Azure, AWS, Google Cloud | Comparative Guide

Version 24.04

Ahmed Abdelwahed
ahmed@abdelwahed.me
LinkedIn

Contents

Global Infrastructure and Reach

Microsoft Azure

- **Regions and Availability Zones**:
  - Azure operates in over 60 regions worldwide, making it one of the most extensive global cloud infrastructures. For example, Azure has regions in North America (like East US, West US), Europe (such as North Europe, West Europe), Asia (like Southeast Asia, East Asia), and Africa (South Africa North).
  - Each region typically contains multiple Availability Zones (AZs), which are physically separated data centers with independent power, cooling, and networking. This design ensures high availability and fault tolerance. For instance, the East US region has three AZs, allowing businesses to distribute their applications across these zones to prevent downtime.
  - Azure regions are strategically distributed to provide low-latency access and compliance with local data residency requirements. For example, the Azure Germany region ensures data is stored and processed within the country to comply with German regulations.
- **Backbone Network:**
  - Azure's backbone network is a private, global fiber-optic network that connects all Azure regions. This network ensures high bandwidth, low latency, and high availability for Azure services. For instance, Azure's network connects data centers from New York to London, enabling fast data transfer for global applications like a multinational e-commerce platform.
  - The network is optimized for both internal traffic (between Azure services) and external traffic (between Azure and customer environments), enabling seamless integration and consistent performance. For example, a company using Azure's services in the East US and West Europe regions can expect consistent performance when transferring data between these locations.
  - Azure's global backbone interconnects its regions and zones with high-speed, low-latency links, ensuring rapid data transfer and reducing latency for global applications. For instance, a video streaming service hosted on Azure can deliver content efficiently across continents with minimal buffering.
- **Redundancy and Disaster Recovery:**
  - Azure's infrastructure is built with redundancy in mind. Each AZ is isolated from others to prevent cascading failures, and services can be replicated across zones for higher availability. For example, an application hosted in Azure's East US region can have its components spread across three AZs, ensuring the application remains operational even if one zone fails.
  - Azure offers geo-redundant storage options, where data is replicated across geographically distant regions to safeguard against regional failures. For instance, data stored in the East US region can be automatically replicated to the West US region, ensuring disaster recovery in case of a regional outage.
  - Azure Site Recovery (ASR) and Azure Backup provide comprehensive disaster recovery solutions, ensuring business continuity even in the face of catastrophic failures. A healthcare provider might use ASR to replicate and failover their electronic health records system to a secondary region in the event of a disaster.

- **Local and Sovereign Cloud Offerings:**
  - Azure provides specialized regions known as Azure Government, which are tailored for U.S. government agencies and their partners, offering compliance with stringent regulatory requirements. For example, a U.S. federal agency can use Azure Government to host classified data securely.
  - Azure also offers regions like Azure China, operated by a local partner, to meet data residency and compliance requirements specific to China. Multinational companies operating in China might choose Azure China to ensure compliance with local data protection laws.
- **Interconnectivity with On-Premises:**
  - Azure's global infrastructure is designed to support hybrid cloud scenarios. Azure **ExpressRoute** provides private, dedicated connections between on-premises environments and Azure data centers, bypassing the public internet for improved security and reliability. A retail chain might use ExpressRoute to connect its on-premises point-of-sale systems to Azure's cloud services.
  - The **Azure Virtual WAN** service Azure Virtual WAN is a comprehensive networking service that unifies various networking, security, and routing functionalities into a single operational interface. It offers a range of features, including:
    - **Branch Connectivity**: Automated connectivity using Virtual WAN Partner devices like SD-WAN or VPN CPE.
    - **Site-to-Site VPN Connectivity**: Securely connect on-premises sites to Azure.
    - **Remote User VPN Connectivity (Point-to-Site)**: Allow remote users to securely access your Azure network.
    - **Private Connectivity (ExpressRoute)**: Establish private, high-bandwidth connections between your on-premises networks and Azure.
    - **Intra-Cloud Connectivity**: Facilitate transitive connectivity between virtual networks within Azure.
    - **VPN ExpressRoute Inter-Connectivity**: Integrate VPN and ExpressRoute connections for flexible networking scenarios.
    - **Routing, Azure Firewall, and Encryption**: Centralized management of routing, security policies, and encryption for private connectivity.

      The service is designed for flexibility, allowing you to start with just one use case and expand your network capabilities as your organization's needs evolve. Azure Virtual WAN is ideal for businesses seeking a scalable, secure, and efficient networking solution that can adapt to their growing requirements.

Amazon AWS

- **Regions and Availability Zones:**
    - AWS operates in over 30 regions worldwide, each containing multiple Availability Zones, making it one of the largest and most mature cloud infrastructure globally. Examples include regions like US East (N. Virginia), Asia Pacific (Sydney), and South America (São Paulo).
    - AWS pioneered the concept of Availability Zones, which are designed to be highly reliable and resilient to failures. Each AZ is isolated from the others within a region, yet interconnected with low-latency links to support synchronous data replication. For example, Amazon.com leverages multiple AZs in the US East (N. Virginia) region to ensure its e-commerce platform remains highly available and resilient.
- **Global Network:**
    - **AWS’s Global Presence**: AWS operates an extensive global network with hundreds of points of presence (PoPs), including edge locations and regional edge caches. This infrastructure supports services like Amazon CloudFront for content delivery and Route 53 for DNS. For instance, Netflix leverages AWS CloudFront to deliver streaming content to users worldwide, ensuring fast load times and reduced latency.
    - **AWS Global Backbone:** AWS's global backbone is a private network engineered for secure, low-latency connections between regions and Availability Zones (AZs). This backbone is crucial for global applications that demand high availability and consistent performance across multiple regions. For example, a global financial trading platform might utilize AWS's global network to ensure real-time data replication and low-latency trading across various continents.
- **High Availability and Resilience:**
    - AWS’s infrastructure is built for redundancy and high availability. Services like Amazon S3 and RDS offer multi-AZ deployment options, where data is automatically replicated across AZs. For example, a database hosted on Amazon RDS in the EU (Ireland) region can be set up to replicate across multiple AZs, ensuring high availability.
    - AWS provides extensive disaster recovery solutions, including cross-region replication for S3, DynamoDB global tables, and multi-region RDS deployments, enabling businesses to maintain data integrity and service availability across regional outages. A media company might use cross-region replication to ensure its video content is available even if a primary region goes down.
- **Dedicated and Specialized Regions:**
    - AWS operates several dedicated regions, such as AWS GovCloud (U.S.), which are isolated for government workloads and meet stringent security and compliance requirements. For example, a defense contractor might use AWS GovCloud to store and process sensitive defense-related data.
    - AWS also offers the AWS Outposts service, allowing customers to run AWS infrastructure on-premises for low-latency applications that require proximity to on-premises data. A healthcare provider might use AWS Outposts to process patient data on-site while maintaining compliance with healthcare regulations.
- **Hybrid and Edge Computing:**
    - **AWS Direct Connect** provides dedicated network connections between customer environments and AWS, bypassing the public internet for enhanced security and performance. A financial institution might use Direct Connect to ensure secure, low-latency data transfers between its on-premises trading systems and AWS.
    - AWS Wavelength and Local Zones extend AWS services to edge locations, closer to end-users and devices, supporting latency-sensitive applications such as IoT, gaming, and real-time analytics. For instance, a smart city project might use AWS Wavelength to process IoT data locally, enabling real-time decision-making.

Google Cloud

- **Regions and Zones:**
  - Google Cloud operates in over 35 regions, with more than 100 availability zones, providing a highly scalable and resilient global infrastructure. Examples include regions like Europe-West3 (Frankfurt), Asia-East1 (Taiwan), and South America-East1 (São Paulo).
  - Google's regions are designed with redundancy and high availability in mind, offering multiple zones per region, each with independent power, cooling, and networking. This design ensures fault tolerance and data safety. For example, a global online marketplace might distribute its services across multiple zones in the Europe-West3 region to ensure continuous uptime.
- **Private Global Fiber Network:**
  - Google Cloud leverages Google's private global fiber network, which is one of the largest and most advanced in the world. This network connects all Google Cloud regions, offering high bandwidth, low latency, and optimized performance. For example, Google Search uses this network to deliver search results quickly to users worldwide, regardless of location.
  - The network is designed to support high-throughput applications, providing fast and secure data transfer across global regions, and enabling global load balancing for distributed applications. An example would be a global ad-serving platform that uses Google Cloud's network to deliver ads with minimal latency to users across different continents.
- **Redundancy and High Availability:**
  - Google Cloud's infrastructure emphasizes redundancy at every layer. Persistent Disks, for example, are replicated across multiple zones within a region to ensure data durability. For example, a SaaS provider might use Persistent Disks in the Asia-East1 region to ensure its services remain available even if one zone experiences a failure.
  - Google Cloud Storage offers multi-regional storage options, automatically replicating data across multiple regions to protect against regional failures. A global research organization might store critical datasets in multi-regional storage to ensure access during a regional outage.
  - Google's commitment to high availability is further demonstrated by services like Google Kubernetes Engine (GKE), which supports multi-zone clusters for fault-tolerant deployments. For example, an e-commerce platform might use GKE to distribute its application across zones in the US-West1 region, ensuring uninterrupted service during traffic spikes.
- **Advanced Networking Capabilities:**
  - Google's Software-Defined Networking (SDN) technology, Andromeda, provides high-performance, flexible, and scalable networking services. It supports global VPCs that span multiple regions, offering seamless and secure connectivity across Google's global infrastructure. For instance, a logistics company might use a global VPC to manage and secure data flows between its operations in North America, Europe, and Asia.
  - Google's global load balancing is built into the network fabric, allowing applications to distribute traffic across multiple regions and provide near-instant failover in case of regional disruptions. An example would be a global social media platform using Google's load balancing to ensure users worldwide can access the service with minimal latency.

- **Compliance and Specialized Regions:**
  - Google Cloud operates specialized regions for compliance with local regulations, such as the Google Cloud Germany region, which is designed to meet stringent European data protection standards. For instance, a European healthcare provider might choose the Germany region to ensure compliance with GDPR.
  - Google Cloud's network also supports interconnect services like Cloud Interconnect and Carrier Peering, enabling secure, high-bandwidth connections between on-premises environments and Google Cloud. A multinational company might use Carrier Peering to optimize its global network connectivity with Google Cloud, reducing costs and improving performance.
- **Edge and Hybrid Cloud Integration:**
  - **Google Cloud Anthos** provides a hybrid and multi-cloud platform, enabling consistent application development and deployment across on-premises, Google Cloud, and other cloud environments. For example, a retail chain might use Anthos to manage its point-of-sale systems across different cloud environments and on-premises servers.
  - Google's edge computing services, including Google Cloud CDN and Edge TPU, extend computing power and data processing capabilities closer to end-users, reducing latency for real-time applications and IoT devices. For example, a smart home device manufacturer might use Edge TPU to process data locally, providing faster responses to user commands.
  - Google Cloud's Dedicated Interconnect and Partner Interconnect services provide direct, high-bandwidth network connections between on-premises networks and Google's network, reducing latency and improving throughput for hybrid cloud deployments. A global media company might use Dedicated Interconnect to stream high-definition video content from its on-premises studios to Google Cloud's infrastructure for global distribution.

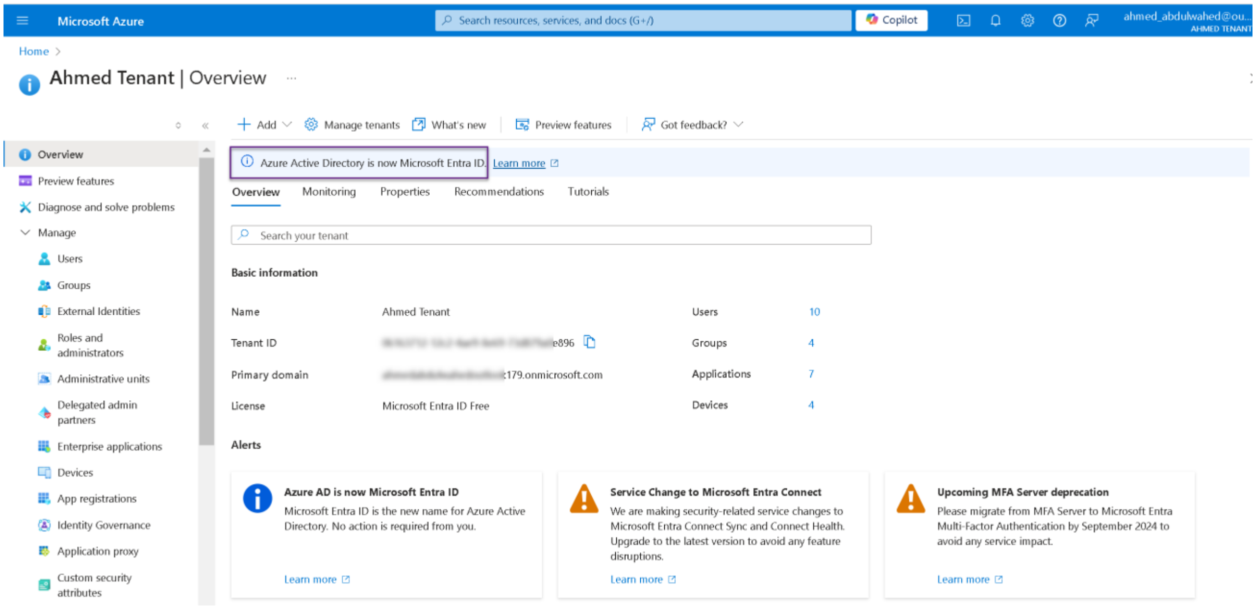
Managing Identity and Access

Microsoft Azure

- **Microsoft Entra ID**:
    - **Service Overview:** Microsoft Entra ID is Microsoft's cloud-based identity and access management service, designed to help organizations manage user identities and secure access to resources both on-premises and in the cloud. Microsoft Entra ID supports single sign-on (SSO), multi-factor authentication (MFA), and conditional access policies.
    - **User and Group Management:**
        - **User Creation**: Administrators can create and manage user identities in Microsoft Entra, either manually through the Azure portal or programmatically via PowerShell or the Microsoft Graph API. For example, an organization might automate the onboarding process by creating user accounts and assigning them to the appropriate groups based on department.
        - **Groups**: Microsoft Entra allows for the creation of security and Microsoft 365 groups to manage permissions across multiple users. For instance, a company might create a group for the finance department, assigning the group access to specific financial applications.
        - **Dynamic Groups**: Microsoft Entra supports dynamic groups, where membership is automatically updated based on user attributes, such as department or location. For example, users in the "Sales" department could automatically be added to a "Sales Team" group that grants access to relevant sales tools.
    - **Role-Based Access Control (RBAC):**
        - **Service Overview**: Azure RBAC is a system that provides fine-grained access management for Azure resources. It allows administrators to assign roles to users, groups, and applications, specifying what actions they can perform on specific resources.
        - **Built-in Roles**: Azure provides numerous built-in roles, such as "Owner," "Contributor," and "Reader," each with predefined permissions. For example, a project manager might be assigned the "Contributor" role on a resource group, allowing them to manage resources without having full administrative rights.
        - **Custom Roles**: Administrators can create custom roles tailored to specific business needs, defining exact permissions at the resource, resource group, or subscription level. For instance, a company might create a custom role that allows users to view network configurations but not modify them.
    - **Multi-Factor Authentication (MFA):**
        - **Service Overview**: Microsoft Entra MFA adds a layer of security by requiring users to verify their identity using a second factor, such as a phone call, SMS, or mobile app notification, in addition to their password.
        - **Conditional Access**: MFA can be enforced through conditional access policies that require additional verification under specific conditions, such as when accessing resources from an unknown location or using an untrusted device. For example, a financial services firm might require MFA for employees accessing sensitive financial data from outside the corporate network.
    - **Microsoft Entra B2B and B2C:**
        - **Microsoft Entra B2B**: Microsoft Entra Business-to-Business (B2B) allows organizations to securely collaborate with external users by granting them access to resources using their existing credentials from another organization or identity provider. For example, a company might invite external consultants to access a shared project portal without creating new user accounts for them.
        - **Microsoft Entra B2C**: Microsoft Entra Business-to-Consumer (B2C) provides identity management for consumer-facing applications, allowing users to sign up and sign in using social accounts (like Google or

Facebook) or custom credentials. An e-commerce site might use Microsoft Entra B2C to manage customer identities and enable secure checkout processes.

- **Identity Protection and Governance:**
    - **Identity Protection**: Microsoft Entra Identity Protection uses machine learning to detect potential identity risks and take automated actions to mitigate them, such as requiring a password reset or blocking access. For example, if an account is accessed from an unusual location, Identity Protection might prompt the user to verify their identity.
    - **Privileged Identity Management (PIM)**: PIM helps manage, control, and monitor access to important resources, reducing the risk of excessive, unnecessary, or misused access permissions. For instance, a company might use PIM to grant temporary administrative rights to IT staff only when needed, rather than permanent access.



Ahmed Tenant | Overview

Azure Active Directory is now Microsoft Entra ID. Learn more

Basic information

Name	Ahmed Tenant	Users	10
Tenant ID	[redacted]e896	Groups	4
Primary domain	[redacted]179.onmicrosoft.com	Applications	7
License	Microsoft Entra ID Free	Devices	4

Alerts

Azure AD is now Microsoft Entra ID
Microsoft Entra ID is the new name for Azure Active Directory. No action is required from you.
Learn more

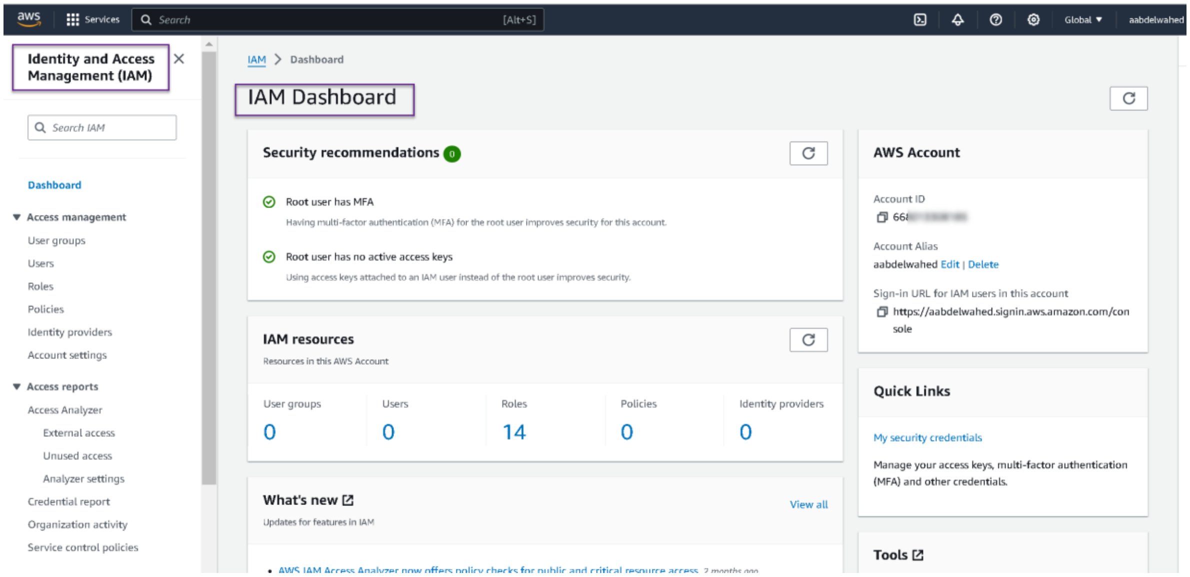
Service Change to Microsoft Entra Connect
We are making security-related service changes to Microsoft Entra Connect Sync and Connect Health. Upgrade to the latest version to avoid any feature disruptions.
Learn more

Upcoming MFA Server deprecation
Please migrate from MFA Server to Microsoft Entra Multi-Factor Authentication by September 2024 to avoid any service impact.
Learn more

Amazon AWS

- **AWS Identity and Access Management (IAM)**:
  - **Service Overview**: AWS Identity and Access Management (IAM) is a service that helps manage access to AWS resources securely. IAM enables you to create and manage AWS users and groups, and use permissions to allow or deny their access to AWS resources.
  - **User and Group Management:**
    - **User Creation**: AWS IAM allows administrators to create user accounts for individuals, providing them with unique credentials for accessing AWS resources. These accounts can be managed via the AWS Management Console, CLI, or APIs. For example, an IT department might create individual IAM user accounts for developers, each with specific access rights.
    - **Groups**: IAM groups simplify access management by allowing you to attach policies to multiple users at once. For instance, all members of a development team can be added to a "Developers" group that grants them access to development resources while restricting production access.
  - **Policies and Permissions:**
    - **Managed Policies**: AWS provides pre-defined managed policies that you can attach to users, groups, and roles, simplifying access management. For example, the "ReadOnlyAccess" policy allows users to view AWS resources without making changes.
    - **Custom Policies**: Administrators can create custom policies using JSON to define specific permissions that suit their organizational needs. For example, a custom policy might grant permission to access specific S3 buckets or restrict EC2 instance management to certain regions.
  - **Roles and Role-Based Access:**
    - **Service Overview**: IAM roles allow you to define a set of permissions for AWS services, which can be assumed by trusted entities such as users, applications, or services. This is useful for granting temporary access or allowing cross-account access.
    - **Service Roles**: Roles can be assigned to AWS services, such as EC2 or Lambda, enabling these services to interact with other AWS resources securely. For example, an EC2 instance might assume a role that grants it permission to read from an S3 bucket, without requiring permanent credentials on the instance.
    - **Cross-Account Access**: IAM roles enable secure cross-account access, allowing resources in one AWS account to access resources in another account. For instance, a central security team might manage all IAM policies for multiple AWS accounts in an organization.
  - **Multi-Factor Authentication (MFA):**
    - **Service Overview**: AWS MFA enhances security by requiring users to provide a second form of authentication, such as a code from a hardware device or a mobile app, in addition to their username and password.
    - **Virtual MFA Devices**: IAM supports virtual MFA devices that can be enabled for users, adding an extra layer of security. For example, a root account in AWS might be secured with MFA to prevent unauthorized access.
    - **IAM Policies for MFA**: Administrators can create IAM policies that enforce MFA for specific actions, such as accessing sensitive resources or performing privileged operations. For example, a policy might require MFA for users attempting to delete S3 buckets.

- ### AWS Single Sign-On (SSO):
  - **Service Overview**: AWS SSO provides centralized access management for AWS accounts and business applications. It integrates with existing identity providers, such as Microsoft Active Directory, to provide seamless single sign-on capabilities.
  - **Application Access**: AWS SSO allows users to access multiple AWS accounts and third-party applications with a single set of credentials, streamlining the login process. For example, a large enterprise might use AWS SSO to manage access to various AWS environments and SaaS applications from a single portal.
- ### Security and Compliance:
  - **AWS IAM Access Analyzer**: This tool helps identify and audit the permissions granted to external entities, ensuring that AWS resources are not unintentionally exposed. For instance, Access Analyzer might alert administrators if an S3 bucket is accidentally made public.
  - **IAM Credential Reports**: IAM provides credential reports that list all IAM users and the status of their credentials, helping administrators ensure compliance with security best practices. A security team might use these reports to verify that all users have enabled MFA.



IAM Dashboard

Security recommendations 0

✓ Root user has MFA

Having multi-factor authentication (MFA) for the root user improves security for this account.

✓ Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	14	0	0

What's new

Updates for features in IAM

View all

- AWS IAM Access Analyzer now offers policy checks for public and critical resource access 2 months ago

AWS Account

Account ID
66[redacted]

Account Alias
aabdelwahed Edit | Delete

Sign-in URL for IAM users in this account
https://aabdelwahed.signin.aws.amazon.com/console

Quick Links

My security credentials

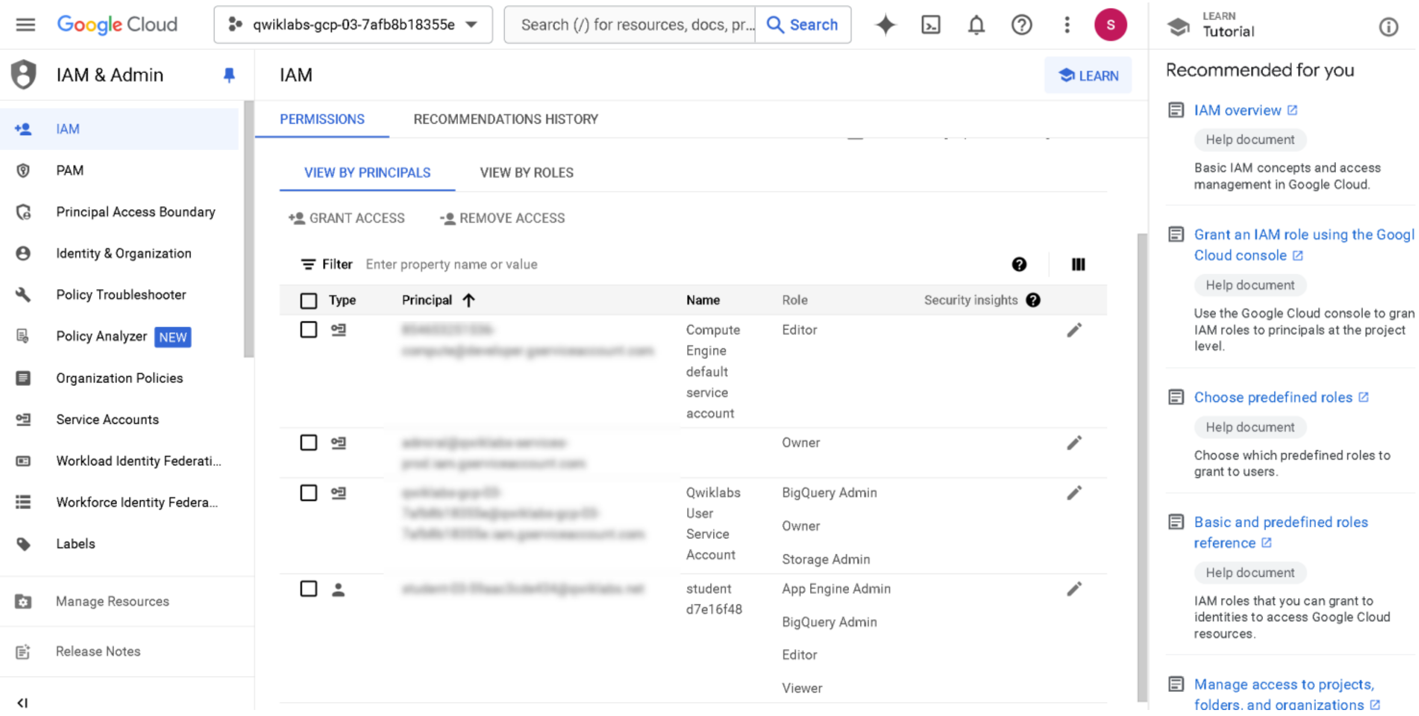
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Google Cloud

- **Google Cloud Identity and Access Management (IAM)**:
  - **Service Overview:** Google Cloud IAM provides a unified access control system that enables administrators to manage access to Google Cloud resources securely. IAM allows for fine-grained control over who can do what with specific resources, helping organizations adhere to the principle of least privilege.
  - **User and Group Management:**
    - **User Accounts**: Google Cloud integrates with Google Workspace and other identity providers, allowing administrators to manage user identities and access rights across Google Cloud resources. For instance, a company using Google Workspace can manage Google Cloud access through the same user accounts.
    - **Groups**: Administrators can manage access at scale by assigning roles to Google Groups, ensuring that users inherit permissions based on their group membership. For example, a development team might be grouped under a single "Developers" group with appropriate access to development resources.
  - **Roles and Permissions:**
    - **Predefined Roles**: Google Cloud IAM offers a variety of predefined roles that bundle permissions for common use cases, such as "Viewer," "Editor," and "Owner." For example, a junior developer might be granted the "Viewer" role on a project, allowing them to view resources without making changes.
    - **Custom Roles**: Administrators can create custom roles tailored to specific job functions or organizational policies, specifying exactly which permissions are granted. For example, a company might create a custom role that allows network engineers to manage VPC settings but not storage resources.
  - **Service Accounts:**
    - **Service Overview**: Service accounts are special Google Cloud IAM accounts used by applications and services to authenticate and interact with Google Cloud resources. Service accounts can be granted specific roles and permissions, allowing secure, automated access to resources.
    - **Use Cases**: A web application might use a service account to access a Google Cloud Storage bucket for storing user uploads, ensuring that the application can access the bucket securely without exposing user credentials.
  - **IAM Policy Management:**
    - **Policy Inheritance**: Google Cloud IAM policies are hierarchical and can be set at the organization, folder, project, or resource level. Policies set at higher levels are inherited by lower-level resources, simplifying access management. For example, a policy set at the project level might automatically apply to all VMs within that project.
    - **Conditional Role Bindings**: Google Cloud supports conditional role bindings, allowing administrators to specify conditions under which a role is granted. For instance, access to a sensitive database might be restricted to business hours.
  - **Identity-Aware Proxy (IAP):**
    - **Service Overview**: Google Cloud IAP provides secure access to web applications and VMs by enforcing identity and access policies at the application layer. IAP integrates with Google Cloud IAM to control access based on user identity and context.
    - **Use Cases**: A company might use IAP to secure an internal web application, allowing only authenticated users from specific IP ranges to access the application.

- **Multi-Factor Authentication (MFA):**
  - **Service Overview**: Google Cloud IAM supports multi-factor authentication (MFA) to enhance security by requiring users to verify their identity with a second factor, such as a code sent to a mobile device.
  - **Enforcement**: MFA can be enforced for all users or selectively based on user roles or the sensitivity of the resources being accessed. For instance, administrators might require MFA for users accessing the Google Cloud Console or sensitive data.
- **Security and Compliance:**
  - **Audit Logs**: Google Cloud maintains detailed audit logs that record all IAM-related actions, helping organizations monitor access and identify potential security issues. For example, an audit log might show who granted a particular user access to a sensitive database.
  - **Access Transparency**: Google Cloud provides Access Transparency logs that show the actions taken by Google employees when accessing customer data, helping organizations meet compliance requirements. For instance, a healthcare provider might use Access Transparency logs to verify that Google employees accessed patient data only under specific, authorized circumstances.



□ Type	Principal ↑	Name	Role	Security insights
□	[redacted]	Compute Engine default service account	Editor	
□	[redacted]		Owner	
□	[redacted]	Qwiklabs User Service Account	BigQuery Admin Owner Storage Admin	
□	[redacted]	student d7e16f48	App Engine Admin BigQuery Admin Editor Viewer	

Recommended for you

IAM overview
Help document
Basic IAM concepts and access management in Google Cloud.

Grant an IAM role using the Googl Cloud console
Help document
Use the Google Cloud console to gran IAM roles to principals at the project level.

Choose predefined roles
Help document
Choose which predefined roles to grant to users.

Basic and predefined roles reference
Help document
IAM roles that you can grant to identities to access Google Cloud resources.

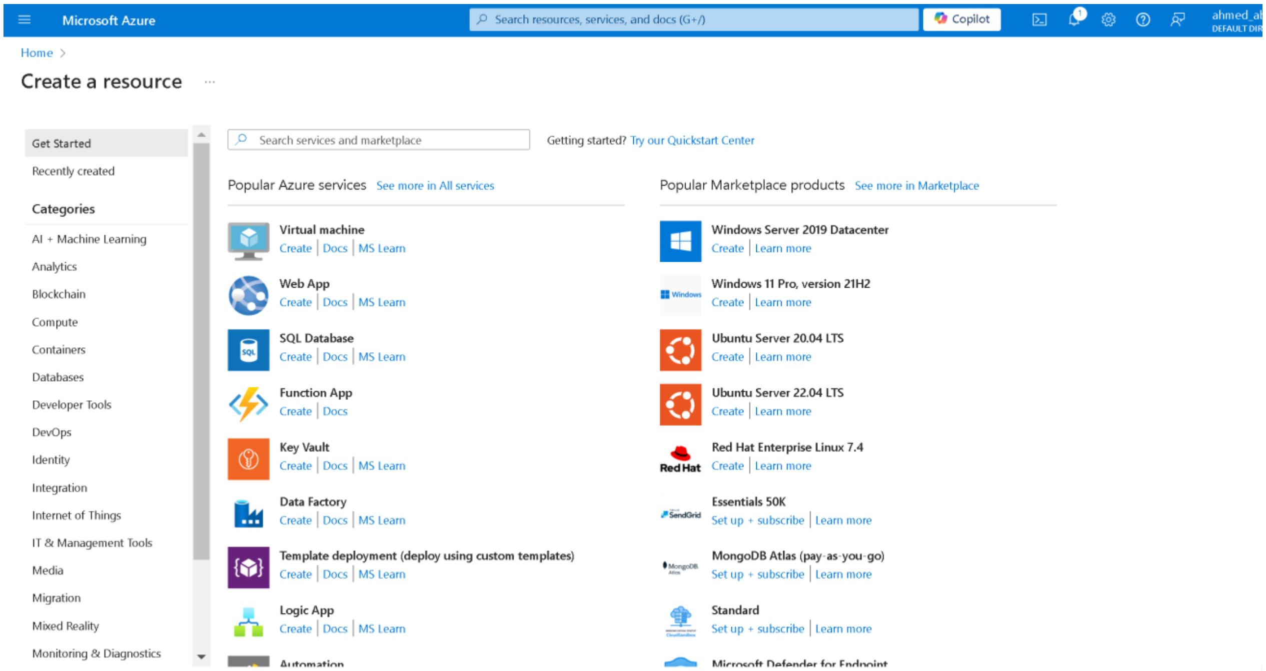
Manage access to projects, folders, and organizations

Virtual Machines (VMs)

Microsoft Azure

- **Virtual Machines (VMs):**
  - **Service Overview**: Azure Virtual Machines (VMs) provide scalable compute resources that can be used to deploy and run a wide range of workloads, from small development environments to large-scale enterprise applications. Azure VMs support both Windows and Linux operating systems, offering flexibility to meet diverse business needs.
  - **Instance Types:** Azure offers a variety of VM sizes and types, tailored to different use cases such as general-purpose workloads (e.g., the Dv3 series), compute-optimized tasks (e.g., the F-series), memory-optimized applications (e.g., the Ev3 series), and storage-optimized instances (e.g., the Lsv2 series). For example, a financial analysis application might use a memory-optimized Ev3 instance to handle large datasets in-memory.
  - **Creation Methods:**
    - **Azure Portal**: VMs can be created via the Azure Portal, where users can configure all aspects of the VM, including the operating system, VM size, storage options, networking, and security settings. For example, an IT admin might use the portal to quickly deploy a development environment.
    - **Azure CLI & PowerShell**: For automation and scripting, VMs can also be created using Azure CLI or PowerShell. This method is ideal for repetitive tasks or complex deployments. For instance, a DevOps engineer might use a script to deploy multiple VMs across different regions for a globally distributed application.
    - **ARM Templates**: Azure Resource Manager (ARM) templates provide infrastructure as code (IaC) capabilities, allowing users to define their VM configurations in JSON files. ARM templates enable consistent and repeatable deployments across environments. For example, a software company might use an ARM template to deploy identical VMs for staging, testing, and production environments.
- **High Availability:**
  - Azure offers several features to enhance the availability of VMs. Availability Sets ensure that VMs are distributed across multiple fault domains and update domains, reducing the impact of hardware failures and maintenance events. For example, an e-commerce platform might use Availability Sets to ensure its web servers remain available during maintenance.
  - **Availability Zones:** For higher levels of resilience, VMs can be deployed across Availability Zones, which are physically separate locations within an Azure region. This configuration protects against datacenter-level failures. For instance, a financial trading application might deploy its critical VMs across different Availability Zones to ensure continuous operation.
- **Scaling:**
  - **Auto-Scaling:** Azure VMs can automatically scale in response to changing demand. For example, during a sales event, an online retailer might configure its VMs to automatically scale out to handle increased web traffic.
  - **Virtual Machine Scale Sets:** This service allows users to deploy and manage a set of identical VMs. Scale sets support autoscaling based on predefined rules or metrics. A gaming company might use a scale set to automatically add more servers as player demand increases.

- **Integration with Other Azure Services:**
  - **Azure Backup:** VMs can be backed up automatically using Azure Backup, ensuring that critical data is protected and recoverable. For example, a law firm might use Azure Backup to regularly back up its legal document management system.
  - **Azure Site Recovery:** Azure VMs can be replicated to a secondary region using Azure Site Recovery, enabling disaster recovery for critical applications. For instance, a healthcare provider might use Site Recovery to ensure that its patient records system remains available during a regional outage.
- **Networking and Security:**
  - **Network Security Groups (NSGs):** Azure VMs can be protected using NSGs, which allow users to control inbound and outbound traffic to and from the VM. For example, a financial institution might use NSGs to restrict access to its VMs based on specific IP addresses or subnets.
  - **Azure Bastion:** Azure Bastion provides secure and seamless RDP and SSH connectivity to VMs directly from the Azure portal without exposing them to the public internet. A company might use Azure Bastion to securely manage its VMs from anywhere in the world.

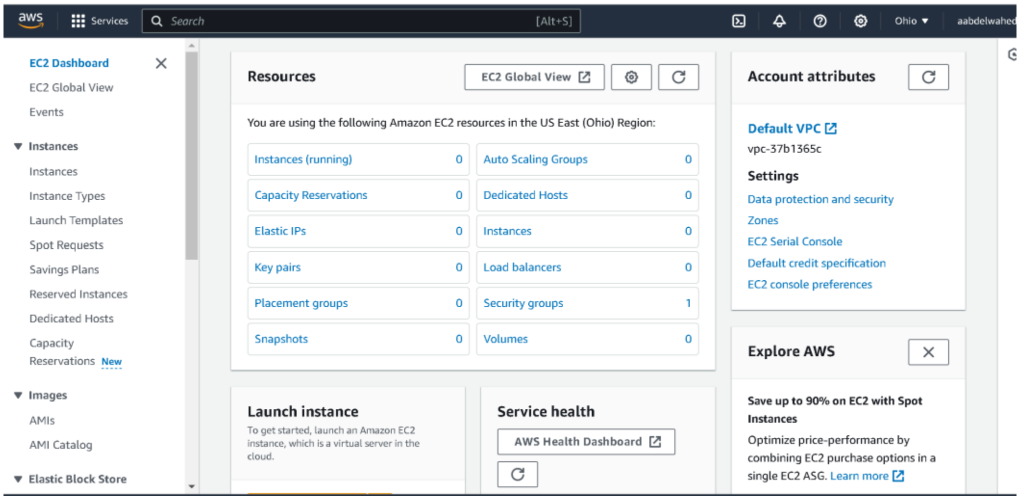


Amazon AWS

- **EC2 Instances:**
  - **Service Overview**: Amazon Elastic Compute Cloud (EC2) provides scalable compute capacity in the AWS cloud. EC2 instances support a wide range of operating systems, including various distributions of Linux and Windows, making it suitable for virtually any workload.
  - **Instance Types**: AWS EC2 offers a broad selection of instance types optimized for different use cases:
    - **General Purpose:** T3, M5 series, suitable for applications that require a balance of compute, memory, and networking. For instance, a startup might use a T3 instance to host its website and small database.
    - **Compute Optimized:** C5 series, ideal for compute-bound applications that benefit from high-performance processors, such as high-performance computing (HPC) tasks. A research lab might use C5 instances for complex simulations.
    - **Memory Optimized:** R5 series, designed for memory-intensive applications, such as databases and real-time big data analytics. A financial services firm might use an R5 instance to run its in-memory database.
    - **Storage Optimized:** I3, D2 series, optimized for applications that require high, sequential read and write access to large datasets on local storage. An analytics company might use I3 instances to process large datasets.
    - **Accelerated Computing:** P3, G4 series, equipped with GPUs for tasks like machine learning, AI, and 3D rendering. A film studio might use G4 instances to render complex visual effects.
  - **Creation Methods**:
    - **AWS Management Console:** Users can launch EC2 instances via the AWS Management Console, selecting from a wide range of AMIs (Amazon Machine Images) and instance types, and configuring networking and security settings. For example, a small business might use the console to launch an EC2 instance to host its CRM application.
    - **AWS CLI:** For automation and bulk operations, EC2 instances can be created using the AWS CLI. This method is often used in scripts and automated workflows. A DevOps team might use the CLI to launch and manage EC2 instances across multiple environments.
    - **CloudFormation:** AWS CloudFormation allows users to define their infrastructure as code using JSON or YAML templates. EC2 instances can be deployed consistently across environments using CloudFormation templates. A software development company might use CloudFormation to deploy and manage a fleet of EC2 instances for testing new software releases.
- **High Availability:**
  - **Auto Scaling Groups (ASGs):** EC2 instances can be organized into Auto Scaling Groups that automatically adjust the number of instances in response to traffic. For instance, an online retailer might use an ASG to automatically scale out EC2 instances during a holiday shopping season.
  - **Multi-AZ Deployments:** EC2 instances can be deployed across multiple Availability Zones within a region, ensuring high availability and resilience against zone failures. For example, a financial application might use Multi-AZ deployments to ensure continuous operation even if one zone goes down.
- **Scaling:**
  - **Elastic Load Balancing (ELB):** ELB distributes incoming application traffic across multiple EC2 instances, providing fault tolerance and improving application availability. A media streaming service might use ELB to manage high volumes of incoming requests.

  - **EC2 Auto Scaling:** EC2 Auto Scaling automatically adjusts the number of instances in an ASG based on demand, ensuring optimal performance and cost-efficiency. For example, a social media platform might scale its EC2 instances up or down based on user activity levels.

- **Integration with Other AWS Services:**
  - **Amazon EBS:** EC2 instances can be paired with Elastic Block Store (EBS) for persistent block storage. EBS volumes can be snapshot and restored independently of the instances. An analytics company might use EBS to store and process large datasets.
  - **AWS Backup:** EC2 instances can be automatically backed up using AWS Backup, providing data protection and disaster recovery capabilities. A healthcare organization might use AWS Backup to ensure the availability of its patient data.
- **Networking and Security:**
  - **Security Groups:** Security Groups in AWS control the inbound and outbound traffic to EC2 instances, acting as a virtual firewall. For instance, a company hosting a web application might use Security Groups to only allow HTTP/HTTPS traffic from specific IP ranges.
  - **AWS Systems Manager:** AWS Systems Manager provides a suite of tools for managing EC2 instances, including patch management, inventory collection, and remote access. A global enterprise might use Systems Manager to ensure all EC2 instances are consistently configured and compliant with security policies.



Resources

You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Instances (running)	0	Auto Scaling Groups	0
Capacity Reservations	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0
Placement groups	0	Security groups	1
Snapshots	0	Volumes	0

Account attributes

Default VPC
vpc-37b1365c

Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences

Explore AWS

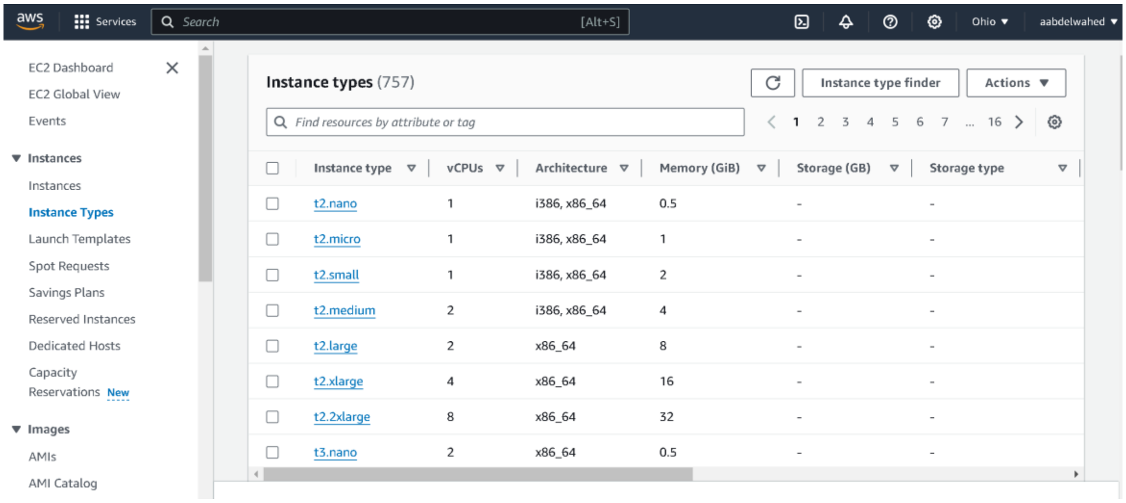
Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Service health



Instance types (757)

□	Instance type	vCPUs	Architecture	Memory (GiB)	Storage (GB)	Storage type
□	t2.nano	1	i386, x86_64	0.5	-	-
□	t2.micro	1	i386, x86_64	1	-	-
□	t2.small	1	i386, x86_64	2	-	-
□	t2.medium	2	i386, x86_64	4	-	-
□	t2.large	2	x86_64	8	-	-
□	t2.xlarge	4	x86_64	16	-	-
□	t2.2xlarge	8	x86_64	32	-	-
□	t3.nano	2	x86_64	0.5	-	-

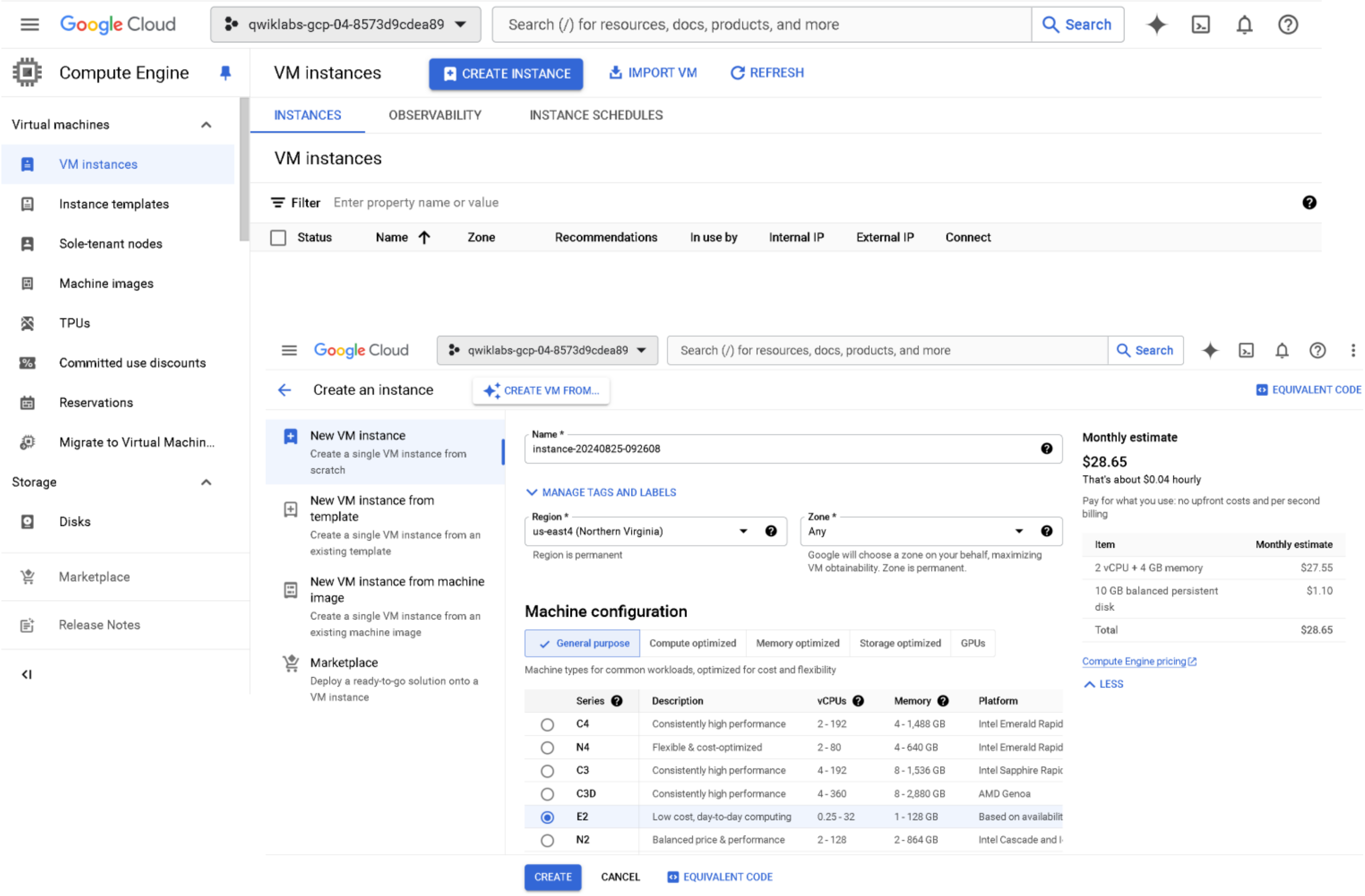
Google Cloud

- **VM Instances:**
  - **Service Overview:** Google Cloud Compute Engine provides scalable and flexible virtual machines that can be customized to fit various workloads, from web hosting to high-performance computing. Compute Engine supports custom machine types, allowing users to tailor CPU, memory, and storage configurations to their specific needs.
  - **Instance Types:**
    - **General Purpose**: E2, N1 series, designed for a balance of performance and cost, suitable for general workloads like web servers and development environments. For example, a startup might use an E2 instance to host its website and development server.
    - **Compute Optimized**: C2 series, ideal for CPU-intensive tasks such as high-performance computing, scientific modeling, and financial risk modeling. A research institution might use C2 instances to run complex simulations.
    - **Memory Optimized**: M1 series, optimized for in-memory databases and large-scale data processing. A large enterprise might use an M1 instance to run SAP HANA for its ERP system.
    - **Accelerator-Optimized**: A2, P4 series, equipped with GPUs for machine learning, artificial intelligence, and 3D visualization. A tech company might use A2 instances for training deep learning models.
  - **Creation Methods:**
    - **Google Cloud Console**: VM instances can be created via the Google Cloud Console, where users can select machine types, images, and customize networking settings. For example, an IT team might use the console to deploy a new application server with specific firewall rules.
    - **gcloud CLI**: The gcloud command-line tool allows users to automate the creation and management of VM instances, making it ideal for scripting and DevOps tasks. A development team might use gcloud to automate the deployment of testing environments.
    - **Deployment Manager**: Google Cloud Deployment Manager is an infrastructure as code service that allows users to define their infrastructure using YAML, Python, or Jinja2 templates. For instance, a software company might use Deployment Manager to provision VM instances and associated resources consistently across environments.
- **High Availability:**
  - **Managed Instance Groups (MIGs):** Google Cloud offers Managed Instance Groups that automatically manage a group of identical VM instances, ensuring high availability and automatic scaling. For example, an online education platform might use MIGs to ensure that additional servers are automatically added as more students access the platform.
  - **Regional Managed Instance Groups:** VMs can be deployed across multiple zones within a region using Regional Managed Instance Groups, providing higher resilience against zonal failures. For instance, a mission-critical application might use Regional MIGs to ensure continuous operation even if one zone experiences an outage.
- **Scaling:**
  - **Autoscaler:** Google Cloud’s Autoscaler adjusts the number of VM instances in response to CPU utilization, load balancing metrics, or custom metrics. For example, an e-commerce website might automatically scale up its VM instances during peak shopping periods.

  - **Global Load Balancing:** Google's global load balancing distributes traffic across multiple regions and VM instances, ensuring low latency and high availability. A multinational SaaS provider might use global load balancing to provide fast and reliable service to users across different continents.

- **Integration with Other Google Cloud Services:**
  - **Persistent Disks:** Google Cloud VMs can be paired with Persistent Disks for high-performance block storage. Persistent Disks can be automatically resized and snapshot for backup. A data analytics firm might use Persistent Disks to store and process large datasets with high I/O requirements.
  - **Google Cloud Backup and DR:** Google Cloud offers integrated backup and disaster recovery solutions for VMs, ensuring business continuity. For instance, a financial institution might use Google Cloud's backup services to protect its transaction processing system.

- **Networking and Security:**
  - **VPC Network:** Google Cloud VMs are deployed within a Virtual Private Cloud (VPC), providing advanced networking features such as subnets, firewall rules, and private access to Google services. For example, a retail company might use a VPC to securely connect its cloud-based inventory system with its on-premises warehouses.
  - **Google Cloud IAM:** Google Cloud's Identity and Access Management (IAM) allows fine-grained access control to VMs and other resources, ensuring that only authorized users can access critical systems. For example, a healthcare provider might use IAM to control who can access sensitive patient data stored on VMs.



VM instances

□	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect

New VM instance
Create a single VM instance from scratch

New VM instance from template
Create a single VM instance from an existing template

New VM instance from machine image
Create a single VM instance from an existing machine image

Marketplace
Deploy a ready-to-go solution onto a VM instance

Name *: instance-20240825-092608

Region *: us-east4 (Northern Virginia)
Region is permanent

Zone *: Any
Google will choose a zone on your behalf, maximizing VM obtainability. Zone is permanent.

Machine configuration

✓ General purpose | Compute optimized | Memory optimized | Storage optimized | GPUs

Machine types for common workloads, optimized for cost and flexibility

	Series	Description	vCPUs	Memory	Platform
○	C4	Consistently high performance	2 - 192	4 - 1,488 GB	Intel Emerald Rapid
○	N4	Flexible & cost-optimized	2 - 80	4 - 640 GB	Intel Emerald Rapid
○	C3	Consistently high performance	4 - 192	8 - 1,536 GB	Intel Sapphire Rapic
○	C3D	Consistently high performance	4 - 360	8 - 2,880 GB	AMD Genoa
●	E2	Low cost, day-to-day computing	0.25 - 32	1 - 128 GB	Based on availabilit
○	N2	Balanced price & performance	2 - 128	2 - 864 GB	Intel Cascade and I

Monthly estimate
$28.65
That's about $0.04 hourly
Pay for what you use: no upfront costs and per second billing

Item	Monthly estimate
2 vCPU + 4 GB memory	$27.55
10 GB balanced persistent disk	$1.10
Total	$28.65

Storage Services

Microsoft Azure

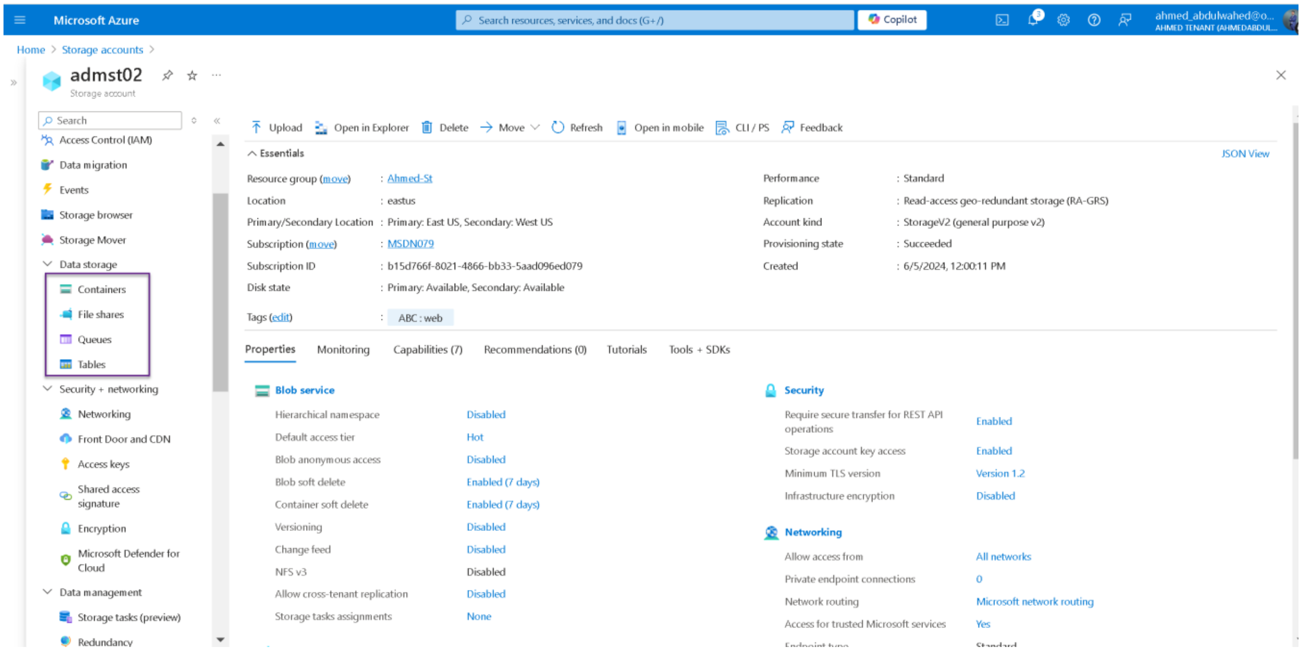
- **Azure Storage Overview**:
  - Azure Storage is a highly scalable, durable, and secure cloud storage solution that provides various data storage options, including object storage, file storage, disk storage, and queue storage. It is designed to handle a wide range of storage needs, from small-scale personal projects to large-scale enterprise applications.
- **Types of Azure Storage:**
  - **Blob Storage:**
    - **Service Overview**: Azure Blob Storage is designed for storing large amounts of unstructured data, such as text or binary data. It is commonly used for serving images, videos, documents, and backups.
    - **Blob Types**: There are three types of blobs in Azure Blob Storage:
      - **Block Blobs**: Optimized for storing large text and binary data, such as documents, images, and videos. For example, a media company might store video files in Block Blobs for streaming to users.
      - **Append Blobs**: Ideal for scenarios where data needs to be appended, such as log files. A web application might use Append Blobs to store logs generated by user activity.
      - **Page Blobs**: Used for storing random access files, such as VHDs (virtual hard disks) used by Azure VMs. A company might store VM images in Page Blobs for quick deployment.
    - **Access Tiers**: Azure Blob Storage supports multiple access tiers, including Hot, Cool, and Archive, allowing cost optimization based on data access patterns. For example, a company might store frequently accessed files in the Hot tier and archive old files in the Archive tier.
  - **File Storage:**
    - **Service Overview**: Azure Files provides fully managed file shares that can be accessed via the Server Message Block (SMB) protocol or Network File System (NFS) protocol. Azure Files is ideal for applications that require shared storage accessible by multiple VMs.
    - **Use Cases**: A company might use Azure Files to provide shared storage for an application running on multiple VMs, ensuring all instances can access the same data.
    - **Azure File Sync**: Azure File Sync allows organizations to centralize their file shares in Azure Files while keeping frequently accessed data cached locally on on-premises servers. For instance, a retail chain might use Azure File Sync to synchronize data across multiple store locations and the cloud.
  - **Disk Storage:**
    - **Service Overview**: Azure Disk Storage provides high-performance block storage for Azure VMs. Disks are managed and can be easily attached to or detached from VMs.
    - **Types of Disks**:
      - **Standard HDD**: Cost-effective storage option for workloads that are not disk I/O intensive. For example, a development environment might use Standard HDDs to reduce costs.
      - **Standard SSD**: Suitable for production workloads requiring consistent performance but not high IOPS. A small web application might use Standard SSDs for its VMs.
      - **Premium SSD**: High-performance SSD storage for mission-critical applications that require low latency and high IOPS. An online transaction processing (OLTP) database might use Premium SSDs to ensure fast transaction processing.

- **Ultra Disk**: Provides the highest performance and lowest latency for Azure VMs, with adjustable IOPS and throughput. Ultra Disk is ideal for data-intensive applications like SAP HANA.

- **Queue Storage:**
  - **Service Overview**: Azure Queue Storage is designed to store and retrieve messages that applications use for communication between components. It is often used in scenarios where application components need to communicate asynchronously.
  - **Use Cases**: A cloud-based order processing system might use Queue Storage to manage the flow of customer orders between different services, ensuring that each order is processed in sequence.

- **Redundancy and Replication Options:**
  - **Locally Redundant Storage (LRS):** Data is replicated three times within a single physical location in the primary region, providing high durability within that location.
  - **Zone-Redundant Storage (ZRS):** Data is replicated synchronously across three different availability zones within a region, ensuring high availability and fault tolerance.
  - **Geo-Redundant Storage (GRS):** Data is replicated to a secondary region, hundreds of miles away from the primary location, providing protection against regional outages.
  - **Read-Access Geo-Redundant Storage (RA-GRS):** Similar to GRS, but with the added capability of read access to the secondary region, providing additional data availability.

- **Integration with Other Azure Services:**
  - **Azure Backup:** Azure Storage integrates with Azure Backup to provide a secure and scalable solution for backing up and restoring data. A healthcare organization might use Azure Backup to protect patient records stored in Blob Storage.
  - **Azure Site Recovery:** Azure Storage can be used with Azure Site Recovery to replicate virtual machines and ensure business continuity in case of disasters. For instance, a financial services firm might use Site Recovery to replicate VMs running critical applications.



Resource group (move) : Ahmed-St
Location : eastus
Primary/Secondary Location : Primary: East US, Secondary: West US
Subscription (move) : MSDN079
Subscription ID : b15d766f-8021-4866-bb33-5aad096ed079
Disk state : Primary: Available, Secondary: Available
Tags (edit) : ABC : web

Performance : Standard
Replication : Read-access geo-redundant storage (RA-GRS)
Account kind : StorageV2 (general purpose v2)
Provisioning state : Succeeded
Created : 6/5/2024, 12:00:11 PM

Blob service

Hierarchical namespace	Disabled
Default access tier	Hot
Blob anonymous access	Disabled
Blob soft delete	Enabled (7 days)
Container soft delete	Enabled (7 days)
Versioning	Disabled
Change feed	Disabled
NFS v3	Disabled
Allow cross-tenant replication	Disabled
Storage tasks assignments	None

Security

Require secure transfer for REST API operations	Enabled
Storage account key access	Enabled
Minimum TLS version	Version 1.2
Infrastructure encryption	Disabled

Networking

Allow access from	All networks
Private endpoint connections	0
Network routing	Microsoft network routing
Access for trusted Microsoft services	Yes
Endpoint type	Standard

Amazon AWS

- **Amazon S3 (Simple Storage Service):**
  - **Service Overview:** Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance. It is designed to store and protect any amount of data for a range of use cases, including backup and restore, archiving, enterprise applications, and big data analytics.
  - **Storage Classes:**
    - **S3 Standard**: Designed for frequently accessed data, providing low latency and high throughput. For example, a media streaming service might store video files in S3 Standard for fast delivery to users.
    - **S3 Intelligent-Tiering**: Automatically moves data between two access tiers (frequent and **infrequent**) based on changing access patterns, optimizing costs. A content management system might use Intelligent-Tiering to store user-generated content.
    - **S3 Standard-IA (Infrequent Access)**: Suitable for data that is accessed less frequently but requires rapid access when needed. A company might use S3 Standard-IA for storing backups that need to be accessed quickly in case of an emergency.
    - **S3 Glacier**: Low-cost storage designed for data archiving and long-term backup. Data retrieval times range from minutes to hours. An insurance company might use S3 Glacier to store historical claim records.
    - **S3 Glacier Deep Archive**: The lowest-cost storage option for data archiving, with retrieval times of up to 12 hours. A research institution might use Glacier Deep Archive to store raw scientific data that needs to be retained for decades.
- **Amazon EFS (Elastic File System):**
  - **Service Overview:** Amazon EFS is a fully managed file storage service that is scalable, elastic, and NFS-compatible. EFS is designed for use with AWS cloud services and on-premises resources, providing a simple interface to create and configure file systems.
  - **Use Cases:** EFS is ideal for applications that require a shared file system, such as web serving, content management, and big data analytics. A web application might use EFS to store and serve static content, ensuring that all instances of the application have access to the same data.
  - **Performance Modes:** EFS offers two performance modes—General Purpose (for latency-sensitive use cases like web servers) and Max I/O (for highly parallelized applications like big data processing).
- **Amazon EBS (Elastic Block Store):**
  - **Service Overview:** Amazon EBS provides block-level storage volumes for use with EC2 instances. EBS volumes are highly available, reliable, and can be attached to a running instance, enabling persistent storage.
  - **Types of EBS Volumes:**
    - **General Purpose SSD (gp2, gp3)**: Balanced performance for a wide range of workloads, such as boot volumes, small databases, and development environments. A small business might use gp3 volumes to store application data and databases.
    - **Provisioned IOPS SSD (io1, io2)**: Designed for I/O-intensive workloads like large databases, offering high throughput and low latency. An enterprise might use io2 volumes to host a high-performance SQL database.
    - **Throughput Optimized HDD (st1)**: Low-cost HDD designed for frequently accessed, throughput-intensive workloads, such as big data processing. A data analytics company might use st1 volumes to store and process large datasets.

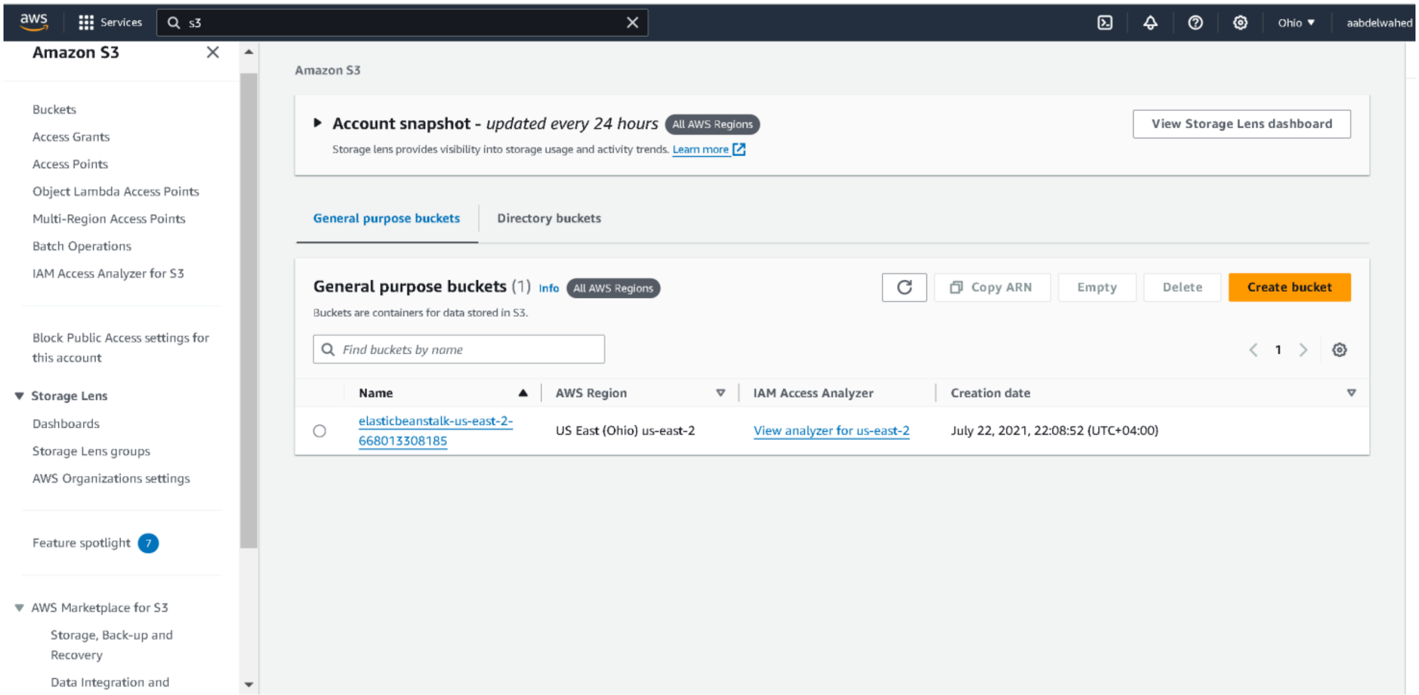
  - **Cold HDD (sc1)**: The lowest-cost HDD storage, suitable for infrequently accessed data. A company might use sc1 volumes for archival storage of log files.

- **Amazon FSx:**

  is a fully managed service that offers two types of file systems: **FSx for Windows File Server**, which provides a Windows-native file system with SMB support, and **FSx for Lustre**, designed for high-performance computing with fast processing of large datasets. Both options are scalable, secure, and integrate with other AWS services. FSx automates administration tasks, offers high performance, and supports a wide range of workloads from enterprise file storage to big data analytics. It's cost-effective, with pricing based on usage.

- **Redundancy and Durability:**
  - **S3 Replication:** S3 supports Cross-Region Replication (CRR) and Same-Region Replication (SRR) to automatically replicate data across different AWS regions or within the same region for compliance or disaster recovery. For instance, a global company might use CRR to replicate critical data to multiple regions.
  - **EBS Snapshots:** EBS volumes can be backed up by taking snapshots, which are stored in S3 and can be used to create new EBS volumes. A company might automate daily EBS snapshots to ensure recoverability of its application data.
  - **Multi-AZ Deployment for EFS:** Amazon EFS automatically stores data across multiple Availability Zones, ensuring high availability and durability. A SaaS provider might use EFS to ensure its application data is always available, even if an AZ fails.

- **Integration with Other AWS Services:**
  - **AWS Backup:** AWS Backup provides centralized backup management across AWS services, including S3, EFS, and RDS. A financial services firm might use AWS Backup to create automated backups of its EBS volumes and RDS databases.
  - **AWS Lambda:** S3 events can trigger AWS Lambda functions, enabling serverless processing of data as it arrives in an S3 bucket. For example, a photo-sharing application might use Lambda to automatically generate thumbnails whenever a new image is uploaded to S3.



Account snapshot - *updated every 24 hours*

Storage lens provides visibility into storage usage and activity trends.

General purpose buckets (1)

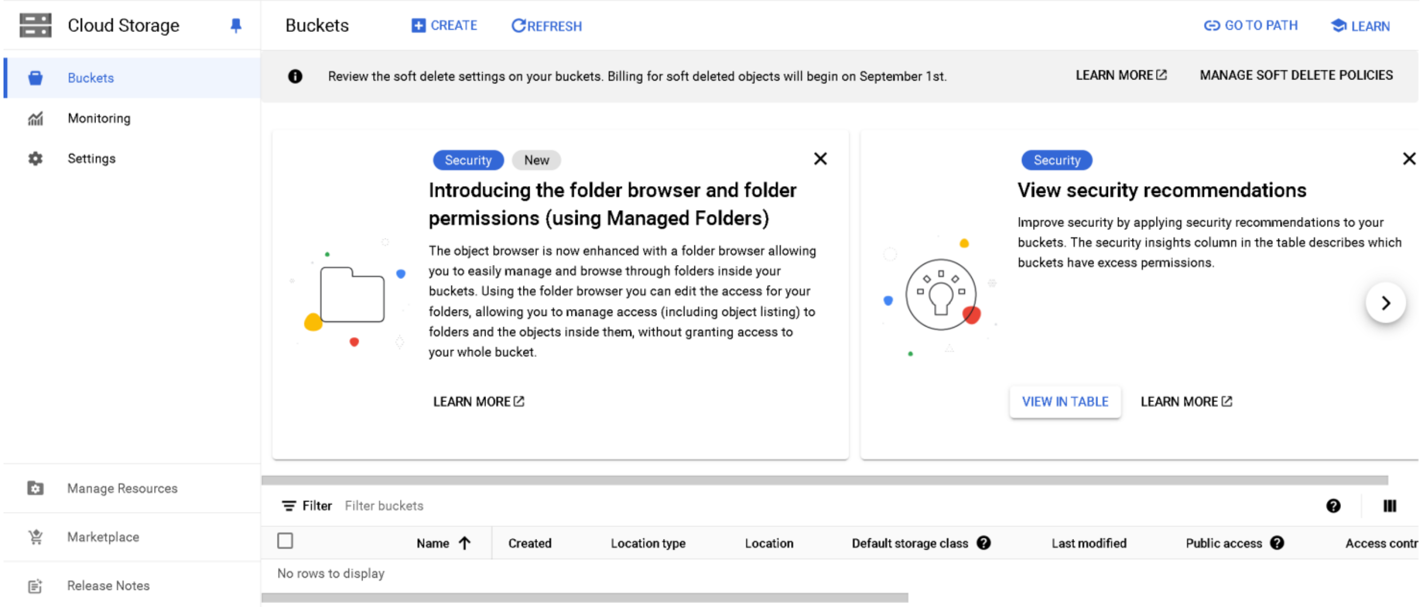
Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	elasticbeanstalk-us-east-2-668013308185	US East (Ohio) us-east-2	View analyzer for us-east-2	July 22, 2021, 22:08:52 (UTC+04:00)

Google Cloud

- **Google Cloud Storage:**
  - **Service Overview:** Google Cloud Storage is a unified object storage service that offers a highly durable, scalable, and secure storage solution for a wide range of data. It supports multiple storage classes, allowing businesses to optimize costs based on data access patterns.
  - **Storage Classes:**
    - **Standard**: For frequently accessed data, providing low latency and high throughput. An e-commerce site might store product images and videos in Standard storage for quick access by customers.
    - **Nearline**: Cost-effective storage for data that is accessed less frequently, typically once a month. A marketing firm might use Nearline storage for quarterly campaign data that needs to be readily accessible but not frequently used.
    - **Coldline**: Designed for data that is accessed infrequently, typically once a year. A healthcare provider might use Coldline to store patient records that are seldom accessed but need to be retained for compliance purposes.
    - **Archive**: The most cost-effective storage for long-term data archiving, suitable for data that is rarely accessed. A university might use Archive storage for archiving research data that needs to be kept for many years.
- **Google Cloud Filestore:**
  - **Service Overview:** Google Cloud Filestore is a fully managed file storage service that provides NFS file shares with high performance and scalability, making it suitable for enterprise applications that require a shared file system.
  - **Use Cases:** Filestore is ideal for workloads like content management, media rendering, and data analytics. A media production company might use Filestore to store and share large video files across multiple rendering nodes.
- **Google Persistent Disks:**
  - **Service Overview:** Google Persistent Disks provide durable and high-performance block storage for Google Compute Engine VMs. Persistent Disks are available in both HDD and SSD options and can be resized without downtime.
  - **Types of Persistent Disks:**
    - **Standard Persistent Disks (HDD)**: Cost-effective storage for workloads that require large amounts of data but do not need high IOPS. For example, a data archiving application might use Standard Persistent Disks for its storage needs.
    - **SSD Persistent Disks**: High-performance storage for workloads that require low latency and high IOPS, such as databases or high-performance applications. A financial trading application might use SSD Persistent Disks to ensure fast access to critical data.
    - **Balanced Persistent Disks**: A middle ground between HDD and SSD, offering a balance of cost and performance for general-purpose workloads. A web application might use Balanced Persistent Disks for its VMs to manage costs while maintaining good performance.

- **Google Cloud Filestore:**
  - **Service Overview:** Google Cloud Filestore is a fully managed file storage service that provides NFS file shares with high performance and scalability, making it suitable for enterprise applications that require a shared file system.
  - **Use Cases:** Filestore is ideal for workloads like content management, media rendering, and data analytics. A media production company might use Filestore to store and share large video files across multiple rendering nodes.
- **Redundancy and Durability:**
  - **Multi-Regional Storage:** Google Cloud Storage offers multi-regional storage that automatically replicates data across multiple locations within a specified region, ensuring high availability and durability. For example, a global media company might store its video content in multi-regional storage to ensure it is available worldwide with minimal latency.
  - **Regional Storage:** Data is stored in a specific geographic location, providing high performance and availability within that region. A European company might choose regional storage within the EU to ensure compliance with GDPR while maintaining high performance.
  - **Zonal Storage:** Designed for workloads that require high availability within a single zone, such as test and development environments. A startup might use zonal storage to reduce costs while developing its application.
- **Integration with Other Google Cloud Services:**
  - **Google Cloud Dataflow:** Google Cloud Storage integrates with Dataflow for serverless data processing, enabling real-time data analytics and ETL workflows. A retail company might use Dataflow to process streaming sales data stored in Google Cloud Storage.
  - **Google Cloud Functions**: Google Cloud Storage can trigger Cloud Functions to execute code in response to changes in data, enabling serverless processing. For example, a content management system might use Cloud Functions to automatically process and categorize new documents uploaded to Cloud Storage.



Review the soft delete settings on your buckets. Billing for soft deleted objects will begin on September 1st.

Introducing the folder browser and folder permissions (using Managed Folders)

The object browser is now enhanced with a folder browser allowing you to easily manage and browse through folders inside your buckets. Using the folder browser you can edit the access for your folders, allowing you to manage access (including object listing) to folders and the objects inside them, without granting access to your whole bucket.

View security recommendations

Improve security by applying security recommendations to your buckets. The security insights column in the table describes which buckets have excess permissions.

□	Name ↑	Created	Location type	Location	Default storage class	Last modified	Public access	Access contr

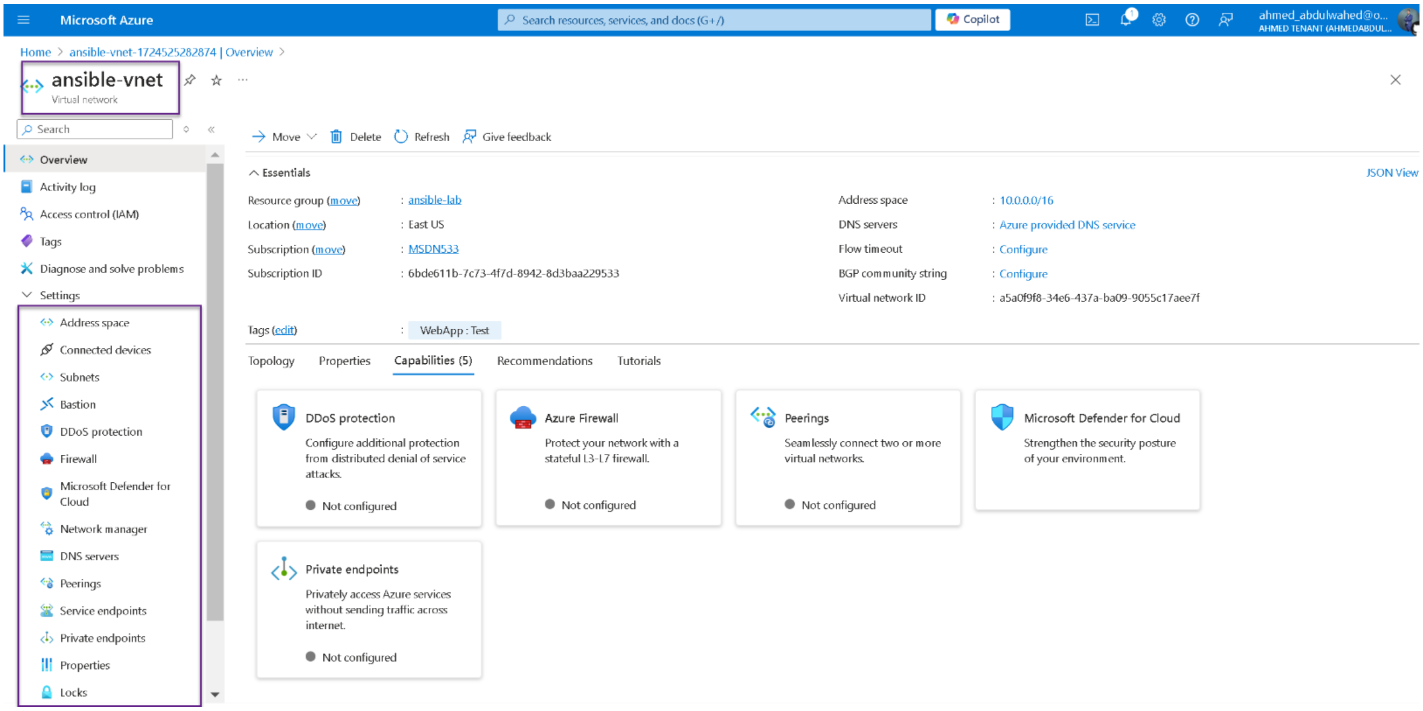
No rows to display

Networking and Connectivity

Microsoft Azure

- **Azure Virtual Network (VNet)**:
  - **Service Overview:** Azure Virtual Network (VNet) is the fundamental building block for private network architecture in Azure. VNets enable Azure resources, such as VMs, to communicate securely with each other, the internet, and on-premises networks.
  - **Subnets:** VNets can be divided into subnets, allowing users to segment the network and allocate specific IP address ranges to different resources. For example, a company might create separate subnets for web servers, application servers, and databases, with each having its own security rules.
  - **Network Security Groups (NSGs):** NSGs allow for the control of inbound and outbound traffic to network interfaces (NICs), VMs, and subnets within a VNet. For instance, an NSG could be configured to allow only HTTP and HTTPS traffic to web servers in a specific subnet.
  - **Peering:** VNet peering enables seamless connectivity between two VNets, whether they are in the same region (intra-region) or different regions (global VNet peering). For example, an organization with VNets in both the East US and West Europe regions could use global VNet peering to facilitate secure communication between resources in these regions.
- **Azure Load Balancer:**
  - **Service Overview:** Azure Load Balancer is a Layer 4 (TCP/UDP) load balancer that distributes incoming network traffic across multiple VMs, ensuring high availability and reliability of applications.
  - **Public and Internal Load Balancers:** Azure provides both public load balancers (for traffic from the internet) and internal load balancers (for traffic within a VNet). For example, a public load balancer might distribute incoming web traffic across a pool of web servers, while an internal load balancer might distribute traffic between application servers.
  - **Health Probes:** Load balancers use health probes to monitor the status of VMs in the backend pool, ensuring traffic is only sent to healthy instances. A web application might use HTTP-based health probes to check the availability of web servers.
- **Azure Application Gateway:**
  - **Service Overview:** Azure Application Gateway is a Layer 7 load balancer that provides advanced routing capabilities for HTTP/HTTPS traffic. It supports features such as SSL termination, URL-based routing, and Web Application Firewall (WAF).
  - **Use Cases:** Application Gateway is ideal for complex web applications that require intelligent traffic routing, such as a multi-tier e-commerce site where traffic needs to be routed based on URL paths to different back-end services.
  - **WAF Integration:** The integrated Web Application Firewall (WAF) helps protect applications from common web vulnerabilities, such as SQL injection and cross-site scripting (XSS). An online banking platform might use WAF to secure its web applications against attacks.
- **Azure VPN Gateway:**
  - **Service Overview:** Azure VPN Gateway provides secure site-to-site VPN connections between Azure VNets and on-premises networks. It supports various VPN protocols, including IPsec and IKE.
  - **Use Cases:** VPN Gateway is commonly used to extend an on-premises network into Azure, allowing secure communication between resources in Azure and on-premises data centers. For example, a company might use VPN Gateway to connect its corporate network to its VMs running in Azure.

- **Azure ExpressRoute:**
  - **Service Overview:** Azure ExpressRoute enables private, dedicated network connections between on-premises infrastructure and Azure, bypassing the public internet. This provides higher security, lower latency, and greater reliability compared to traditional VPN connections.
  - **Use Cases:** ExpressRoute is ideal for scenarios requiring high-throughput, low-latency connectivity, such as data replication, large-scale migrations, and hybrid cloud environments. A financial institution might use ExpressRoute to connect its data center to Azure, ensuring secure and fast communication for critical applications.
- **Azure Traffic Manager:**
  - **Service Overview:** Azure Traffic Manager is a DNS-based traffic load balancer that distributes traffic across multiple endpoints globally. It supports various routing methods, including priority, weighted, and geographic routing.
  - **Use Cases:** Traffic Manager is used to ensure high availability and responsiveness by directing user traffic to the nearest or most appropriate endpoint. For instance, a global e-commerce platform might use Traffic Manager to direct customers to the closest regional datacenter, reducing latency and improving user experience.



ansible-vnet
Virtual network

Resource group (move) : ansible-lab
Location (move) : East US
Subscription (move) : MSDN533
Subscription ID : 6bde611b-7c73-4f7d-8942-8d3baa229533
Address space : 10.0.0.0/16
DNS servers : Azure provided DNS service
Flow timeout : Configure
BGP community string : Configure
Virtual network ID : a5a0f9f8-34e6-437a-ba09-9055c17aee7f
Tags (edit) : WebApp : Test

DDoS protection
Configure additional protection from distributed denial of service attacks.
● Not configured

Azure Firewall
Protect your network with a stateful L3-L7 firewall.
● Not configured

Peerings
Seamlessly connect two or more virtual networks.
● Not configured

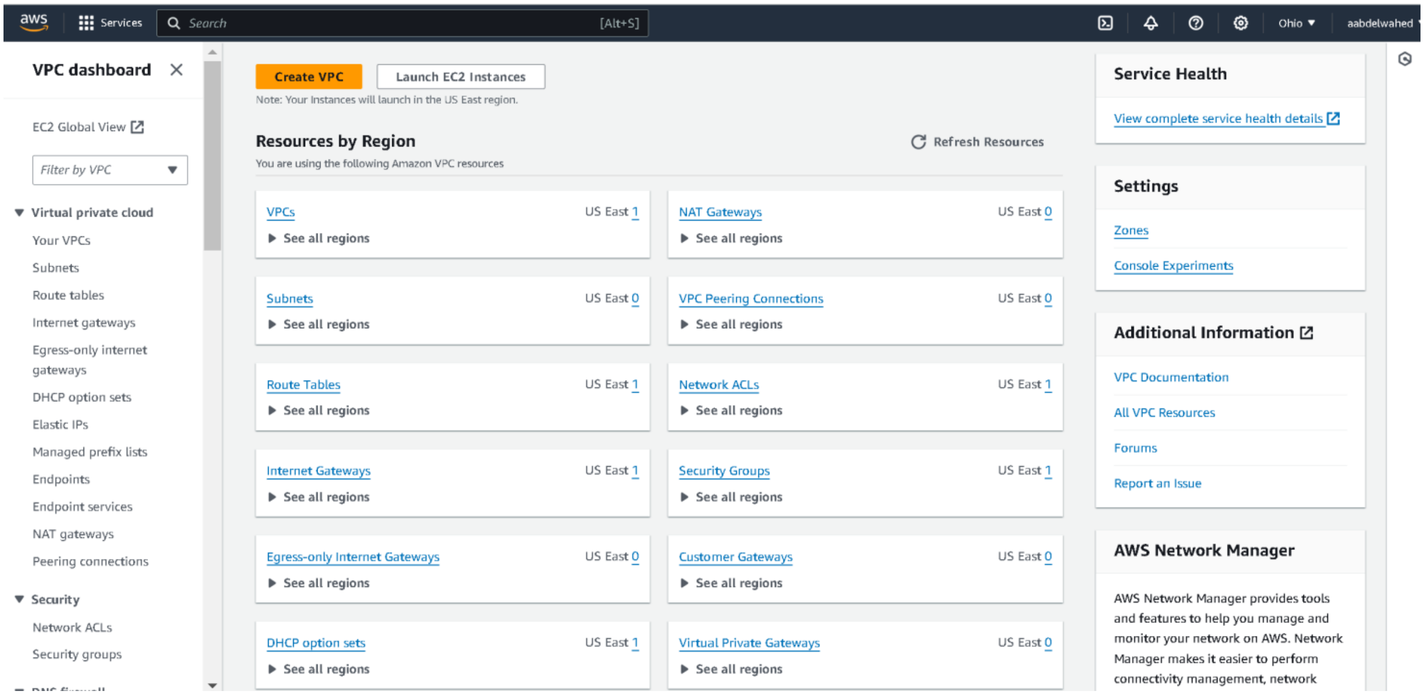
Microsoft Defender for Cloud
Strengthen the security posture of your environment.

Private endpoints
Privately access Azure services without sending traffic across internet.
● Not configured

Amazon AWS

- **Amazon Virtual Private Cloud (VPC):**
  - **Service Overview**: Amazon VPC allows users to provision logically isolated sections of the AWS cloud where they can launch AWS resources in a virtual network defined by the user. VPCs provide full control over IP address ranges, subnets, route tables, and network gateways.
  - **Subnets:** VPCs can be divided into public and private subnets, allowing for segmentation of resources based on their exposure to the internet. For example, public subnets might host web servers accessible from the internet, while private subnets host databases that are only accessible internally.
  - **Security Groups and Network ACLs:** Security Groups act as virtual firewalls controlling inbound and outbound traffic at the instance level, while Network ACLs provide similar control at the subnet level. A company might use Security Groups to permit specific traffic types to its web servers and use Network ACLs to block unauthorized access across the subnet.
- **Elastic Load Balancing (ELB):**
  - **Service Overview:** ELB automatically distributes incoming application traffic across multiple targets, such as EC2 instances, containers, and IP addresses, across multiple Availability Zones.
  - **Types of Load Balancers:**
    - **Application Load Balancer (ALB)**: Operates at Layer 7 and is best suited for load balancing HTTP and HTTPS traffic. It supports features like host-based routing, path-based routing, and Web Application Firewall (WAF) integration. A microservices architecture might use ALB to route requests to specific services based on URL paths.
    - **Network Load Balancer (NLB)**: Operates at Layer 4 and is designed for ultra-low latency and high throughput, making it ideal for load balancing TCP/UDP traffic. A gaming platform might use NLB to manage large volumes of real-time game data.
    - **Classic Load Balancer (CLB)**: Operates at both Layer 4 and Layer 7, providing basic load balancing for HTTP/HTTPS and TCP traffic. CLB is often used in legacy applications.
- **AWS Direct Connect:**
  - **Service Overview:** AWS Direct Connect provides dedicated network connections between a customer’s on-premises data center and AWS, bypassing the public internet to offer lower latency and higher security.
  - **Use Cases:** Direct Connect is used for applications that require stable, high-bandwidth connections to AWS, such as real-time data processing, financial services, and hybrid cloud deployments. A media company might use Direct Connect to transfer large video files to AWS for processing.
- **AWS Transit Gateway:**
  - **Service Overview:** AWS Transit Gateway enables customers to connect multiple VPCs, AWS accounts, and on-premises networks to a single gateway. It simplifies network architecture by acting as a hub for all network traffic.
  - **Use Cases:** Transit Gateway is ideal for large enterprises that need to manage complex networking across multiple regions, accounts, or hybrid environments. For example, a global enterprise might use Transit Gateway to centralize network management across its AWS environments and data centers.

- **Amazon Route 53:**
  - **Service Overview:** Amazon Route 53 is a highly available and scalable DNS web service designed to route end-user requests to appropriate endpoints based on factors such as latency, health, and geographic location.
  - **Use Cases:** Route 53 can be used for domain registration, DNS traffic management, and health checks. A global website might use Route 53 to route users to the closest AWS region to minimize latency and improve performance.
- **AWS VPN**:
  - **Service Overview:** AWS VPN establishes secure connections between on-premises networks and AWS VPCs using IPsec tunnels. It includes AWS Site-to-Site VPN and AWS Client VPN.
  - **Use Cases:** AWS VPN is commonly used to extend on-premises networks into AWS, providing secure, encrypted communications. A remote workforce might use AWS Client VPN to securely access corporate resources hosted in AWS.



Note: Your instances will launch in the US East region.

Resources by Region

You are using the following Amazon VPC resources

VPCs ▶ See all regions	US East 1	NAT Gateways ▶ See all regions	US East 0
Subnets ▶ See all regions	US East 0	VPC Peering Connections ▶ See all regions	US East 0
Route Tables ▶ See all regions	US East 1	Network ACLs ▶ See all regions	US East 1
Internet Gateways ▶ See all regions	US East 1	Security Groups ▶ See all regions	US East 1
Egress-only Internet Gateways ▶ See all regions	US East 0	Customer Gateways ▶ See all regions	US East 0
DHCP option sets ▶ See all regions	US East 1	Virtual Private Gateways ▶ See all regions	US East 0

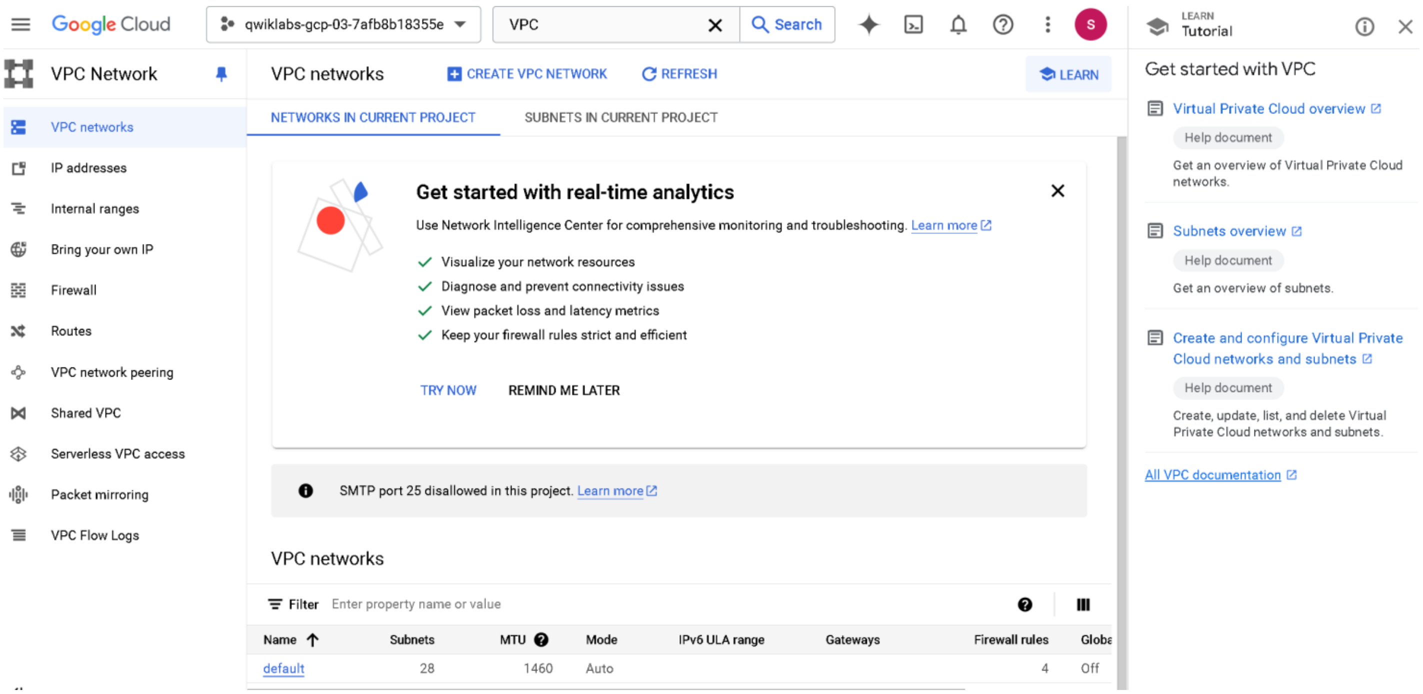
AWS Network Manager

AWS Network Manager provides tools and features to help you manage and monitor your network on AWS. Network Manager makes it easier to perform connectivity management, network

Google Cloud

- **Google Cloud Virtual Private Cloud (VPC)**:
  - **Service Overview:** Google Cloud VPC provides a global, scalable, and flexible network that allows customers to connect Google Cloud resources across regions using a private IP address space. VPCs are global in scope but can be segmented into regional subnets.
  - **Subnets:** VPCs can have subnets that span multiple regions, enabling a global architecture while maintaining regional isolation for resources. For instance, an organization might deploy a multi-region application with subnets in both the US and Europe for redundancy and low latency.
  - **Firewall Rules:** Google Cloud VPC includes firewall rules that can be applied globally or to specific subnets, controlling inbound and outbound traffic. A company might configure firewall rules to restrict access to sensitive data stored in a private subnet.
- **Google Cloud Load Balancing:**
  - **Service Overview:** Google Cloud Load Balancing is a fully distributed, software-defined managed service that supports load balancing across multiple regions and various protocols, including HTTP(S), TCP/SSL, and UDP.
  - **Types of Load Balancers:**
    - **HTTP(S) Load Balancer**: A global, Layer 7 load balancer that distributes traffic across multiple backend services and regions, supporting advanced features like URL routing, SSL offloading, and Google Cloud Armor integration. For example, a global e-commerce platform might use HTTP(S) Load Balancer to route traffic to the nearest regional backend for fast content delivery.
    - **TCP/SSL Load Balancer**: Operates at Layer 4, balancing TCP and SSL traffic across backend instances within a single region. This type of load balancer is suitable for non-HTTP traffic such as gaming and VoIP applications.
    - **Internal Load Balancer**: Provides private, regional load balancing for internal workloads within a VPC. An enterprise application might use Internal Load Balancer to distribute traffic among backend services within a secure VPC.
- **Google Cloud Interconnect:**
  - **Service Overview:** Google Cloud Interconnect provides dedicated, high-bandwidth connectivity between on-premises data centers and Google Cloud, ensuring low latency and secure communication. It includes Dedicated Interconnect and Partner Interconnect options.
  - **Use Cases:** Interconnect is ideal for enterprises that require high-performance, reliable connections for data-intensive applications, such as media production or large-scale data migrations. A financial firm might use Dedicated Interconnect for secure, low-latency connections to its Google Cloud-hosted trading systems.
- **Google Cloud VPN:**
  - **Service Overview:** Google Cloud VPN provides secure IPsec tunnels to connect on-premises networks or other cloud environments to Google Cloud VPCs. It supports both high-availability (HA) VPN for critical workloads and classic VPN for general use.
  - **Use Cases:** Cloud VPN is often used to extend on-premises networks into Google Cloud, enabling secure, encrypted communication. For instance, a manufacturing company might use Cloud VPN to securely connect its on-premises ERP system to Google Cloud resources.

- **Google Cloud Armor:**
  - **Service Overview:** Google Cloud Armor is a security service that provides DDoS protection and WAF capabilities for Google Cloud Load Balancing. It allows users to define security policies that filter traffic based on IP addresses, geolocation, and Layer 7 application data.
  - **Use Cases:** Cloud Armor is essential for protecting web applications from common threats like DDoS attacks and SQL injection. An online gaming platform might use Cloud Armor to safeguard against malicious traffic, ensuring uninterrupted service for its users.
- **Google Cloud DNS:**
  - **Service Overview:** Google Cloud DNS is a scalable, reliable, and managed DNS service that allows users to publish and manage DNS zones and records using Google's infrastructure.
  - **Use Cases:** Google Cloud DNS is used for domain name resolution, supporting both internal and public DNS records. A SaaS provider might use Cloud DNS to manage domain names for its customer-facing applications, ensuring high availability and low latency.
- **Google Cloud Network Connectivity Center:**
  - **Service Overview**: Network Connectivity Center offers a unified view and control over global networking by connecting Google Cloud, on-premises, and other cloud networks through a central hub.
  - **Use Cases:** Ideal for complex hybrid and multi-cloud environments, where centralizing network management and connectivity is crucial. A global enterprise might use Network Connectivity Center to connect and manage its diverse network infrastructure across multiple regions and cloud providers.



Get started with real-time analytics

Use Network Intelligence Center for comprehensive monitoring and troubleshooting. Learn more

- ✓ Visualize your network resources
- ✓ Diagnose and prevent connectivity issues
- ✓ View packet loss and latency metrics
- ✓ Keep your firewall rules strict and efficient

SMTP port 25 disallowed in this project. Learn more

VPC networks

Name ↑	Subnets	MTU	Mode	IPv6 ULA range	Gateways	Firewall rules	Globa
default	28	1460	Auto			4	Off

Get started with VPC

Virtual Private Cloud overview
Help document
Get an overview of Virtual Private Cloud networks.

Subnets overview
Help document
Get an overview of subnets.

Create and configure Virtual Private Cloud networks and subnets
Help document
Create, update, list, and delete Virtual Private Cloud networks and subnets.

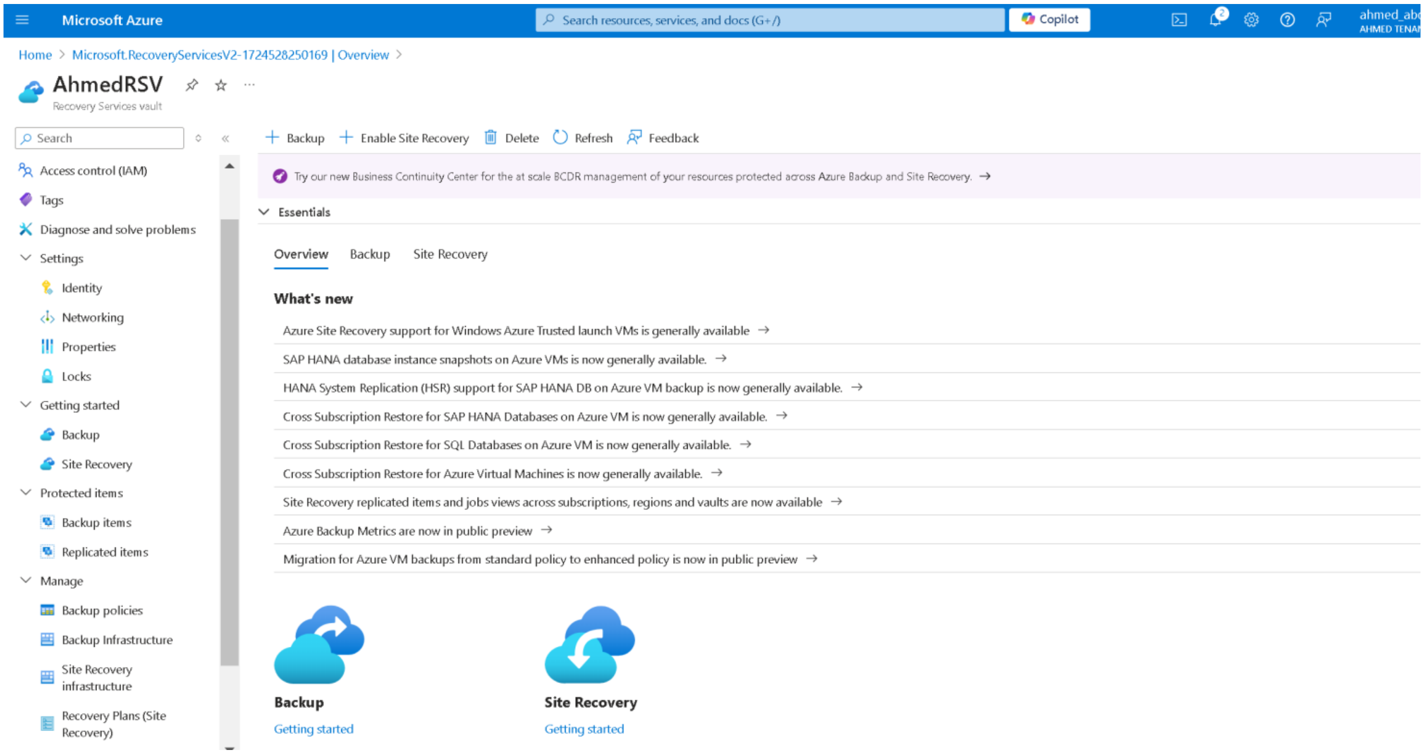
All VPC documentation

Backup and Recovery

Microsoft Azure

- **Azure Backup**:
  - **Service Overview:** Azure Backup is a scalable, secure, and reliable service that provides backup and restore capabilities for on-premises, Azure-based, and hybrid cloud environments. It helps protect against data loss by backing up files, folders, VMs, applications, and databases.
  - **Key Features:**
    - **Azure VM Backup**: Azure Backup provides backup services for Azure VMs by capturing consistent snapshots of the VM, including its operating system, system state, and data. For example, a business might schedule daily backups of its critical VMs to ensure data is protected against accidental deletions or ransomware attacks.
    - **Azure File Share Backup**: Protects data stored in Azure File shares, enabling recovery of individual files or entire shares. An organization using Azure Files for shared document storage might use this feature to regularly back up its file shares.
    - **SQL Server Backup**: Azure Backup supports backing up SQL Server databases running on Azure VMs, ensuring application-consistent backups that can be restored as needed. A financial institution might use this feature to safeguard its transaction databases.
    - **Long-Term Retention**: Supports long-term retention of backups, enabling compliance with regulatory requirements by keeping backups for months or years. For instance, a healthcare provider might retain patient data backups for several years to comply with legal mandates.
    - **Incremental Backups**: Azure Backup uses incremental backups, storing only the changes since the last backup, reducing storage costs and speeding up the backup process. A company might benefit from incremental backups by minimizing the impact on network bandwidth and storage consumption.
- **Azure Site Recovery (ASR):**
  - **Service Overview:** Azure Site Recovery (ASR) is a disaster recovery service that helps ensure business continuity by replicating workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. In the event of a disruption at the primary site, services can be quickly restored in the secondary location.
  - **Key Features:**
    - **Automated Disaster Recovery**: ASR automates the failover and failback process, reducing downtime and ensuring rapid recovery of critical applications. For example, an e-commerce platform might use ASR to replicate its VMs to a secondary region, ensuring minimal downtime in case of a regional outage.
    - **Replication for VMs**: Supports replication of both Azure VMs and on-premises VMs to Azure, allowing for flexible disaster recovery strategies. A hybrid cloud setup might replicate on-premises VMs to Azure to enable recovery in case of local data center failures.
    - **Application-Consistent Snapshots**: Ensures that application data is consistent across multiple VMs during replication, providing reliable recovery points. For instance, an organization running a multi-tier application might use ASR to ensure all components are consistently backed up and recoverable.
    - **Compliance and Retention**: ASR supports compliance requirements by offering retention policies for recovery points, ensuring data is available for the required duration. A financial services firm might configure ASR to retain recovery points for a specified period to meet regulatory needs.

- **Azure Archive Storage:**
  - **Service Overview:** Azure Archive Storage provides a low-cost, long-term storage solution for data that is rarely accessed but must be retained for long periods. It is ideal for archival storage of compliance data, backup data, and other infrequently accessed datasets.
  - **Key Features**:
    - **Cost-Effective Storage**: Archive Storage is designed for cost efficiency, making it a suitable option for storing large volumes of data that do not require frequent access. An organization might use Archive Storage to store historical data that needs to be preserved for regulatory reasons but is not needed for day-to-day operations.
    - **Data Retrieval Options**: Archive Storage supports multiple retrieval options, including standard retrieval (within hours) and expedited retrieval (within minutes), depending on the urgency of data access. A legal firm might use expedited retrieval to quickly access archived case files when needed.



Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery. →

What's new

Azure Site Recovery support for Windows Azure Trusted launch VMs is generally available →

SAP HANA database instance snapshots on Azure VMs is now generally available. →

HANA System Replication (HSR) support for SAP HANA DB on Azure VM backup is now generally available. →

Cross Subscription Restore for SAP HANA Databases on Azure VM is now generally available. →

Cross Subscription Restore for SQL Databases on Azure VM is now generally available. →

Cross Subscription Restore for Azure Virtual Machines is now generally available. →

Site Recovery replicated items and jobs views across subscriptions, regions and vaults are now available →

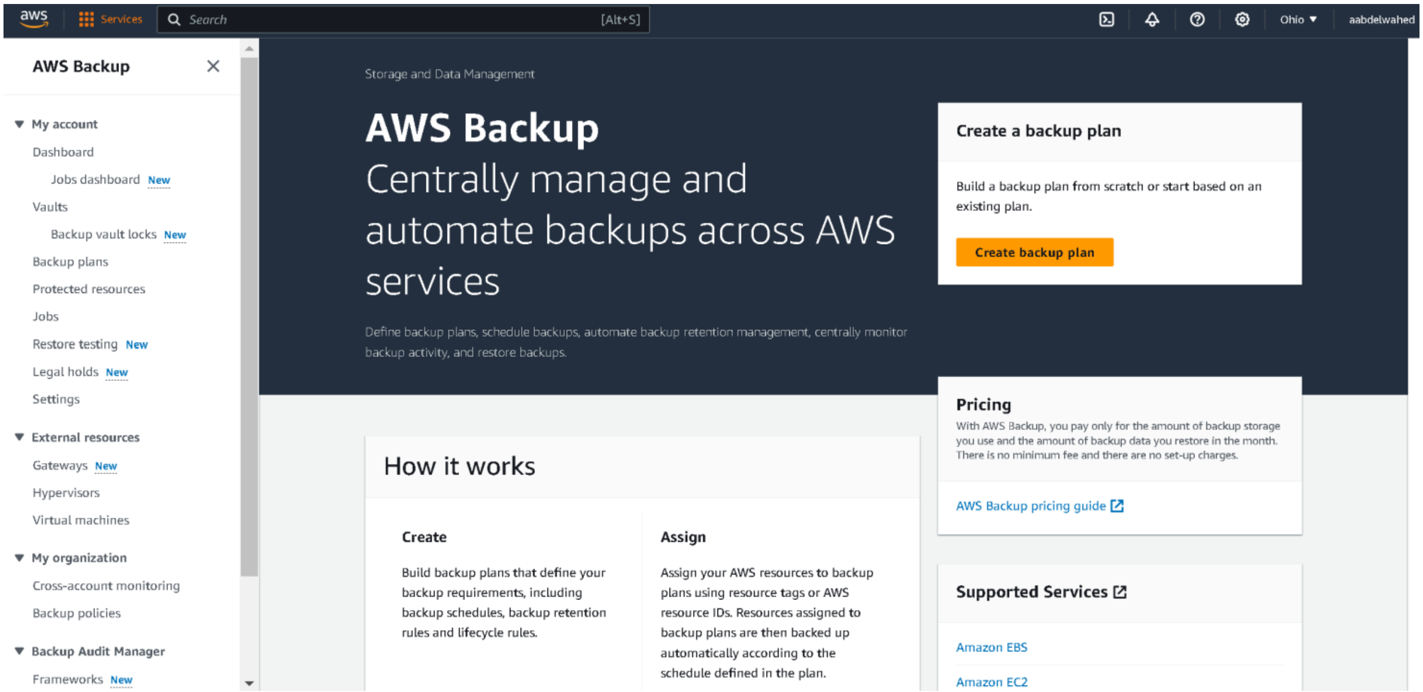
Azure Backup Metrics are now in public preview →

Migration for Azure VM backups from standard policy to enhanced policy is now in public preview →

Amazon AWS

- **AWS Backup**:
  - **Service Overview:** AWS Backup is a fully managed service that automates and centralizes the backup of data across AWS services, including Amazon EBS, Amazon RDS, Amazon DynamoDB, Amazon EFS, and AWS Storage Gateway. It provides a unified backup strategy for diverse workloads.
  - **Key Features:**
    - **Centralized Backup Management**: AWS Backup offers a single interface to manage backups across multiple AWS services, streamlining backup operations and ensuring consistent policies. A large enterprise might use AWS Backup to manage backup schedules for its diverse AWS resources from a central location.
    - **Automated Backup Scheduling**: Supports automated backup schedules based on user-defined policies, ensuring that backups are performed regularly without manual intervention. A healthcare provider might schedule daily backups of its patient records stored in RDS.
    - **Lifecycle Management**: Enables automated transition of backups from frequent access storage tiers to infrequent access or archival tiers, optimizing costs. A company might move older backups to lower-cost storage like S3 Glacier after a certain retention period.
    - **Compliance and Retention Policies**: AWS Backup supports compliance by allowing users to define retention policies, ensuring backups are retained for the required duration and automatically deleted afterward. A financial institution might configure retention policies to keep backups for seven years as required by regulations.
- **AWS Elastic Disaster Recovery (DRS):**
  - **Service Overview:** AWS Elastic Disaster Recovery is a service that helps organizations minimize downtime and data loss by replicating on-premises servers or AWS EC2 instances to a disaster recovery site in another AWS region. It supports continuous data replication and orchestrated recovery processes.
  - **Key Features:**
    - **Continuous Data Replication**: Ensures that data is continuously replicated from the source to the recovery site, providing up-to-date recovery points in the event of a disaster. A global retail chain might use DRS to replicate its transactional data to a secondary region for disaster recovery.
    - **Automated Recovery**: DRS automates the failover process, enabling quick recovery with minimal downtime. For example, a SaaS provider might use DRS to ensure that its services can be quickly restored in another region if the primary region experiences an outage.
    - **Non-Disruptive Testing**: Allows organizations to perform disaster recovery tests without impacting production environments, ensuring that recovery plans work as expected. A financial services firm might conduct regular DR tests to verify its readiness for an actual disaster event.
    - **Cross-Region Replication**: Supports cross-region replication, allowing organizations to choose a geographically distant AWS region for disaster recovery. A multinational company might replicate its mission-critical applications to a different continent to ensure resilience against regional disasters.
- **Amazon S3 Glacier and S3 Glacier Deep Archive:**
  - **Service Overview:** Amazon S3 Glacier and S3 Glacier Deep Archive are designed for long-term, archival storage of infrequently accessed data. These services offer a low-cost solution for preserving data over extended periods, with varying retrieval options based on urgency.

- **Key Features:**
  - **Cost-Effective Archival Storage**: S3 Glacier is optimized for cost, making it suitable for storing large amounts of data that are rarely accessed but must be retained for compliance or historical purposes. An enterprise might store years of transactional logs in S3 Glacier.
  - **Retrieval Options**: S3 Glacier offers three retrieval options: expedited (1-5 minutes), standard (3-5 hours), and bulk (5-12 hours), allowing flexibility based on the retrieval urgency. For instance, a research institution might use expedited retrieval to quickly access archived datasets needed for a new study.
  - **S3 Glacier Deep Archive**: Provides the lowest-cost storage option for data that is rarely accessed, with retrieval times of up to 12 hours. A government agency might use Glacier Deep Archive to store historical records that need to be preserved indefinitely.



Storage and Data Management

AWS Backup

Centrally manage and automate backups across AWS services

Define backup plans, schedule backups, automate backup retention management, centrally monitor backup activity, and restore backups.

Create a backup plan

Build a backup plan from scratch or start based on an existing plan.

Pricing

With AWS Backup, you pay only for the amount of backup storage you use and the amount of backup data you restore in the month. There is no minimum fee and there are no set-up charges.

How it works

Create

Build backup plans that define your backup requirements, including backup schedules, backup retention rules and lifecycle rules.

Assign

Assign your AWS resources to backup plans using resource tags or AWS resource IDs. Resources assigned to backup plans are then backed up automatically according to the schedule defined in the plan.

Supported Services

Google Cloud

- **Google Cloud Backup and DR:**
  - **Service Overview:** Google Cloud Backup and DR is a fully managed, centralized service that offers backup and disaster recovery capabilities for Google Cloud workloads, including Compute Engine, Cloud SQL, and Google Kubernetes Engine (GKE).
  - **Key Features:**
    - **Centralized Management**: Provides a unified platform for managing backups and disaster recovery, simplifying the process of protecting critical workloads. An organization might use this service to manage the backups of its entire cloud infrastructure from a single console.
    - **Automated Backup Scheduling**: Supports automated, policy-based backup scheduling, ensuring that backups are regularly performed according to organizational requirements. A tech startup might schedule nightly backups of its GKE clusters to ensure business continuity.
    - **Cross-Region Replication**: Enables cross-region replication of backups, ensuring that data is available even if a regional disaster occurs. A multinational company might replicate its backups to multiple Google Cloud regions to safeguard against data loss.
    - **Granular Recovery Options**: Offers granular recovery options, allowing users to restore entire environments or specific components, such as individual VMs, databases, or application configurations. A financial services firm might use granular recovery to restore a specific database instance without affecting the entire system.
- **Google Cloud Disaster Recovery:**
  - **Service Overview:** Google Cloud provides disaster recovery solutions that help organizations maintain business continuity by replicating workloads across multiple regions, enabling rapid recovery in the event of a disaster.
  - **Key Features:**
    - **Multi-Region Deployment**: Supports deploying applications across multiple regions to ensure high availability and resilience. A global e-commerce platform might deploy its application across several regions to ensure customers can always access the service, even during regional outages.
    - **Snapshot and Restore**: Provides snapshot capabilities for Google Cloud resources, enabling quick restoration of data in the event of accidental deletion or corruption. A development team might use snapshots to recover a VM instance that was mistakenly deleted during testing.
    - **Automated Failover**: Automates the failover process to a secondary region in the event of a disaster, reducing downtime and ensuring that services remain operational. A healthcare provider might configure automated failover for its patient management system to ensure uninterrupted access to critical data.
    - **Compliance and Retention**: Google Cloud offers retention policies that align with compliance requirements, ensuring that backups are kept for the required duration. A law firm might configure retention policies to retain client records for a specific period in compliance with legal regulations.

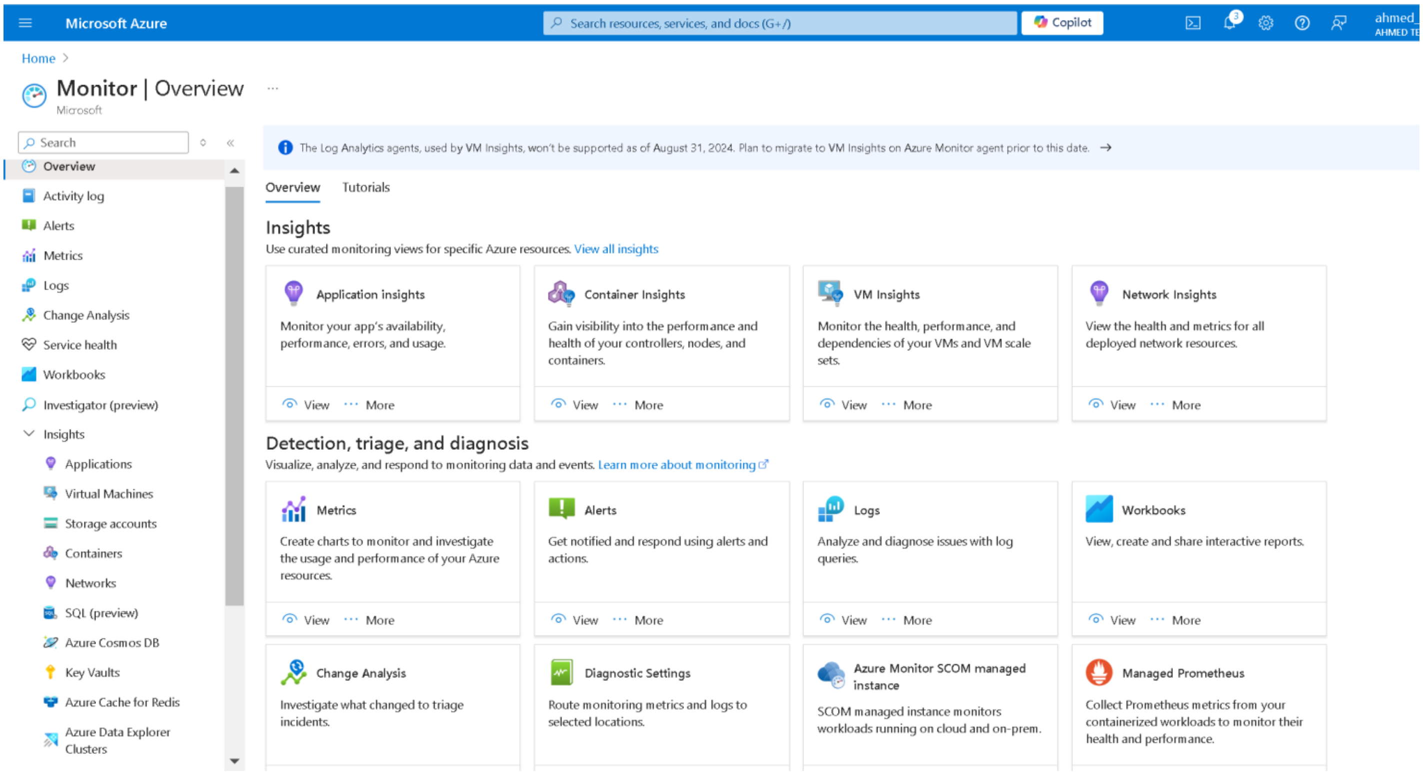
- **Google Cloud Storage - Nearline, Coldline, and Archive:**
  - **Service Overview:** Google Cloud Storage offers multiple storage classes, including Nearline, Coldline, and Archive, providing cost-effective solutions for backing up and archiving data with varying access frequencies.
  - **Key Features**:
    - **Nearline Storage**: Designed for data that is accessed less frequently, typically once a month. Ideal for backups and long-term storage of infrequently accessed data. For instance, a marketing firm might use Nearline to store monthly campaign data.
    - **Coldline Storage**: Optimized for data that is accessed less frequently, typically once a year, offering lower costs than Nearline. A media company might use Coldline to store archived video footage that is rarely accessed but must be retained.
    - **Archive Storage**: The most cost-effective option for long-term data retention, suitable for data that is rarely accessed. A university might use Archive Storage to retain historical research data that needs to be preserved for decades.

Monitoring and Alerts

Microsoft Azure

- **Azure Monitor**:
  - **Service Overview:** Azure Monitor is a comprehensive monitoring service that provides full visibility into the performance and health of your applications and infrastructure. It collects and analyzes telemetry data from Azure resources, on-premises environments, and hybrid clouds.
  - **Key Features:**
    - **Metrics**: Azure Monitor collects real-time metrics from Azure resources, providing insights into resource utilization, performance, and operational health. For example, an IT administrator might monitor the CPU usage of VMs to ensure they are not over or under-utilized.
    - **Logs**: Azure Monitor aggregates log data from various sources, such as Azure services, applications, and operating systems, enabling detailed analysis and troubleshooting. A development team might use log analytics to diagnose issues with a web application.
    - **Application Insights**: A feature of Azure Monitor, Application Insights provides deep insights into application performance, helping developers detect and diagnose issues in real time. For example, a SaaS provider might use Application Insights to monitor response times and error rates in their application.
    - **Log Analytics**: Azure Monitor’s Log Analytics workspace enables advanced querying and visualization of log data, helping teams identify patterns, anomalies, and trends. A security team might use Log Analytics to detect suspicious activity across their infrastructure.
- **Azure Alerts:**
  - **Service Overview:** Azure Alerts allow users to set up automatic notifications and actions based on metrics, logs, or health events within Azure Monitor. Alerts can be configured to notify users via email, SMS, or integrated with external systems like ITSM tools.
  - **Key Features:**
    - **Metric Alerts**: Trigger alerts based on specific metric thresholds, such as CPU usage exceeding 80% or disk space falling below a certain level. For example, an administrator might set up a metric alert to receive notifications when a VM’s CPU usage consistently exceeds 85%.
    - **Log Alerts**: Alerts can be configured based on queries run against log data. For instance, an alert might be triggered if there are repeated failed login attempts within a certain time frame, indicating a potential security threat.
    - **Action Groups**: Action Groups define the set of actions that should be taken when an alert is triggered. These can include sending notifications, running an Azure Logic App, or invoking an Azure Automation runbook. For example, a company might configure an Action Group to automatically scale out additional VMs when a specific load threshold is reached.
    - **Smart Alerts**: Azure Monitor can use machine learning to detect anomalies in metrics and trigger alerts when unusual patterns are detected, even if predefined thresholds are not breached. This can help identify emerging issues before they become critical.

- **Azure Service Health:**
  - **Service Overview:** Azure Service Health provides personalized alerts and guidance when Azure service issues affect your resources. It helps organizations stay informed about service disruptions, planned maintenance, and other important events.
  - **Key Features:**
    - **Service Issues**: Alerts users to ongoing service issues that may impact their Azure resources, providing updates and workarounds as available. For example, an administrator might receive a notification about a regional outage affecting Azure SQL Database.
    - **Planned Maintenance**: Informs users about upcoming maintenance events that may impact **service** availability, allowing them to plan accordingly. A company might receive advance notice about a scheduled update to the Azure VMs hosting their applications.
    - **Health Advisories**: Provides proactive alerts about potential issues that could impact service performance, such as outdated software versions or deprecated features. An IT team might receive a health advisory suggesting updates to their VM images to avoid compatibility issues with upcoming platform changes.



Monitor | Overview

Microsoft

The Log Analytics agents, used by VM Insights, won't be supported as of August 31, 2024. Plan to migrate to VM Insights on Azure Monitor agent prior to this date. →

Insights

Use curated monitoring views for specific Azure resources. View all insights

Application insights: Monitor your app's availability, performance, errors, and usage.

Container Insights: Gain visibility into the performance and health of your controllers, nodes, and containers.

VM Insights: Monitor the health, performance, and dependencies of your VMs and VM scale sets.

Network Insights: View the health and metrics for all deployed network resources.

Detection, triage, and diagnosis

Visualize, analyze, and respond to monitoring data and events. Learn more about monitoring

Metrics: Create charts to monitor and investigate the usage and performance of your Azure resources.

Alerts: Get notified and respond using alerts and actions.

Logs: Analyze and diagnose issues with log queries.

Workbooks: View, create and share interactive reports.

Change Analysis: Investigate what changed to triage incidents.

Diagnostic Settings: Route monitoring metrics and logs to selected locations.

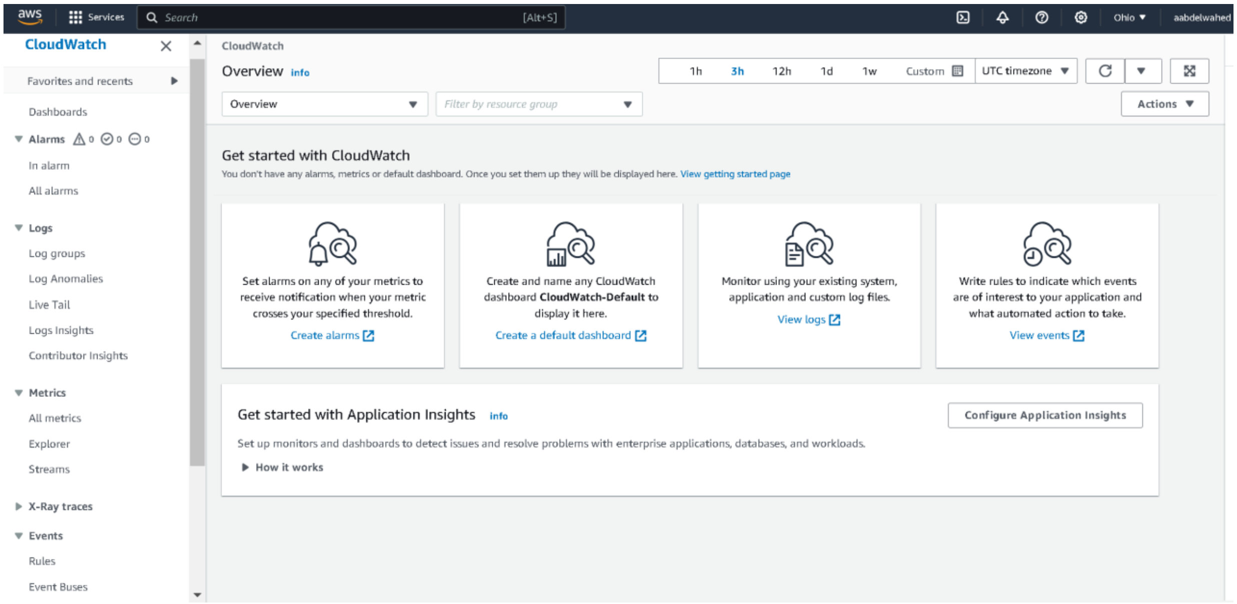
Azure Monitor SCOM managed instance: SCOM managed instance monitors workloads running on cloud and on-prem.

Managed Prometheus: Collect Prometheus metrics from your containerized workloads to monitor their health and performance.

Amazon AWS

- **Amazon CloudWatch:**
  - **Service Overview:** Amazon CloudWatch is a monitoring and observability service that provides data and actionable insights for AWS resources, applications, and services. It enables users to collect and track metrics, monitor log files, set alarms, and automatically react to changes in their AWS environment.
  - **Key Features:**
    - **Metrics**: CloudWatch collects metrics from AWS services, such as EC2 instances, RDS databases, and S3 buckets, allowing users to monitor performance and utilization. For example, a cloud architect might monitor the latency of an EC2 instance to ensure it meets application performance requirements.
    - **Logs**: CloudWatch Logs allows users to collect and store log files from AWS services and custom applications, providing a centralized location for log analysis. A developer might use CloudWatch Logs to debug an issue with a Lambda function by examining its execution logs.
    - **CloudWatch Alarms**: Alarms can be set to monitor specific metrics and trigger actions, such as sending notifications or invoking an AWS Lambda function. For example, an alarm might be configured to trigger when an RDS database's CPU utilization exceeds 90%, prompting the system to automatically scale the database.
    - **CloudWatch Dashboards**: Provides customizable dashboards that display metrics, alarms, and logs in a single view, making it easier to monitor the health and performance of AWS environments. A DevOps team might create a dashboard to monitor the key performance indicators (KPIs) of a microservices application.
- **AWS CloudTrail:**
  - **Service Overview:** AWS CloudTrail records AWS API calls and events for an account, enabling governance, compliance, operational auditing, and risk auditing of AWS accounts. It helps users track changes to their AWS environment and detect any unauthorized activity.
  - **Key Features:**
    - **Event History**: Provides detailed event history of actions taken by users, roles, or AWS services, helping organizations understand the changes made to resources. For instance, a security team might review CloudTrail logs to investigate unauthorized changes to an S3 bucket's access policy.
    - **Insights**: CloudTrail Insights helps identify unusual operational activity, such as sudden increases in API call volume, which could indicate a security breach or misconfiguration. For example, an administrator might use CloudTrail Insights to detect anomalous behavior suggesting that an IAM user account has been compromised.
    - **Compliance Reports**: CloudTrail provides audit logs that can be used to generate compliance reports for regulatory requirements such as GDPR or HIPAA. A financial institution might use CloudTrail logs to demonstrate compliance during an audit.

- **AWS Config:**
  - **Service Overview:** AWS Config provides a detailed view of the configuration of AWS resources in an account, enabling users to monitor and assess configurations, track changes, and ensure compliance with defined policies.
  - **Key Features:**
    - **Resource Inventory**: Maintains an inventory of AWS resources and their configurations, allowing users to track changes over time. For instance, an IT team might use AWS Config to ensure that all EC2 instances have encryption enabled for their attached EBS volumes.
    - **Compliance Monitoring**: AWS Config allows users to define rules that check for compliance with internal policies or regulatory standards. If resources are found to be non-compliant, AWS Config can trigger remediation actions. For example, a rule might check that all S3 buckets are configured to block public access, and automatically remediate any violations.
    - **Change Management**: Tracks and records configuration changes to resources, helping teams identify the cause of operational issues. A DevOps engineer might use AWS Config to troubleshoot a performance issue by reviewing recent changes to the associated load balancer.
- **AWS Health:**
  - **Service Overview:** AWS Health provides personalized information about AWS service events that may impact a user's AWS environment. It delivers timely notifications about issues affecting AWS services, including outages, planned maintenance, and other operational events.
  - **Key Features:**
    - **Service Health Dashboard**: Displays the current status of AWS services across all regions, allowing users to quickly check for service disruptions. For instance, an IT manager might refer to the dashboard to determine if an ongoing service issue is affecting their resources.
    - **Personal Health Dashboard**: Provides a personalized view of service issues, maintenance events, and other notifications that specifically impact a user's AWS resources. A company might use the Personal Health Dashboard to receive updates on a scheduled maintenance event affecting their RDS instances.
    - **Event Notifications**: Sends notifications via email, SMS, or SNS about service events, allowing users to respond quickly to potential issues. For example, an alert might notify administrators of an impending hardware failure affecting one of their EC2 instances.



Get started with CloudWatch

You don't have any alarms, metrics or default dashboard. Once you set them up they will be displayed here. View getting started page

Set alarms on any of your metrics to receive notification when your metric crosses your specified threshold.

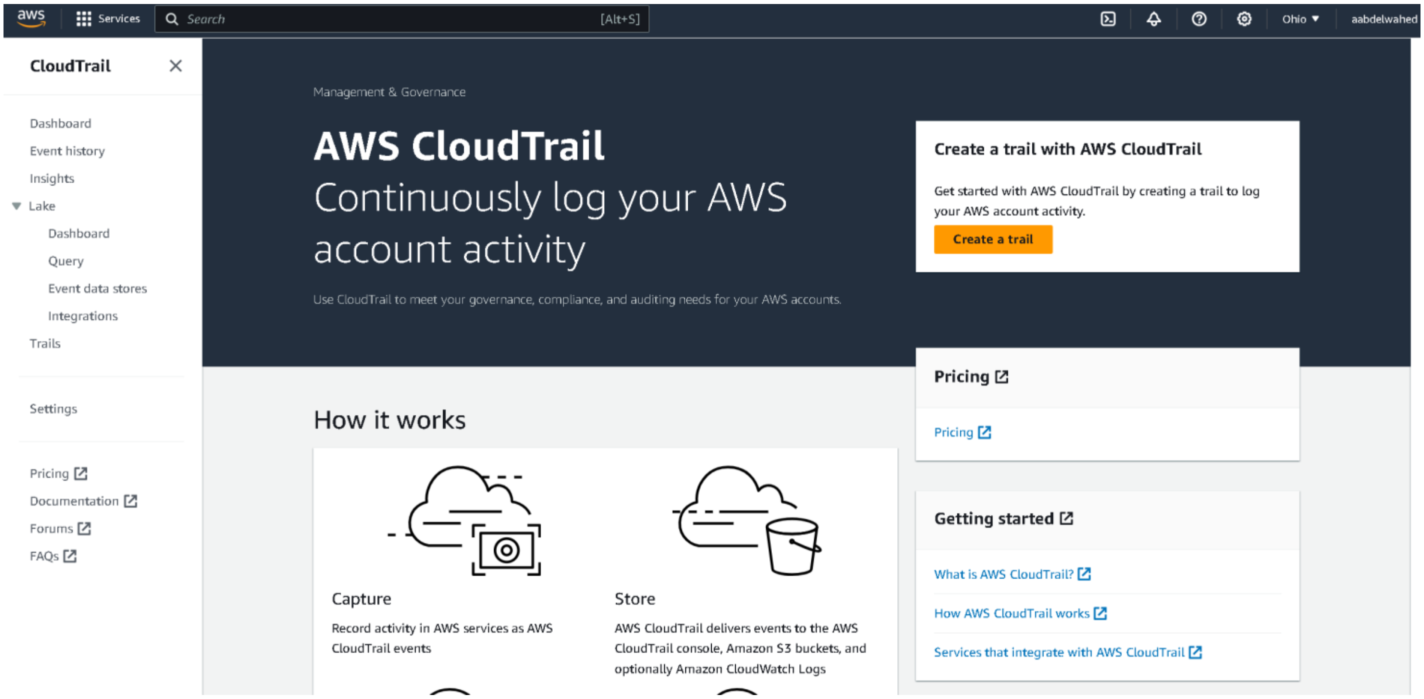
Create and name any CloudWatch dashboard **CloudWatch-Default** to display it here.

Monitor using your existing system, application and custom log files.

Write rules to indicate which events are of interest to your application and what automated action to take.

Get started with Application Insights

Set up monitors and dashboards to detect issues and resolve problems with enterprise applications, databases, and workloads.



CloudTrail ✕

- Dashboard
- Event history
- Insights
- ▼ Lake
  - Dashboard
  - Query
  - Event data stores
  - Integrations
- Trails

Settings

Pricing
Documentation
Forums
FAQs

Management & Governance

AWS CloudTrail
Continuously log your AWS account activity

Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.

Create a trail with AWS CloudTrail

Get started with AWS CloudTrail by creating a trail to log your AWS account activity.

Create a trail

Pricing

Pricing

Getting started

What is AWS CloudTrail?
How AWS CloudTrail works
Services that integrate with AWS CloudTrail

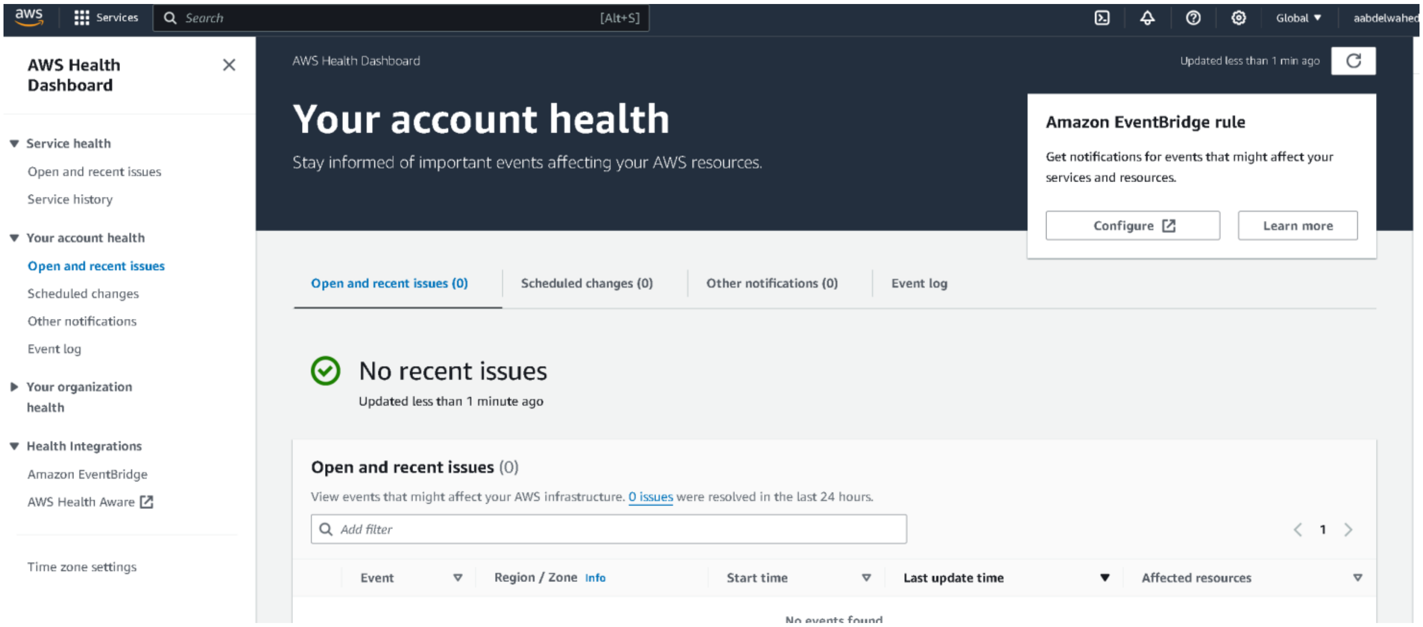
How it works

Capture

Record activity in AWS services as AWS CloudTrail events

Store

AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs



AWS Health Dashboard ✕

- ▼ Service health
  - Open and recent issues
  - Service history
- ▼ Your account health
  - Open and recent issues
  - Scheduled changes
  - Other notifications
  - Event log
- ▶ Your organization health
- ▼ Health Integrations
  - Amazon EventBridge
  - AWS Health Aware

Time zone settings

AWS Health Dashboard

Updated less than 1 min ago

Your account health
Stay informed of important events affecting your AWS resources.

Amazon EventBridge rule

Get notifications for events that might affect your services and resources.

Configure | Learn more

Open and recent issues (0) | Scheduled changes (0) | Other notifications (0) | Event log

✓ No recent issues
Updated less than 1 minute ago

Open and recent issues (0)

View events that might affect your AWS infrastructure. 0 issues were resolved in the last 24 hours.

Add filter

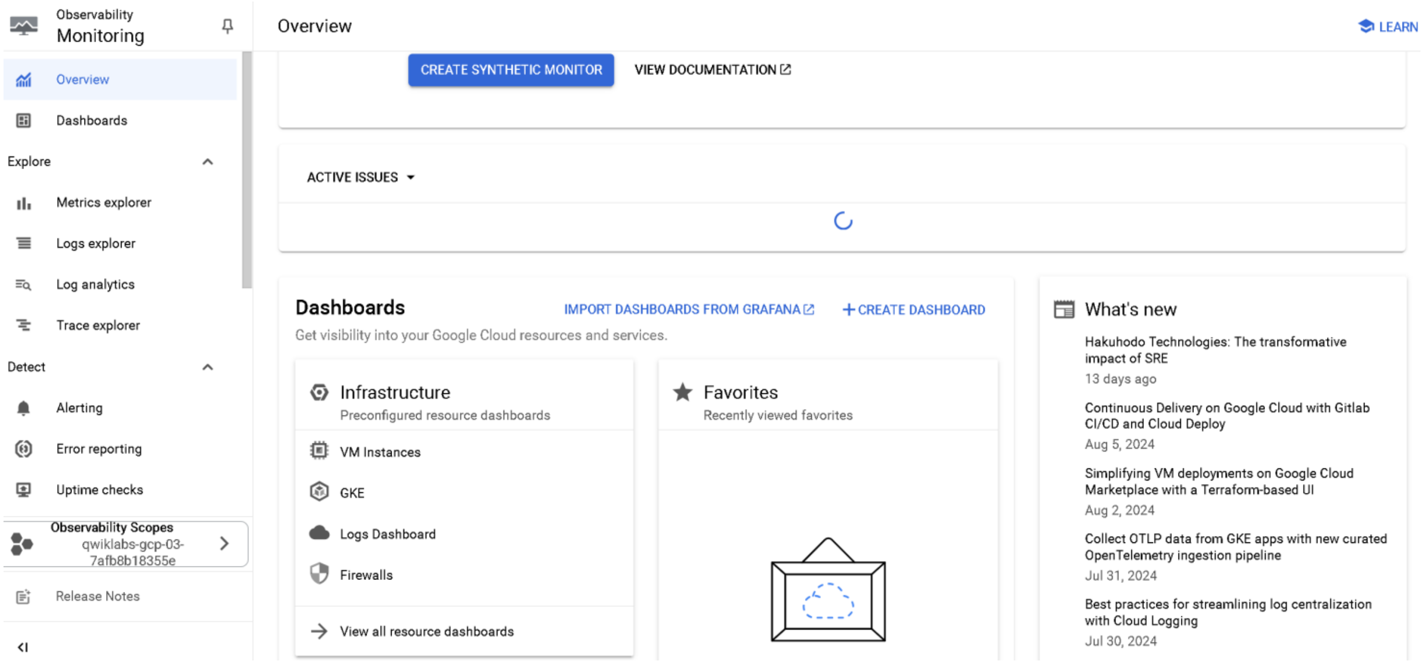
Event	Region / Zone Info	Start time	Last update time	Affected resources

No events found

Google Cloud

- **Google Cloud Operations Suite (formerly Stackdriver):**
  - **Service Overview:** Google Cloud Operations Suite provides comprehensive monitoring, logging, and diagnostics for applications and services running on Google Cloud and other platforms. It includes features like Monitoring, Logging, Trace, Debugger, and Error Reporting.
  - **Key Features:**
    - **Cloud Monitoring**: Collects metrics, dashboards, and alerts for Google Cloud resources, helping users monitor the performance and availability of their applications. For example, an engineering team might monitor the response time of their APIs using Cloud Monitoring.
    - **Cloud Logging**: Aggregates and analyzes log data from Google Cloud resources, applications, and system software, enabling users to search, filter, and analyze logs. A developer might use Cloud Logging to diagnose issues in a Kubernetes cluster by examining the logs from various containers.
    - **Cloud Trace**: Provides distributed tracing capabilities, helping users analyze the latency of requests as they travel through various services. An application developer might use Cloud Trace to identify bottlenecks in a microservices architecture.
    - **Cloud Error Reporting**: Automatically detects and aggregates errors in cloud applications, providing alerts and insights to help developers resolve issues quickly. A development team might use Cloud Error Reporting to track and fix runtime exceptions in a production environment.
    - **Cloud Profiler**: Provides continuous profiling of CPU and memory usage, helping developers identify and optimize resource-intensive parts of their applications. For instance, a software company might use Cloud Profiler to reduce the memory footprint of a high-traffic web application.
- **Google Cloud Alerts:**
  - **Service Overview:** Google Cloud Alerts enable users to set up custom alerts based on metrics and logs collected by Cloud Monitoring and Cloud Logging. Alerts can be configured to trigger notifications, automate responses, or escalate issues to ensure timely resolution.
  - **Key Features:**
    - **Metric-Based Alerts**: Trigger alerts when specified metrics exceed defined thresholds, such as CPU utilization or request latency. For example, an alert might notify administrators when the CPU usage of a Compute Engine instance exceeds 90% for a sustained period.
    - **Log-Based Alerts**: Alerts can be based on specific log events, such as errors or warnings, helping users respond to issues quickly. A security team might configure log-based alerts to detect unauthorized access attempts in their environment.
    - **Incident Management Integration**: Google Cloud integrates with third-party incident management tools, such as PagerDuty or Slack, enabling seamless alerting and incident resolution workflows. An IT operations team might use this integration to ensure that critical alerts are promptly escalated to the appropriate personnel.
    - **Notification Channels**: Alerts can be sent via various notification channels, including email, SMS, and mobile apps, ensuring that the right people are informed in real-time. A site reliability engineer might receive mobile notifications for critical system outages.

- **Google Cloud Operations Suite - Uptime Monitoring:**
  - **Service Overview:** Uptime Monitoring in Google Cloud Operations Suite allows users to monitor the availability of their applications and services from multiple locations around the world, ensuring they meet their Service Level Objectives (SLOs).
  - **Key Features:**
    - **Global Availability Checks**: Regularly checks the availability of applications from different geographic locations, ensuring global uptime. For instance, a global e-commerce platform might use uptime monitoring to verify that its site is accessible to users in different regions.
    - **Customizable Alerts**: Alerts can be configured to trigger if uptime checks fail, enabling rapid response to downtime or service disruptions. A DevOps team might set up alerts to immediately notify on-call staff if a critical service becomes unavailable.
    - **Detailed Reporting**: Provides reports on uptime and latency, helping teams identify trends and address issues proactively. A service provider might use these reports to demonstrate compliance with uptime guarantees to customers.
- **Google Cloud Status Dashboard:**
  - **Service Overview:** Google Cloud Status Dashboard provides real-time information about the health of Google Cloud services, including details on outages, disruptions, and planned maintenance.
  - **Key Features**:
    - **Service Health Updates**: Displays current and historical information on the status of Google Cloud services, helping users quickly determine if their resources are affected by an ongoing issue. For example, an IT administrator might check the dashboard during an incident to confirm whether a service outage is impacting their project.
    - **Incident Notifications**: Users can subscribe to receive updates on service incidents, ensuring they are informed of any issues affecting their cloud environment. A business might subscribe to incident notifications for critical services to stay informed of any disruptions.



Get visibility into your Google Cloud resources and services.

Hakuhodo Technologies: The transformative impact of SRE
13 days ago

Continuous Delivery on Google Cloud with Gitlab CI/CD and Cloud Deploy
Aug 5, 2024

Simplifying VM deployments on Google Cloud Marketplace with a Terraform-based UI
Aug 2, 2024

Collect OTLP data from GKE apps with new curated OpenTelemetry ingestion pipeline
Jul 31, 2024

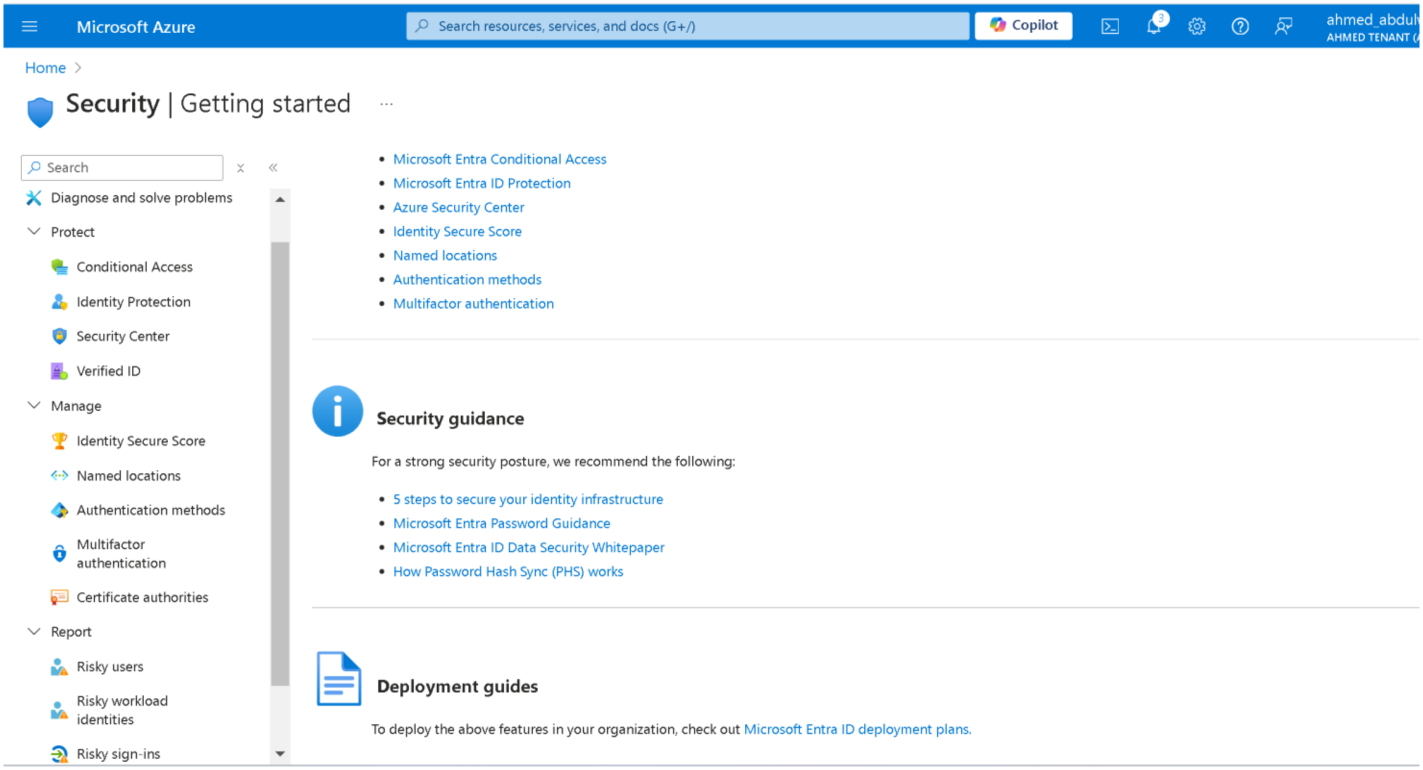
Best practices for streamlining log centralization with Cloud Logging
Jul 30, 2024

Security Best Practices

Microsoft Azure

- **Identity and Access Management (IAM)**:
  - **Use Azure Active Directory (Microsoft Entra):**
    - **Single Sign-On (SSO)**: Implement SSO with Microsoft Entra to centralize and secure user access to multiple applications, reducing the risk of password fatigue and unauthorized access. For example, an organization can use SSO to manage access to both on-premises and cloud-based applications through a single authentication point.
    - **Multi-Factor Authentication (MFA)**: Enforce MFA for all users, particularly for those with administrative privileges, to add an extra layer of security. MFA requires users to provide two or more verification methods, such as a password and a phone verification code, before granting access.
    - **Conditional Access Policies**: Implement conditional access policies to control access based on conditions like user location, device compliance, and risk level. For instance, you can require MFA when users attempt to access resources from unfamiliar locations.
- **Network Security:**
  - **Network Security Groups (NSGs):** Use NSGs to control inbound and outbound traffic to Azure resources at the subnet and network interface levels. Define specific rules to allow or deny traffic based on IP addresses, protocols, and ports.
    - **Example**: Restrict access to a web server by allowing only HTTP/HTTPS traffic from known IP ranges while blocking all other traffic.
  - **Azure Firewall:** Deploy Azure Firewall to centrally manage and enforce network security policies across multiple Azure VNets. Azure Firewall provides both inbound and outbound filtering rules, including threat intelligence-based filtering to block traffic from known malicious IP addresses.
  - **Virtual Network (VNet) Peering:** Securely connect different VNets using VNet Peering, ensuring that data transfer between them remains within the Azure backbone network and does not traverse the public internet.
- **Data Protection:**
  - **Encryption at Rest and in Transit:** Ensure that all sensitive data is encrypted both at rest and in transit. Azure provides encryption options for data stored in Azure Storage, SQL Database, and other services, as well as SSL/TLS for data in transit.
    - **Example**: Enable Transparent Data Encryption (TDE) for Azure SQL Database to encrypt data, logs, and backups.
  - **Azure Key Vault:** Use Azure Key Vault to securely store and manage cryptographic keys, secrets, and certificates. Key Vault helps safeguard encryption keys and secrets used by cloud applications and services.
    - **Example**: Store API keys, connection strings, and passwords in Azure Key Vault instead of embedding them in application code or configuration files.
- **Monitoring and Alerts:**
  - **Azure Security Center:** Use Azure Security Center to gain visibility into your security posture, identify vulnerabilities, and receive recommendations for improving security. Security Center continuously monitors Azure resources and provides actionable insights.

        - **Example**: Set up alerts for non-compliant resources and receive recommendations for enabling security features like MFA and encryption.
    - **Azure Monitor and Log Analytics:** Leverage Azure Monitor and Log Analytics to collect and analyze logs and metrics from Azure resources, enabling proactive detection of security issues. Use custom queries to detect unusual activity, such as failed login attempts or unauthorized configuration changes.
- **Compliance and Governance:**
    - **Azure Policy:** Implement Azure Policy to enforce compliance with organizational standards and regulatory requirements. Azure Policy allows you to create, assign, and manage policies that automatically evaluate and remediate non-compliant resources.
        - **Example**: Enforce a policy that requires all storage accounts to have encryption enabled.
    - **Blueprints:** Use Azure Blueprints to define a repeatable set of Azure resources that implement and adhere to organizational standards, patterns, and requirements. Blueprints help ensure that deployments are consistent and compliant from the start.
        - **Example**: Create a blueprint for deploying a secure environment that includes a VNet, NSGs, Azure Firewall, and necessary compliance policies.



Security | Getting started

- Microsoft Entra Conditional Access
- Microsoft Entra ID Protection
- Azure Security Center
- Identity Secure Score
- Named locations
- Authentication methods
- Multifactor authentication

Security guidance

For a strong security posture, we recommend the following:

- 5 steps to secure your identity infrastructure
- Microsoft Entra Password Guidance
- Microsoft Entra ID Data Security Whitepaper
- How Password Hash Sync (PHS) works

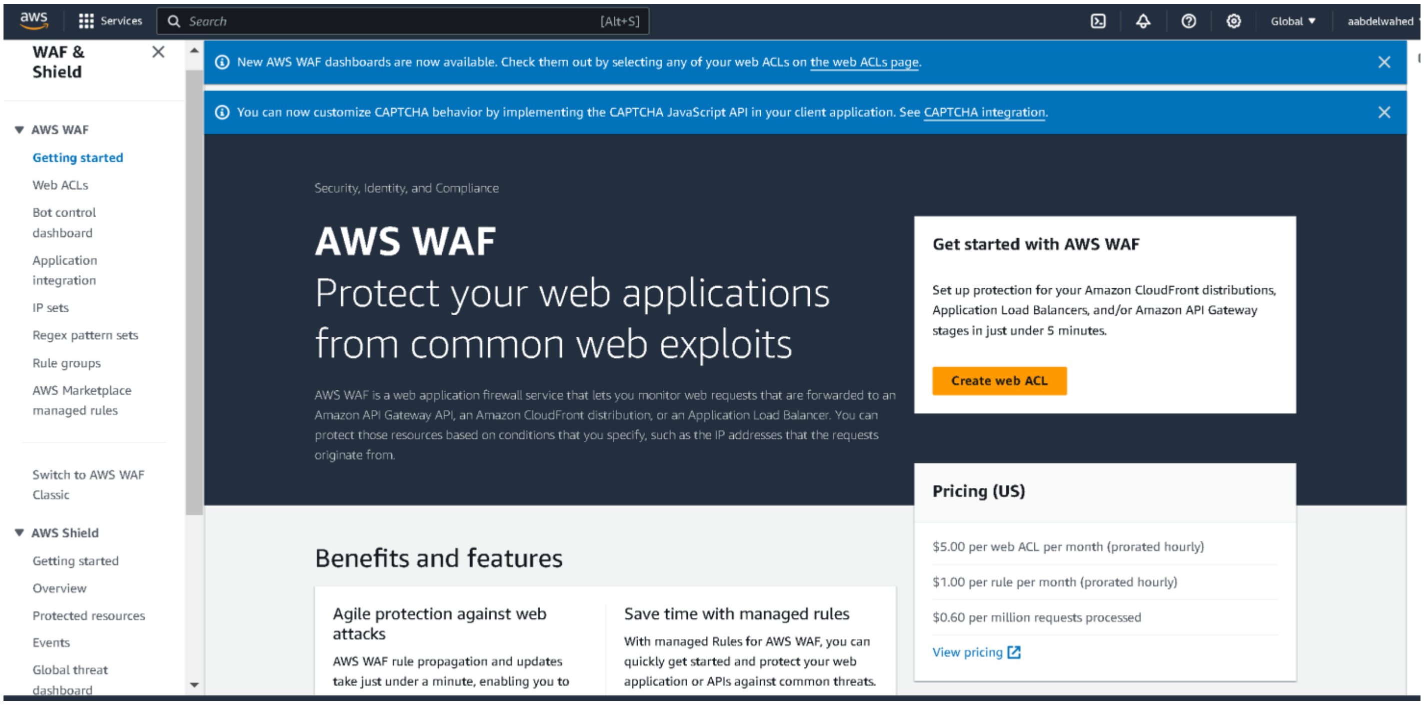
Deployment guides

To deploy the above features in your organization, check out Microsoft Entra ID deployment plans.

Amazon AWS

- **Identity and Access Management (IAM):**
  - **AWS IAM Best Practices:**
    - **Least Privilege Principle**: Always grant the minimum permissions necessary for users, groups, and roles to perform their tasks. Regularly review and update IAM policies to ensure they remain aligned with current roles and responsibilities.
      - **Example**: Instead of granting full s3:* permissions, grant specific actions like s3:PutObject and s3:GetObject only to the necessary buckets.
    - **MFA Enforcement**: Require MFA for all IAM users, especially those with access to sensitive resources or administrative privileges. MFA adds an additional layer of security by requiring a second form of authentication.
    - **IAM Roles and Temporary Credentials**: Use IAM roles instead of long-term access keys for applications and services that need to interact with AWS resources. IAM roles provide temporary credentials, reducing the risk of compromised access keys.
      - **Example**: Assign an IAM role to an EC2 instance that requires access to an S3 bucket, rather than embedding access keys in the instance.
- **Network Security:**
  - **VPC Security:**
    - **Security Groups**: Use Security Groups to control inbound and outbound traffic to AWS resources at the instance level. Define rules that allow only necessary traffic, such as restricting SSH access to specific IP addresses.
      - **Example**: Allow only HTTP/HTTPS traffic to a web server while blocking all other inbound traffic.
    - **Network ACLs (NACLs)**: Use NACLs to provide an additional layer of security at the subnet level, controlling inbound and outbound traffic. NACLs can be used to block specific IP ranges or protocols across multiple instances.
  - **AWS WAF (Web Application Firewall):** Deploy AWS WAF to protect web applications from common web exploits such as SQL injection and cross-site scripting (XSS). WAF allows you to create custom rules to filter out malicious traffic before it reaches your application.
      - **Example**: Use AWS WAF to block requests that match known attack patterns, such as those targeting common web application vulnerabilities.
- **Data Protection:**
  - **Encryption:**
    - **Encryption at Rest**: Use AWS KMS (Key Management Service) to manage encryption keys for encrypting data at rest across various AWS services, including S3, EBS, and RDS.
      - **Example**: Enable server-side encryption (SSE) with KMS keys (SSE-KMS) for S3 buckets storing sensitive data.
    - **Encryption in Transit**: Ensure that all data transmitted between clients and AWS services is encrypted using SSL/TLS to protect against man-in-the-middle attacks.
  - **AWS Secrets Manager:** Use AWS Secrets Manager to securely store and manage sensitive information such as API keys, database credentials, and tokens. Secrets Manager automatically rotates secrets, reducing the risk of exposure.
    - **Example**: Store and rotate database credentials used by a Lambda function in Secrets Manager.

- **Monitoring and Alerts:**
  - **Amazon CloudWatch:** Use CloudWatch to monitor AWS resources and applications in real-time. Set up CloudWatch Alarms to trigger notifications or automated actions based on specified metrics, such as high CPU usage or low available memory.
    - **Example**: Configure an alarm to notify administrators if an EC2 instance's CPU usage exceeds 90% for a prolonged period.
  - **AWS CloudTrail:** Enable CloudTrail to log all API calls made within your AWS environment, providing a complete audit trail for compliance and security purposes. Regularly review CloudTrail logs to detect unauthorized or suspicious activity.
    - **Example**: Use CloudTrail to monitor and alert on changes to critical resources, such as unauthorized modifications to security groups.
- **Compliance and Governance:**
  - **AWS Config:** Use AWS Config to monitor and assess the configuration of AWS resources, ensuring they comply with internal policies and regulatory requirements. AWS Config can automatically remediate non-compliant resources based on predefined rules.
    - **Example**: Set up AWS Config rules to ensure that all EC2 instances have encryption enabled for attached EBS volumes.
  - **AWS Organizations and Service Control Policies (SCPs):** Use AWS Organizations to centrally manage and enforce security policies across multiple AWS accounts. SCPs allow you to define and apply governance policies that restrict actions across all accounts in your organization.
    - **Example**: Implement an SCP that prevents users from disabling CloudTrail logging across all AWS accounts in the organization.



New AWS WAF dashboards are now available. Check them out by selecting any of your web ACLs on the web ACLs page.

You can now customize CAPTCHA behavior by implementing the CAPTCHA JavaScript API in your client application. See CAPTCHA integration.

Security, Identity, and Compliance

AWS WAF

Protect your web applications from common web exploits

AWS WAF is a web application firewall service that lets you monitor web requests that are forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer. You can protect those resources based on conditions that you specify, such as the IP addresses that the requests originate from.

Get started with AWS WAF

Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.

Create web ACL

Pricing (US)

$5.00 per web ACL per month (prorated hourly)

$1.00 per rule per month (prorated hourly)

$0.60 per million requests processed

View pricing

Benefits and features

Agile protection against web attacks

AWS WAF rule propagation and updates take just under a minute, enabling you to

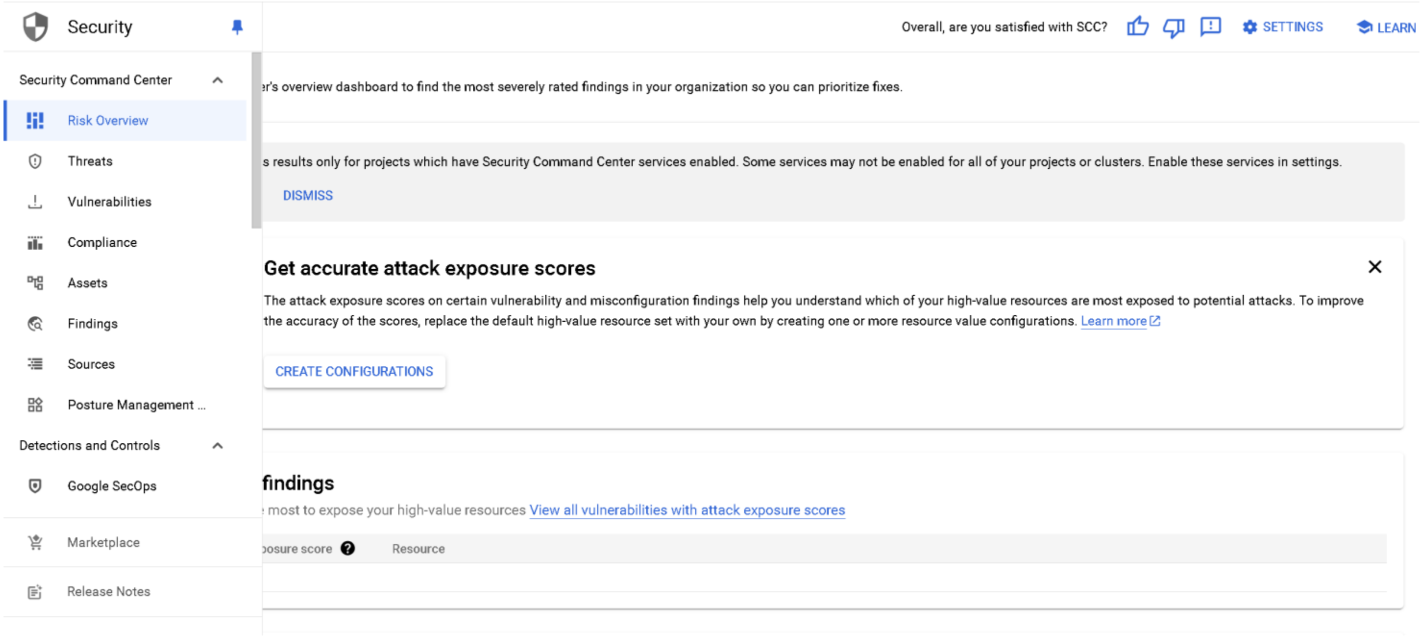
Save time with managed rules

With managed Rules for AWS WAF, you can quickly get started and protect your web application or APIs against common threats.

Google Cloud

- **Identity and Access Management (IAM):**
  - **Google Cloud IAM Best Practices:**
    - **Principle of Least Privilege**: Assign only the necessary permissions to users, groups, and service accounts based on their roles and responsibilities. Regularly audit IAM policies to ensure they adhere to the principle of least privilege.
      - **Example**: Instead of granting roles/editor to a user, assign more granular roles like roles/storage.objectViewer for specific buckets.
    - **Service Accounts**: Use service accounts with appropriate roles for applications and services, avoiding the use of user credentials for automation. Limit the scope of service accounts to only the resources they need to access.
      - **Example**: Create a dedicated service account for a GKE application that needs to access a Cloud Storage bucket, and assign only the roles/storage.objectAdmin role.
    - **Two-Step Verification**: Enforce two-step verification (2SV) for all Google Cloud users to add an extra layer of security to account access.
- **Network Security:**
  - **Virtual Private Cloud (VPC):**
    - **Firewall Rules**: Implement firewall rules to control traffic to and from instances within your VPC. Define rules that allow only necessary traffic, minimizing the exposure of resources to the public internet.
      - **Example**: Create a firewall rule to allow SSH access only from specific IP addresses while blocking all other inbound traffic.
    - **VPC Service Controls**: Use VPC Service Controls to define security perimeters around Google Cloud resources, preventing data exfiltration and unauthorized access. VPC Service Controls help protect sensitive data by restricting access to resources based on network boundaries.
      - **Example**: Set up a service perimeter around Cloud Storage and BigQuery to ensure that data cannot be accessed or transferred outside the defined perimeter.
  - **Google Cloud Armor:** Deploy Google Cloud Armor to protect web applications from DDoS attacks and other common web vulnerabilities. Cloud Armor provides customizable security policies that filter traffic based on IP addresses, geolocation, and Layer 7 parameters.
      - **Example**: Use Cloud Armor to block traffic from regions known for high levels of malicious activity while allowing access from trusted regions.
- **Data Protection:**
  - **Encryption:**
    - **Encryption at Rest and in Transit**: Google Cloud automatically encrypts data at rest and in transit between Google services. Additionally, you can manage your own encryption keys using Cloud KMS (Key Management Service).
      - **Example**: Use Cloud KMS to manage and rotate encryption keys used to protect data stored in Cloud Storage.
    - **Customer-Managed Encryption Keys (CMEK)**: For additional control, use CMEK to manage encryption keys for Google Cloud services, ensuring that you control the key lifecycle.
      - **Example**: Enable CMEK for BigQuery datasets containing sensitive information to retain control over the encryption keys.
  - **Google Secret Manager:** Store and manage secrets, such as API keys and passwords, using Google Secret Manager. Secret Manager provides secure, centralized storage with built-in encryption and access controls.
    - **Example**: Store database credentials in Secret Manager and configure automatic rotation to enhance security.

- **Monitoring and Alerts:**
  - **Google Cloud Operations Suite:**
    - **Cloud Monitoring**: Use Cloud Monitoring to collect metrics from Google Cloud resources, applications, and services. Set up alerts to notify administrators when thresholds are breached or anomalies are detected.
      - **Example**: Configure an alert to trigger when the CPU utilization of a Compute Engine instance exceeds 85% for an extended period.
    - **Cloud Logging**: Leverage Cloud Logging to collect and analyze logs from Google Cloud services, enabling proactive detection of security issues. Use custom log queries to identify unusual activity, such as repeated failed login attempts.
      - **Example**: Set up a log-based alert to notify the security team if a specific service account is used outside of its expected context.
  - **Security Command Center:** Use Security Command Center to gain visibility into your Google Cloud environment, identify vulnerabilities, and respond to threats. It provides a centralized dashboard for monitoring security risks across your Google Cloud resources.
    - **Example**: Enable Security Health Analytics within the Security Command Center to receive alerts on common security misconfigurations, such as open firewall rules or public buckets.
- **Compliance and Governance:**
  - **Google Cloud Resource Manager:** Use Google Cloud Resource Manager to organize and manage resources across projects, folders, and organizations. Apply IAM policies at different levels to enforce security and governance standards.
    - **Example**: Apply an organization-wide policy that restricts the creation of public IP addresses, ensuring compliance with internal security guidelines.
  - **Organization Policies:** Implement organization policies to enforce governance and compliance across Google Cloud projects. These policies help prevent configuration drift and ensure that resources adhere to organizational standards.
    - **Example**: Enforce a policy that requires all Cloud Storage buckets to have uniform access control, preventing the use of fine-grained access controls that could lead to misconfigurations.



›r's overview dashboard to find the most severely rated findings in your organization so you can prioritize fixes.

s results only for projects which have Security Command Center services enabled. Some services may not be enabled for all of your projects or clusters. Enable these services in settings.

Get accurate attack exposure scores

The attack exposure scores on certain vulnerability and misconfiguration findings help you understand which of your high-value resources are most exposed to potential attacks. To improve the accuracy of the scores, replace the default high-value resource set with your own by creating one or more resource value configurations. Learn more

findings

› most to expose your high-value resources View all vulnerabilities with attack exposure scores