



1ST EDITION

Cloud Auditing Best Practices

Perform Security and IT Audits across AWS, Azure, and GCP by building effective cloud auditing plans



SHINESA CAMBRIC | MICHAEL RATEMO

Preface

As many companies move to the cloud and shift business operations to hybrid, single cloud, or multi-cloud environments, it's important that enterprise IT auditors be prepared with the tools and knowledge to effectively assess risk and controls, given this a business trend that is here to stay. Using assessment procedures and frameworks based on on-premise and legacy environments doesn't fully translate to cloud environments, leaving the enterprise with potential gaps in risk control coverage. This book will guide an auditor to understand where security controls can and do exist, procedures for accessing them for review, and best practices for testing their effectiveness. By the end of the book, you will be able to build an audit plan and assess security and compliance controls for the three major enterprise cloud environments (Amazon, Google, and Microsoft).

Who this audiobook is for

This book is primarily intended for IT and security auditors who are responsible for building audit plans and testing the effectiveness of controls within an enterprise that may be moving, or has already moved to adopting cloud services. This book provides insight for beginner to advanced IT and Security auditors looking to learn more about what exists in the cloud so that they can ask questions and leverage tools that may lead to better test coverage. Other IT professionals whose job includes assessing compliance, such as DevSecOps teams, identity, and access management analysts, cloud engineers, and cloud security architects, will also find plenty of useful information in this book. Before you get started, you'll need a basic understanding of IT systems, cloud environments, and a solid grasp of IT general computing controls and cybersecurity basics. However, past experience configuring or performing a risk assessment on cloud environments is not required.

What this audiobook covers

Chapter 1, Cloud Architecture and Navigation, provides a fundamental understanding of what a cloud environment is, navigating through different cloud provider environments, and roles and responsibilities between the cloud service provider and an auditor.

Chapter 2, Effective Techniques for Preparing to Audit Cloud Environments, covers the standard resources available to develop an audit plan, and align controls to a cloud environment, and the tools for policy and compliance automation.

Chapter 3, Identity and Access Management Controls, walks through configuration and control options for a digital identity, including authentication and authorization and reviewing activity logs.

Chapter 4, Network, Infrastructure, and Security Controls, looks at policies and options for defining and controlling network and infrastructure access and navigating security control centers.

Chapter 5, Financial Resource and Change Management Controls, introduces features available within each of the cloud environments for resource management, including billing and cost controls, and tracking changes within the cloud environment.

Chapter 6, Tips and Techniques for Advanced Auditing, provides guidance on common pitfalls an IT auditor should look out for, tips and techniques to leverage, and ideas for preparing for more advanced audits, including a primer on other cloud environments such as Alibaba, IBM, and Oracle.

Chapter 7, Tools for Monitoring and Assessing, gives a deeper insight on tools and options that exist for auditors to monitor cloud platforms, within each of the three major cloud providers.

Chapter 8, Walk-Through – Assessing IAM Controls, covers simple assessments for hands-on experience assessing identity and access management controls within the three major cloud providers.

Chapter 9, Walk-Through – Assessing Policy Settings and Resource Controls, provides practice opportunities for assessing security and compliance settings, and reviewing resource management controls.

Chapter 10, Walk-Through – Assessing Change Management, Logging, and Monitoring Policies, offers an opportunity to practice assessing compliance for changes made within the cloud environment, as well as how to leverage cloud native tools for performing logging and monitoring in the cloud.

To get the most out of this audiobook

To navigate through the hands-on practice chapters of the audiobook, it's best to have a "sandbox" environment with some administrative privileges or set up your own personal cloud environment for Amazon Web Services, Microsoft Azure, and Google Cloud Platform. If you choose to set up your own personal cloud environment, at the time of this writing, each of the three major cloud providers has options for a setup that is free for at least the first 30 days and then moves to a "pay-as-you-go" model. Please carefully review the terms and agreements to understand the financial implications of long-term usage.

Software/hardware covered in the book	Operating system requirements
Any of the latest versions of Google Chrome or Microsoft Edge	Windows, macOS, or Linux (any)
Amazon Web Services	Windows, macOS, or Linux (any)
Microsoft Azure	Windows, macOS, or Linux (any)
Google Cloud Platform	Windows, macOS, or Linux (any)

Download the color images

We also provide a PDF file that has color images of the screenshots and diagrams used in this book. You can download it here: <https://packt.link/Kg3mI>.

Chapter 1

Figures

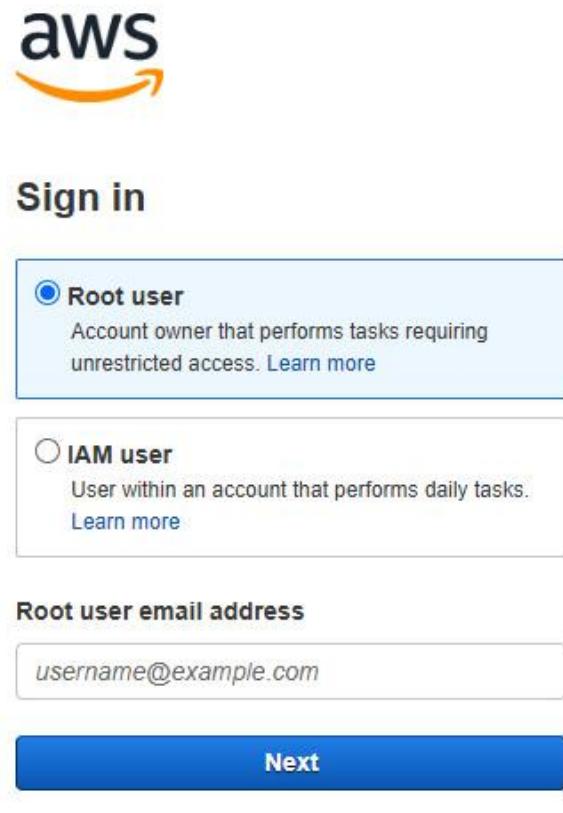


Figure 1.1 – AWS console initial sign-in

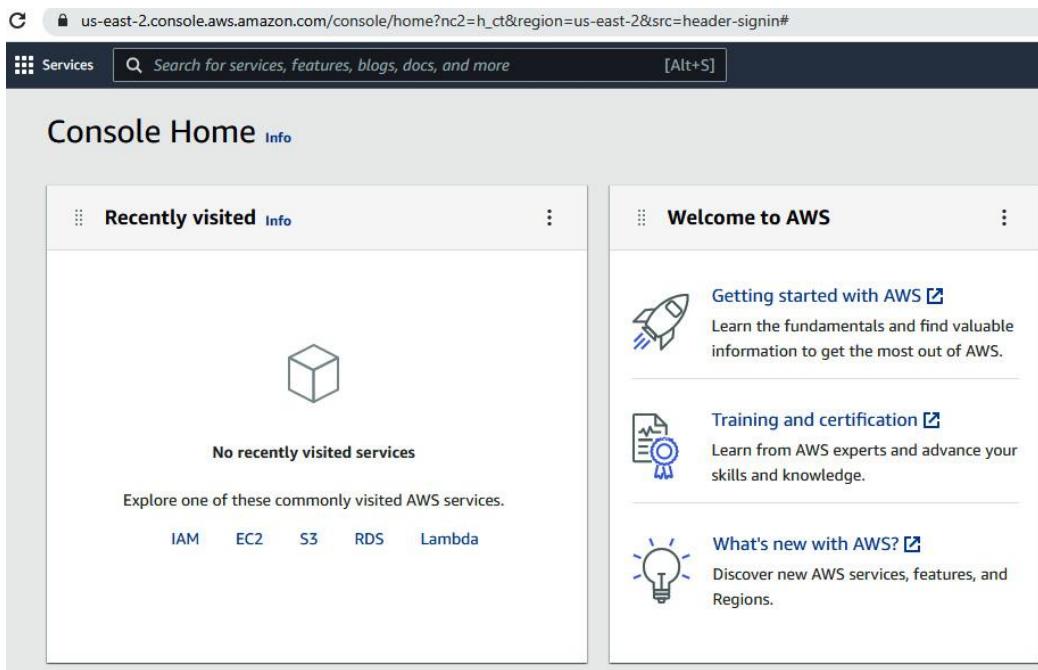


Figure 1.2 – AWS Console Home main page

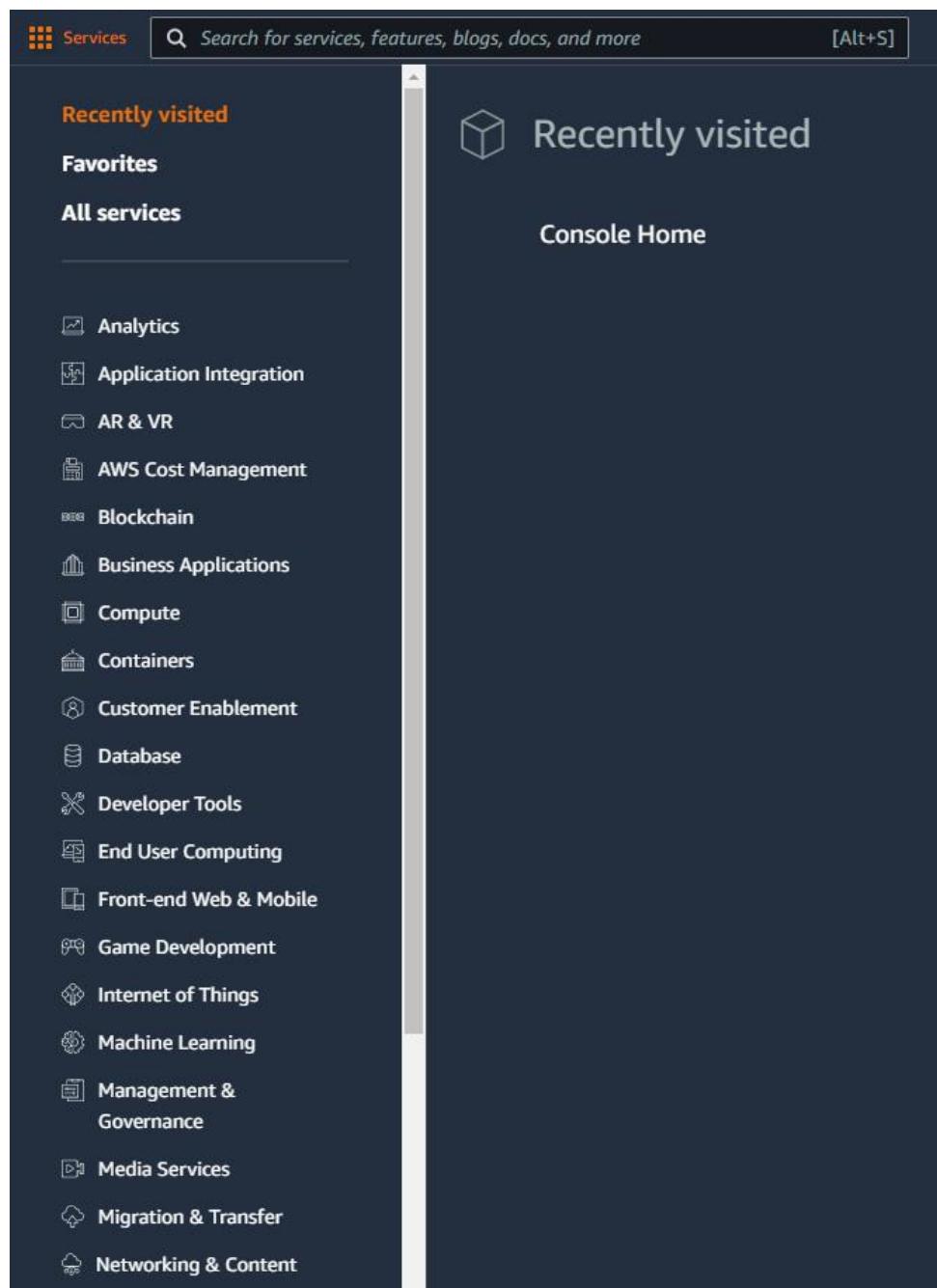


Figure 1.3 – AWS Console Home Services list

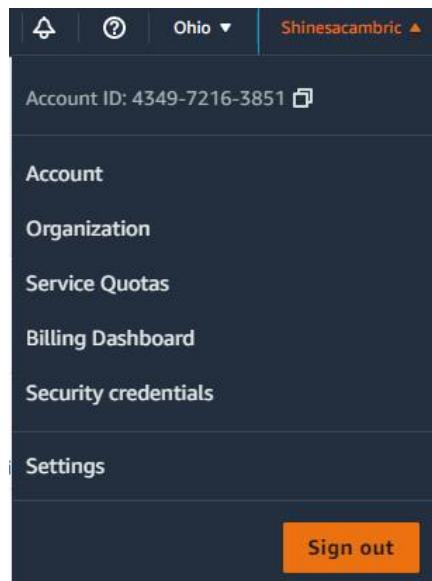


Figure 1.4 – AWS Console Home account sign-In details

Welcome to AWS

 [Getting started with AWS](#) 
Learn the fundamentals and find valuable information to get the most out of AWS.

 [Training and certification](#) 
Learn from AWS experts and advance your skills and knowledge.

 [What's new with AWS?](#) 
Discover new AWS services, features, and Regions.

AWS Health Info

Open issues
0 Past 7 days

Scheduled changes
0 Upcoming and past 7 days

Other notifications
0 Past 7 days

[Go to AWS Health](#)

Build a solution Info

Start building with simple wizards and automated workflows.

 Launch a virtual machine With EC2 (2 mins)	 Register a domain With Route 53 (3 mins)
 Start a development project With CodeStar (5 mins)	 Build a web app With AWS App Runner (5 mins)
 Connect an IoT device With AWS IoT (5 mins)	 Deploy a serverless microservice With API Gateway (2 mins)
 Build using virtual servers With Lightsail (2 mins)	 Start migrating to AWS With AWS MGN (2 mins)
 Host a static web app With AWS Amplify Console (2 mins)	

Figure 1.5 – AWS Console Home widgets

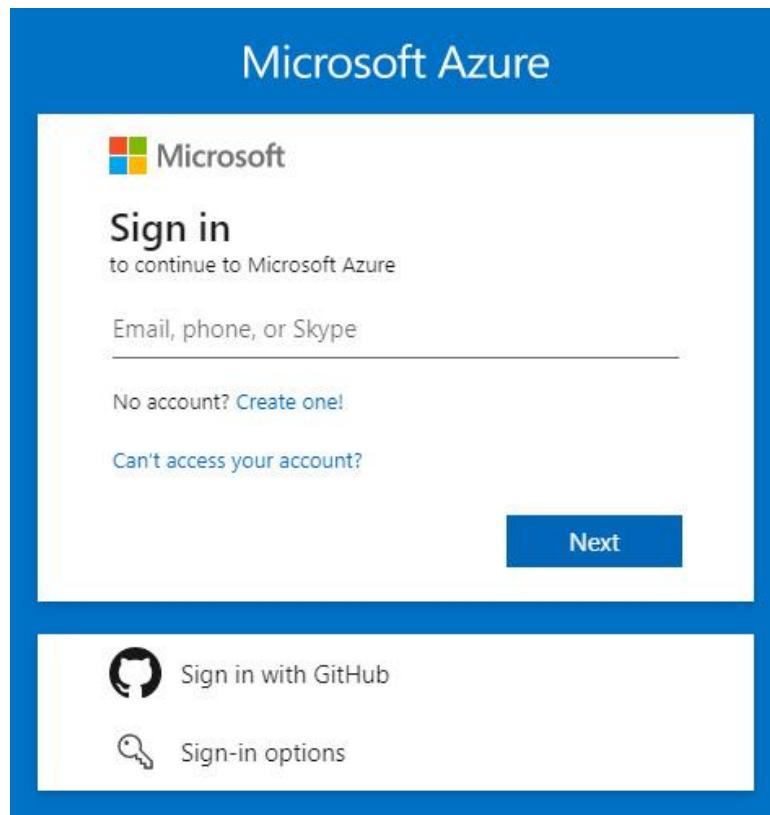


Figure 1.6 – Microsoft Azure initial sign-in

The image shows the Microsoft Azure portal home page. At the top, there is a navigation bar with icons for back, forward, refresh, and the URL "portal.azure.com/#home". The title is "Microsoft Azure" and there is a search bar. Below the navigation bar is a section titled "Azure services" with various icons and links: "Create a resource", "Azure Active Directory", "Azure AD Identity Secur...", "Microsoft Defender for...", "External Identities", "Service providers", "Azure AD Risky workload...", "Managed Identities", "Multi-Factor Authentication", and "All services". Below this is a section titled "Recent resources" with columns for "Name", "Type", and "Last Viewed".

Figure 1.7 – Microsoft Azure portal home page

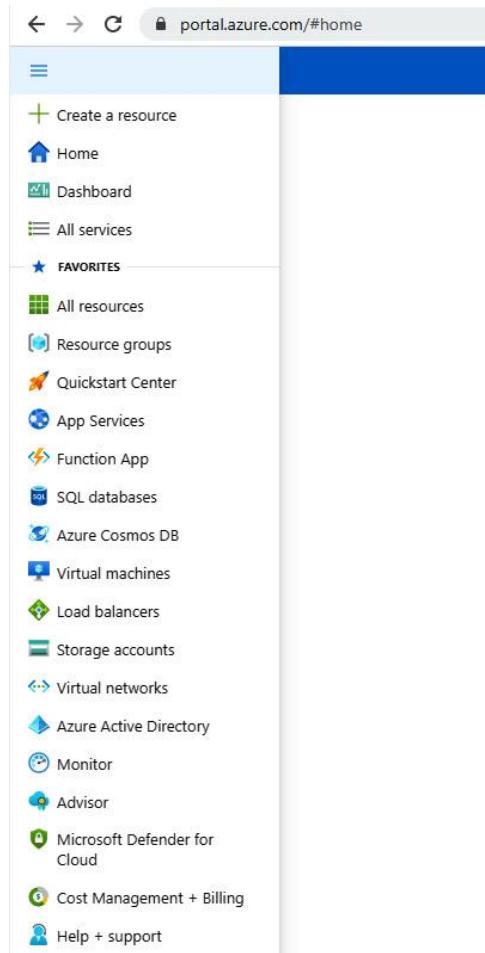


Figure 1.8 – Microsoft Azure portal home page navigation panel

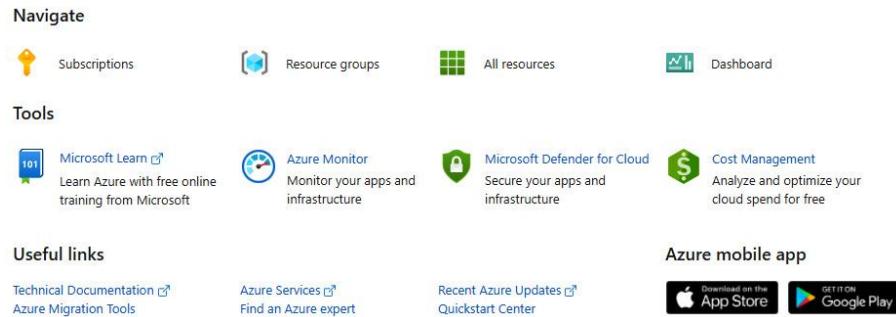


Figure 1.9 – Microsoft Azure portal dashboard Navigate section

The screenshot shows the Microsoft Azure portal's personal dashboard. At the top, there are navigation icons (back, forward, search), a URL bar with the address 'portal.azure.com/#@shinesacambricoutlook.onmicrosoft.com/dashboard/private/345fccde-ab98-4697-a6c...', and a search bar labeled 'Search resources, services, and docs'. Below the header is a blue navigation bar with the text 'Microsoft Azure' and a dropdown menu 'My Dashboard'. The main content area is divided into two sections: 'All resources' on the left and 'Quickstarts + tutorials' on the right.

All resources

All subscriptions

- ManagedID
- tsecstorage
- DefaultWorkspace-fdb... Log Analytics works...
- risktest623
- RiskTest-nsg
- RiskValidation-vnet
- RiskValidation-vnet-ip
- RiskTest
- t-DevSentinel
- DefaultWorkspace-fdb... Log Analytics works...
- NetworkWatcher_australiaeast
- NetworkWatcher_centralus
- RiskTest-ip

See more...

Quickstarts + tutorials

- Azure getting started made easy! Launch an app of your choice on Azure in a few quick steps [Create DevOps Starter](#)
- Windows Virtual Machines Provision Windows Server, SQL Server, SharePoint VMs
- Linux Virtual Machines Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs
- App Service Create Web Apps using .NET, Java, Node.js, Python, PHP
- Functions Process events with a serverless code architecture
- SQL Database Managed relational SQL Database as a Service

Service Health Marketplace

Figure 1.10 – Microsoft Azure portal personal dashboard

The screenshot shows the Microsoft Azure portal's sign-in details page. The top navigation bar includes icons for search, refresh, and settings, along with the user's email 'shinesacambric@outlook.com' and 'DEFAULT DIRECTORY'. The Microsoft logo is on the left, and 'Sign out' is on the right. The main content area displays the user's profile picture (a camera icon), name 'Shinesa Cambric', email 'shinesacambric@outlook.com', and links to 'My Microsoft account' and 'Switch directory'. There is also a '...' button.

Figure 1.11 – Microsoft Azure portal sign-in details

Shinesa Cambric

shinesacambric@outlook.com

[My Microsoft account](#)



Figure 1.12 – Microsoft Azure portal account details

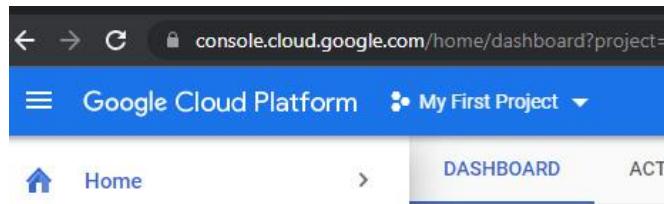


Figure 1.13 – GCP home page

A detailed screenshot of the Google Cloud Platform dashboard for the 'My First Project'. The left sidebar lists various services like Home, Recent, View all products, Marketplace, Billing, APIs & Services, Support, IAM & Admin, Getting started, Compliance, Security, Anthos, Compute Engine, Kubernetes Engine, VMware Engine, and Distributed Cloud. The main dashboard area has several cards: 'Project info' (Project name: My First Project, Project number: 56105575590, Project ID: metal-air-304103), 'API APIs' (Requests (requests/sec) chart from 6:15 to 7 PM), 'Google Cloud Platform status' (All services normal), 'Monitoring' (Create my dashboard, Set up alerting policies, Create uptime checks, Go to Monitoring), 'API Error Reporting' (No sign of any errors. Have you set up Error Reporting?, Learn how to set up Error Reporting), and 'News' (How to manage data on Cloud VMs: A conversation, What's new in cloud-native apps?, Announcing Serverless Spark components for Vertex AI Pipelines). A search bar at the top is set to 'Products, resources, docs'.

Figure 1.14 – GCP home page dashboard

Links

Additional resources on shared responsibility with the three major CSPs can be found in the following list:

- **Shared Responsibility Model, Amazon Web Services (AWS) Elastic Compute Cloud (EC2):** <https://aws.amazon.com/compliance/shared-responsibility-model/>
- **Shared Responsibility Model, Microsoft Azure:** <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
- **Shared Responsibility Model, GCP:** <https://cloud.google.com/blog/products/identity-security/google-cloud-security-foundations-guide>
- **Cloud Security Alliance explains shared responsibility:** <https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/>

Chapter 2

Links

- In AWS, these reports are available in Amazon Artifact: <https://aws.amazon.com/artifact/>.
- In Azure, the reports are available in Microsoft Trust Center: <https://www.microsoft.com/en-us/security>.
- Finally, in GCP, the reports are available in Google Compliance Reports Manager: <https://cloud.google.com/security/compliance/compliance-reports-manager>.
- You can refer to the AWS Security Hub documentation at <https://docs.aws.amazon.com/securityhub/index.html> for more information.
- The Microsoft Defender for Cloud documentation can be found at <https://docs.microsoft.com/en-us/azure/defender-for-cloud>.
- The Google Security Command Center documentation can be found at <https://cloud.google.com/security-command-center/>.
- Google Cloud's Operations Suite documentation can be found at <https://cloud.google.com/products/operations>.
- The CIS AWS Security Benchmarks documentation can be found at https://www.cisecurity.org/benchmark/amazon_web_services.
- The CIS Microsoft Azure Benchmarks documentation can be found at <https://www.cisecurity.org/benchmark/azure>.
- The CIS GCP Benchmarks documentation can be found at https://www.cisecurity.org/benchmark/google_cloud_computing_platform.

Figures

The screenshot shows the AWS Security Hub interface. On the left, there's a sidebar with links for Summary, Security standards, Insights (which is currently selected), Findings, Integrations, Settings, and What's new. The main area is titled "Insights (35)" and contains a search bar and a dropdown menu set to "All insights". Below this are six cards, each representing a different type of security finding:

- 1. AWS resources with the most findings: Security Hub managed insight, 1 current result, 90-day finding trend.
- 2. S3 buckets with public write or read permissions: Security Hub managed insight, 0 current result, 90-day finding trend.
- 3. IAMs that are generating the most findings: Security Hub managed insight, 0 current result, 90-day finding trend.
- 4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs): Security Hub managed insight, 0 current result, 90-day finding trend.
- 5. AWS principals with suspicious access key activity: Security Hub managed insight, 2 current result, 90-day finding trend.
- 6. AWS resources instances that don't meet security standards / best practices: Security Hub managed insight, 0 current result, 90-day finding trend.

Figure 2.1 – Interface of AWS Security Hub



Figure 2.2 – Trusted Advisor interface

The AWS Config interface shows a list of resources categorized by type and compliance status. The sidebar includes links for Dashboard, Conformance packs, Rules, Resources (which is selected), Aggregators, Advanced queries, Settings, What's new, Documentation, Partners, FAQs, Pricing, and Share feedback.

Resource identifier	Type	Compliance
cloud_user	IAM User	Noncompliant
vol-006d50ce2a61c2314	EC2 Volume	Noncompliant
vol-0f43af40f66bb4a574	EC2 Volume	Noncompliant
vol-050be45c05048575	EC2 Volume	Noncompliant
sg-011f34d1d115905738	EC2 SecurityGroup	Noncompliant
sg-068e32db8848463c2c	EC2 SecurityGroup	Noncompliant
sg-0e02defffb5003ff2	EC2 SecurityGroup	Noncompliant
aws-athena-query-results-218650569701-us-east-1	S3 Bucket	Noncompliant
aws-cloudtrail-logs-218650569701-501b03ed	S3 Bucket	Noncompliant
config-bucket-218650569701	S3 Bucket	Noncompliant

Figure 2.3 – AWS Config interface

The screenshot shows the Amazon Inspector interface with the following details:

- Inspector** sidebar: Includes links for Dashboard, Findings (selected), By vulnerability, By instance, By container image, By repository, All findings, and Suppression rules.
- Findings: All findings** section: Shows 2 findings, both Medium severity and Unhealthy.
- Filtering and Actions:** Buttons for Export findings and Create suppression rule, along with a dropdown for Active status and a search bar for Add filter.
- Table:** Displays findings with columns for Severity, Title, and Impacted resource.

Severity	Title	Impacted resource
Medium	Port 22 is reachable from an Internet Gateway	i-0d298e4aa6e9aeb04
Medium	Port 3389 is reachable from an Internet Gateway	i-022cc3ba9c7998e81

Figure 2.4 – Amazon Inspector interface

The screenshot shows the Microsoft Defender for Cloud interface with the following details:

- Left sidebar:** Includes General (Overview, Getting started, Recommendations, Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems, Cloud Security, Security posture, Regulatory compliance, Workload protections, Firewall Manager, Management).
- Header:** Microsoft Azure, Search resources, services, and docs (G+), Home > Microsoft Defender for Cloud, Showing subscription 'P0-Real Hands-On Lab'.
- Recommendations section:** Secure score recommendations (High 1/6, High 1/4, High 0/4) and All recommendations (Unhealthy 1, Healthy 2, Not applicable 2).
- Search and Filter:** Search recommendations, Recommendation status == None, Severity == None, Add filter, More (4), Show my items only (Off).
- Table:** Displays recommendations with columns for Severity, Name, Status, Initiatives, Unhealthy resources, and Insights.

Severity	Name	Status	Initiatives	Unhealthy resources	Insights
High	Adaptive application controls for defining safe applications should be applied on all virtual machines.	Completed	ASC Default	0 of 1 virtual machines	
High	Adaptive network hardening recommendations should be applied on all virtual machines.	Completed	ASC Default	0 of 1 virtual machines	
High	Management ports of virtual machines should be protected with just-in-time security.	Completed	ASC Default	0 of 1 virtual machines	3
High	Allowlist rules in your adaptive application control policy should be defined for all virtual machines.	Completed	ASC Default	0 of 1 virtual machines	
High	All network ports should be restricted on network security groups at the instance level.	Completed	ASC Default	0 of 1 virtual machines	
Medium	Internet-facing virtual machines should be connected with network security groups.	Inacce... (Inacce...)	ASC Default	1 of 1 virtual machines	Red

Figure 2.5 – Microsoft Defender for Cloud

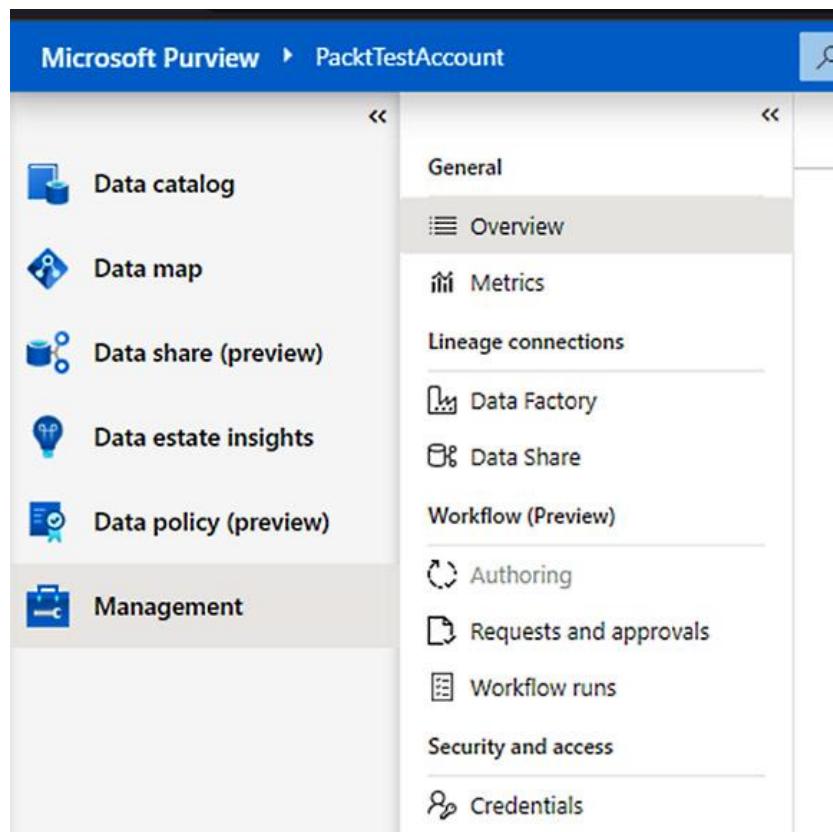


Figure 2.6 – Microsoft Purview

The screenshot shows the Google Security Command Center interface. The left sidebar lists various security services: Security Command Center, reCAPTCHA Enterprise, BeyondCorp Enterprise, Policy Troubleshooter for ..., Identity-Aware Proxy, Access Context Manager, VPC Service Controls, Binary Authorization, Data Loss Prevention, Key Management, Certificate Authority Serv..., Secret Manager, and Risk Manager. The 'Security Command Center' service is selected.

The main content area has tabs for OVERVIEW, VULNERABILITIES (selected), ASSETS, FINDINGS, SOURCES, and EXPLORE. The VULNERABILITIES tab displays a table of findings:

Status	Last scanned	Category	Recommendation	Active	Severity	Standards
⚠️	August 30, 2022 at 3:01:56 PM GMT-5	MFA not enforced	Multi-factor authentication should be enabled for all users in your org unit	1	Medium	CIS 1.0.1.2, CIS 1.1.12, CIS 1.2.1.2, PCI 8.3, NIST: IA-2, ISO: A.9.4.2
🟢	August 30, 2022 at 2:21:56 PM GMT-5	Dataproc: Image	Dataproc clusters should not use images affected by Log4j vulnerability	0	Medium	CIS 1.0.1.1, CIS 1.1.1.1, CIS 1.2.1.1, PCI 7.1.2, NIST: AC-3, ISO: A.9.2.3
🟡	N/A	Non org IAM me...	Corporate login credentials should be used instead of Gmail accounts	0	Medium	PCI 1.2.1, NIST: SC-7, ISO: A.13.1.1
🟡	N/A	Open ciscosecur...	Firewall rules should not allow connections from all IP addresses on TCP port 9090	0	Medium	PCI 1.2.1, NIST: SC-7, ISO: A.13.1.1
🟡	N/A	Open directory s...	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 445	0	Medium	PCI 1.2.1, NIST: SC-7, ISO: A.13.1.1
🟡	N/A	Open firewall	Firewall rules should not allow connections from all IP addresses	0	Medium	PCI 1.2.1

Figure 2.7 – Google Security Command Center

The screenshot shows the Google Cloud Monitoring interface. On the left, a sidebar menu includes 'Metrics Scope' (1 project), 'Overview', 'Dashboards' (selected), 'Integrations', 'Services', 'Metrics explorer', 'Alerting', 'Uptime checks', 'Groups', 'Managed Prometheus', 'Permissions', and 'Settings'. The main area is titled 'Dashboards Overview' with a '+ CREATE DASHBOARD' button. It features tabs for 'DASHBOARD LIST' (selected) and 'SAMPLE LIBRARY'. Below this is a 'Categories' section with filters for 'All', 'Recently Viewed', 'Favorites', 'Custom', 'GCP', 'Integrations', and 'Other'. A 'Labeled' section follows. To the right is a 'All Dashboards' table with columns for 'Name', 'Type', and 'Last updated'. The table lists four dashboards: 'Disks' (Google Cloud Platform, last updated 2 days ago), 'Firewalls' (Google Cloud Platform, last updated 2 days ago), 'Infrastructure Summary' (Google Cloud Platform, last updated 2 days ago), and 'VM Instances' (Google Cloud Platform, last updated 2 days ago).

	Name	Type	Last updated
1	Disks	Google Cloud Platform	2 days ago
2	Firewalls	Google Cloud Platform	2 days ago
3	Infrastructure Summary	Google Cloud Platform	2 days ago
4	VM Instances	Google Cloud Platform	2 days ago

Figure 2.8 – Cloud Monitoring

Chapter 3

Figures

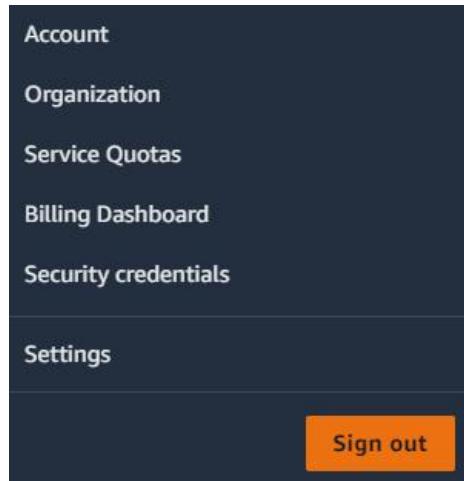


Figure 3.1 – Navigating to the Organization configuration settings

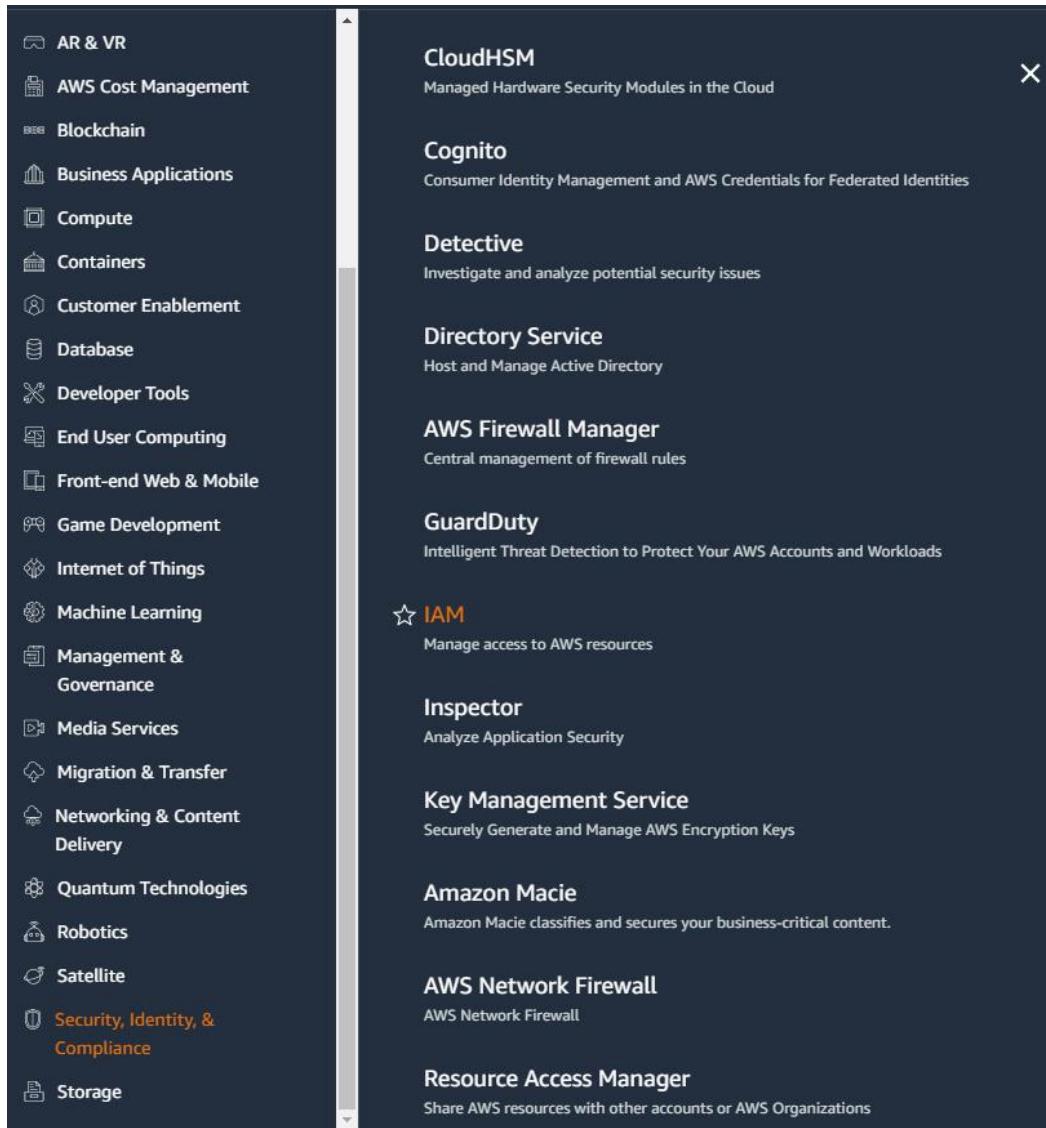


Figure 3.2 – AWS navigation to IAM configuration

The screenshot shows the AWS Identity and Access Management (IAM) dashboard. On the left, there's a sidebar with navigation links: Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access analyzer, Archive rules, Analyzers, Settings), and a search bar labeled "Search IAM". The main content area is titled "IAM dashboard" and contains sections for "Security recommendations" and "IAM resources". Under "Security recommendations", two items are listed: "Root user has MFA" (Having multi-factor authentication (MFA) for the root user improves security for this account) and "Root user has no active access keys" (Using access keys attached to an IAM user instead of the root user improves security). Under "IAM resources", a table provides counts for User groups (1), Users (0), Roles (3), Policies (0), and Identity providers (0). A "What's new" section at the bottom right includes a "View all" link.

Figure 3.3 – AWS IAM configurations

The screenshot shows the Microsoft Azure "All services | Identity" page. At the top, there's a header with the Microsoft Azure logo and a search bar labeled "Search resources, services, and docs (G+)". The main content area is titled "All services | Identity". On the left, there's a sidebar with a "Categories" section containing links for General, Compute, Networking, Storage, Web, Mobile, Containers, Databases, Analytics, AI + machine learning, Internet of things, Mixed reality, Integration, Identity (which is highlighted in grey), and Security. To the right, there's a list of Azure identity services, each with an icon and a name: Azure Active Directory, Azure AD B2C, Azure AD Domain Services, Azure Information Protection, Groups, Users, Azure AD Connect Health, Enterprise applications, Identity Governance, Azure AD Conditional Access, Managed Identities, Azure AD Privileged Identity Management, Azure AD Security, Azure AD Identity Protection, User settings, AD Connect, App proxy, Security, Tenant properties, Administrative units, Azure AD roles and administrators, Create custom Azure AD roles, and External Identities.

Figure 3.4 – Microsoft Azure IAM configurations

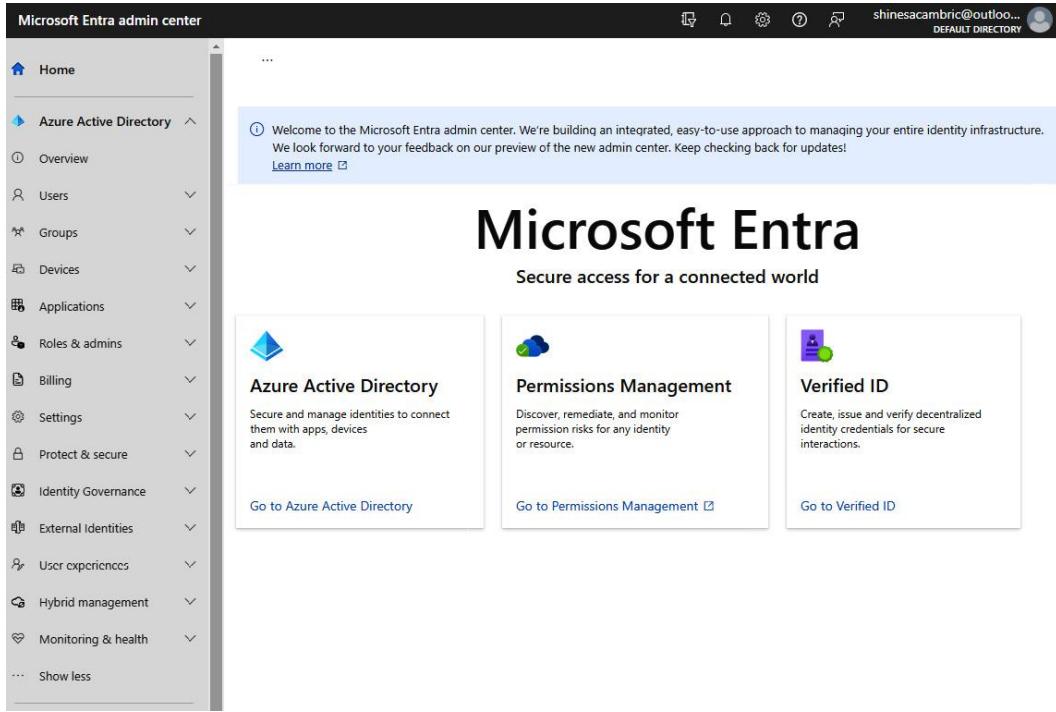


Figure 3.5 – Microsoft Entra admin center

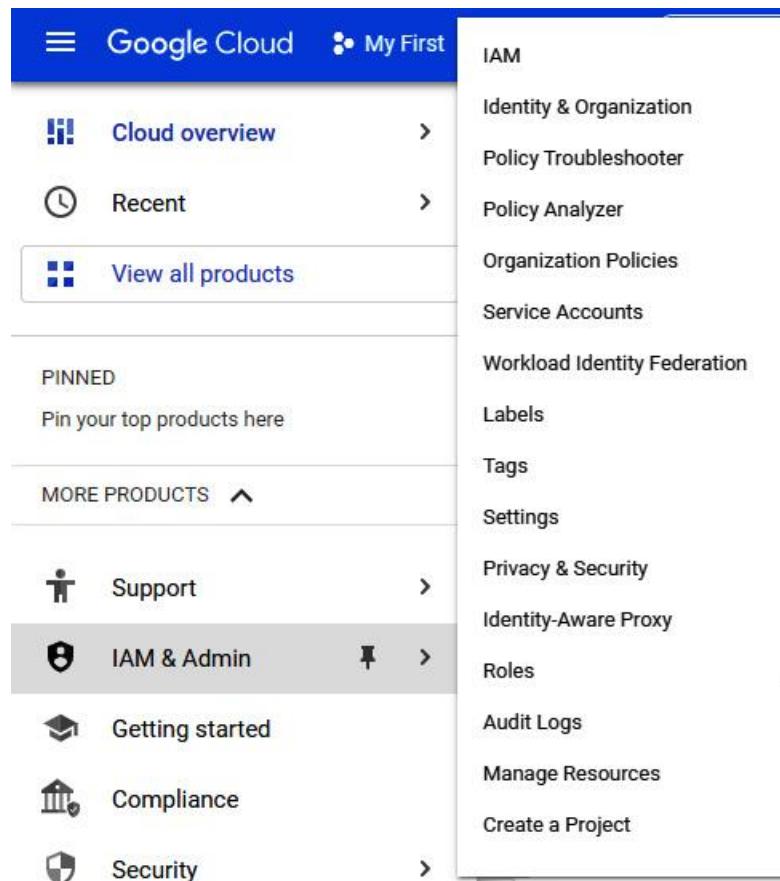


Figure 3.6 – GCP IAM & Admin configuration options

The screenshot shows the Google Cloud IAM & Admin interface. On the left, a sidebar lists various services: IAM, Identity & Organization (which is selected and highlighted in blue), Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federat..., Labels, Tags, Settings, Privacy & Security, and Identity-Aware Proxy. The main content area is titled "Identity" and contains the heading "Set up Google Cloud for your organization". It provides a brief overview of the setup checklist: "Use the Google Cloud setup checklist to set up Google Cloud for scalable, production-ready enterprise workloads. By completing the checklist, administrators for your organization can do the following:" followed by a bulleted list: "Manage user accounts and groups for employees", "Create organizational structure and centrally control all of your organization's projects and resources", and "Configure security guardrails". A "GO TO THE CHECKLIST" button is located at the bottom of this section.

Figure 3.7 – Establishing an organization within GCP

The screenshot shows the AWS IAM Policies page. The top navigation bar includes "IAM" and "Policies". The main content area has a title "Policies (954) Info" and a sub-instruction "A policy is an object in AWS that defines permissions.". Below this is a search bar with the placeholder "Filter policies by property or policy name and press enter". To the right of the search bar are "Actions" and a "New policy" button. At the bottom of the table are navigation links for pages 1 through 7. The table itself has columns: "Policy name", "Type", and "Used as". The data rows list various AWS managed policies:

Policy name	Type	Used as
AWSDirectConnectReadOnlyAccess	AWS managed	Permissions policy (1)
AmazonGlacierReadOnlyAccess	AWS managed	None
AWSMarketplaceFullAccess	AWS managed	None
ClientVPNServiceRolePolicy	AWS managed	None
AWSSSODirectoryAdministrator	AWS managed	None
AWSIoT1ClickReadOnlyAccess	AWS managed	None
AutoScalingConsoleReadOnlyAccess	AWS managed	None
AmazonDMSRedshiftS3Role	AWS managed	None
AWSQuickSightListIAM	AWS managed	None

Figure 3.8 – List of available AWS managed policies

IAM > Roles > AWSServiceRoleForSecurityHub

AWSServiceRoleForSecurityHub

A service-linked role required for AWS Security Hub to access your resources.

Summary

Delete **Edit**

Creation date	ARN
June 19, 2022, 17:46 (UTC-05:00)	arn:aws:iam::434972163851:role/aws-service-role/securityhub.amazonaws.com/AWSServiceRoleForSecurityHub
Last activity	Maximum session duration
1 hour ago	1 hour

Permissions **Trust relationships** **Tags** **Access Advisor**

Permissions policies (1)

Policy name	Type	Attached entities
AWSecurityHubServiceRolePolicy	AWS managed	1

Figure 3.9 – AWS time-bound access

Organization policies

HELP ASSISTANT

Organization policies for project "My First Project"

Cloud Organization Policies let you constrain access to resources at and below this organization, folder or project. You can edit restrictions on the policy detail page.

Filter Filter by policy name or ID

Name	ID	Inheritance
Allow extending lifetime of OAuth 2.0 access tokens to up to 12 hours	constraints/iam.allowServiceAccountCredentialLifetimeExtension	Inherited
Allowed AWS accounts that can be configured for workload identity federation in Cloud IAM	constraints/iam.workloadIdentityPoolAwsAccounts	Inherited
Allowed Binary Authorization Policies (Cloud Run)	constraints/run.allowedBinaryAuthorizationPolicies	Inherited
Allowed Destinations for Exporting Resources	constraints/resourcemanager.allowedExportDestinations	Inherited
Allowed external Identity Providers for workloads in Cloud IAM	constraints/iam.workloadIdentityPoolProviders	Inherited
Allowed ingress settings (Cloud Functions)	constraints/cloudfunctions.allowedIngressSettings	Inherited
Allowed ingress settings (Cloud Run)	constraints/run.allowedIngress	Inherited
Allowed Integrations (Cloud Build)	constraints/cloudbuild.allowedIntegrations	Inherited
Allowed Sources for Importing Resources	constraints/resourcemanager.allowedImportSources	Inherited

Figure 3.10 – Example GCP organization policies with inheritance

Search by name or description Add filters

Role	Description	Type	...
<input type="checkbox"/> Application administrator	Can create and manage all aspects of app registrations and enterprise apps.	Built-in	...
<input type="checkbox"/> Application developer	Can create application registrations independent of the 'Users can register ...	Built-in	...
<input type="checkbox"/> Attack payload author	Can create attack payloads that an administrator can initiate later.	Built-in	...
<input type="checkbox"/> Attack simulation administrator	Can create and manage all aspects of attack simulation campaigns.	Built-in	...
<input type="checkbox"/> Attribute assignment administrator	Assign custom security attribute keys and values to supported Azure AD obj...	Built-in	...
<input type="checkbox"/> Attribute assignment reader	Read custom security attribute keys and values for supported Azure AD obj...	Built-in	...
<input type="checkbox"/> Attribute definition administrator	Define and manage the definition of custom security attributes.	Built-in	...
<input type="checkbox"/> Attribute definition reader	Read the definition of custom security attributes.	Built-in	...
<input type="checkbox"/> Authentication administrator	Has access to view, set, and reset authentication method information for an...	Built-in	...
<input type="checkbox"/> Authentication policy administrator	Can create and manage all aspects of authentication methods and passwor...	Built-in	...
<input type="checkbox"/> Azure AD joined device local administrator	Users assigned to this role are added to the local administrators group on ...	Built-in	...
<input type="checkbox"/> Azure Auditor	Azure Auditor	Custom	...

Figure 3.11 – Example Azure built-in and custom roles

All services > Default Directory >

Devices | Overview Default Directory - Azure Active Directory

Overview Got feedback? << ...

Overview Monitoring Tutorials

Search by name, device ID, or object ID

Overview

All devices Device settings Enterprise State Roaming BitLocker keys (Preview) Diagnose and solve problems

Activity Audit logs Bulk operation results (Preview)

Troubleshooting + Support New support request

Alerts

Stale devices 0 Devices stale for 6+ months. See all stale devices

Noncompliant devices 0 This number may not reflect all recent changes. See all noncompliant devices

Unmanaged devices 0 This number may not reflect all recent changes. See all unmanaged devices

Figure 3.12 – Example Microsoft Azure device policy overview

Links

To learn more about default authentication and authorization settings, check out the following links:

- AWS: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html
- Azure: <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults> and <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions>
- GCP: <https://cloud.google.com/iam/docs/overview>

- To find a comprehensive list of CIS benchmark controls, go to <https://www.cisecurity.org/benchmark>.
- You can access more on the CCM matrix from CSA at <https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4>. Please note that the matrix is periodically updated, so be sure you are accessing the latest version.
- Direct navigation to the IAM console is also possible through <https://console.aws.amazon.com/iam/>.
- You can access more information on installing and using the AWS CLI at <https://aws.amazon.com/cli>, and you can find command references specific to IAM at <https://docs.aws.amazon.com/cli/latest/reference/iam/index.html>.
- Microsoft has developed a new branded administrator experience for Azure Active Directory IAM functions that can be found at <https://entra.microsoft.com/>
- Permission requirements for accessing and configuring these functions remain the same as accessing the administrative functions through <https://portal.azure.com>.
- Documentation and information on installing and using the Azure CLI, including tutorials, can be found at <https://learn.microsoft.com/en-us/cli/azure>.
- Learn more about specific access permissions and policies within AWS by going to <https://docs.aws.amazon.com/IAM/latest/UserGuide/access.html>
- You can find more in-depth information on these at <https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html> and <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>.
- You can get more details on roles and permissions at <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>:
- More information about these capabilities can be found at <https://learn.microsoft.com/en-us/azure/active-directory/identity-protection>.
- You can learn more about these, and other roles, at <https://cloud.google.com/iam/docs/understanding-roles>.
- You can learn more at <https://cloud.google.com/iam/docs/overview>.
- You can find more information about each of these features at <https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/monitoring-and-logging.html>.
- To find out more information about these features, please visit <https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring>.

- You can learn more about GCP Cloud Logging at
<https://cloud.google.com/logging/docs/audit/>.

Chapter 4

Figures

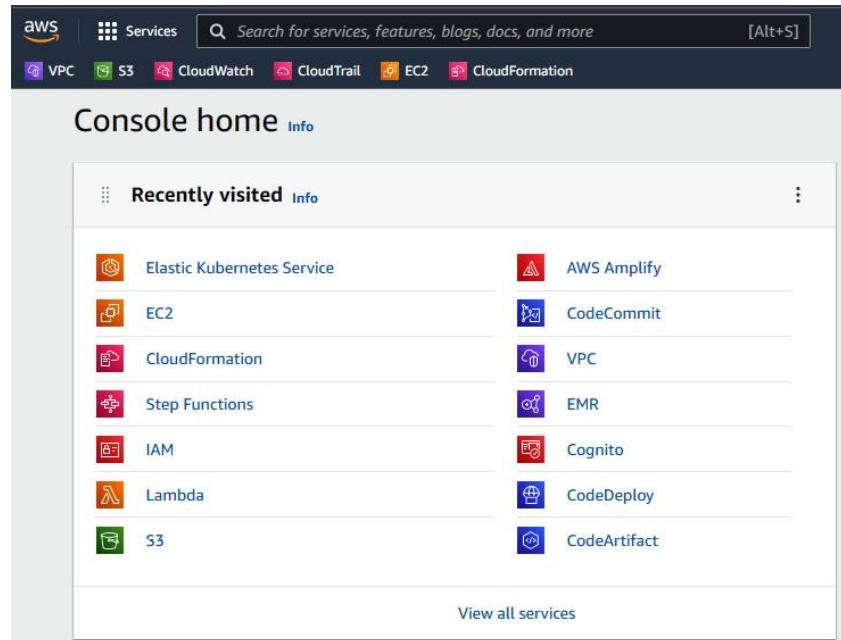


Figure 4.1 – AWS Console home

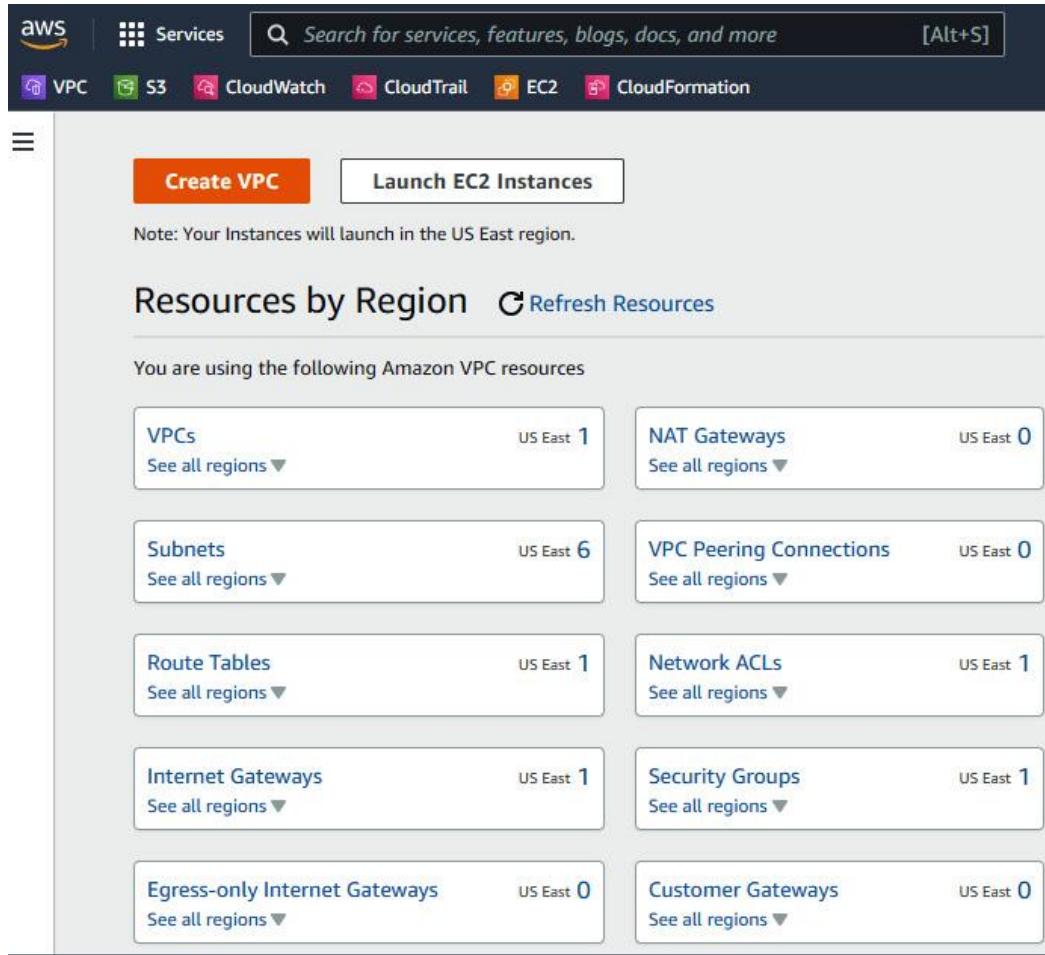


Figure 4.2 – AWS – Resources by Region

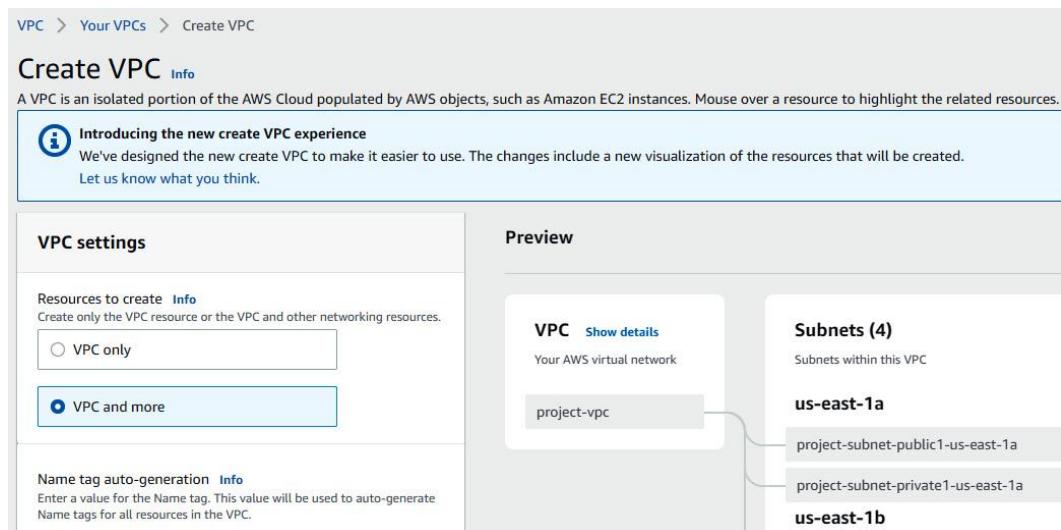


Figure 4.3 – AWS Create VPC configuration options

IPv4 CIDR block [Info](#)
 Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16	65,536 IPs
-------------	------------

IPv6 CIDR block [Info](#)

- No IPv6 CIDR block
- Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Default	▼
---------	---

Number of Availability Zones (AZs) [Info](#)
 Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1	2	3
---	---	---

► **Customize AZs**

Figure 4.4 – AWS Create VPC – IP address options

Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0	2
---	---

Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0	2	4
---	---	---

► **Customize subnets CIDR blocks**

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None	In 1 AZ	1 per AZ
------	---------	----------

VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None	S3 Gateway
------	------------

Figure 4.5 – AWS Create VPC – subnet options

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None	In 1 AZ	1 per AZ
------	---------	----------

VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None	S3 Gateway
------	------------

DNS options [Info](#)

- Enable DNS hostnames
- Enable DNS resolution

[Cancel](#)

[Create VPC](#)

Figure 4.6 – AWS Create VPC – NAT gateway options, VPC endpoints, and DNS options

Creating VPC Resources

Thank you for using the new create VPC experience. Let us know what you think.

Success

▼ Details

- Create VPC: [vpc-0f44770a31005476b](#) 
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: [vpc-0f44770a31005476b](#) 
- Create S3 endpoint: [vpce-08d7d7dafcf4a724d](#) 
- Create subnet: [subnet-06298802f05f19d7c](#) 
- Create subnet: [subnet-0011f053d2f99b9a0](#) 
- Create subnet: [subnet-09de4aa8b01422f17](#) 
- Create subnet: [subnet-0f7da1ea703f80172](#) 
- Create internet gateway: [igw-03e8a166dd614ce6e](#) 
- Attach internet gateway to the VPC
- Create route table: [rtb-047bee77b3117948d](#) 
- Create route
- Associate route table
- Associate route table
- Create route table: [rtb-0724ee59265204497](#) 
- Associate route table
- Create route table: [rtb-0a311cc736f41c3ef](#) 
- Associate route table
- Verifying route table creation
- Associate S3 endpoint with private subnet route tables: [vpce-08d7d7dafcf4a724d](#) 

View VPC

Figure 4.7 – AWS – Creating VPC Resources

The screenshot shows the AWS VPC configuration for a VPC named 'vpc-Of44770a31005476b / project-vpc'. The 'Details' tab is selected, displaying information such as VPC ID, State, DNS hostnames, DNS resolution, Tenancy, Default, Default VPC, Route 53 Resolver DNS Firewall rule groups, and Owner ID. Below the details, the 'CIDRs' tab is selected, showing a table with one entry for IPv4 with CIDR 10.0.0.0/16.

VPC ID	State	DNS hostnames	DNS resolution
vpc-Of44770a31005476b	Available	Enabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	dopt-0ba03a46b1c43dd55	rtb-0d0a28591f641b793	acl-0d6e023dd7afe80fe
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR (Network border group)
No	10.0.0.0/16	-	-
Route 53 Resolver DNS Firewall rule groups	Owner ID		
-	517432808191		

Address type	CIDR	Network Border Group	Pool
IPv4	10.0.0.0/16	-	-

Figure 4.8 – AWS VPC deployed

The screenshot shows the Azure Marketplace search results for 'Virtual network'. The search bar is set to 'Virtual network'. The results section displays five items: 'Virtual network' (Microsoft), 'Virtual network gateway' (Microsoft), 'Azure Virtual Network Endpoints Management' (KoçSistem Bilgi ve İletişim), 'Local network gateway' (Microsoft), and 'Network interface' (Microsoft). Each item has a 'Create' button and a heart icon.

Figure 4.9 – Azure portal

Create virtual network

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * ⓘ P2-Real Hands-On Labs

Resource group * ⓘ 1-7391f37c-playground-sandbox

[Create new](#)

Instance details

Name * AuditCloudTest

Region * West US

Figure 4.10 – Creating an Azure VNet

Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)

Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

[+ Add subnet](#) [Remove subnet](#)

<input type="checkbox"/> Subnet name	Subnet address range	NAT gateway
<input type="checkbox"/> default	10.0.0.0/24	-

[i](#) Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to

Figure 4.11 – Azure VNet IP address configuration options

Create virtual network ...

Basics IP Addresses **Security** Tags Review + create

BastionHost ⓘ Disable Enable

DDoS Protection Standard ⓘ Disable Enable

Firewall ⓘ Disable Enable

Figure 4.12 – Azure VNet security configuration options

Create virtual network ...

Validation passed

Basics IP Addresses Security Tags **Review + create**

Basics

Subscription	P2-Real Hands-On Labs
Resource group	1-7391f37c-playground-sandbox
Name	AuditCloudTest
Region	West US

IP addresses

Address space	10.0.0.0/16
Subnet	default (10.0.0.0/24)

Tags

None

Create < Previous Next > Download a template for automation

Figure 4.13 – Azure validation of VPC configuration

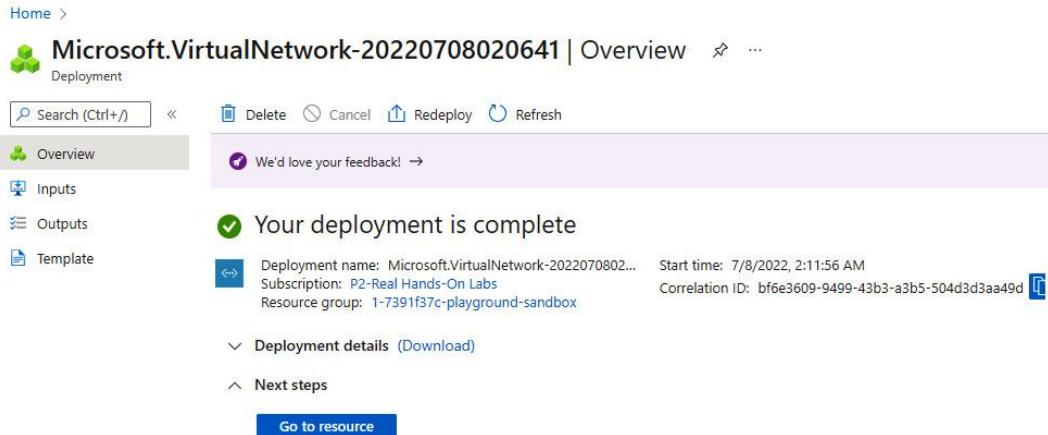


Figure 4.14 – Azure VNet deployed

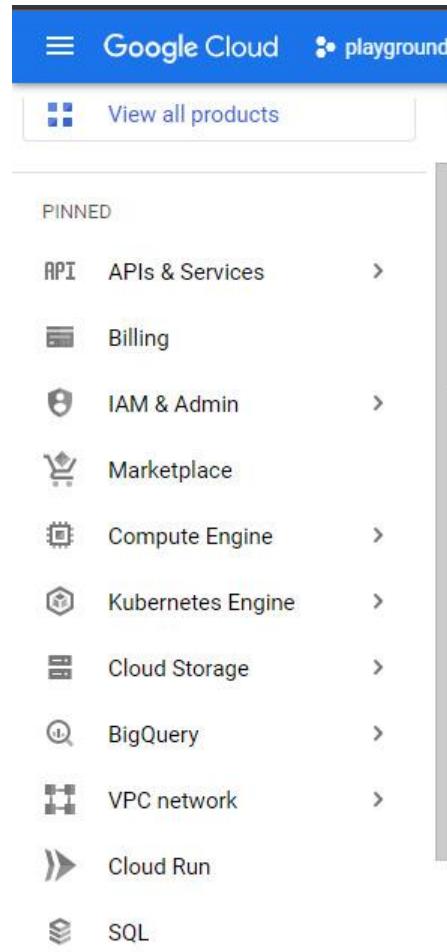


Figure 4.15 – Google Cloud Console

VPC networks [+ CREATE VPC NETWORK](#) [REFRESH](#)

Name	Region	Subnets	MTU	Mode	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateways
▼ default		11	1460	Auto	None			
	us-central1	default			10.128.0.0/20	None	None	10.128.0.1
	europe-west1	default			10.132.0.0/20	None	None	10.132.0.1
	us-west1	default			10.138.0.0/20	None	None	10.138.0.1
	us-east1	default			10.142.0.0/20	None	None	10.142.0.1
	us-east4	default			10.150.0.0/20	None	None	10.150.0.1
	australia-southeast1	default			10.152.0.0/20	None	None	10.152.0.1
	us-west2	default			10.168.0.0/20	None	None	10.168.0.1
	us-west3	default			10.180.0.0/20	None	None	10.180.0.1
	us-west4	default			10.182.0.0/20	None	None	10.182.0.1
	us-east5	default			10.202.0.0/20	None	None	10.202.0.1
	us-south1	default			10.206.0.0/20	None	None	10.206.0.1

Figure 4.16 – GCP VPC networks

[←](#) Create a VPC network

Name *

Lowercase letters, numbers, hyphens allowed

Description

Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. [Learn more](#)

Subnet creation mode

- Custom
- Automatic

Figure 4.17 – GCP – Create a VPC network

[←](#) Create a VPC network

Firewall rules [?](#)

Select any of the firewall rules below that you would like to apply to this VPC network. Once the VPC network is created, you can manage all firewall rules on the Firewall rules page.

IPV4 FIREWALL RULES		IPV6 FIREWALL RULES					
<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority 
<input type="checkbox"/>	auditcloudtest-allow-custom 	Ingress	Apply to all	IP ranges: 10.128.0.0/9	all	Allow	65,534
<input type="checkbox"/>	auditcloudtest-allow-icmp 	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65,534
<input type="checkbox"/>	auditcloudtest-allow-rdp 	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65,534
<input type="checkbox"/>	auditcloudtest-allow-ssh 	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65,534
	auditcloudtest-deny-all-ingress 	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Deny	65,535
	auditcloudtest-allow-all-egress 	Egress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	65,535

Dynamic routing mode [?](#)

Regional

Cloud Routers will learn routes only in the region in which they were created

Global

Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

Figure 4.18 – GCP – Firewall rules configuration options

[← Create a VPC network](#)

<input type="checkbox"/>	auditcloudtest-allow-ssh ?	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65,534
<input type="checkbox"/>	auditcloudtest-deny-all-ingress ?	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Deny	65,535
<input type="checkbox"/>	auditcloudtest-allow-all-egress ?	Egress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	65,535

Dynamic routing mode [?](#)

Regional
Cloud Routers will learn routes only in the region in which they were created

Global
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

Enable DNS API to pick a DNS policy [ENABLE](#)

Maximum transmission unit (MTU) —
1460

[CREATE](#) [CANCEL](#)

EQUIVALENT COMMAND LINE ▾

Figure 4.19 – GCP – creating VPC resources

VPC networks		+ CREATE VPC NETWORK	REFRESH					
Name ↑	Region	Subnets	MTU ?	Mode	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateways
auditcloudtest	us-central1	auditcloudtest	1460	Auto	None			
	europe-west1	auditcloudtest			10.128.0.0/20	None	None	10.128.0.1
	us-west1	auditcloudtest			10.132.0.0/20	None	None	10.132.0.1
	us-east1	auditcloudtest			10.138.0.0/20	None	None	10.138.0.1
	us-east4	auditcloudtest			10.142.0.0/20	None	None	10.142.0.1
	australia-southeast1	auditcloudtest			10.150.0.0/20	None	None	10.150.0.1
	us-west2	auditcloudtest			10.152.0.0/20	None	None	10.152.0.1
	us-west3	auditcloudtest			10.168.0.0/20	None	None	10.168.0.1
	us-west4	auditcloudtest			10.180.0.0/20	None	None	10.180.0.1
	us-east5	auditcloudtest			10.182.0.0/20	None	None	10.182.0.1
	us-south1	auditcloudtest			10.202.0.0/20	None	None	10.202.0.1
default	us-central1	default	1460	Auto	None			
	europe-west1	default			10.128.0.0/20	None	None	10.128.0.1
	us-west1	default			10.132.0.0/20	None	None	10.132.0.1
	us-west1	default			10.138.0.0/20	None	None	10.138.0.1

Figure 4.20 – GCP VPC deployed

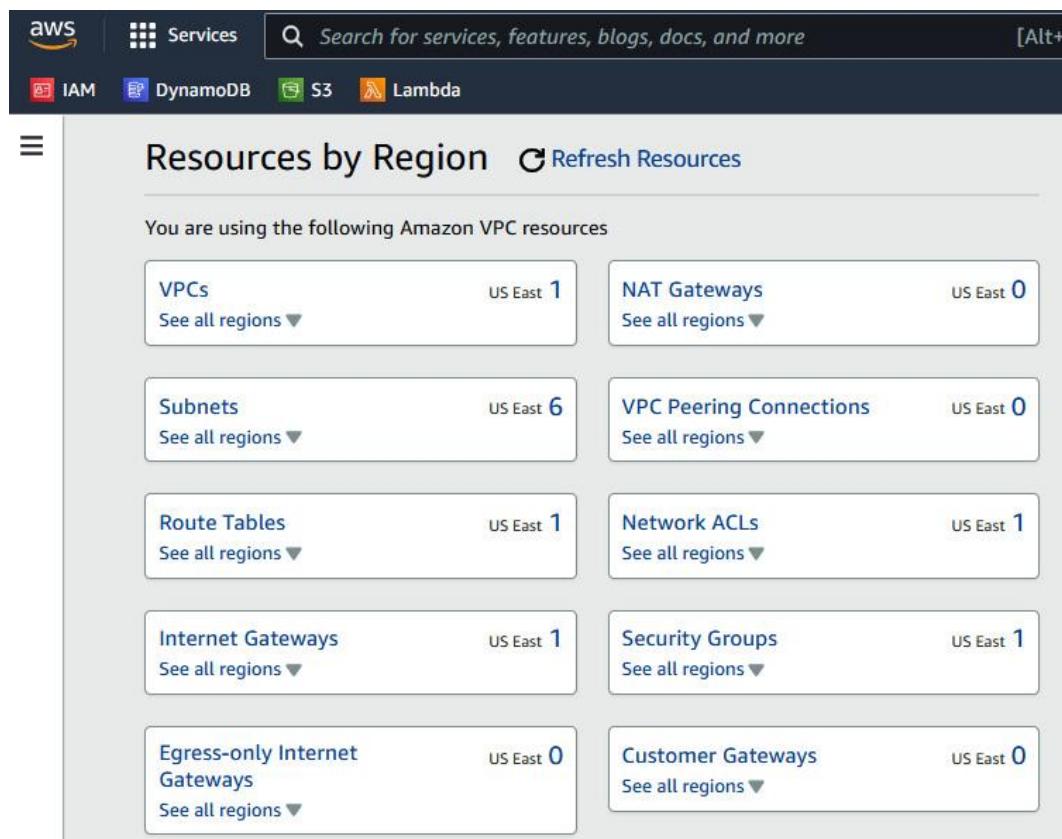


Figure 4.21 – AWS Resources by Region

The screenshot shows the 'Network ACLs' list page in the AWS Management Console. The header includes a search bar, a refresh button, an 'Actions' dropdown, and a 'Create network ACL' button. The main area displays a table with one item:

Name	Network ACL ID	Associated with	Default	VPC ID
-	acl-0db0d6d6dda4bbc...	6 Subnets	Yes	vpc-06d88e2a30646ca53

Figure 4.22 – AWS – Network ACLs

Inbound rules	Outbound rules	Subnet associations	Tags		
You can now check network connectivity with Reachability Analyzer					
Run Reachability Analyzer X					
Inbound rules (2)					
<input type="text"/> Filter inbound rules					
Rule number ▾ Type ▾ Protocol ▾ Port range ▾ Source ▾ Allow/Deny ▾					
100	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Deny

Figure 4.23 – AWS Inbound rules

Inbound rules	Outbound rules	Subnet associations	Tags		
You can now check network connectivity with Reachability Analyzer					
Run Reachability Analyzer X					
Outbound rules (2)					
<input type="text"/> Filter outbound rules					
Rule number ▾ Type ▾ Protocol ▾ Port range ▾ Destination ▾ Allow/Deny ▾					
100	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Allow
*	All traffic	All	All	0.0.0.0/0	<input checked="" type="checkbox"/> Deny

Figure 4.24 – AWS Outbound rules

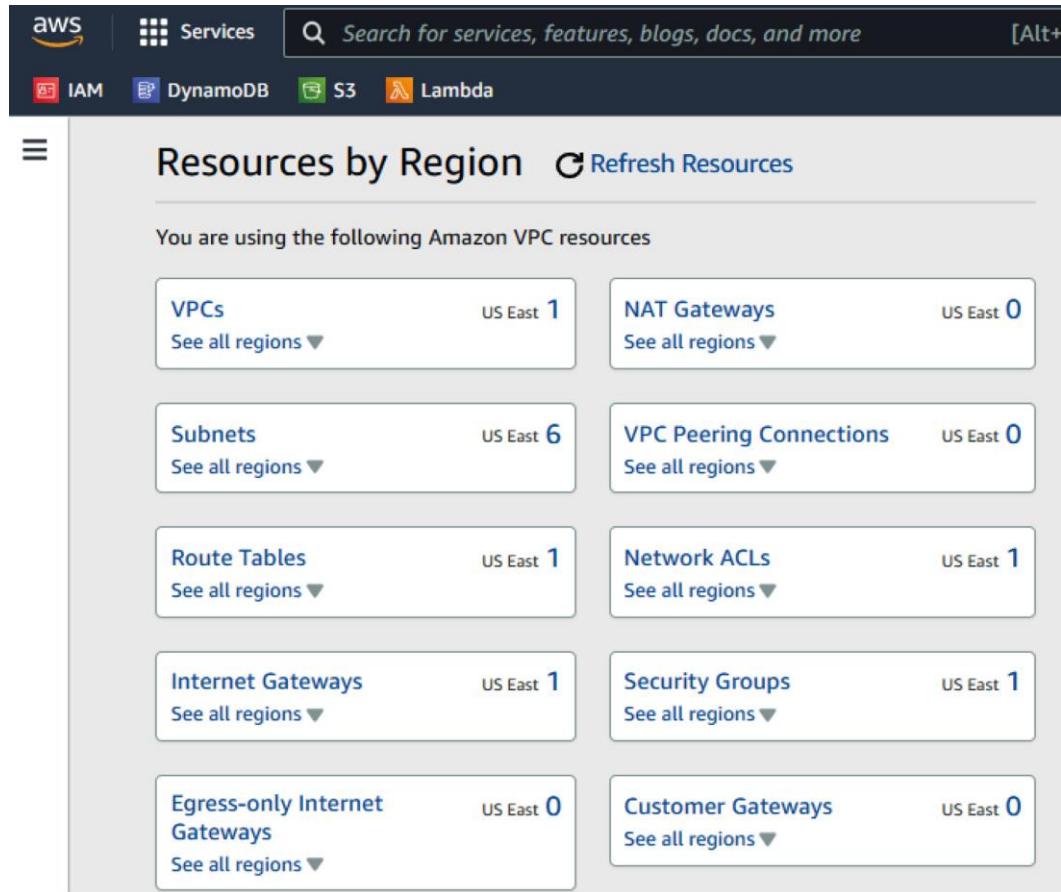


Figure 4.25 – AWS Resources by Region

The screenshot shows the 'Security Groups' page in the AWS Management Console. It displays one security group named 'default'. The table includes columns for Name, Security group ID, Security group name, VPC ID, and Description.

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0474f3f4c4b43b222	default	vpc-095a4cb2f2274af88	default VPC security gr...

Figure 4.26 – AWS – Security Groups

VPC > [Security Groups](#) > sg-0474f3f4c4b43b222 - default

sg-0474f3f4c4b43b222 - default

[Actions ▾](#)

Details			
Security group name default	Security group ID sg-0474f3f4c4b43b222	Description default VPC security group	VPC ID vpc-095a4cb2f2274af88
Owner 967756262698	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

[Inbound rules](#) | [Outbound rules](#) | [Tags](#)

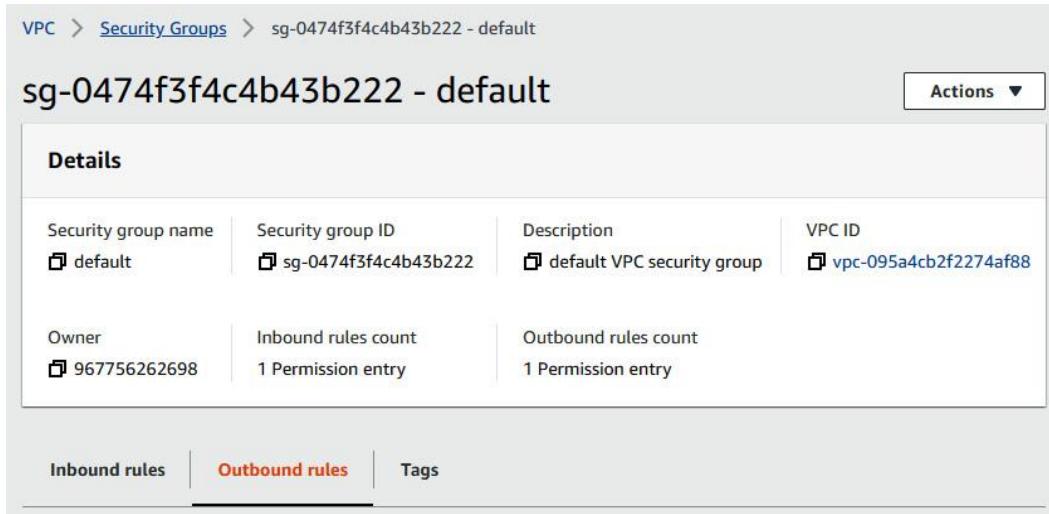


Figure 4.27 – AWS Security Group details

[Inbound rules](#) | [Outbound rules](#) | [Tags](#)

Inbound rules (1/1)

[C](#) [Manage tags](#) [Edit inbound rules](#)

Filter security group rules

<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol
<input checked="" type="checkbox"/>	-	sgr-02c41127fb7fd525d	-	All traffic	All

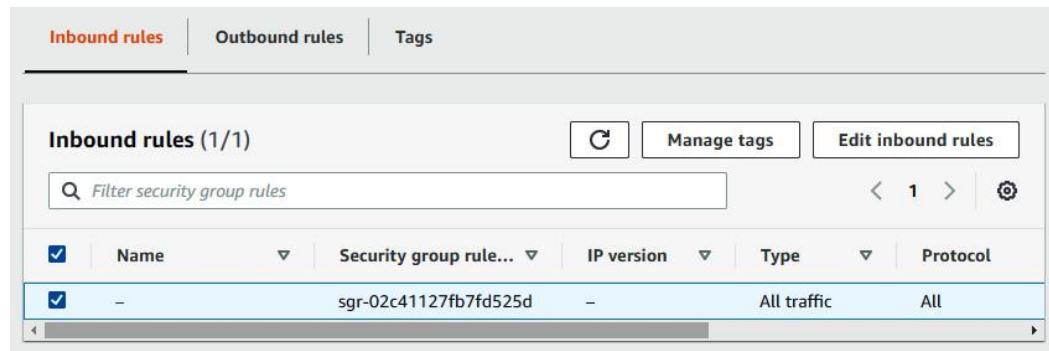


Figure 4.28 – AWS Inbound rules

[Inbound rules](#) | [Outbound rules](#) | [Tags](#)

Outbound rules (1/1)

[C](#) [Manage tags](#) [Edit outbound rules](#)

Filter security group rules

<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol
<input checked="" type="checkbox"/>	-	sgr-0ccc96229bc4e5d11	IPv4	All traffic	All

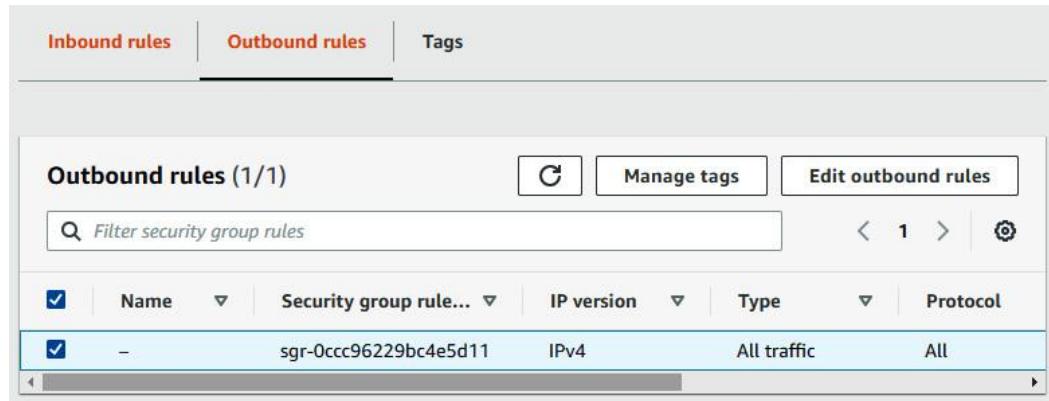


Figure 4.29 – AWS Outbound rules

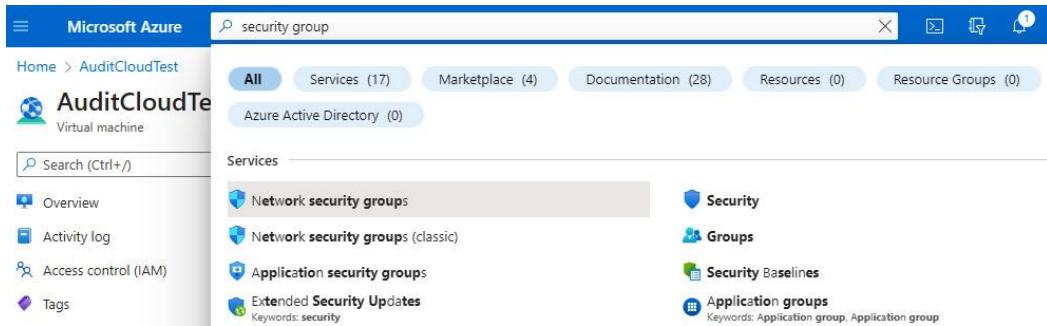


Figure 4.30 – Azure security group search

Priority	Name	Port	Protocol	Source	Destination	Action
300	⚠️ SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Figure 4.31 – Azure NSG – Inbound port rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Figure 4.32 – Azure NSG – Outbound port rules

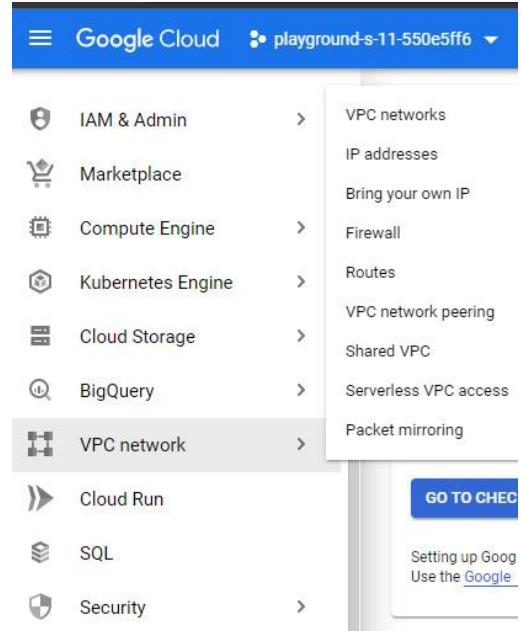


Figure 4.33 – Google Cloud Console

A screenshot of the "Firewall resources" section within the GCP VPC interface. The left sidebar lists: VPC networks, IP addresses, Bring your own IP, Firewall (which is selected and highlighted in blue), Routes, VPC network peering, Shared VPC, Serverless VPC access, and Packet mirroring. The main content area has two tabs: "VPC FIREWALL RULES" (selected) and "NETWORK FIREWALL POLICIES". There is also a "GO TO CHECK" button.

Figure 4.34 – GCP VPC – Firewall resources

Firewall					CREATE FIREWALL POLICY	HIDE INFO PANEL
VPC firewall rules						
Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more						
Note: App Engine firewalls are managed in the App Engine Firewall rules section .						
REFRESH	CONFIGURE LOGS	DELETE				
<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / po	
<input type="checkbox"/>	default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	▼
<input type="checkbox"/>	default-allow-internal	Ingress	Apply to all	IP ranges: 10.0.0.0/8	tcp:0-65535 udp:0-65535 icmp	▼
<input type="checkbox"/>	default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	▼
<input type="checkbox"/>	default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	▼

Figure 4.35 – GCP – VPC firewall rules

Network firewall policies			
REFRESH	DELETE		
<input type="checkbox"/>	Policy name	Firewall rules	Description
No rows to display			

Figure 4.36 – GCP VPC – Network firewall policies

AuditCloudTest

Virtual network

Resource group (move) : 1-7391f37c-playground-sandbox

Location (move) : West US

Subscription (move) : P2-Real Hands-On Labs

Subscription ID : 964df7ca-3ba4-48b6-a695-1ed9db5723f8

Address space : 10.0.0.0/16

DNS servers : Azure provided DNS service

Flow timeout : Configure

BGP community string : Configure

Virtual network ID : bef7ea00-1f23-406b-b9a0-659883f397e1

Tags (edit) : Click here to add tags

Capabilities (5)

Topology Recommendations Tutorials

- DDoS protection** : Configure additional protection from distributed denial of service. Status: Not configured.
- Azure Firewall** : Protect your network with a stateful L3-L7 firewall. Status: Not configured.
- Peerings** : Seamlessly connect two or more virtual networks. Status: Not configured.
- Security** : Filter network traffic to and from Azure resources.
- Private endpoints** : Privately access Azure services without sending traffic across.

Figure 4.37 – Azure VNet – Capabilities

Create a firewall

Basics Tags Review + create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more](#).

Project details

Subscription * : P2-Real Hands-On Labs

Resource group * : 1-7391f37c-playground-sandbox

[Create new](#)

Instance details

Name * :

Region * : West US

Availability zone : None

Figure 4.38 – Azure VNet – Create a firewall



Figure 4.39 – Azure VNet – DDoS protection

The screenshot shows the 'AuditCloudTest' Virtual network overview page. It displays basic information like Resource group, Location, Subscription, and Virtual network ID. Under 'Settings', the 'Capabilities' tab is selected, showing five items: 'DDoS protection' (Not configured), 'Azure Firewall' (Not configured), 'Peering' (Not configured), 'Security' (Not configured), and 'Private endpoints' (Not configured).

Figure 4.40 – Azure VNet – Peerings

Microsoft Azure Search resources, services, and docs (G+)

Home > AuditCloudTest >

Add peering

AuditCloudTest

Info For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.

This virtual network

Peering link name *

Traffic to remote virtual network ⓘ

Allow (default)

Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

Allow (default)

Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

Use this virtual network's gateway or Route Server

Use the remote virtual network's gateway or Route Server

Figure 4.41 – Azure VNet – Add peering

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia cloud_user @ 4702

EC2 Route 53 Simple Queue Service Systems Manager Elastic Container Registry CodeCommit IAM CloudFormation S3 VPC

New VPC Experience Tell us what you think

VPC dashboard EC2 Global View New Filter by VPC: Select a VPC

Default		dopt-06553b95962d3597d	rtb-0b4700cdecf990e39	acl-0ef267e3f1fb45bff
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR (Network border group)	
No	10.0.0.0/16	–	–	
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID	–	
Disabled	–	470272736787	–	

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways Carrier gateways DHCP option sets Elastic IPs

CIDRs Flow logs Tags

Flow logs (1/1) Info Actions Create flow log

Filter flow logs

Name	Flow log ID	Filter	Destination type
packtestflowlog	fl-0676b6b39ee887f07	ALL	cloud-watch-logs

Figure 4.42 – AWS VPC – Flow logs

Links

- At the time of writing, the benchmarks from the Center for Internet Security can be found at <https://www.cisecurity.org/cis-benchmarks>.

Chapter 5

Figures

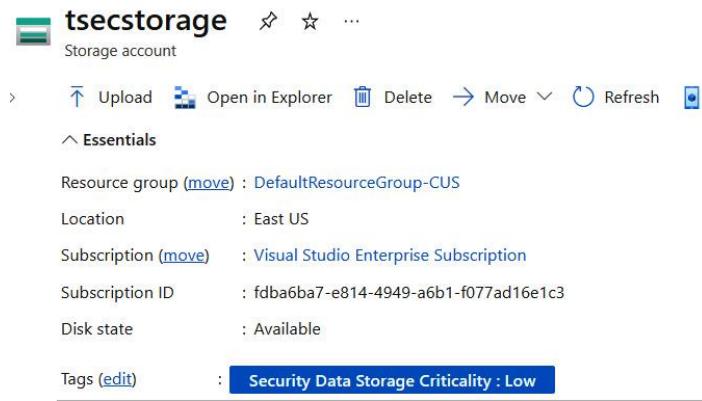


Figure 5.1 – Example Microsoft Azure resource tagging

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Tag names are case insensitive, but tag values are case sensitive. [Learn more about tags](#)

Subscriptions: Visual Studio Enterprise Subscription

The screenshot shows a list of tags under the 'Visual Studio Enterprise Subscription' section. A search bar at the top says 'Filter items...'. Below it, there is a sorting option 'Tags ↑↓' and two tags listed:

- Audit : Audit
- Security Data Storage Criticality : Low

Figure 5.2 – Microsoft Azure key-value tag pairing

The screenshot shows the Microsoft Azure Policy blade. At the top left is the Microsoft Azure logo and a navigation bar with 'Home > Policy'. A search bar contains the text 'policy'. Below the search bar are several filter buttons: 'All' (selected), 'Services (7)', 'Marketplace (13)', 'Documentation (20)', 'Azure Active Directory (3)', 'Resources (0)', and 'Resource Groups (0)'. The main content area has a 'Scope' section set to 'Visual Studio Enterprise Subscription'. A note says 'Compliance state change events are not available for Function, Logic App, or any other supported resource type'. Below this is an 'Overall resource compliance' section showing '25%' (1 out of 4). To the right is a 'Services' sidebar with links to 'Policy', 'Firewall Policies', 'Service endpoint policies', and 'Web Application Firewall policies (WAF)'. A link 'Continue searching in Azure Active Directory' is also present. At the bottom right of the sidebar is a 'Give feedback' button.

Figure 5.3 – Microsoft Azure Policy blade

The screenshot shows the Microsoft Azure Policy blade. It features two main sections: 'Resources by compliance state' (4 total, 1 compliant, 0 exempt, 3 non-compliant) and 'Non-compliant policies' (21 out of 206). Below these are tabs for 'Groups', 'Policies', 'Non-compliant resources', and 'Events', with 'Groups' being the active tab. A 'Filter by group name...' input field and a 'Subgroup : All subgroups' button are visible. Under the 'Non-compliant resources' tab, there is a table with columns: Name, Compliance, Subgroup, Non-compliant p..., and Total policies. Two rows are listed:

Name	Compliance	Subgroup	Non-compliant p...	Total policies
Enable threat detection capabilities	Non-compliant	Logging and Threat D...	4	16
Enable threat detection for identit...	Non-compliant	Logging and Threat D...	4	16

Figure 5.4 – Microsoft Azure Policy blade

AWS Resource Groups

- ▼ Resources
 - Create Resource Group
 - Saved Resource Groups
- ▼ Tagging
 - Tag Editor**
 - Tag Policies

What's new

Find resources to tag

You can search for resources that you want to tag across regions. Then, you can add, remove, or edit tags for resources in your search results. [Learn more](#)

Regions

Select regions ▾

us-east-1 X

Resource types

Select resource types ▾

All supported resource types X

Tags – Optional

Tag key ▾

Optional tag value ▾

Add

Figure 5.5 – AWS Resource Groups and tagging

Organization policies

Organization policies for project "My First Project"

Cloud Organization Policies let you constrain access to resources at and below this organization, folder or project. You can edit restrictions on the policy detail page.

Name	ID	Inheritance
Allow extending lifetime of OAuth 2.0 access tokens to up to 12 hours	constraints/iam.allowServiceAccountCredentialLifetimeExtension	Inherited
Allowed AWS accounts that can be configured for workload identity federation in Cloud IAM	constraints/iam.workloadIdentityPoolAwsAccounts	Inherited
Allowed Binary Authorization Policies (Cloud Run)	constraints/run.allowedBinaryAuthorizationPolicies	Inherited
Allowed Destinations for Exporting Resources	constraints/resourcemanager.allowedExportDestinations	Inherited
Allowed external identity Providers for workloads in Cloud IAM	constraints/iam.workloadIdentityPoolProviders	Inherited
Allowed ingress settings (Cloud Functions)	constraints/cloudfunctions.allowedIngressSettings	Inherited
Allowed ingress settings (Cloud Run)	constraints/run.allowedIngress	Inherited
Allowed Integrations (Cloud Build)	constraints/cloudbuild.allowedIntegrations	Inherited
Allowed Sources for Importing Resources	constraints/resourcemanager.allowedImportSources	Inherited
Allowed VPC Connector egress settings (Cloud Functions)	constraints/cloudfunctions.allowedVpcConnectorEgressSettings	Inherited
Allowed VPC egress settings (Cloud Run)	constraints/run.allowedVpcEgress	Inherited
Allowed VPC Service Controls mode for Anthos Service Mesh Managed Control Planes	constraints/meshconfig.allowedVpcscModes	Inherited
Allowed Worker Pools (Cloud Build)	constraints/cloudbuild.allowedWorkerPools	Inherited
Cloud Storage - restrict authentication types	constraints/storage.restrictAuthTypes	Inherited
Compute Storage resource use restrictions (Compute Engine disks, images, and snapshots)	constraints/compute.storageResourceUseRestrictions	Inherited
Datastream - Block Public Connectivity Methods	constraints/datasream.disablePublicConnectivity	Inherited

Figure 5.6 – Google Cloud Platform organizational-level policies

Home > RiskValidation

RiskValidation | Locks

Resource group

Search Add Subscription Refresh Feedback

Overview Activity log Access control (IAM) Tags Resource visualizer Events

Lock name Lock type Scope Notes

NoChanges	Read-only	RiskValidation	Block any changes
-----------	-----------	----------------	-------------------

Settings

This screenshot shows the Microsoft Azure Locks interface for a resource group named 'RiskValidation'. On the left, there's a sidebar with links for Overview, Activity log, Access control (IAM), Tags, Resource visualizer, and Events. The main area displays a table of locks. There is one lock entry: 'NoChanges' (Lock name), 'Read-only' (Lock type), 'RiskValidation' (Scope), and 'Block any changes' (Notes). A 'Settings' link is at the bottom of the table.

Figure 5.7 – Example Microsoft Azure read-only lock applied

Recently visited

Favorites

All services

Analytics

Application Integration

AR & VR

AWS Cost Management

Blockchain

Business Applications

Compute

Containers

Customer Enablement

Database

Developer Tools

End User Computing

Front-end Web & Mobile

Game Development

Cloud9
A Cloud IDE for Writing, Running, and Debugging Code

CloudShell
A browser-based shell with AWS CLI access from the AWS Management Console

CodeArtifact
Secure, scalable, and cost-effective artifact management for software development

CodeBuild
Build and Test Code

CodeCommit
Store Code in Private Git Repositories

CodeDeploy
Automate Code Deployments

CodePipeline
Release Software using Continuous Delivery

CodeStar
Quickly develop, build, and deploy applications

AWS FIS
Improve resiliency and performance with controlled experiments.

This screenshot shows the AWS Developer Tools page. The left sidebar lists recently visited services like Analytics, Application Integration, and Compute, along with categories such as All services, Favorites, and Recently visited. The main content area lists several AWS services: Cloud9, CloudShell, CodeArtifact, CodeBuild, CodeCommit, CodeDeploy, CodePipeline, CodeStar, and AWS FIS. Each service has a brief description below its name.

Figure 5.8 – AWS Developer Tools

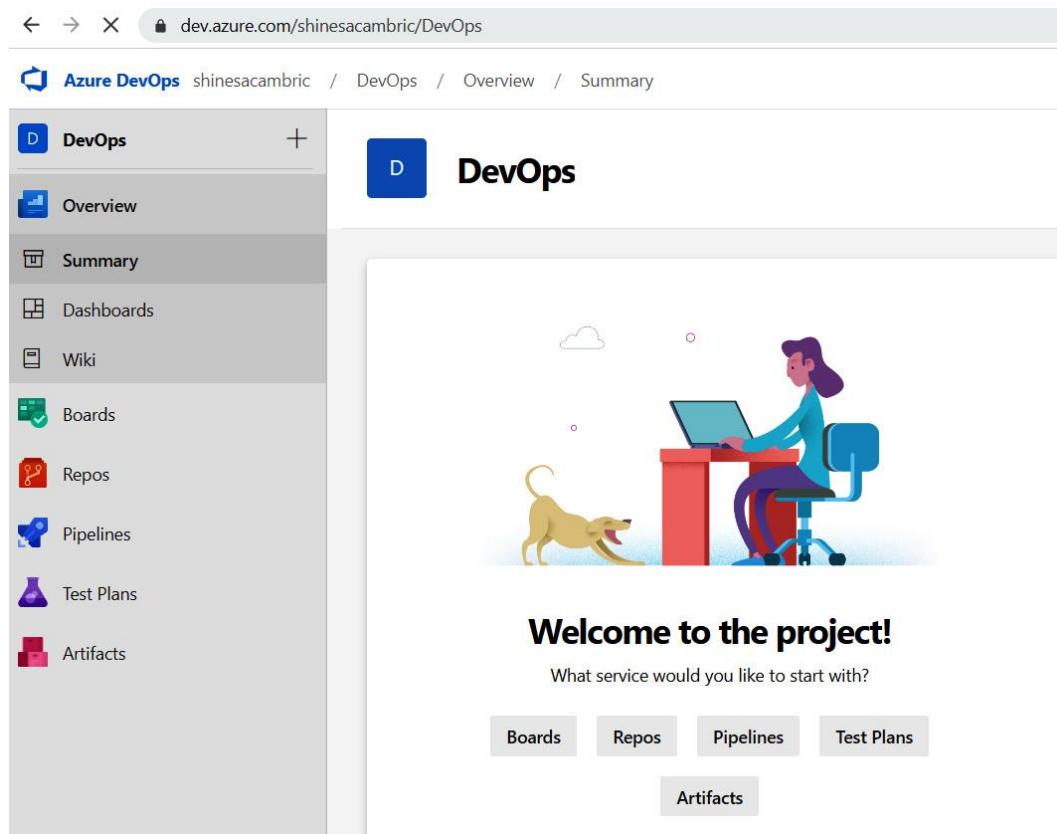


Figure 5.9 – Microsoft Azure DevOps

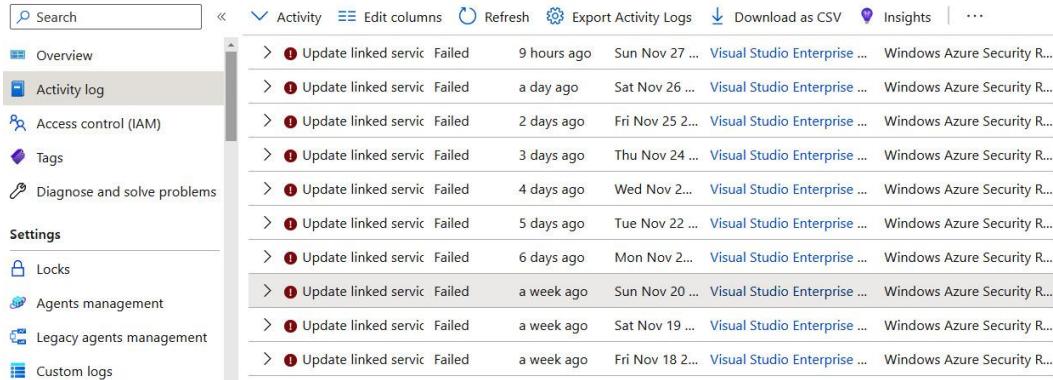
CI/CD	Name	Description	Actions
Integrate and deliver continuously	Cloud Build	Continuous integration delivery platform	
	Container Registry	Private container registry storage	
	Source Repositories	Hosted private git repos	
	Artifact Registry	Universal build artifact management	
	Cloud Deploy	Managed continuous delivery to GKE	

Figure 5.10 – Google Cloud Platform CI/CD features

Monitoring

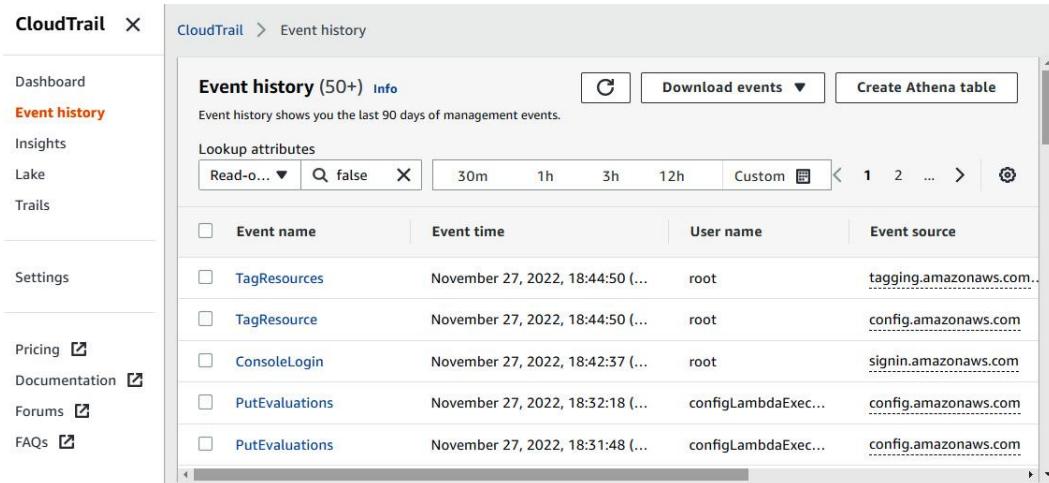
-  Sign-in logs
-  Audit logs
-  Provisioning logs
-  Log Analytics
-  Diagnostic settings
-  Workbooks
-  Usage & insights

Figure 5.11 – Azure Monitoring



Activity							Export Activity Logs	Download as CSV	Insights	...
>	1	Update linked service	Failed	9 hours ago	Sun Nov 27 ...	Visual Studio Enterprise ...	Windows Azure Security R...			
>	1	Update linked service	Failed	a day ago	Sat Nov 26 ...	Visual Studio Enterprise ...	Windows Azure Security R...			
>	1	Update linked service	Failed	2 days ago	Fri Nov 25 ...	Visual Studio Enterprise ...	Windows Azure Security R...			
>	1	Update linked service	Failed	3 days ago	Thu Nov 24 ...	Visual Studio Enterprise ...	Windows Azure Security R...			
>	1	Update linked service	Failed	4 days ago	Wed Nov 23 ...	Visual Studio Enterprise ...	Windows Azure Security R...			
>	1	Update linked service	Failed	5 days ago	Tue Nov 22 ...	Visual Studio Enterprise ...	Windows Azure Security R...			
>	1	Update linked service	Failed	6 days ago	Mon Nov 21 ...	Visual Studio Enterprise ...	Windows Azure Security R...			
>	1	Update linked service	Failed	a week ago	Sun Nov 20 ...	Visual Studio Enterprise ...	Windows Azure Security R...			
>	1	Update linked service	Failed	a week ago	Sat Nov 19 ...	Visual Studio Enterprise ...	Windows Azure Security R...			
>	1	Update linked service	Failed	a week ago	Fri Nov 18 2 ...	Visual Studio Enterprise ...	Windows Azure Security R...			

Figure 5.12 – Microsoft Azure Activity log for a resource



Event history (50+)				Info	Download events	Create Athena table
Event history shows you the last 90 days of management events.						
Lookup attributes						
<input type="button" value="Read-only"/>	<input type="button" value="Q false"/>	X	30m	1h	3h	12h
<input type="checkbox"/>	Event name	Event time	User name	Event source		
<input type="checkbox"/>	TagResources	November 27, 2022, 18:44:50 (...)	root	tagging.amazonaws.com...		
<input type="checkbox"/>	TagResource	November 27, 2022, 18:44:50 (...)	root	config.amazonaws.com		
<input type="checkbox"/>	ConsoleLogin	November 27, 2022, 18:42:37 (...)	root	signin.amazonaws.com		
<input type="checkbox"/>	PutEvaluations	November 27, 2022, 18:32:18 (...)	configLambdaExec...	config.amazonaws.com		
<input type="checkbox"/>	PutEvaluations	November 27, 2022, 18:31:48 (...)	configLambdaExec...	config.amazonaws.com		

Figure 5.13 – AWS CloudTrail

The screenshot shows the Google Cloud Audit Logs configuration page. On the left, a sidebar lists various IAM & Admin options, with 'Audit Logs' selected. The main area displays a table titled 'Data Access audit logs configuration' with columns for Service, Admin Read, Data Read, Data Write, and Exempted principals. A filter bar at the top allows searching by property name or value. To the right, there's a panel titled 'Access Approval' with sections for 'LOG TYPES' (Admin Read, Data Read, Data Write) and 'EXEMPTED PRINCIPALS'. A 'SAVE' button is located at the bottom right of this panel.

Service	Admin Read	Data Read	Data Write	Exempted principals
Access Approval	—	—	—	0
AI Platform Notebooks	—	—	—	0
AlloyDB API	—	—	—	0
Anthos Multi-cloud API	—	—	—	0
Apigee	—	—	—	0
Apigee Connect API	—	—	—	0
Apigee Integration API	—	—	—	0
Apigee Registry API	—	—	—	0
Artifact Registry API	—	—	—	0
Bare Metal Solution API	—	—	—	0
BeyondCorp Enterprise API	—	—	—	0
BigQuery Analytics Hub API	—	—	—	0
BigQuery Data Policy API	—	—	—	0
BigQuery Migration API	—	—	—	0

Figure 5.14 – Google Cloud audit log configuration

The screenshot shows the Google Cloud Logs Storage configuration page. On the left, a sidebar lists 'Operations Logging' options, with 'Logs Storage' selected. The main area displays a table titled 'Log buckets' with columns for Name, Description, Previous month usage, Month-to-date usage (MTD), Retention period, Region, Status, Created, and Last updated. A filter bar at the top allows filtering by Name. The table shows two entries: '_Default' (Default bucket, 0 B, 0 B, 30 days, global, Unlocked) and '_Required' (Audit bucket, Not billed, Not billed, 400 days, global, Locked).

Name	Description	Previous month usage	Month-to-date usage (MTD)	Retention period	Region	Status	Created	Last updated
_Default	Default bucket	0 B	0 B	30 days	global	Unlocked		
_Required	Audit bucket	Not billed	Not billed	400 days	global	Locked		

Figure 5.15 – Google Cloud audit log storage configuration

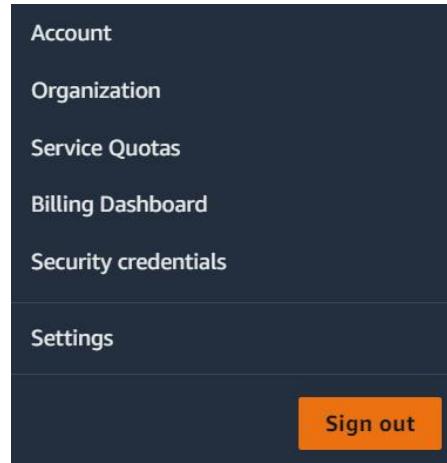


Figure 5.16 – AWS navigation to Service Quotas and Billing Dashboard

A screenshot of the AWS Billing Dashboard. On the left is a sidebar with navigation links: Home (highlighted), Billing, Bills, Payments, Credits, Purchase orders, Cost & Usage Reports, Cost Categories, Cost allocation tags, Free Tier, Billing Conductor (with a gear icon), Cost Management, Cost Explorer, Budgets, Budgets Reports, Savings Plans (with a gear icon), Preferences, Billing preferences, Payment methods, and Consolidated billing. The main area shows the "AWS Billing Dashboard" with a page refresh time of Saturday, August 6, 2022 at 10:02:21 PM CDT. It includes sections for "AWS summary" and "Highest cost".

Current month's total forecast	Current MTD balance	Prior month for the same period with trend
USD 0.72	USD 0.22	No data to display ↓ 0.0%

Total number of active services	Total number of active AWS accounts	Total number of active AWS Regions
1	1	1

Highest cost		Highest service spend	
Viewing highest service spend.		Highest service spend ▾	
Service name	Trend compared to prior month	Current MTD balance	Prior month for the same period
Security Hub	↓ 0.0%	USD 0.22	No data to display

View your bill

Figure 5.17 – AWS Billing Dashboard

Figure 5.18 – Azure navigation to Cost Management + Billing

Subscription name	Subscription ID	Status	Last billed amount	Due date	Current
Visual Studio Enterprise ...	fdba6ba7-e814-4949-a6b1-f077ad16e1c3	Active	Not available	Not available	\$1.27

Figure 5.19 – Azure Cost Management + Billing

... > Cost Management + Billing | Cost Management > Cost Management: Tenant Root Group | Budgets >

Create budget

Budget

May 2022 - Apr 2023

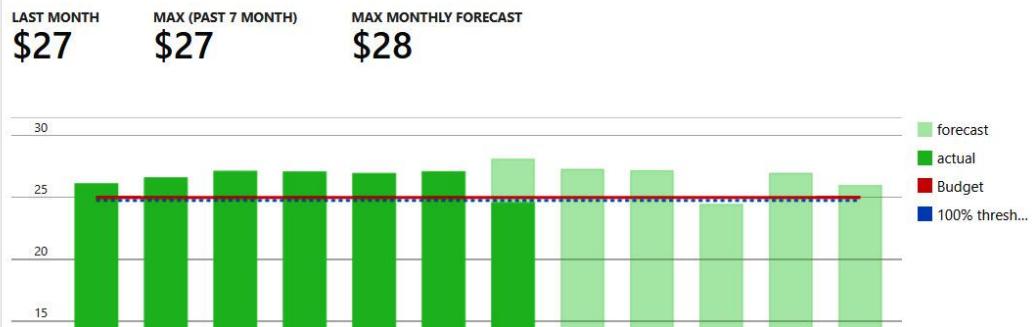


Figure 5.20 – Azure – Create budget

Google Cloud

Cloud overview >

Recent >

View all products

PINNED

Billing

MORE PRODUCTS ▾

Marketplace

Billing

APIs & Services >

Support >

IAM & Admin >

Getting started

account ID	Status	Last 30 days' spend	Account type	Organization	Health checks

Figure 5.21 – Google Cloud Billing

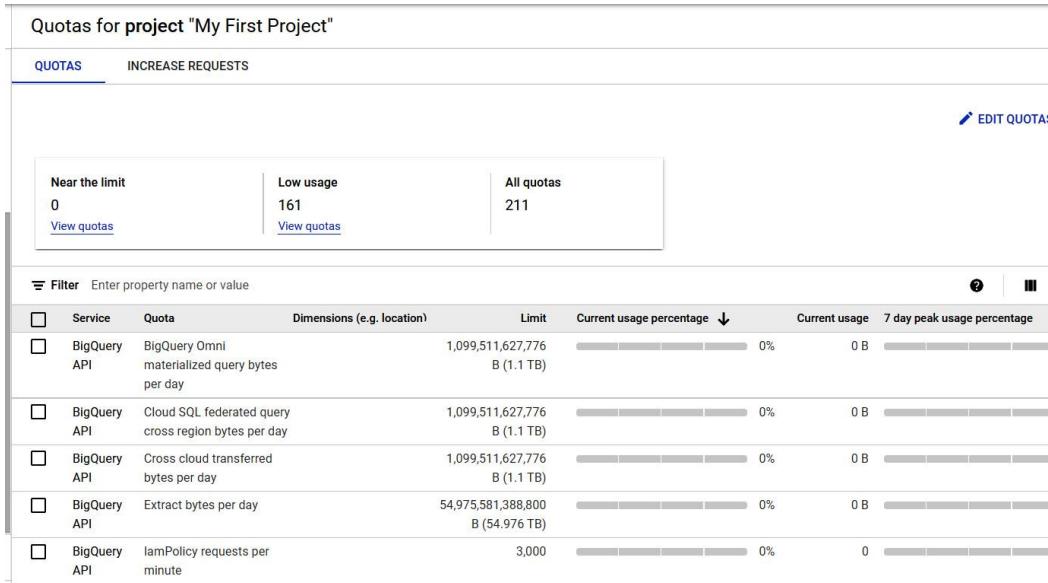


Figure 5.22 – Google Cloud quota increase

Links

- To find a comprehensive list of CIS benchmark controls, go to <https://www.cisecurity.org/benchmark>.
- You can find out more about the CCM matrix from CSA at <https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/>.
- To learn more about the Blueprint or Landing Zone features of the three major cloud providers, visit the following links:
- AWS: <https://docs.aws.amazon.com/controltower/latest/userguide/what-is-control-tower.html>
- Azure: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/>
- Google Cloud Platform (GCP): <https://cloud.google.com/anthos-config-management/docs/concepts/blueprints>
- Additional details about the use of tags and policies within Microsoft Azure can be found at <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>.

- To learn more about this, you can check out https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_attribute-based-access-control.html.
- Cloud Custodian: <https://aws.amazon.com/blogsopensource/compliance-as-code-and-auto-remediation-with-cloud-custodian/>.
- Gatekeeper: <https://github.com/open-policy-agent/gatekeeper>.
- Terraform by HashiCorp: <https://developer.hashicorp.com/terraform/intro> and <https://terraform-compliance.com/>.
- To find out more about VPC Flow Logs, go to <https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html>.
- More information on audit log options for each of the three providers can be found at the following links:
 - AWS: <https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/monitoring-and-logging.html>
 - Microsoft Azure: <https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/>
 - GCP: <https://cloud.google.com/logging/docs/audit>

Chapter 6

Figures

The screenshot shows the AWS Tag Editor interface. On the left, a sidebar menu includes 'Resources' (Create Resource Group, Saved Resource Groups), 'Tagging' (Tag Editor, Tag Policies), and 'What's new'. The main area is titled 'Tag Editor' and contains a 'Find resources to tag' section. It features a 'Regions' dropdown set to 'us-east-1', a 'Resource types' dropdown set to 'All supported resource types', and two input fields for 'Tag key' and 'Optional tag value'. A note at the bottom says 'Type the tag key and optional values shared by the resources you want to search for, and then choose Add or press Enter.'

Figure 6.1 – Finding resources to tag

The screenshot shows the 'Resource search results (58)' page. The sidebar is identical to Figure 6.1. The main table lists 58 resources, each with a checkbox, Identifier, Tag: Name, Service, Type, Region, and Tags. The first resource listed is 'cfst-1449-95e9a645e...', which is associated with CloudFormation, Stack, us-east-1, and has a blue circled '1' icon next to it. Other resources include EC2 instances, InternetGateways, NetworkAcls, RouteTables, SecurityGroups, and Subnets.

Identifier	Tag: Name	Service	Type	Region	Tags
cfst-1449-95e9a645e...	(not tagged)	CloudFormation	Stack	us-east-1	1
dopt-070b3b1e8a7fd8...	(not tagged)	EC2	DHCOOptions	us-east-1	-
igw-0ca6a5aa08a0235...	(not tagged)	EC2	InternetGat...	us-east-1	-
acl-0ca829f8f575d3241	(not tagged)	EC2	NetworkAcl	us-east-1	-
rtb-0ff45f7a27b53a8a7	(not tagged)	EC2	RouteTable	us-east-1	-
sg-0c33a3528946f4956	(not tagged)	EC2	SecurityGroup	us-east-1	-
subnet-0bb9728624a...	(not tagged)	EC2	Subnet	us-east-1	-
subnet-0611110ba46...	(not tagged)	EC2	Subnet	us-east-1	-

Figure 6.2 – Resource search results

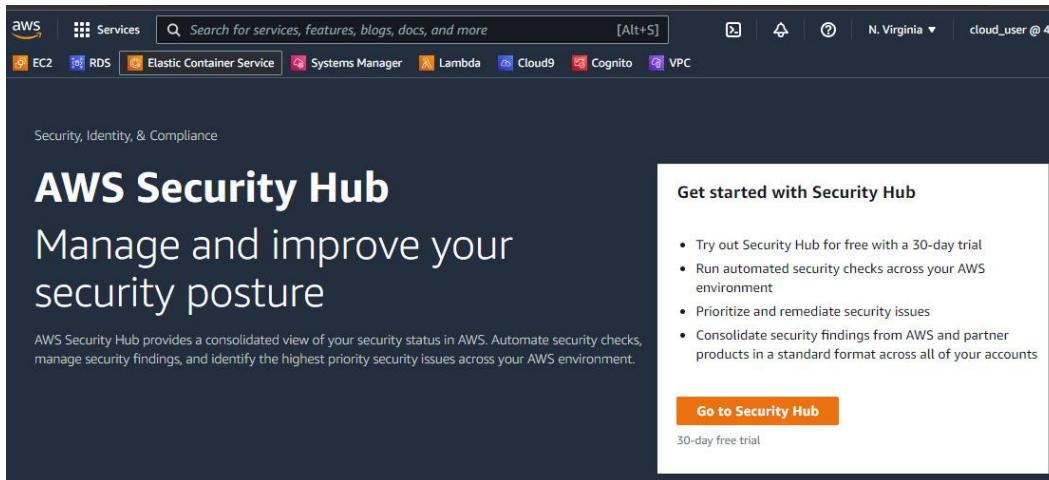


Figure 6.3 – AWS Security Hub

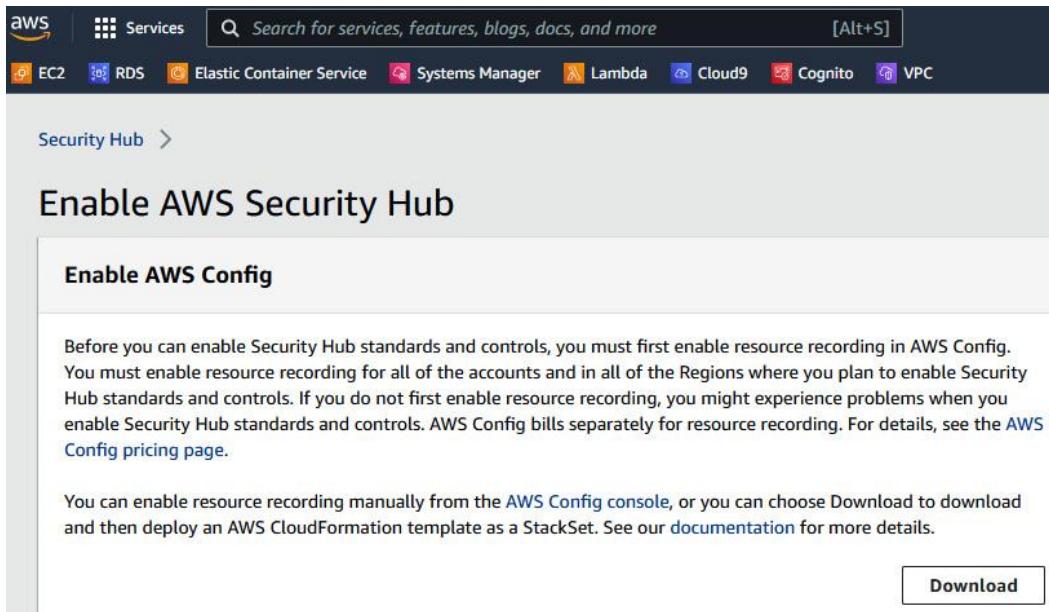


Figure 6.4 – Enabling AWS Config

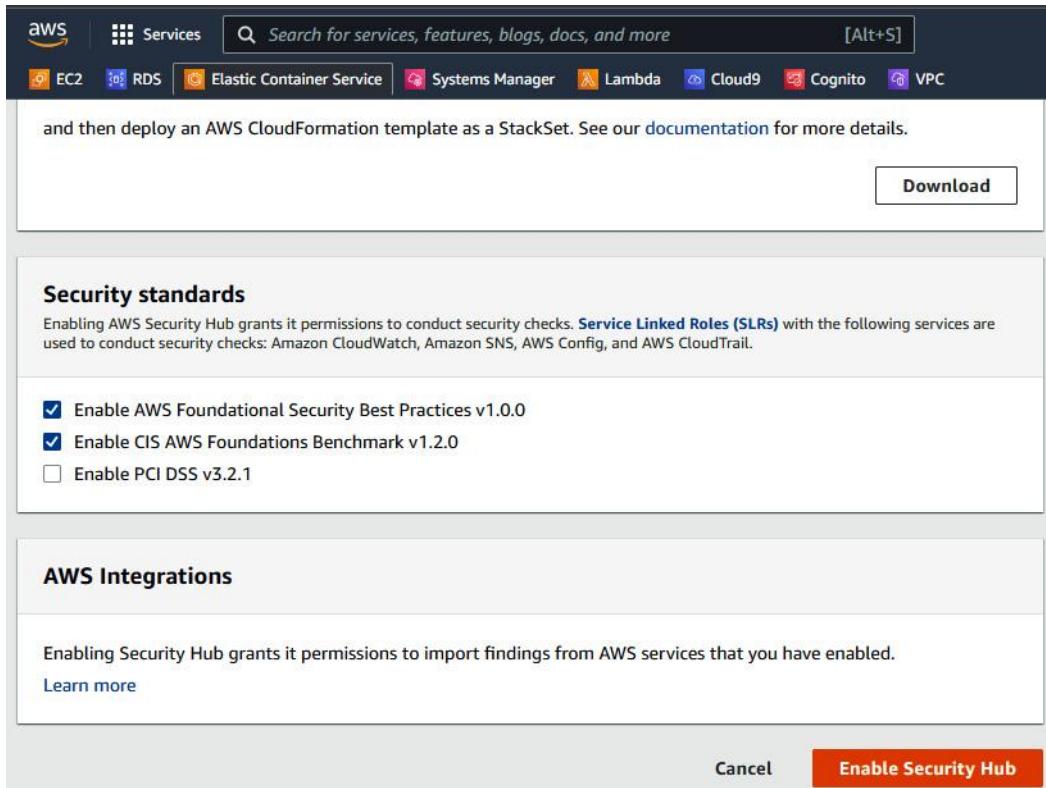


Figure 6.5 – Security standards

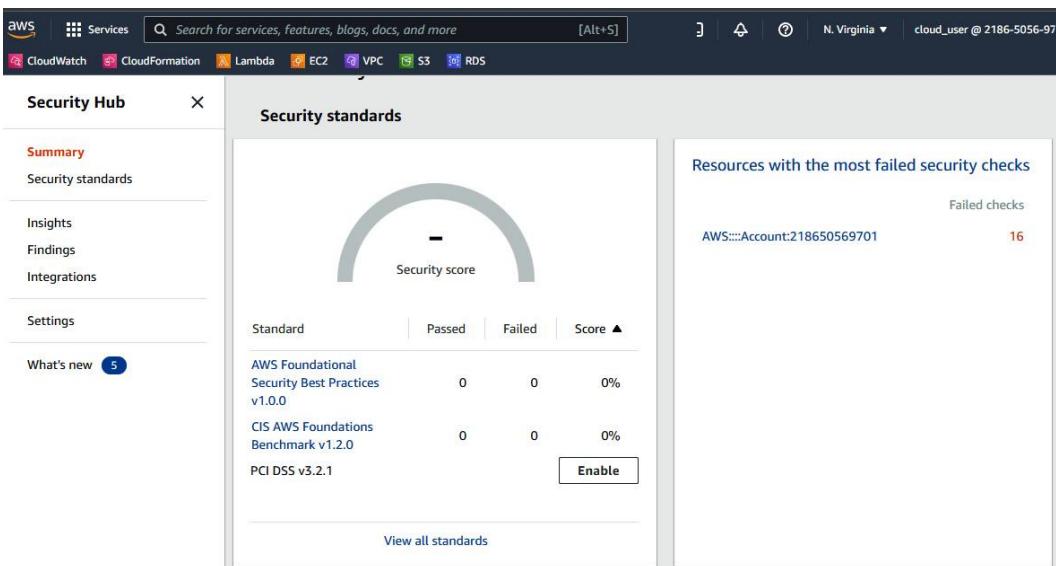


Figure 6.6 – The Summary tab

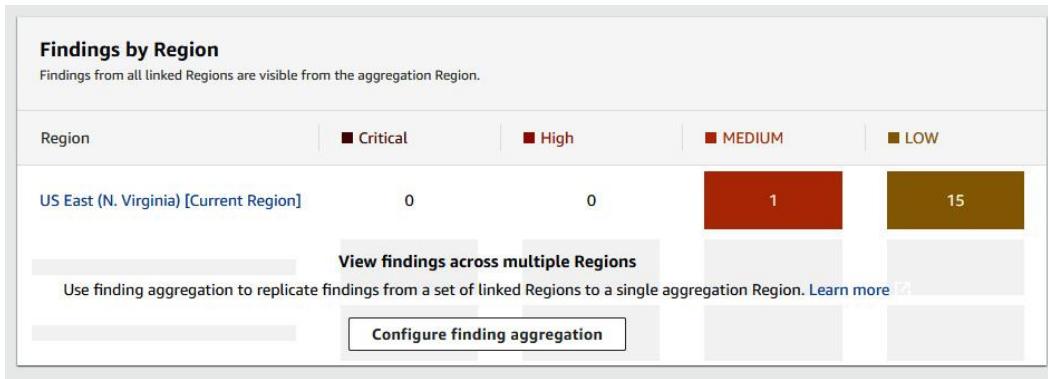


Figure 6.7 – Findings by region

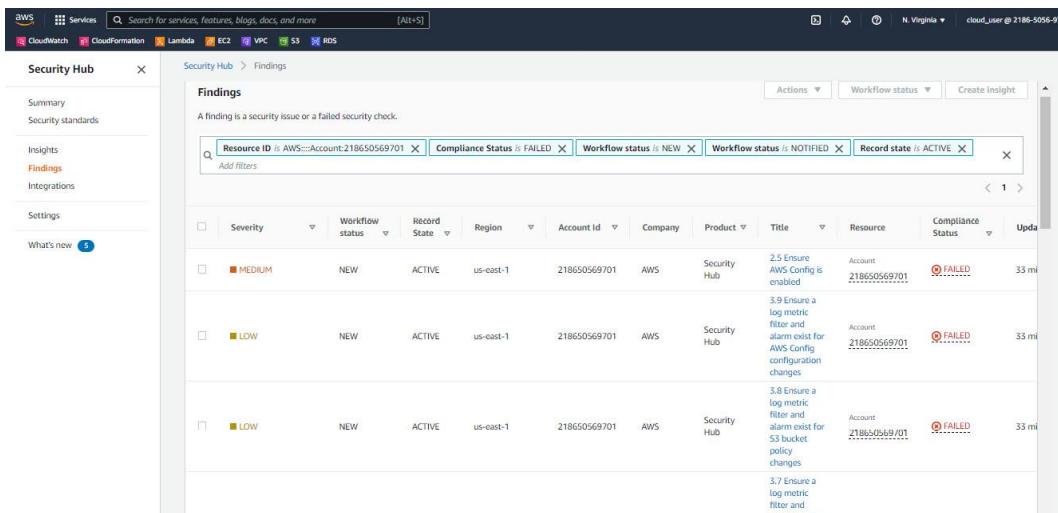


Figure 6.8 – Findings

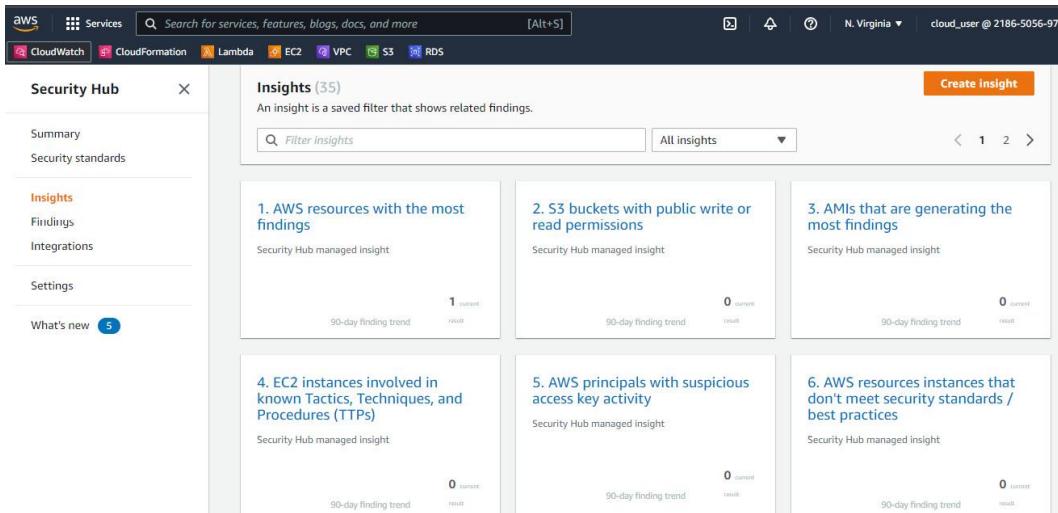


Figure 6.9 – The Insights tab

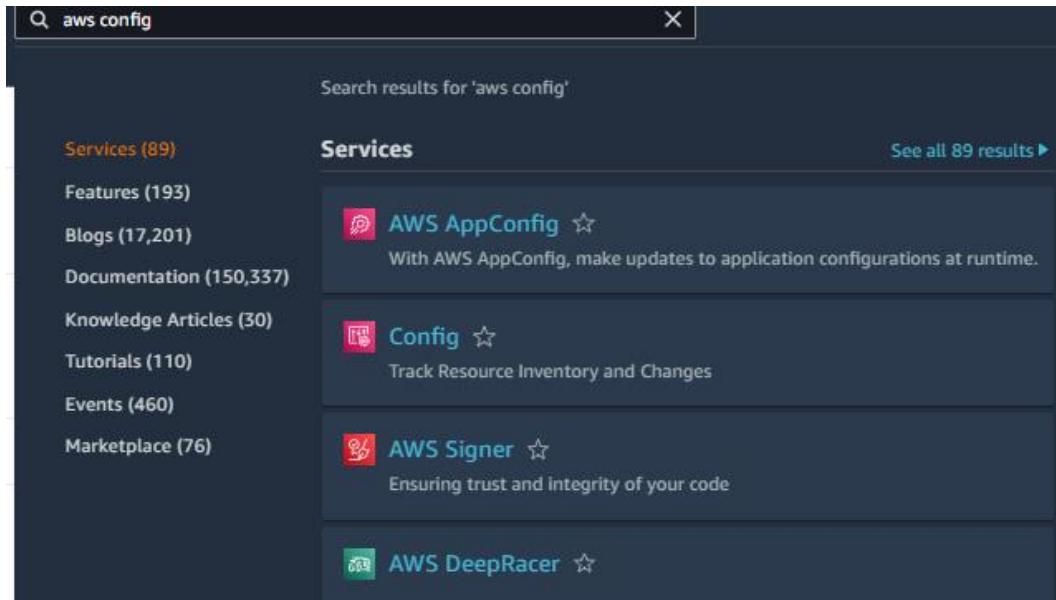


Figure 6.10 – AWS Config search

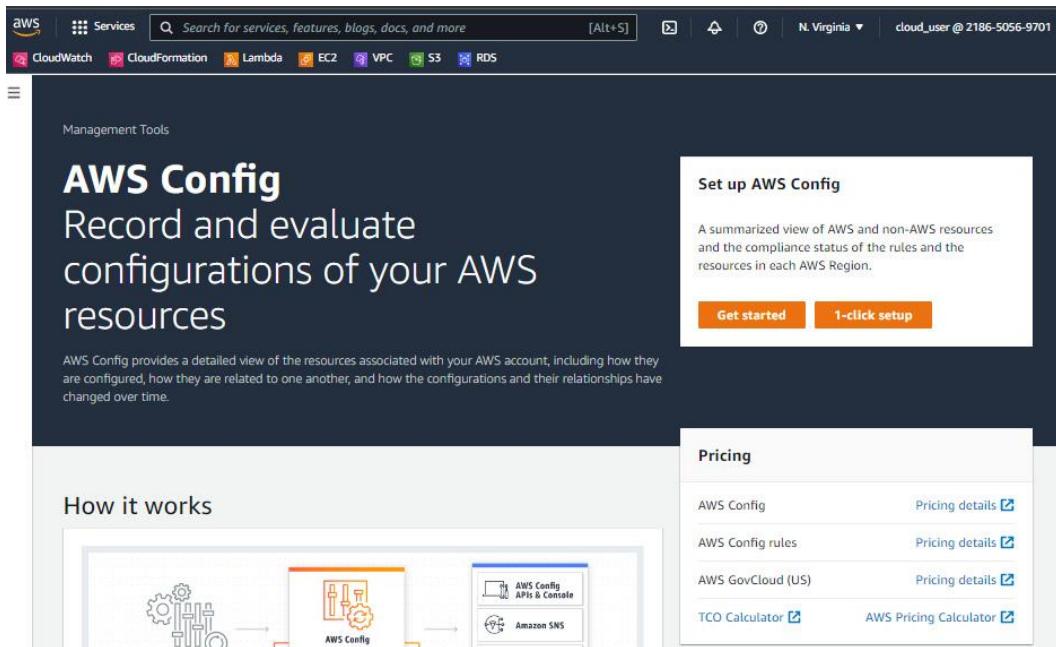


Figure 6.11 - Enabling AWS Config

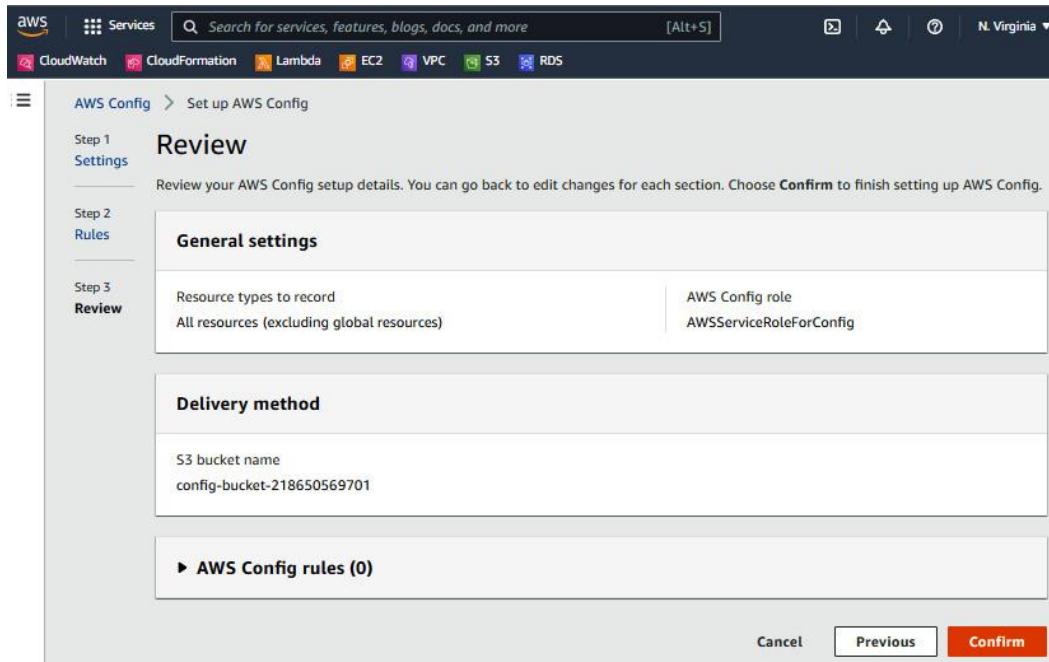


Figure 6.12 – Setting up AWS Config

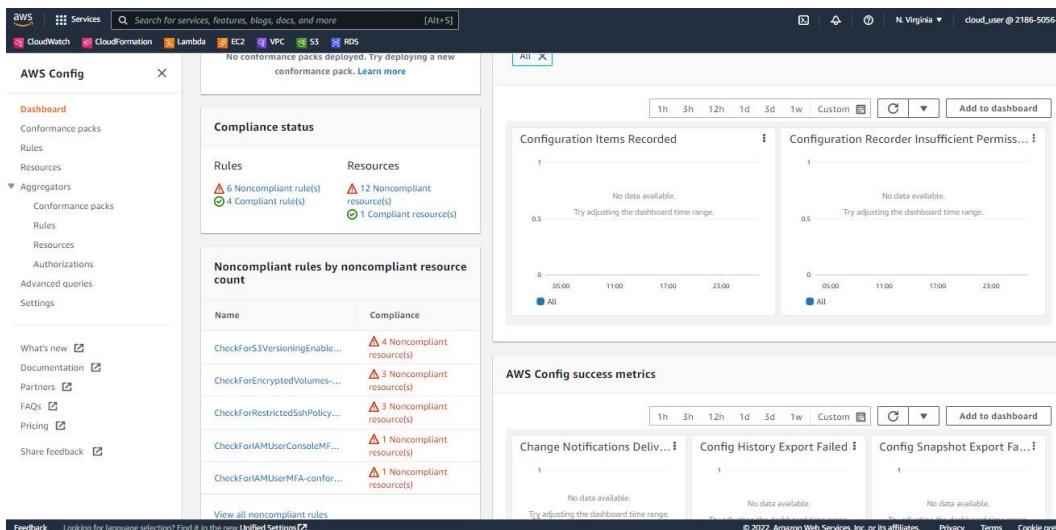


Figure 6.13 – The Dashboard tab

The screenshot shows the AWS Config Rules page. The left sidebar has 'Rules' selected under 'Resources'. The main content area is titled 'Rules' and contains a table of non-compliant rules. The table columns are Name, Remediation action, Type, and Compliance. Each row shows a rule name starting with 'CheckFor...', its status as 'Not set', it being an 'AWS managed' type, and a red warning icon indicating '1 Noncompliant resource(s)'.

Name	Remediation action	Type	Compliance
CheckForEncryptedVolumes-conformance-pack-uconsord	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
CheckForRestrictedSSHPolicy-conformance-pack-uconsord	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
CheckForIAMUserConsoleMFA-conformance-pack-uconsord	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
CheckForIAMUserMFA-conformance-pack-uconsord	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
CheckForRootMfa-conformance-pack-uconsord	Not set	AWS managed	⚠ 1 Noncompliant resource(s)
CheckForS3VersioningEnabled-conformance-pack-uconsord	Not set	AWS managed	⚠ 2 Noncompliant resource(s)

Figure 6.14 – The Rules tab

The screenshot shows the AWS Config Resources page. The left sidebar has 'Resources' selected under 'Resources'. The main content area is titled 'Resources' and contains a table of non-compliant resources. The table columns are Resource identifier, Type, and Compliance. The resources listed include various AWS services like IAM User, EC2 Volume, EC2 SecurityGroup, S3 Bucket, and CloudTrail logs, all marked as 'Noncompliant'.

Resource identifier	Type	Compliance
cloud_user	IAM User	⚠ Noncompliant
vol-006d50ce2a61c2314	EC2 Volume	⚠ Noncompliant
vol-0843af40f66b8a574	EC2 Volume	⚠ Noncompliant
vol-0b0be451c05048575	EC2 Volume	⚠ Noncompliant
sg-011f34d1d15905738	EC2 SecurityGroup	⚠ Noncompliant
sg-068e32d8848463c2c	EC2 SecurityGroup	⚠ Noncompliant
sg-0e02deeffb5003ff2	EC2 SecurityGroup	⚠ Noncompliant
aws-athena-query-results-218650569701-us-east-1	S3 Bucket	⚠ Noncompliant
aws-cloudtrail-logs-218650569701-501b03ed	S3 Bucket	⚠ Noncompliant
config-bucket-218650569701	S3 Bucket	⚠ Noncompliant

Figure 6.15 – The Resources tab

Q Trusted X

Search results for 'Trusted'

Services (3)

Features (3)

Blogs (270)

Documentation (14,484)

Knowledge Articles (30)

Tutorials (1)

Events (9)

Marketplace (1,620)

Services

 Trusted Advisor ☆
Optimize Performance and Security

 Elastic Kubernetes Service ☆
The most trusted way to start, run, and scale Kubernetes

 AWS Signer ☆
Ensuring trust and integrity of your code

Features

Trusted access for AWS services
 AWS Organizations feature

Roles
 IAM feature

Blogs See all 270 results ►

AWS Trusted Advisor – New Priority Capability ↗

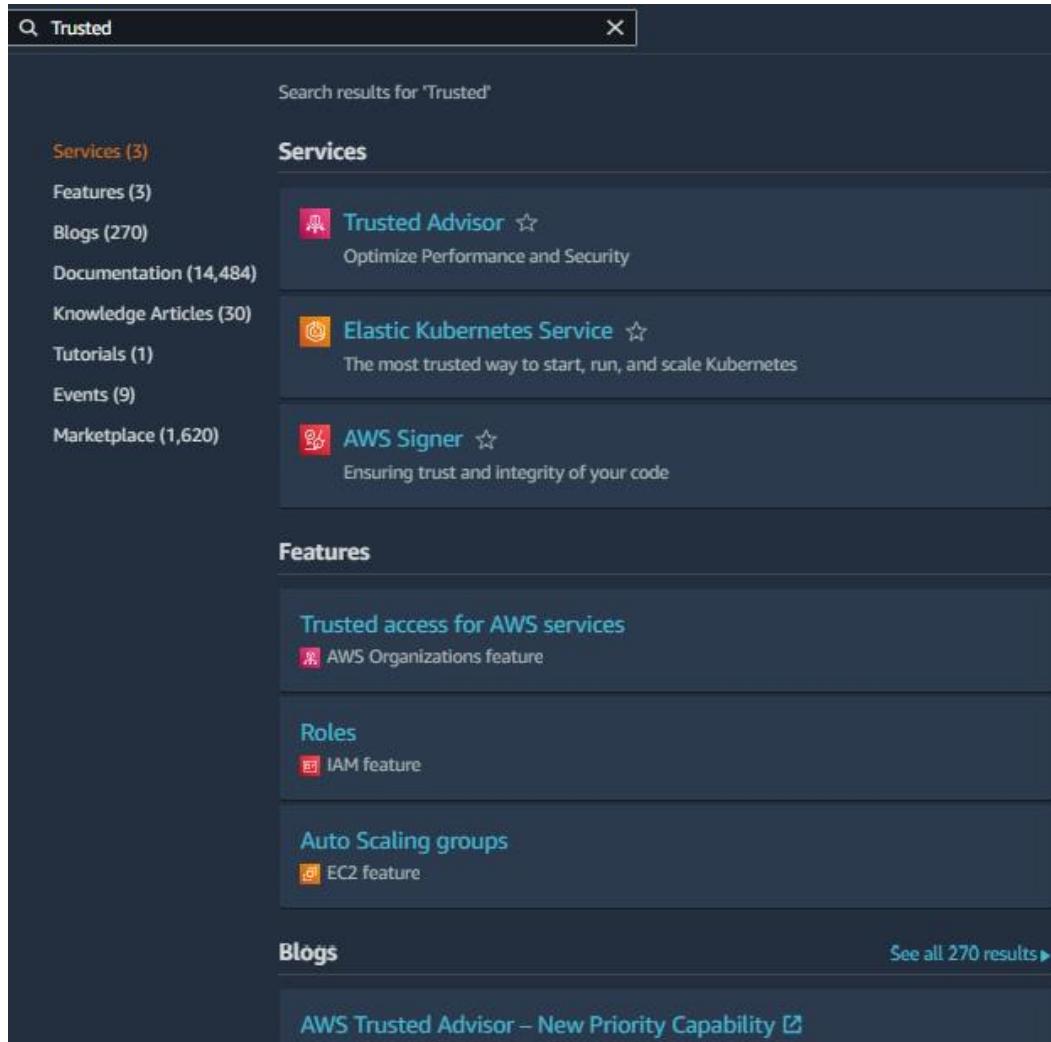


Figure 6.16 – Searching for AWS Trusted Advisor



Figure 6.17 – The AWS Trusted Advisor interface

The screenshot shows the Microsoft Defender for Cloud Overview tab. At the top, there's a search bar and a navigation bar with links for Subscriptions, What's new, and other account-related options. The main area has a header "Microsoft Defender for Cloud | Overview" and a sub-header "Showing subscription 'P2-Real Hands-On Labs'". On the left, a sidebar lists General, Recommendations, Security alerts, Inventory, Workbooks, Community, and Diagnose and solve problems sections. Under Cloud Security, it shows Security posture, Regulatory compliance, and Workload protections. The main content area features a "Security posture" section with a "Secure score" gauge at 0% (labeled "Azure" and "AWS"). It also displays "OMI vulnerabilities published" (0/0) and "Active recommendations" (0). A note about an OMI elevation of privilege vulnerability (CVE-2022-29149) is present, along with a link to auto-update support. There's also a "Read guidance >" link and a "Upgrade to New Containers plan" button.

Figure 6.18 – The Overview tab

The screenshot shows the Microsoft Defender for Cloud Inventory tab. The top navigation bar includes a search bar and various filter and action buttons like Refresh, Add non-Azure servers, Open query, Assign tags, Download CSV report, Trigger logic app, Learn more, and Guides & Feedback. The left sidebar follows the same structure as Figure 6.18, with the "Inventory" section selected. The main content area displays four categories: Total resources (5), Unhealthy resources (1), Unmonitored resources (0), and Unregistered subscriptions (0). Below these are detailed tables for each category. For "Unhealthy resources", the table shows one entry: "packttest" (Virtual machines, P2-Real Hands-On Labs). For "Unregistered subscriptions", the table shows two entries: "1-9e05760f-playground-sandbox-vnet" and "default" (both Subnets, P2-Real Hands-On Labs). At the bottom, there are navigation buttons for Previous, Page 1 of 1, and Next.

Figure 6.19 – The Inventory tab

The screenshot shows the Microsoft Defender for Cloud interface with the 'Recommendations' tab selected. On the left, a navigation menu includes 'General', 'Cloud Security', and 'Management' sections. The main area displays a summary of recommendations: 1/6 High, 1/4 High, 0/4 High. Below this is a table titled 'All recommendations' with columns for Severity, Name, Status, Initiatives, Unhealthy resources, and Insights. The table lists five recommendations, all marked as 'Completed'. At the bottom right is a 'Give us feedback' button.

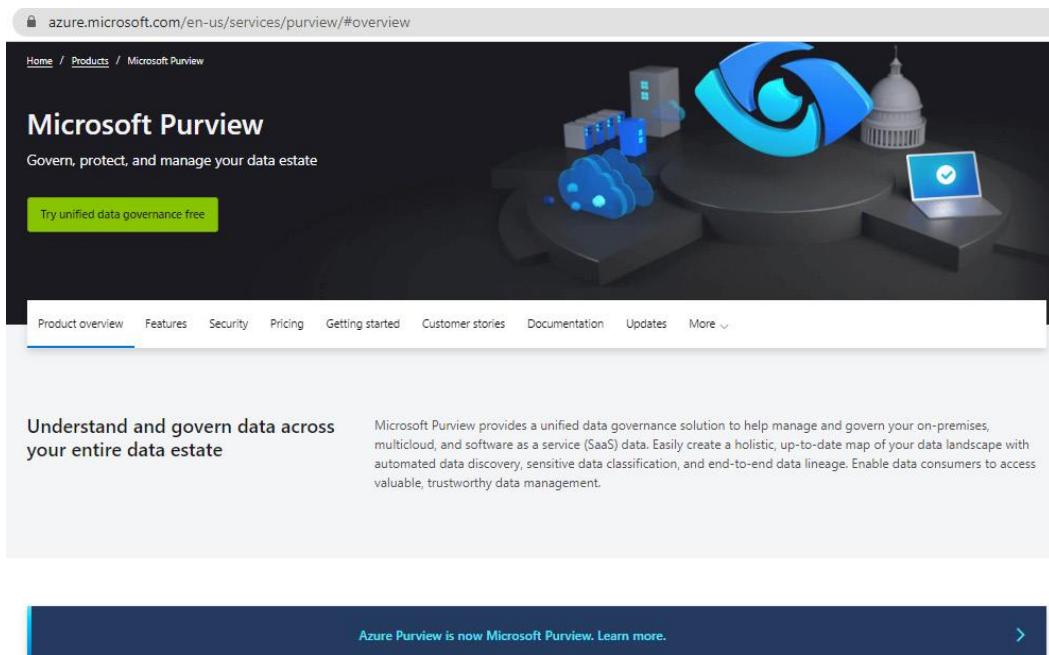
Figure 6.20 – The Recommendations tab

The screenshot shows the Microsoft Defender for Cloud interface with the 'Security posture' tab selected. The left navigation menu includes 'Cloud Security' and 'Management' sections. The main area displays an 'Azure environment' summary with a 'Secure score' of 'N/A'. It shows 2 Management groups, 1 Subscriptions, and 3 Recommendations. Below this is a table titled 'Environment' with columns for Name, Secure score, Unhealthy resources, and Recommendations. The table lists one environment named 'Azure'.

Figure 6.21 – The Security posture tab

The screenshot shows the Microsoft Defender for Cloud interface with the 'Regulatory compliance' tab selected. The left navigation menu includes 'Cloud Security' and 'Management' sections. A message at the top states: 'You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.' Below this is a section titled 'Insufficient permissions' with a note: 'You do not have permissions on the currently selected subscriptions. Please select different subscriptions or contact your subscription owner to receive permissions.' To the right is a 'Audit reports' section with a 'Open' button.

Figure 6.22 – Regulatory compliance



Azure Purview is now Microsoft Purview. Learn more. >

Figure 6.23 – Azure Purview

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Create Microsoft Purview account

Provide Microsoft Purview account info

Project details

Subscription * P2-Real Hands-On Labs

Resource group * 1-9e05760f-playground-sandbox

Create new

Instance details

Microsoft Purview account name * PacktTestAccount

Location * South Central US

Managed resources

Managed resource group name * managed-rg-PacktTestAccount

Storage account name Name will be auto-generated during account creation.

Review + Create **Previous** **Next: Networking >**

Figure 6.24 – Creating the Microsoft Purview account

Microsoft Purview

cloud_user_p_660b1
LINUX ACADEMY PRODUC

Select a Microsoft Purview account

Microsoft Purview is a unified data governance service that enables a foundational understanding of your on-premises, multi-cloud, operational and SaaS data. [Learn more](#)

Azure Active Directory

Account name

PacktTestAccount

Continue

Figure 6.25 – Selecting an account

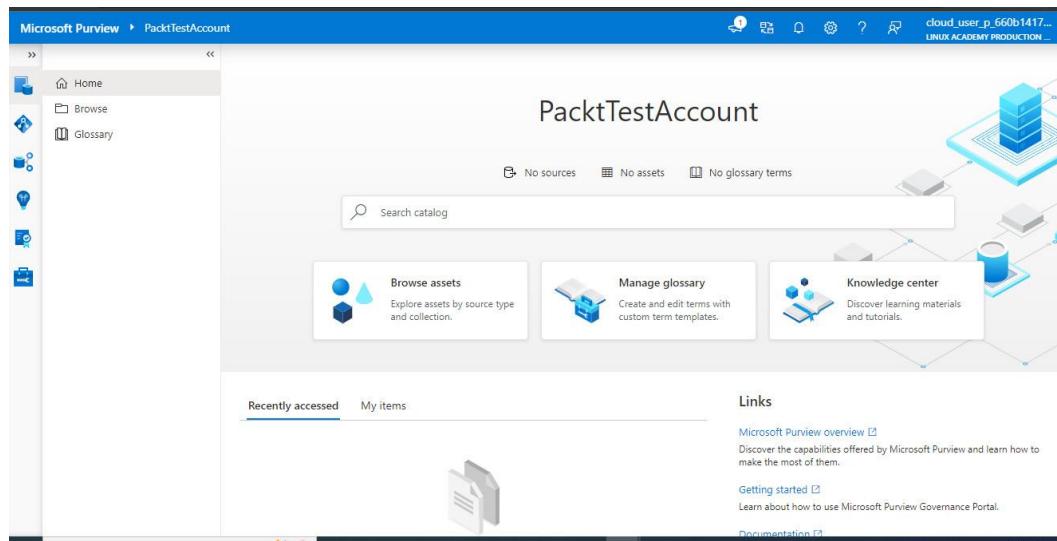


Figure 6.26 – Microsoft Purview Home page

The screenshot shows the "Browse assets" page. The title is "Browse assets". It features a "Refresh" button and filters for "By collection" and "By source type". A "Filter by keyword" input field is available. The main content area shows "Showing 1 collection" with a table:

Name	Description	Assets	Collection admin
PacktTestAccount	The root collection.	-	Cloud Student

Figure 6.27 – Browse assets

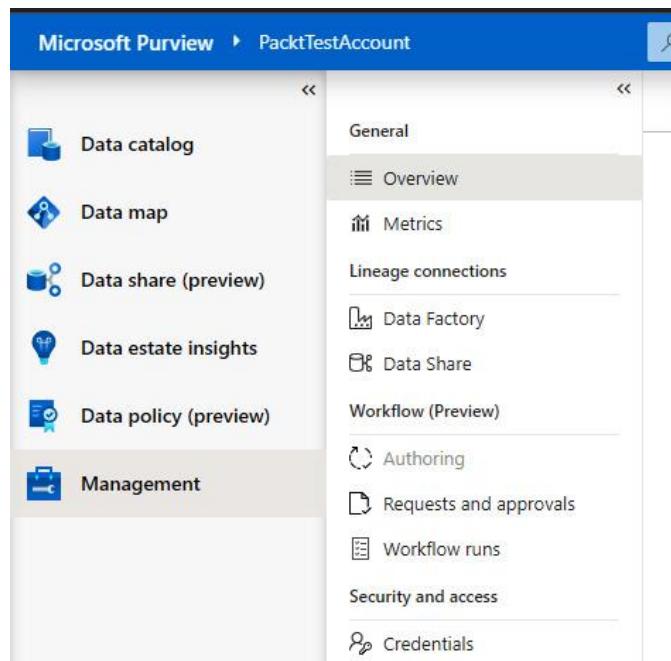


Figure 6.28 – Management | Overview

A screenshot of the Google Cloud Security Command Center landing page. The URL in the browser bar is 'cloud.google.com/security-command-center'. The page features a navigation bar with links for Overview, Solutions, Products, Pricing, Resources, Docs, and Support. Below the navigation is a search bar. The main content area has a title 'Security Command Center' and a subtitle 'Security and risk management platform for Google Cloud.' A 'Go to console' button is prominently displayed. To the left, there is a sidebar with sections for 'Security Command Center', 'Benefits', 'Key features', 'Customers', 'What's new', 'Documentation', 'All features', and 'Pricing'. The 'Benefits' section is currently selected, indicated by a blue vertical bar on the left.

Figure 6.29 – Security Command Center

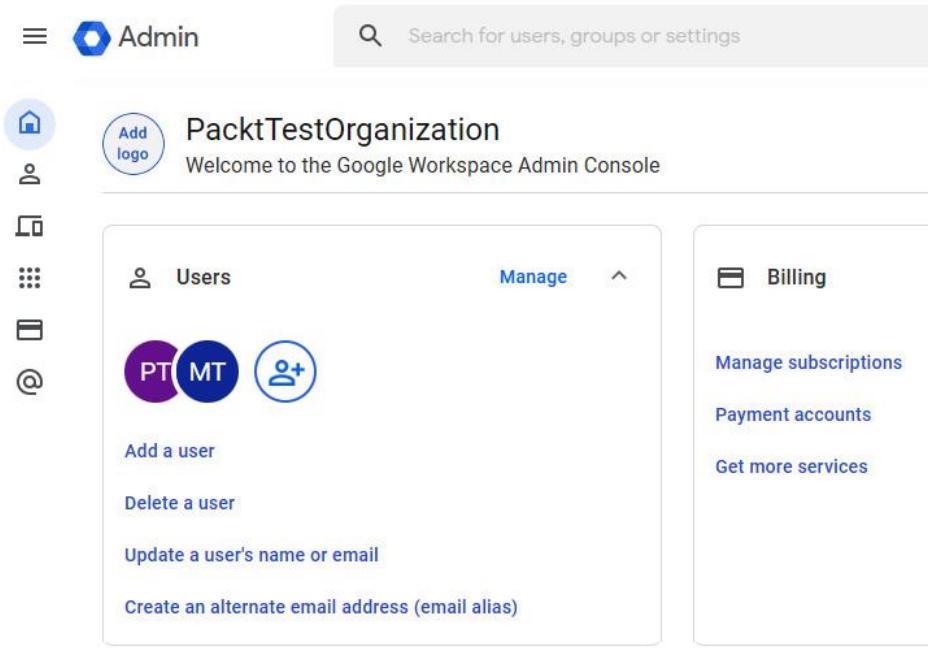


Figure 6.30 – The Admin console

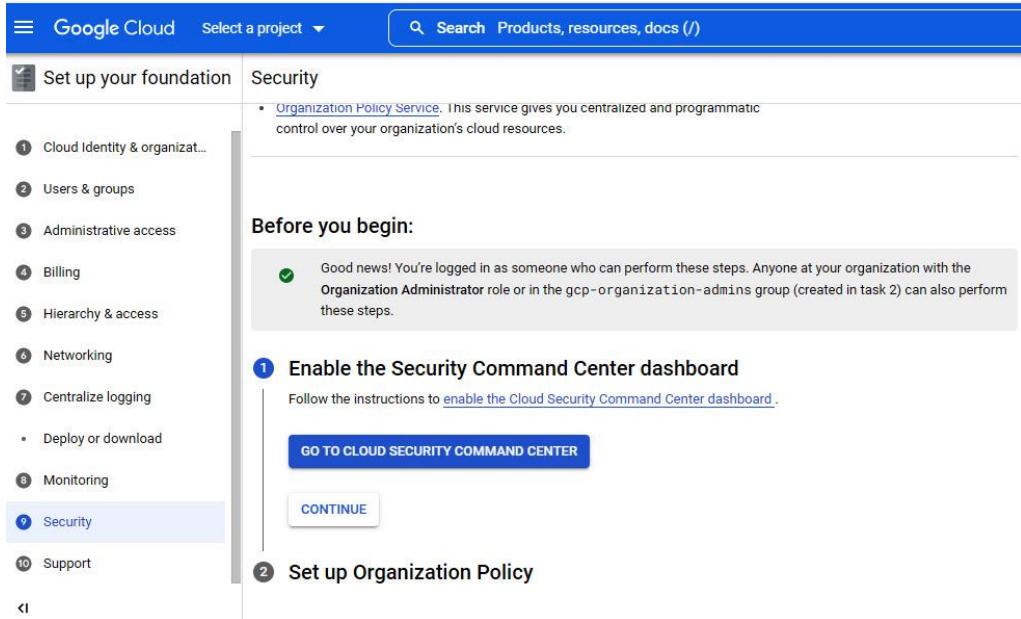


Figure 6.31 – The Security tab

The screenshot shows the Google Cloud Security Command Center Services setup interface. On the left, a sidebar lists various services: reCAPTCHA Enterprise, BeyondCorp Enterprise, Policy Troubleshooter for ..., Identity-Aware Proxy, Access Context Manager, VPC Service Controls, Binary Authorization, Data Loss Prevention, Key Management, and Certificate Authority Serv... . The 'Security Command Center' service is selected and highlighted in blue. The main content area is titled 'Services' and contains sections for 'Security Health Analytics' (with a dropdown menu showing 'Enabled'), 'Web Security Scanner' (marked as 'Premium' and noting it's not available for Standard Security Command Center), and 'Event Threat Detection' (also marked as 'Premium' and noting it's not available for Standard Security Command Center). A search bar at the top right says 'Search products, resources, docs ()'.

Figure 6.32 – Services setup

The screenshot shows the Google Cloud Security Command Center Overview page. The sidebar on the left includes the same list of services as Figure 6.32, with 'Security Command Center' selected. The main area is titled 'Security Command Center' and features an 'OVERVIEW' tab. Under 'OVERVIEW', there is a chart titled 'Active Vulnerabilities Over Time By Severity' showing 1 active vulnerability across a scale from 0 to 2. The legend indicates: Critical (dark red), High (red), Medium (orange), Low (yellow), and Unspecified (light gray). Below the chart is a section titled 'Active Vulnerabilities' showing 1 active vulnerability. It includes tabs for 'FINDINGS BY CATEGORY', 'FINDINGS BY RESOURCE TYPE', and 'FINDINGS BY PROJECT'. A filter section allows filtering by 'Severity' (dropdown set to 'MFA not enforced') and 'Finding Category'. A total finding count of 1 is displayed. A red rectangular box highlights the 'Active Vulnerabilities' section.

Figure 6.33 – Security Command Center | OVERVIEW

Status	Last scanned	Category	Recommendation	Active	Severity	Standards
⚠️	August 30, 2022 at 3:01:56 PM GMT-5	MFA not enforced	Multi-factor authentication should be enabled for all users in your org unit	1	High	CIS 1.0 : 1.2 CIS 1.1 : 1.2 CIS 1.2 : 1.2 PCI : 8.3 NIST : IA-2 ISO : A.9.4.2
✓	August 30, 2022 at 2:21:56 PM GMT-5	Dataproc image ...	Dataproc clusters should not use images affected by Log4j vulnerability	0	Medium	
ⓘ	N/A	Non org IAM me...	Corporate login credentials should be used instead of Gmail accounts	0	Medium	CIS 1.0 : 1.1 CIS 1.1 : 1.1 CIS 1.2 : 1.1 PCI : 7.1.2 NIST : AC-3 ISO : A.9.2.3
ⓘ	N/A	Open ciscosecur...	Firewall rules should not allow connections from all IP addresses on TCP port 9090	0	Medium	PCI : 1.2.1 NIST : SC-7 ISO : A.13.1.1
ⓘ	N/A	Open directory s...	Firewall rules should not allow connections from all IP addresses on TCP or UDP port 445	0	Medium	PCI : 1.2.1 NIST : SC-7 ISO : A.13.1.1
ⓘ	N/A	Open firewall	Firewall rules should not allow connections from all IP addresses	0	Medium	PCI : 1.2.1

Figure 6.34 – Security Command Center | VULNERABILITIES

View by	RESOURCE TYPE	PROJECT	ASSETS CHANGED
Find resource type	No assets selected SET SECURITY MARKS		
Resource type ↑	Count	<input type="checkbox"/> resourceProperties.name securityCenterProperties.resourceType ↑ <input type="checkbox"/> organizations/342503585489 google.cloud.resourcemanager.Organization <input type="checkbox"/> My Project 8196 google.cloud.resourcemanager.Project <input type="checkbox"/> serviceusage.googleapis.com google.serviceusage.Service <input type="checkbox"/> datastore.googleapis.com google.serviceusage.Service <input type="checkbox"/> servicemanagement.googleapis.com google.serviceusage.Service <input type="checkbox"/> monitoring.googleapis.com google.serviceusage.Service <input type="checkbox"/> bigquerystorage.googleapis.com google.serviceusage.Service <input type="checkbox"/> storage.googleapis.com google.serviceusage.Service <input type="checkbox"/> bigquerymigration.googleapis.com google.serviceusage.Service	
All	1		
Organization	1		
resourcemanager.Project	1		
serviceusage.Service	15		

Figure 6.35 – Security Command Center | ASSETS

Findings for organization "cybersecuritysimplified.com"

Use Security Command Center's findings display to review possible security risks for your Google Cloud resources.

View by **CATEGORY** SOURCE TYPE FINDINGS CHANGED SEVERITY MORE OPTIONS **EXPORT**

No findings selected CHANGE ACTIVE STATE SET SECURITY MARKS MUTE OPTIONS

Category ↑	Count	Filter Attributes, properties and marks				
All	1	<input type="checkbox"/> category	resourceName	eventTime ↓	createTime	parent
		<input type="checkbox"/> MFA_NOT_ENFORCED	//cloudresourcemanager.googleapis.com/organizations/342503585489	August 30, 2022 at 3:01:55 PM UTC-5	August 30, 2022 at 3:01:56 PM UTC-5	organizations/342503585489/source/s/1520748722826384149

Figure 6.36 - Security Command Center | FINDINGS

Security Command Center

OVERVIEW VULNERABILITIES ASSETS FINDINGS SOURCES EXPLORE

Sources for organization "cybersecuritysimplified.com"

Use Security Command Center's sources display to review a summary of assets and findings from the security sources you have enabled.

Assets **Findings**

Time range — Last day

Assets summary
17 total assets

Asset	New	Deleted	Total
Organization	1	0	1
resourcemanager.Project	1	0	1
Service	15	0	15

Findings by source
1 total security findings

Source	Count
Security Health Analytics	1

Web Security Scanner
No active findings

Figure 6.37 – Security Command Center | SOURCES



Cloud Asset Inventory

Register for the [first Google Cloud Security Talks of 2022!](#) Learn about modern approaches to threat detection.

Cloud Asset Inventory

A metadata inventory service that allows you to view, monitor, and analyze all your GCP and Anthos assets across projects and services.

[Go to console](#)

[View documentation](#) for this product.

Figure 6.38 – Cloud Asset Inventory

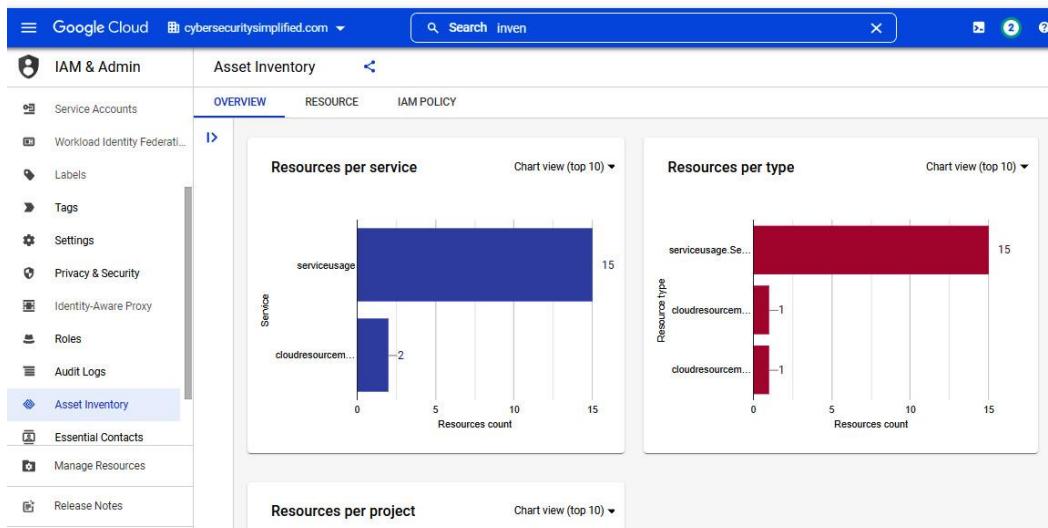


Figure 6.39 – The Asset Inventory OVERVIEW tab

The screenshot shows the Google Cloud Asset Inventory interface. The left sidebar is titled 'IAM & Admin' and includes options like Settings, Privacy & Security, Identity-Aware Proxy, Roles, Audit Logs, Asset Inventory (which is selected and highlighted in blue), Essential Contacts, Groups, Quotas, Manage Resources, Release Notes, and ..

The main area has tabs for OVERVIEW, RESOURCE (which is selected and highlighted in blue), and IAM POLICY.

On the left, under 'Filter results', there are filters for Resource type (serviceusage.Service, cloudresourcemanager.Organization, cloudresourcemanager.Project), Project (turing-botany-361019), and Location (global). The results count is 17.

The results table has columns: Display name, Resource type, Project Id, and Location. The data is as follows:

Display name	Resource type	Project Id	Location
biggquery.googleapis.com	serviceusage.Service	turing-botany-361019	global
biggquerymigration.googleapis.com	serviceusage.Service	turing-botany-361019	global
biggquerystorage.googleapis.com	serviceusage.Service	turing-botany-361019	global
clouddapis.googleapis.com	serviceusage.Service	turing-botany-361019	global
clouddebugger.googleapis.com	serviceusage.Service	turing-botany-361019	global
cloudtrace.googleapis.com	serviceusage.Service	turing-botany-361019	global
datastore.googleapis.com	serviceusage.Service	turing-botany-361019	global
logging.googleapis.com	serviceusage.Service	turing-botany-361019	global
monitoring.googleapis.com	serviceusage.Service	turing-botany-361019	global
servicemanagement.googleapis.com	serviceusage.Service	turing-botany-361019	global
serviceusage.googleapis.com	serviceusage.Service	turing-botany-361019	global

Figure 6.40 – The Asset Inventory RESOURCES tab

The screenshot shows the Google Cloud Asset Inventory interface, similar to Figure 6.40, but with the 'IAM POLICY' tab selected. The left sidebar and overall layout are identical.

The main area has tabs for OVERVIEW, RESOURCE, and IAM POLICY (which is selected and highlighted in blue).

On the left, under 'Filter results', there are filters for Query presets (Open policies, Non group members, Service Account as owners, Privileged roles) and Filters (Resource type: cloudresourcemanager.Organization, cloudresourcemanager.Project). The results count is 2.

The results table has columns: Resource and Role. The data is as follows:

Resource ↑	Role
cybersecuritysimplified.com	Actions Admin
//cloudr esourcemanager.googleapis.com/projects/turing-botany-361019	Owner

Figure 6.41 – The Asset Inventory IAM policy

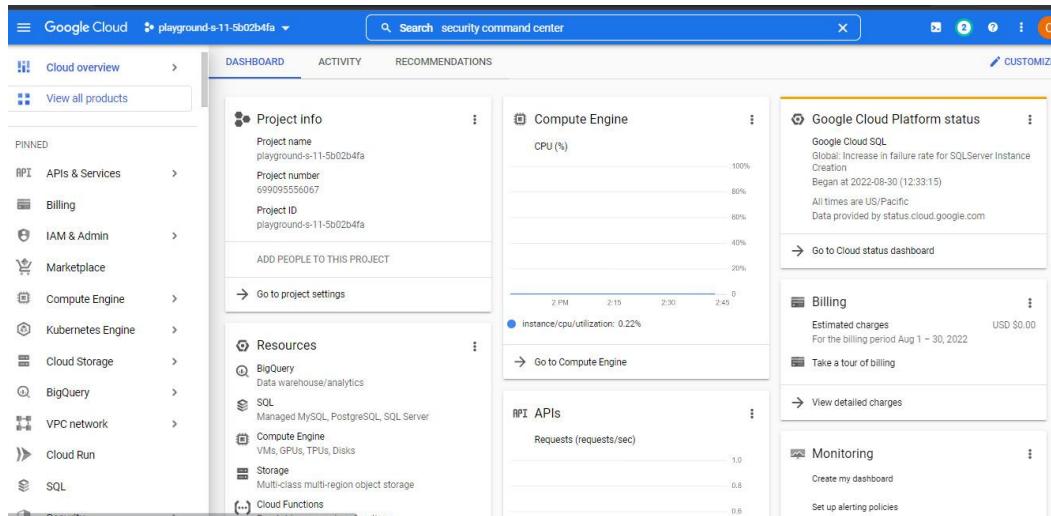


Figure 6.42 – The Cloud Overview DASHBOARD

	DASHBOARD	ACTIVITY	RECOMMENDATIONS
Today			
12:30 PM	Update project	1032835570213@cloudservices.gserviceaccount.com updated playground-s-11-5b02b4fa	
12:25 PM	Completed: Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest-allow-ssh	
12:25 PM	Completed: Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest-allow-rdp	
12:25 PM	Completed: Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest-allow-icmp	
12:24 PM	Completed: Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest-allow-custom	
12:24 PM	Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest-allow-ssh	
12:24 PM	Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest-allow-rdp	
12:24 PM	Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest-allow-icmp	
12:24 PM	Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest-allow-custom	
12:24 PM	Completed: Create network	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest	
12:24 PM	Create network	cloud_user_p_c8ce62b0@linuxacademygclabs.com created packttest	
12:22 PM	Completed: Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created default-allow-http	
12:22 PM	Completed: Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created default-allow-https	
12:22 PM	Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created default-allow-https	
12:22 PM	Create firewall rule	cloud_user_p_c8ce62b0@linuxacademygclabs.com created default-allow-http	
12:22 PM	Completed: Create VM	cloud_user_p_c8ce62b0@linuxacademygclabs.com created instance-1	
12:22 PM	Create VM	cloud_user_p_c8ce62b0@linuxacademygclabs.com created instance-1	
11:28 AM	Completed: google.api.serviceusage.v1beta1.ServiceUsage.Crea...	google.api.serviceusage.v1beta1.ServiceUsage.CreateConsumerOverride was executed on %2	

Figure 6.43 – The Cloud Overview ACTIVITY tab

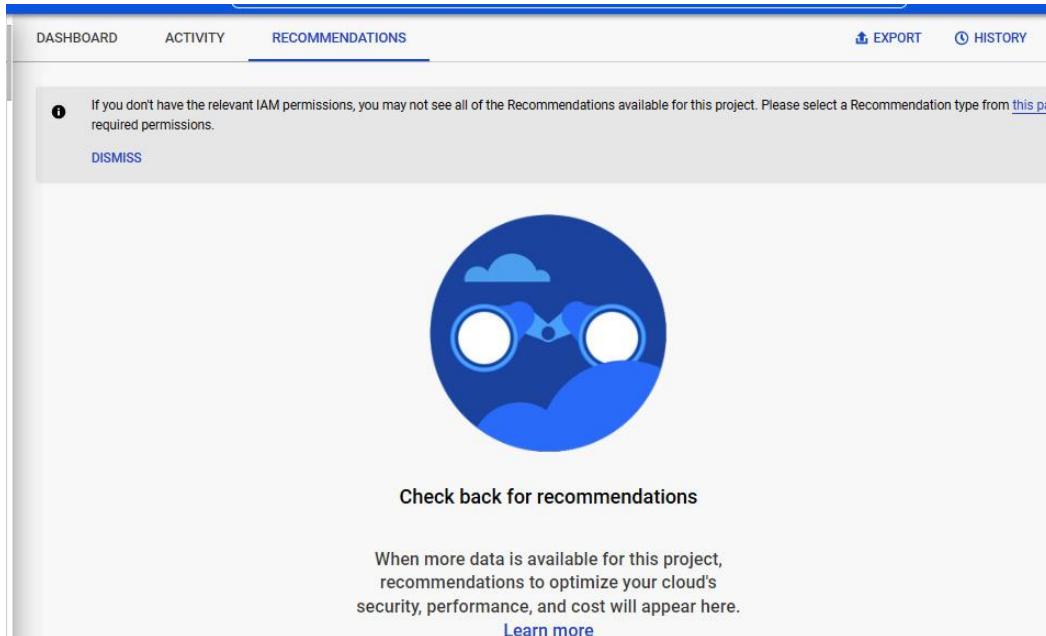


Figure 6.44 – The Cloud Overview RECOMMENDATIONS tab

```
Command Prompt - aws configure
C:\Users\antagonist>aws configure
AWS Access Key ID [None]: AKIA6GPHQ7SD2ZQY2G63
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: json
```

Figure 6.45 – The AWS CLI configuration settings to interact with AWS

```
Command Prompt
C:\Users\antagonist>aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "cloud_user",
            "UserId": "AIDA6GPHQ7SD2DYA5SQ6K",
            "Arn": "arn:aws:iam::975980002439:user/cloud_user",
            "CreateDate": "2022-08-23T05:11:58+00:00",
            "PasswordLastUsed": "2022-08-23T05:29:31+00:00"
        }
    ]
}
```

Figure 6.46 – AWS list users in IAM

```
Command Prompt - aws ec2 describe-security-groups
C:\Users\antagonist>aws ec2 describe-security-groups
```

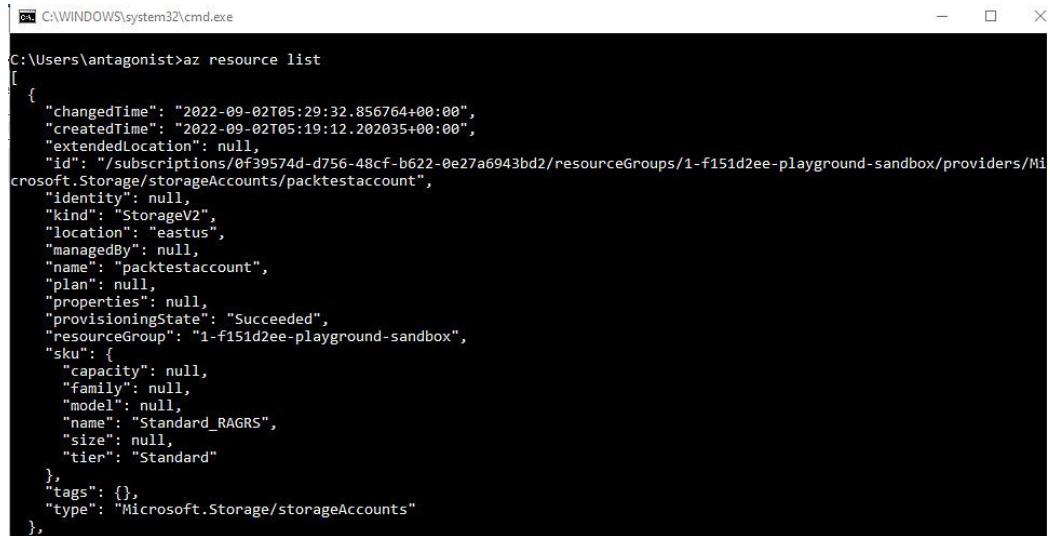
Figure 6.47 – AWS describe-security-groups

```
Command Prompt - aws ec2 describe-security-groups
[{"SecurityGroups": [
  {
    "Description": "default VPC security group",
    "GroupName": "default",
    "IpPermissions": [
      {
        "IpProtocol": "-1",
        "IpRanges": [],
        "Ipv6Ranges": [],
        "PrefixListIds": [],
        "UserIdGroupPairs": [
          {
            "GroupId": "sg-0b7a1022de50fd306",
            "UserId": "975980002439"
          }
        ]
      }
    ],
    "OwnerId": "975980002439",
    "GroupId": "sg-0b7a1022de50fd306",
    "IpPermissionsEgress": [
      {
        "IpProtocol": "-1",
        "IpRanges": [
          {
            "CidrIp": "0.0.0.0/0"
          }
        ],
        "UserId": "975980002439"
      }
    ]
  }
],-- More --
```

Figure 6.48 – AWS security groups and their attributes

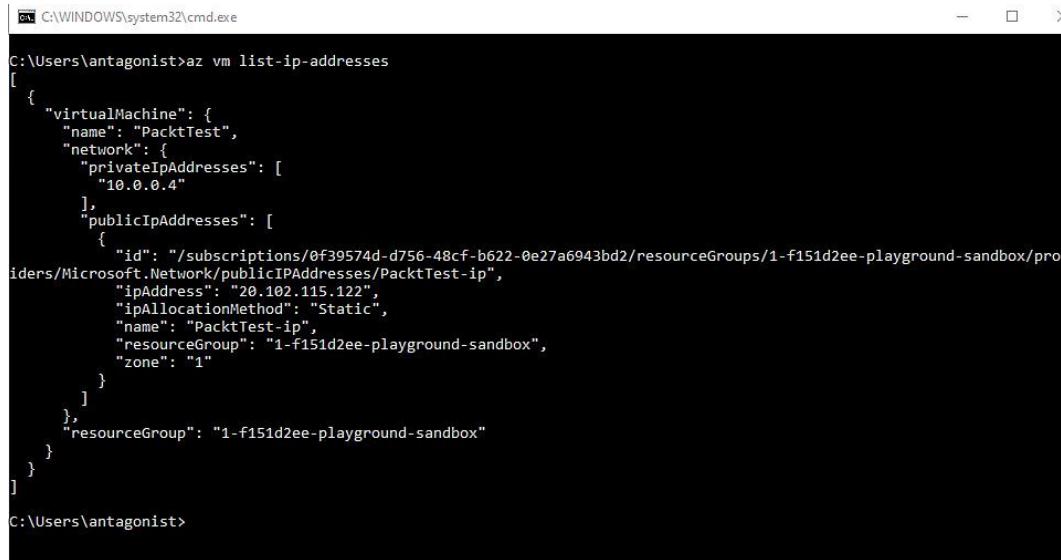
```
C:\Users\antagonist>az login
A web browser has been opened at https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize. Please continue
the login in the web browser. If no web browser is available or if the web browser fails to open, use device code flow
with `az login --use-device-code`.
[{"cloudName": "AzureCloud",
"homeTenantId": "3617ef9b-98b4-40d9-ba43-e1ed6709cf0d",
"id": "0f39574d-d756-48cf-b622-0e27a6943bd2",
"isDefault": true,
"managedByTenants": [],
"name": "P3-Real Hands-On Labs",
"state": "Enabled",
"tenantId": "3617ef9b-98b4-40d9-ba43-e1ed6709cf0d",
"user": {
"name": "cloud_user_p_52b4d0dd@azurelabs.linuxacademy.com",
"type": "user"
}
}]
```

Figure 6.49 – Logging in to Azure



```
C:\WINDOWS\system32\cmd.exe
C:\Users\antagonist>az resource list
[{"changedTime": "2022-09-02T05:29:32.856764+00:00",
"createdTime": "2022-09-02T05:19:12.202035+00:00",
"extendedLocation": null,
"id": "/subscriptions/0f39574d-d756-48cf-b622-0e27a6943bd2/resourceGroups/1-f151d2ee-playground-sandbox/providers/Microsoft.Storage/storageAccounts/packtestaccount",
"identity": null,
"kind": "StorageV2",
"location": "eastus",
"managedBy": null,
"name": "packtestaccount",
"plan": null,
"properties": null,
"provisioningState": "Succeeded",
"resourceGroup": "1-f151d2ee-playground-sandbox",
"sku": {
"capacity": null,
"family": null,
"model": null,
"name": "Standard_RAGRS",
"size": null,
"tier": "Standard"
},
"tags": {},
"type": "Microsoft.Storage/storageAccounts"
},
```

Figure 6.50 – The resource list



```
C:\WINDOWS\system32\cmd.exe
C:\Users\antagonist>az vm list-ip-addresses
[
  {
    "virtualMachine": {
      "name": "PacktTest",
      "network": {
        "privateIpAddresses": [
          "10.0.0.4"
        ],
        "publicIpAddresses": [
          {
            "id": "/subscriptions/0f39574d-d756-48cf-b622-0e27a6943bd2/resourceGroups/1-f151d2ee-playground-sandbox/providers/Microsoft.Network/publicIPAddresses/PacktTest-ip",
            "ipAddress": "20.102.115.122",
            "ipAllocationMethod": "Static",
            "name": "PacktTest-ip",
            "resourceGroup": "1-f151d2ee-playground-sandbox",
            "zone": "1"
          }
        ],
        "resourceGroup": "1-f151d2ee-playground-sandbox"
      }
    }
]
C:\Users\antagonist>
```

Figure 6.51 – Listing IP addresses associated with a VM

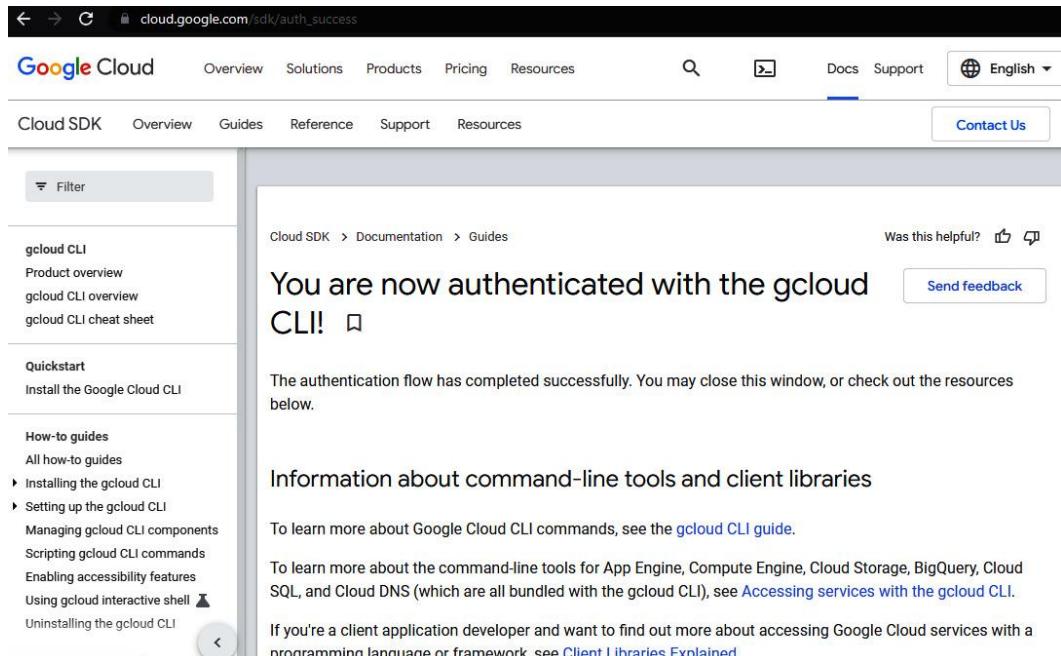


Figure 6.52 – Authentication



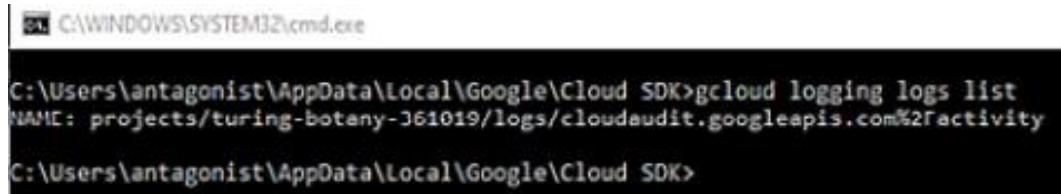
```
C:\WINDOWS\SYSTEM32\cmd.exe
C:\Users\antagonist\AppData\Local\Google\Cloud SDK>gcloud auth list
Credentialed Accounts

ACTIVE: *
ACCOUNT: packttest@cybersecuritysimplified.com

To set the active account, run:
  $ gcloud config set account `ACCOUNT`

C:\Users\antagonist\AppData\Local\Google\Cloud SDK>
```

Figure 6.53 – Listing credential accounts



```
C:\WINDOWS\SYSTEM32\cmd.exe
C:\Users\antagonist\AppData\Local\Google\Cloud SDK>gcloud logging logs list
NAME: projects/turing-botany-361019/logs/cloudaudit.googleapis.com%2Factivity
C:\Users\antagonist\AppData\Local\Google\Cloud SDK>
```

Figure 6.54 – Listing logs

Links

- For detailed information on setting up Security Command Center, please view the Google Cloud Documentation at <https://cloud.google.com/security-command-center/docs/set-up>.
- Instructions on getting started and installing the AWS CLI can be found at <https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-started.html>.
- Instructions on getting started and installing the Azure CLI can be found at <https://docs.microsoft.com/en-us/cli/azure/get-started-with-azure-cli>.
- AWS has a command library that can be found at <https://awscli.amazonaws.com/v2/documentation/api/latest/index.html>.
- The full Azure CLI command reference can be found at <https://docs.microsoft.com/en-us/cli/azure/reference-index?view=azure-cli-latest>.
- Instructions on getting started and installing the Google Cloud CLI can be found at <https://cloud.google.com/sdk/docs/install>.
- The Google Cloud CLI cheat sheet can be found at <https://cloud.google.com/sdk/docs/cheatsheet>.

Commands

Command 6.1

To list the number of users within AWS, we type in the following command:

```
aws iam-list users
```

Command 6.2

As another example, if you need to know which groups are connected to AWS VPCs, you can type the following command:

```
aws ec2 describe-security-groups
```

Command 6.3

To list all the resource groups we have, use the following command:

```
az resource list
```

Command 6.4

To get a list of IP addresses associated with a VM, we can use the following command:

```
az vm list-ip-addresses
```

Command 6.5

To list all credential accounts, type the following command:

```
gcloud auth list
```

Command 6.6

To list your project's logs, type the following command:

```
gcloud logging logs list
```

Figures

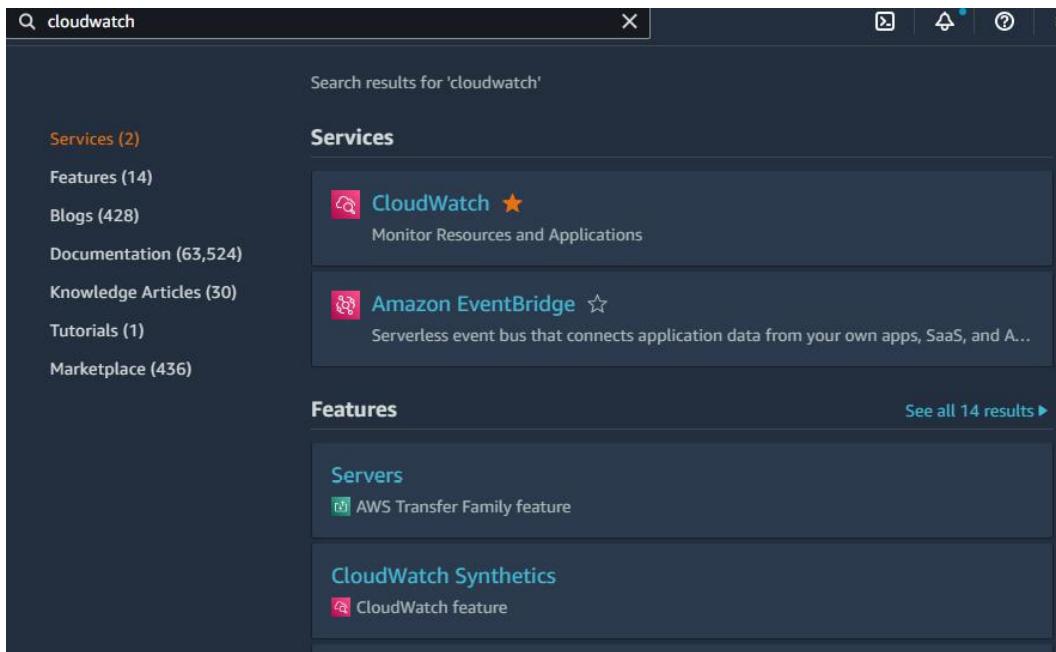


Figure 7.1 – Searching for Amazon CloudWatch

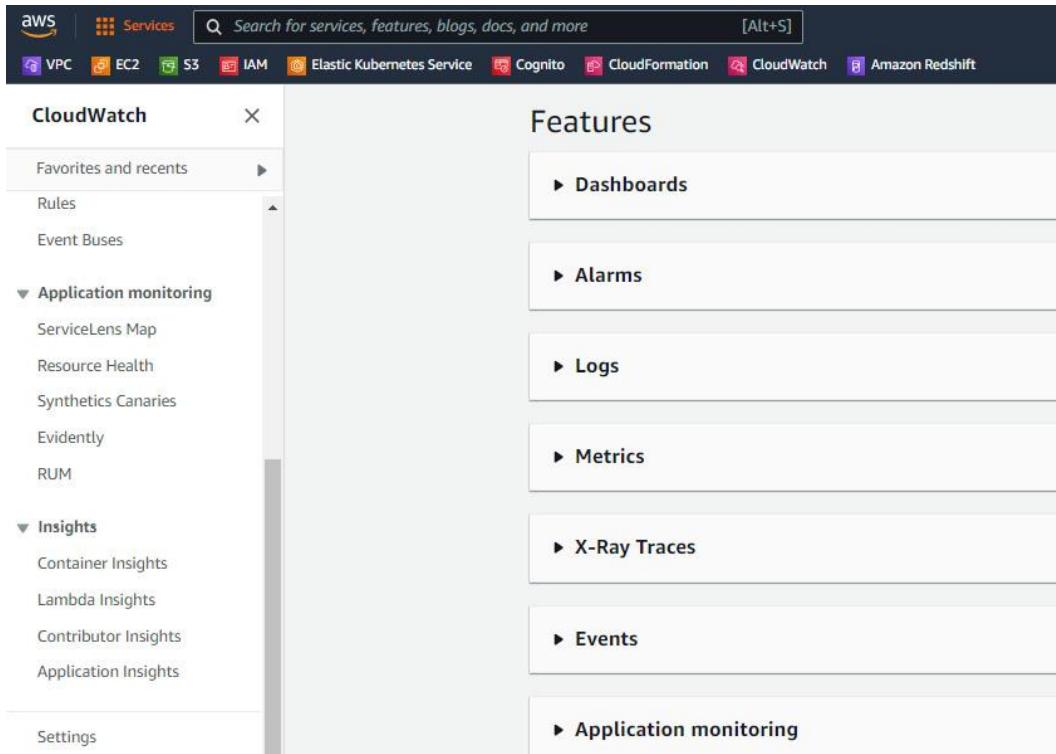


Figure 7.2 – Features

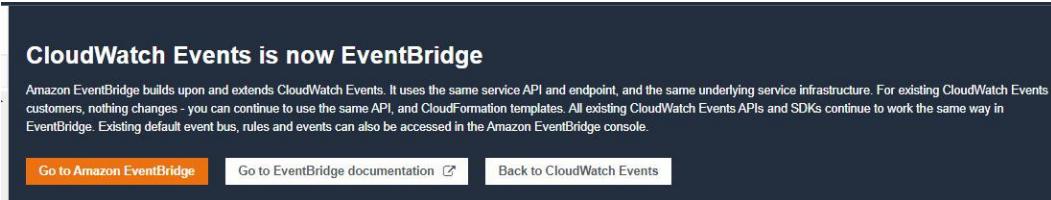


Figure 7.3 – EventBridge main page

This screenshot shows the "Define rule detail" configuration page. The title is "Rule detail".

- Name:** packttestrule (Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-_,_)
- Description - optional:** Enter description
- Event bus:** default (Info) Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.
- Enable the rule on the selected event bus:** (radio button selected)
- Rule type:** Rule with an event pattern (Info) A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.
- Schedule:** (radio button unselected) A rule that runs on a schedule

At the bottom right are "Cancel" and "Next" buttons.

Figure 7.4 – Define rule detail

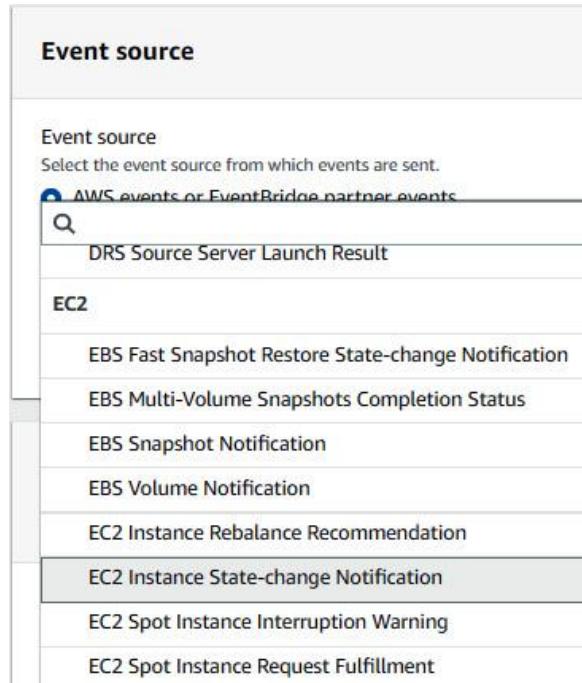


Figure 7.5 – Event source

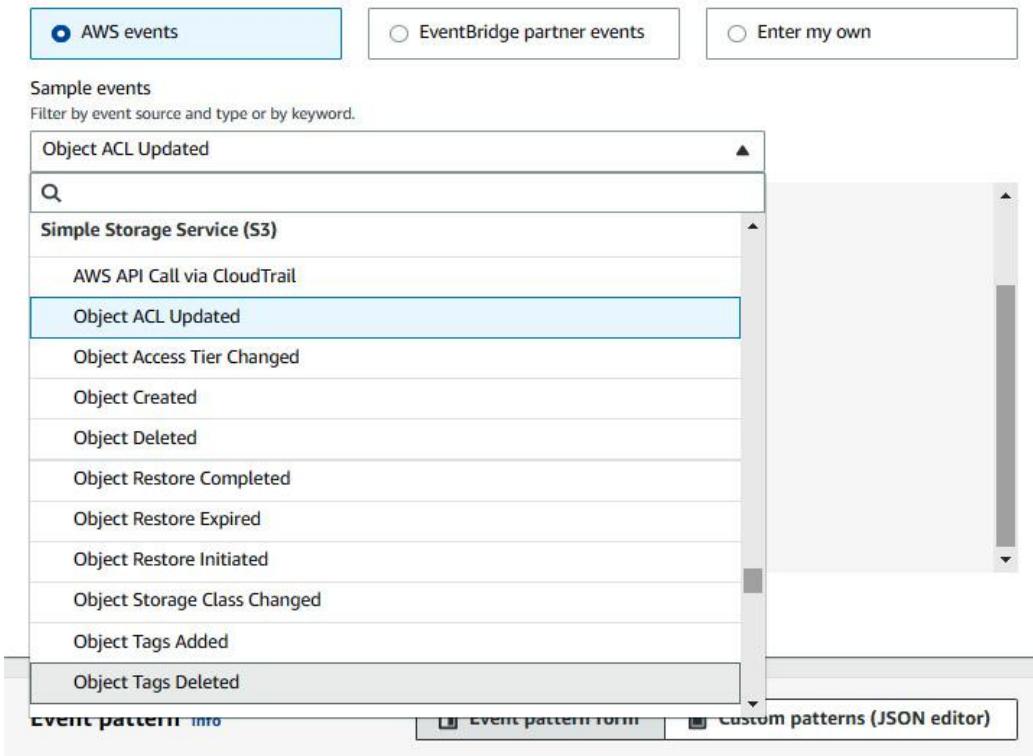


Figure 7.6 – Object ACL Updated

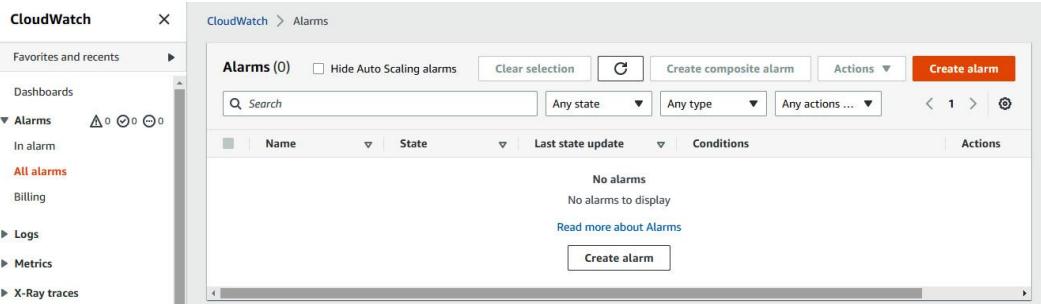


Figure 7.7 – The Alarms tab

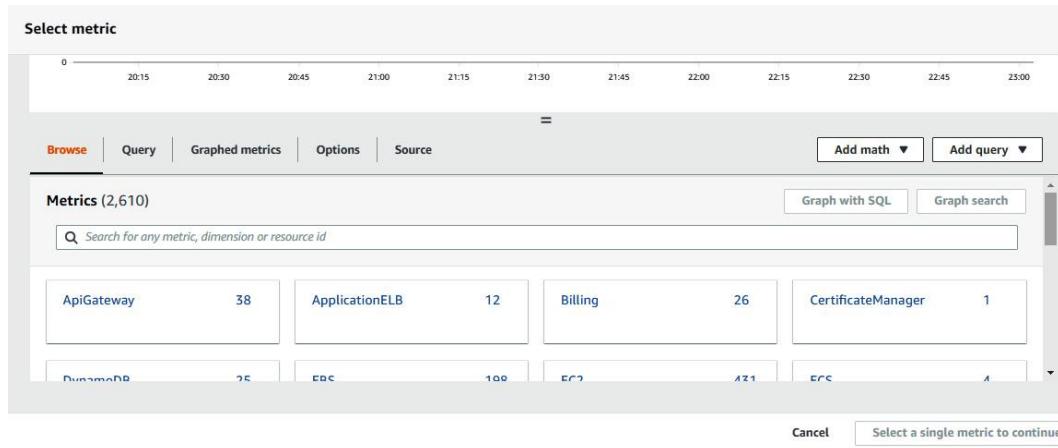


Figure 7.8 – Metrics

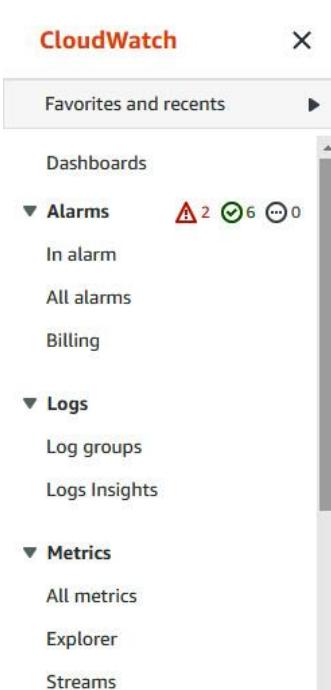


Figure 7.9 – Dashboards

The screenshot shows the CloudWatch Alarms interface. At the top, there are buttons for 'Clear selection', 'Create composite alarm', 'Actions', and a prominent red 'Create alarm' button. Below this is a search bar and filters for 'In alarm', 'Any type', and 'Any actions ...'. A navigation bar indicates page 1 of 1. The main table lists two alarms:

Name	State	Last state update	Conditions	Actions
TargetTracking-table/packttable-AlarmLow- b8085448-3d1d- 448e-94e1- 78a2aabf665c	⚠️ In alarm	2022-09-06 23:25:05	ConsumedWriteCapacityUnits < 30 for 15 datapoints within 15 minutes	<input checked="" type="checkbox"/> Actions
TargetTracking-table/packttable-AlarmLow- 6bf7d40a-ccaa- 428e-9d17- eedb56422a74	⚠️ In alarm	2022-09-06 23:24:31	ConsumedReadCapacityUnits < 30 for 15 datapoints within 15 minutes	<input checked="" type="checkbox"/> Actions

Figure 7.10 – Example alarms



Figure 7.11 – Amazon Inspector

The screenshot shows the 'Enable Inspector' configuration page. It starts with a title 'Enable Inspector' and an 'Info' link. Below this is a 'Service permissions' section with a 'View role permissions' button. A note explains that enabling Inspector grants permission to discover, classify, and protect sensitive data. At the bottom is a large red 'Enable Inspector' button.

Figure 7.12 – Enabling Amazon Inspector

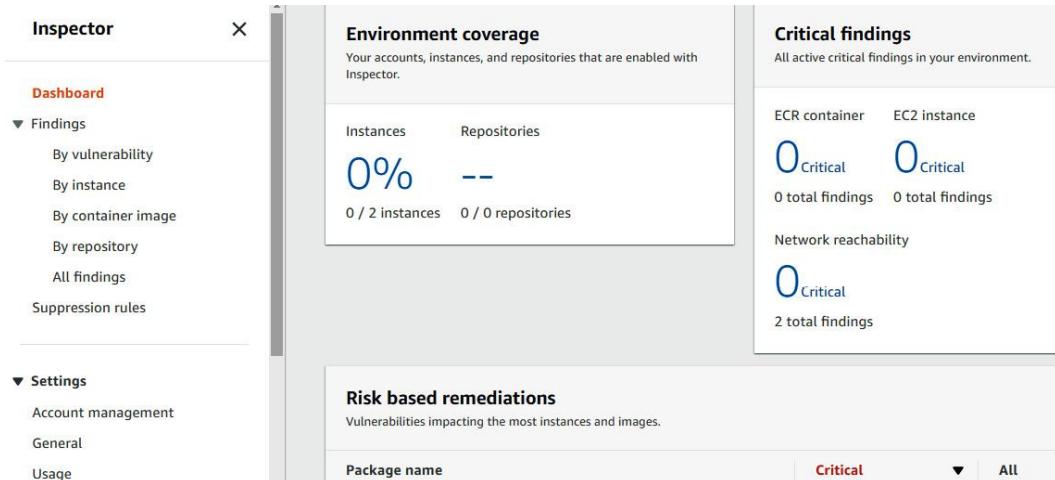


Figure 7.13 – The Amazon Inspector dashboard

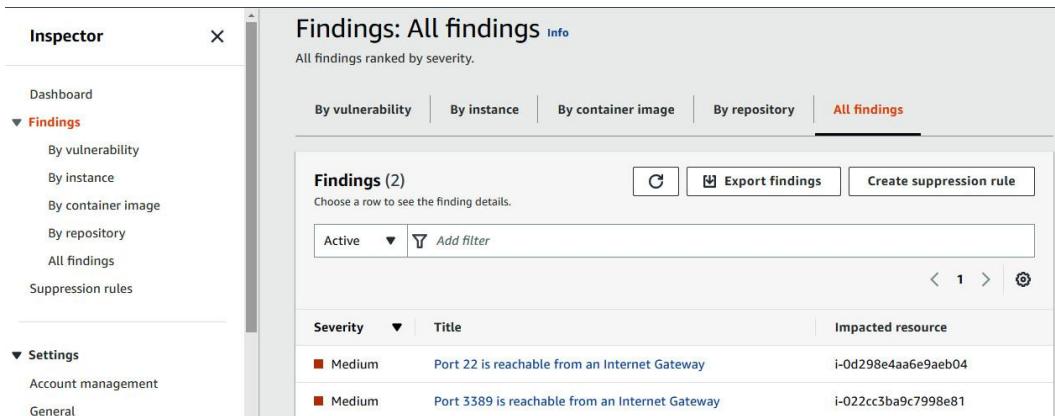


Figure 7.14 – The Amazon Inspector findings

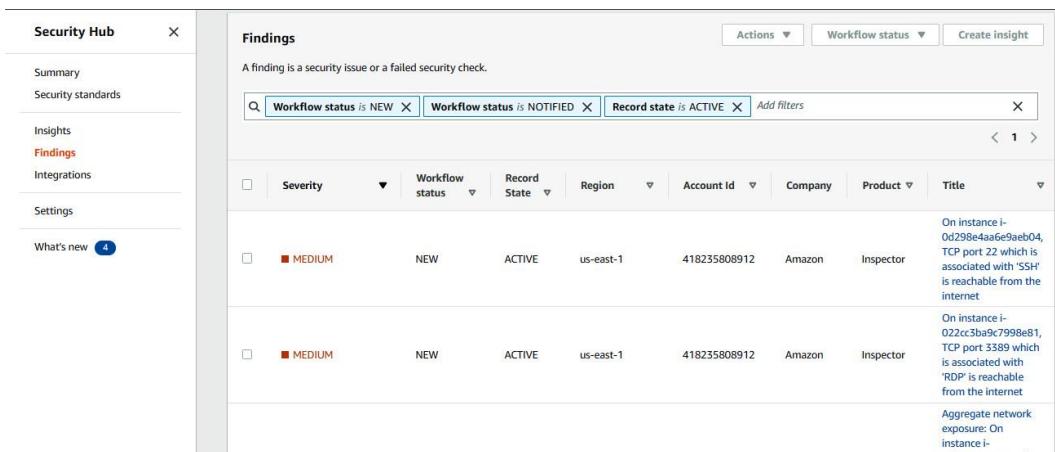


Figure 7.15 – Integration with AWS Security Hub

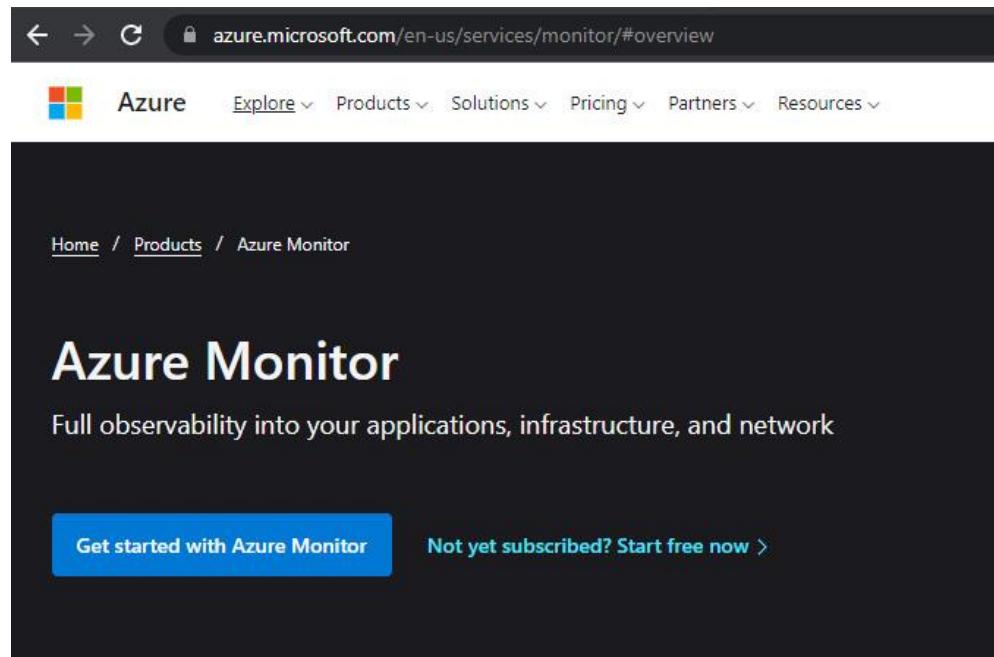


Figure 7.16 – Azure Monitor

A screenshot of the Azure Monitor Overview page. The top navigation bar shows 'Microsoft Azure' and a search bar. The main title is 'Monitor | Overview'. On the left, there's a sidebar with sections for 'Overview', 'Activity log', 'Alerts', 'Metrics', 'Logs', 'Change Analysis', 'Service Health', and 'Workbooks'. Below this is another sidebar for 'Insights' with options like 'Applications', 'Virtual Machines', 'Storage accounts', 'Containers', 'Networks', 'SQL (preview)', 'Azure Cosmos DB', and 'Key Vaults'. The main content area is divided into several cards: 'Application insights' (monitor app availability, performance, errors), 'Container Insights' (gain visibility into controller, node, and container health), 'VM Insights' (monitor VM health and dependencies), 'Network Insights' (view health and metrics for deployed network resources), 'Metrics' (create charts to monitor usage and performance), 'Alerts' (get notified and respond using alerts and actions), 'Logs' (analyze and diagnose issues with log queries), 'Workbooks' (create and share interactive reports), 'Change Analysis' (investigate what changed to trigger incidents), and 'Diagnostic Settings' (route monitoring metrics and logs to relevant services). Each card has a 'View More' link.

Figure 7.17 – Azure Monitor Overview

Home > Monitor

Monitor | Activity log

Activity Overview Export Activity Logs Download as CSV Insights Pin current filters Reset filters

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. Visit Log Analytics

Search Quick insights

Subscription : P2-Real Hands-On Labs Event severity : All Timespan : Last 6 hours Add Filter

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Validate Deployment	Started	5 minutes a...	Thu Sep 08 ...	P2-Real Hands-On Labs	cloud_user_p_d28d77d3@...
Create Deployment	Started	8 minutes a...	Thu Sep 08 ...	P2-Real Hands-On Labs	cloud_user_p_d28d77d3@...
> Validate Deployment	Succeeded	8 minutes a...	Thu Sep 08 ...	P2-Real Hands-On Labs	cloud_user_p_d28d77d3@...
> Create Deployment	Succeeded	8 minutes a...	Thu Sep 08 ...	P2-Real Hands-On Labs	cloud_user_p_d28d77d3@...
> Validate Deployment	Succeeded	8 minutes a...	Thu Sep 08 ...	P2-Real Hands-On Labs	cloud_user_p_d28d77d3@...
> Create Deployment	Succeeded	9 minutes a...	Thu Sep 08 ...	P2-Real Hands-On Labs	cloud_user_p_d28d77d3@...
> Validate Deployment	Succeeded	9 minutes a...	Thu Sep 08 ...	P2-Real Hands-On Labs	cloud_user_p_d28d77d3@...
> Create role assignment	Failed	11 minutes ...	Thu Sep 08 ...	P2-Real Hands-On Labs	cloud_user_p_d28d77d3@...
> Update resource group	Succeeded	an hour ago	Wed Sep 07 ...	P2-Real Hands-On Labs	laas-vader-standard
> Create Deployment	Succeeded	an hour ago	Wed Sep 07 ...	P2-Real Hands-On Labs	laas-vader-standard

Figure 7.18 – Azure Monitor Activity log

Home > Monitor | Alerts >

Create an alert rule

Scope Condition Actions Details Tags Review + create

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Selected signal: All Administrative operations

Chart period Over the last week

Data shown in the graph only represents a subset of activity logs for the filter configured and is shown as an aid for configuring better alert rules. For exact analysis use Activity Logs.

activityLogHistoryBarSeries

Figure 7.19 – Creating an alert rule

The screenshot shows the 'Network Watcher | Get started' page. On the left, there's a sidebar with a search bar and links for Overview, Get started, Monitoring (Topology, Connection monitor (classic), Connection monitor, Network Performance Monitor), Network diagnostic tools (IP flow verify, NSG diagnostic, Next hop, Effective security rules, VPN troubleshoot, Packet capture, Connection troubleshoot), and Metrics. The main content area has a title 'Monitor, diagnose, view metrics, and manage logs'. It includes a brief description of Network Watcher's purpose, followed by three cards: 'Track resource health' (with a lightbulb icon), 'Monitor connectivity' (with a computer icon), and 'Analyze connectivity' (with a waveform icon). Each card has a 'Learn more' link and a corresponding button: 'Explore AMN', 'View connection monitor', and 'View NSG flow logs'.

Figure 7.20 – Azure Network Watcher

The screenshot shows the 'Network Watcher | Effective security rules' page. The sidebar is identical to Figure 7.20. The main area has a message 'Showing only top 50 security rules in each grid, click Download above to see all.' Below are dropdown menus for Subscription (P2-Real Hands-On Labs), Resource group (1-9377d34b-playground-sandbox), and Virtual machine (packttest2). A section titled 'Select a network interface below to see the effective security rules and network security groups associated with it.' shows a 'Scope' of 'Virtual machine (packttest2)' and a 'Network interface' of 'packttest252'. Under 'Associated NSGs', it lists 'packttest2-nsg (Network interface)'. A note says 'Click on a rule row to see the expanded list of prefixes.' At the bottom, there's a list of security rules starting with 'packttest2-nsg'.

Figure 7.21 – Effective security rules

Microsoft Azure | Search resources, services, and docs (G+ /)

Home > Network Watcher | Effective security rules >

packttest2-nsg Network security group

Subscription (move) : P2-Real Hands-On Labs
Subscription ID : 964df7ca-36a4-48b6-a695-1ed9d5723f8
Tags (edit) : Click here to add tags

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑	Name ↓	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
300	HTTP	80	TCP	Any	Any	Allow
320	HTTPS	443	TCP	Any	Any	Allow
340	SSH	22	TCP	Any	Any	Allow
360	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
65000	AllowNetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Figure 7.22 – packttest2-nsg

Google Cloud playground-s-11-dedc1d8b ▾ Search monitor

Monitoring

Metrics Scope 1 project

- Overview
- Dashboards
- Integrations NEW
- Services
- Metrics explorer
- Alerting
- Uptime checks
- Groups
- Managed Prometheus
- Permissions NEW
- Settings
- Release Notes

Complete these steps to better understand your system

Integrate with Google Cloud services
Monitor cloud resources with zero configuration

- Install an agent Collect additional system and application metrics
- Create a dashboard Visually analyze metrics important to you
- Create an uptime check Probe endpoints to determine what resources are available
- Create an alert Resolve problems quickly with timely notifications

Ops agent
The Ops Agent is the primary agent from your Compute Engine instances. It collects metrics into a single agent, the Ops Agent, which supports high-throughput OpenTelemetry Collector for metrics.

You can also configure the Ops Agent to collect logs from third-party applications.

Dashboards
Get visibility into your Google Cloud resources and services.

+ CREATE DASHBOARD

Infrastructure Preconfigured resource dashboards

Favorites Recently viewed favorites

VM Instances

GKE

Disks

Figure 7.23 – Google Cloud Monitoring Overview

Category	Name	Type
All	Disks	Google Cloud Platform
Recently Viewed	Firewalls	Google Cloud Platform
Favorites	Infrastructure Summary	Google Cloud Platform
Custom	VM Instances	Google Cloud Platform
GCP		
Integrations		
Other		

Figure 7.24 – Dashboards Overview

Name	Group ID	Rules	Instances
default-allow-http	3970130856637640315	1	2
default-allow-https	7955625692873633403	1	2
default-allow-icmp	7827715502304968744	1	0
default-allow-internal	9030649775064924200	3	0
default-allow-rdp	4019051215157641256	1	0
default-allow-ssh	3340866114244886568	1	0
packttest-allow-custom	1522849948686888630	1	0
packttest-allow-icmp	3039254922101272245	1	0
packttest-allow-rdp	1890941629640224436	1	0
packttest-allow-ssh	1736883278741515955	1	0
packttest2-allow-custom	7521867277679210139	1	0
packttest2-allow-icmp	6185150275501960857	1	0
packttest2-allow-rdp	7689936052415639191	1	0
packttest2-allow-ssh	56223319815630486	1	0

Figure 7.25 – The Firewalls dashboard

Name	Group ID	Rules	Instances
default-allow-ssh	3340866114244886568	1	2
default-allow-https			2
① default-allow-icmp			0
① default-allow-internal			0
① default-allow-rdp			0
① default-allow-ssh			0
① packttest-allow-custom			0
① packttest-allow-icmp			0
① packttest-allow-rdp			0
① packttest-allow-ssh			0
① packttest2-allow-custom	7521867277679210139	1	0
① packttest2-allow-icmp	6185150275501960857	1	0
① packttest2-allow-rdp	7689936052415639191	1	0
① packttest2-allow-ssh	56223319815630486	1	0

Figure 7.26 – Security Rules

The screenshot shows the Google Cloud Monitoring Alerts interface. The left sidebar has 'Alerting' selected. The main area displays a summary with 0 incidents firing, 0 incidents acknowledged, and 0 alert policies. A note says 'Monitoring now supports both user-scoped and device-scoped Cloud Console Mobile notification channels'. Below the summary is an 'Incidents' section with a table header for State, Policy name, Incident summary, and Opened, and a message 'No rows to display'.

Figure 7.27 – Alerts

This screenshot is identical to Figure 7.27, showing the Google Cloud Monitoring Alerts interface. The left sidebar has 'Alerting' selected. The main area displays a summary with 0 incidents firing, 0 incidents acknowledged, and 0 alert policies. A note says 'Monitoring now supports both user-scoped and device-scoped Cloud Console Mobile notification channels'. Below the summary is an 'Incidents' section with a table header for State, Policy name, Incident summary, and Opened, and a message 'No rows to display'.

Figure 7.27 – Alerts

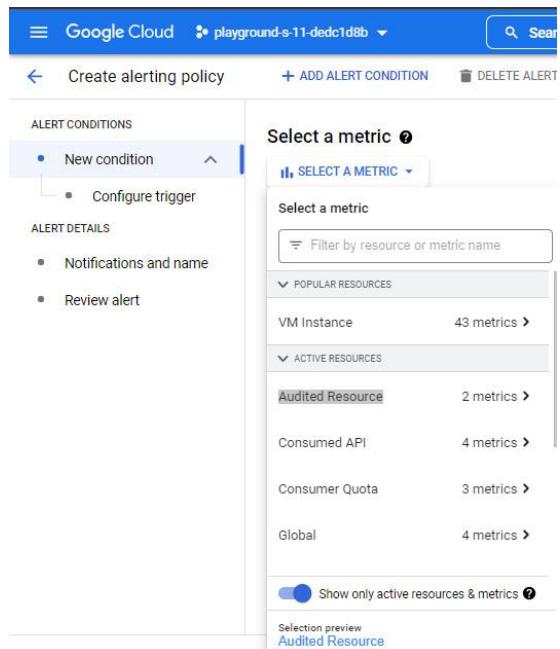


Figure 7.28 – Selecting a metric

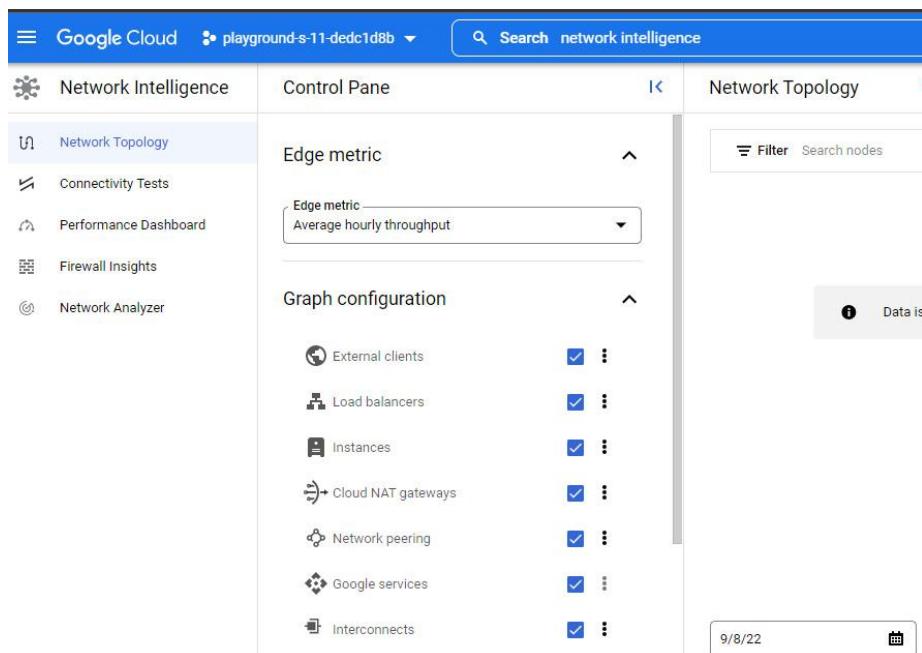


Figure 7.29 – Network Intelligence

The screenshot shows the Google Cloud Firewall Insights page. At the top, there's a search bar and navigation links for 'SAVE AS', 'CONFIGURATION', and 'DISMISS HISTORY'. Below the header, there are several sections:

- Shadowed rules**: A note says "Currently, shadowed rule insights are not enabled. You can enable shadowed rule insights in 'Configuration'".
- Deny rules with hits**: Shows 0 rules, 1 day observation period, and last update time as "Not applicable". It includes a table with columns 'Firewall' and 'Hit count'.
- Allow rules with no hits**: A note says "Currently, overly permissive rule insights are not enabled. You can enable overly permissive rule insights in 'Configuration'".
- Allow rules with unused attributes**: A note says "Currently, overly permissive rule insights are not enabled. You can enable overly permissive rule insights in 'Configuration'".
- Allow rules with overly permissive IP address or port ranges**: A note says "Currently, overly permissive rule insights are not enabled. You can enable overly permissive rule insights in 'Configuration'".

Figure 7.30 – Firewall Insights

VPC firewall rules

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Note: App Engine firewalls are managed in the [App Engine Firewall rules section](#).

The screenshot shows a table of VPC firewall rules. The columns are: Name, Type, Targets, Filters, Protocols / ports, Action, and Network. There are seven rows, each with a checkbox for selection:

Name	Type	Targets	Filters	Protocols / ports	Action	Network
default-allow-https	Ingress	https-server	IP ranges: 0.0.0.0/0	tcp:443	Allow	default
default-allow-http	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:80	Allow	default
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	default
default-allow-internal	Ingress	Apply to all	IP ranges: 10.0.0.0/16	tcp:0-65535 udp:0-65535 icmp	Allow	default
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	default
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	default

Figure 7.31 – VPC firewalls rules

The screenshot shows the Google Cloud Network Intelligence interface. On the left, a sidebar lists 'Network Topology', 'Connectivity Tests', 'Performance Dashboard', 'Firewall Insights', and 'Network Analyzer' (which is selected). The main area is titled 'Network Analyzer' with 'PREVIEW' and 'CHANGE SCOPE PROJECT UPDATE' buttons. A message states 'Network Analyzer has scanned 1 project. There are no insights for the current metric scope.' Below this is a 'Summary' section with a last run time of 'Sep 8, 2022, 1:55:08 AM'. It includes a table of insights by category:

Insight category	Total insights	Details	Description
VPC network	0	Covers basic VPC network setup and configuration issues, such as information about or issues with IP addresses...	▼
Network services	0	Lists load balancer related issues and informational insights suggesting best practices. Examples include load ...	▼
Kubernetes engine	0	Covers GKE related networking issues that can impact GKEs operation and connectivity. Network analyzer also ...	▼
Hybrid connectivity	0	Lists hybrid connectivity related issues and information suggesting best practices for Cloud VPN, Cloud Interco...	▼
Managed services	0	Lists connectivity issues with Google-managed services. Network Analyzer supports detecting connectivity issu...	▼

Below the summary is a 'Insights by priority' section with four categories: Critical (0), High (0), Medium (0), and Low (0), each with a 'FILTER' button.

Figure 7.32 – Network Analyzer

Links

- For detailed instructions on creating a rule that triggers an event from an AWS resource, go to <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-get-started.html>.

Chapter 8

Figures

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a navigation sidebar with options like Dashboard, Access management, and Access reports. Under Access reports, 'Credential report' is selected. The main area is titled 'Credential Report' and contains a button labeled 'Download Report'. Below the button, there's a note: 'Click the button to download a report that lists all your account's users and the status of their various credentials. After a report is created, it is stored for up to four hours. For more information see the documentation.' A 'Download Report' button is also present at the bottom of the page.

Figure 8.1 – AWS IAM Credential Report

C	D	E	F	G	H
user_creation_time	password_enabled	password_last_used	password_last_changed	password_mfa_active	
2020-09-14T11:17:53+00:00	not_supported	2022-09-11T22:03:35+00:00	not_supported	not_supported	TRUE
2022-09-11T22:05:13+00:00	TRUE	no_information	2022-09-11T22:05:13+00:00	N/A	FALSE

Figure 8.2 – AWS credential report download

The screenshot shows the Microsoft Azure portal's 'Users | All users' page. At the top, there's a search bar and several action buttons: '+ New user', '+ New guest user', 'Bulk operations', 'Refresh', 'Reset password', 'Per-user multifactor authentication', 'Delete user', 'Columns', and 'Got feedback?'. Below the search bar, a message says 'Try out the new user list experience improvements. Refresh to enable the preview.' On the left, there's a sidebar with links like 'All users (preview)', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage', 'Deleted users (preview)', 'Password reset', 'User settings', 'Bulk operation results', 'Troubleshooting + Support', and 'New support request'. The main area shows a table of users with columns: Name, User principal name, Directory synced, Account enabled, Identity issuer, Company name, and Creation type. A modal window titled 'Pick a field' is open over the table, showing a dropdown menu for 'Creation time' with options like 'Last 7 days', 'Last 14 days', 'Last 30 days', 'Last 90 days', 'Last 360 days', and 'More than 360 days ago'.

Figure 8.3 – Microsoft Azure user list

6 users found

<input type="checkbox"/>	Display name ↑	User principal name	User type	On-premises sy...	Identities	Company name	Created date time
<input type="checkbox"/>	Captain America	avenger@shinesa...	Member	No	shinesacambricoutlook.onmicrosoft.com		May 7, 2021, 9:24
<input type="checkbox"/>	Carmen Sandiego	CarmenS@shines...	Member	No	shinesacambricoutlook.onmicrosoft.com		Nov 24, 2021, 11:5
<input type="checkbox"/>	Gleauxbal	GleauxbalTest@sh...	Member	No	shinesacambricoutlook.onmicrosoft.com		Oct 14, 2021, 6:27
<input type="checkbox"/>	Scooby Do	scoobydo@shines...	Member	No	shinesacambricoutlook.onmicrosoft.com		May 7, 2021, 9:21

Figure 8.4 – Microsoft Azure filtered user list

The screenshot shows the Azure portal's user management interface. On the left, a sidebar lists options like Overview, Audit logs, Sign-in logs, and Diagnose and solve problems. The main area is titled 'Carmen Sandiego' and shows basic information: User principal name (CarmenS@shinesacambricoutlook.onmicrosoft.com), Object ID (53ebe5a0-6f71-4118-9d3f-93606d225d93), Created date time (Nov 24, 2021, 11:52 AM), User type (Member), and Identities (shinesacambricoutlook.onmicrosoft.com). Below this, there's a 'My Feed' section with cards for Account status (Enabled), Sign-ins (Last sign-in: -- --), and B2B collaboration (Convert this internal user to be a B2B user).

Figure 8.5 – Microsoft Azure selected user with sign-in details

This screenshot shows a summary of a user's sign-in history. It features a large card with a 'Sign-ins' icon, the text 'Last sign-in: -- --', and a 'See all sign-ins' button.

Figure 8.6 – Microsoft Azure user sign-in history

The screenshot shows the 'Audit logs' section under 'Roles and administrators'. The table header includes columns for Date, Service, Category, Activity, Status, Status reason, Target(s), Initiated by (act...), and User Agent. A single entry is visible: '8/18/2022, 3:47:52 PM PIM RoleManagement Triggered PIM alert Success The organization do... Azure AD PIM'.

Figure 8.7 – Microsoft Azure role management audit logs

Audit Log Details

Activity	Target(s)	Modified Properties
Activity		
Date	8/18/2022, 3:47 PM	
Activity Type	Triggered PIM alert	
Correlation ID	86543f84-501e-4f61-870e-6ac48bdcf2f1	
Category	RoleManagement	
Status	success	
Status reason		
User Agent		
Initiated by (actor)		Additional Details
Type	Application	
Display Name	Azure AD PIM	
App ID		
Service principal ID	9dfd627f-bdc5-4b1c-af9d-c85097fdeff8	
Service principal name		

Figure 8.8 – Microsoft Azure audit log entry performed by a default service

The screenshot shows the GCP Policy Analyzer interface. At the top, there's a navigation bar with 'Policy Analyzer', 'HELP ASSISTANT', and 'LEARN' buttons. Below the navigation, a section titled 'Create query from template' is shown. It says 'Top query questions are listed below. Select a template to help you get started.' There are six templates displayed in a grid:

- Custom query**: Run queries on principal, resource, or access. Includes a 'CREATE CUSTOM QUERY' button.
- Who can impersonate a service account?**: Example query question. Includes a 'CREATE QUERY' button.
- Who can change firewall rules in my project?**: Example query question. Includes a 'CREATE QUERY' button.
- What access does my employee (or terminated employee) have?**: Example query question. Includes a 'CREATE QUERY' button.
- What roles does a specific user have on a given resource?**: Example query question. Includes a 'CREATE QUERY' button.
- Who can delete GCS buckets?**: Example query question. Includes a 'CREATE QUERY' button.

Figure 8.9 – GCP Policy Analyzer custom query

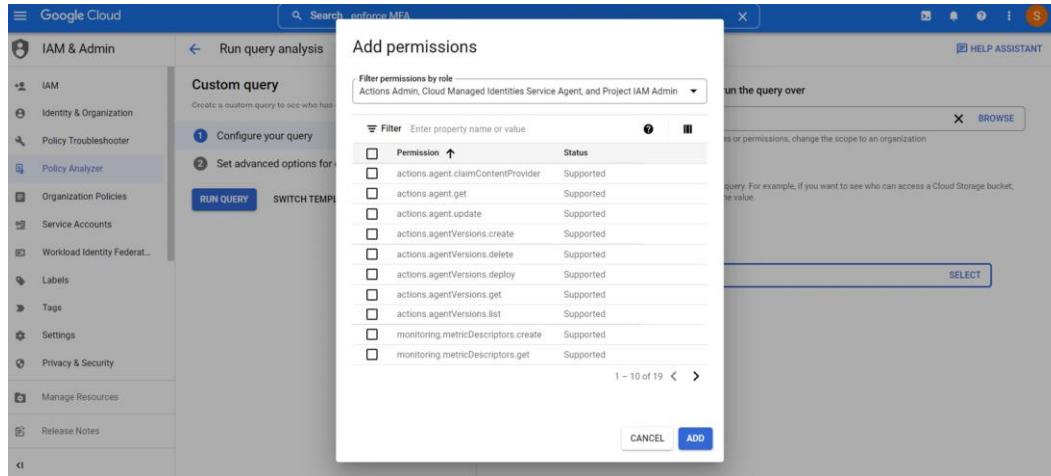


Figure 8.10 – GCP Policy Analyzer custom query filter

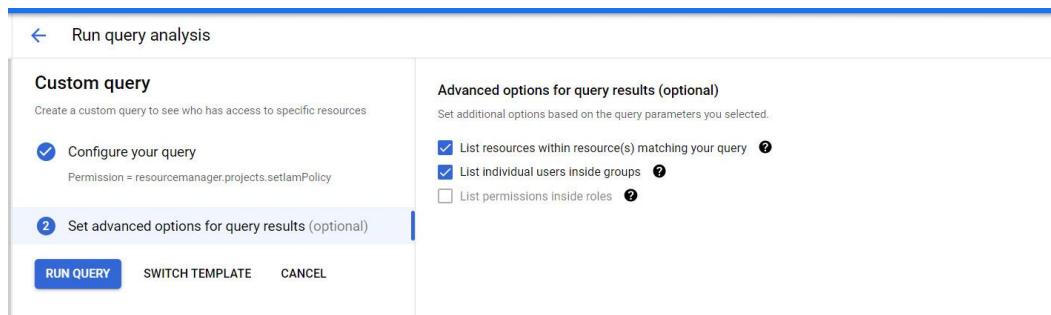


Figure 8.11 – GCP Policy Analyzer custom query and inheritance options

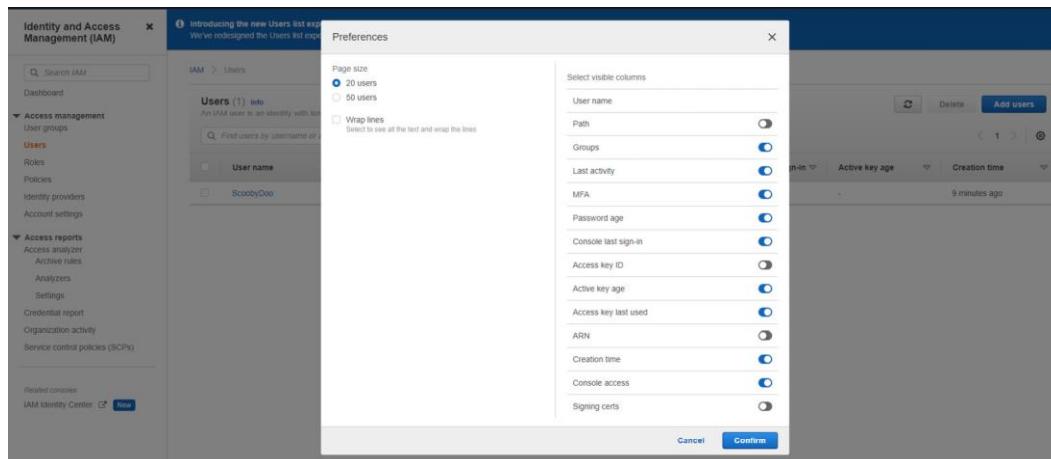


Figure 8.12 – AWS EC2 Users report column selection

The screenshot shows the Microsoft Azure Roles and administrators blade. At the top, there's a breadcrumb navigation: Home > Default Directory | Roles and administrators >. Below it, the title is "Roles and administrators | All roles". Underneath the title, it says "Default Directory - Azure Active Directory". There are several buttons at the top right: "New custom role", "Delete custom role", and "Download assignments".

Figure 8.13 – The Microsoft Azure Roles and administrators blade

The screenshot shows the Microsoft Azure Roles and administrators bulk operation results page. The title is "Roles and administrators | Bulk operation results". It includes a search bar for "File name" and a "Add filters" button. Below is a table with columns: Activity, Type, and File name. The table contains three rows: "Access reviews" (role assignments export, file name: exportRoleAssignments_All_2022-9-11.csv), "Audit logs" (role assignments export, file name: exportRoleAssignments_All_2022-9-11.csv), and "Bulk operation results" (highlighted in grey).

Figure 8.14 – Microsoft Azure Roles and administrators bulk operation reports

roleDisplayName	isBuiltIn	principalName	userPrincipalName	displayName	objectType
Application Administrator	TRUE	d965573e-scoobydo@shinesaca	Scooby Do user		Dc user
Conditional Access Administrator	TRUE	a0b2c84e-avenger@shinesaca	Captain America		Ai user
Directory Readers	TRUE	9ae2fe0d-00000014-0000-0000	Microsoft.servicePrincipal		
Global Administrator	TRUE	8aa2ca2b-shinesacambric_out	Shinesaca		C user
Global Administrator	TRUE	811ec4a9-WaldoJ@shinesacar	Waldo J		Jer user
Groups Administrator	TRUE	a0b2c84e-avenger@shinesaca	Captain America		Ai user

Figure 8.15 – The AWS EC2 Users report column selection

The screenshot shows the AWS IAM Users report column selection interface. On the left, there's a sidebar with "Identity and Access Management (IAM)" and a "Users" section. The main area is titled "Users (1) Info" and shows a table with columns: User name, Groups, Last activity, MFA, Password active, Console last sign-in, Active key age, and Access key last used. A single user named "ScoobyDoo" is listed.

Figure 8.16 – The AWS IAM Users report column selection

C	D	E	F	G	H
user_creation_time	password_enabled	password_last_used	password_last_changed	password_mfa_active	
2020-09-14T11:17:53+00:00	not_supported	2022-09-11T22:03:35+00:00	not_supported	not_supported	TRUE

Figure 8.17 – The AWS IAM Users report column selection

The screenshot shows the Microsoft Azure Devices Overview page. On the left, there's a navigation sidebar with links like Home, Default Directory, Devices, Overview, All devices, Device settings, BitLocker keys (Preview), Diagnose and solve problems, Audit logs, Bulk operation results (Preview), Troubleshooting + Support, and New support request. The main area has a search bar labeled 'Search by name, device ID, or object ID'. Below it, there are three cards under the 'Alerts' section:

- Stale devices:** 0 devices stale for 6+ months. See all stale devices.
- Noncompliant devices:** 0 devices. This number may not reflect all recent changes. See all noncompliant devices.
- Unmanaged devices:** 0 devices. This number may not reflect all recent changes. See all unmanaged devices.

Figure 8.18 – Microsoft Azure Devices | Overview

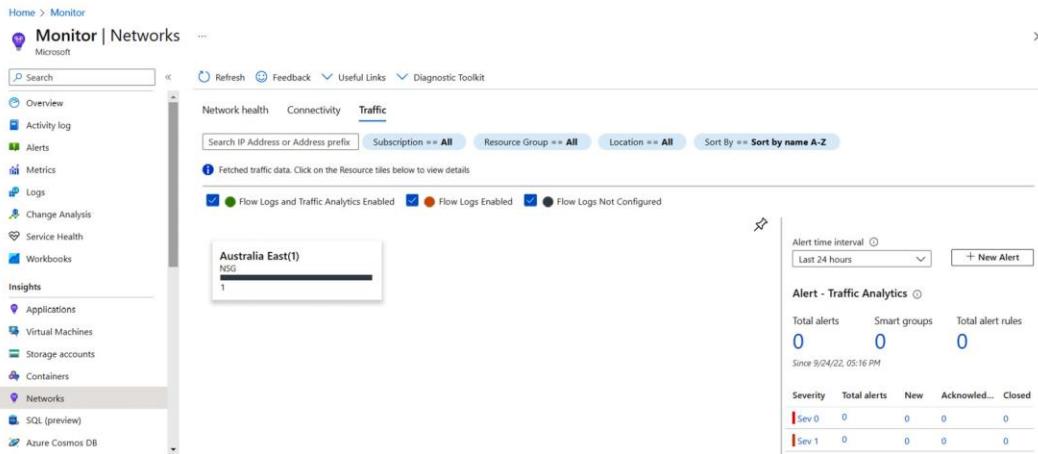
The screenshot shows the Microsoft Azure Device settings page. The left sidebar includes links for Home, Default Directory, Devices, Overview, All devices, Device settings (which is selected), BitLocker keys (Preview), Diagnose and solve problems, Activity (Audit logs, Bulk operation results (Preview)), Troubleshooting + Support, and New support request. The main content area has several configuration sections:

- Users may join devices to Azure AD:** Buttons for All, Selected, and None. The 'Selected' button is highlighted.
- Users may register their devices with Azure AD:** Buttons for All and None.
- Require Multi-Factor Authentication to register or join devices with Azure AD:** Buttons for Yes and No. A warning message states: "⚠ We recommend that you require Multi-Factor Authentication to register or join devices with Azure AD using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access."
- Maximum number of devices per user:** A dropdown menu set to 50.

Figure 8.19 – Microsoft Azure Device settings

Chapter 9

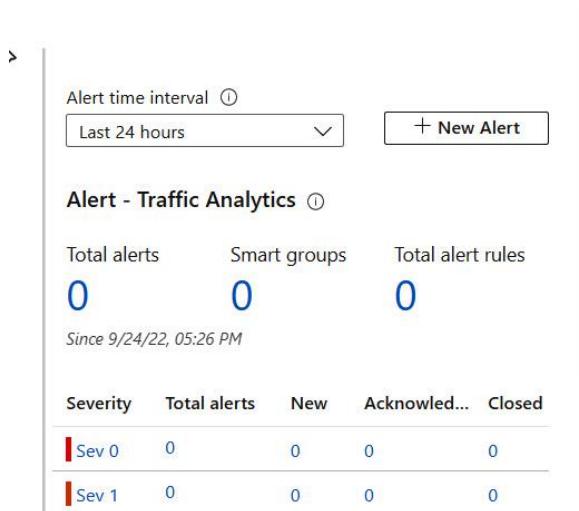
Figures



The screenshot shows the Microsoft Azure Monitor interface for Networks. The left sidebar includes links for Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service Health, Workbooks, Insights (Applications, Virtual Machines, Storage accounts, Containers, Networks), SQL (preview), and Azure Cosmos DB. The main area is titled 'Monitor | Networks' and has tabs for Network health, Connectivity, and Traffic. The Traffic tab is selected, showing a search bar for 'Search IP Address or Address prefix' and filters for Subscription (All), Resource Group (All), Location (All), and Sort By (Sort by name A-Z). Below this, it says 'Fetched traffic data. Click on the Resource tiles below to view details.' There is a checkbox for 'Flow Logs and Traffic Analytics Enabled'. On the right, there's a section for 'Alert - Traffic Analytics' with an alert time interval set to 'Last 24 hours' and a '+ New Alert' button. It displays 'Total alerts: 0', 'Smart groups: 0', and 'Total alert rules: 0'. A timestamp 'Since 9/24/22, 05:16 PM' is shown. Below this is a severity table:

Severity	Total alerts	New	Acknowledged...	Closed
Sev 0	0	0	0	0
Sev 1	0	0	0	0

Figure 9.1 – Microsoft Azure network traffic logging



This screenshot shows the 'Alerts' section of the Microsoft Azure Monitor Networks Traffic page. It features an 'Alert time interval' dropdown set to 'Last 24 hours' and a '+ New Alert' button. Below this is a summary for 'Alert - Traffic Analytics': 'Total alerts: 0', 'Smart groups: 0', and 'Total alert rules: 0'. A timestamp 'Since 9/24/22, 05:26 PM' is displayed. At the bottom is a severity table:

Severity	Total alerts	New	Acknowledged...	Closed
Sev 0	0	0	0	0
Sev 1	0	0	0	0

Figure 9.2 – Microsoft Azure network traffic alerts

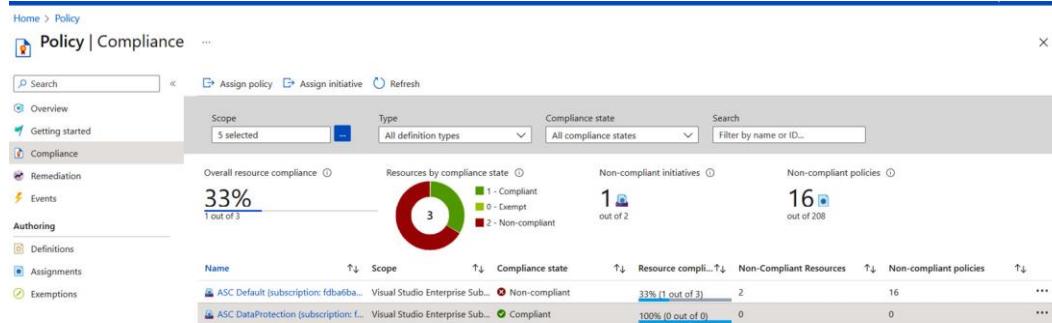


Figure 9.3 – Microsoft Azure compliance policies

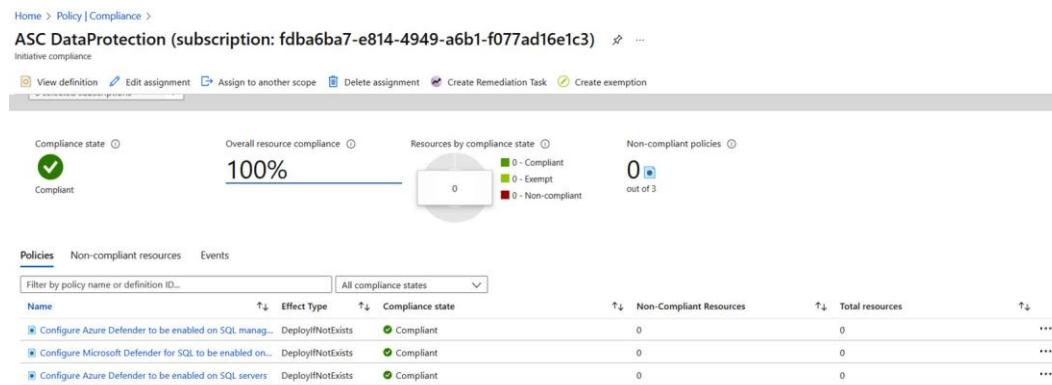


Figure 9.4 – Microsoft Azure compliance, no policies applied

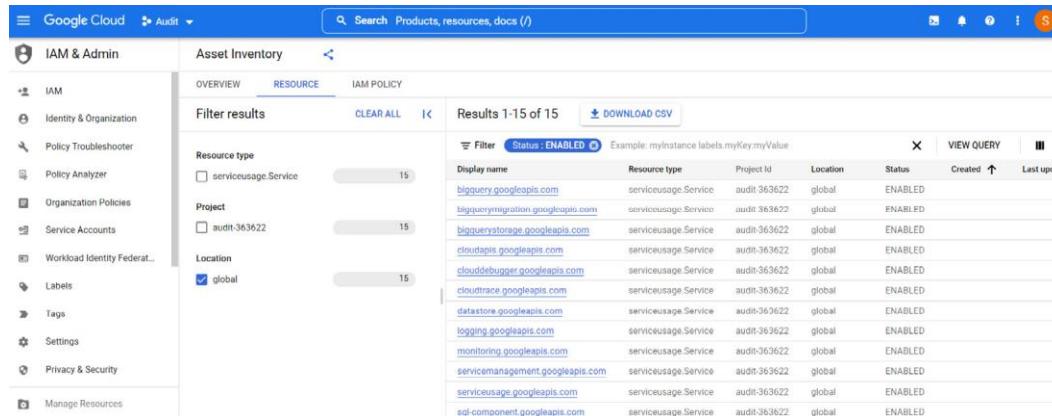


Figure 9.5 – GCP Asset Inventory

L	M	N	O	P
Location	Labels	Network tags	Additional attributes	
global				

Figure 9.6 – GCP Asset Inventory labels and network tags

The screenshot shows the AWS Security Hub Findings page. A specific finding is selected, detailing a low-severity issue related to CloudTrail logs and CloudWatch Metrics. The finding includes a description, workflow status (New), record state (Active), and various metadata fields like AWS account ID, compliance status (Failed), and product name (Security Hub). The right side of the interface displays sections for types and resources, with a dropdown menu showing 'AWS::Account::134972163851'.

Figure 9.7 – AWS EC2 data security findings

Default encryption

Automatically encrypt new objects stored in this bucket. Learn more [\[?\]](#)

Default encryption
Disabled

Intelligent-Tiering Archive configurations (0)

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. Learn more [\[?\]](#)

[View details](#) [Edit](#) [Delete](#) [Create configuration](#)

Find Intelligent-Tiering Archive configurations

Name	Status	Scope	Days until transition to Archive Access tier	Days until transition to Deep Archive Access tier
No archive configurations				
No configurations to display.				
Create configuration				

Server access logging

Log requests for access to your bucket. Learn more [\[?\]](#)

Server access logging
Disabled

AWS CloudTrail data events

Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. Learn more [\[?\]](#)

[Configure in CloudTrail](#) [\[?\]](#)

Figure 9.8 – AWS S3 bucket properties

Home > All resources >

tsecstorage Storage account

Tags (edit) Security Data Storage Criticality: Low

Properties Monitoring Capabilities (7) Recommendations (2) Tutorials Developer Tools

Blob service

Hierarchical namespace	Disabled
Default access tier	Hot
Blob public access	Enabled
Blob soft delete	Enabled (7 days)
Container soft delete	Disabled
Versioning	Enabled
Change feed	Enabled
NFS v3	Disabled
Allow cross-tenant replication	Enabled

File service

Large file share	Disabled
Active Directory	Not configured
Soft delete	Enabled (7 days)
Share capacity	5 TiB

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	Selected networks
Number of private endpoint connections	0
Network routing	Microsoft network routing
Access for trusted Microsoft services	Yes
Endpoint type	Standard

Figure 9.9 – Microsoft Azure Storage account overview

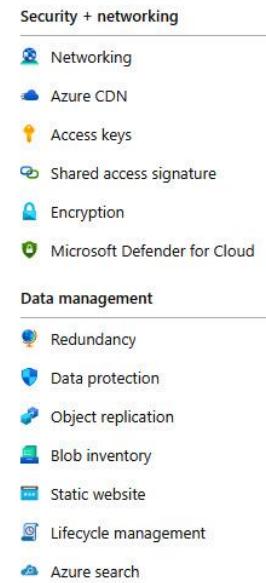


Figure 9.10 – Azure data security

This screenshot shows the 'Encryption scopes' blade in the Azure portal. It has tabs for 'Encryption' (selected) and 'Encryption scopes'. Buttons for '+ Add', 'Refresh', 'Enable', and 'Disable' are available. A checkbox 'Only show enabled scopes' is checked. The table lists 0 scopes. Headers for the table are: Name, Status, Encryption type, Key, and Automated key rotation. A note says 'No results.'

Figure 9.11 – Azure encryption settings and scopes

Chapter 10

Figures

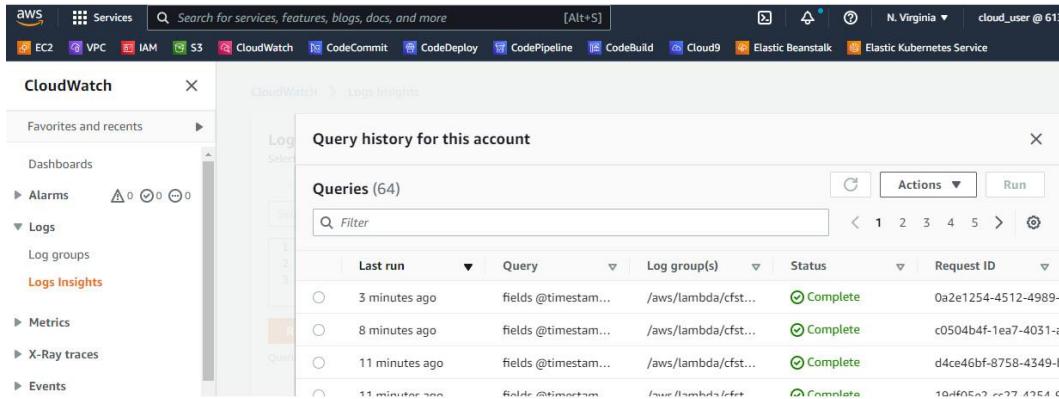


Figure 10.1 – Amazon CloudWatch Logs | Logs Insights

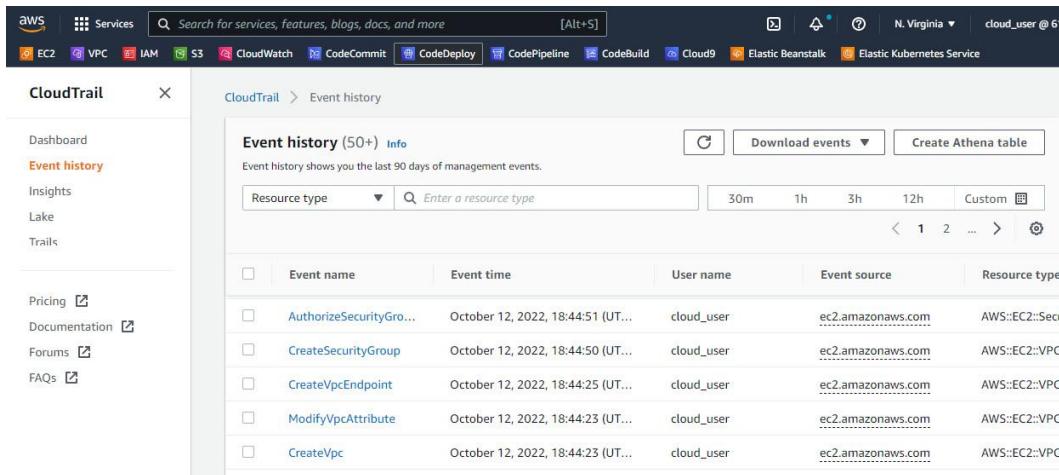


Figure 10.2 – AWS CloudWatch Logs | Event history

The screenshot shows the Microsoft Azure Monitor Activity log page. The left sidebar includes links for Overview, Activity log (which is selected), Alerts, Metrics, Logs, Change Analysis, Service Health, and Workbooks. The main area displays a table of recent events with columns for Operation name, Status, Time, Time stamp, Subscription, and Event initiated by. The table shows several successful operations like 'Create or Update Virtual Machine' and 'Validate Deployment' from the 'P1-Real Hands-On Labs' subscription.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
> Create or Update Virtual Machine	Succeeded	5 minutes ago	Wed Oct 12...	P1-Real Hands-On Labs	cloud_user_p_58a8eb19@...
> Validate Deployment	Started	5 minutes ago	Wed Oct 12...	P1-Real Hands-On Labs	cloud_user_p_58a8eb19@...
> Create or Update Virtual Machine	Accepted	6 minutes ago	Wed Oct 12...	P1-Real Hands-On Labs	cloud_user_p_58a8eb19@...
> Validate Deployment	Succeeded	6 minutes ago	Wed Oct 12...	P1-Real Hands-On Labs	cloud_user_p_58a8eb19@...
> Validate Deployment	Succeeded	6 minutes ago	Wed Oct 12...	P1-Real Hands-On Labs	cloud_user_p_58a8eb19@...
> Validate Deployment	Succeeded	8 minutes ago	Wed Oct 12...	P1-Real Hands-On Labs	cloud_user_p_58a8eb19@...

Figure 10.3 – Azure Monitor | Activity log

The screenshot shows the Microsoft Azure Monitor Change Analysis page. The left sidebar includes links for Overview, Activity log, Alerts, Metrics, Logs, Change Analysis (which is selected), Service Health, and Workbooks. The main area displays a table of recent changes with columns for Changes, Name, Old Value, and New Value. The table shows changes for a virtual machine named 'packttest2', including its provisioning state being set to 'Succeeded' and its network interfaces being updated to 'ubuntu'.

Changes	Name	Old Value	New Value
10/12/2022, 7:12:36 PM CDT (1)	properties.provisioningState	Creating	Succeeded
10/12/2022, 7:12:26 PM CDT (3)	properties.extended.instanceView.osVer...	packttest	<None>
	properties.extended.instanceView.osNa...	packttest	ubuntu
	properties.extended.instanceView.comp...	packttest	packttest
10/12/2022, 7:12:22 PM CDT (1)	properties.networkInterfaces	packttest-nsg	<None>
			View multi-line value
10/12/2022, 7:12:10 PM CDT (2)			

Figure 10.4 – Azure Monitor | Change Analysis

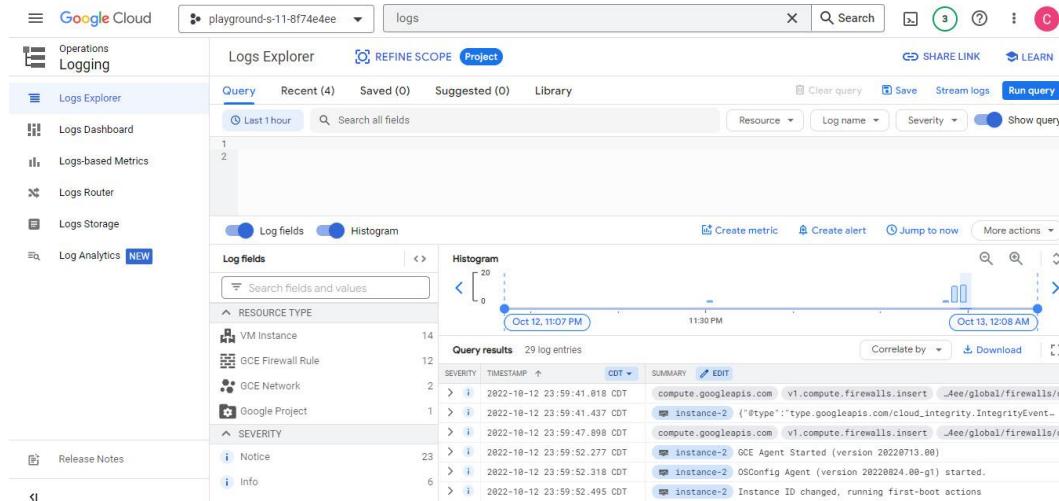


Figure 10.5 – GCP Logs Explorer

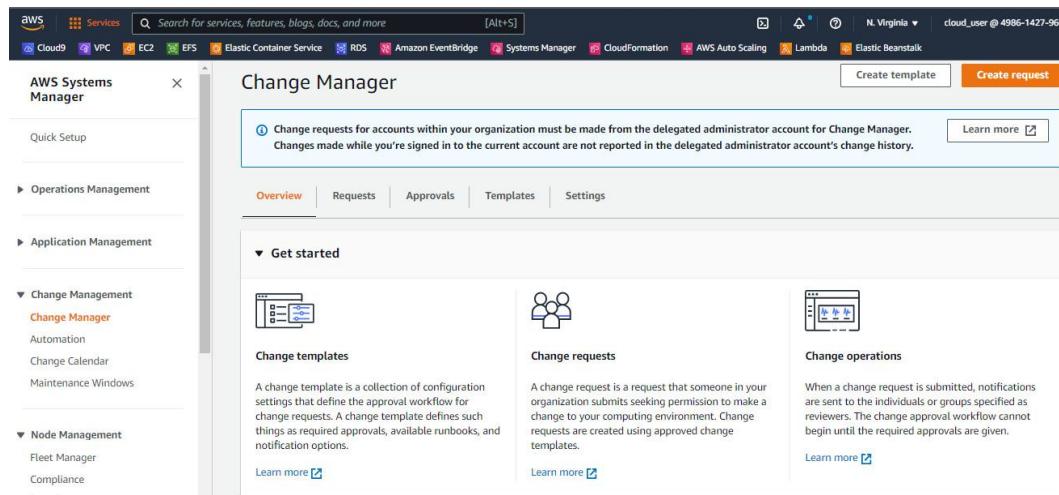


Figure 10.6 – AWS Systems Manager | Change Manager

Change request approvals

Specify up to five levels of approvers for change requests created from this change template. Each level can include one or more groups, individual users, or IAM roles. All approvals from one level must be received before next-level approvers are notified.

First-level approvals

Approver	Type	Required
Approver	-	1
1 approver to be specified at the request.		
Add approver		
Selected SNS topics		
None		
Amazon SNS topic for approval notifications - <i>optional</i>		
Specify the Amazon SNS topic to notify approvers at this level. Make sure the approvers are subscribed to the topic.		
<input type="radio"/> Enter an AWS Lambda function ARN <input checked="" type="radio"/> Create an Amazon SNS topic		

Figure 10.7 – Change Manager | Change request approvals

The screenshot shows the AWS Change Manager interface. The left sidebar has sections for Application Management (Application Manager, AppConfig, Parameter Store), Change Management (Change Manager, Automation, Change Calendar, Maintenance Windows), and Node Management. The main area is titled "Change Manager" and shows four summary boxes: "My pending requests" (0), "My rejected requests" (0), "My approved requests" (0), and "My closed requests" (0). Below these is a section for "Change requests (0)" with a "View details" button and a date range selector from "Create date range" to "1h 4h 1d 4d 1w 4w < 1 ... >".

Figure 10.8 – Change Manager | Requests

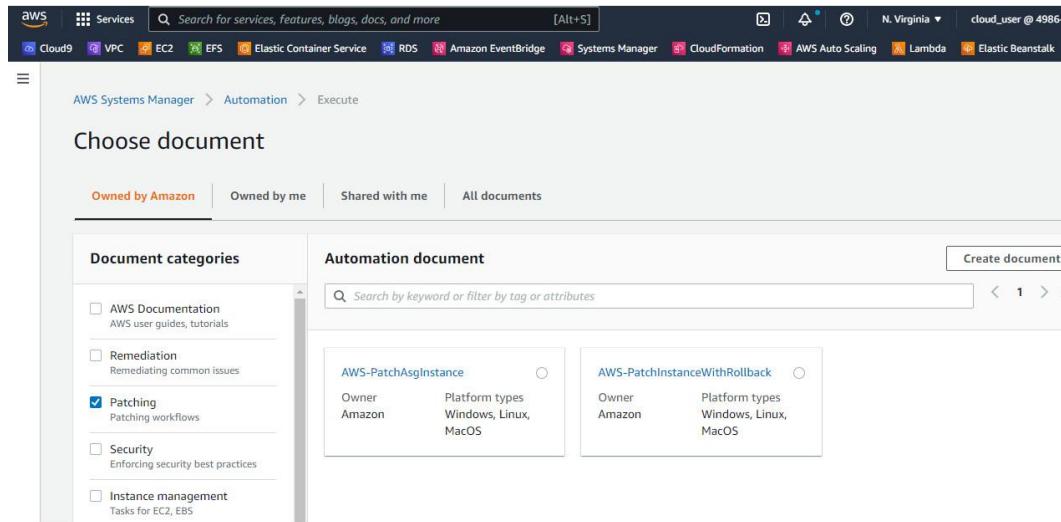


Figure 10.9 – AWS Systems Manager | Automation

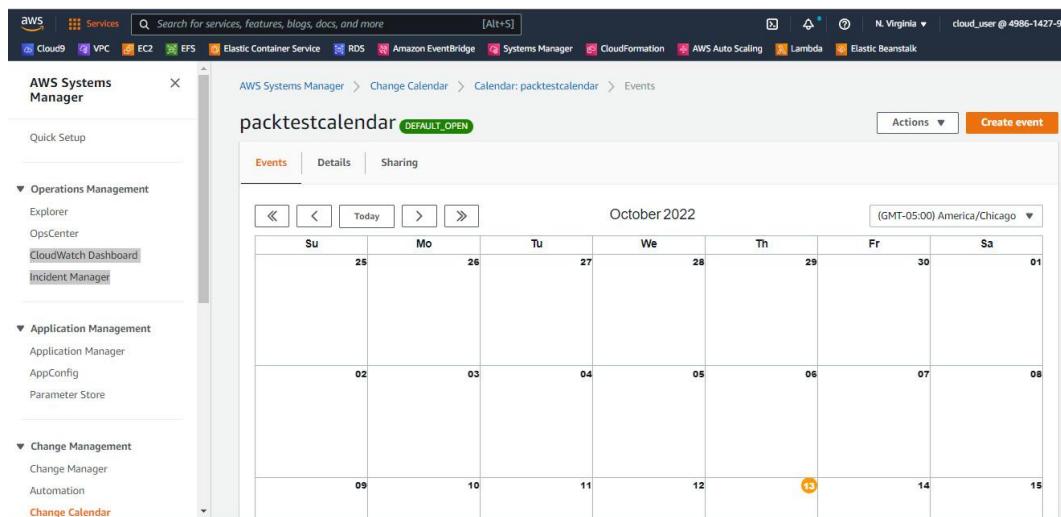


Figure 10.10 – AWS Systems Manager | Change Calendar

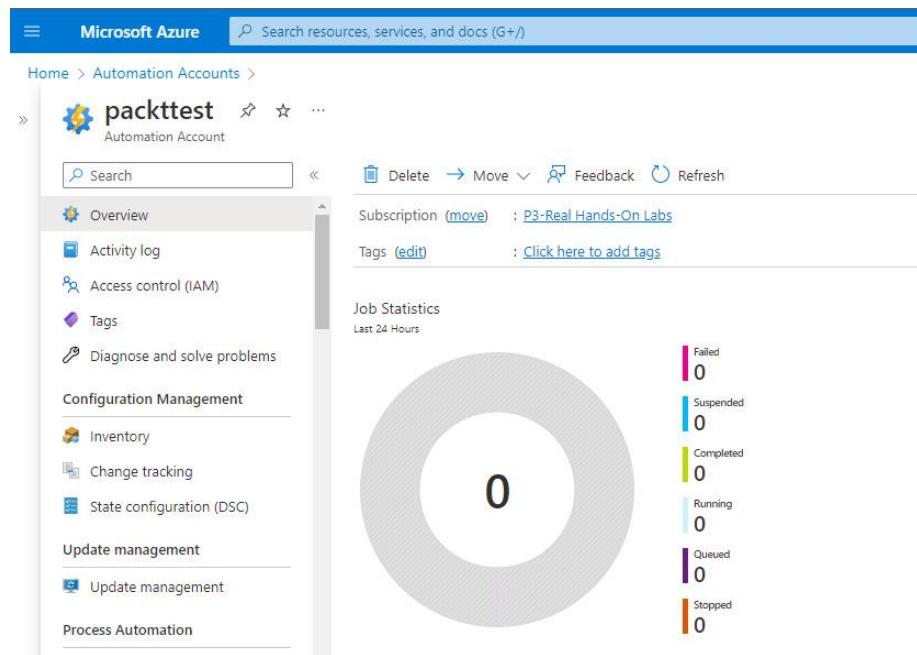


Figure 10.11 – Azure Automation Configuration Management | Change tracking

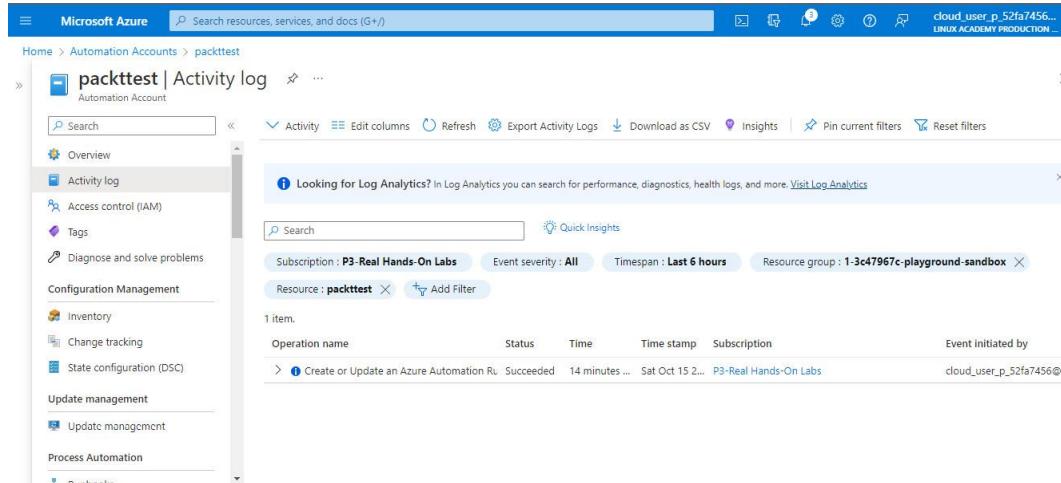


Figure 10.12 – Azure Automation | Activity log

```

# Generating Access Key and Secret Key
provider "aws" {
  region      = "us-east-1"
  access_key  = "AKIAWWE6G4DQY7JAARQE"
  secret_key  = "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"
}

terraform {
  required_providers {
    aws = {
      source = "hashicorp/aws"
    }
  }
}

resource "aws_instance" "i-0e117de41c0ee94bd" {
  ami          = var.ami
  instance_type = var.instance_type

```

Figure 10.13 – Terraform configuration

```

PS C:\users\antagonist\documents\aws> terraform init

Initializing the backend...

Initializing provider plugins...
- Finding latest version of hashicorp/aws...
- Installing hashicorp/aws v4.35.0...
- Installed hashicorp/aws v4.35.0 (signed by HashiCorp)

Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
PS C:\users\antagonist\documents\aws>

```

Figure 10.14 – The terraform init command

```

if you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
PS C:\users\antagonist\documents\aws> terraform plan

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:
+ create

Terraform will perform the following actions:

# aws_instance.i-0e117de41c0ee94bd will be created
+ resource "aws_instance" "i-0e117de41c0ee94bd" {
    ami                                = "ami-026b57f3c383c2eec"
    arn                                = (known after apply)
    associate_public_ip_address        = (known after apply)
    availability_zone                  = (known after apply)
    cpu_core_count                     = (known after apply)
    cpu_threads_per_core              = (known after apply)
    disable_api_stop                  = (known after apply)
    disable_api_termination           = (known after apply)
    ebs_optimized                      = (known after apply)
    get_password_data                 = false
    host_id                            = (known after apply)
    host_resource_group_arn            = (known after apply)
    id                                 = (known after apply)
    instance_initiated_shutdown_behavior = (known after apply)
    instance_state                     = (known after apply)
    instance_type                      = "t2.micro"
    ipv6_address_count                = (known after apply)
    ipv6_addresses                     = (known after apply)
    key_name                           = (known after apply)
    monitoring                         = (known after apply)
    outpost_arn                        = (known after apply)
    password_data                      = (known after apply)
    placement_group                   = (known after apply)
    placement_partition_number         = (known after apply)
    primary_network_interface_id      = (known after apply)
    private_dns                         = (known after apply)
    private_ip                          = (known after apply)
    public_dns                          = (known after apply)
    public_ip                           = (known after apply)
    secondary_private_ips              = (known after apply)
    security_groups                    = (known after apply)
    subnet_id                           = (known after apply)
    tags_all                            = (known after apply)
    tenancy                             = (known after apply)
    user_data                           = (known after apply)
    user_data_base64                   = (known after apply)
    user_data_replace_on_change        = false
}

```

Figure 10.15 – The terraform plan command

```

PS C:\users\antagonist\documents\aws> terraform apply --auto-approve

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:
+ create

Terraform will perform the following actions:

# aws_instance.i-0e117de41c0ee94bd will be created
+ resource "aws_instance" "i-0e117de41c0ee94bd" {
    ami                                = "ami-026b57f3c383c2eec"
    arn                                = (known after apply)
    associate_public_ip_address        = (known after apply)
    availability_zone                  = (known after apply)
    cpu_core_count                     = (known after apply)
    cpu_threads_per_core              = (known after apply)
    disable_api_stop                  = (known after apply)
    disable_api_termination           = (known after apply)
    ebs_optimized                      = (known after apply)
    get_password_data                 = false
    host_id                            = (known after apply)
    host_resource_group_arn            = (known after apply)
    id                                 = (known after apply)
    instance_initiated_shutdown_behavior = (known after apply)
    instance_state                     = (known after apply)
    instance_type                      = "t2.micro"
    ipv6_address_count                = (known after apply)
    ipv6_addresses                     = (known after apply)
    key_name                           = (known after apply)
    monitoring                         = (known after apply)
    outpost_arn                        = (known after apply)
    password_data                      = (known after apply)
    placement_group                   = (known after apply)
    placement_partition_number         = (known after apply)
    primary_network_interface_id      = (known after apply)
    private_dns                         = (known after apply)
    private_ip                          = (known after apply)
    public_dns                          = (known after apply)
    public_ip                           = (known after apply)
    secondary_private_ips              = (known after apply)
    security_groups                    = (known after apply)
    subnet_id                           = (known after apply)
    tags_all                            = (known after apply)
    tenancy                             = (known after apply)
    user_data                           = (known after apply)
    user_data_base64                   = (known after apply)
}

```

Figure 10.16 – The terraform apply command

```

PS C:\users\antagonist\documents\aws> terraform login
Terraform will request an API token for app.terraform.io using your browser.

If login is successful, Terraform will store the token in plain text in
the following file for use by subsequent commands:
  C:\Users\antagonist\AppData\Roaming\terraform.d\credentials.tfrc.json

Do you want to proceed?
  Only 'yes' will be accepted to confirm.

  Enter a value: yes

-----
Terraform must now open a web browser to the tokens page for app.terraform.io.

If a browser does not open this automatically, open the following URL to proceed:
  https://app.terraform.io/app/settings/tokens?source=terraform-login

-----
Generate a token using your browser, and copy-paste it into this prompt.

Terraform will store the token in plain text in the following file
for use by subsequent commands:
  C:\Users\antagonist\AppData\Roaming\terraform.d\credentials.tfrc.json

Token for app.terraform.io:
  Enter a value:

```

Figure 10.17 – Terraform Enterprise login with API token

```

Administrator: Windows PowerShell
PS C:\users\antagonist\documents\aws> terraform graph
graph TD
    compound = "true"
    newrank = "true"
    subgraph "root" {
        "[root] aws_instance.i-0e117de41c0ee94bd (expand)" [label = "aws_instance.i-0e117de41c0ee94bd", shape = "box"]
        "[root] provider[\"registry.terraform.io/hashicorp/aws\"]" [label = "provider[\"registry.terraform.io/hashicorp/aws\"], shape = \"diamond\"]"
        "[root] var.ami" [label = "var.ami", shape = "note"]
        "[root] var.instance_type" [label = "var.instance_type", shape = "note"]
        "[root] aws_instance.i-0e117de41c0ee94bd (expand)" --> "[root] provider[\"registry.terraform.io/hashicorp/aws\"]"
        "[root] aws_instance.i-0e117de41c0ee94bd (expand)" --> "[root] var.ami"
        "[root] aws_instance.i-0e117de41c0ee94bd (expand)" --> "[root] var.instance_type"
        "[root] provider[\"registry.terraform.io/hashicorp/aws\"] (close)" --> "[root] aws_instance.i-0e117de41c0ee94bd (expand)"
        "[root] root" --> "[root] provider[\"registry.terraform.io/hashicorp/aws\"] (close)"
    }
}

PS C:\users\antagonist\documents\aws>

```

Figure 10.18 – The terraform graph command

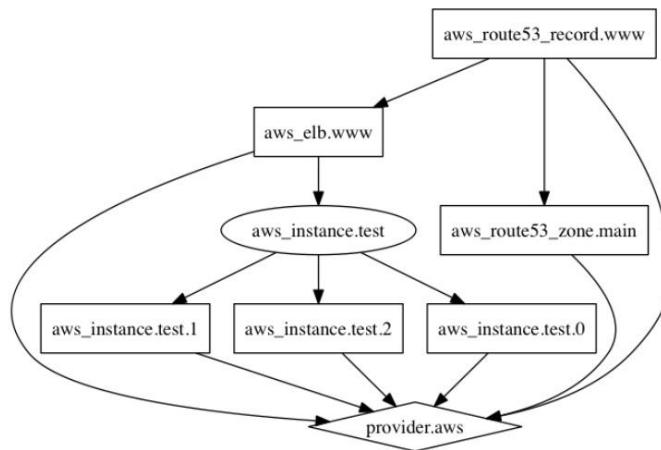


Figure 10.19 – Example of a Terraform graph output

```

c:\Users\antagonist\AppData\Local\Programs\Python\Python310\Scripts>pip3 install -user policy_sentry
Requirement already satisfied: policy_sentry in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (0.12.4)
Requirement already satisfied: schema in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from policy_sentry) (0.7.5)
Requirement already satisfied: click in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from policy_sentry) (8.1.3)
Requirement already satisfied: beautifulsoup in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from policy_sentry) (4.11.1)
Requirement already satisfied: PyYAML in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from policy_sentry) (6.0)
Requirement already satisfied: requests in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from policy_sentry) (2.28.1)
Requirement already satisfied: soupsieve<1.2 in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from beautifulsoup4->policy_sentry) (2.3
Requirement already satisfied: colorama in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from click->policy_sentry) (0.4.5)
Requirement already satisfied: idna<4,>=2.5 in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from requests->policy_sentry) (3.4)
Requirement already satisfied: certifi>=2017.4.17 in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from requests->policy_sentry) (2022
Requirement already satisfied: charset-normalizer<3,>=2 in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from requests->policy_sentry)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from requests->policy_sentry) (1
Requirement already satisfied: contextlib2>=0.5.5 in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from schema->policy_sentry) (21.6.0
)

[notice] A new release of pip available: 22.2.2 -> 22.3.3
[notice] To update, run: python.exe -m pip install --upgrade pip
c:\Users\antagonist\AppData\Local\Programs\Python\Python310\Scripts>

```

Figure 10.20 – Policy Sentry installation on the command line

```

Requirement already satisfied: contextlib2>=0.5.5 in c:\users\antagonist\appdata\local\programs\python\python310\lib\site-packages (from schema->policy_sentry)
[notice] A new release of pip available: 22.2.2 -> 22.3.1
[notice] To update, run: python.exe -m pip install --upgrade pip

c:\Users\antagonist\AppData\Local\Programs\Python\Python310\Scripts>
c:\Users\antagonist\AppData\Local\Programs\Python\Python310\Scripts>aws configure
AWS Access Key ID [*****FX6B]: AKIAVYDOBT6WPTGBZ6UG
AWS Secret Access Key [*****/mAA]: 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
Default region name [us-east-1]: us-east-1
Default output format [json]:

```

Figure 10.21 – Connecting to AWS through the CLI

Figure 10.22 – The policy_sentry query command, example one

```
c:\Users\antagonist\AppData\Local\Programs\Python\Python310\Scripts>policy_sentry query action-table --service ram --access-level permissions-management
all IAM actions under the ram service that have the access level permissions-management:
[
    "ram:AcceptResourceShareInvitation",
    "ram:AssociateResourceShare",
    "ram>CreateResourceShare",
    "ram>DeleteResourceShare",
    "ram:DisassociateResourceShare",
    "ram:EnableSharingWithAwsOrganization",
    "ram:RejectResourceShareInvitation",
    "ram:UpdateResourceShare"
]
c:\Users\antagonist\AppData\Local\Programs\Python\Python310\Scripts>
```

Figure 10.23 – The policy_sentry query command, example two

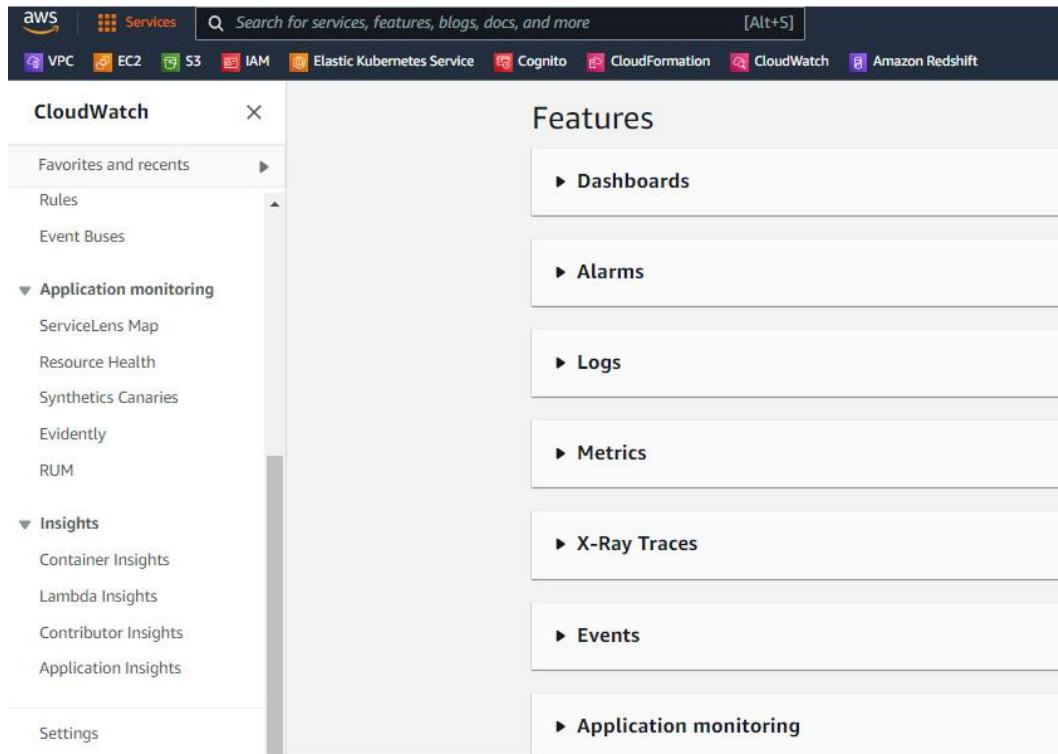


Figure 10.24 – Amazon CloudWatch

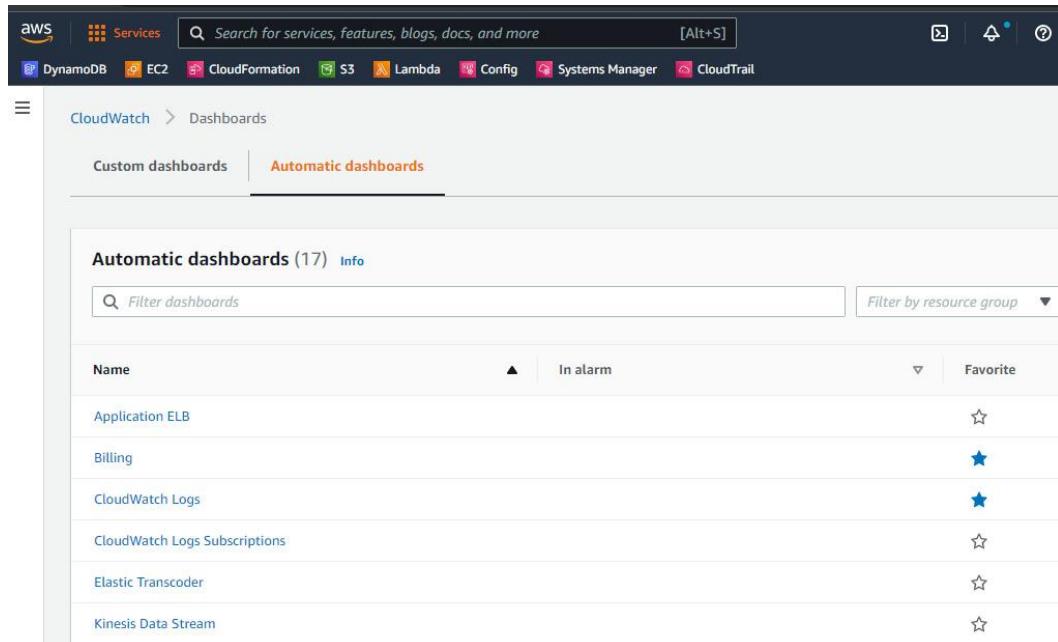


Figure 10.25 – CloudWatch | Dashboards

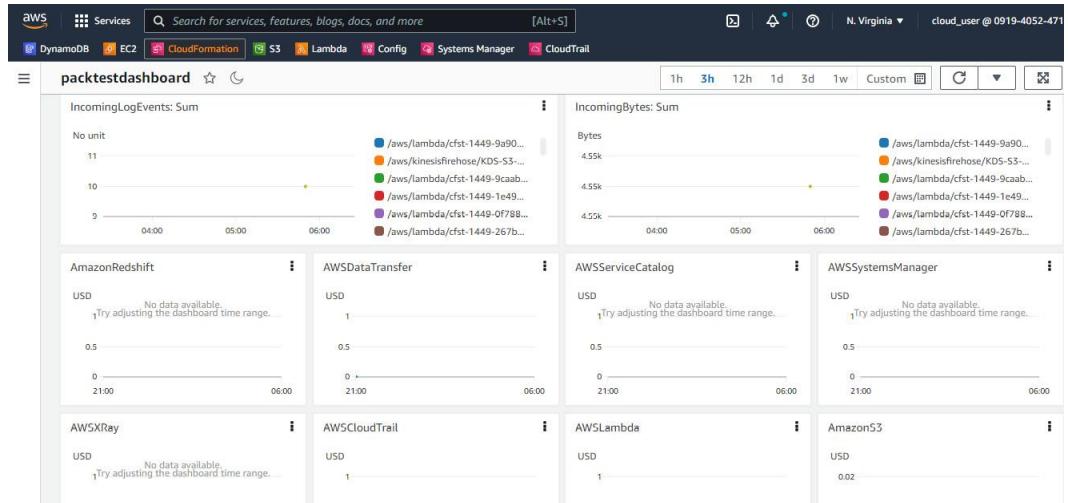


Figure 10.26 – CloudWatch | packtestdashboard

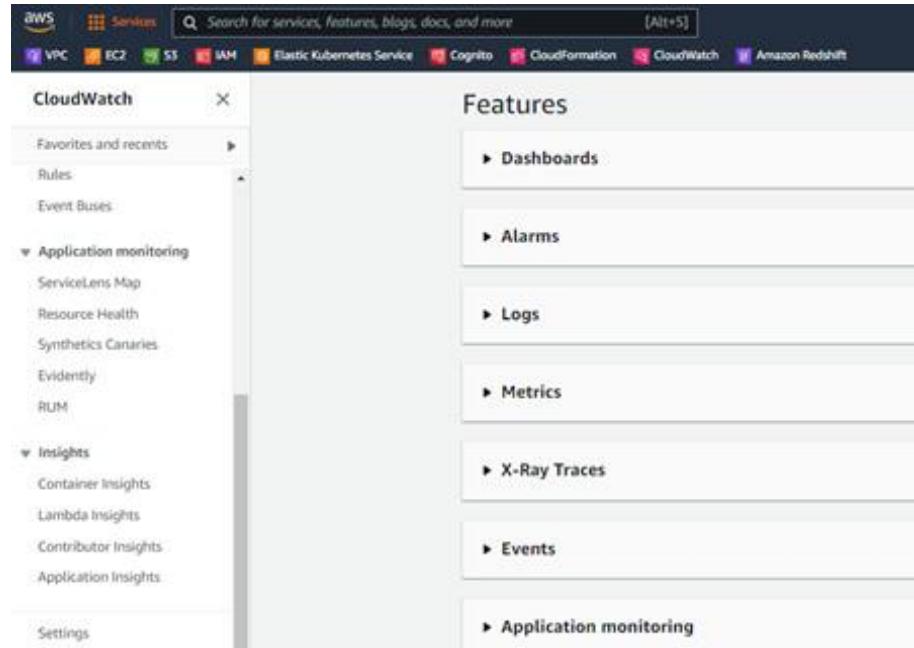


Figure 10.27 – CloudWatch | Alarms

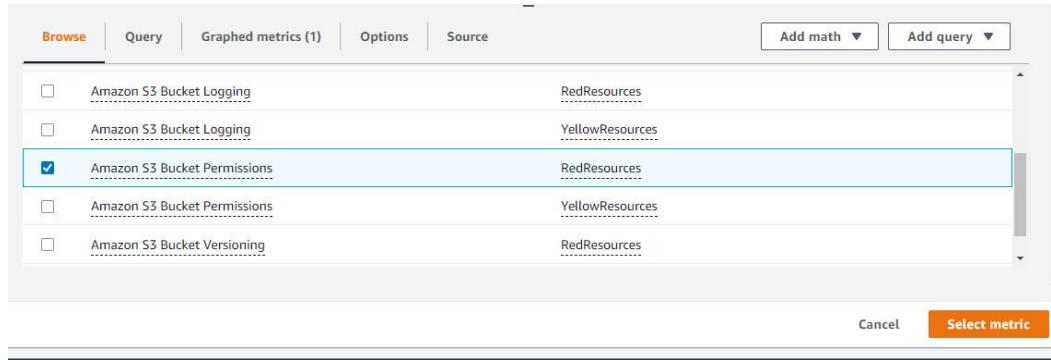


Figure 10.28 – Amazon S3 Bucket Permissions metric

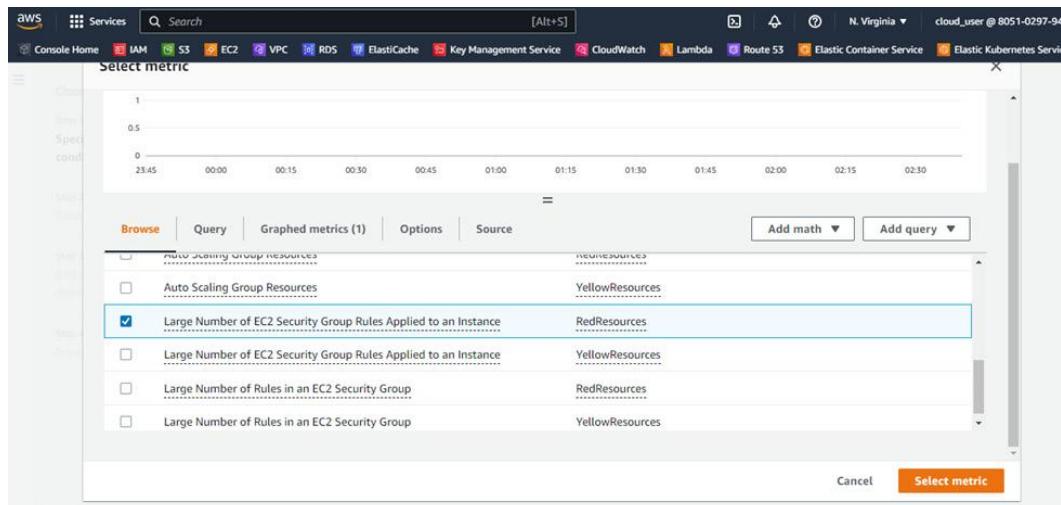


Figure 10.29 – The Large Number of EC2 Security Group Rules Applied to an Instance metric

The screenshot shows the Microsoft Azure Monitor Change Analysis feature. The left sidebar includes links for Overview, Activity log, Alerts, Metrics, Logs, Change Analysis (which is currently selected), Service Health, Workbooks, Insights, Applications, Virtual Machines, Storage accounts, and Containers. The main pane displays a table of recent changes:

Changes	Name	Old Value	New Value
10/12/2022, 7:12:36 PM CDT (0)	properties.provisioningState	packtest2	Creating
10/12/2022, 7:12:26 PM CDT (3)	properties.extended.instanceview.osName	packtest	+None+
10/12/2022, 7:12:26 PM CDT (3)	properties.extended.instanceview.osName	packtest	+None+
10/12/2022, 7:12:26 PM CDT (3)	properties.extended.instanceview.computerName	packtest	+None+
10/12/2022, 7:12:22 PM CDT (0)	properties.networkInterface	packtest-nsg	+None+
10/12/2022, 7:12:10 PM CDT (2)			View multi-line value

Figure 10.30 – Azure Monitor | Change Analysis

The screenshot shows the Azure Monitor | Alert rules page. At the top, there are buttons for 'Create', 'Columns', 'Refresh', 'Export to CSV', 'Open query', 'Delete', 'Enable', and 'Disable'. Below this is a search bar and filter buttons for 'Subscription : all', 'Target scope : all', 'Target resource type : all', 'Signal type : all', 'Severity : all', and 'Status : Enabled'. A dropdown menu shows 'No grouping'. The main table has columns: Name, Condition, Severity, Target scope, Target resource type, Signal type, and Status. One row is shown for 'packtest'.

Name	Condition	Severity	Target scope	Target resource type	Signal type	Status
packtest	Category=Administrative 4 - Verbose	1-C003A2B4-PLAYGROUND	Resource group	Activity log	Enabled	

Figure 10.31 – Azure Monitor | Alert rules

The screenshot shows the Azure Monitor | Alerts page. On the left is a navigation sidebar with 'Overview', 'Activity log', 'Alerts' (selected), 'Metrics', 'Logs', 'Change Analysis', 'Service Health', and 'Workbooks'. The main area shows a summary of alerts: Total alerts (6), Critical (0), Error (0), Warning (0), Informational (0), and Verbose (6). Below this is a table of fired alerts with columns: Name, Severity, Alert condition, User response, and Fire time. The table lists six entries for 'packtest'.

Name	Severity	Alert condition	User response	Fire time
packtest	4 - Verbose	Fired	New	10/12/2022, 7:21 PM
packtest	4 - Verbose	Fired	New	10/12/2022, 7:21 PM
packtest	4 - Verbose	Fired	New	10/12/2022, 7:21 PM
packtest	4 - Verbose	Fired	New	10/12/2022, 7:21 PM
packtest	4 - Verbose	Fired	New	10/12/2022, 7:20 PM
packtest	4 - Verbose	None	New	10/12/2022, 7:20 PM

Figure 10.32 – Azure Monitor | Alerts

The screenshot shows the Azure Monitor | Activity log page. On the left is a navigation sidebar with 'Overview', 'Activity log' (selected), 'Alerts', 'Metrics', 'Logs', 'Change Analysis', 'Service Health', and 'Workbooks'. The main area shows a table of activity logs with columns: Operation name, Status, Time, Time stamp, and Subscription. The table lists five items related to creating or updating a virtual machine, validating deployment, creating role assignment, and updating resource group.

Operation name	Status	Time	Time stamp	Subscription
Create or Update Virtual Machine	Succeeded	6 minutes ago	Tue Nov 29 ...	P1-Real Hands-On Labs
Create or Update SSH Public Key	Started	6 minutes ago	Tue Nov 29 ...	P1-Real Hands-On Labs
Validate Deployment	Succeeded	6 minutes ago	Tue Nov 29 ...	P1-Real Hands-On Labs
Create role assignment	Succeeded	24 minutes ago	Tue Nov 29 ...	P1-Real Hands-On Labs
Update resource group	Succeeded	24 minutes ago	Tue Nov 29 ...	P1-Real Hands-On Labs

Figure 10.33 – Azure Monitor | Activity log

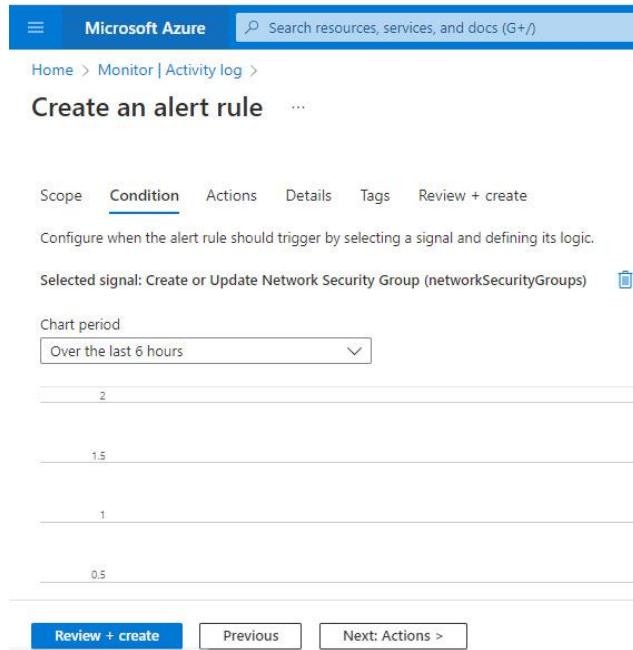


Figure 10.34 – Alert Rule: Create or Update Network Security Group

The screenshot shows the Google Cloud Monitoring interface. The left sidebar includes 'Monitoring', 'Metrics Scope' (1 project), 'Overview', 'Dashboards' (selected), 'Integrations', 'Services', 'Metrics explorer', 'Alerting', 'Uptime checks', 'Groups', 'Managed Prometheus', 'Permissions', and 'Settings'. The main area shows a 'DASHBOARDS LIST' tab selected over 'SAMPLE LIBRARY'. It features a table for 'All Dashboards' with columns for 'Categories', 'Name', and 'Type'. The table lists four dashboards: 'Disks' (Google Cloud Platform), 'Firewalls' (Google Cloud Platform), 'Infrastructure Summary' (Google Cloud Platform), and 'VM Instances' (Google Cloud Platform). There are also sections for 'Recently Viewed', 'Favorites', 'Custom', 'GCP', 'Integrations', and 'Other'.

Figure 10.35 – Google Cloud Monitoring

The screenshot shows the Google Cloud interface for monitoring. On the left, there's a sidebar with 'Monitoring' selected. The main area is titled 'FIREWALLS' with a search bar and time filters (1H, 6H, 1D, 1W). A table lists various firewall rules:

Name	Group ID	Rules	Instances
default-allow-http	3970130856637640315	1	2
default-allow-https	7955625692873633403	1	2
① default-allow-icmp	7827715502304968744	1	0
① default-allow-internal	9030649775064924200	3	0
① default-allow-rdp	4819851215157641250	1	0
① default-allow-ssh	3340866114244886568	1	0
① packttest-allow-custom	1522849948686888630	1	0
① packttest-allow-icmp	3039254922101272245	1	0
① packttest-allow-rdp	18990941629640224436	1	0
① packttest-allow-ssh	17368832278741515955	1	0
① packttest2-allow-custom	7521867277679210139	1	0
① packttest2-allow-icmp	6185150275501960857	1	0
① packttest2-allow-rdp	7689936052415639191	1	0
① packttest2-allow-ssh	56223319815630486	1	0

Figure 10.36 – Google Cloud Monitoring | Dashboards

A modal window titled 'Security Rules' is open over the firewall list. It shows a single rule: 'default-allow-ssh (3340866114244886568)'. Below it, another section titled 'Ingress Rules' shows a table:

Port	CIDR IP	Source Group
TCP 22	0.0.0.0/0	

Figure 10.37 – Security Rules

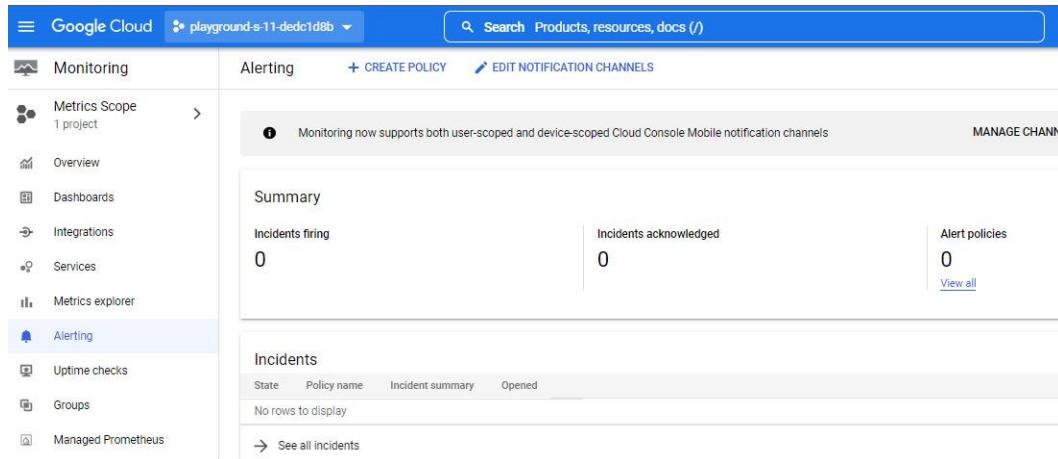


Figure 10.38 – Google Cloud Monitoring | Alerting

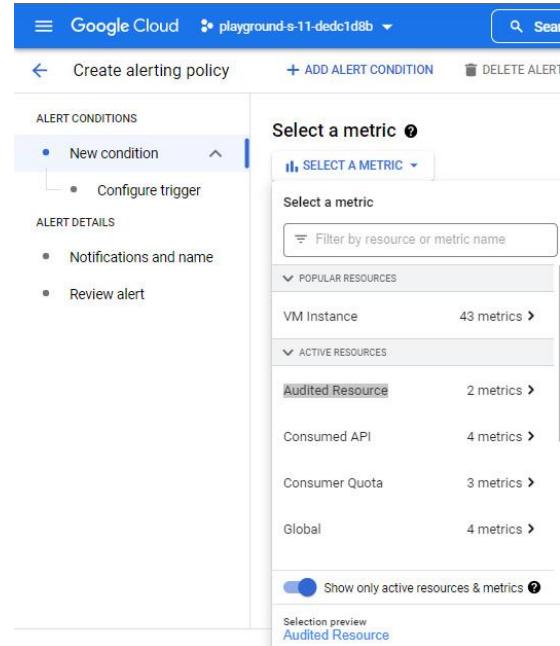


Figure 10.39 – Create alerting policy | Audited Resource metric

Commands

Command 10.1

Install Policy Sentry using the following command:

```
pip3 install --user policy_sentry
```

Command 10.2

Some commands an IT auditor can execute to query the AWS IAM database.

The first command is the following:

```
policy_sentry query action-table --service all --access-level  
permissions-management
```

This command gets a list of all IAM actions across **all** services that have **permissions-management** access, as seen in **Figure 10.22**:

Now let's use the second command:

```
policy_sentry query action-table --service ram --access-level  
permissions-management
```

This gets a list of all IAM actions under the RAM service that have the **permissions-management** access level, as seen in **Figure 10.23**:

Links

For detailed instructions on creating CloudWatch alarms, go to:

- <https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-get-started.html>.
- <https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html>.