

* Azure Key Vault seamlessly integrates with various Azure services and resources, making it easy to protect your application secrets and keys used in Azure VMs, Azure Functions, Azure App Service, Azure SQL Database, and more.
* Azure Bastion is integrated with the Azure Portal, making it easy to connect to your VMs without leaving the Azure environment.
* Azure Service Bus (messaging service) allows you to build asynchronous and reliable communication between applications.

**Cost and Pricing Model**

* Azure Reservations enables you to [scope your reservations](https://learn.microsoft.com/en-us/azure/cost-management-billing/reservations/prepare-buy-reservation#scope-reservations) to apply to a resource group, a subscription, or a set of subscriptions. This means that you can take advantage of reservations, even if you shard your workload across multiple subscriptions.
* **Azure savings plan for compute:** Azure savings plan for compute is a flexible cost-saving plan that generates significant savings over pay-as-you-go prices. You agree to a one-year or three-year contract and receive discounts on eligible compute services.

**Management and Monitoring**

* Azure Monitor stores metrics and logs in a central location called a [Log Analytics workspace](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview). This data is processed and analyzed to provide insights and alerts.
* Azure Monitor collects, indexes, and stores the data your AKS cluster generates. You can configure Container Insights to monitor managed Kubernetes clusters hosted on AKS and other cluster configurations. Container Insights can monitor AKS health and performance with visualization tailored to Kubernetes environments. Similar to EKS, enabling Container Insights for your AKS cluster deploys a containerized version of the Log Analytics agent, which is responsible for sending data to your Log Analytics workspace.
* Azure uses Automation runbook and hybrid runbook worker to automate processes. Automation account is needed to automates configuration and management across your Azure and non-Azure environments.
* Azure Key Vault provides logging and auditing capabilities, allowing you to monitor access and actions taken on your keys and secrets. This is essential for compliance and security monitoring.

**Service-Level Agreements (SLAs)**

* Azure Uptime SLA guarantees 99.95% availability of the Kubernetes API server endpoint for clusters that use Availability Zones and 99.9% of availability for clusters that don't use Availability Zones
* Azure Support Standard plan includes guaranteed initial response times of within one hour for critical cases. The Azure Support Professional Direct plan offers even faster response times and dedicated support resources.
* Microsoft provides a financially-backed 24/7 service availability SLA for Azure support, and if they fail to meet the response time SLAs.