# Azure, AWS & Google Cloud

## A Comprehensive Comparative Guide

Version 26.03  |  March 2026

**Ahmed Abdelwahed**

Technical Trainer | Cloud & Infrastructure Specialist

| ✉ Email | 🌐 Blog | 🗂 LinkedIn |
|---|---|---|
| ahmed@abdelwahed.me | www.abdelwahed.me | linkedin.com/in/ahmedmct |

# Contents

# 1. Global Infrastructure and Reach

| **Microsoft Azure**<br>Azure Regions & Availability Zones | **Amazon AWS**<br>AWS Regions & AZs | **Google Cloud**<br>GCP Regions & Zones |
|---|---|---|

Cloud providers have invested heavily in global infrastructure to minimize latency, ensure compliance with data residency regulations, and deliver high availability. As of 2026, all three platforms continue to expand their footprints at a rapid pace.

## Microsoft Azure

### Regions and Availability Zones

- Azure operates in 60+ regions worldwide — the broadest geographic coverage of any cloud provider.
- Each region contains multiple Availability Zones (AZs): physically separate data centers with independent power, cooling, and networking.
- Azure added 10 new regions between 2024–2026, including expansions in Southeast Asia, Africa, and the Middle East.
- Azure Government and Azure China are sovereign cloud offerings for regulated workloads in the US and China respectively.

### Backbone Network

- Azure's private, global fiber-optic backbone connects all regions with high-bandwidth, low-latency links.
- ExpressRoute provides dedicated private connectivity (up to 100 Gbps) bypassing the public internet.
- Azure Virtual WAN unifies VPN, ExpressRoute, and SD-WAN connectivity into a single managed fabric.

### New in 2025–2026

- Azure Orbital Ground Station expanded to 10 global sites, enabling direct satellite data ingestion.
- Availability Zone support extended to 40+ additional services including Azure SQL Managed Instance and Azure Cache for Redis.
- Azure confidential computing nodes (DCsv3/DCdsv3) now available in 15 regions.

## Amazon AWS

### Regions and Availability Zones

- AWS operates in 34 geographic regions with 108 Availability Zones as of early 2026.
- AWS Local Zones extend infrastructure to metro areas (50+ locations) for ultra-low latency applications.
- AWS Wavelength embeds compute within telco networks for 5G edge scenarios.

- AWS GovCloud (US-East and US-West) serves US federal, state, and local government workloads.

## Global Network

- AWS operates 600+ Points of Presence globally, powering CloudFront CDN and Route 53 DNS.
- AWS Direct Connect provides dedicated 1–100 Gbps connections from customer premises to AWS.
- AWS Transit Gateway enables hub-and-spoke networking across hundreds of VPCs and accounts.

## New in 2025–2026

- AWS launched 4 new regions: Malaysia, Thailand, New Zealand, and the Kingdom of Saudi Arabia.
- AWS Outposts expanded with Outposts Servers — smaller 1U/2U form factors for space-constrained edge deployments.
- AWS Dedicated Local Zones for single-tenant, on-premises-adjacent infrastructure are now generally available.

# Google Cloud

## Regions and Zones

- Google Cloud operates in 40+ regions with 120+ availability zones as of 2026.
- Google's software-defined networking (Andromeda) provides global VPCs that span regions natively.
- Cloud CDN and Media CDN leverage 2,600+ edge PoPs globally for content delivery.

## Private Fiber Network

- Google owns and operates one of the world's largest private submarine cable networks (Dunant, Grace Hopper, Firmina, and others).
- Global load balancing is built into the network fabric — traffic is routed to the nearest healthy backend automatically.
- Cloud Interconnect (Dedicated and Partner) provides 10–100 Gbps private connectivity.

## New in 2025–2026

- Google Cloud expanded to 5 new regions: Malaysia, Thailand, Mexico, Greece, and Norway.
- Distributed Cloud Edge now supports air-gapped sovereign deployments for governments and critical infrastructure.
- Cross-Cloud Network (formerly Network Connectivity Center) now supports direct interconnects to Azure and AWS.

# Infrastructure Comparison at a Glance

| Category | Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|---|
| **Regions (2026)** | 70+ | 34 | 40+ |
| **Availability Zones** | Multiple per region | 108 total | 120+ zones |
| **Edge/Local Zones** | Azure Edge Zones | 50+ Local Zones + Wavelength | Distributed Cloud Edge |
| **Private Backbone** | Global fiber + VWAN | AWS Global Backbone (600+ PoPs) | Andromeda SDN + private cables |
| **Dedicated Connectivity** | ExpressRoute (up to 100Gbps) | Direct Connect (up to 100Gbps) | Cloud Interconnect (up to 100Gbps) |
| **Sovereign Cloud** | Azure Government / China | GovCloud US-East & West | Distributed Cloud Air-Gapped |
| **On-premises Extension** | Azure Stack HCI / Arc | Outposts / Local Zones | Distributed Cloud / Anthos |

## 2. Identity and Access Management

| Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|
| Microsoft Entra ID | AWS IAM & IAM Identity Center | Google Cloud IAM |

Identity is the new perimeter. All three providers have significantly matured their IAM offerings, with Zero Trust architecture, AI-driven risk detection, and workload identity federation becoming standard capabilities in 2025–2026.

## Microsoft Azure — Microsoft Entra ID

- **Entra ID (formerly Azure AD):** Cloud-native identity platform supporting SSO, MFA, Conditional Access, SSPR, and passwordless authentication.
- **External Identities:** Entra B2B (guest collaboration) and B2C (customer identity) allow secure external access without provisioning internal accounts.
- **Privileged Identity Management (PIM):** Just-in-time privileged access with approval workflows, time-bound roles, and access reviews. Reduces standing privileged access.
- **Conditional Access:** Policy engine that grants/denies access based on user, device, location, application, and real-time risk signals.
- **Microsoft Entra Workload ID:** Manages identities for apps, service principals, and managed identities — critical for securing DevOps pipelines and service-to-service calls.
- **Entra Verified ID:** Decentralized identity (DID) standard for verifiable credentials — enables passwordless onboarding for employees and partners.
- **New 2025–2026:** Entra Internet Access and Entra Private Access (formerly Global Secure Access) provide ZTNA/SWG capabilities natively integrated with identity.

## Amazon AWS — IAM & IAM Identity Center

- **AWS IAM:** Foundation service for managing users, groups, roles, and policies. Supports identity-based and resource-based policies.
- **IAM Identity Center:** Centralized SSO portal for AWS accounts and SAML 2.0 applications. Replaces the legacy SSO service with enhanced attribute-based access control (ABAC).
- **IAM Roles Anywhere:** Extends IAM roles to on-premises servers, containers, and CI/CD systems using X.509 certificates — eliminates long-lived credentials.
- **Permission Boundaries:** Set maximum permissions for IAM entities, enabling safe delegation without privilege escalation.
- **IAM Access Analyzer:** Continuously scans policies for overly permissive access, generates least-privilege refinements using ML, and validates CloudFormation/CDK templates.
- **Service Control Policies (SCPs):** Organization-level guardrails applied across all member accounts — prevents even root users from exceeding defined boundaries.
- **New 2025–2026:** AWS Resource Control Policies (RCPs) added as a new policy type — controls permissions from the resource side across accounts.

## Google Cloud — Cloud IAM

- **Cloud IAM:** Unified access control with fine-grained roles at organization, folder, project, and resource levels. Supports hierarchical policy inheritance.
- **Service Accounts & Workload Identity Federation:** Enables GKE pods, CI/CD systems, and on-premises workloads to authenticate using short-lived tokens without service account keys.
- **IAP (Identity-Aware Proxy):** Application-layer access control that enforces identity and context policies before requests reach your backend — core Zero Trust component.
- **VPC Service Controls:** Creates security perimeters around APIs and data — prevents data exfiltration even by authorized users.
- **Access Context Manager:** Defines fine-grained, attribute-based access levels (device, network, identity) used by IAP and VPC Service Controls.
- **Policy Intelligence:** AI-powered tools: Policy Analyzer, Policy Troubleshooter, Policy Simulator, and Recommender — continuously optimizes IAM posture.
- **New 2025–2026:** Principal Access Boundary policies restrict what resources any principal can access, regardless of which IAM roles are granted.

## IAM Comparison at a Glance

| Category | Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|---|
| **Core Service** | Microsoft Entra ID | AWS IAM + IAM Identity Center | Google Cloud IAM |
| **SSO/Federation** | Entra SSO (SAML, OIDC, WS-Fed) | IAM Identity Center (SAML 2.0) | Cloud Identity / Workforce Identity Federation |
| **MFA / Passwordless** | Entra MFA, FIDO2, Authenticator App | Virtual MFA, Hardware MFA, Passkeys | TOTP, Security Keys, Google Authenticator |
| **Privileged Access Mgmt** | PIM (just-in-time + approval) | IAM Access Analyzer + Permission Boundaries | Privileged Access Manager (PAM) - Preview |
| **Machine Identity** | Managed Identity / Workload ID | IAM Roles Anywhere / EC2 Instance Profiles | Workload Identity Federation / Service Accounts |
| **Policy Analysis / AI** | Entra Identity Protection (ML risk) | IAM Access Analyzer ML Refinements | Policy Intelligence Suite |
| **Zero Trust Network** | Entra Internet/Private Access (ZTNA) | AWS Verified Access | BeyondCorp Enterprise / IAP |

# 3. Virtual Machines

| Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|
| Azure Virtual Machines | Amazon EC2 | Google Compute Engine |

## Microsoft Azure — Virtual Machines

- **VM Families (2026):** D-series (general purpose), E-series (memory optimized), F-series (compute optimized), L-series (storage optimized), N-series (GPU), M-series (SAP HANA scale-up).
- **Spot VMs:** Up to 90% discount for fault-tolerant workloads with capacity-based eviction notices.
- **Confidential VMs:** AMD SEV-SNP and Intel TDX-based VMs (DCasv5/ECasv5) provide hardware-enforced memory encryption and attestation.
- **Azure Boost:** Purpose-built host infrastructure offloads networking, storage, and security processing from the hypervisor to dedicated hardware — improving VM performance by up to 200%.
- **Hibernate & Restore:** GA in 2025 — VMs can be hibernated to disk and restored in seconds, reducing costs for dev/test workloads.
- **VM Scale Sets (Flex):** Flexible orchestration mode enables mixing VM sizes and combining on-demand/spot within a single scale set.

## Amazon AWS — EC2

- **Instance Families (2026):** General (M7, T4g), Compute (C7g Graviton3), Memory (R8g), Storage (I4i), Accelerated (P5/Trn2/Inf2), HPC (Hpc7a).
- **Graviton Processors:** AWS Graviton4 (ARM-based) offers up to 30% better compute performance and 40% better price-performance than comparable x86 instances.
- **Spot Instances:** Up to 90% savings; EC2 Auto Scaling and Spot Fleet manage mixed On-Demand/Spot pools with automatic failover.
- **EC2 Nitro System:** Custom silicon offloads hypervisor functions to dedicated hardware for near bare-metal performance.
- **EC2 Capacity Blocks for ML:** Reserve GPU capacity (P5/Trn2) in blocks of 1–14 days for AI/ML training — generally available in 2025.
- **Dedicated Hosts / Bare Metal:** Full physical server access for BYOL, licensing compliance, or hardware-level isolation.

# Google Cloud — Compute Engine

- **Machine Series (2026):** General (N4, E2), Compute (C3D/C4 with Intel Emerald Rapids), Memory (M3), GPU (A3 Ultra/Mega with H100s), Arm (T2A Ampere).
- **Custom Machine Types:** Define exact vCPU and memory configurations — avoid over-provisioning without being locked into fixed T-shirt sizes.
- **Spot VMs:** Preemptible/Spot VMs at up to 91% discount; 30-second preemption notice and 24-hour max runtime policy removed in 2025.
- **Confidential VMs:** AMD SEV and Intel TDX support across N2D, C3 series — memory encrypted during processing.
- **Hyperdisk ML:** New in 2025 — high-throughput block storage purpose-built for serving large AI model weights at inference time.
- **Live Migration:** Industry-leading VM live migration capability maintains uptime during host maintenance without user intervention.

# VM Comparison at a Glance

| Category | Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|---|
| **Processor Options** | x86 (Intel/AMD) + Ampere ARM | x86 + Graviton4 (ARM) | x86 + Ampere ARM (T2A) |
| **GPU Instances** | NC/ND/NV series (A100, H100) | P5 (H100), Trn2, Inf2 (Trainium) | A3 Ultra/Mega (H100 x 8/16) |
| **Spot/Preemptible** | Azure Spot VMs (up to 90% off) | EC2 Spot Instances (up to 90% off) | Spot VMs (up to 91% off) |
| **Confidential Compute** | AMD SEV-SNP / Intel TDX | AMD SEV (Nitro Enclaves) | AMD SEV / Intel TDX |
| **Custom Sizing** | Fixed sizes (many options) | Fixed sizes (757 instance types) | Custom machine types available |
| **Reserved Pricing** | Reserved Instances (1 or 3 yr) | Reserved Instances / Savings Plans | Committed Use Discounts (CUDs) |
| **Auto Scaling** | VM Scale Sets (Flex + Uniform) | EC2 Auto Scaling Groups | Managed Instance Groups (MIGs) |

# 4. Containers and Kubernetes

| Microsoft Azure AKS + Azure Container Apps | Amazon AWS EKS + ECS + Fargate | Google Cloud GKE + Cloud Run |
| --- | --- | --- |

Containers have become the default deployment unit for cloud-native applications. Each provider offers managed Kubernetes as well as serverless container platforms that abstract cluster management entirely.

## Microsoft Azure

- **AKS (Azure Kubernetes Service):** Managed Kubernetes with node auto-provisioning, cluster autoscaler, Workload Identity, GitOps via Flux, and KEDA-based event-driven scaling.
- **AKS Automatic:** New in 2025 — fully managed AKS tier that auto-upgrades, auto-heals, and auto-scales with minimal operator intervention.
- **Azure Container Apps:** Serverless container platform built on Kubernetes and KEDA. Ideal for microservices and event-driven workloads without K8s expertise.
- **Azure Container Registry (ACR):** Private OCI-compliant registry with geo-replication, vulnerability scanning via Microsoft Defender, and RBAC-controlled access.
- **Azure Arc-enabled Kubernetes:** Manage and govern any Kubernetes cluster (on-prem, other clouds) from Azure using Azure Policy, Defender, and GitOps.

## Amazon AWS

- **EKS (Elastic Kubernetes Service):** Managed Kubernetes with EKS Anywhere (on-prem), EKS Auto Mode (2025), Karpenter node provisioner, and EKS Hybrid Nodes.
- **EKS Auto Mode:** Launched in 2025 — AWS manages compute, storage, and networking decisions automatically; operators focus on workloads only.
- **ECS (Elastic Container Service):** AWS-native container orchestrator; simpler than K8s for teams not needing full Kubernetes capabilities.
- **AWS Fargate:** Serverless compute for ECS and EKS — no node management, priced per vCPU/memory per second.
- **Amazon ECR:** Fully managed OCI registry with lifecycle policies, image scanning (enhanced with Amazon Inspector), and cross-account/cross-region replication.

## Google Cloud

- **GKE (Google Kubernetes Engine):** The most mature managed K8s offering — GKE Autopilot manages nodes/pods automatically; Standard mode gives full control.
- **GKE Enterprise:** Multi-cluster management across clouds and on-prem via Fleet management, Policy Controller, Config Sync, and Service Mesh.
- **Cloud Run:** Fully managed serverless containers — scales to zero, supports gRPC, WebSockets, and HTTP/2. Gen2 runtime launched in 2024.

- **Artifact Registry:** Universal package registry supporting Docker, Helm, npm, Maven, Python — with SBOM generation and binary authorization policies.
- **Anthos / GKE Enterprise:** Hybrid/multi-cloud Kubernetes management platform; runs on GCP, AWS, Azure, bare metal, or VMware.

## Container Comparison at a Glance

| Category | Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|---|
| **Managed Kubernetes** | AKS (+ AKS Automatic) | EKS (+ EKS Auto Mode) | GKE Standard / Autopilot |
| **Serverless Containers** | Azure Container Apps | AWS Fargate (ECS/EKS) | Cloud Run (Gen2) |
| **Container Registry** | Azure Container Registry | Amazon ECR | Artifact Registry |
| **K8s on-prem/multi-cloud** | Arc-enabled Kubernetes | EKS Anywhere / Hybrid Nodes | GKE Enterprise / Anthos |
| **Node Provisioner** | Node Auto-Provisioning (NAP) | Karpenter | GKE Node Auto-Provisioning |
| **Vulnerability Scanning** | Microsoft Defender for Containers | Amazon Inspector (Enhanced) | Artifact Analysis / GKE Security Posture |

# 5. Serverless Computing

| Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|
| Azure Functions + Logic Apps | AWS Lambda + Step Functions | Cloud Functions + Workflows |

## Microsoft Azure

- **Azure Functions v4:** Event-driven FaaS supporting C#, Python, Node.js, Java, PowerShell. Flex Consumption plan (2025) adds per-instance concurrency and faster cold starts.
- **Durable Functions:** Stateful orchestrations (fan-out/fan-in, human approval, async HTTP) using the Virtual Actor pattern.
- **Logic Apps (Standard):** Low-code workflow orchestration; now runs in single-tenant mode on Azure Functions infrastructure with local dev support.
- **Azure API Management:** Full lifecycle API gateway: throttling, OAuth2, JWT validation, developer portal, monetization, and mock policies.

## Amazon AWS

- **AWS Lambda:** Industry-leading FaaS — 15-minute max timeout, 10 GB memory, Lambda SnapStart (Java), response streaming, and up to 10x faster cold starts with SnapStart.
- **Lambda Function URLs:** Direct HTTPS endpoints for Lambda without API Gateway — ideal for single-function microservices.
- **AWS Step Functions:** Visual workflow orchestration for Lambda and 200+ AWS services. Express Workflows for high-volume, short-duration tasks.
- **Amazon EventBridge:** Serverless event bus connecting AWS services, SaaS applications, and custom apps — foundational for event-driven architectures.
- **AWS SAM / CDK:** Infrastructure-as-code toolkits purpose-built for serverless applications.

## Google Cloud

- **Cloud Functions (2nd Gen):** Based on Cloud Run infrastructure — longer timeouts (60 min), larger instances (32 GB RAM), concurrent requests per instance.
- **Cloud Run Functions:** 2025 rebranding of Cloud Functions to emphasize unified Cloud Run platform.
- **Cloud Workflows:** Serverless orchestration with built-in retries, parallel steps, and callbacks — integrates with any HTTP API.
- **Eventarc:** Unified event routing from 90+ Google Cloud sources to Cloud Run, Cloud Functions, GKE, and Workflows.
- **API Gateway + Apigee:** Cloud API Gateway for simple proxying; Apigee for enterprise API management with analytics and monetization.

# 6. Storage Services

| Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|
| Azure Blob / Files / Disks | Amazon S3 / EFS / EBS | Cloud Storage / Filestore / Persistent Disks |

## Microsoft Azure

- **Azure Blob Storage:** Massively scalable object storage. Access tiers: Hot, Cool, Cold (new in 2023), and Archive. Supports lifecycle management policies.
- **Azure Data Lake Storage Gen2:** Hierarchical namespace on top of Blob Storage for big data analytics — Hadoop-compatible, petabyte scale.
- **Azure Files:** Fully managed SMB/NFS file shares. Azure File Sync enables hybrid caching on Windows Server. Supports Kerberos authentication.
- **Azure Disks:** Block storage: Standard HDD, Standard SSD, Premium SSD v2, Ultra Disk. Premium SSD v2 enables sub-millisecond latency with adjustable IOPS/throughput without downtime.
- **Azure Elastic SAN:** New storage area network (SAN) service offering block storage for large-scale VM and container workloads at 80% lower cost.
- **Redundancy:** LRS, ZRS, GRS, GZRS, RA-GRS, RA-GZRS — up to 6 copies across 2 regions.

## Amazon AWS

- **Amazon S3:** Foundational object storage — 11 nines durability, S3 Express One Zone (single-digit ms latency), Intelligent-Tiering, Glacier Instant/Flexible/Deep Archive.
- **S3 Express One Zone:** New in 2024 — purpose-built for latency-sensitive workloads requiring single-digit millisecond access (10x faster than S3 Standard).
- **Amazon EBS:** Block storage for EC2: gp3, io2 Block Express (256,000 IOPS), st1, sc1. EBS Snapshots stored in S3.
- **Amazon EFS:** Fully managed NFS for Linux workloads; scales automatically; Elastic throughput mode adjusts automatically.
- **Amazon FSx:** Managed file systems: FSx for Windows File Server, Lustre (HPC), NetApp ONTAP, and OpenZFS — covering enterprise storage migration scenarios.
- **AWS Storage Gateway:** Hybrid storage bridge: File Gateway, Tape Gateway, Volume Gateway for on-premises to cloud transitions.

## Google Cloud

- **Cloud Storage:** Object storage with unified namespace. Classes: Standard, Nearline (monthly), Coldline (quarterly), Archive. Autoclass feature automatically transitions objects.
- **Persistent Disks:** Zonal and Regional PDs in HDD, Balanced, SSD, and Extreme tiers. Regional PD replicates synchronously across two zones.
- **Hyperdisk:** Next-gen block storage: Hyperdisk Balanced, Extreme, Throughput, and ML (for AI inference). IOPS/throughput are independently configurable and can be adjusted live.

- **Cloud Filestore:** Managed NFS at Basic, High Scale, and Enterprise tiers. Enterprise tier provides zonal replication and backups.
- **NetApp Google Cloud Volumes:** First-party managed NetApp ONTAP service on GCP — supports NFS v3/v4, SMB, and dual-protocol access.
- **Parallelstore:** New in 2024 — Google-managed Lustre-compatible parallel file system for AI/ML and HPC workloads. Sub-millisecond latency with hundreds of GB/s throughput.

## Storage Comparison at a Glance

| Category | Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|---|
| **Object Storage** | Azure Blob Storage (Hot/Cool/Cold/Archive) | Amazon S3 (Standard/IA/Glacier/Express) | Cloud Storage (Standard/Nearline/Coldline/Archive) |
| **Block Storage** | Premium SSD v2 / Ultra Disk | EBS gp3 / io2 Block Express | Hyperdisk Extreme / Balanced |
| **Managed NFS** | Azure Files (SMB + NFS) | Amazon EFS | Cloud Filestore / NetApp Volumes |
| **HPC File System** | Azure Managed Lustre | FSx for Lustre | Parallelstore (Lustre-compatible) |
| **Hybrid Storage** | Azure File Sync / StorSimple | AWS Storage Gateway | Storage Transfer Service |
| **Max Block IOPS** | Ultra Disk: 400,000 IOPS | io2 Block Express: 256,000 IOPS | Hyperdisk Extreme: 350,000 IOPS |

# 7. Networking and Connectivity

| Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|
| Azure VNet + ExpressRoute | Amazon VPC + Direct Connect | Google VPC + Cloud Interconnect |

## Microsoft Azure

- **Azure Virtual Network (VNet):** Private network fabric with subnets, NSGs, route tables, service endpoints, and private endpoints for PaaS services.
- **Azure Load Balancer:** Layer 4 TCP/UDP load balancer with Standard tier supporting Availability Zones and cross-region load balancing.
- **Azure Application Gateway v2:** Layer 7 WAF-integrated load balancer with URL routing, SSL offload, autoscaling, and Web Application Firewall (WAF_v2).
- **Azure Front Door:** Global CDN and Layer 7 load balancer with built-in WAF, DDoS protection, and private link origin support.
- **Azure DDoS Protection:** Standard tier provides adaptive tuning and telemetry — protects against volumetric, protocol, and application layer attacks.
- **Azure Private Link:** Private connectivity to Azure PaaS and partner services over the Microsoft backbone — no public IP exposure.
- **Azure Virtual WAN:** Cloud-managed WAN hub integrating SD-WAN, VPN, ExpressRoute, and inter-VNet routing in a unified topology.

## Amazon AWS

- **Amazon VPC:** Logically isolated virtual network with granular control over CIDR blocks, subnets, route tables, NACLs, and security groups.
- **Elastic Load Balancing:** ALB (Layer 7), NLB (Layer 4), GWLB (inline security appliances), and CLB (legacy). ALB supports gRPC and HTTP/2.
- **AWS Transit Gateway:** Hub-and-spoke networking for thousands of VPCs and on-premises sites. Supports multicast and inter-region peering.
- **AWS PrivateLink:** Expose services privately to other VPCs and accounts without routing through the internet.
- **Amazon CloudFront:** Global CDN with 600+ PoPs, Lambda@Edge, CloudFront Functions, and real-time logs.
- **AWS Shield Advanced:** Managed DDoS protection with 24/7 SRT access, cost protection, and proactive engagement.
- **AWS Network Firewall:** Managed stateful firewall with intrusion detection (IDS/IPS), filtering rules, and Suricata-compatible rule groups.

## Google Cloud

- **Google Cloud VPC:** Global VPC — a single VPC can span all regions with subnets per region. Supports shared VPC for multi-project architectures.
- **Cloud Load Balancing:** Fully distributed, software-defined load balancing. Global HTTP(S) LB, Regional External/Internal LB, TCP/SSL, UDP Proxy.
- **Cloud Armor:** DDoS protection and WAF tightly integrated with the global load balancer. Supports adaptive DDoS protection and reCAPTCHA Enterprise integration.
- **Cloud CDN:** Integrated with HTTP(S) Load Balancing; 2,600+ edge PoPs. Supports signed URLs, range caching, and cache invalidation.
- **Media CDN:** New dedicated CDN for media streaming — Google's YouTube CDN infrastructure made available to customers.
- **Private Service Connect:** Private endpoint model for connecting to Google APIs and partner services without public IP exposure.
- **Network Intelligence Center:** Unified network monitoring: Topology, Connectivity Tests, Performance Dashboard, Firewall Insights, and Network Analyzer.

## Networking Comparison at a Glance

| Category | Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|---|
| **Virtual Network** | Azure VNet (regional) | Amazon VPC (regional) | Google Cloud VPC (global) |
| **Layer 7 Load Balancer** | App Gateway v2 / Front Door | ALB / CloudFront | Global HTTPS Load Balancer |
| **DDoS Protection** | Azure DDoS Protection Standard | AWS Shield Advanced | Cloud Armor + Adaptive Protection |
| **CDN** | Azure Front Door / CDN | Amazon CloudFront | Cloud CDN / Media CDN |
| **Private Connectivity** | Azure Private Link / Endpoint | AWS PrivateLink / VPC Endpoint | Private Service Connect |
| **Network Firewall** | Azure Firewall Premium (IDPS) | AWS Network Firewall (Suricata) | Cloud NGFW (Palo Alto) |
| **WAN / Hub** | Azure Virtual WAN | AWS Transit Gateway | Network Connectivity Center |

# 8. Databases

| Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|
| Azure SQL + Cosmos DB | Amazon RDS + DynamoDB | Cloud SQL + Spanner + Firestore |

## Microsoft Azure — Key Database Services

- **Azure SQL Database:** Fully managed SQL Server PaaS — Hyperscale tier scales up to 100TB, Serverless auto-pauses for cost savings, Ledger for immutable audit trails.
- **Azure SQL Managed Instance:** Near 100% SQL Server compatibility for lift-and-shift migrations; supports SQL Agent, linked servers, and CLR.
- **Azure Cosmos DB:** Multi-model, globally distributed NoSQL database supporting SQL, MongoDB, Cassandra, Gremlin, and Table APIs. 99.999% SLA. New Distributed PostgreSQL (preview).
- **Azure Database for PostgreSQL (Flexible Server):** Managed PostgreSQL 16 with vertical scaling, read replicas, logical decoding, and Azure AI extension for vector search.
- **Azure Cache for Redis:** Managed Redis Enterprise — supports RediSearch, RedisJSON, and active-active geo-replication.

## Amazon AWS — Key Database Services

- **Amazon RDS:** Managed relational DB: MySQL, PostgreSQL, MariaDB, Oracle, SQL Server. Multi-AZ and Read Replicas. Optimized Reads (local NVMe) in 2024.
- **Amazon Aurora:** MySQL/PostgreSQL-compatible with up to 5x MySQL performance. Aurora Serverless v2 scales in fine-grained increments. Aurora I/O-Optimized for write-intensive workloads.
- **Amazon DynamoDB:** Serverless NoSQL with single-digit millisecond performance at any scale. Global Tables, DynamoDB Streams, PartiQL, Zero-ETL integration.
- **Amazon ElastiCache / MemoryDB:** Redis-compatible ElastiCache for caching; MemoryDB for durable, in-memory primary database with Redis API.
- **Amazon DocumentDB:** MongoDB-compatible managed document database. Elastic clusters for multi-master write workloads.

## Google Cloud — Key Database Services

- **Cloud SQL:** Managed MySQL, PostgreSQL, and SQL Server. DataStream for CDC replication. AlloyDB Omni can run on-prem.
- **AlloyDB for PostgreSQL:** Google-built PostgreSQL-compatible database — 4x faster analytics and 2x faster OLTP than standard PostgreSQL. ML-accelerated vacuum and autovacuum.
- **Cloud Spanner:** Globally distributed, strongly consistent relational database. ANSI SQL support, multi-region writes, 99.999% SLA. Spanner Graph added in 2025.
- **Firestore / Datastore:** Serverless document database with real-time sync for mobile/web apps. Datastore mode for server-side workloads.
- **BigTable:** Petabyte-scale, low-latency NoSQL for time-series, IoT, and analytics. HBase-compatible API.
- **Memorystore:** Managed Redis and Valkey (open-source Redis fork). Memorystore for Redis Cluster supports horizontal scaling.

# 9. Backup and Disaster Recovery

| Microsoft Azure<br>Azure Backup + ASR | Amazon AWS<br>AWS Backup + DRS | Google Cloud<br>Google Cloud Backup and DR |
|---|---|---|

## Microsoft Azure

- **Azure Backup:** Centralized, policy-driven backup for VMs, SQL Server, SAP HANA, Azure Files, blobs, and AKS. Immutable vaults (2024) prevent ransomware deletion.
- **Azure Site Recovery (ASR):** Replicates VMs and physical servers to Azure or a secondary region. Supports Hyper-V, VMware, and Azure-to-Azure replication with RPO as low as 30 seconds.
- **Azure Business Continuity Center:** Unified BCDR governance dashboard launched in 2024 — single pane of glass for backup and ASR across subscriptions.
- **Retention & Compliance:** Soft delete, cross-subscription restore, and Azure Policy integration for enforcing backup compliance.

## Amazon AWS

- **AWS Backup:** Centralized backup across EBS, RDS, DynamoDB, EFS, FSx, EC2, S3, and VMware. Backup Audit Manager provides compliance reporting.
- **AWS Elastic Disaster Recovery (DRS):** Continuous block-level replication for on-premises or cross-region EC2 recovery. RPO in seconds, RTO in minutes.
- **S3 Versioning & MFA Delete:** Object-level protection against accidental/malicious deletion. S3 Object Lock for WORM compliance.
- **AWS Backup Restore Testing:** New in 2024 — automated restore tests on a schedule with pass/fail reporting for compliance.

## Google Cloud

- **Google Cloud Backup and DR:** Managed backup service for Compute Engine, Cloud SQL, GKE, and VMware Engine. Instant disk recovery for VMs.
- **Cross-Region Replication:** Synchronous or async replication of Persistent Disks and Cloud Storage across regions.
- **Cloud Storage Retention Policies:** Object-level WORM locks and retention policies for compliance (SEC 17a-4, FINRA, CFTC).
- **Backup for GKE:** Application-consistent Kubernetes backup and restore — protects namespaces, workloads, and persistent volumes.

## Backup & DR Comparison

| Category | Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|---|
| **Unified Backup Service** | Azure Backup + Business Continuity Center | AWS Backup + Audit Manager | Google Cloud Backup and DR |
| **Disaster Recovery** | Azure Site Recovery (ASR) | AWS Elastic Disaster Recovery (DRS) | Cross-Region Disk Replication |
| **Ransomware Protection** | Immutable Vault + Soft Delete | S3 Object Lock / Backup Vault Lock | WORM Retention Policies |
| **RPO Capability** | As low as 30 seconds (ASR) | Seconds (DRS block-level sync) | Near-synchronous (Regional PD) |
| **RTO Capability** | Minutes (ASR failover) | Minutes (DRS automated failover) | Minutes (snapshot restore) |
| **Archival Storage** | Azure Archive (Blob) | S3 Glacier Deep Archive | Cloud Storage Archive |

# 10. Monitoring and Observability

| Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|
| Azure Monitor + App Insights | Amazon CloudWatch + X-Ray | Google Cloud Ops Suite |

## Microsoft Azure

- **Azure Monitor:** Platform-wide telemetry hub: Metrics (near real-time), Logs (Log Analytics / KQL queries), Traces, and Change Analysis.
- **Application Insights:** APM for web applications — request tracking, dependency monitoring, Live Metrics, Profiler, Snapshot Debugger.
- **Azure Monitor Alerts:** Metric, log, activity log, and smart detection alerts. Action Groups trigger email, SMS, webhooks, runbooks, or ITSM tickets.
- **Azure Managed Grafana:** Fully managed Grafana workspace — natively reads Azure Monitor, Prometheus, and Log Analytics data sources.
- **Azure Managed Prometheus:** Metrics collection and storage at scale for AKS clusters; integrates with Azure Managed Grafana.
- **Microsoft Sentinel:** Cloud-native SIEM/SOAR with AI-driven threat detection, investigation, and automated response playbooks.

## Amazon AWS

- **Amazon CloudWatch:** Metrics, logs, alarms, dashboards, Contributor Insights, Anomaly Detection, and Synthetics for canary monitoring.
- **AWS X-Ray:** Distributed tracing for microservices; traces requests across Lambda, EC2, ECS, API Gateway with service maps.
- **Amazon Managed Prometheus / Grafana:** Open-source compatible managed services — AMP for Prometheus metrics, AMG for Grafana dashboards.
- **AWS CloudTrail:** Records all API calls — governance, compliance, and security auditing. CloudTrail Lake for SQL-queryable event analysis.
- **AWS Config:** Resource inventory, configuration history, and compliance evaluation against managed/custom rules with auto-remediation.
- **Amazon DevOps Guru:** ML-powered operational insights — identifies anomalous behaviors and recommends remediation steps automatically.

## Google Cloud

- **Cloud Monitoring:** Full-stack observability with 1,500+ built-in metrics, alerting policies, uptime checks, and SLO monitoring.
- **Cloud Logging:** Petabyte-scale log management with Log Router, Log-Based Metrics, Log Analytics (BigQuery-backed), and Data Access audit logs.
- **Cloud Trace:** Distributed tracing with latency analysis and automatically sampled request graphs across GCP services.
- **Cloud Profiler:** Always-on, low-overhead CPU/memory profiling for production workloads — available for Go, Java, Node, Python, Ruby.
- **Error Reporting:** Automatic error grouping and alerting for exceptions in applications — integrates with Cloud Monitoring.
- **Security Command Center:** Centralized security and risk management — Asset Inventory, Threat Detection, Vulnerability Assessment, and Compliance Posture.

## Monitoring Comparison at a Glance

| Category | Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|---|
| **Core Platform** | Azure Monitor (KQL) | Amazon CloudWatch | Cloud Monitoring (MQL/PromQL) |
| **APM** | Application Insights | AWS X-Ray + CloudWatch Synthetics | Cloud Trace + Cloud Profiler |
| **Log Analytics** | Log Analytics (KQL) | CloudWatch Logs Insights / CloudTrail Lake | Cloud Logging (Log Analytics + BigQuery) |
| **Managed Grafana** | Azure Managed Grafana | Amazon Managed Grafana (AMG) | Google Cloud Managed Service for Prometheus |
| **SIEM** | Microsoft Sentinel (SIEM+SOAR) | Amazon Security Lake + GuardDuty | Chronicle (Google SecOps) |
| **Compliance Audit** | Azure Policy + Microsoft Defender | AWS Config + Security Hub | Security Command Center + Audit Logs |

# 11. DevOps and CI/CD

| Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|
| Azure DevOps + GitHub Actions | AWS CodePipeline + CodeBuild | Cloud Build + Cloud Deploy |

## Microsoft Azure

- **Azure DevOps:** End-to-end DevOps platform: Boards (Agile planning), Repos (Git), Pipelines (CI/CD), Test Plans, Artifacts.
- **GitHub Actions:** Event-driven CI/CD natively integrated into GitHub repositories. 20,000+ actions in the Marketplace. Hosted and self-hosted runners.
- **Azure Artifacts:** Universal package feed for npm, NuGet, Maven, Python, and Cargo. Upstream sources and retention policies.
- **Deployment Environments:** New in 2024 — Azure Deployment Environments provisions IaC-defined app infrastructure on-demand for developers.
- **Microsoft Dev Box:** Cloud-hosted, preconfigured developer workstations — ready in minutes, governed by IT, customizable by developers.

## Amazon AWS

- **AWS CodePipeline:** Managed CI/CD orchestration — connects CodeCommit/GitHub, CodeBuild, and CodeDeploy into automated release pipelines.
- **AWS CodeBuild:** Fully managed build service with Docker support, concurrent builds, and ARM64 (Graviton) build environments.
- **AWS CodeDeploy:** Automated deployment to EC2, Lambda, and ECS with blue/green and canary strategies.
- **Amazon CodeCatalyst:** Unified software development service launched in 2023 — Spaces, Projects, Dev Environments, and Workflows.
- **AWS CDK / CloudFormation:** Infrastructure as code: CloudFormation (JSON/YAML declarative) and CDK (TypeScript, Python, Java, Go — imperative).

## Google Cloud

- **Cloud Build:** Managed CI service with Docker container builds, parallel steps, caching, and security scanning integration.
- **Cloud Deploy:** Managed continuous delivery service with canary, blue/green, and progressive delivery strategies across GKE, Cloud Run, and Anthos.
- **Artifact Registry:** Central hub for container images and language packages — signed images, vulnerability scanning, Binary Authorization.
- **Cloud Workstations:** Managed cloud-based developer desktops — custom configurations, persistent home directories, accessible via browser.
- **Skaffold + Terraform:** Google maintains Skaffold (Kubernetes app development), and Terraform providers for GCP are first-class supported.

# 12. AI and Machine Learning Services

| Microsoft Azure<br>Azure AI + OpenAI Service | Amazon AWS<br>Amazon SageMaker + Bedrock | Google Cloud<br>Vertex AI + Gemini |
|---|---|---|

## Microsoft Azure

- **Azure OpenAI Service:** Exclusive access to OpenAI models (GPT-4o, GPT-4 Turbo, o1, o3-mini, DALL-E 3, Whisper) with enterprise SLA, content filtering, and private endpoints.
- **Azure AI Studio:** Unified platform for building, evaluating, and deploying generative AI applications with prompt flow, fine-tuning, and RAG patterns.
- **Azure Machine Learning:** MLOps platform: automated ML, pipelines, model registry, monitoring, and responsible AI tools. Integrated with GitHub Actions.
- **Azure AI Services (Cognitive):** Vision, Speech, Language, Document Intelligence, and Search — composable AI APIs with private endpoint support.
- **Microsoft Fabric AI:** Unified analytics platform combining OneLake, Spark, Data Factory, and AI Copilot capabilities.
- **Phi-4 / Phi-3 (SLMs):** Microsoft's open-source small language models — available via Azure AI Studio for cost-efficient, on-device, or fine-tuned deployments.

## Amazon AWS

- **Amazon Bedrock:** Serverless access to foundation models from Anthropic (Claude), Meta (Llama), Mistral, Amazon (Titan, Nova), Stability AI, and others. Guardrails, Agents, and Knowledge Bases built-in.
- **Amazon Nova:** AWS's new proprietary multimodal model family (Nova Micro, Lite, Pro, Canvas, Reel) — generally available from December 2024.
- **Amazon SageMaker:** End-to-end ML platform: Studio, Pipelines, Model Registry, Feature Store, JumpStart (model catalog), Canvas (no-code), HyperPod (training clusters).
- **Amazon Q:** Generative AI assistant for AWS developers and business users — integrated across the AWS Console, IDEs, and business applications.
- **AWS Trainium2 / Inferentia2:** Purpose-built ML accelerator chips at lower cost than GPU instances for training and inference respectively.

## Google Cloud

- **Vertex AI:** Unified AI platform: Model Garden (100+ models), Vertex AI Studio, Training, Prediction, Feature Store, Pipelines, and Model Monitoring.
- **Gemini Models:** Gemini 2.0 Pro/Flash available via Vertex AI — multimodal (text, image, video, audio, code) with 2M token context window.
- **Gemini for Google Cloud:** AI-powered assistance embedded throughout the Cloud Console, BigQuery, Security Command Center, and Looker.
- **Agent Builder / Dialogflow CX:** Build conversational AI agents and multi-agent systems with Vertex AI Agent Builder and DFCX for enterprise chatbots.
- **TPU v5 / v5p:** Google's Tensor Processing Units remain the most powerful purpose-built AI accelerators — available via Cloud TPU and TPU VMs.
- **NotebookLM:** AI-powered research tool available within Google Workspace and as a standalone product — built on Gemini.

## AI/ML Comparison at a Glance

| Category | Microsoft Azure | Amazon AWS | Google Cloud |
|---|---|---|---|
| Gen AI / LLM Access | Azure OpenAI (GPT-4o, o1, o3) | Amazon Bedrock (Claude, Nova, Llama) | Vertex AI (Gemini 2.0, Llama, Mistral) |
| Proprietary Models | Phi-4 (SLM) | Amazon Nova (multimodal) | Gemini 2.0 (multimodal, 2M ctx) |
| ML Platform | Azure Machine Learning + Fabric | Amazon SageMaker | Vertex AI Platform |
| Managed Training | AML Compute / Azure NDH100 clusters | SageMaker HyperPod | Cloud TPU v5p / A3 Mega clusters |
| AI Hardware | NDH100 v5 (H100 80GB SXM5) | Trainium2 + Inferentia2 + P5 (H100) | TPU v5p + A3 Ultra (H100) |
| Vector Search | Azure AI Search (hybrid) | Amazon OpenSearch + Bedrock KB | Vertex AI Vector Search (ANN) |
| AI Safety/Guardrails | Azure AI Content Safety | Amazon Bedrock Guardrails | Vertex AI Safety Filters / Responsible AI |

# 13. Security Best Practices

| Microsoft Azure
Microsoft Defender for Cloud | Amazon AWS
AWS Security Hub + GuardDuty | Google Cloud
Security Command Center |
|---|---|---|

Security is a shared responsibility. The following best practices reflect the 2025–2026 security landscape where Zero Trust, AI-driven threat detection, and supply chain security have become core requirements.

## Identity and Access

- **Enforce MFA / Passwordless:** Require phishing-resistant MFA (FIDO2/passkeys) for all privileged accounts and gradually roll out to all users.
- **Least Privilege & RBAC:** Grant minimum permissions, prefer roles over direct policies, and use access reviews to clean up stale permissions.
- **Privileged Access Workstations (PAWs):** Manage cloud infrastructure from dedicated, hardened workstations to prevent credential theft.
- **Eliminate Long-Lived Credentials:** Replace IAM user access keys / service account keys with managed identity / IAM Roles Anywhere / Workload Identity Federation.

## Network Security

- **Defense in Depth:** Layer NSGs/Security Groups, WAF, NGFW, and DDoS protection rather than relying on a single perimeter.
- **Zero Trust Network Access:** Replace legacy VPN with ZTNA (Entra Private Access / AWS Verified Access / BeyondCorp) — authenticate every request, every time.
- **Private Endpoints for PaaS:** Ensure all PaaS services (storage, databases, AI APIs) are accessed via private endpoints, not public internet.
- **Immutable Infrastructure:** Use infrastructure as code to ensure environments are reproducible — avoid manual changes in production.

## Data Protection

- **Encrypt Everything:** Enforce encryption at rest (platform-managed or customer-managed keys) and in transit (TLS 1.2+) for all data.
- **Key Management:** Azure Key Vault / AWS KMS / Cloud KMS — centralize key lifecycle, rotation, and access control. Use Hardware Security Modules (HSMs) for highly sensitive keys.
- **Secrets Management:** Never hardcode credentials. Use Azure Key Vault Secrets / AWS Secrets Manager / Google Secret Manager with automatic rotation.
- **Data Classification:** Tag and classify data by sensitivity — use Microsoft Purview / AWS Macie / Google Cloud DLP to discover and protect sensitive data automatically.

# Cloud Security Posture Management (CSPM)

- **Enable Native CSPM Tools:** Microsoft Defender for Cloud / AWS Security Hub / Google Security Command Center — enable by default across all accounts/subscriptions.
- **Threat Detection:** Microsoft Sentinel / Amazon GuardDuty / Google Threat Intelligence — AI-driven anomaly detection with automated response playbooks.
- **Supply Chain Security:** Sign container images, enforce Binary Authorization / AWS Signer, generate SBOMs, and scan dependencies with Trivy or Snyk.
- **Infrastructure as Code (IaC) Scanning:** Scan Terraform / Bicep / CloudFormation / Deployment Manager templates with Checkov, tfsec, or provider-native tools before deployment.

# Compliance and Governance

- **Azure Policy / SCPs / Organization Policies:** Enforce guardrails automatically — deny non-compliant resource creation before it happens rather than detecting after.
- **Enable Audit Logging:** Azure Activity Log / AWS CloudTrail / Cloud Audit Logs — ensure all control plane and data plane actions are logged and immutable.
- **Regular Penetration Testing:** Schedule red team exercises and use each provider's native pentest authorization to test cloud security posture.
- **Incident Response Runbooks:** Pre-build IR runbooks in Logic Apps / Step Functions / Cloud Workflows that trigger automatically on critical security alerts.