packt

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/Kq3mr.

Chapter 1

Figures

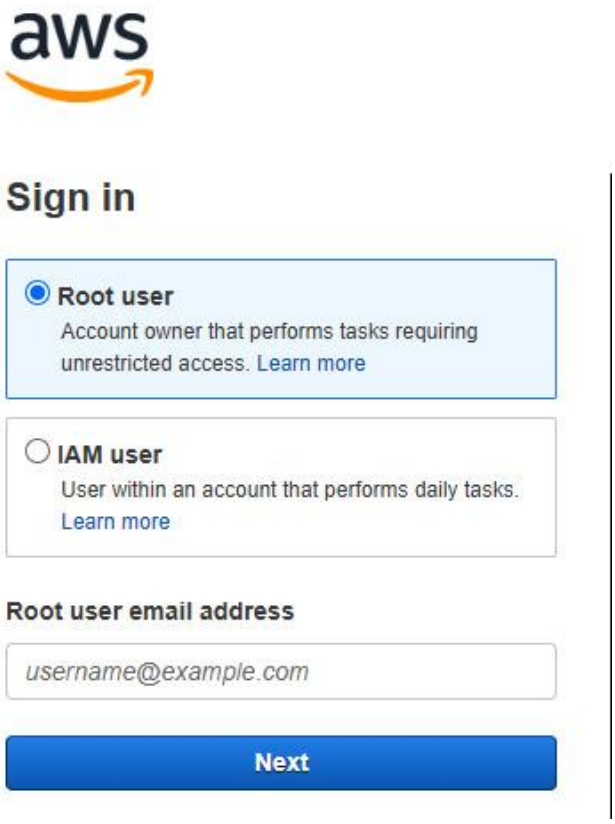

Figure 1.1 – AWS console initial sign-in

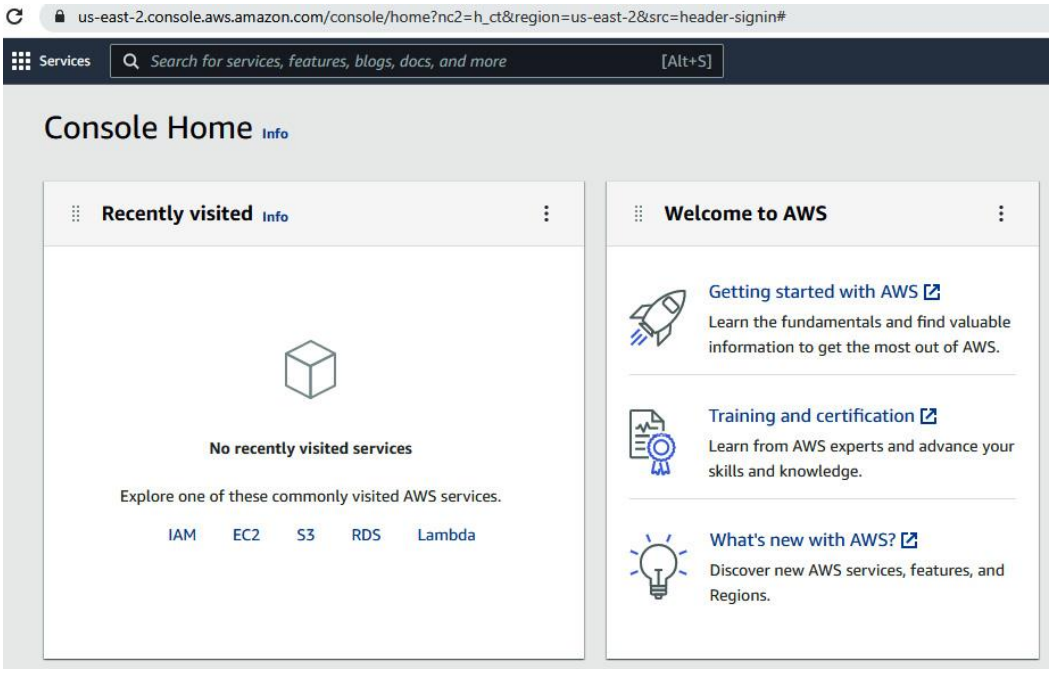

Figure 1.2 – AWS Console Home main page

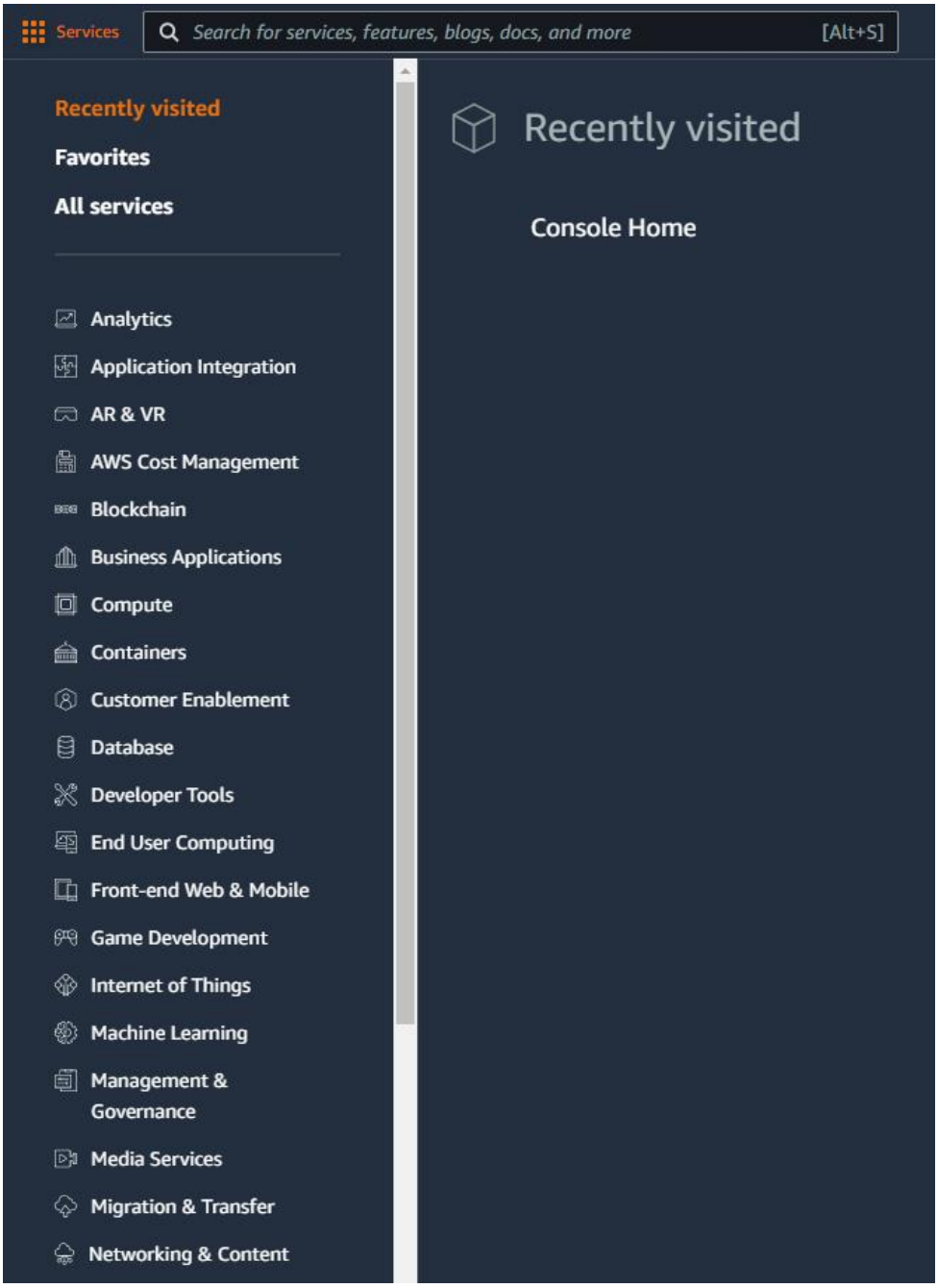

Figure 1.3 – AWS Console Home Services list

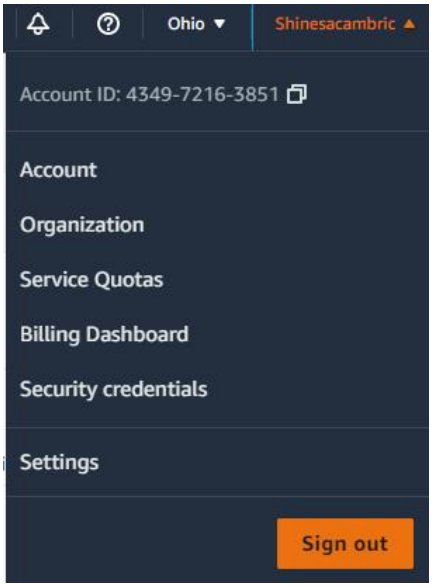

Figure 1.4 – AWS Console Home account sign-In details

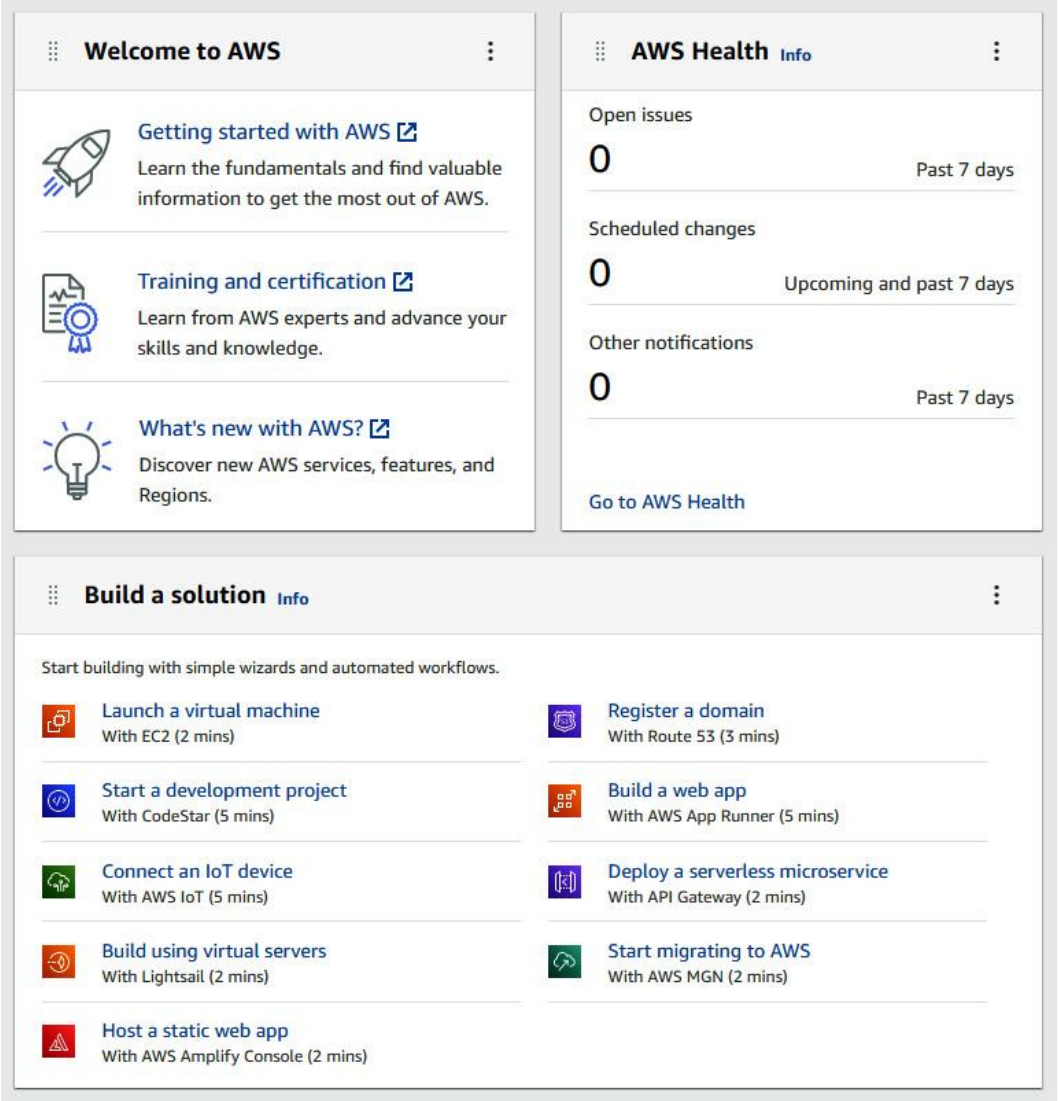

Figure 1.5 – AWS Console Home widgets

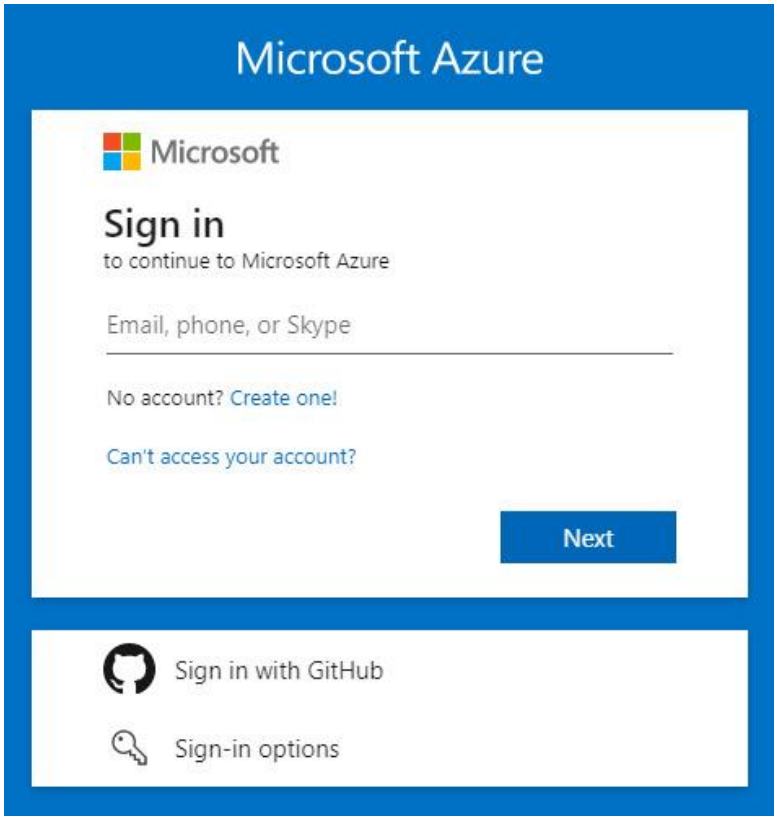

Figure 1.6 – Microsoft Azure initial sign-in

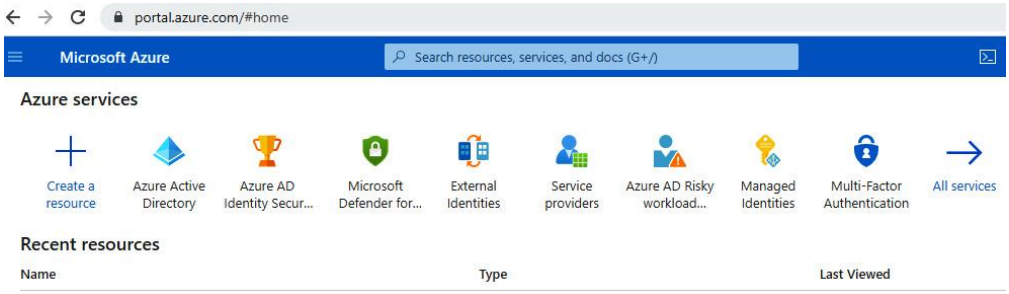

Figure 1.7 – Microsoft Azure portal home page

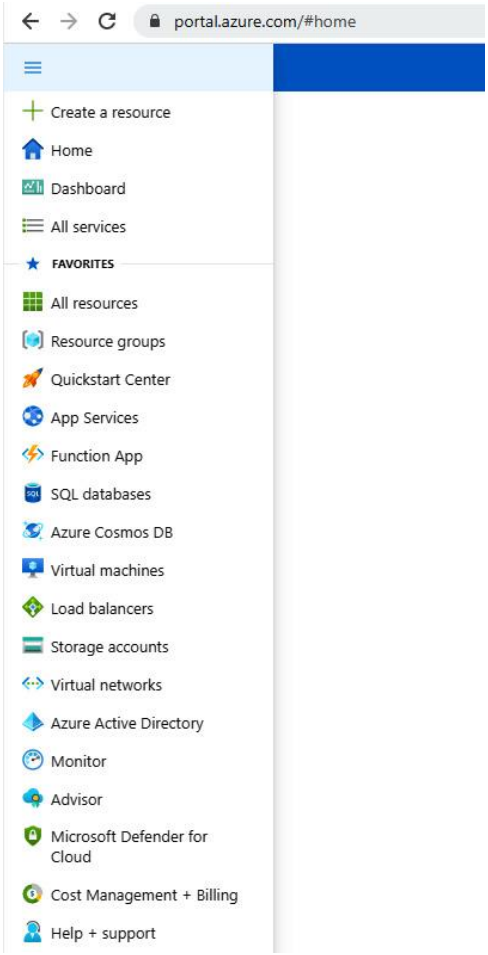

Figure 1.8 – Microsoft Azure portal home page navigation panel

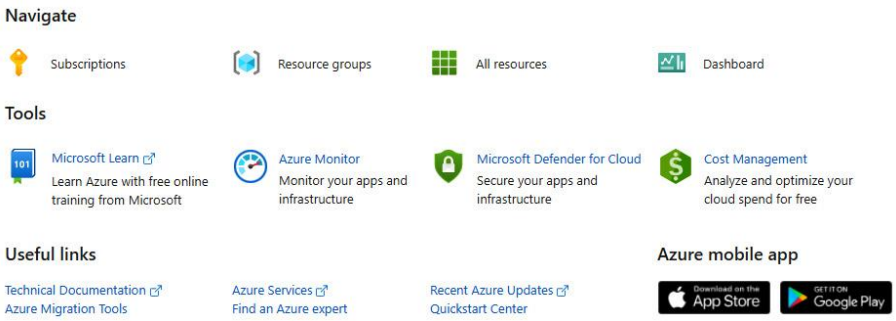

Figure 1.9 – Microsoft Azure portal dashboard Navigate section

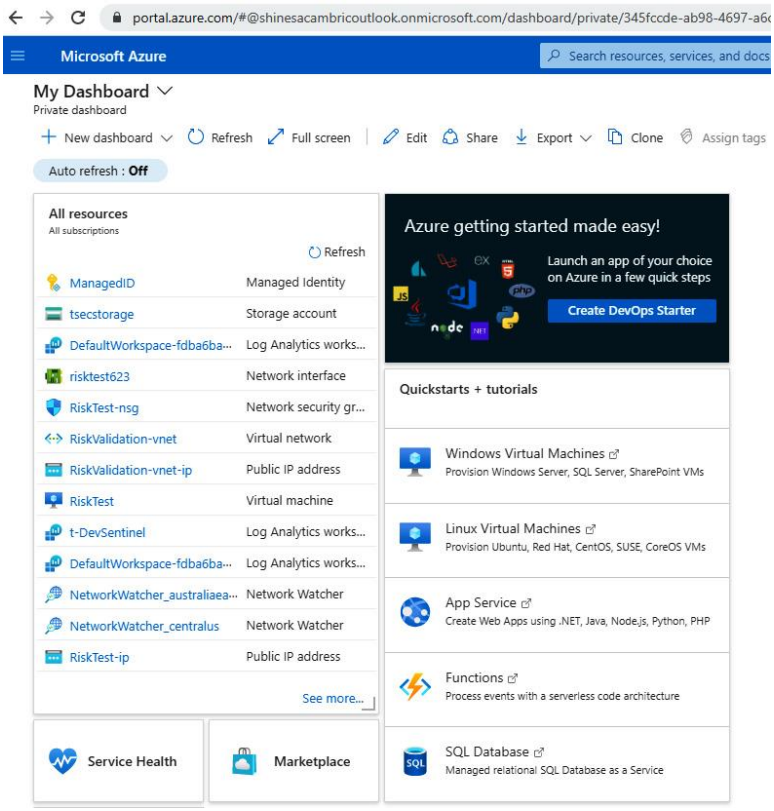

Figure 1.10 – Microsoft Azure portal personal dashboard

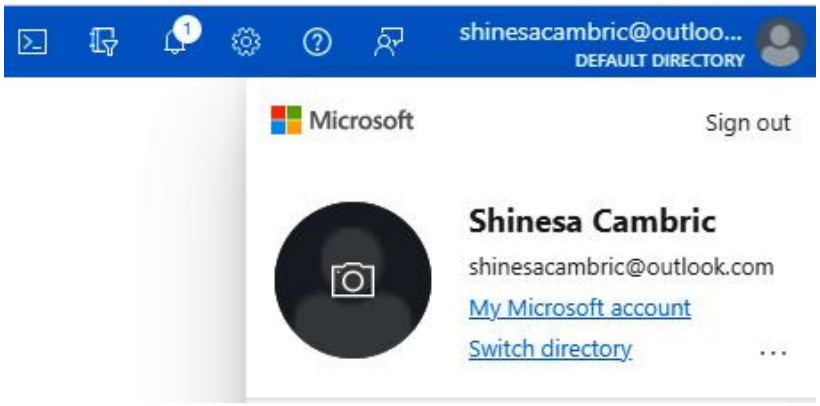

Figure 1.11 – Microsoft Azure portal sign-in details

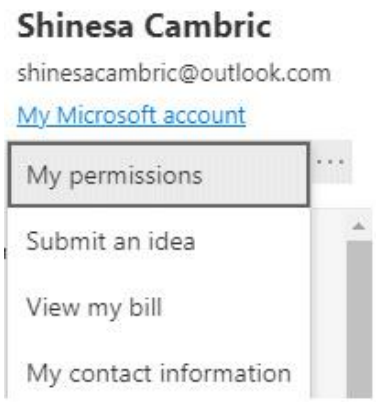

Figure 1.12 – Microsoft Azure portal account details

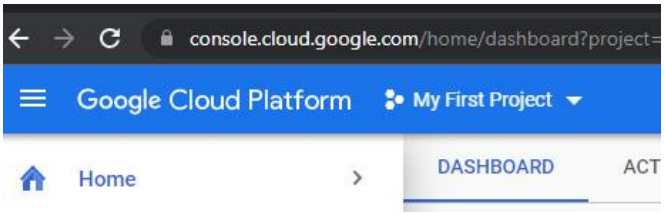

Figure 1.13 – GCP home page

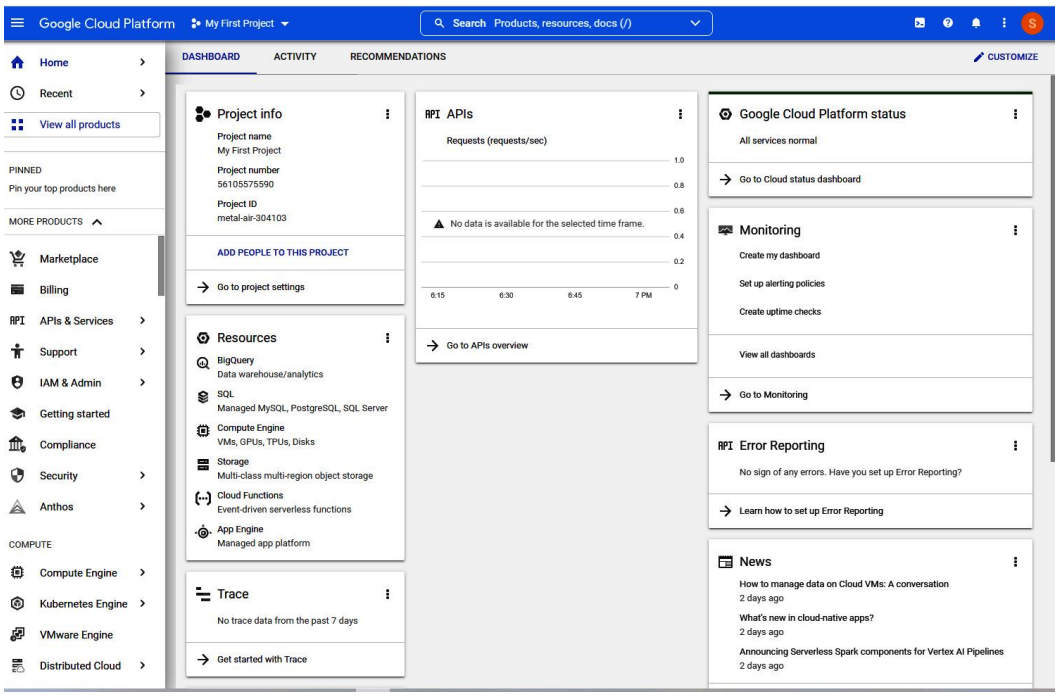

Figure 1.14 – GCP home page dashboard

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

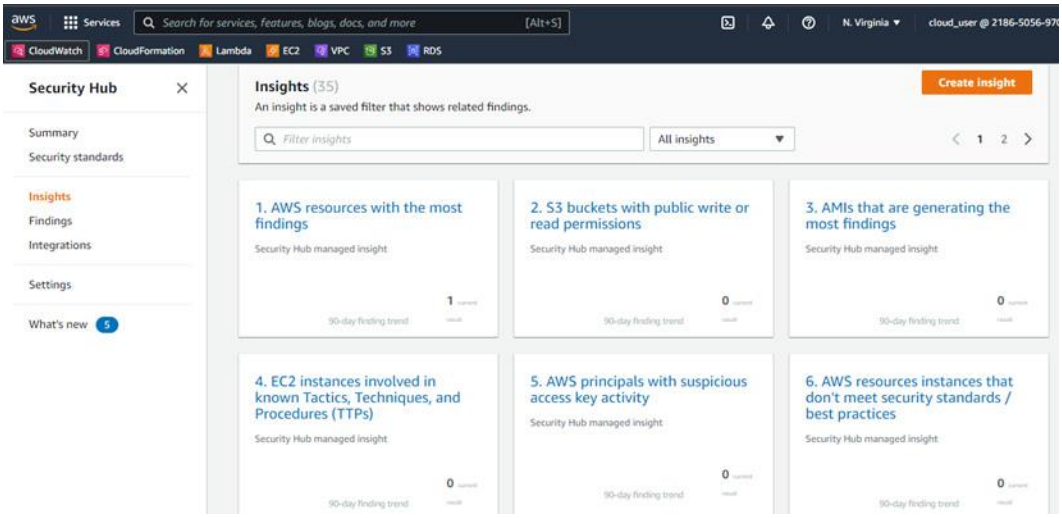

Figure 2.1 – Interface of AWS Security Hub

Figure 2.2 – Trusted Advisor interface

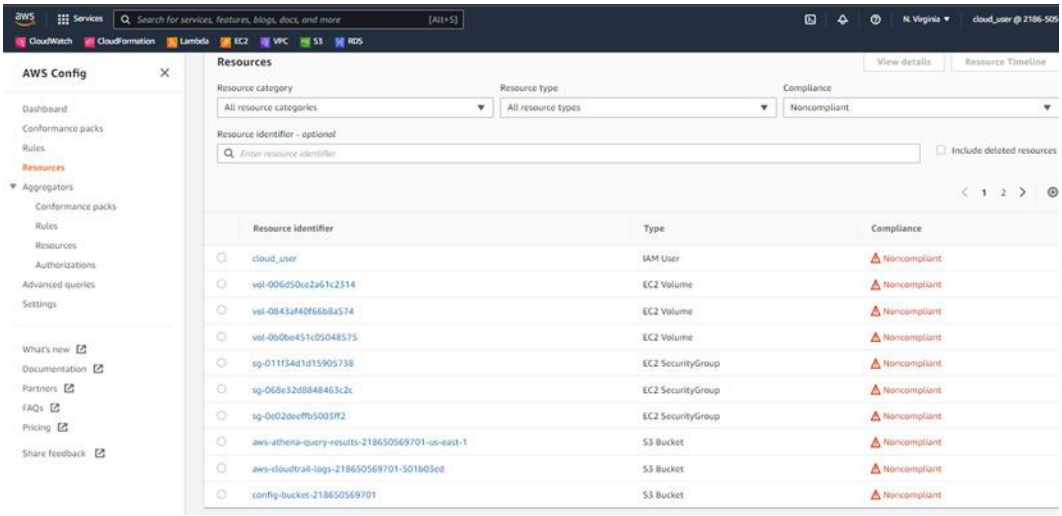

Figure 2.3 – AWS Config interface

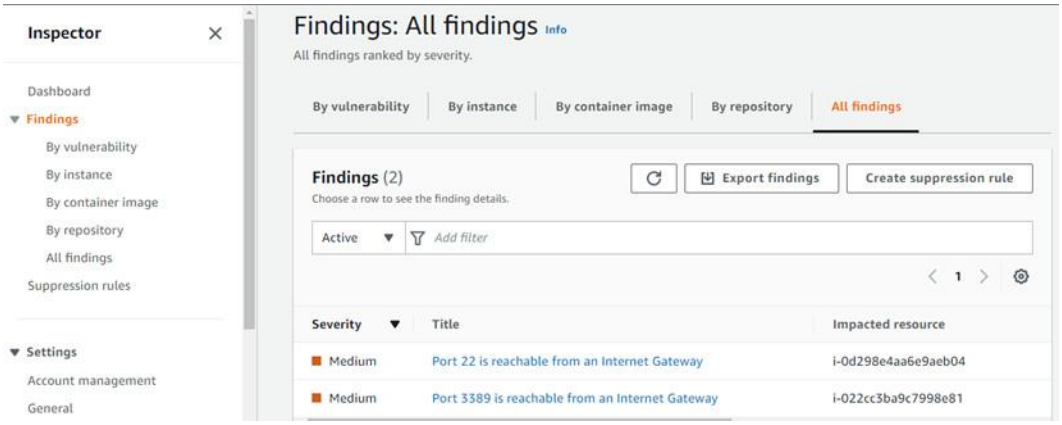

Figure 2.4 – Amazon Inspector interface

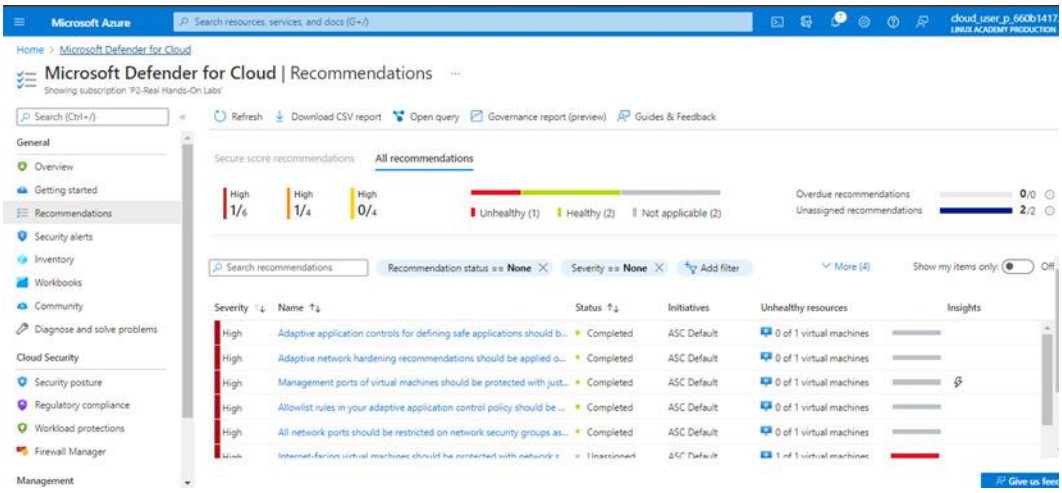

Figure 2.5 – Microsoft Defender for Cloud

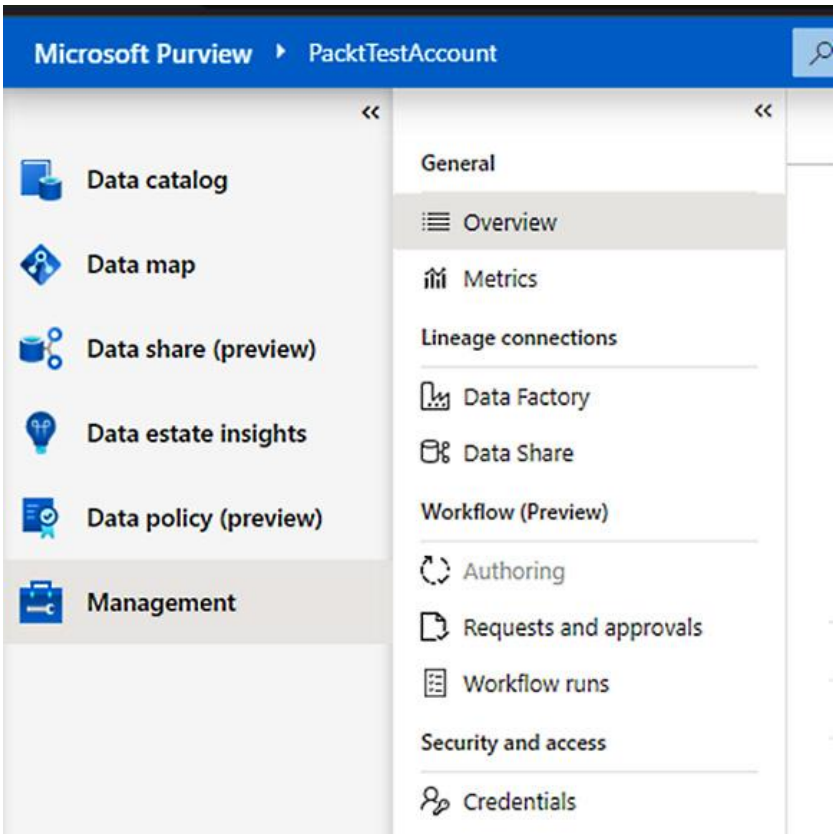

Figure 2.6 – Microsoft Purview

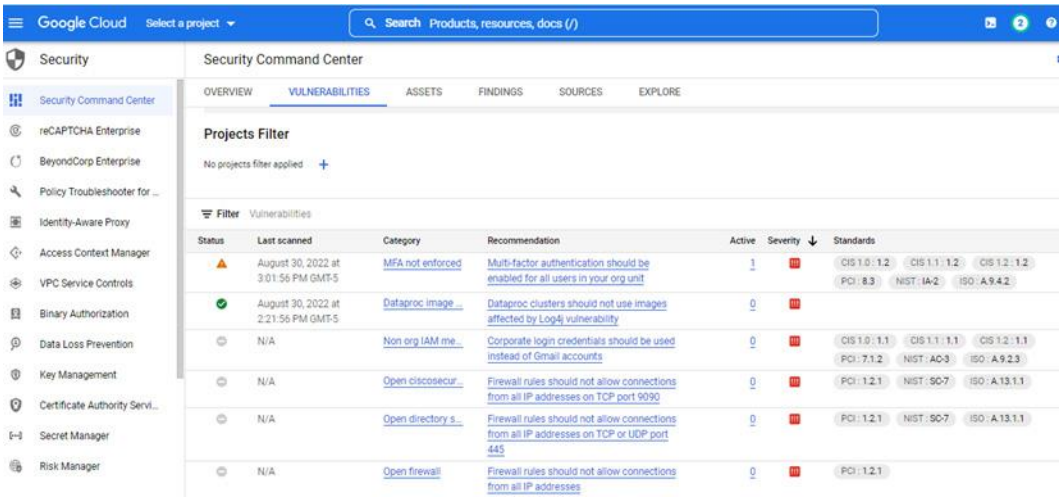

Figure 2.7 – Google Security Command Center

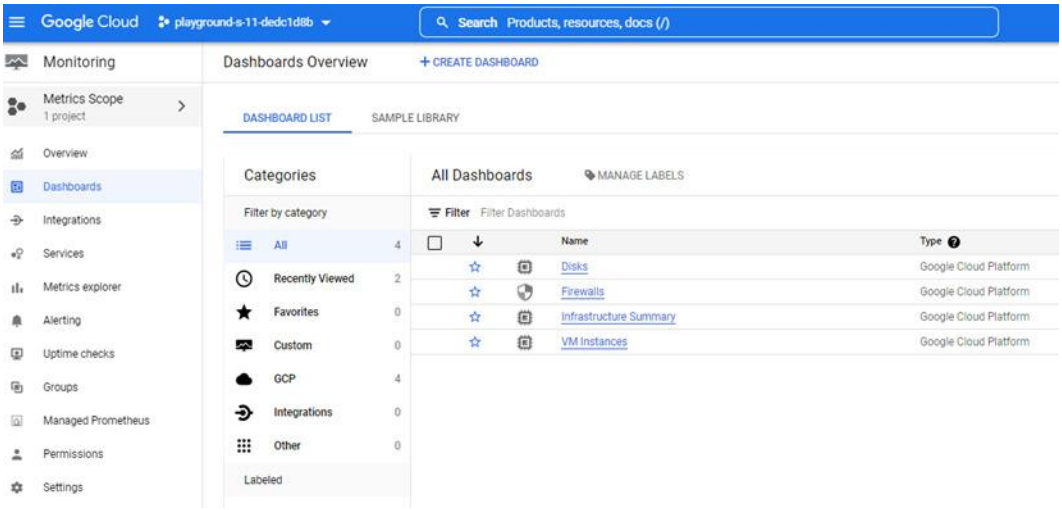

Figure 2.8 – Cloud Monitoring

Chapter 3

Figures

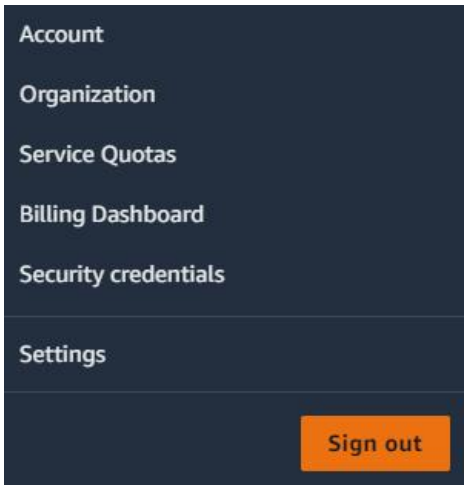

Figure 3.1 – Navigating to the Organization configuration settings

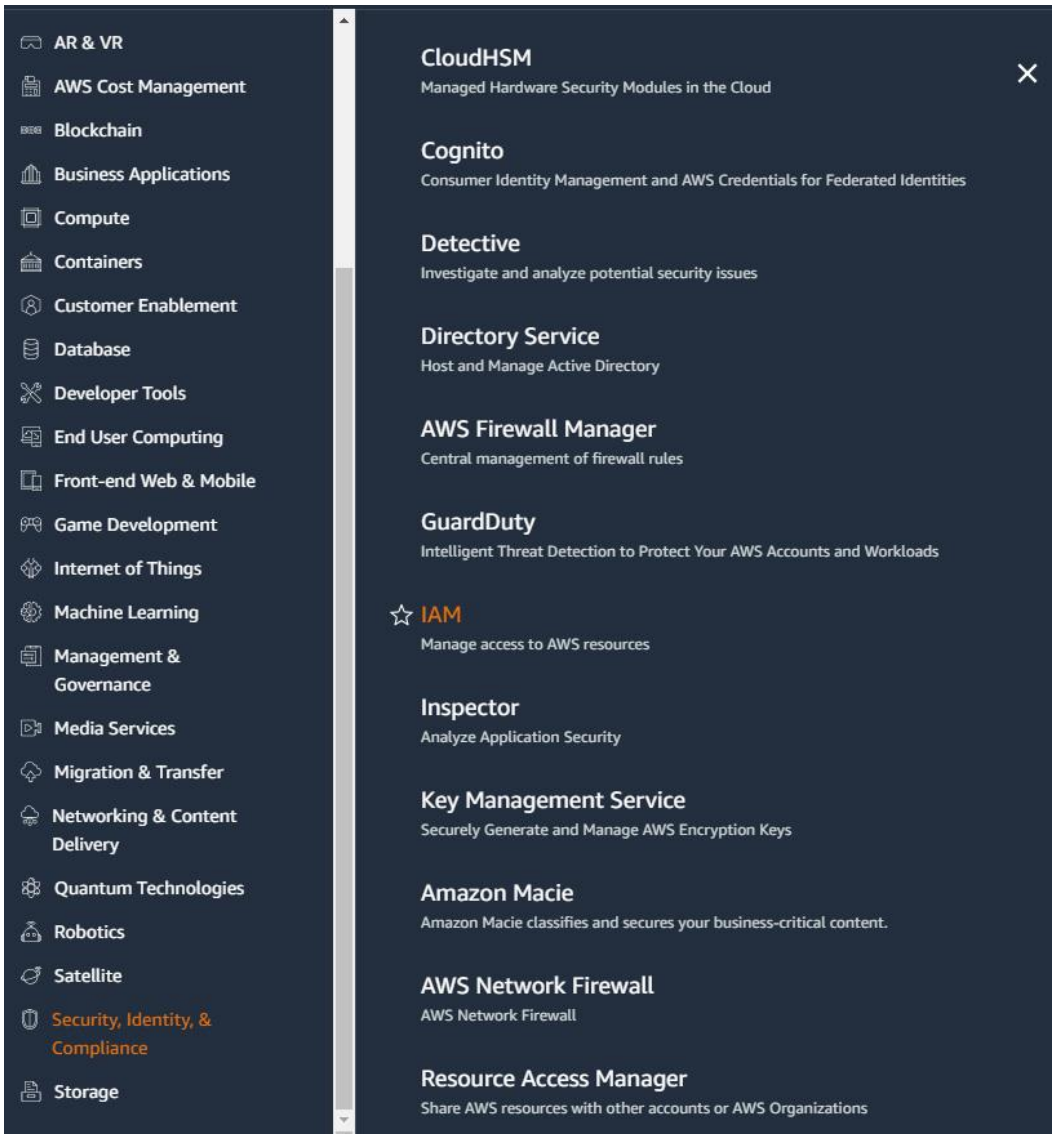

Figure 3.2 – AWS navigation to IAM configuration

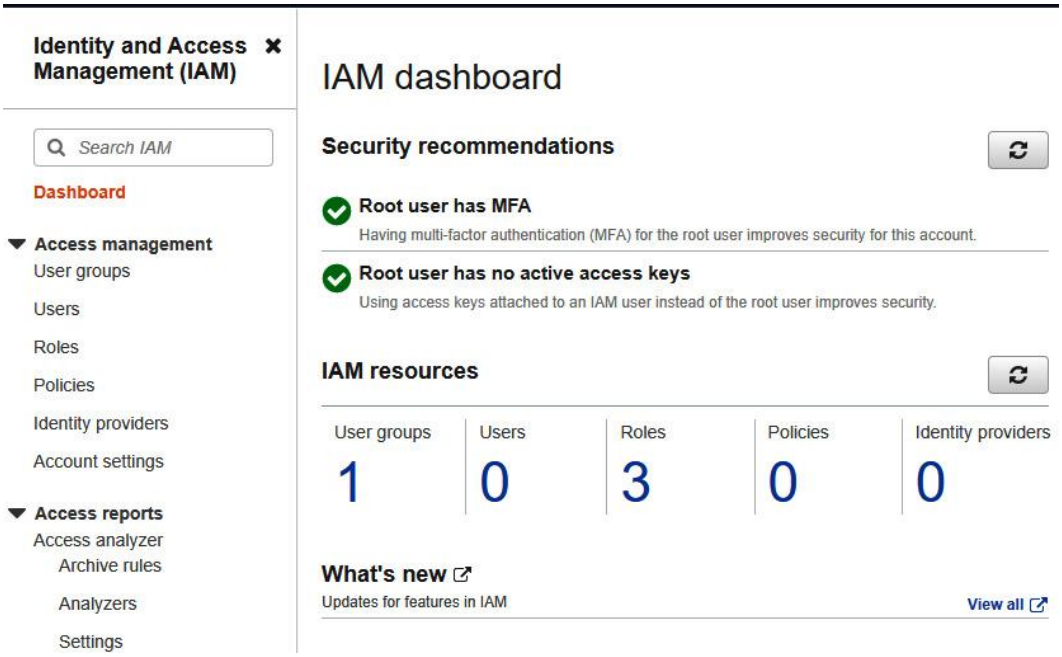

Figure 3.3 – AWS IAM configurations

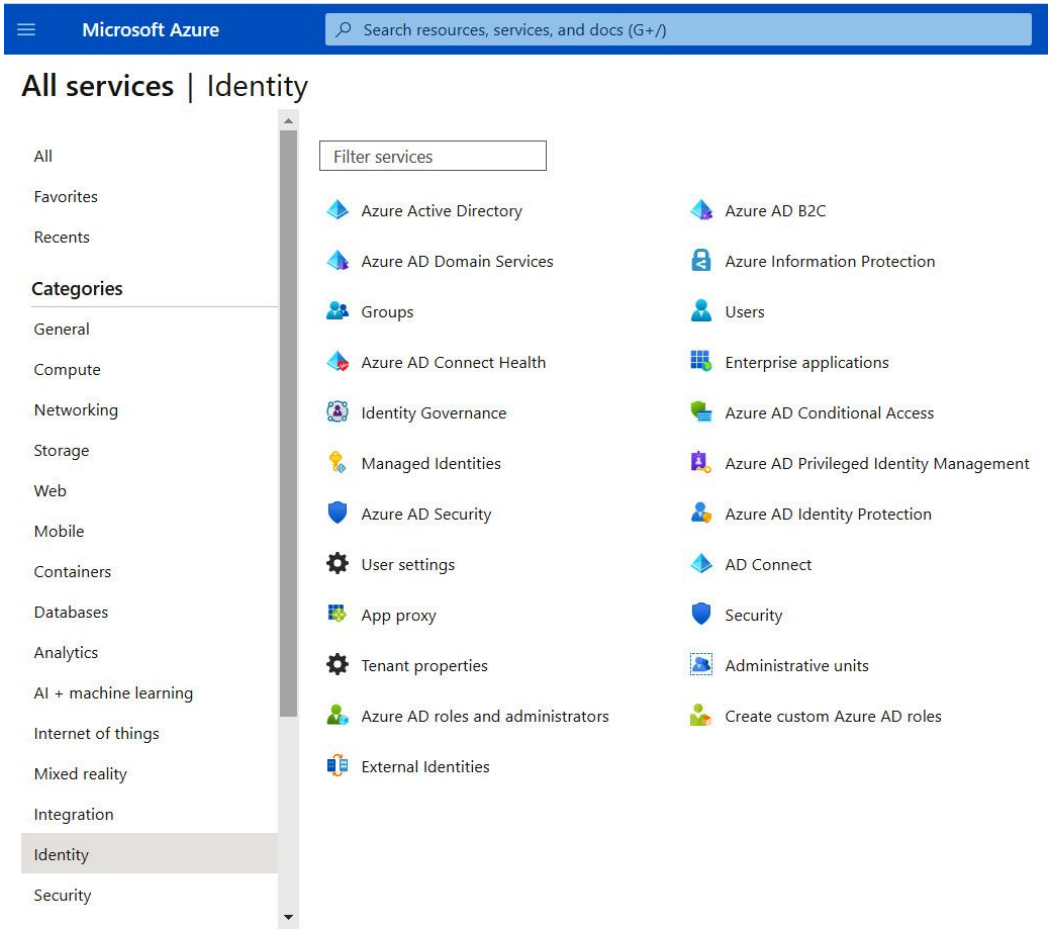

Figure 3.4 – Microsoft Azure IAM configurations

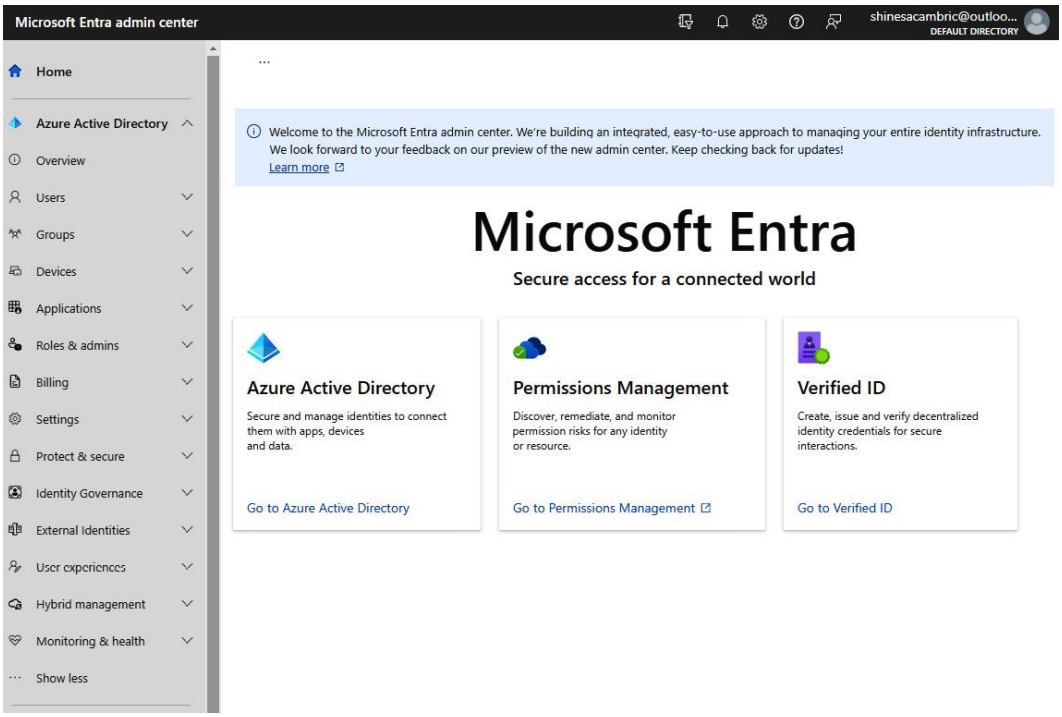

Figure 3.5 – Microsoft Entra admin center

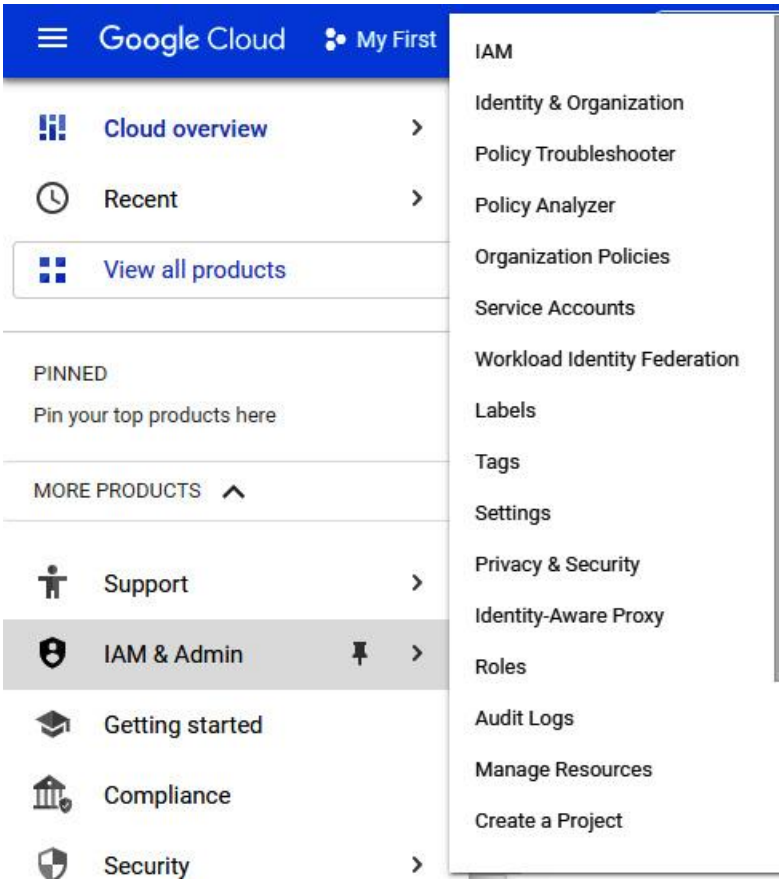

Figure 3.6 – GCP IAM & Admin configuration options

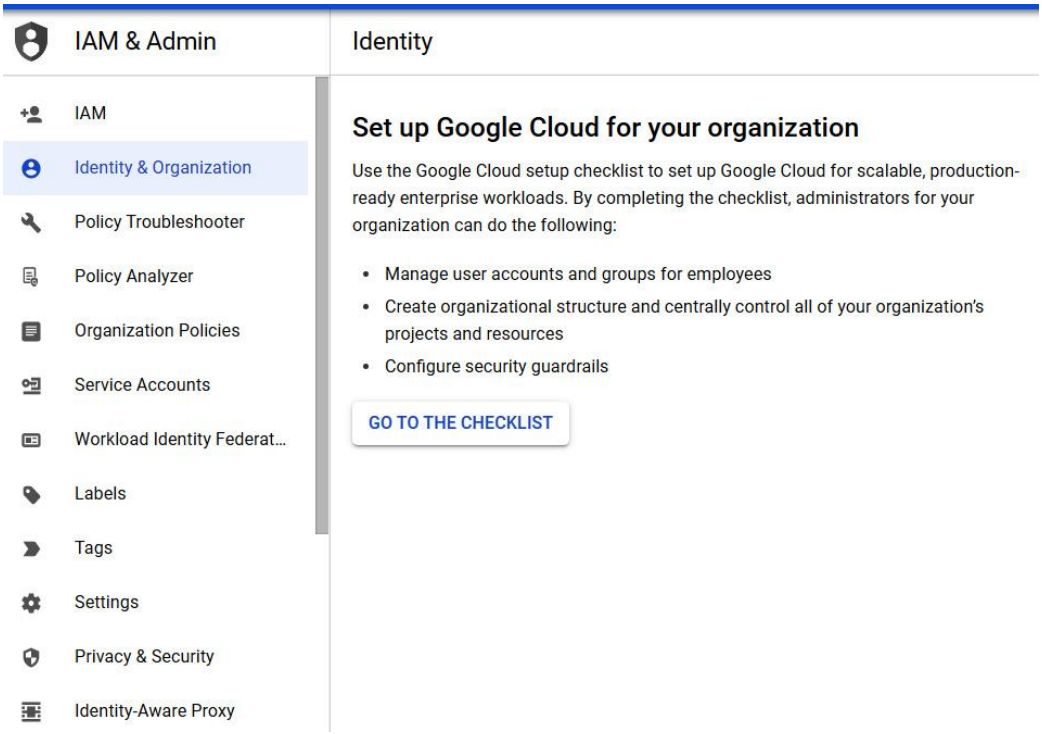

Figure 3.7 – Establishing an organization within GCP

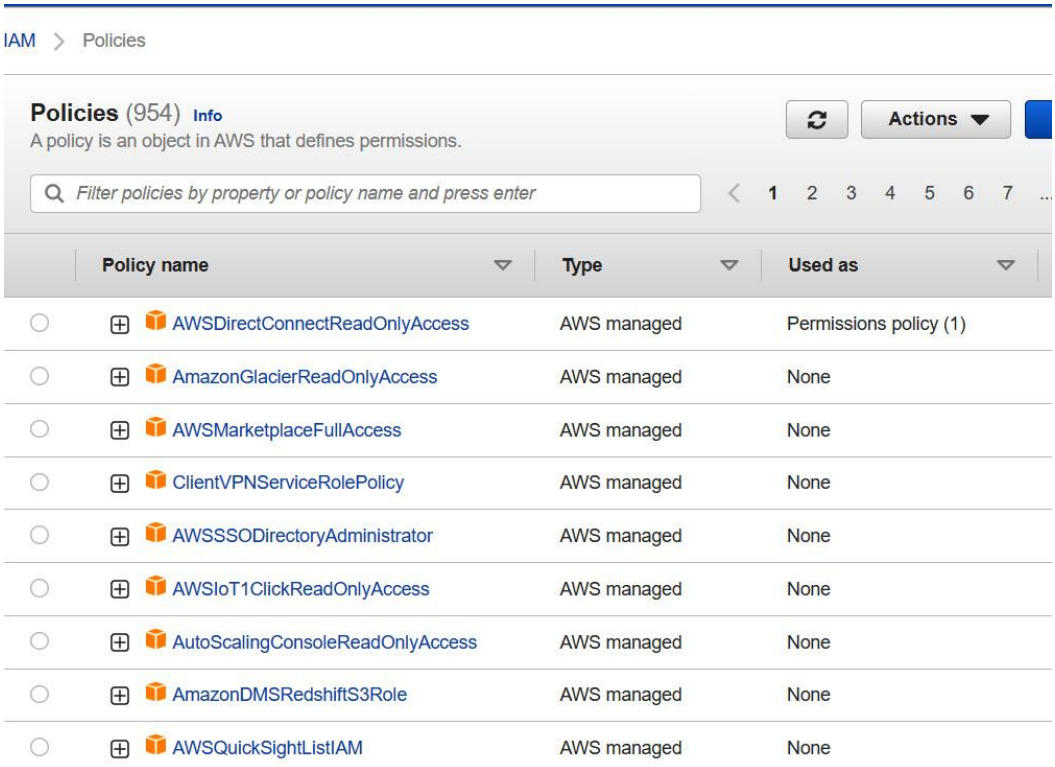

Figure 3.8 – List of available AWS managed policies

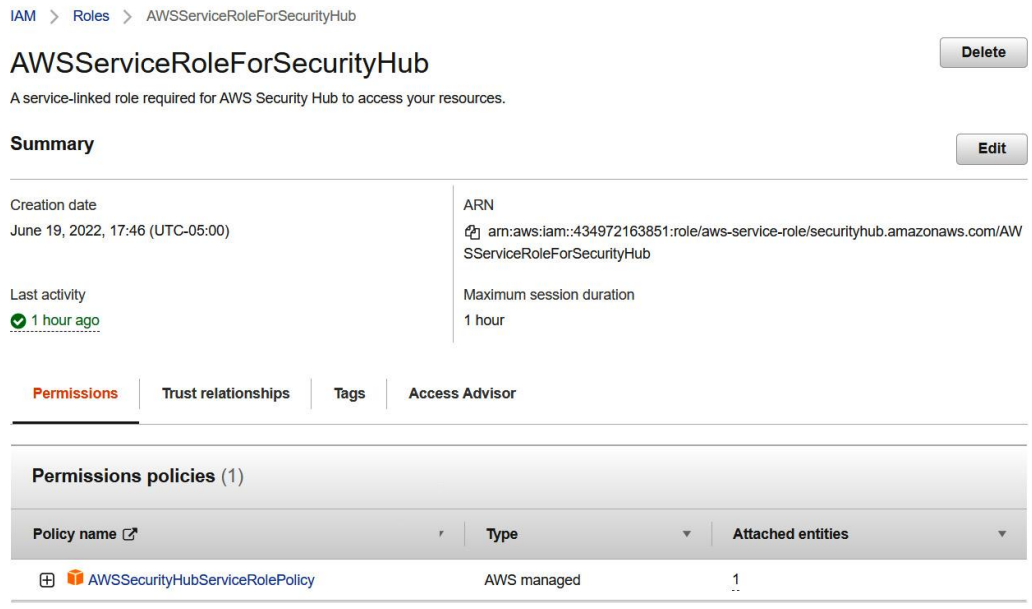

Figure 3.9 – AWS time-bound access

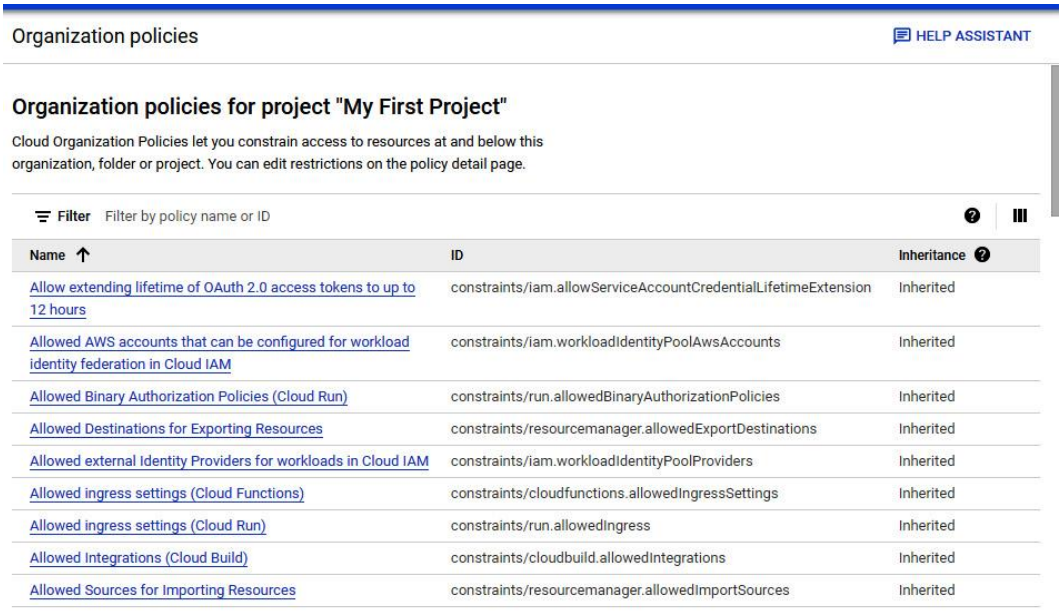

Figure 3.10 – Example GCP organization policies with inheritance

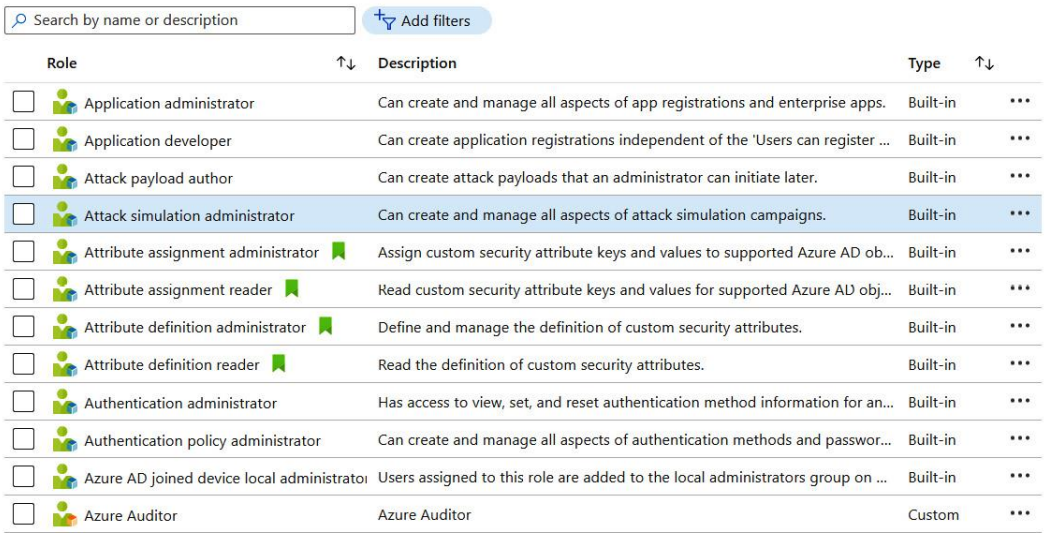

Figure 3.11 – Example Azure built-in and custom roles

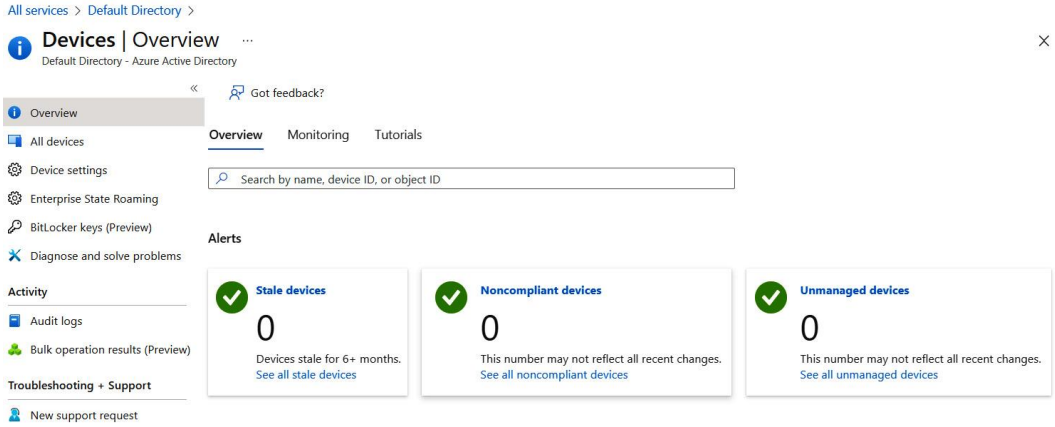

Figure 3.12 – Example Microsoft Azure device policy overview

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

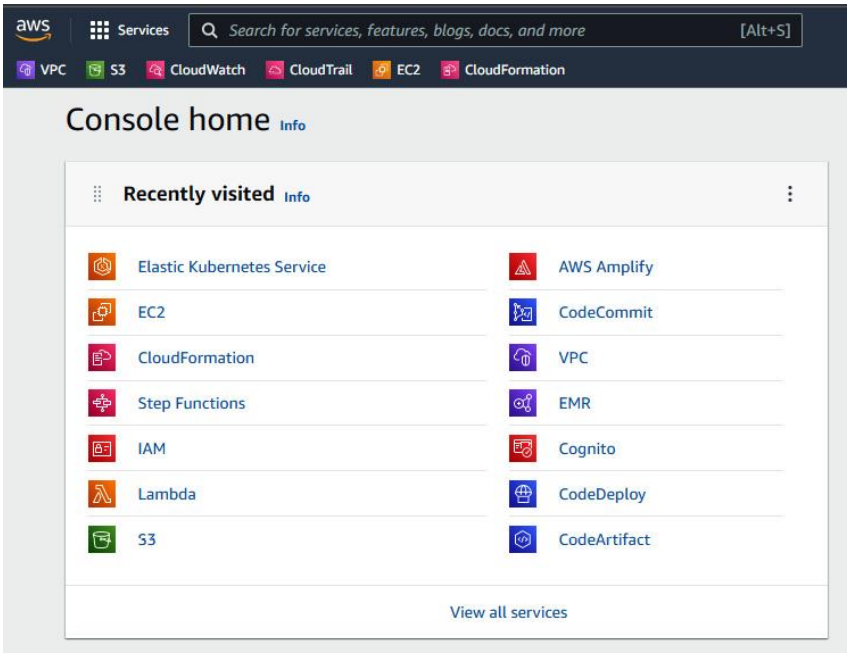

Figure 4.1 – AWS Console home

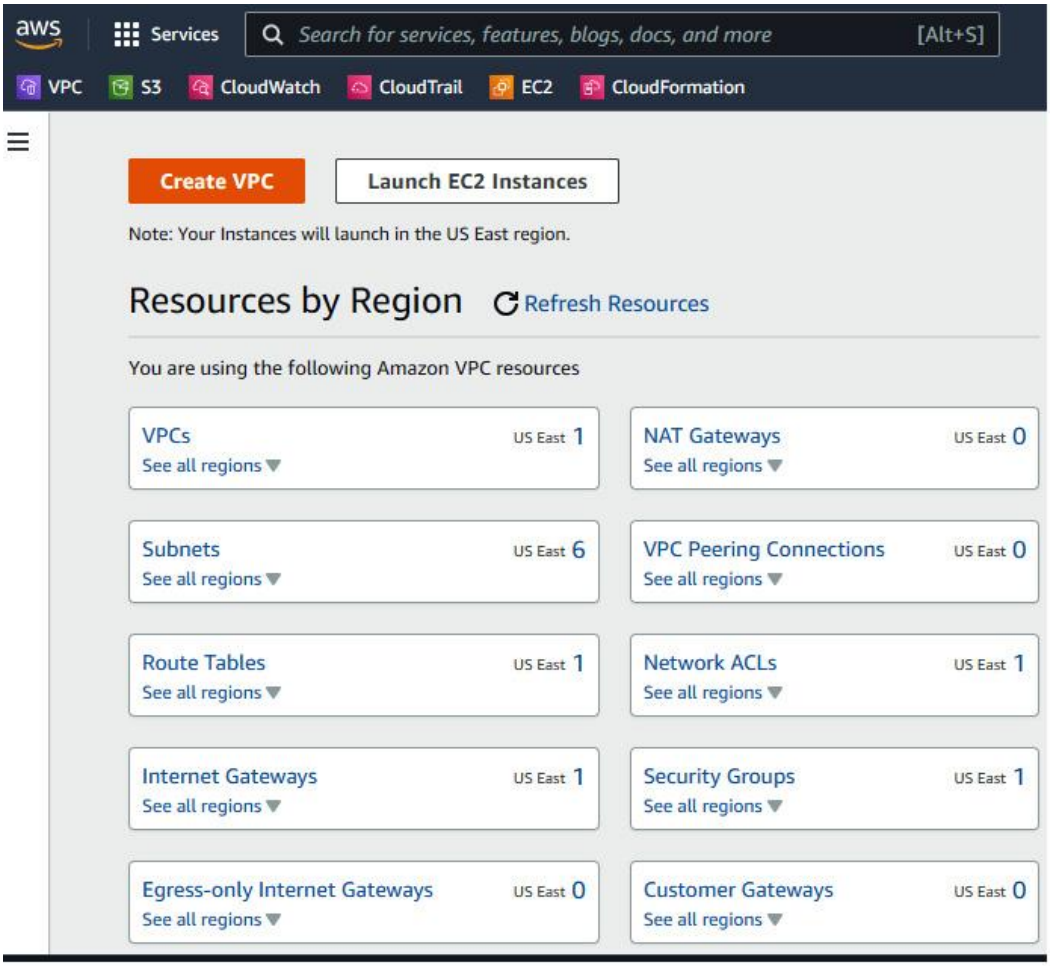

Figure 4.2 – AWS – Resources by Region

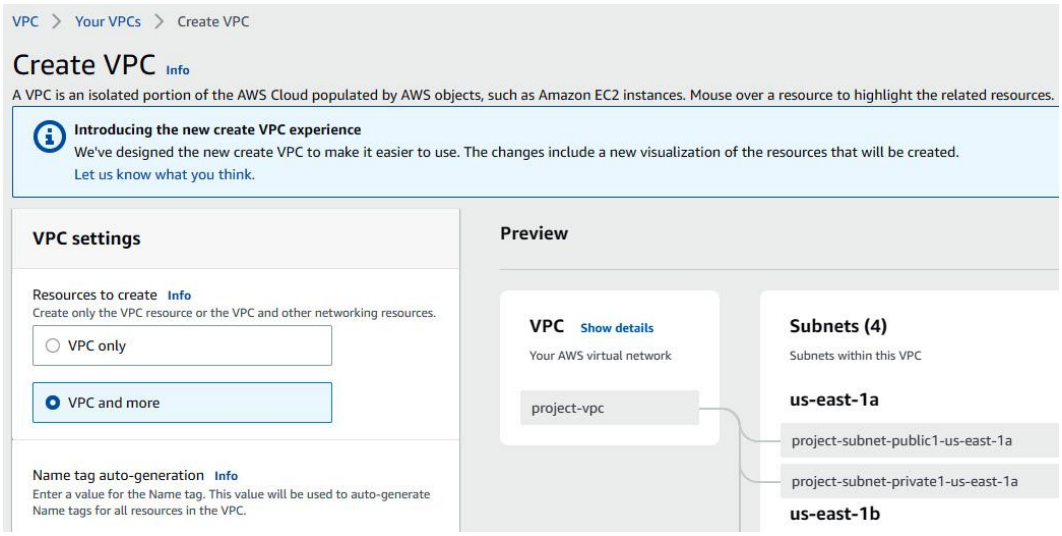

Figure 4.3 – AWS Create VPC configuration options

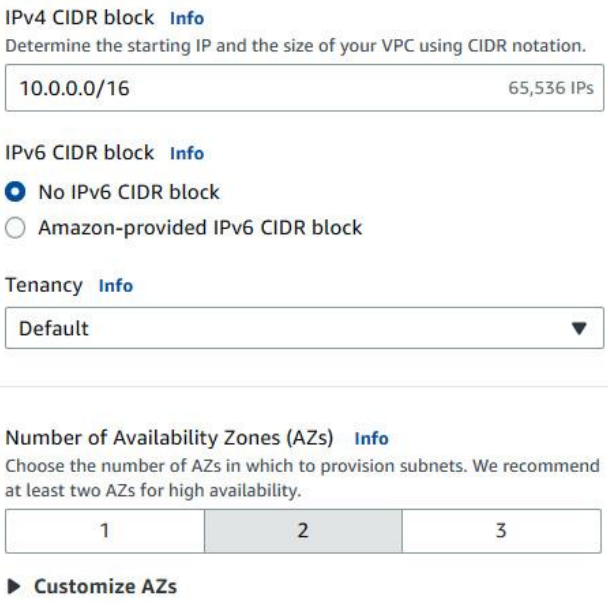

Figure 4.4 – AWS Create VPC – IP address options

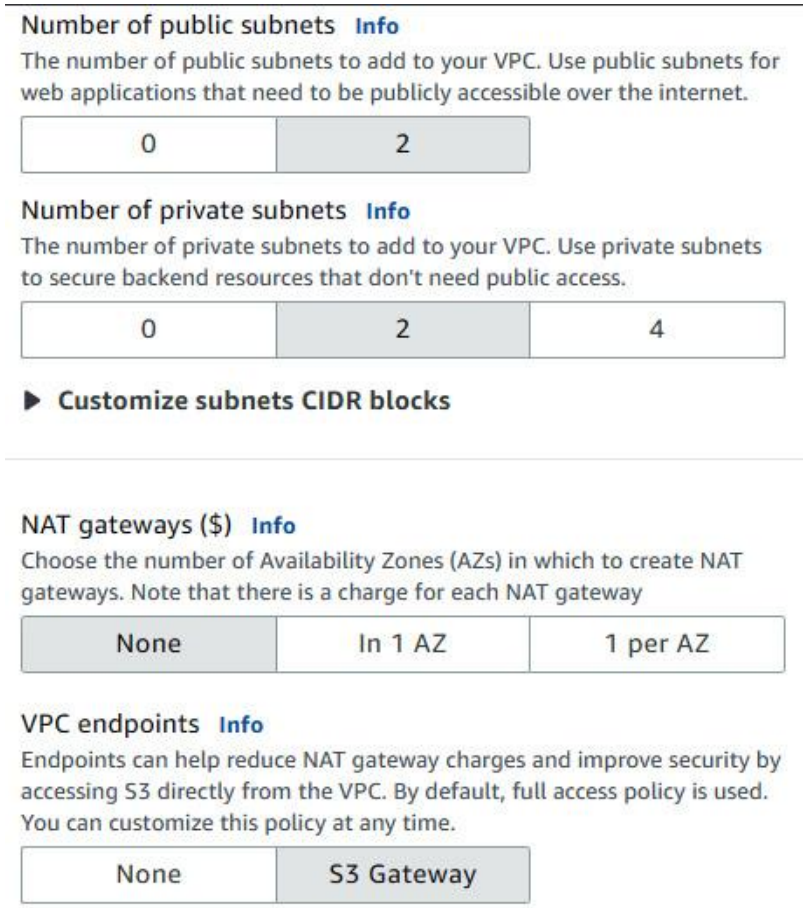

Figure 4.5 – AWS Create VPC – subnet options

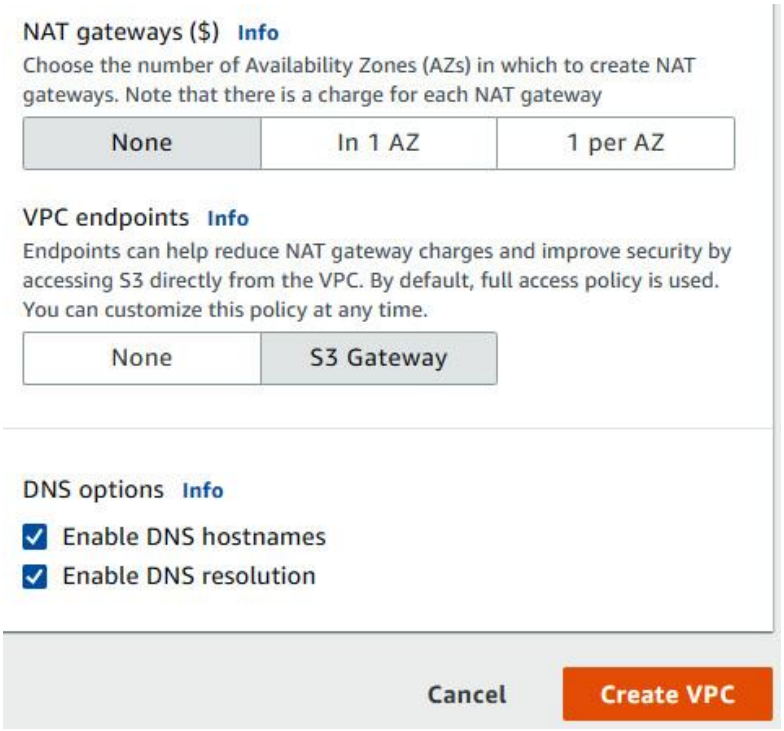

Figure 4.6 – AWS Create VPC – NAT gateway options, VPC endpoints, and DNS options

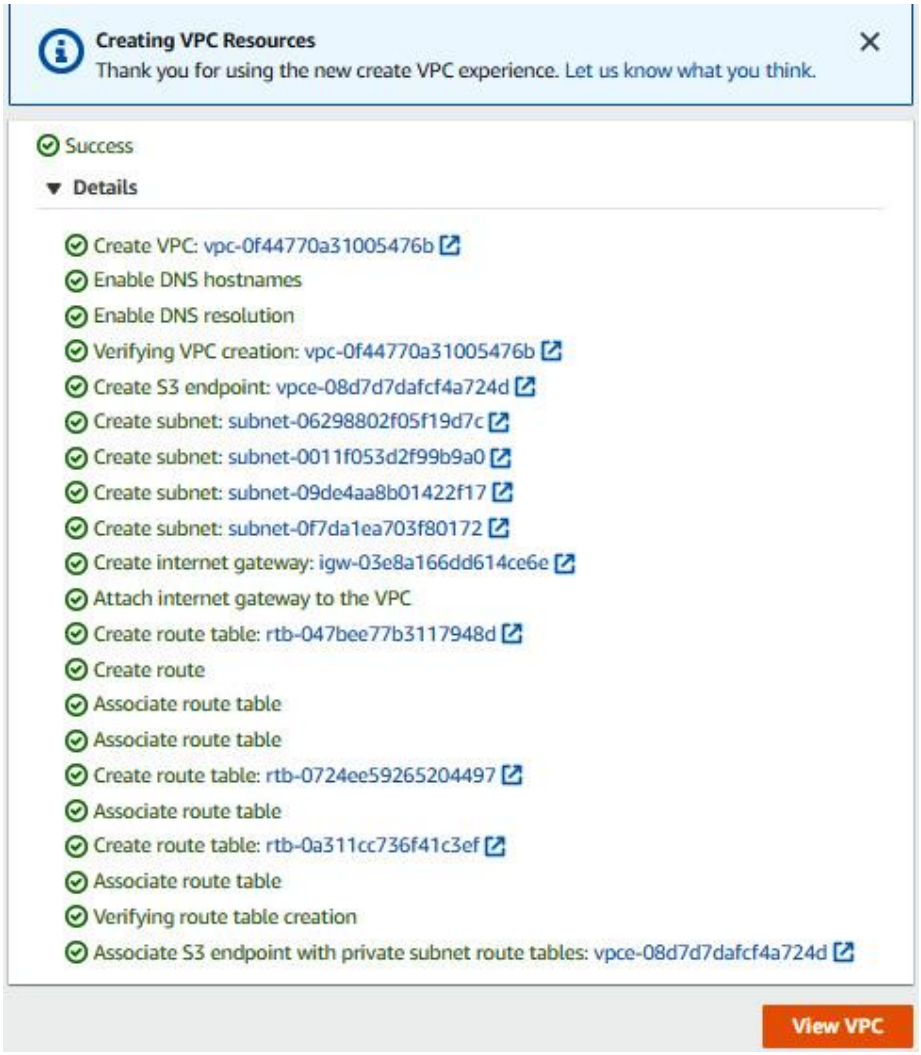

Figure 4.7 – AWS – Creating VPC Resources

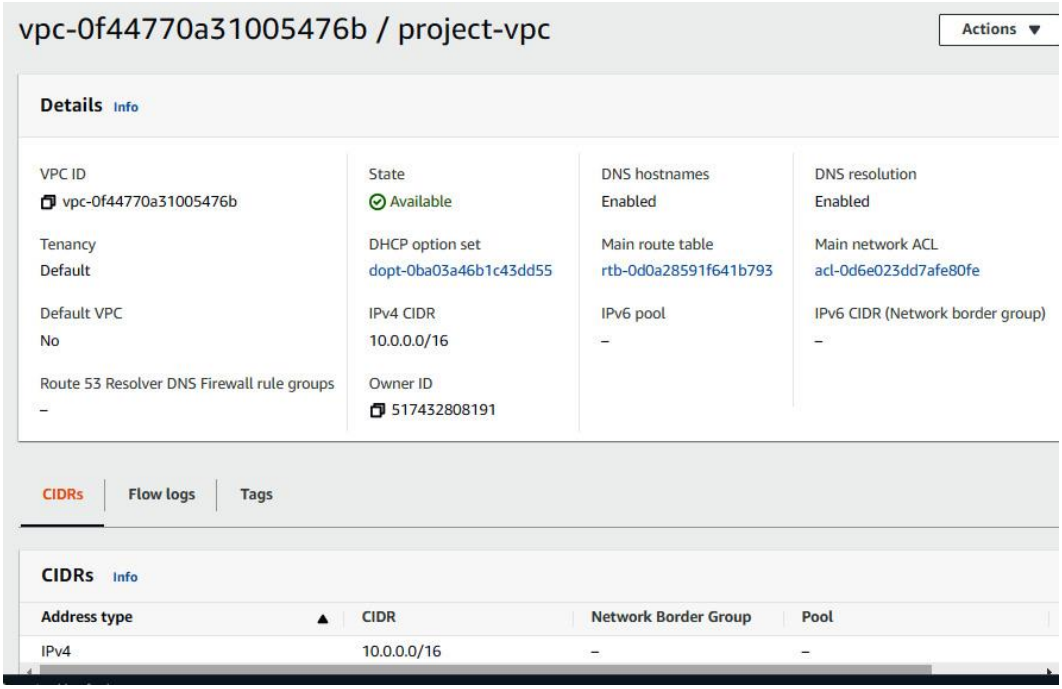

Figure 4.8 – AWS VPC deployed

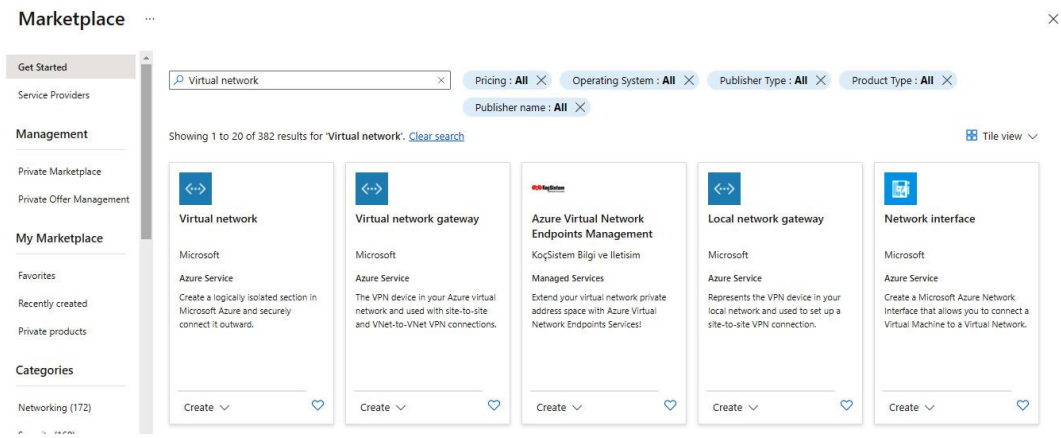

Figure 4.9 – Azure portal

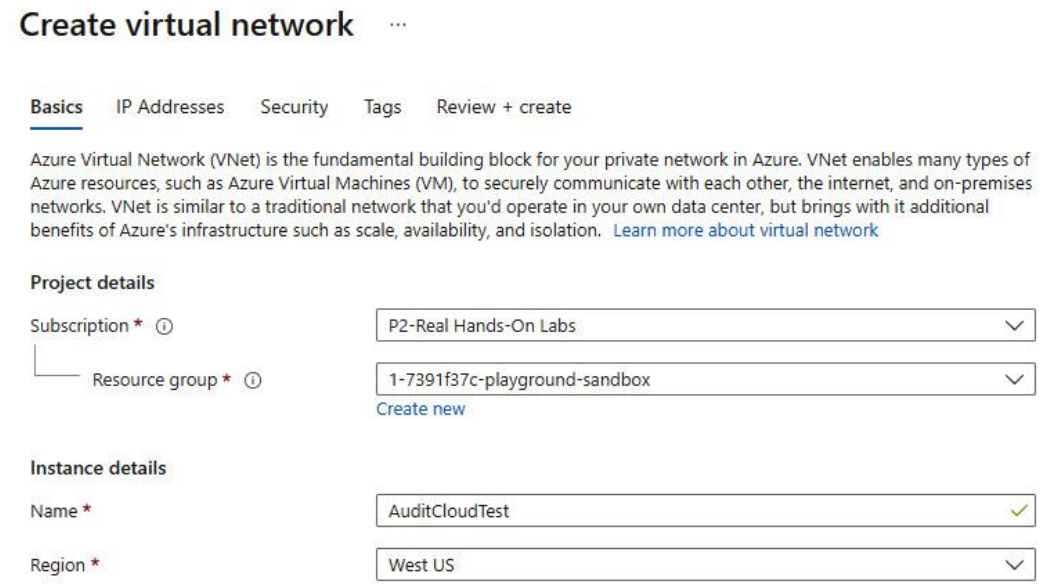

Figure 4.10 – Creating an Azure VNet

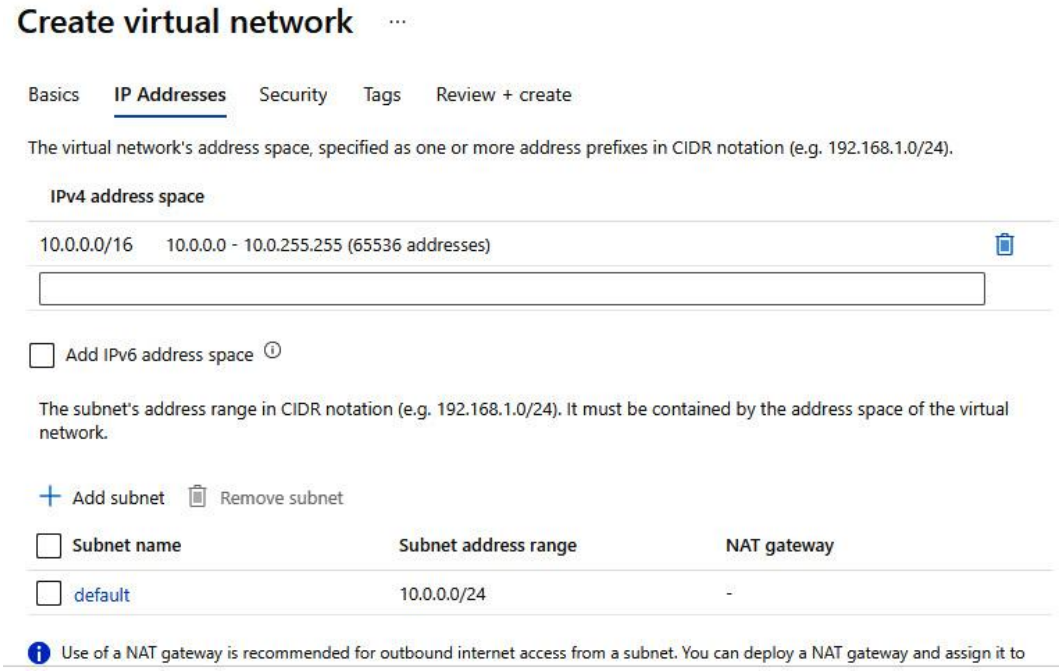

Figure 4.11 – Azure VNet IP address configuration options

Figure 4.12 – Azure VNet security configuration options

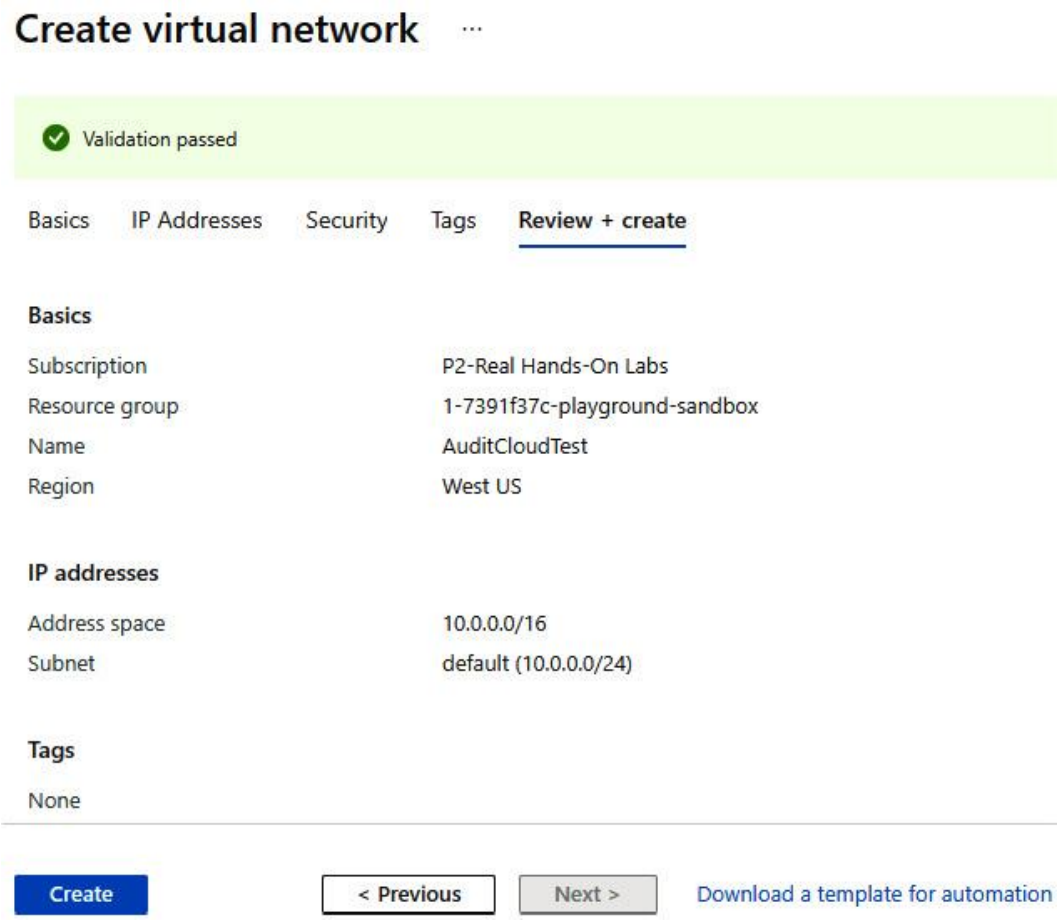

Figure 4.13 – Azure validation of VPC configuration

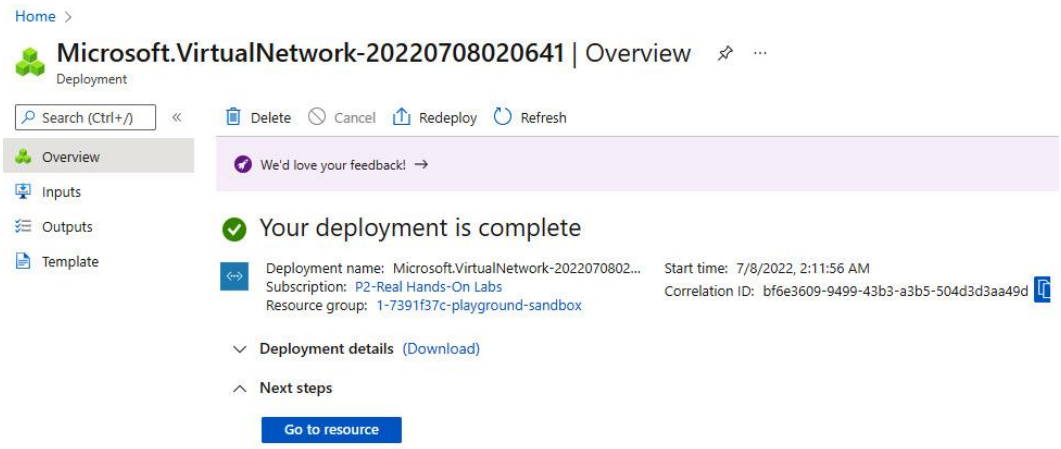

Figure 4.14 – Azure VNet deployed

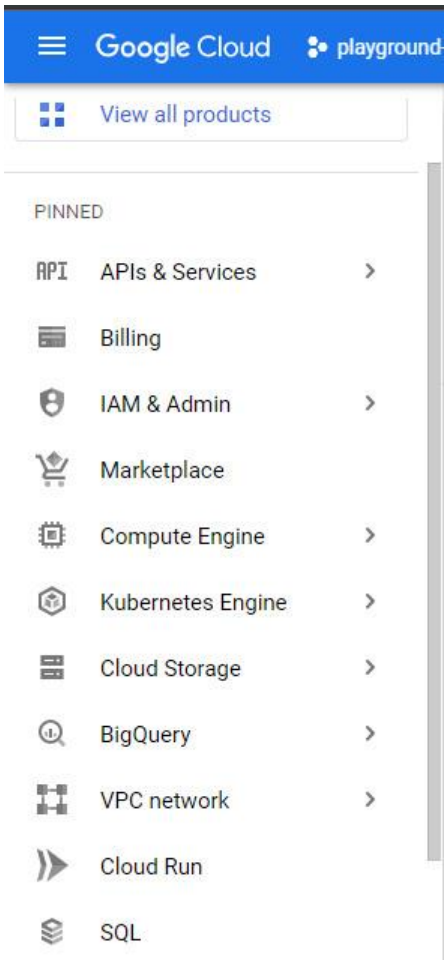

Figure 4.15 – Google Cloud Console

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

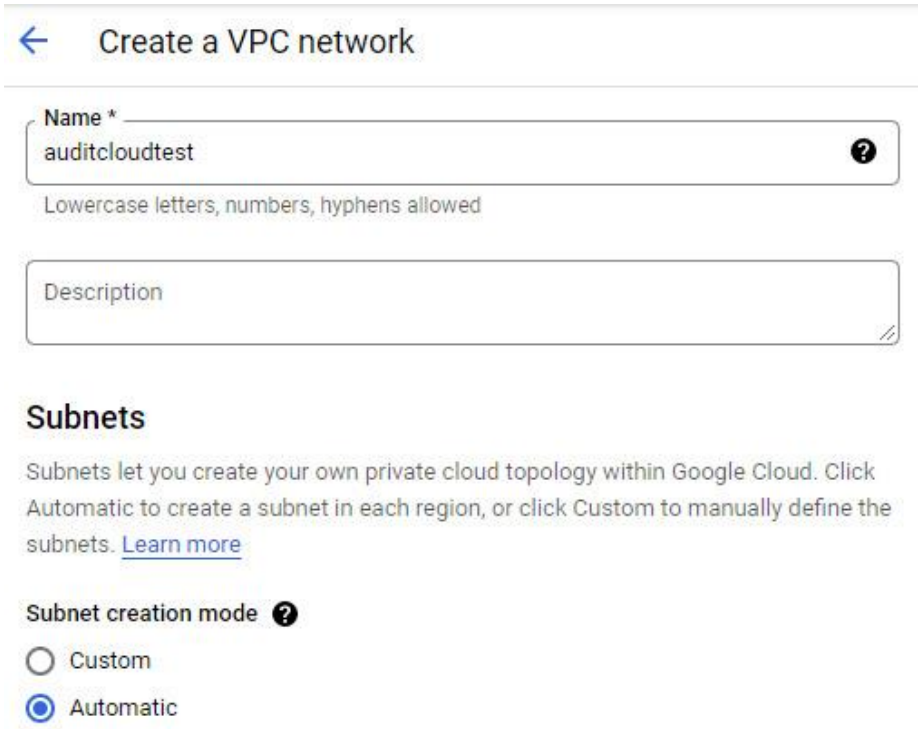

Figure 4.17 – GCP – Create a VPC network

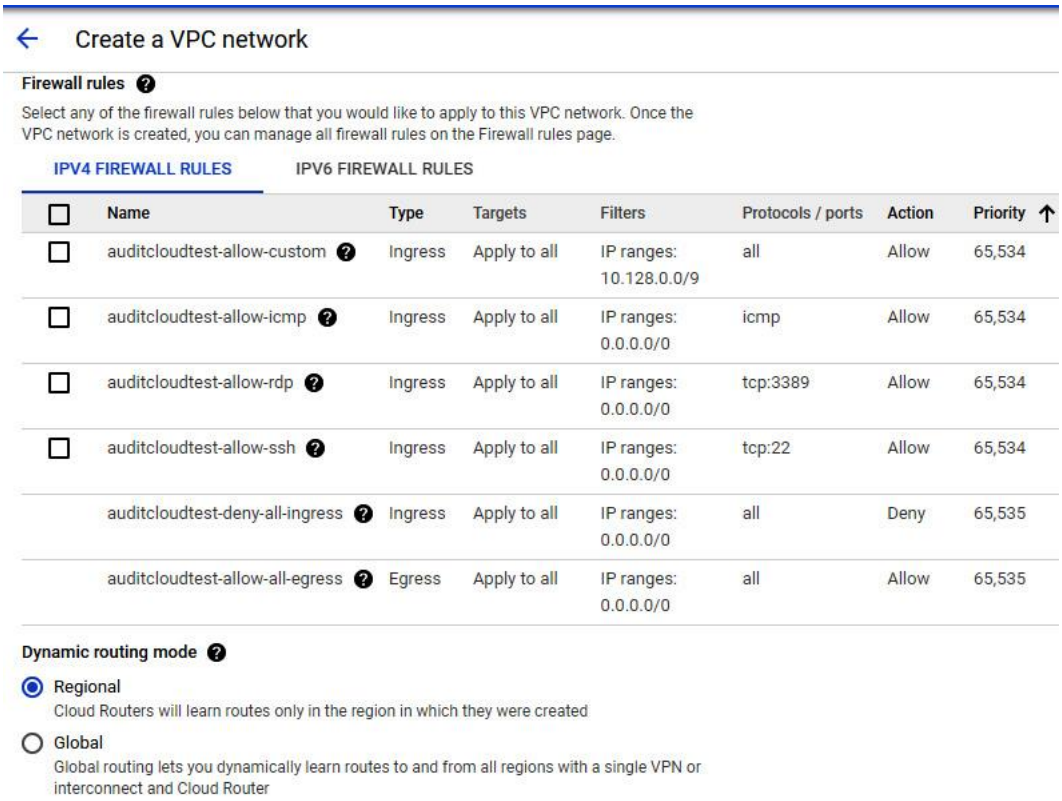

Figure 4.18 – GCP – Firewall rules configuration options

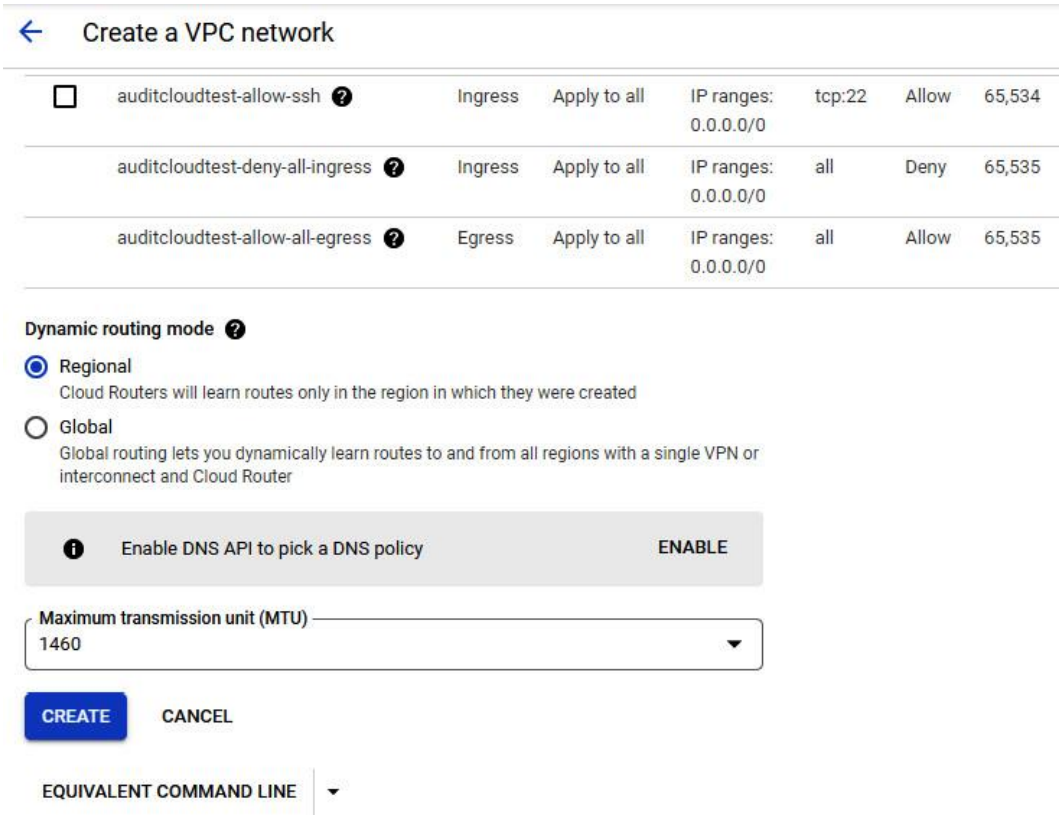

Figure 4.19 – GCP – creating VPC resources

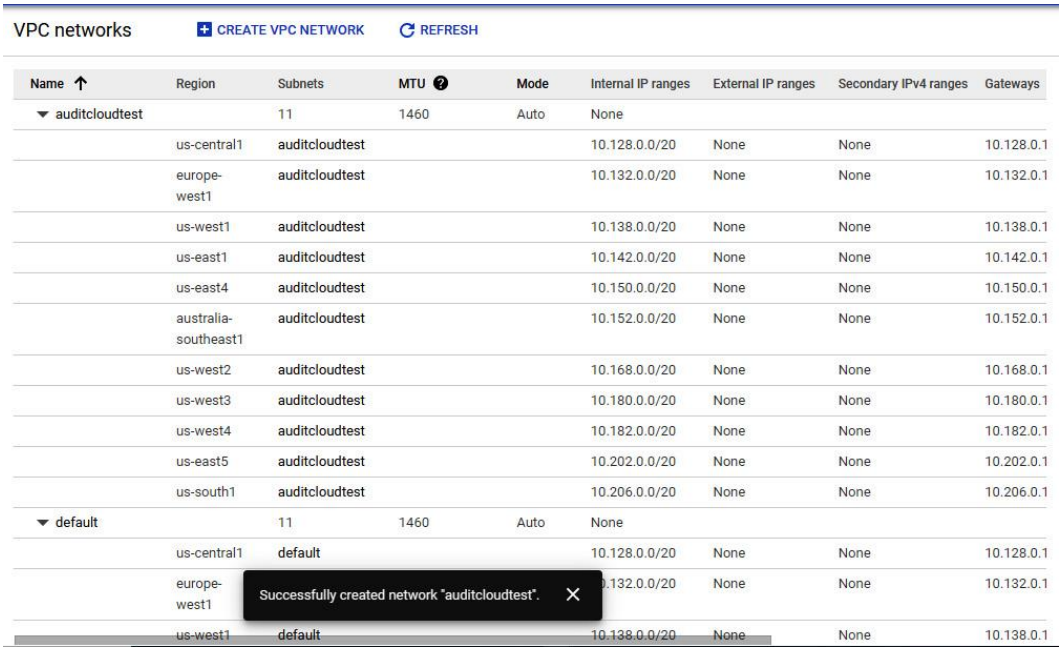

Figure 4.20 – GCP VPC deployed

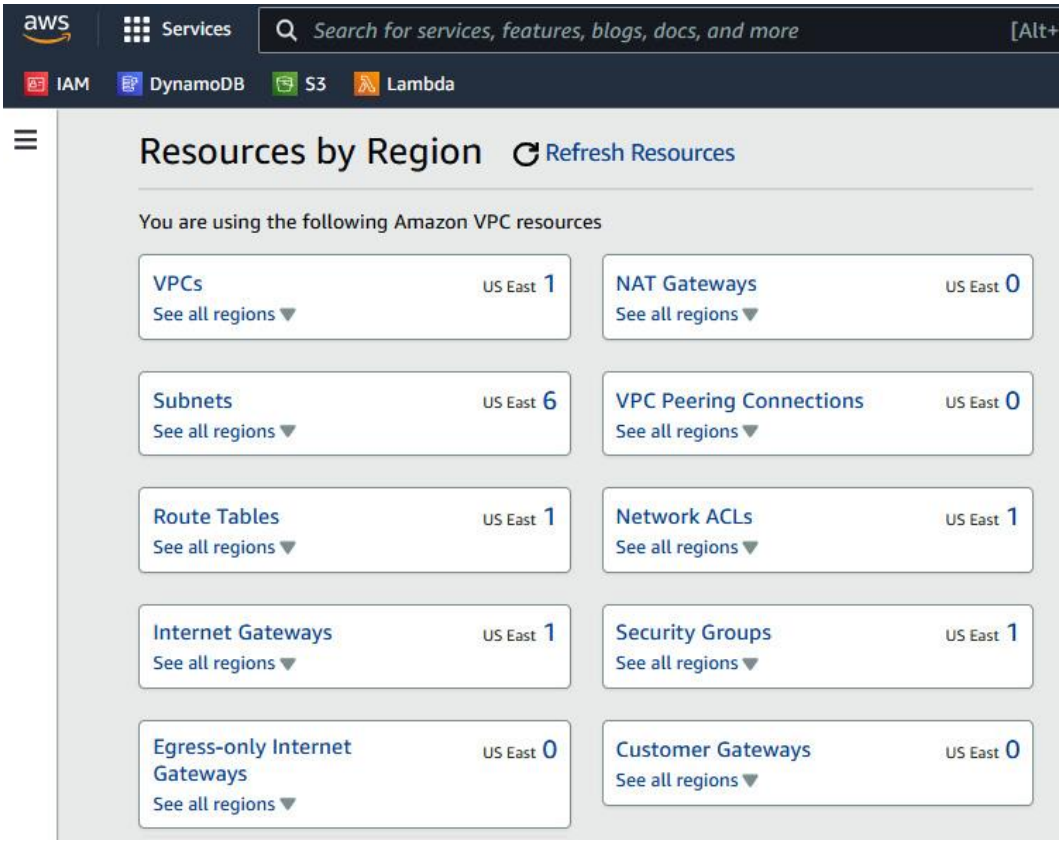

Figure 4.21 – AWS Resources by Region

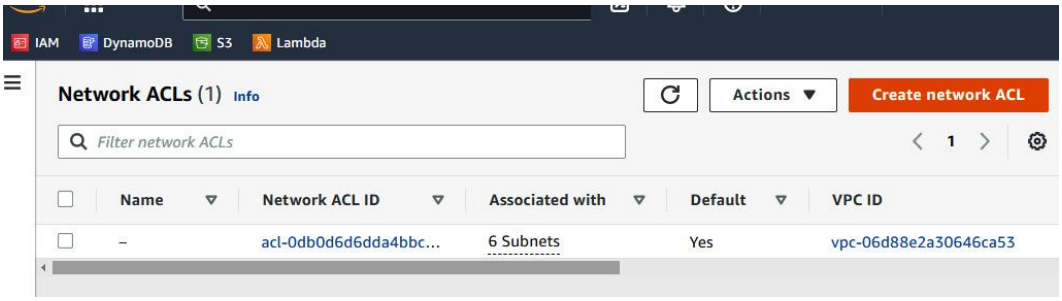

Figure 4.22 – AWS – Network ACLs

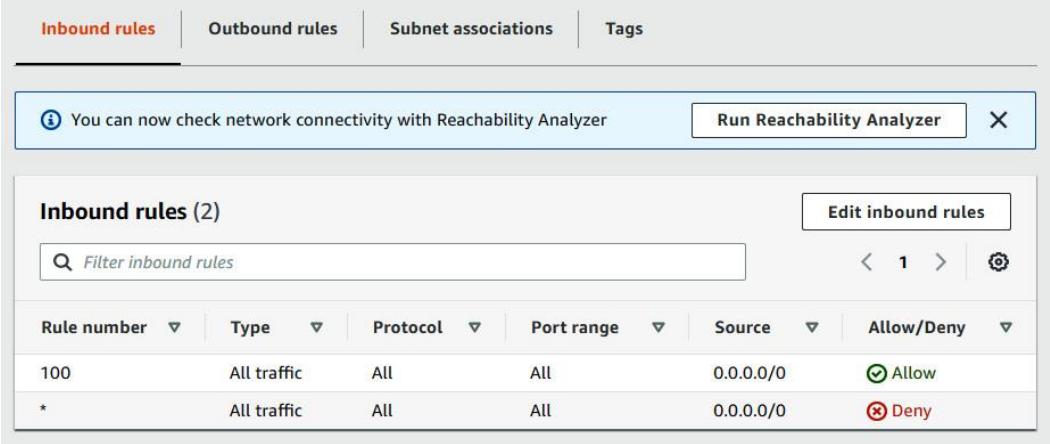

Figure 4.23 – AWS Inbound rules

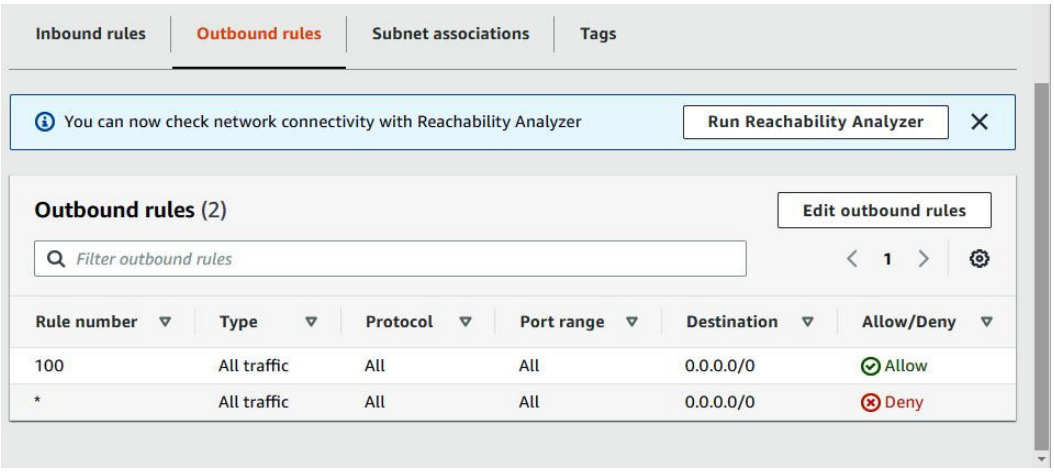

Figure 4.24 – AWS Outbound rules

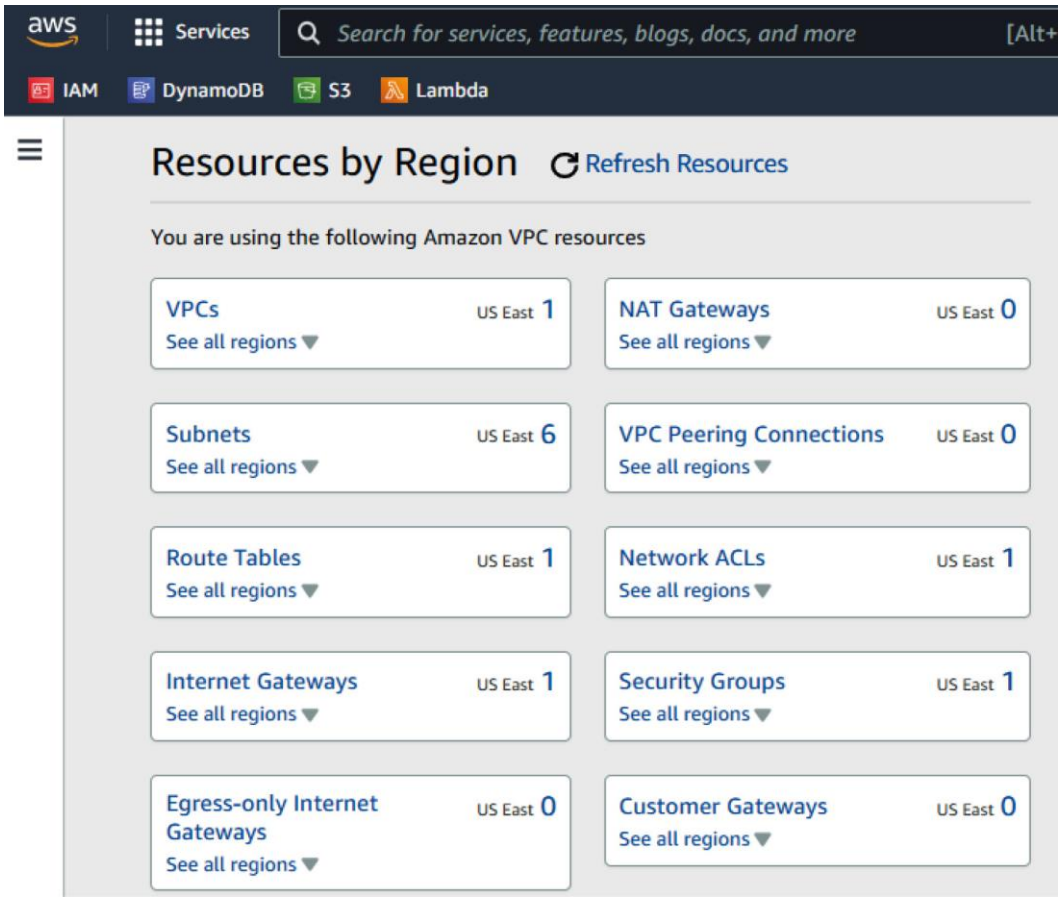

Figure 4.25 – AWS Resources by Region

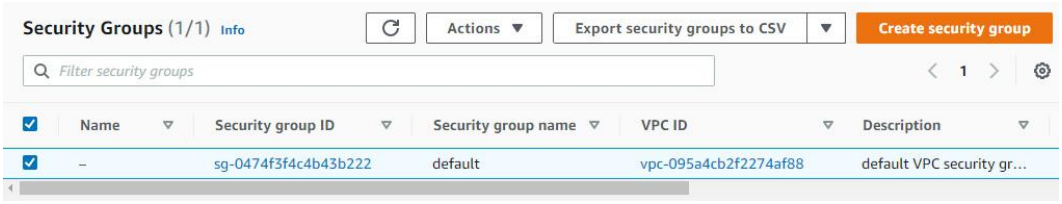

Figure 4.26 – AWS – Security Groups

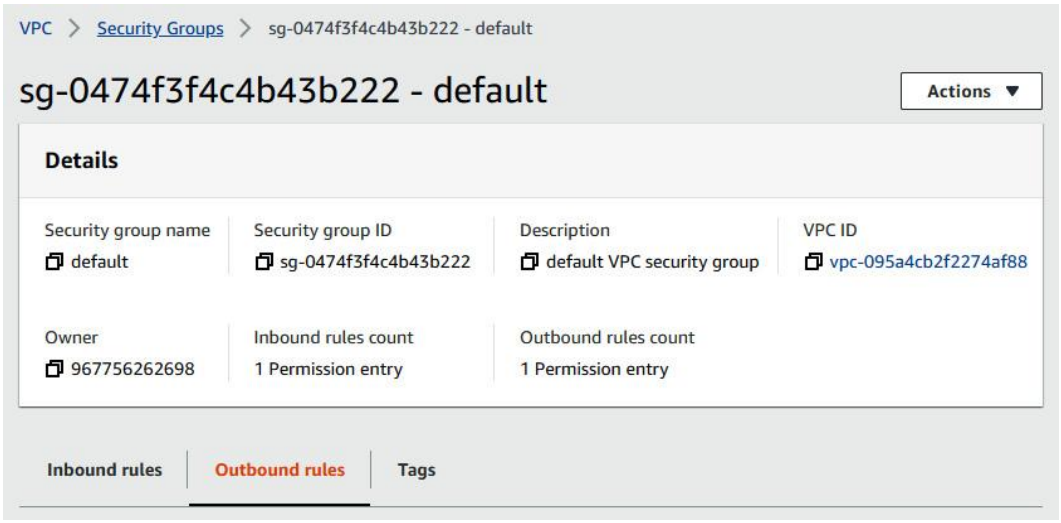

Figure 4.27 – AWS Security Group details

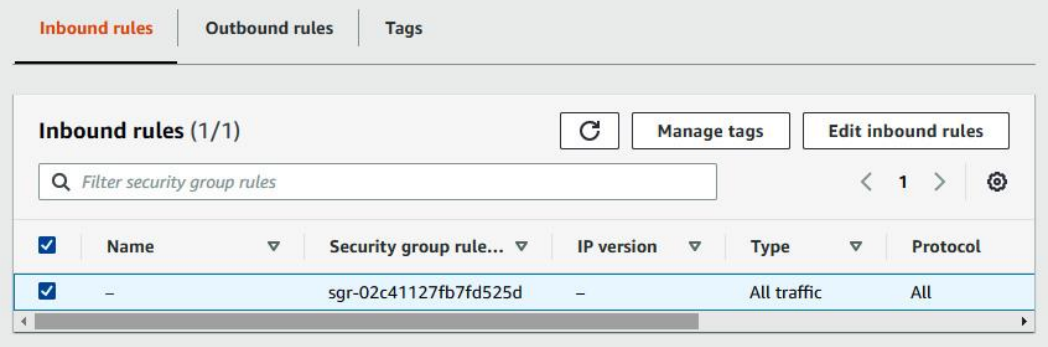

Figure 4.28 – AWS Inbound rules

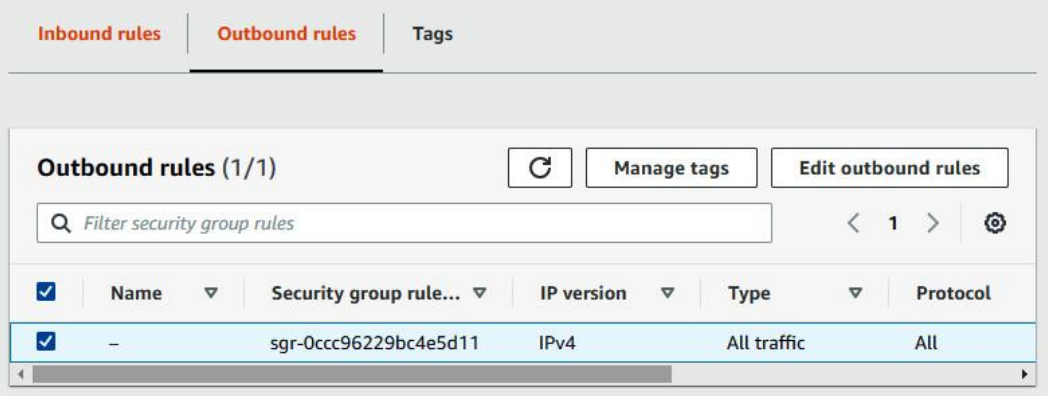

Figure 4.29 – AWS Outbound rules

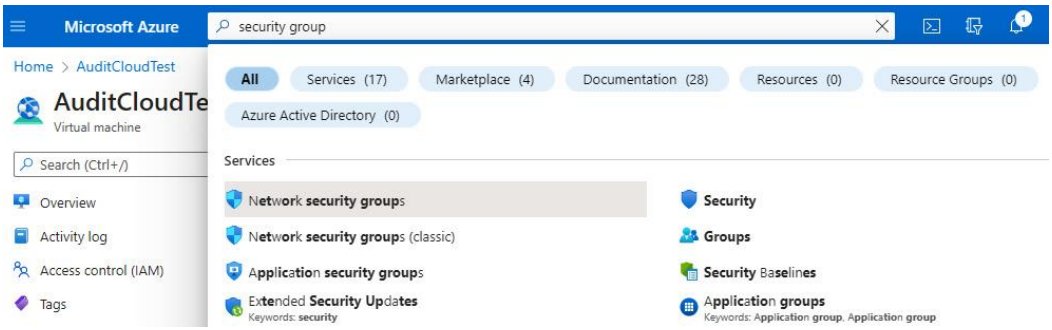

Figure 4.30 – Azure security group search

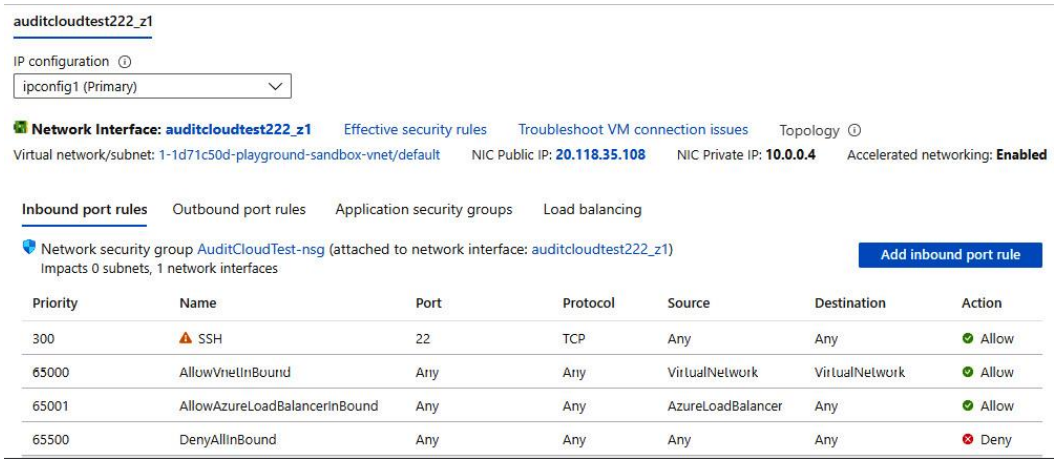

Figure 4.31 – Azure NSG – Inbound port rules

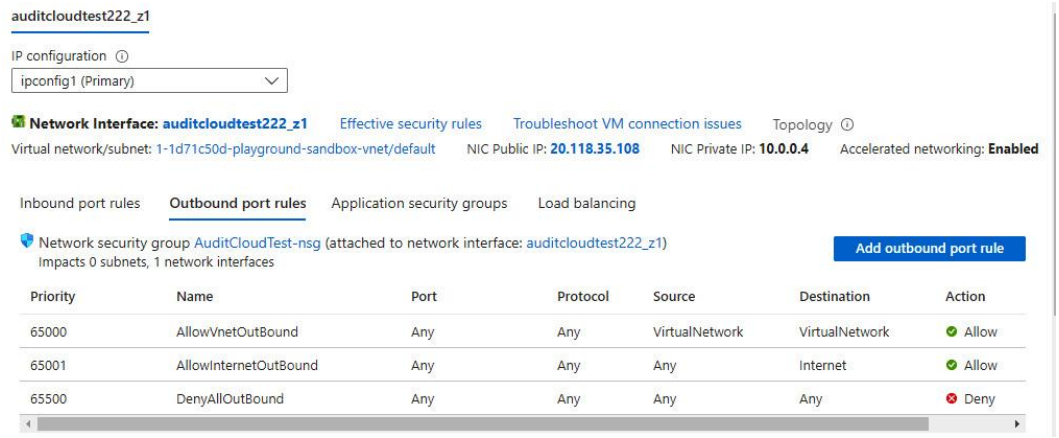

Figure 4.32 – Azure NSG – Outbound port rules

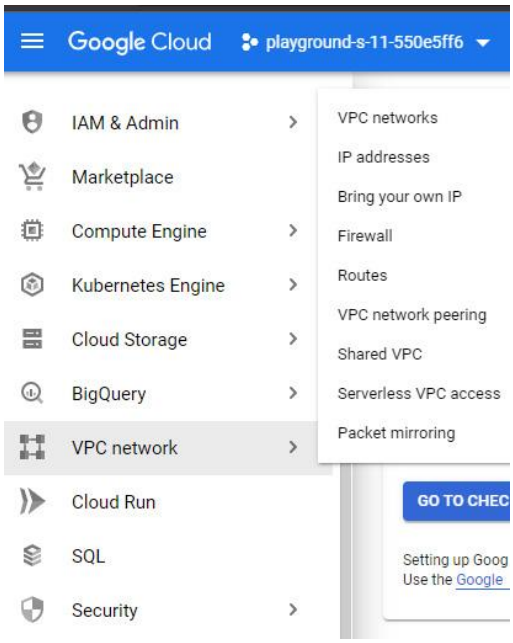

Figure 4.33 – Google Cloud Console

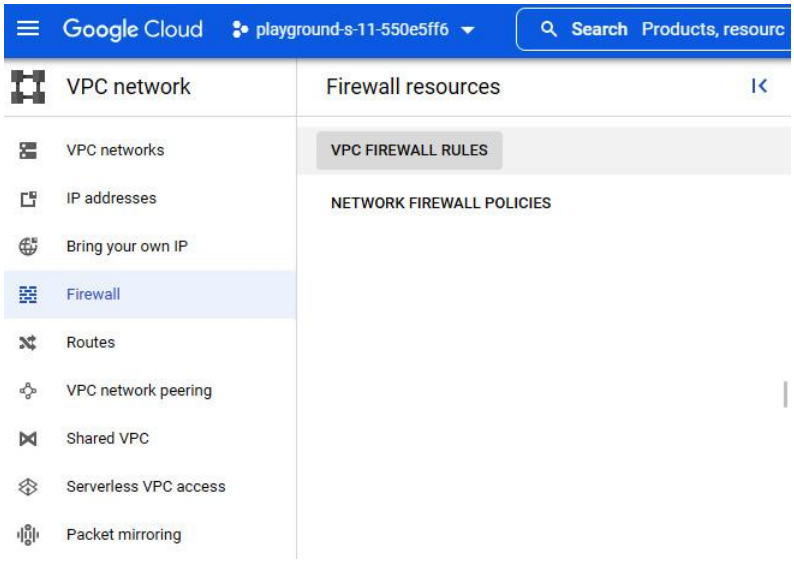

Figure 4.34 – GCP VPC – Firewall resources

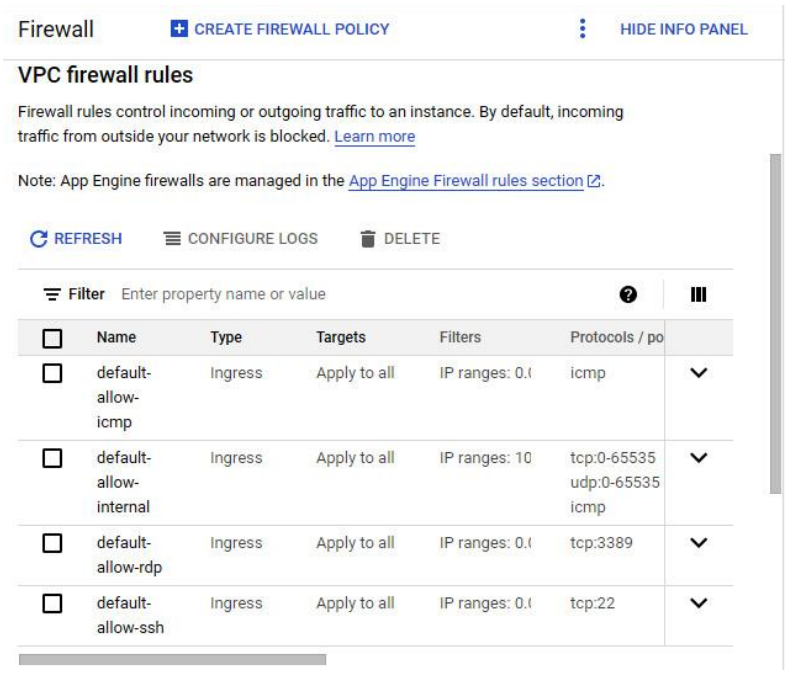

Figure 4.35 – GCP – VPC firewall rules

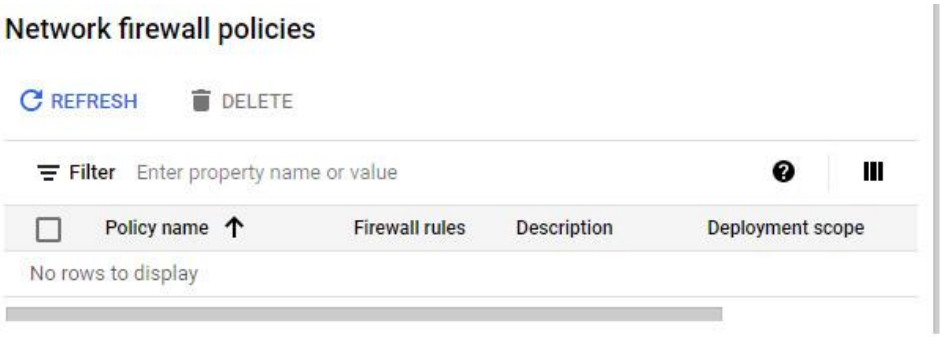

Figure 4.36 – GCP VPC – Network firewall policies

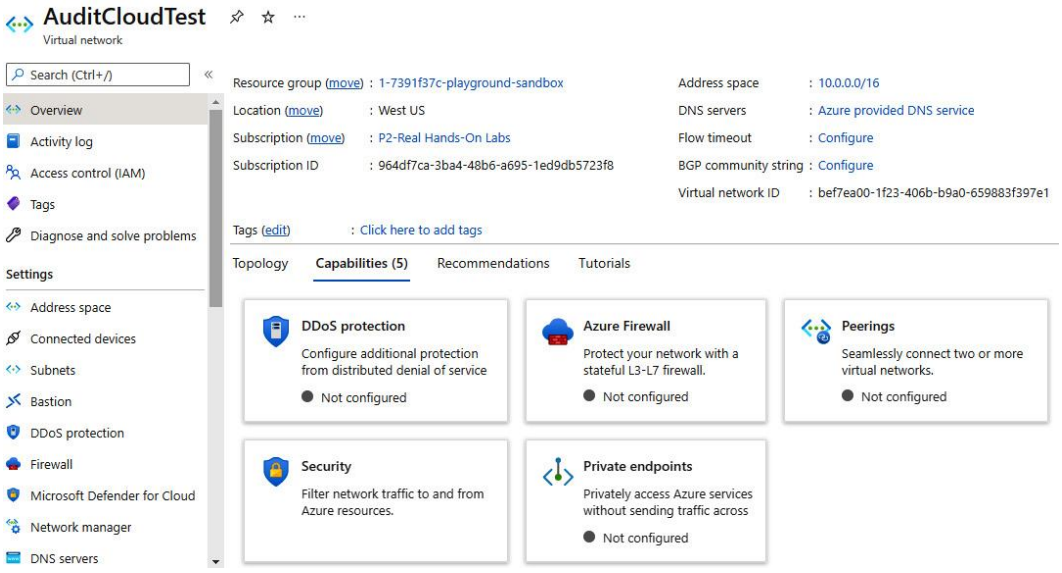

Figure 4.37 – Azure VNet – Capabilities

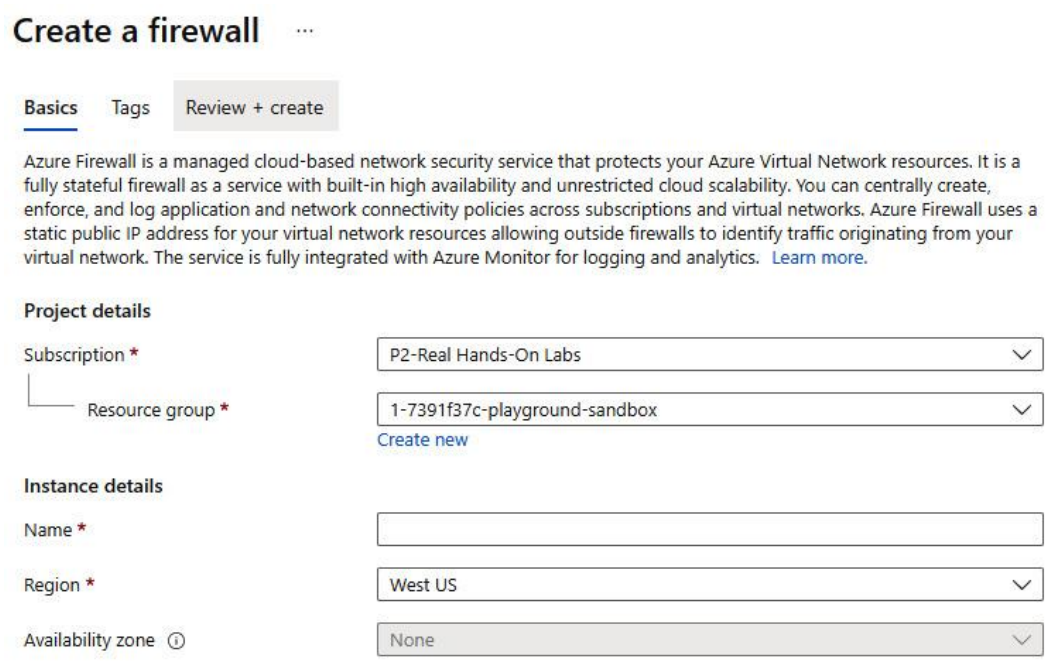

Figure 4.38 – Azure VNet – Create a firewall

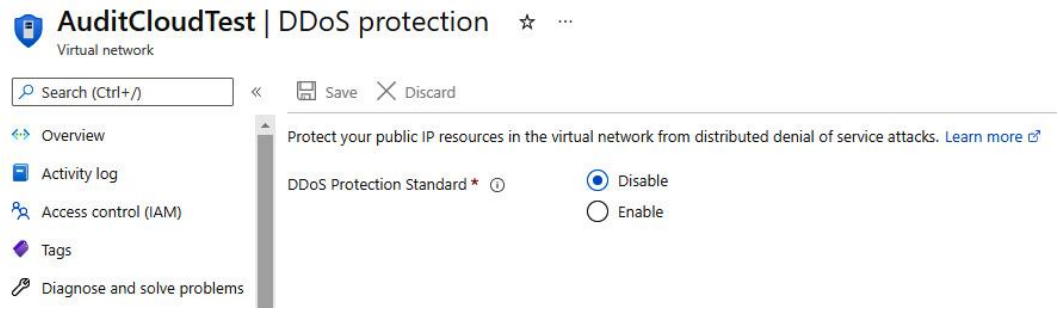

Figure 4.39 – Azure VNet – DDos protection

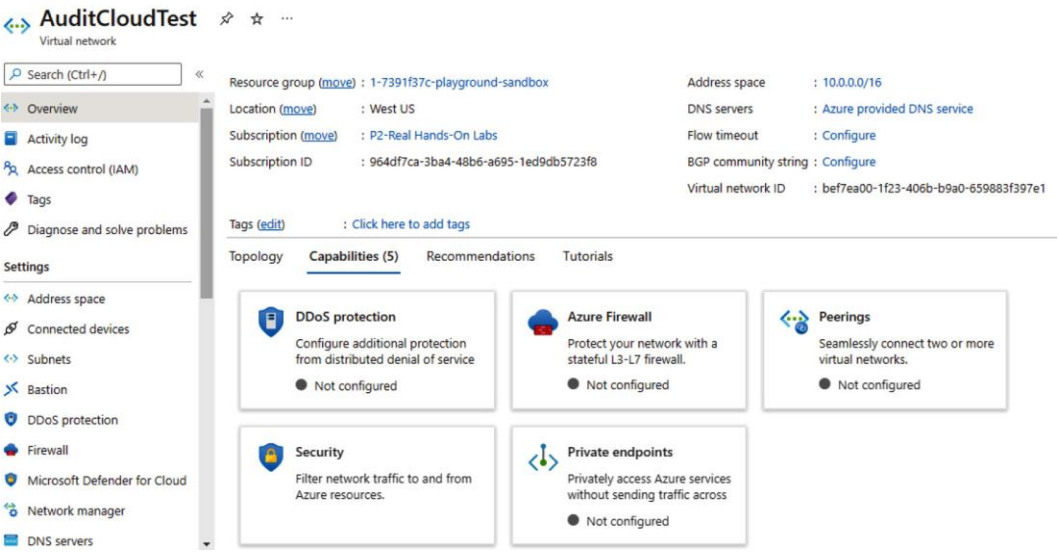

Figure 4.40 – Azure VNet – Peerings

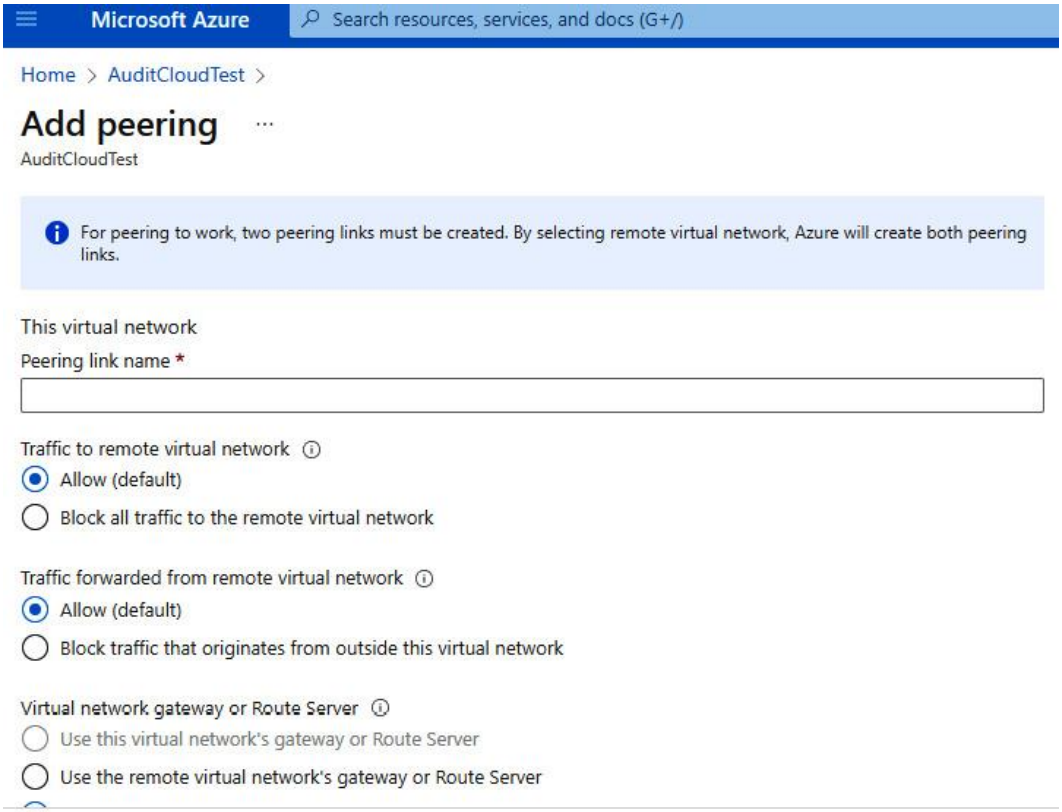

Figure 4.41 – Azure VNet – Add peering

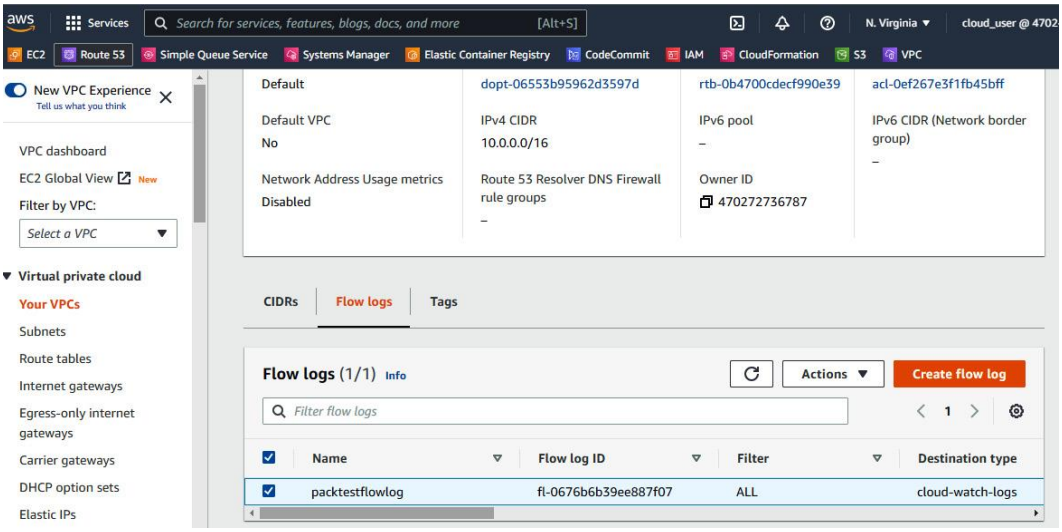

Figure 4.42 – AWS VPC – Flow logs

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

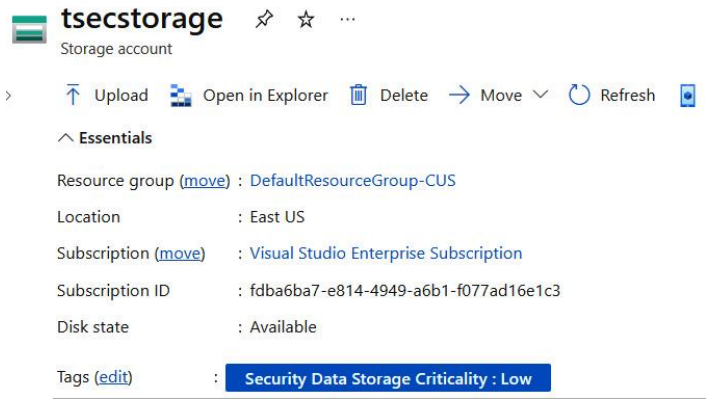

Figure 5.1 – Example Microsoft Azure resource tagging

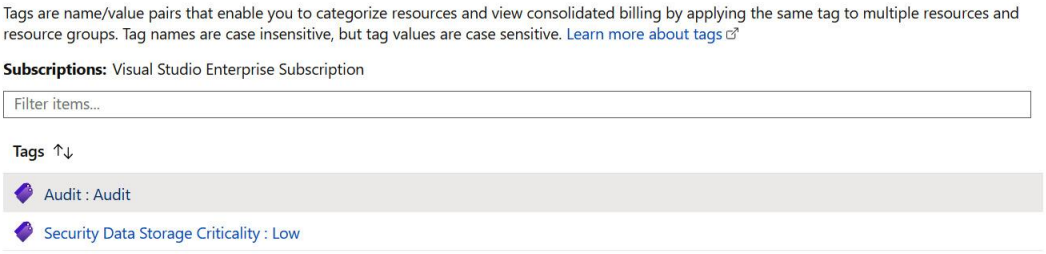

Figure 5.2 – Microsoft Azure key-value tag pairing

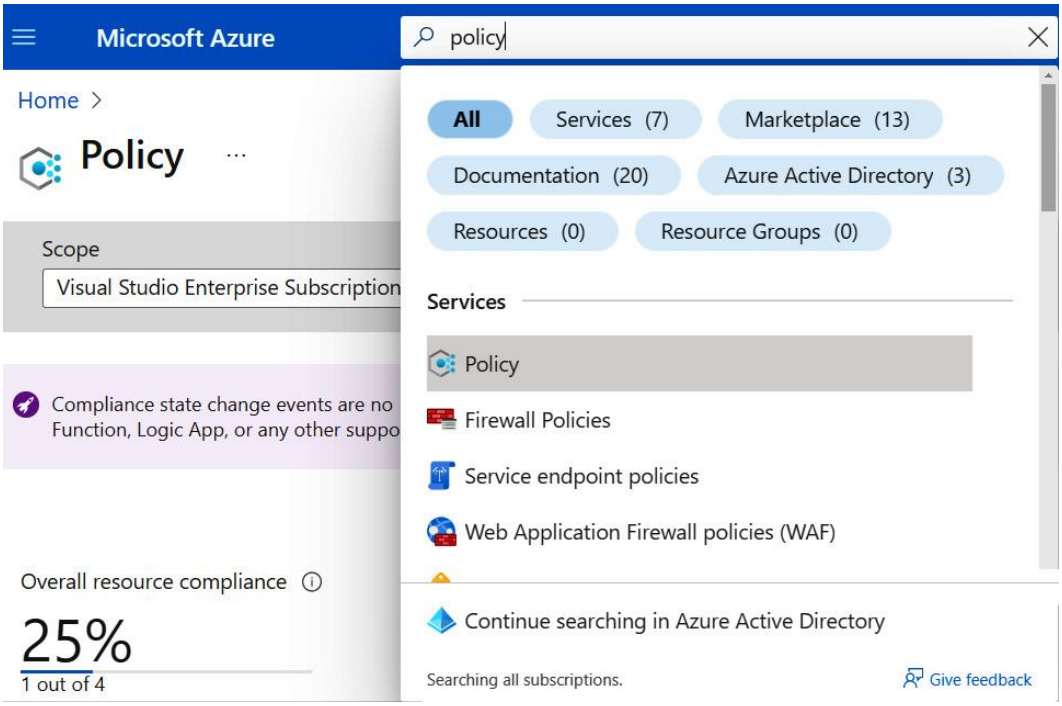

Figure 5.3 – Microsoft Azure Policy blade

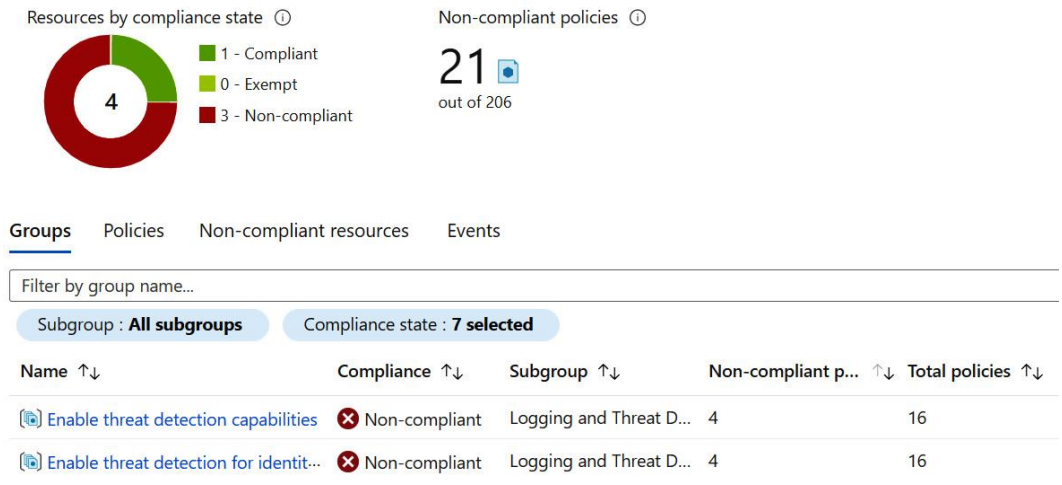

Figure 5.4 – Microsoft Azure Policy blade

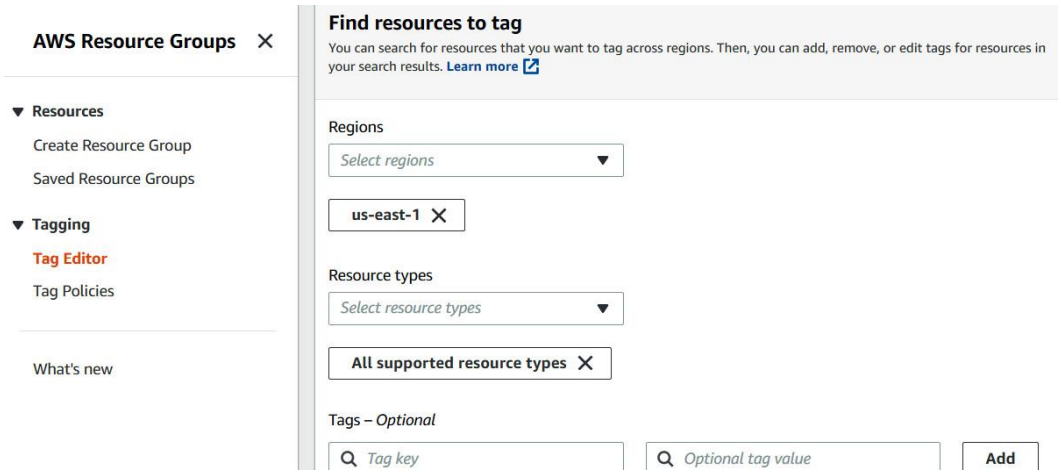

Figure 5.5 – AWS Resource Groups and tagging

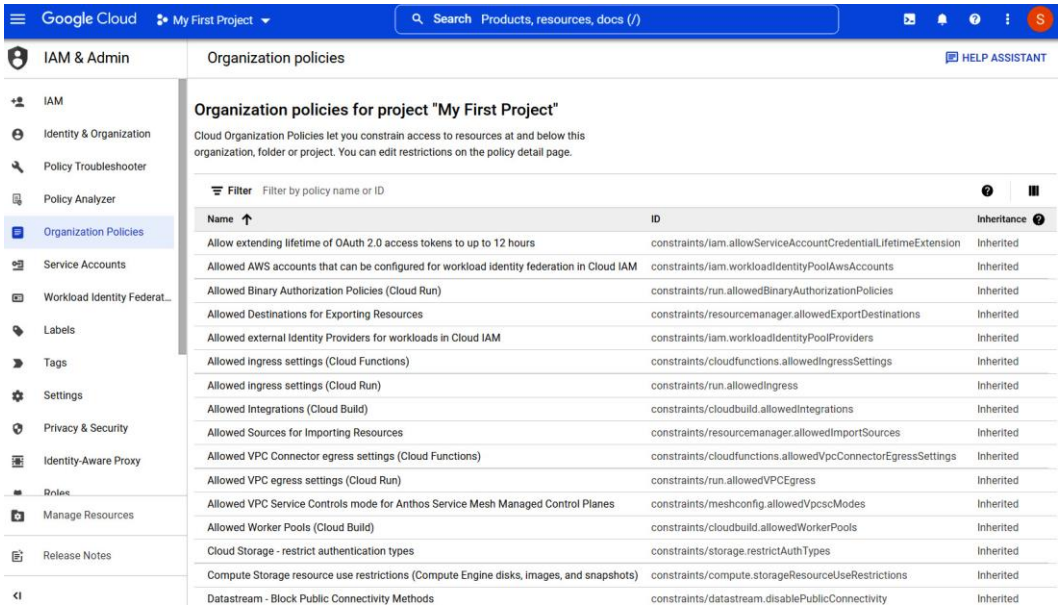

Figure 5.6 – Google Cloud Platform organizational-level policies

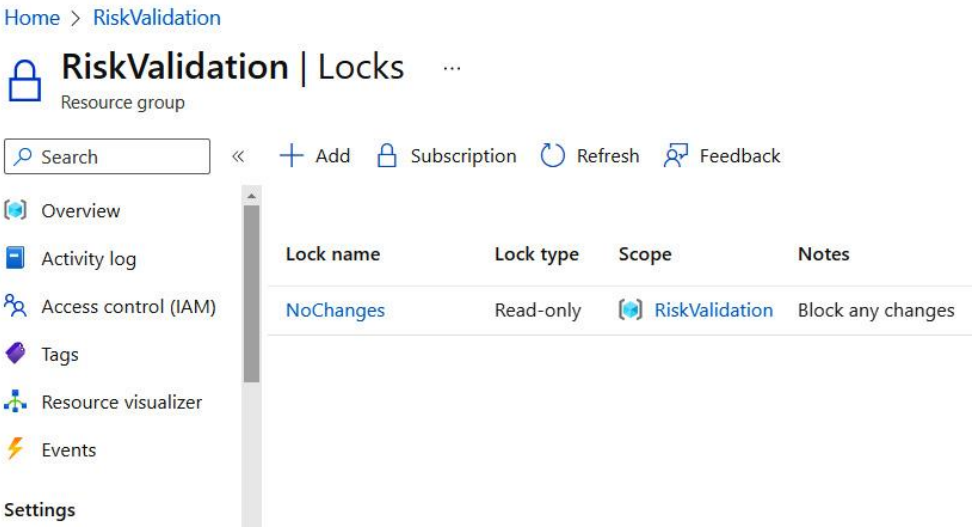

Figure 5.7 – Example Microsoft Azure read-only lock applied

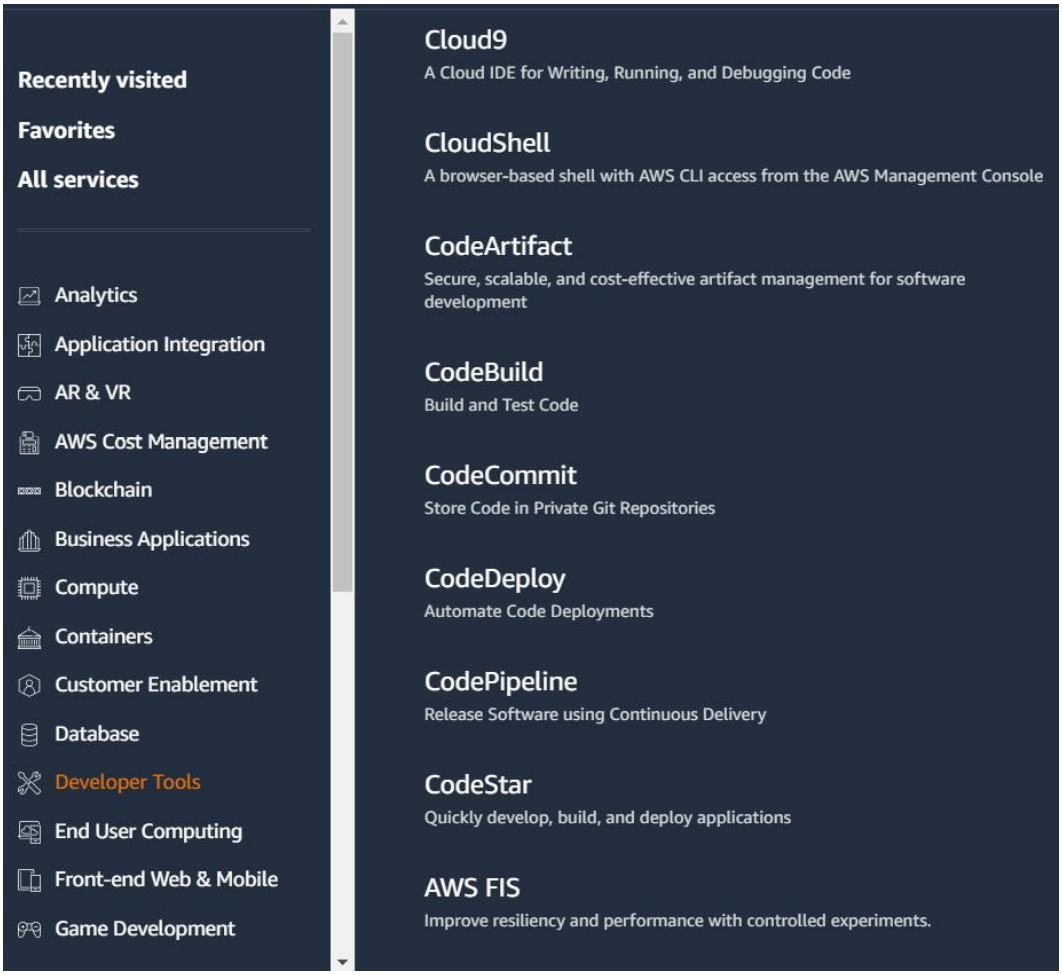

Figure 5.8 – AWS Developer Tools

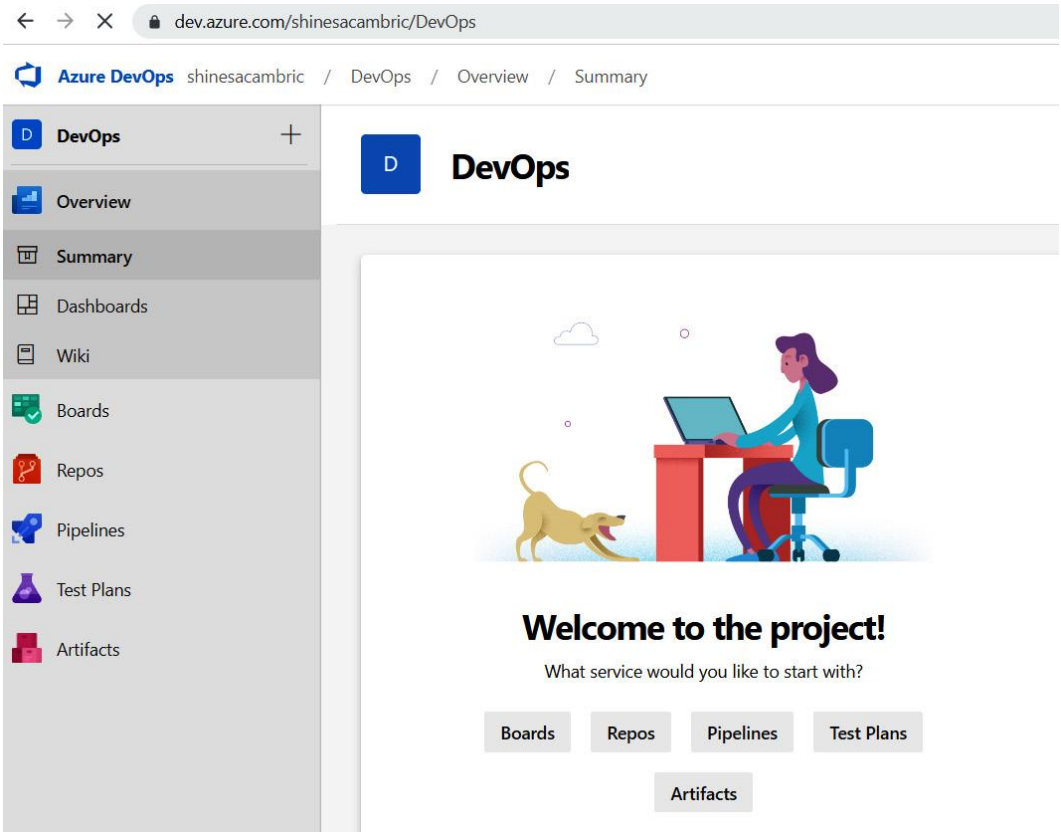

Figure 5.9 – Microsoft Azure DevOps

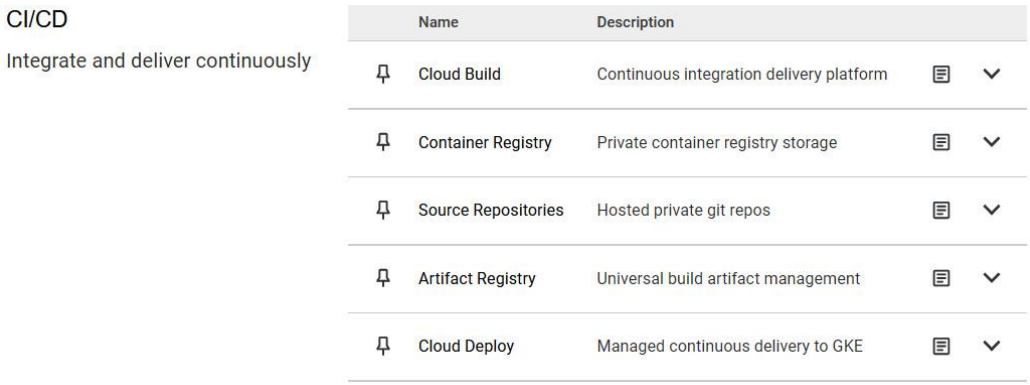

Figure 5.10 – Google Cloud Platform CI/CD features

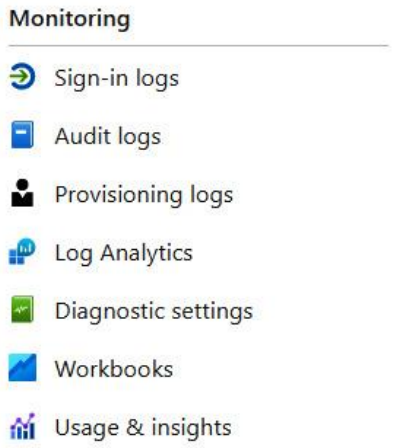

Figure 5.11 – Azure Monitoring

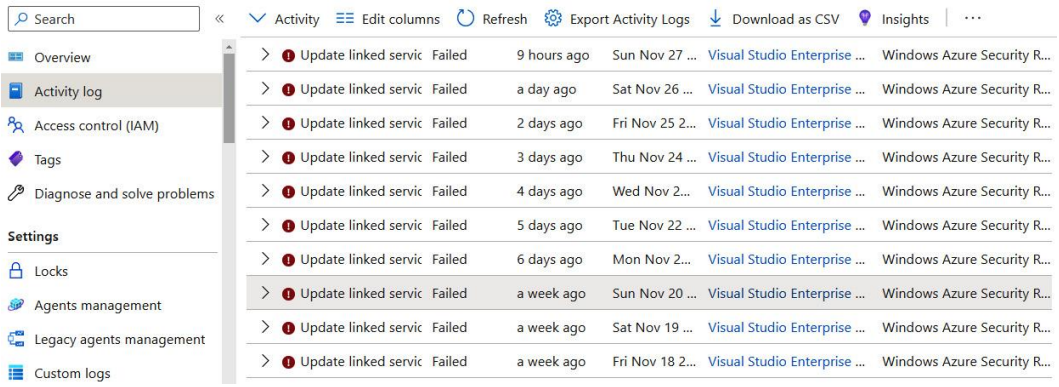

Figure 5.12 – Microsoft Azure Activity log for a resource

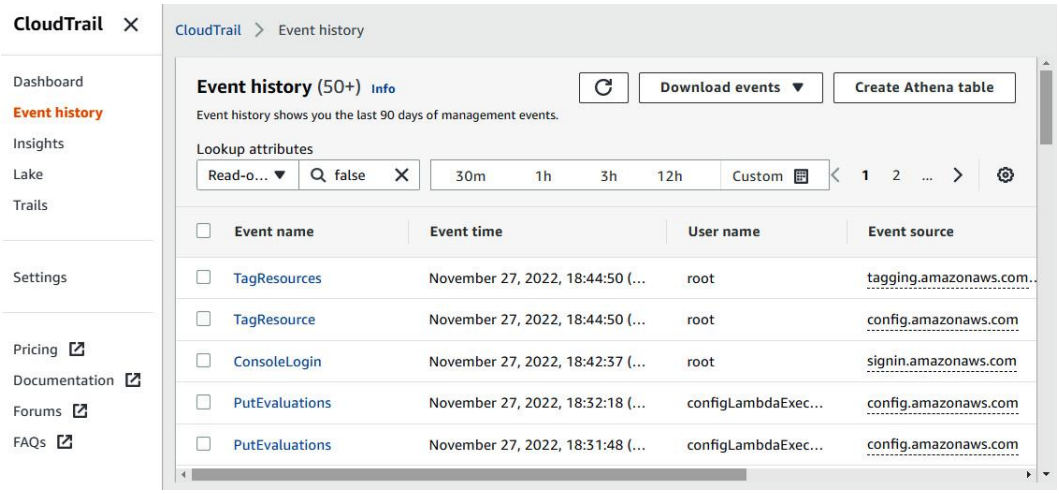

Figure 5.13 – AWS CloudTrail

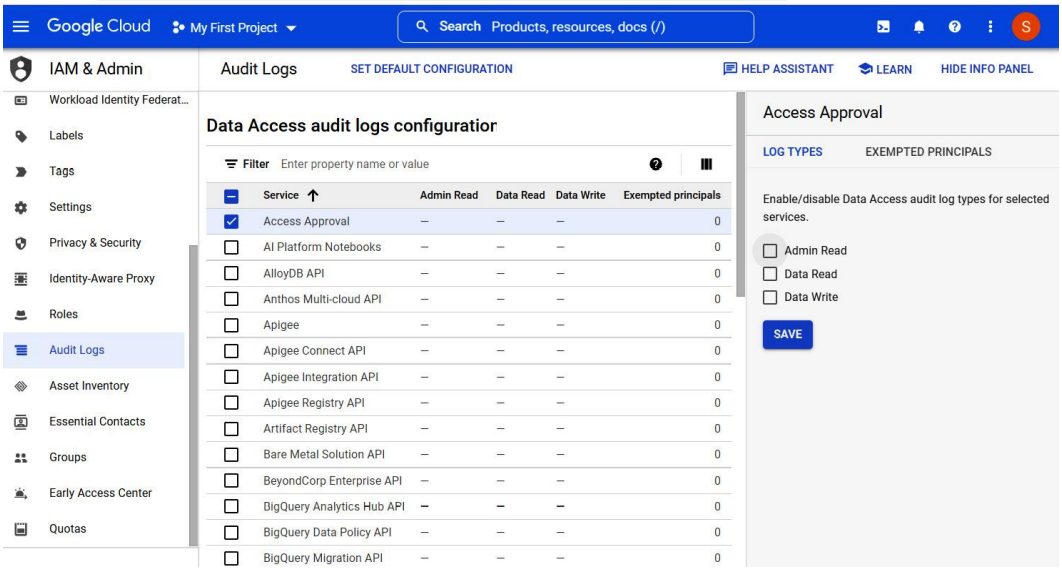

Figure 5.14 – Google Cloud audit log configuration

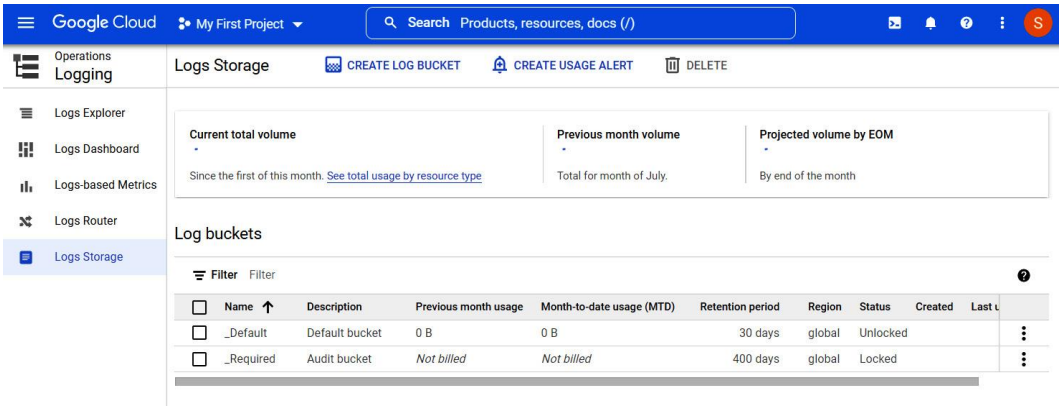

Figure 5.15 – Google Cloud audit log storage configuration

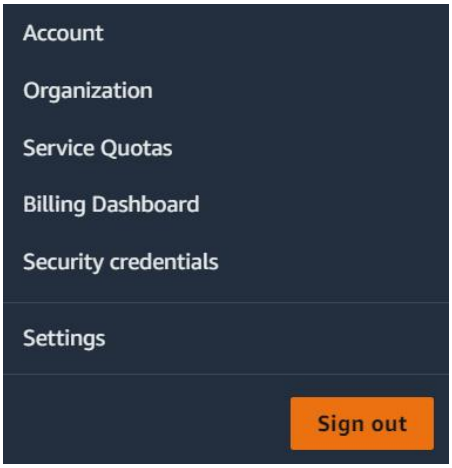

Figure 5.16 – AWS navigation to Service Quotas and Billing Dashboard

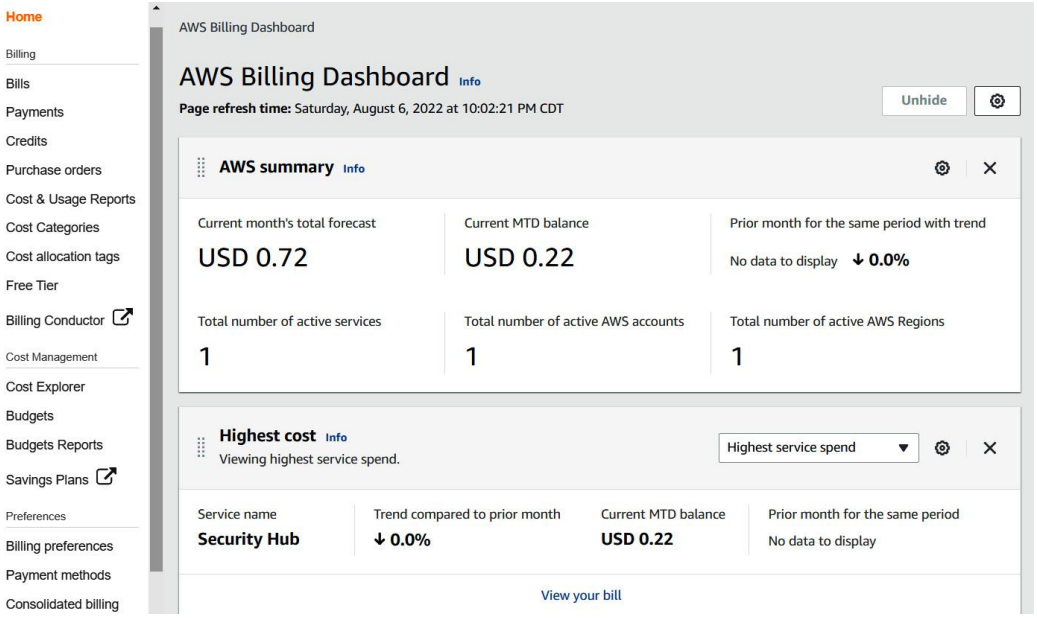

Figure 5.17 – AWS Billing Dashboard

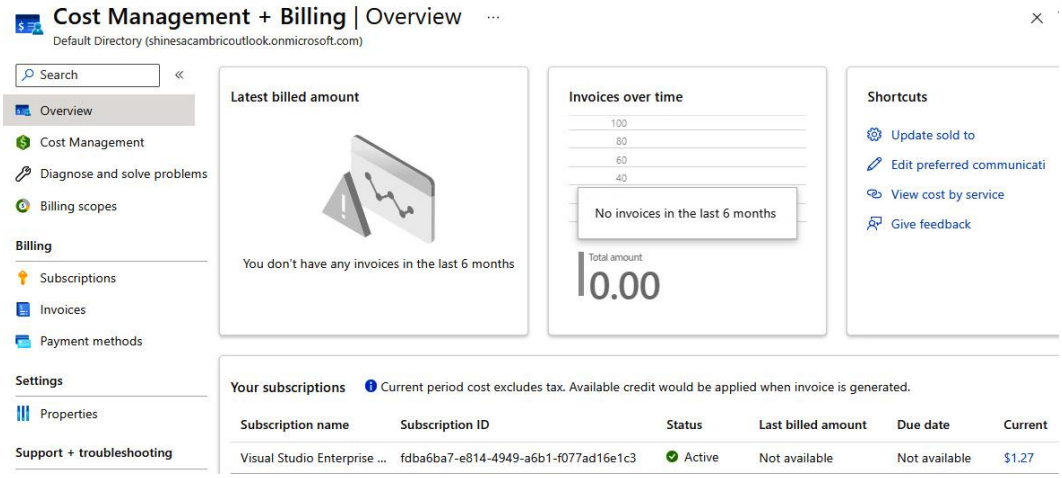

Figure 5.18 – Azure navigation to Cost Management + Billing

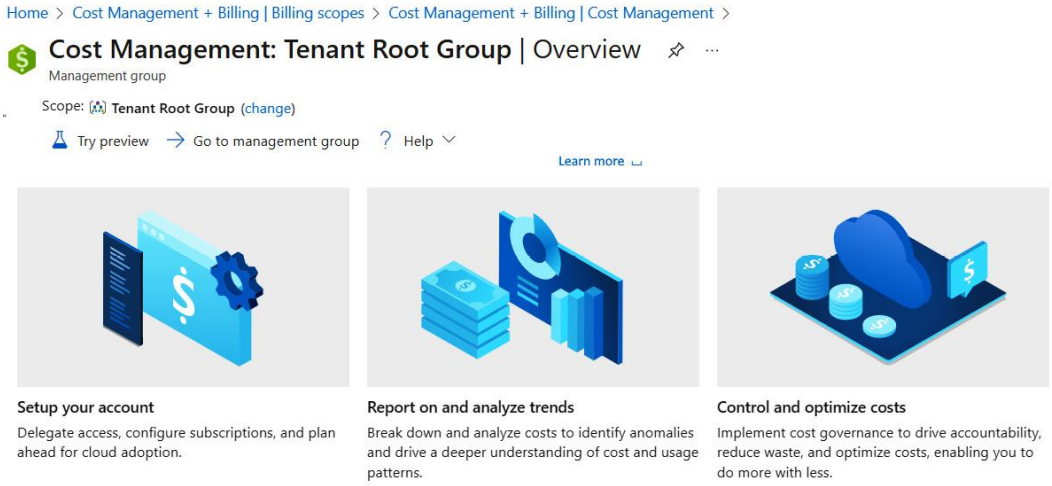

Figure 5.19 – Azure Cost Management + Billing

Figure 5.20 – Azure – Create budget

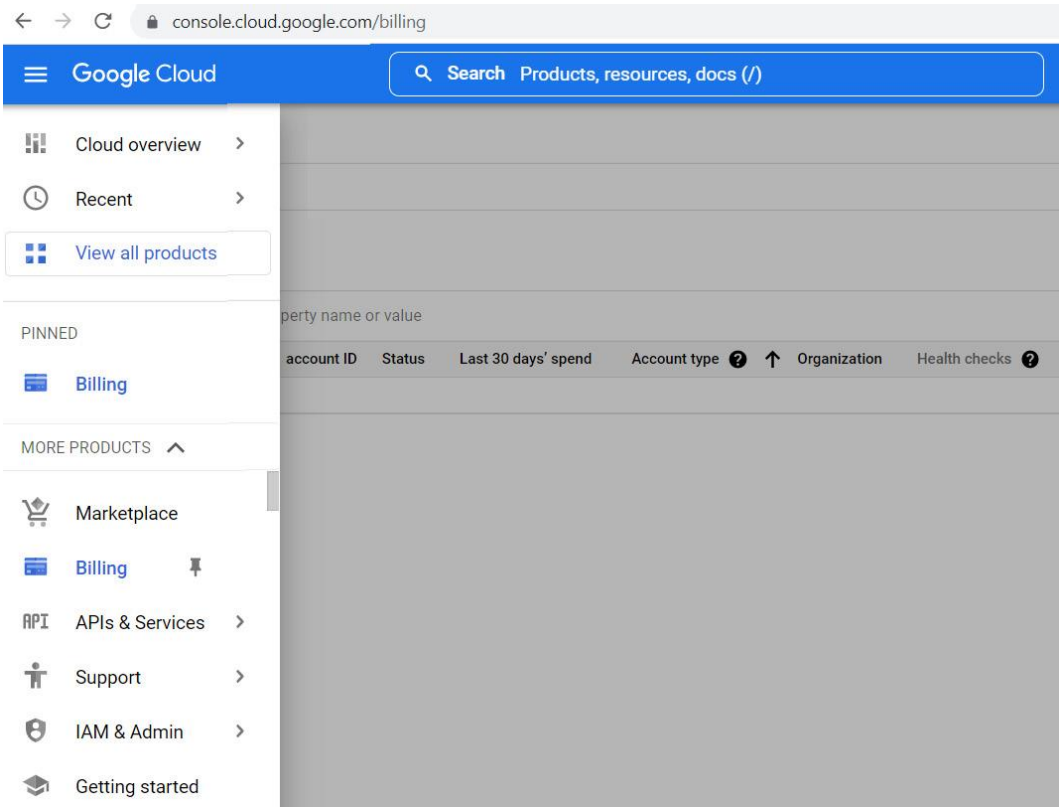

Figure 5.21 – Google Cloud Billing

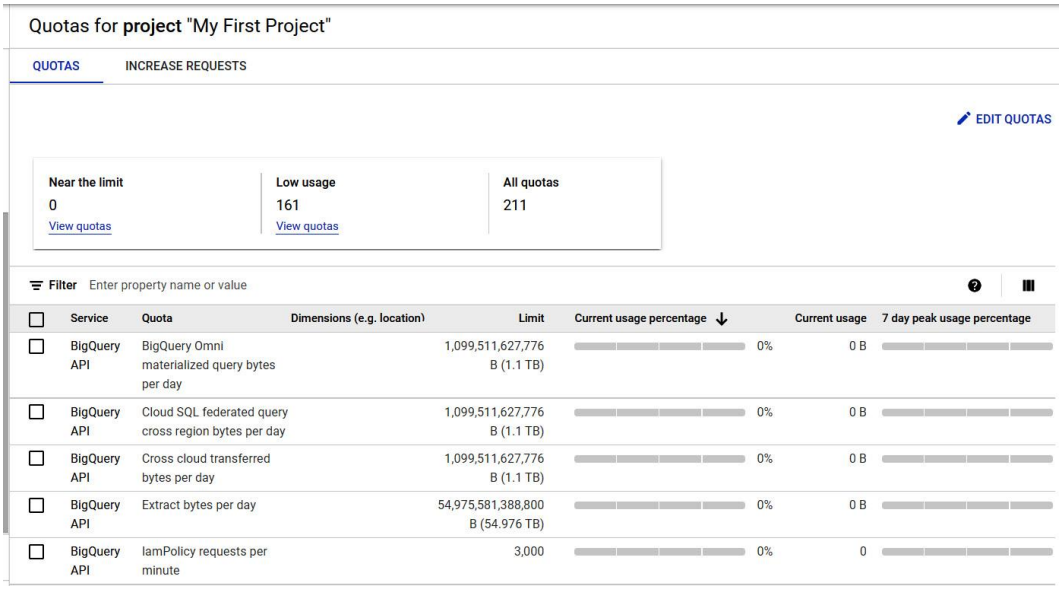

Figure 5.22 – Google Cloud quota increase

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/blogs/opensource/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

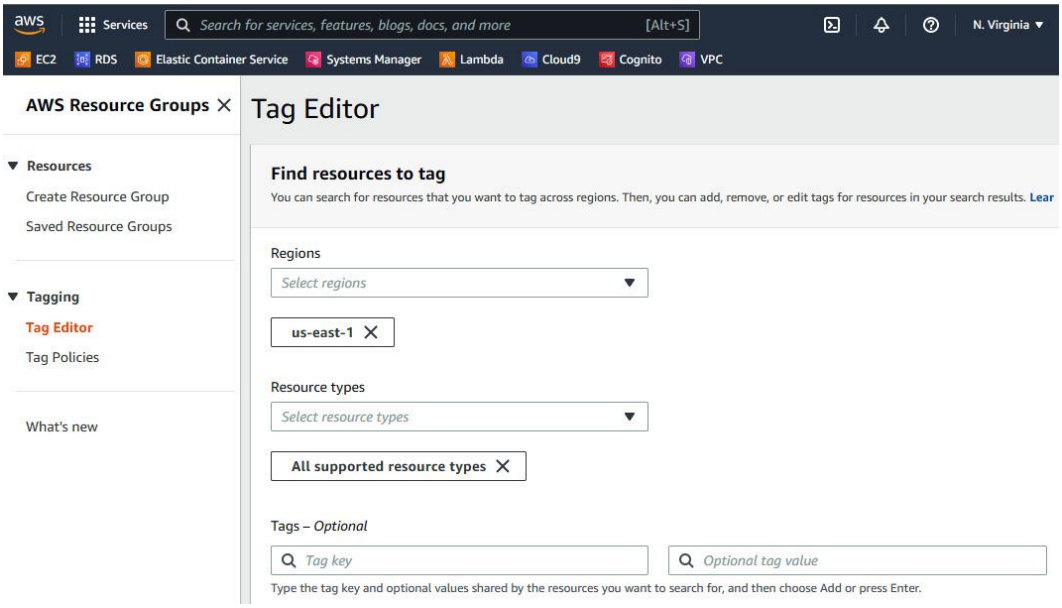

Figure 6.1 – Finding resources to tag

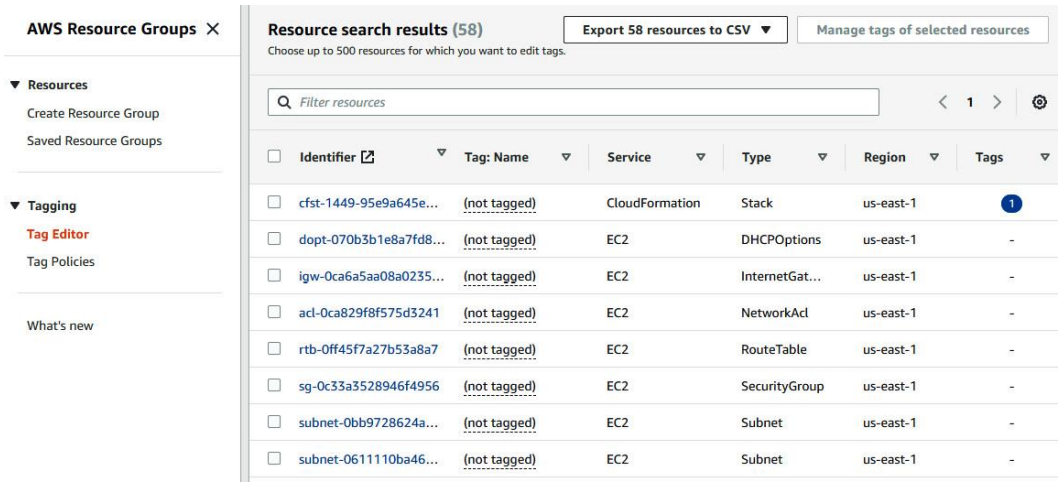

Figure 6.2 – Resource search results

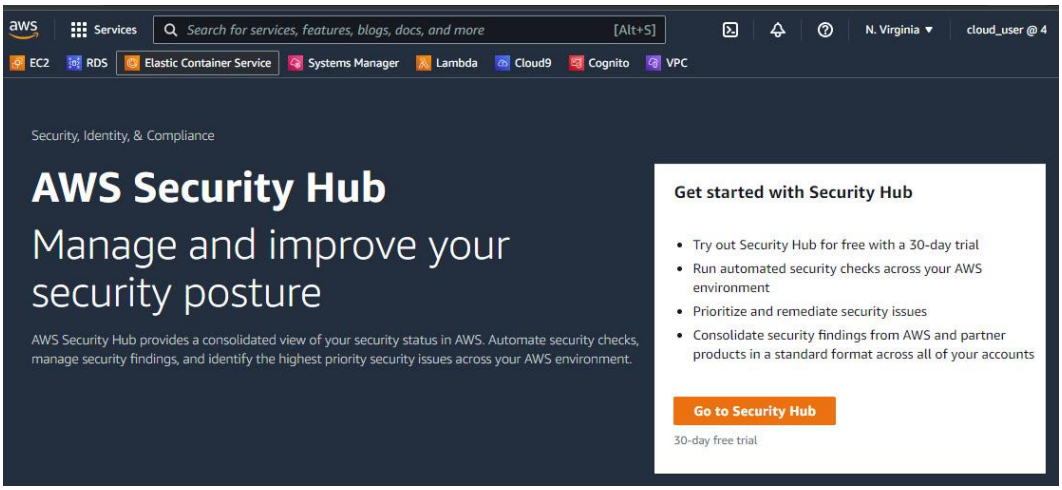

Figure 6.3 – AWS Security Hub

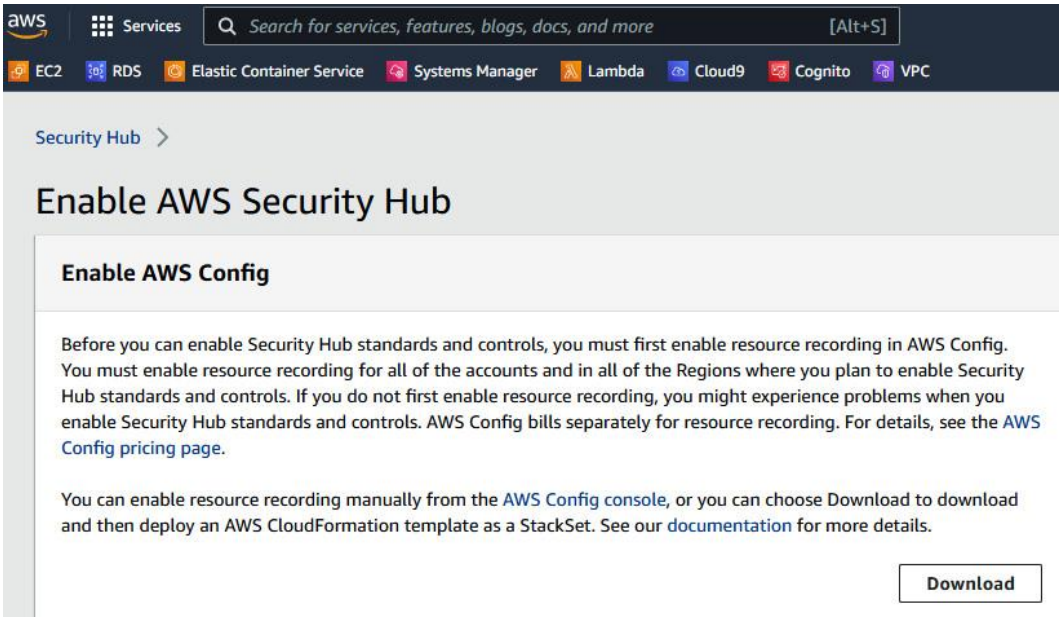

Figure 6.4 – Enabling AWS Config

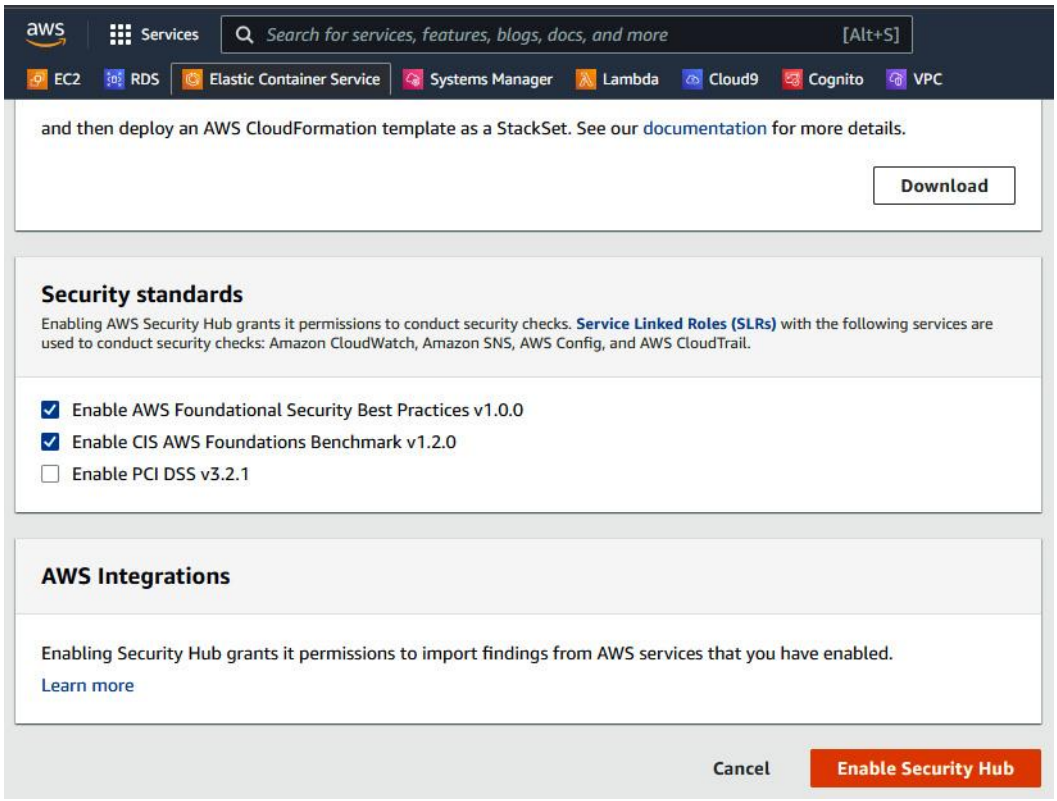

Figure 6.5 – Security standards

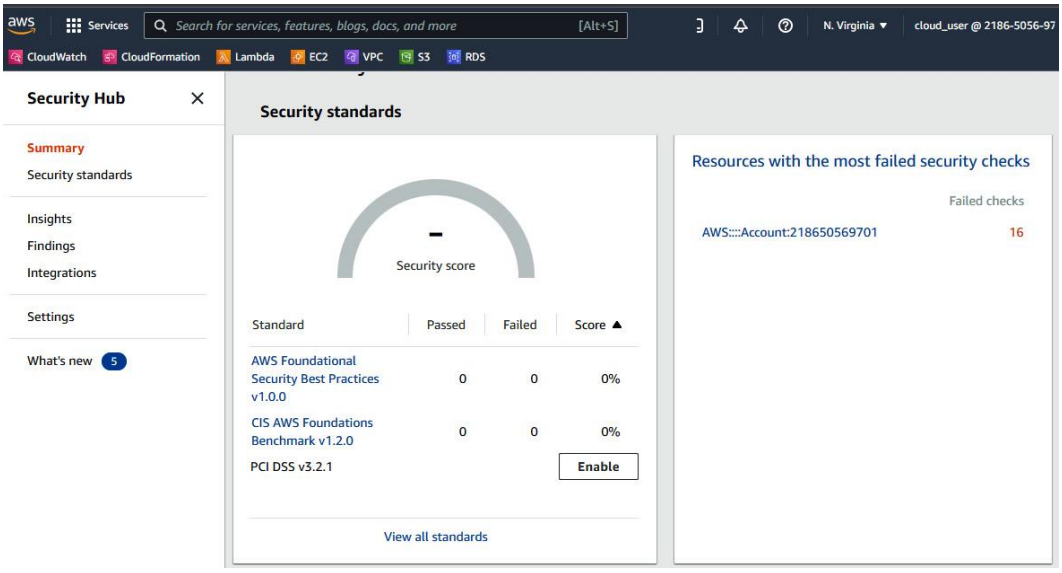

Figure 6.6 – The Summary tab

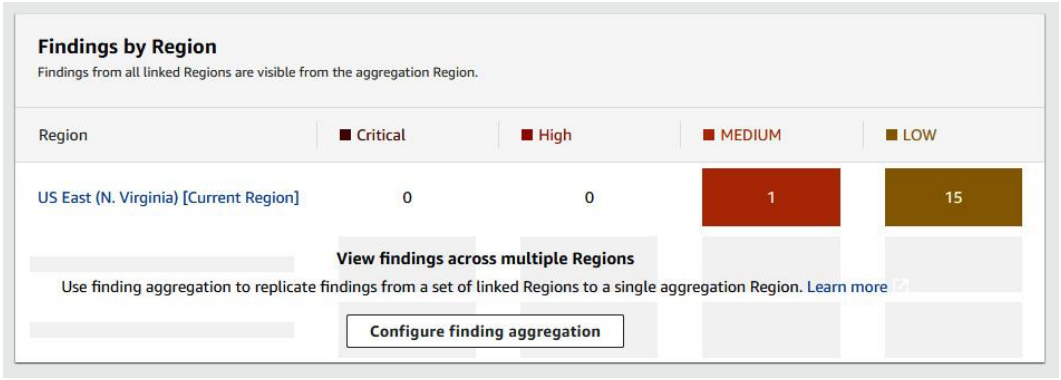

Figure 6.7 – Findings by region

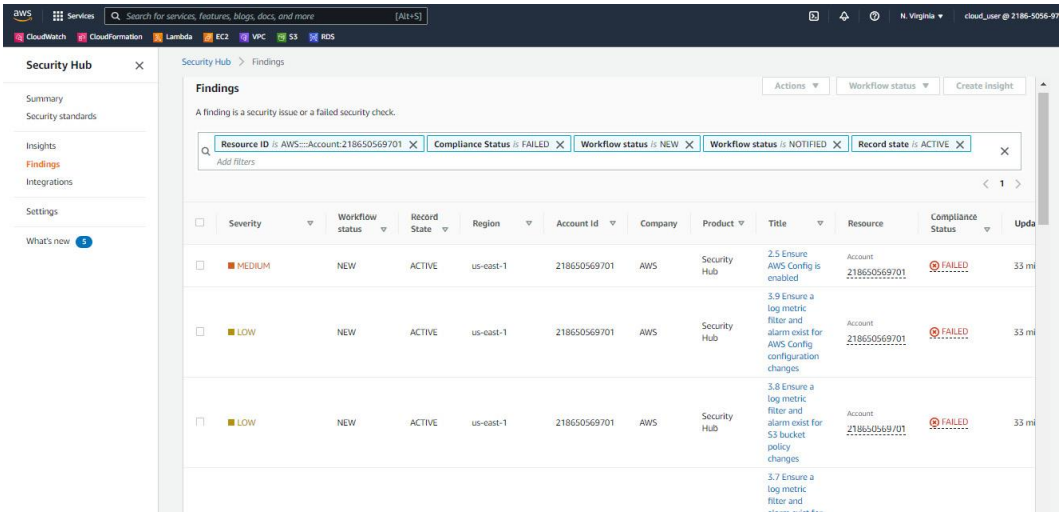

Figure 6.8 – Findings

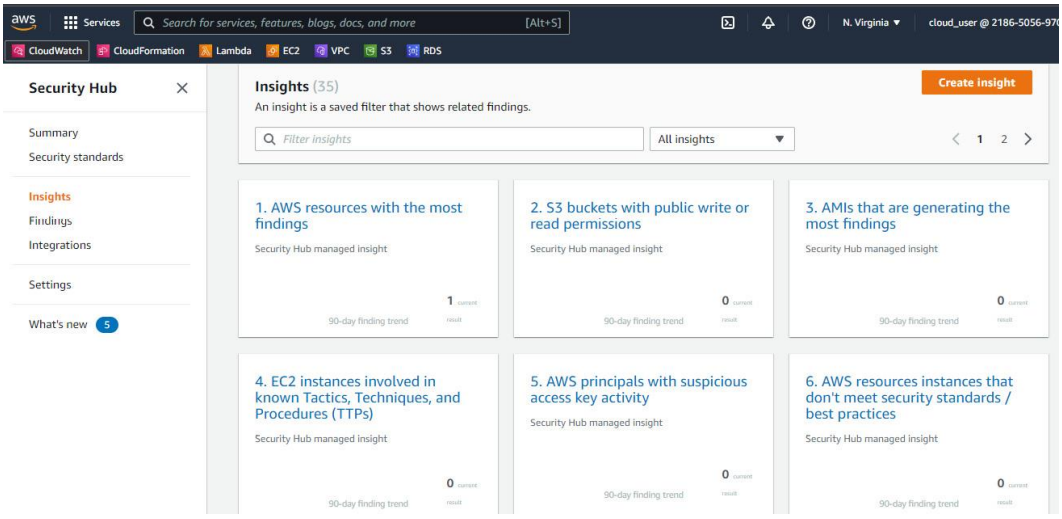

Figure 6.9 – The Insights tab

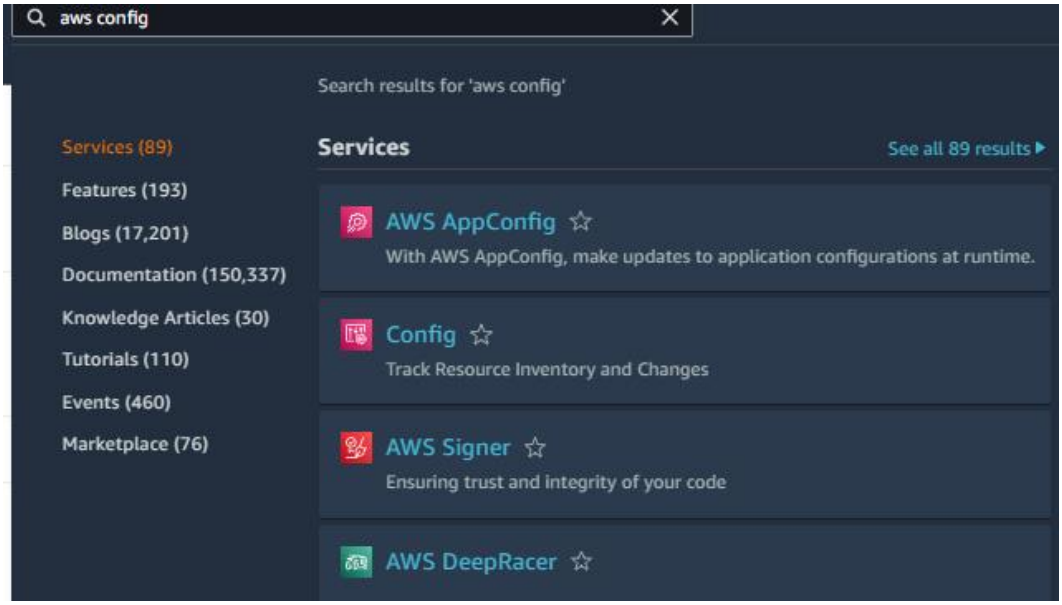

Figure 6.10 – AWS Config search

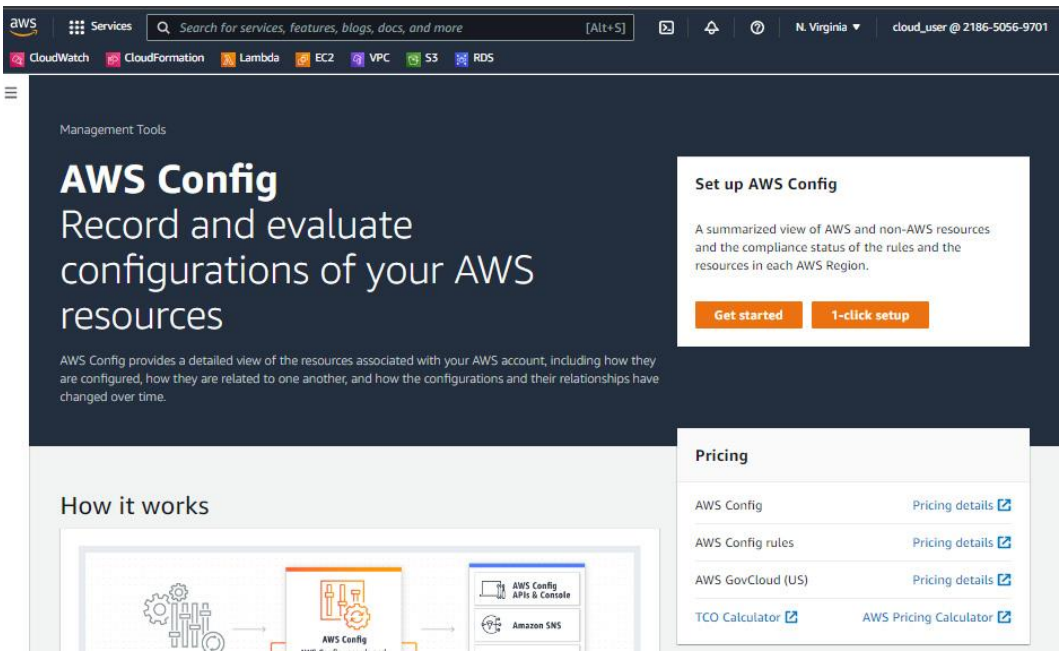

Figure 6.11 - Enabling AWS Config

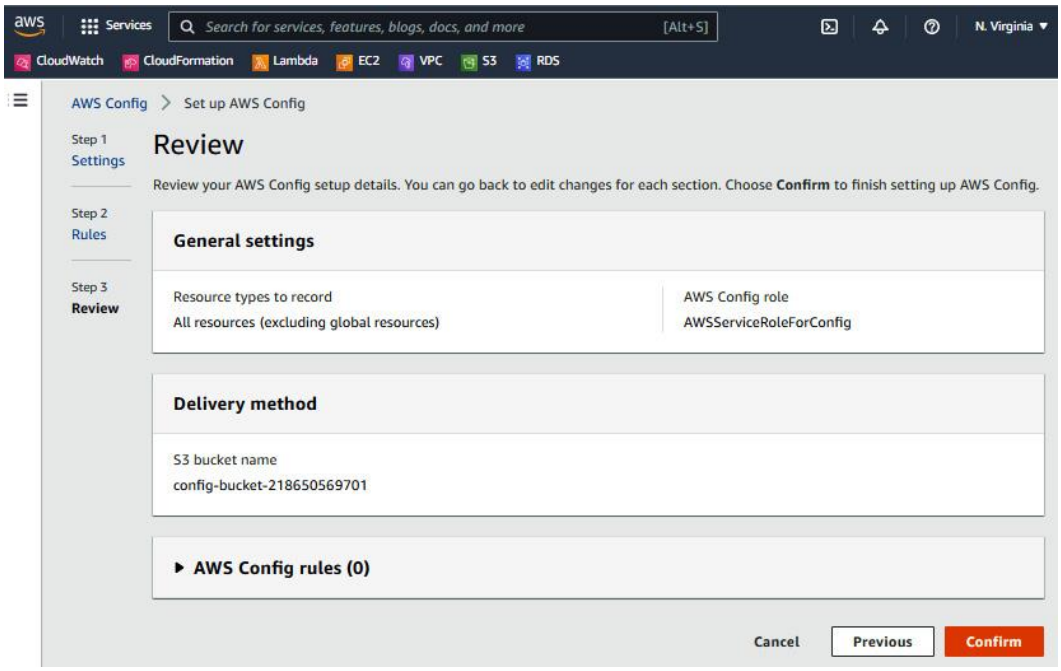

Figure 6.12 – Setting up AWS Config

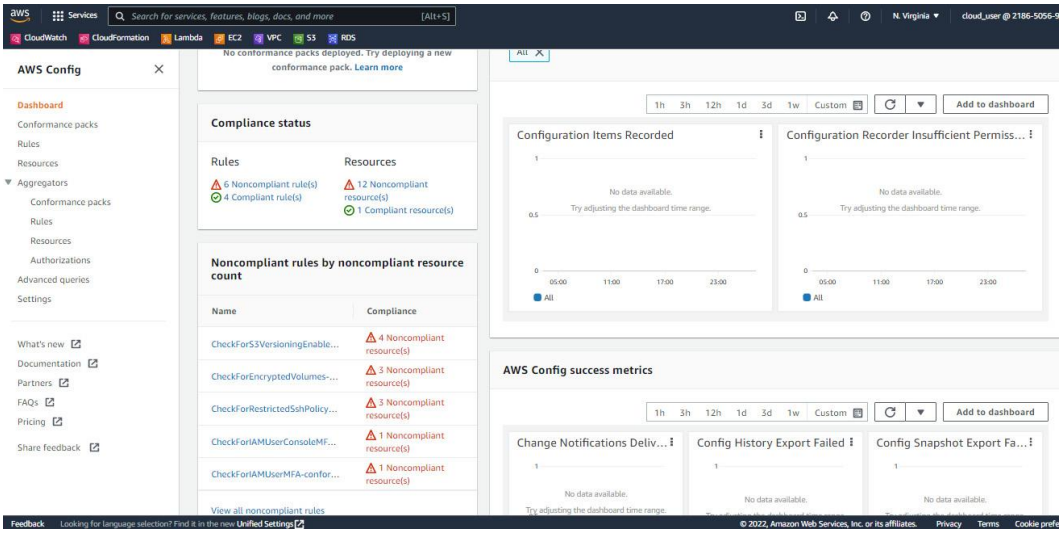

Figure 6.13 – The Dashboard tab

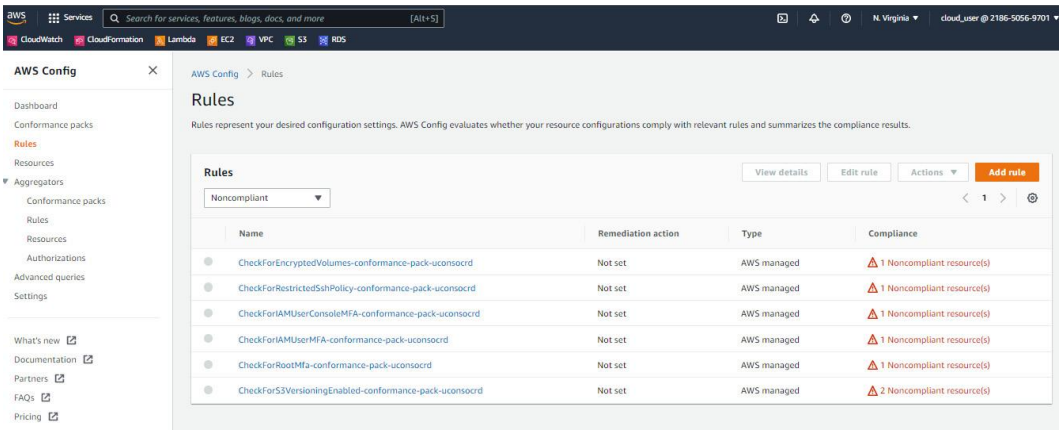

Figure 6.14 – The Rules tab

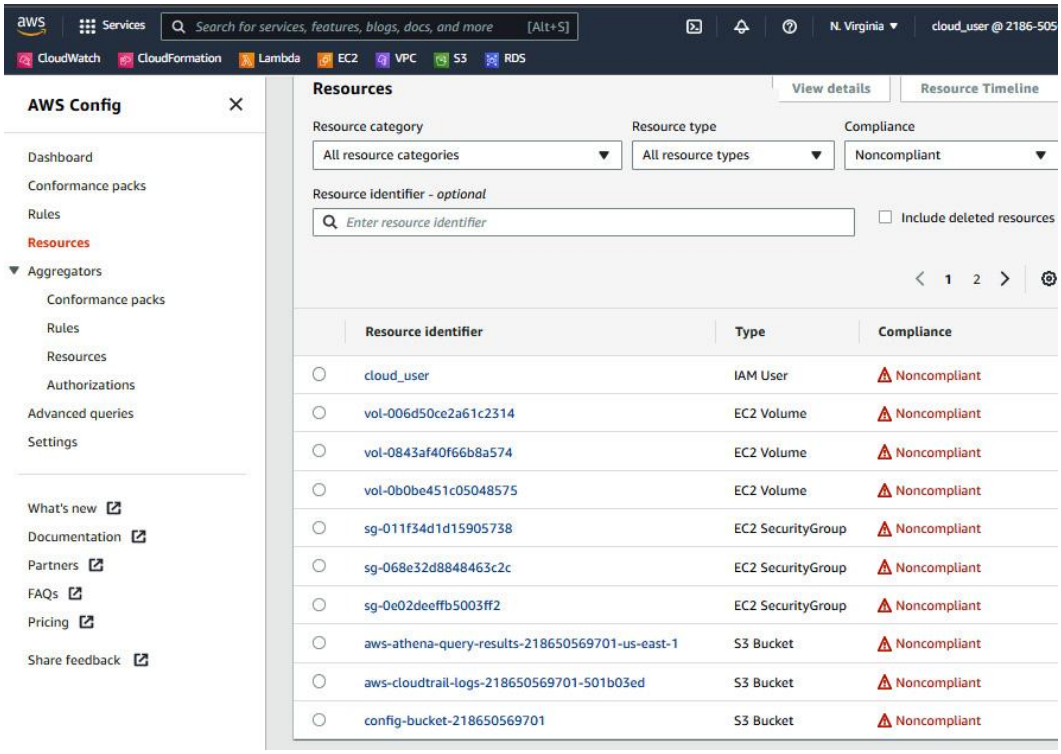

Figure 6.15 – The Resources tab

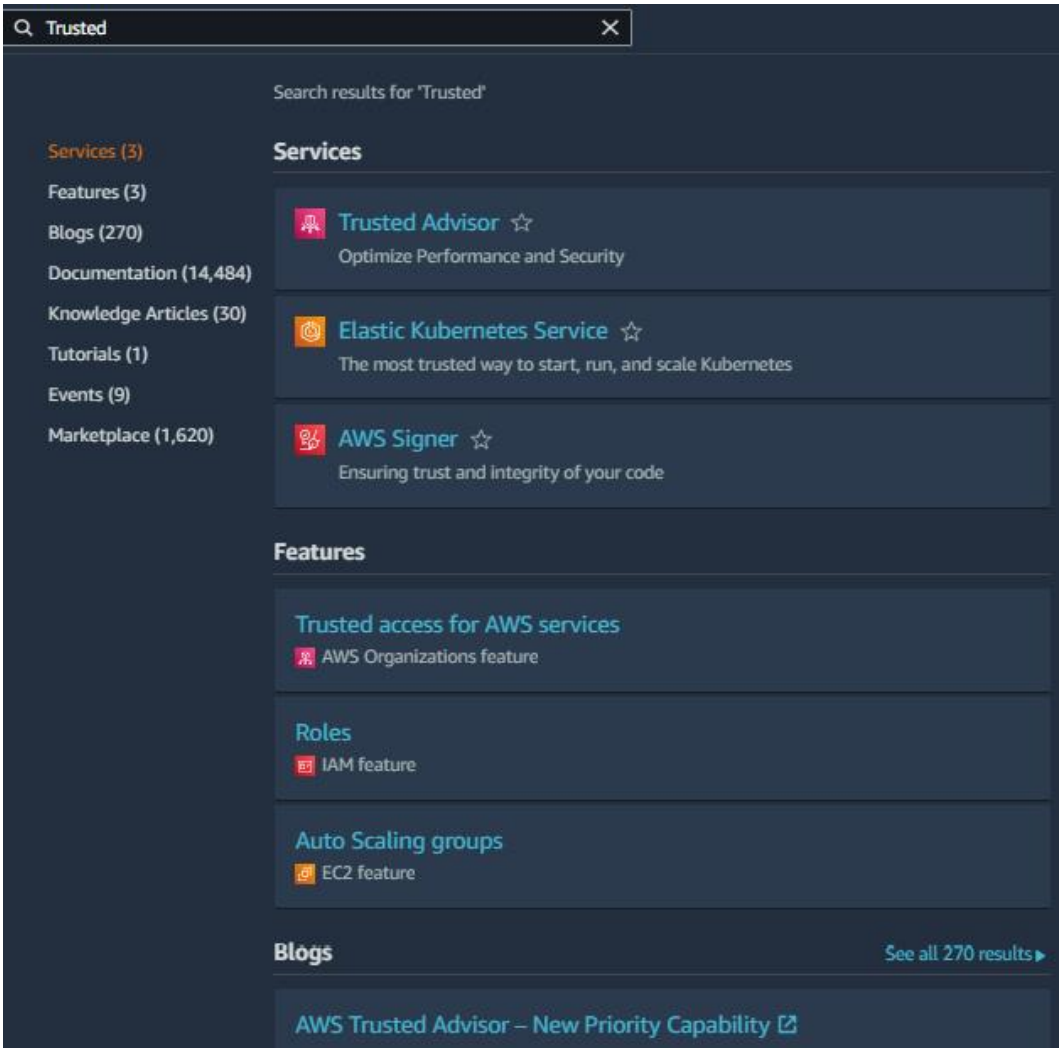

Figure 6.16 – Searching for AWS Trusted Advisor

Figure 6.17 – The AWS Trusted Advisor interface

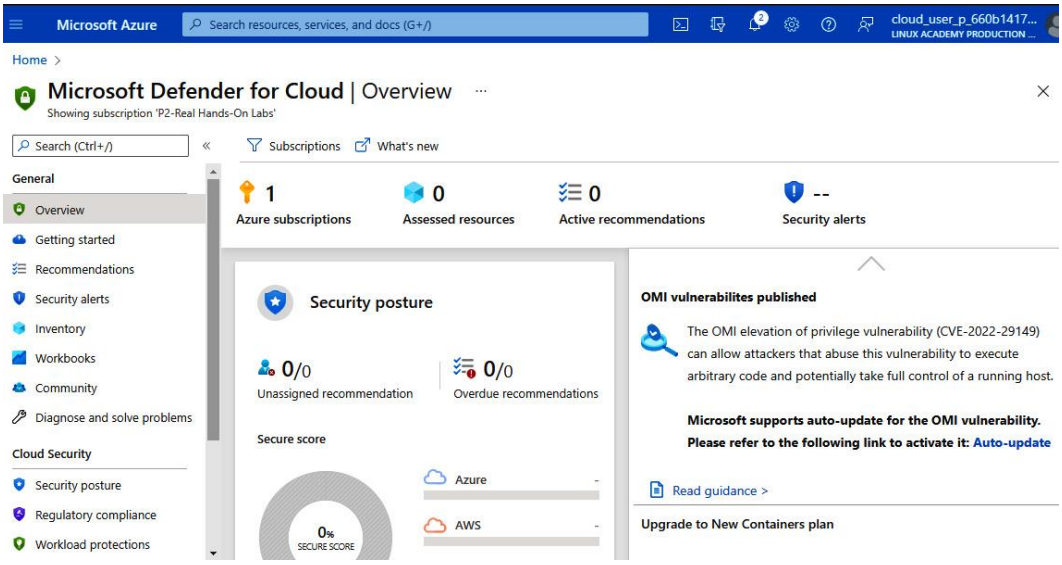

Figure 6.18 – The Overview tab

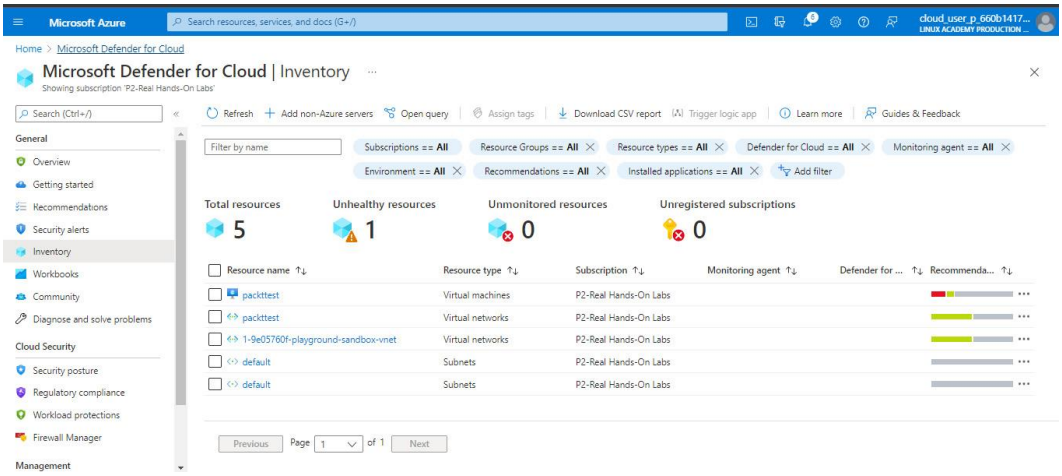

Figure 6.19 – The Inventory tab

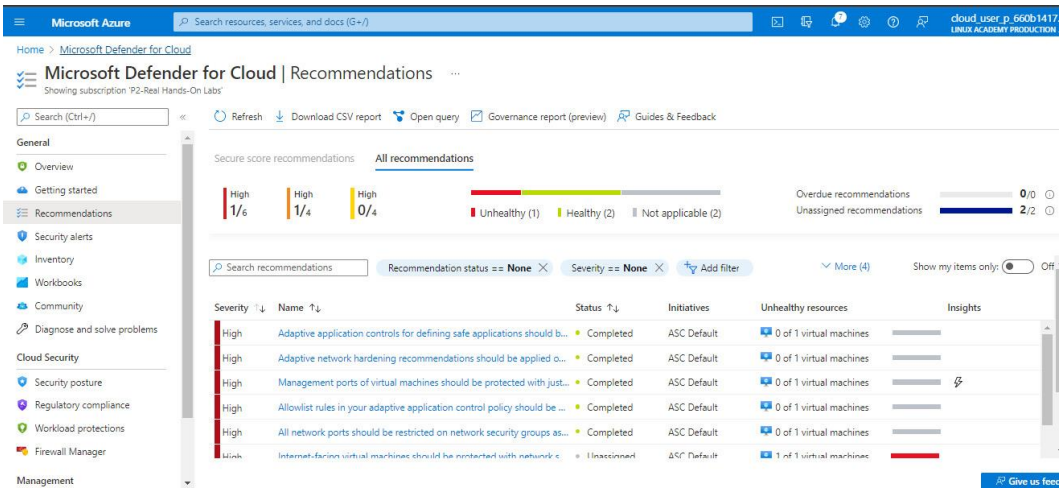

Figure 6.20 – The Recommendations tab

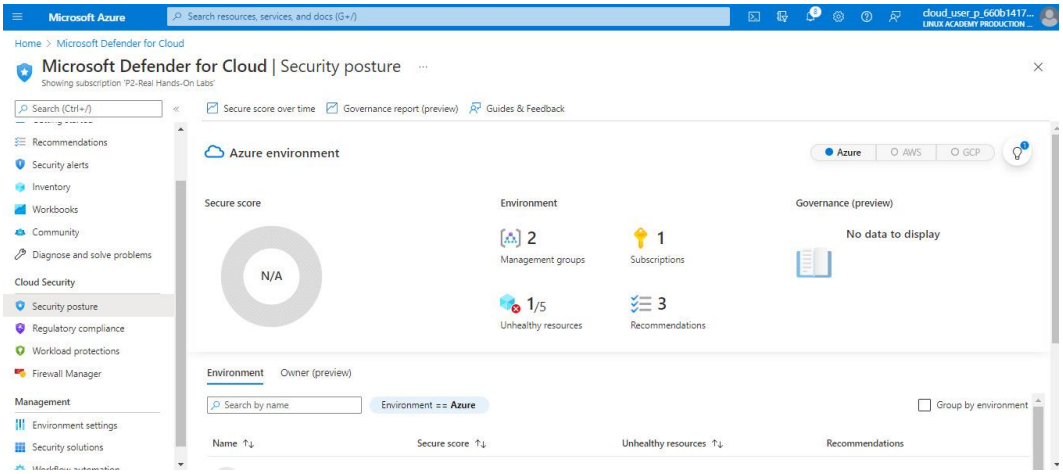

Figure 6.21 – The Security posture tab

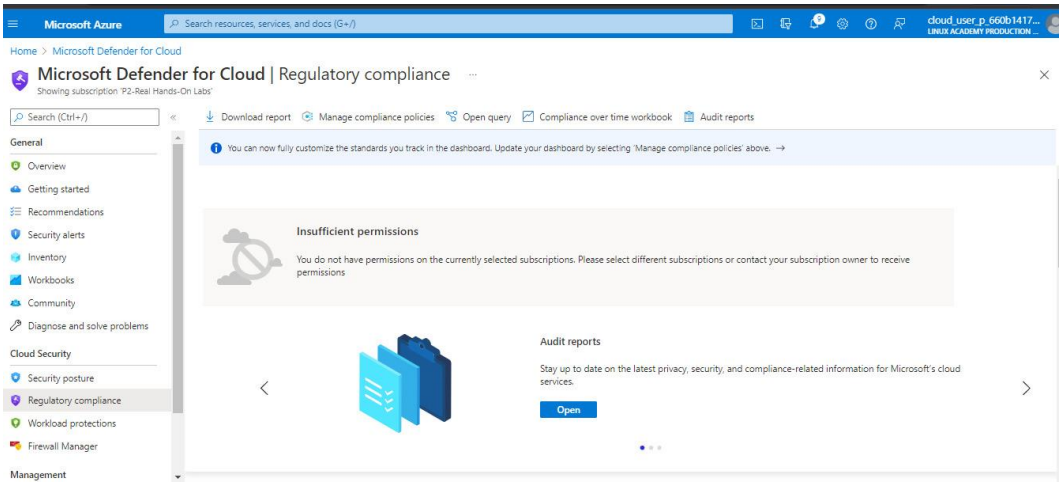

Figure 6.22 – Regulatory compliance

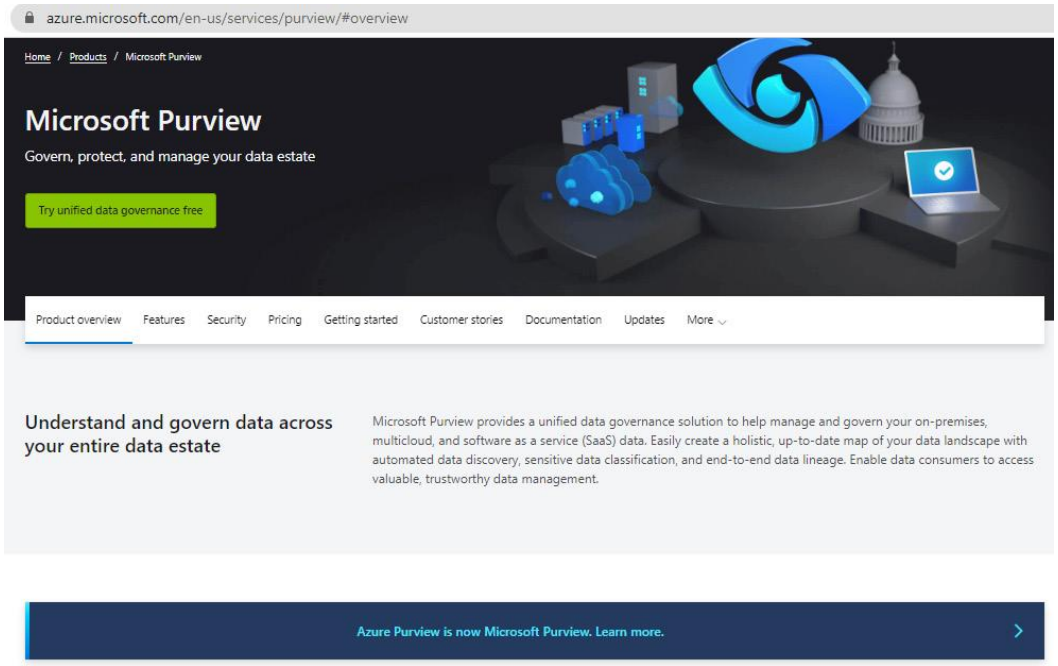

Figure 6.23 – Azure Purview

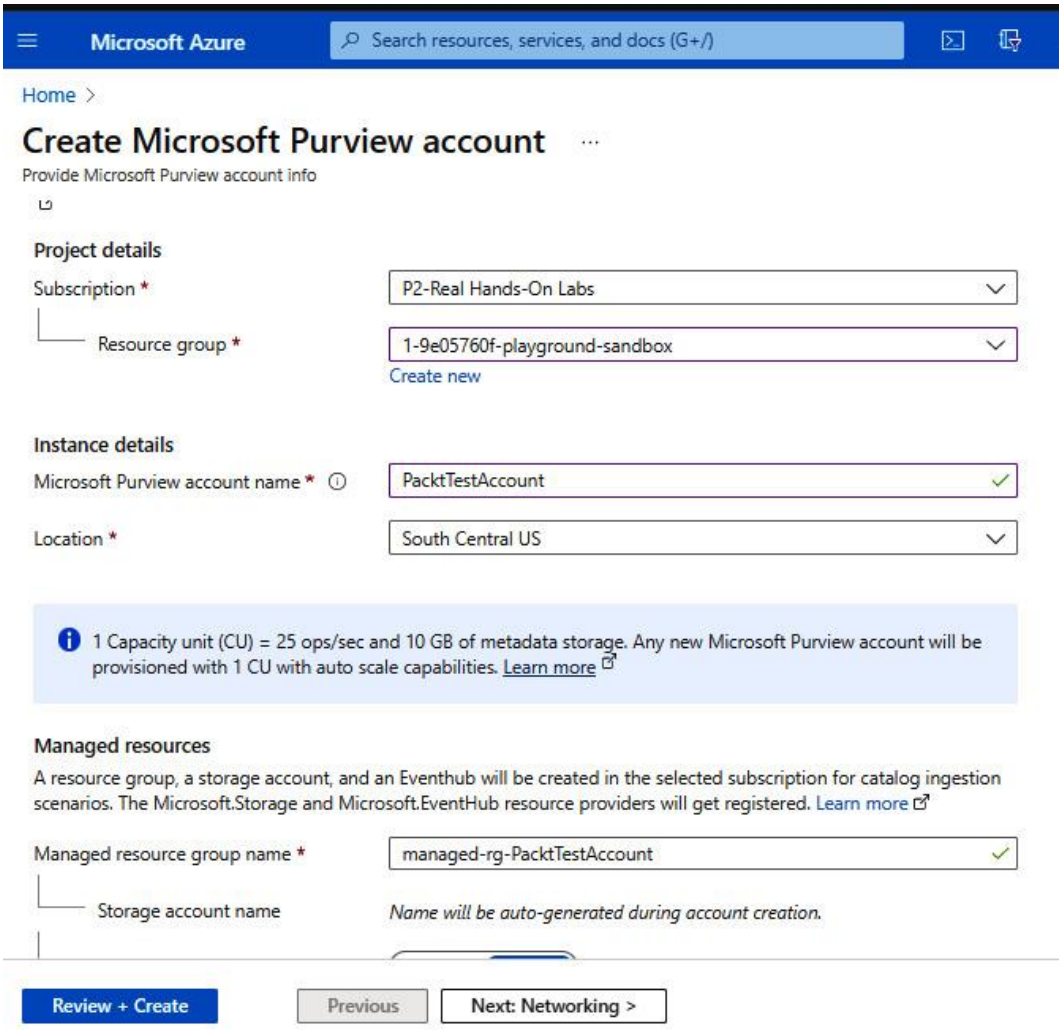

Figure 6.24 – Creating the Microsoft Purview account

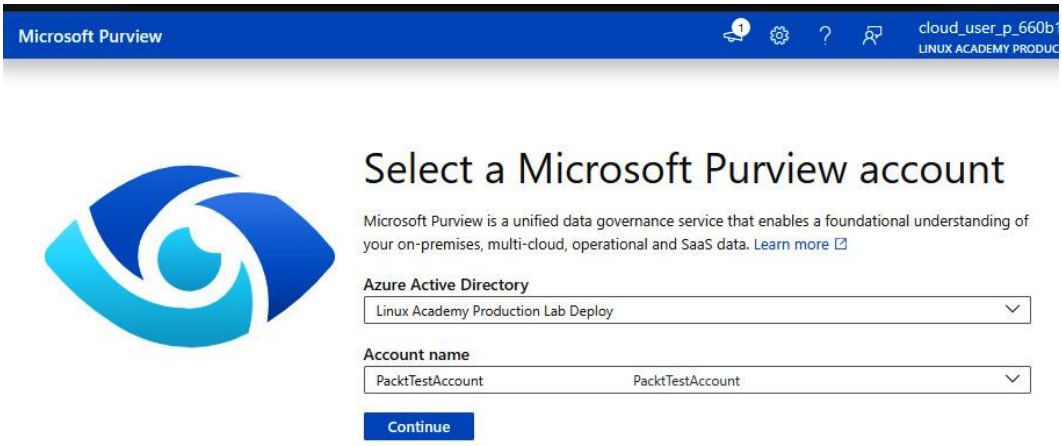

Figure 6.25 – Selecting an account

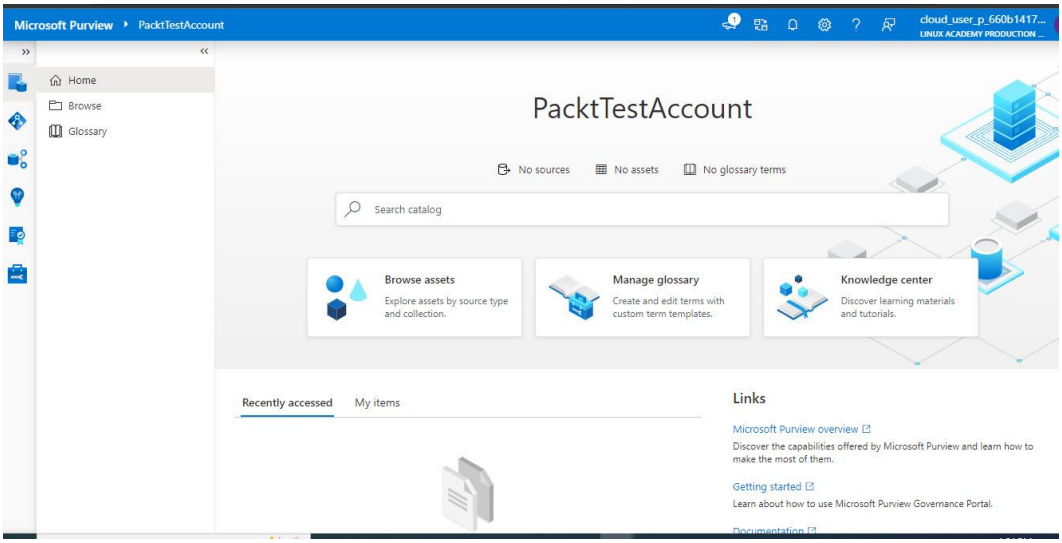

Figure 6.26 – Microsoft Purview Home page

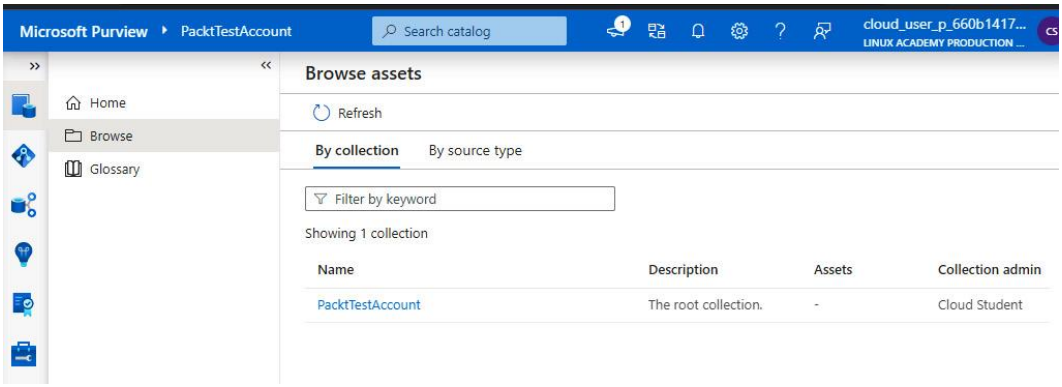

Figure 6.27 – Browse assets

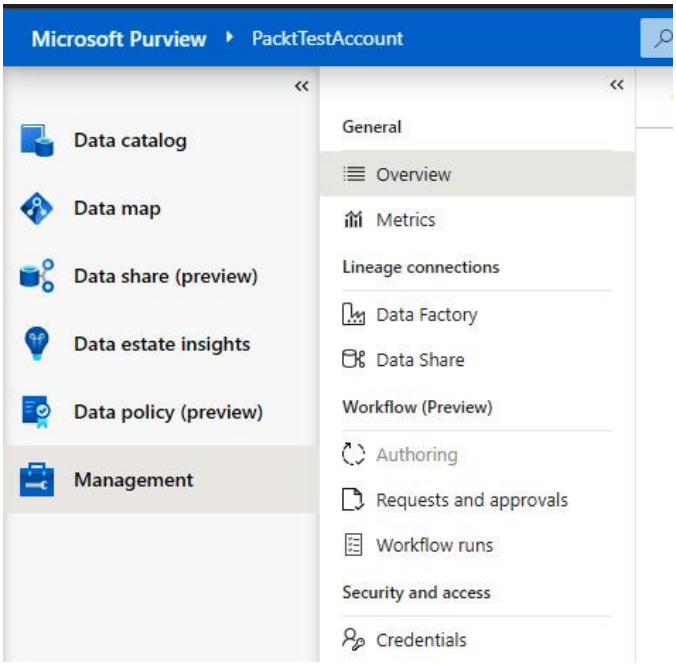

Figure 6.28 – Management | Overview

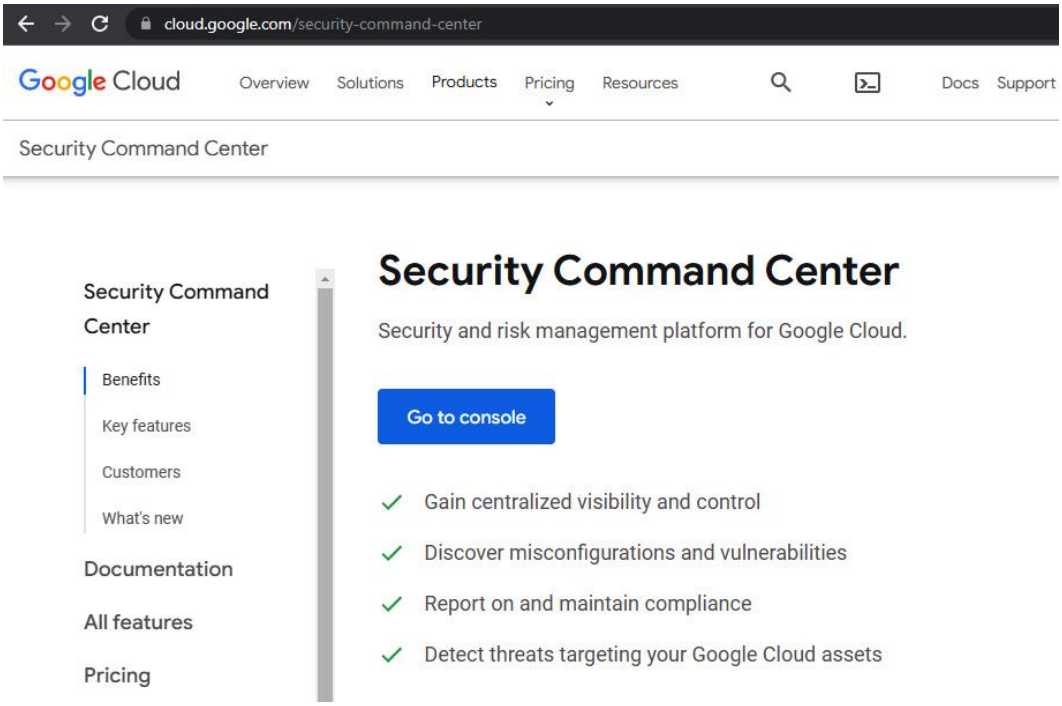

Figure 6.29 – Security Command Center

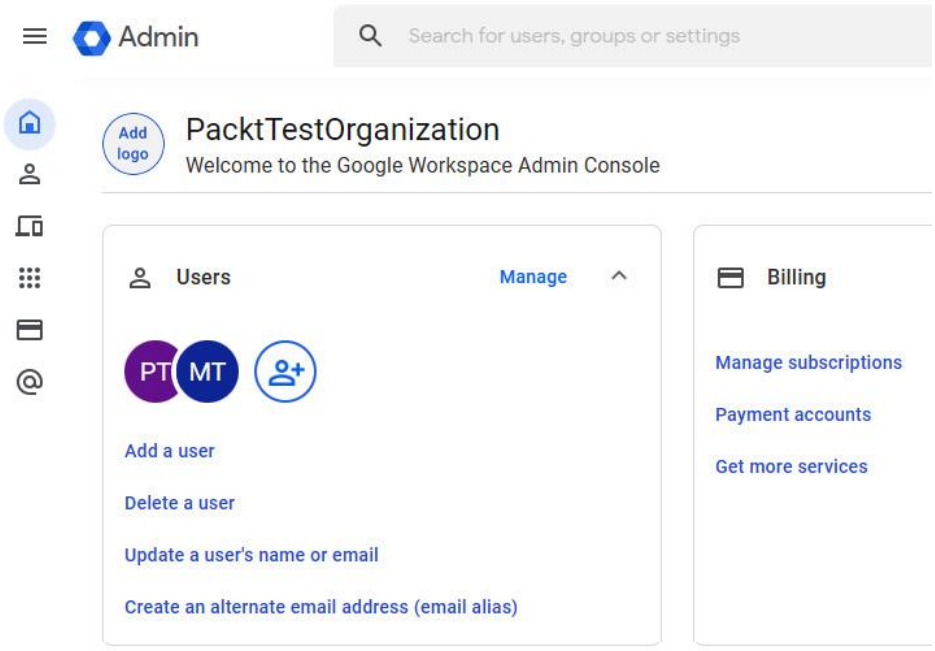

Figure 6.30 – The Admin console

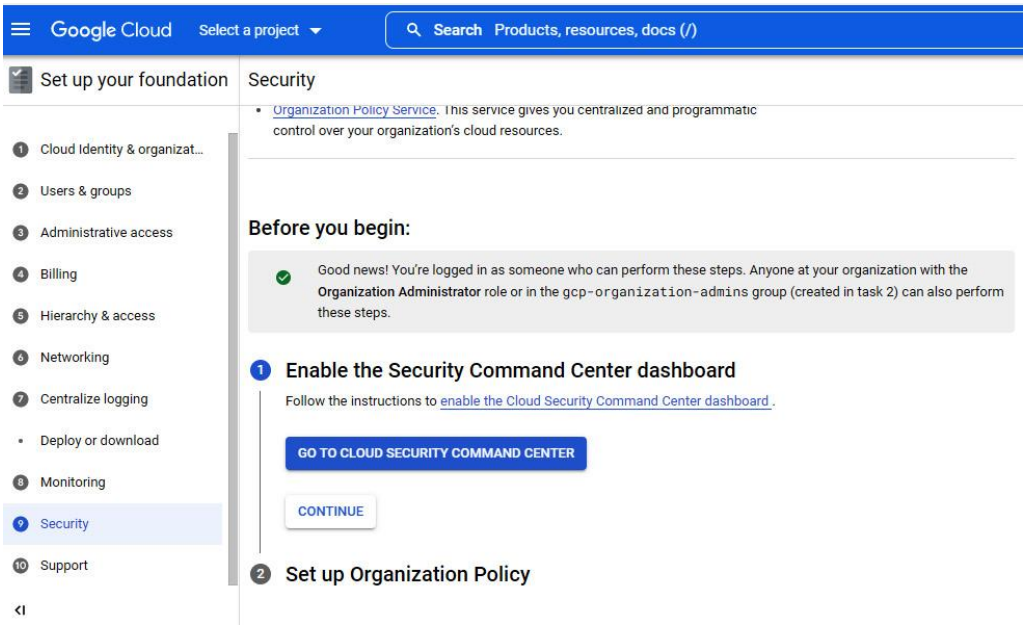

Figure 6.31 – The Security tab

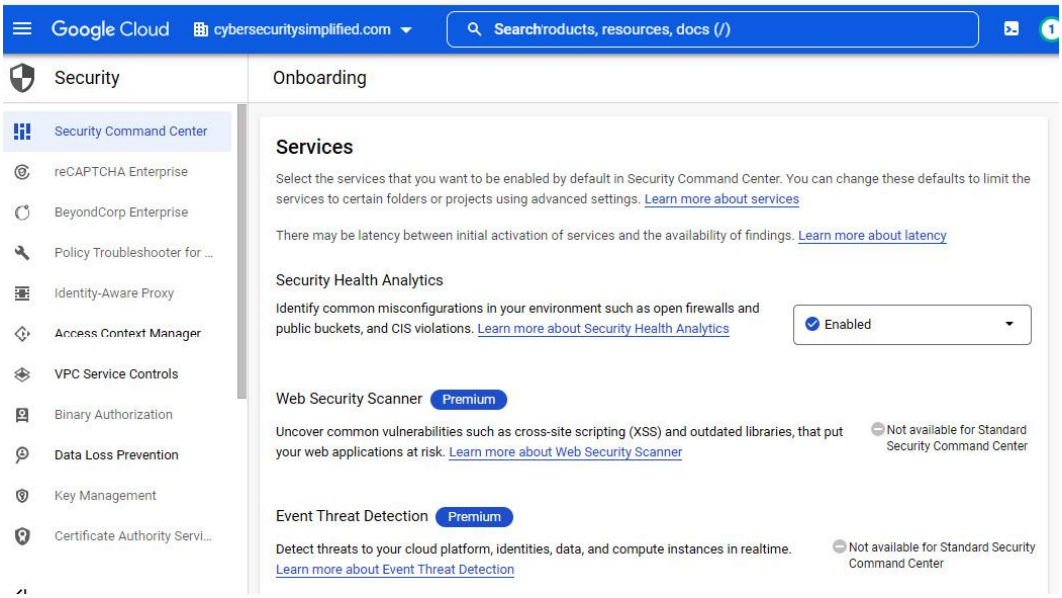

Figure 6.32 – Services setup

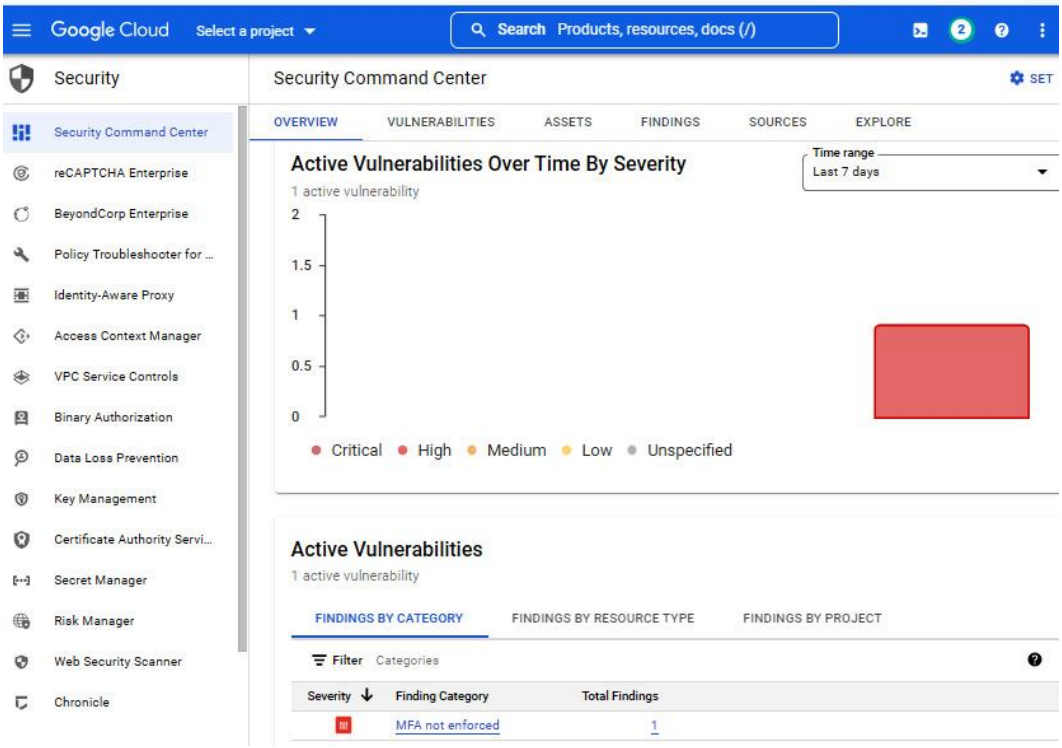

Figure 6.33 – Security Command Center | OVERVIEW

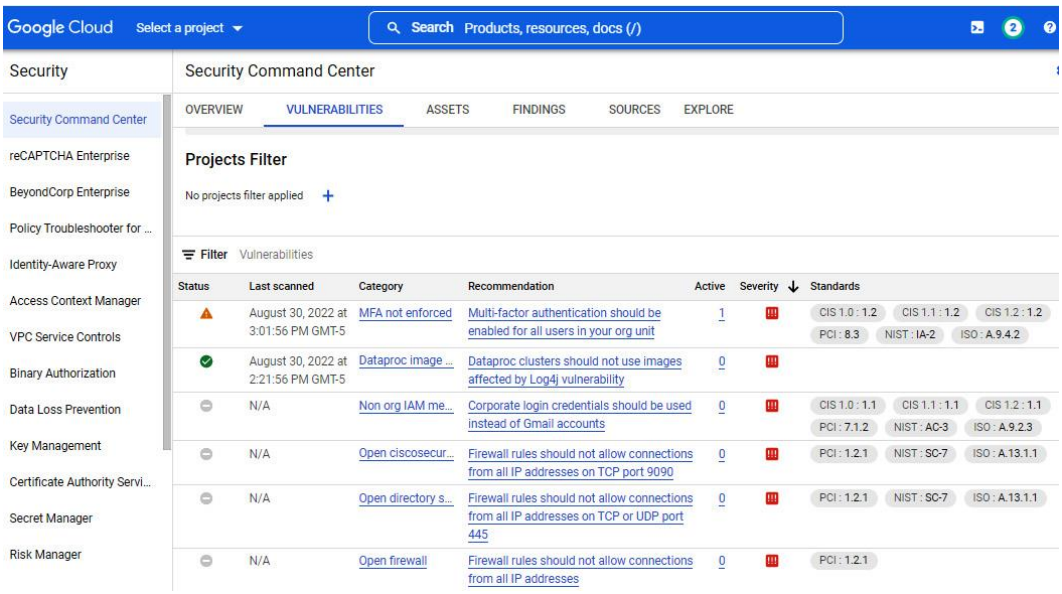

Figure 6.34 – Security Command Center | VULNERABILITIES

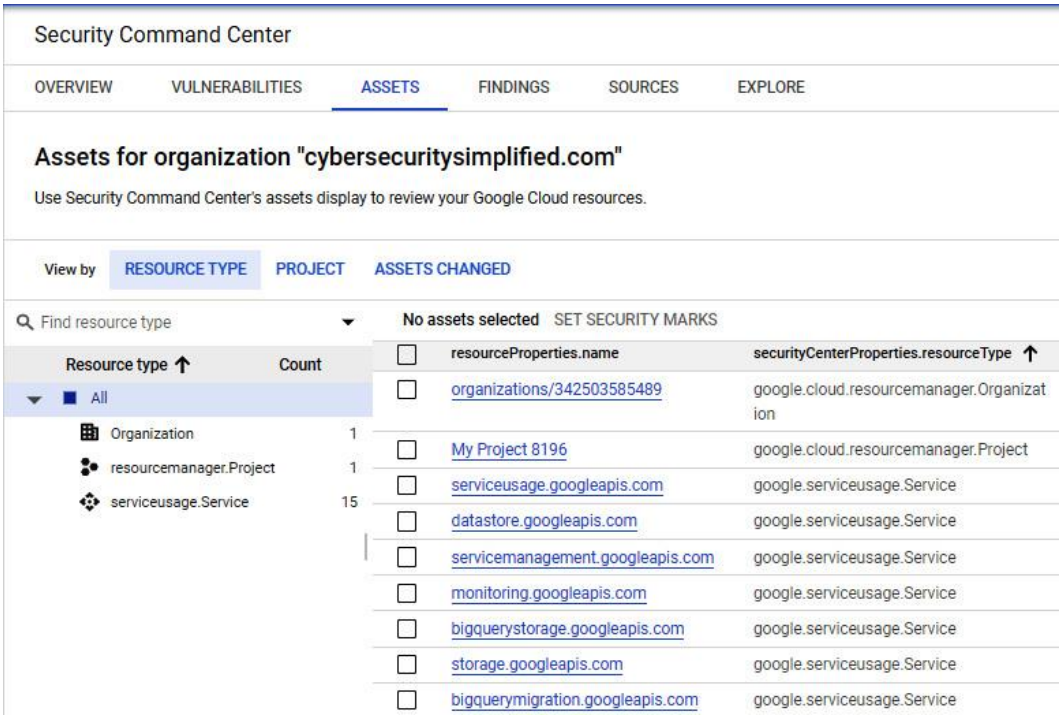

Figure 6.35 – Security Command Center | ASSETS

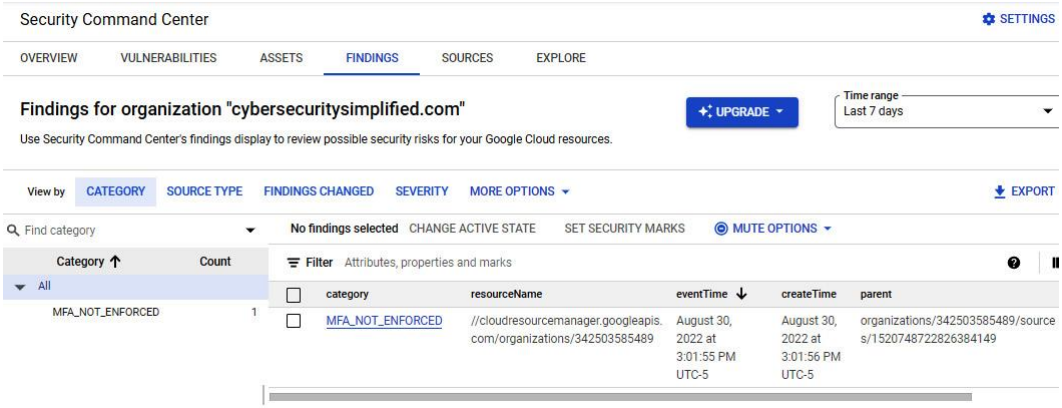

Figure 6.36 - Security Command Center | FINDINGS

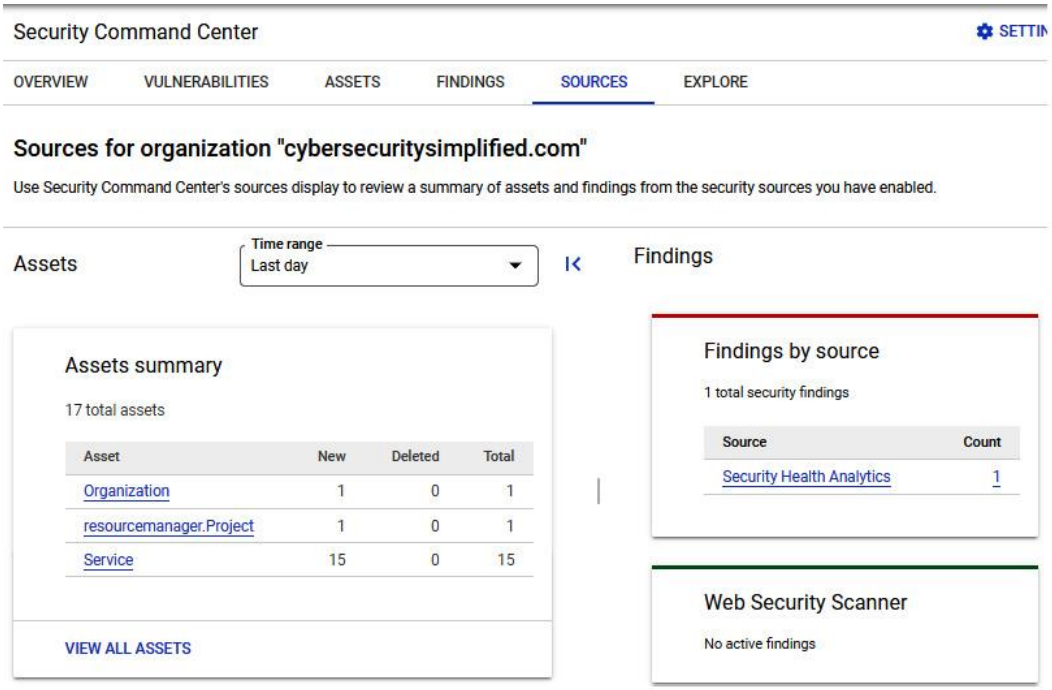

Figure 6.37 – Security Command Center | SOURCES

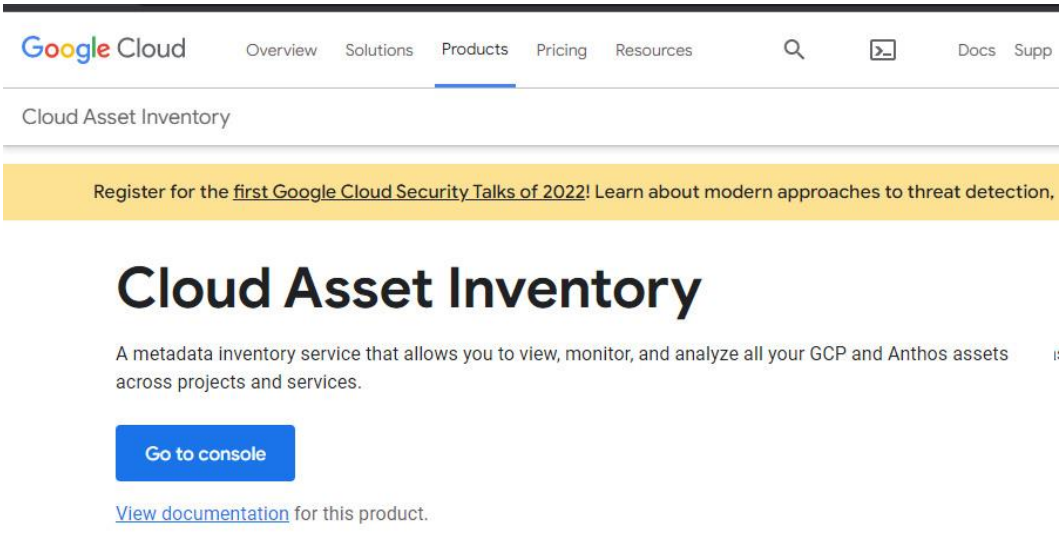

Figure 6.38 – Cloud Asset Inventory

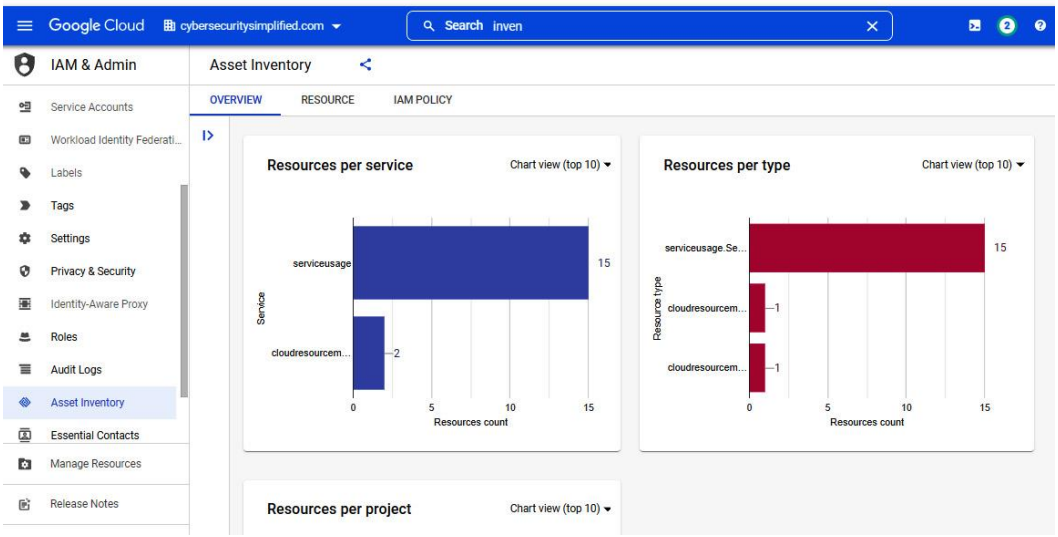

Figure 6.39 – The Asset Inventory OVERVIEW tab

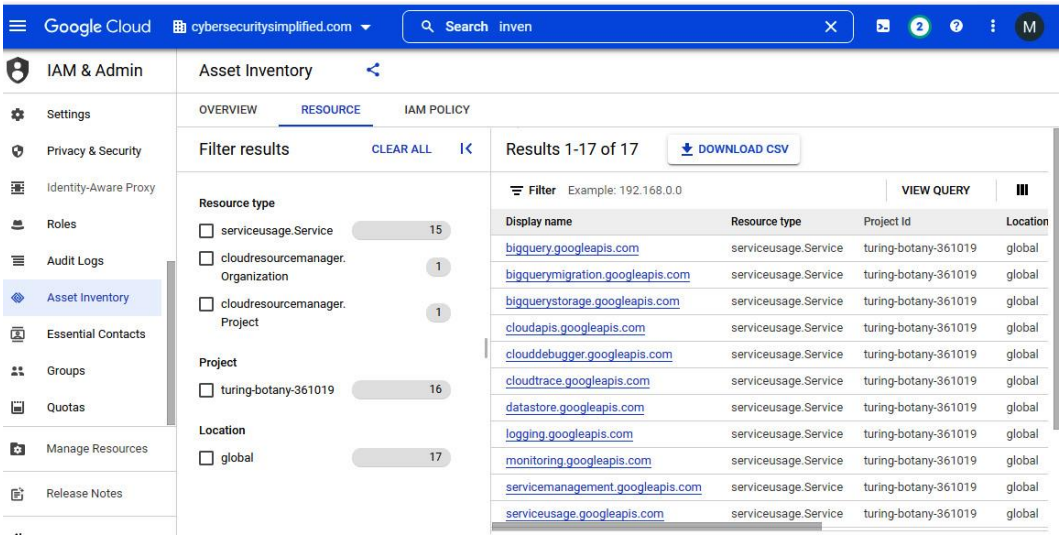

Figure 6.40 – The Asset Inventory RESOURCES tab

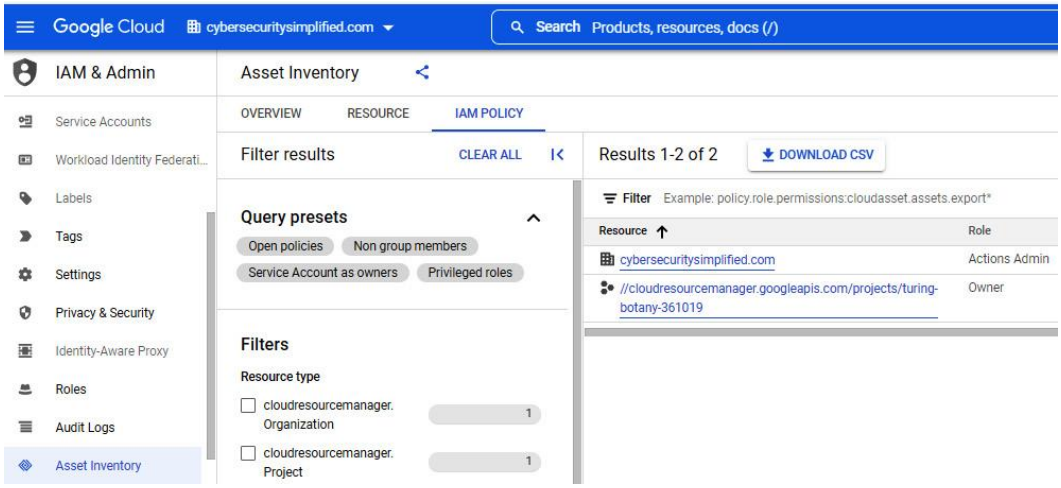

Figure 6.41 – The Asset Inventory IAM policy

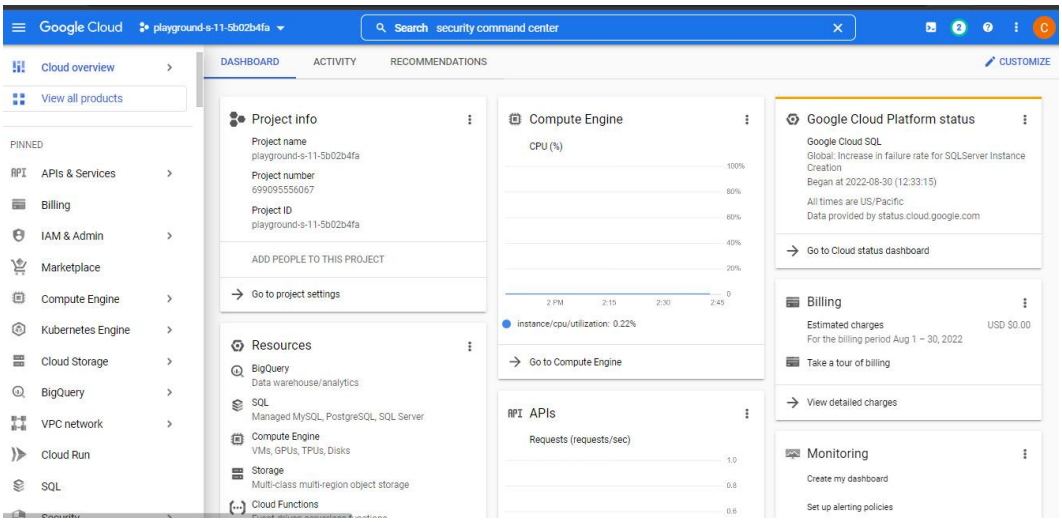

Figure 6.42 – The Cloud Overview DASHBOARD

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

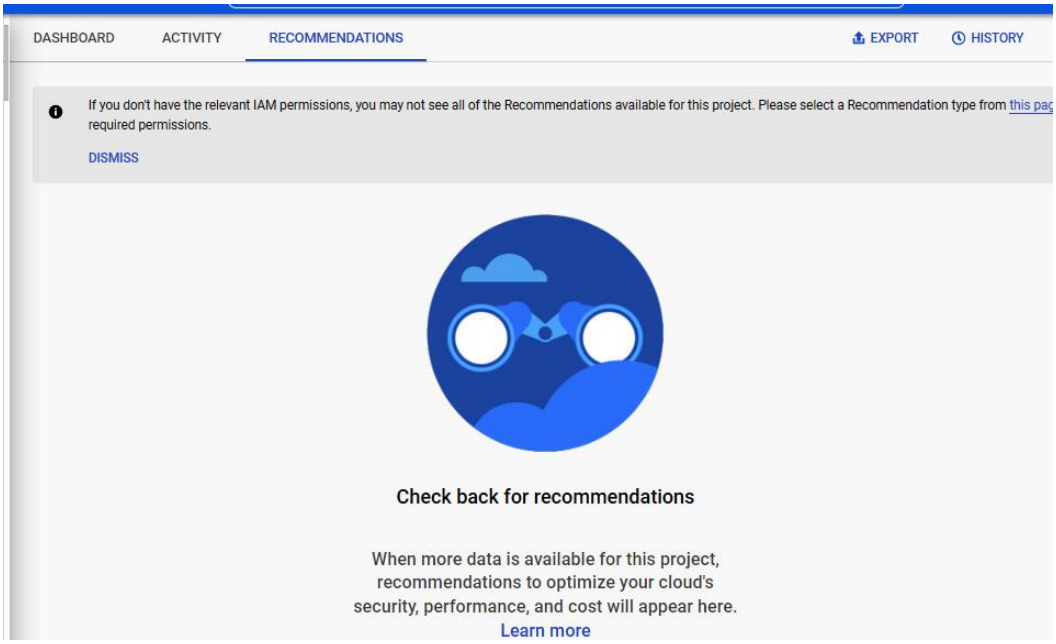

Figure 6.44 – The Cloud Overview RECOMMENDATIONS tab

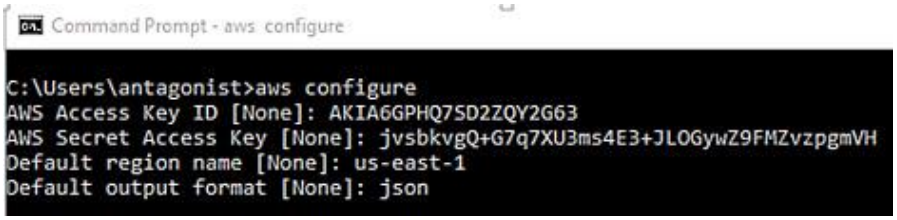

Figure 6.45 – The AWS CLI configuration settings to interact with AWS

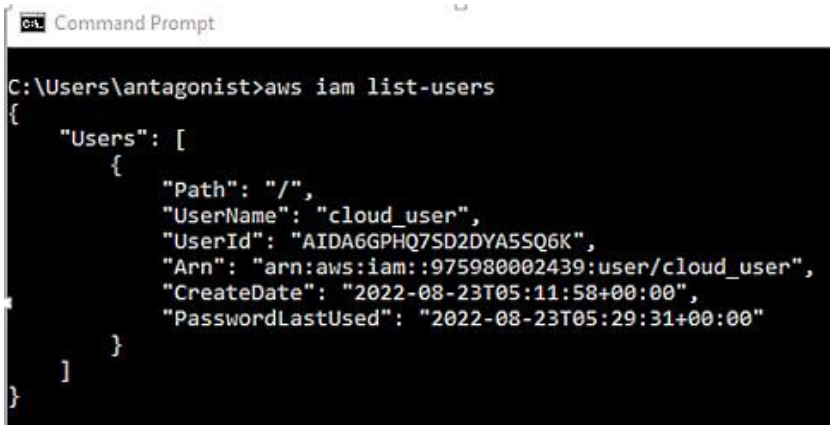

Figure 6.46 – AWS list users in IAM

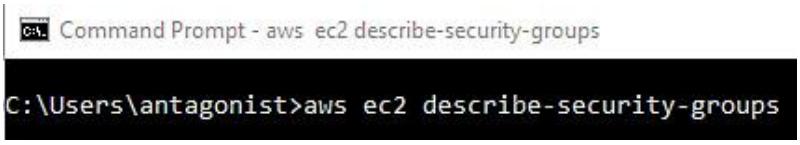

Figure 6.47 – AWS describe-security-groups

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
ith `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"
    }
  }
]

C:\Users\antagonist>
```

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/Mi
crosoft.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

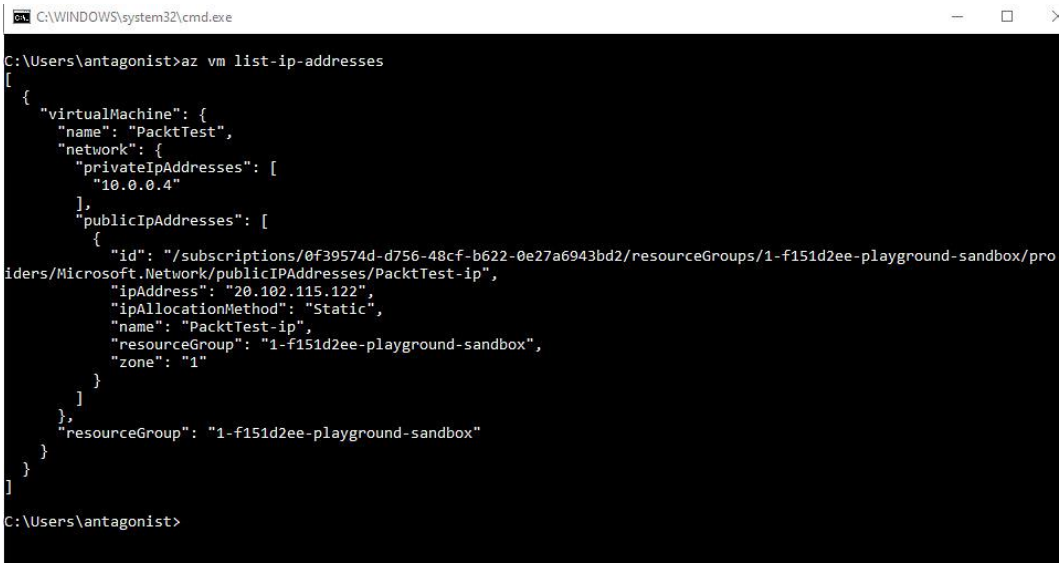

Figure 6.51 – Listing IP addresses associated with a VM

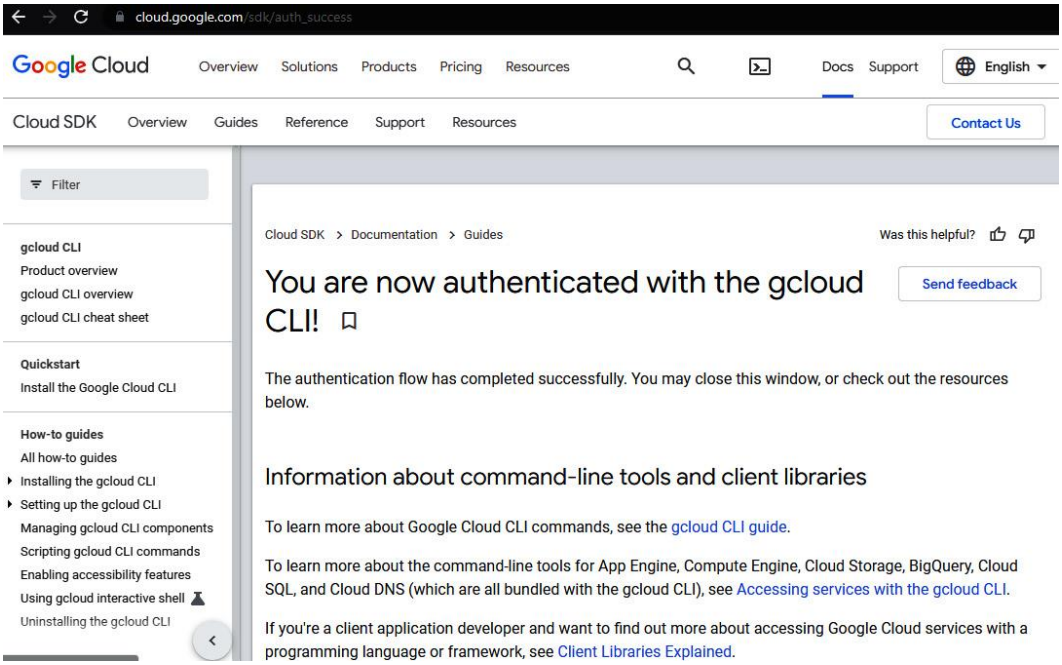

Figure 6.52 – Authentication

Figure 6.53 – Listing credential accounts

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
```

Chapter 7

Figures

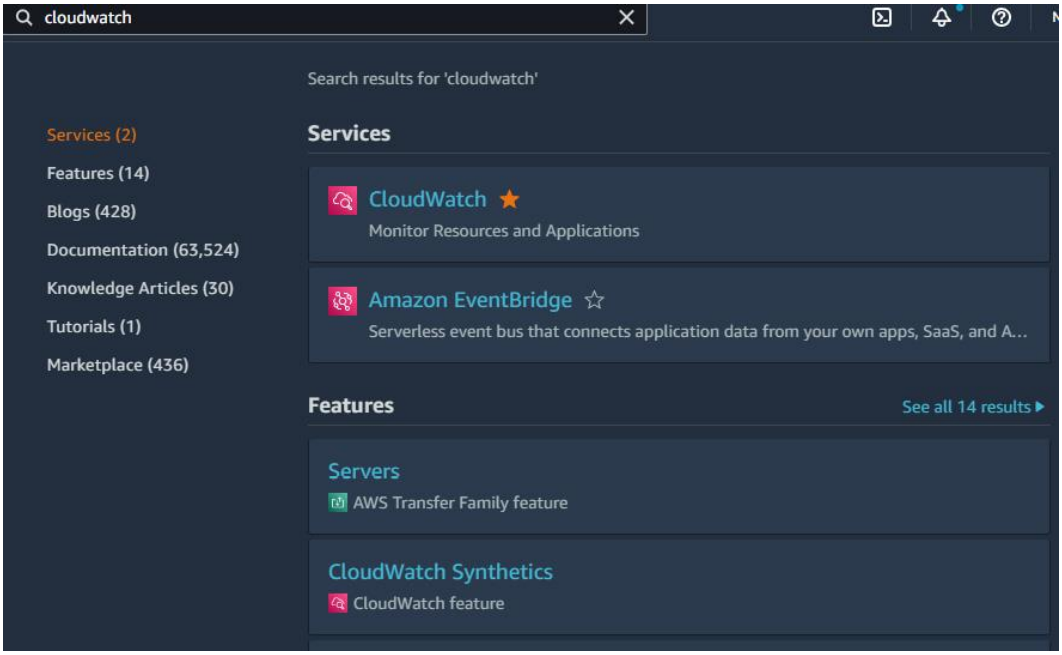

Figure 7.1 – Searching for Amazon CloudWatch

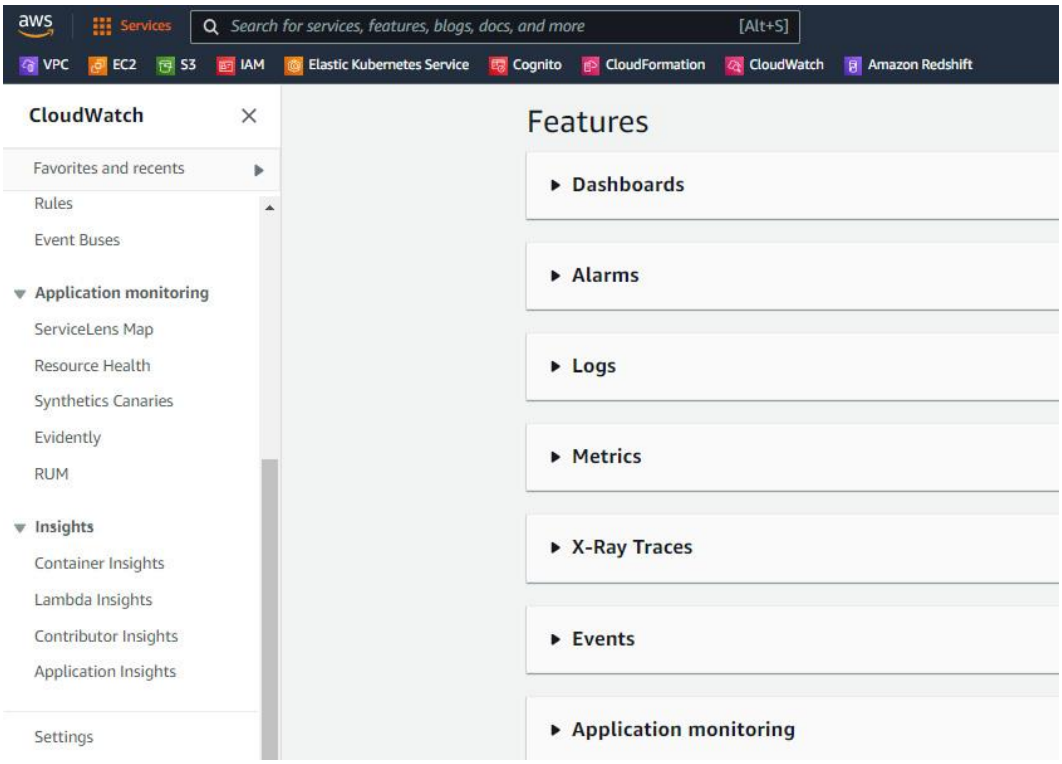

Figure 7.2 – Features

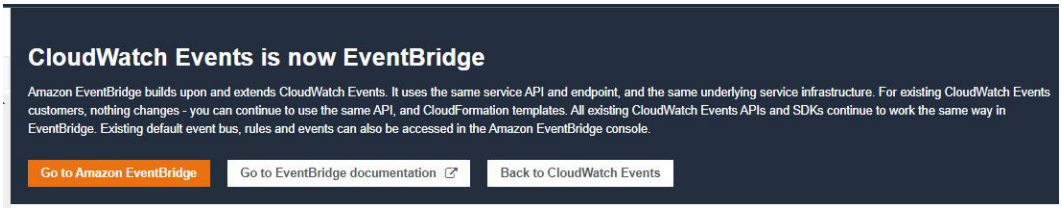

Figure 7.3 – EventBridge main page

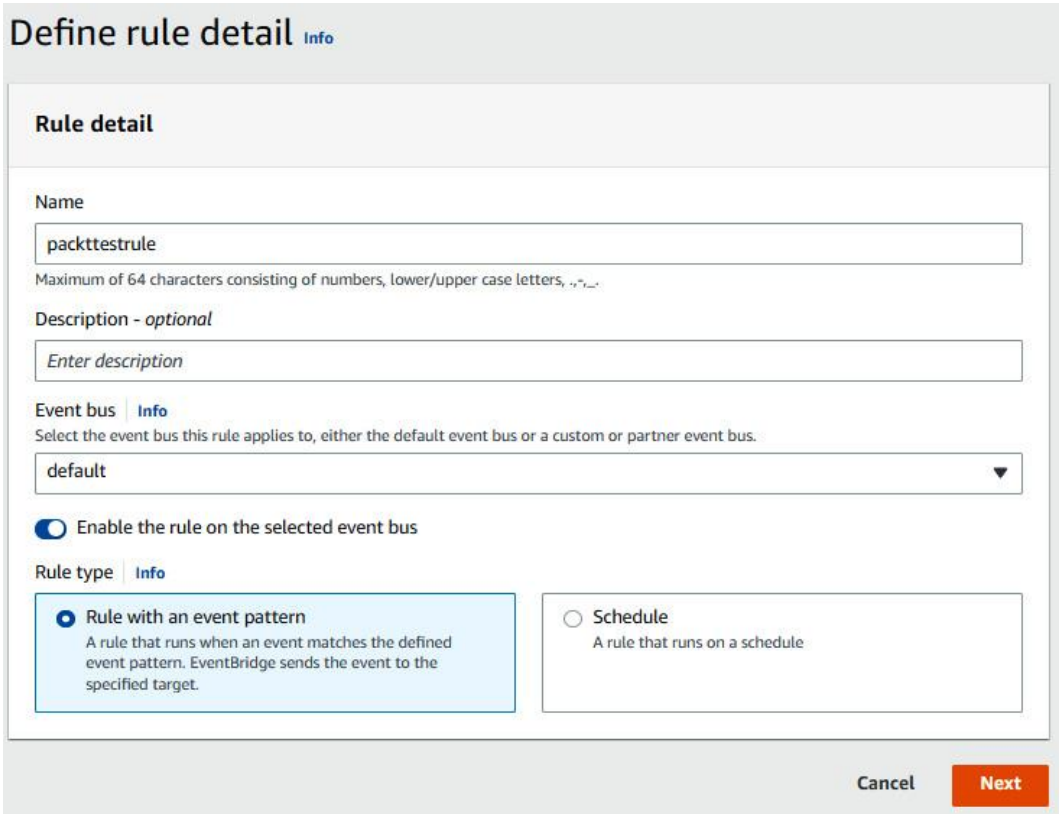

Figure 7.4 – Define rule detail

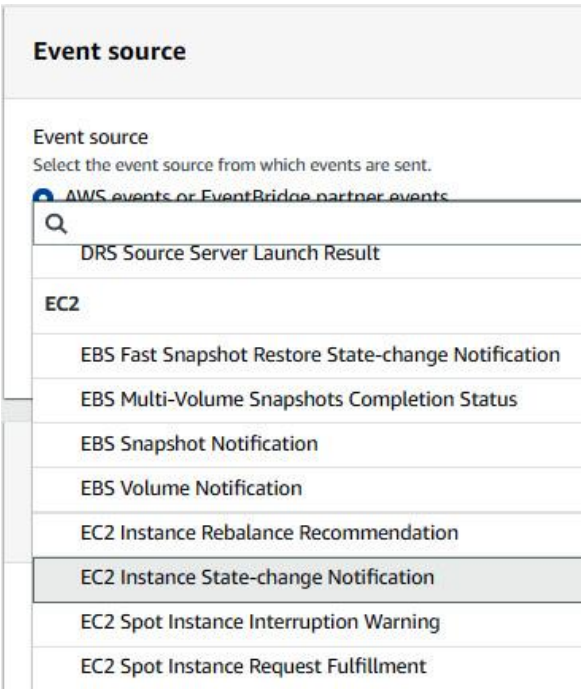

Figure 7.5 – Event source

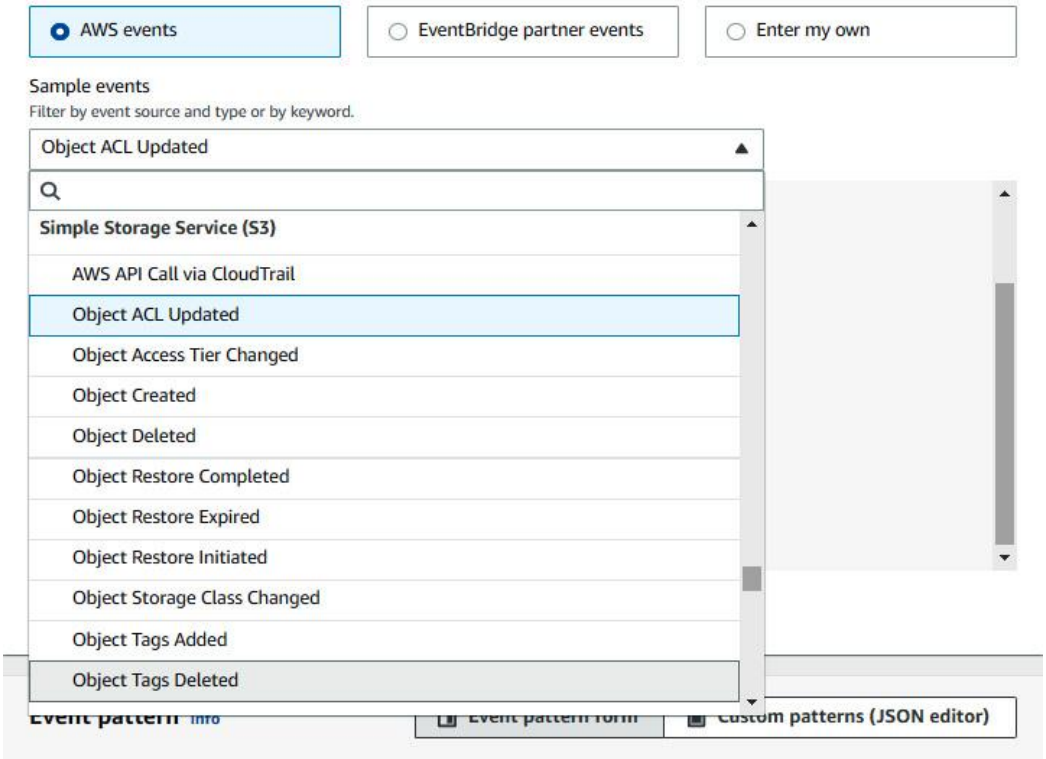

Figure 7.6 – Object ACL Updated

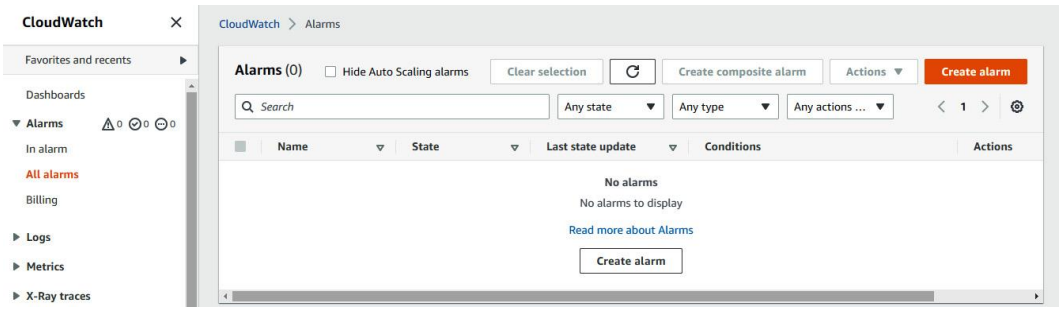

Figure 7.7 – The Alarms tab

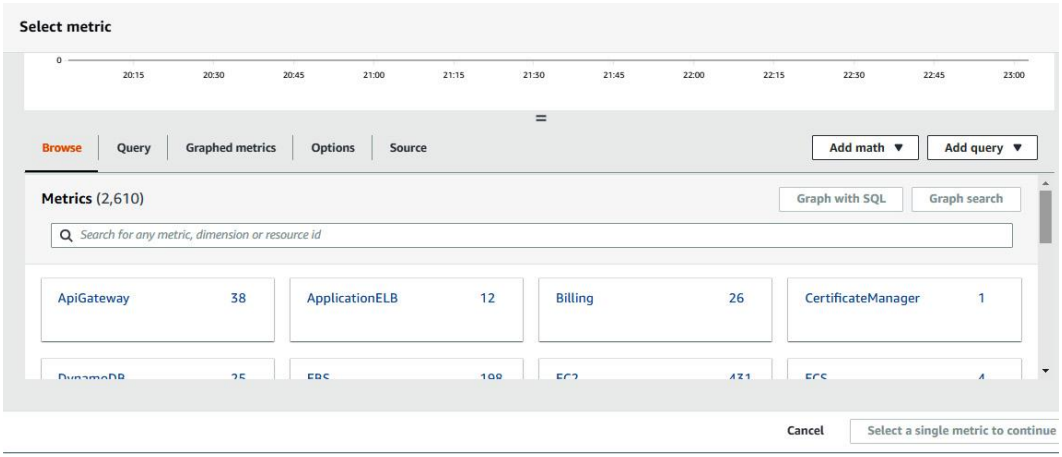

Figure 7.8 – Metrics

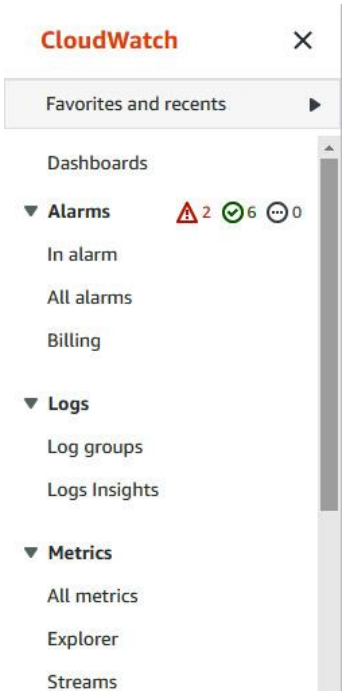

Figure 7.9 – Dashboards

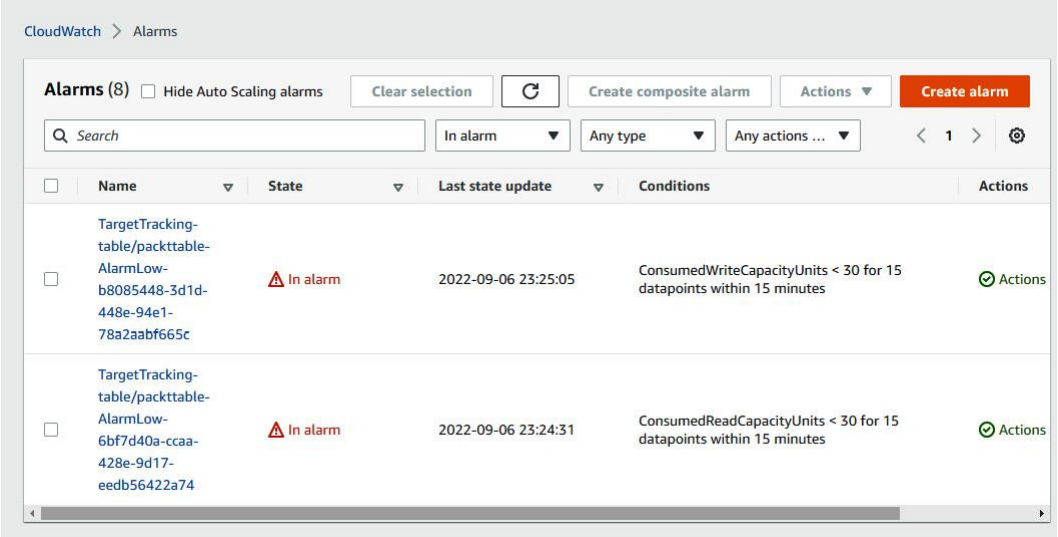

Figure 7.10 – Example alarms

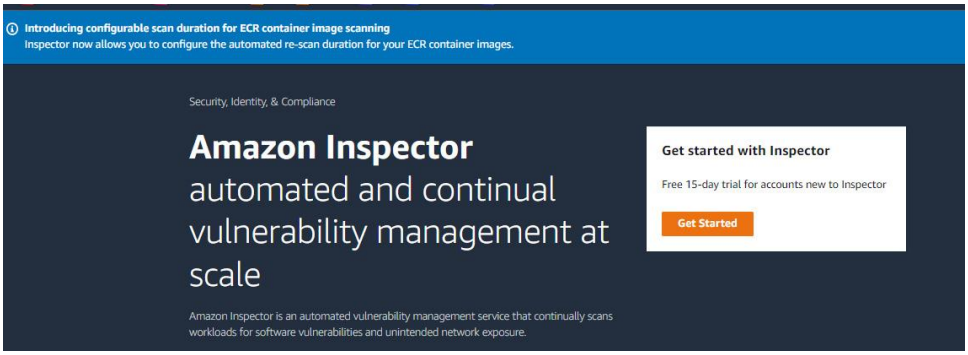

Figure 7.11 – Amazon Inspector

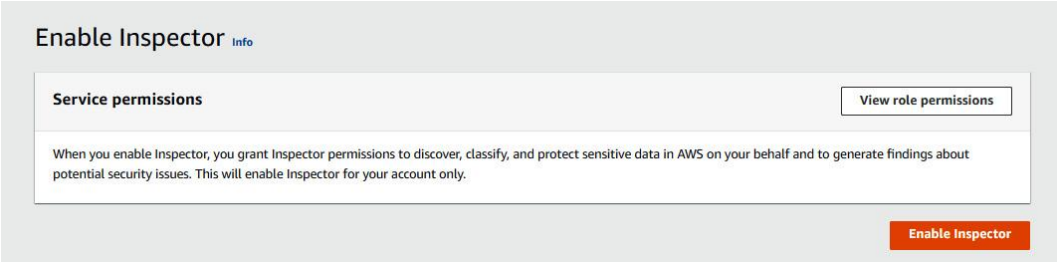

Figure 7.12 – Enabling Amazon Inspector

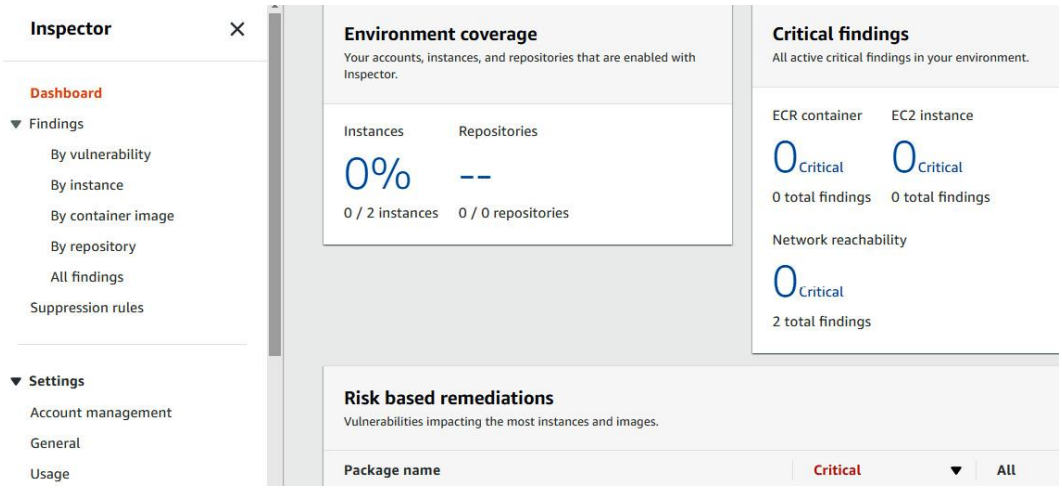

Figure 7.13 – The Amazon Inspector dashboard

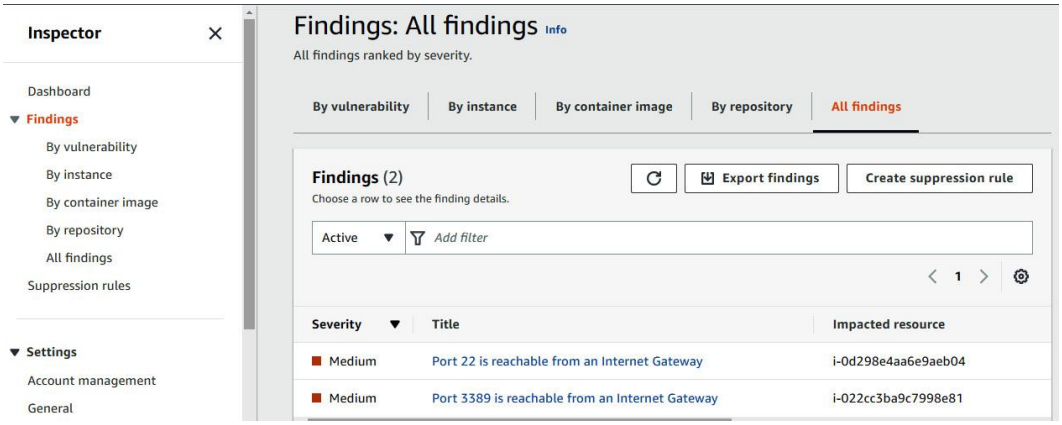

Figure 7.14 – The Amazon Inspector findings

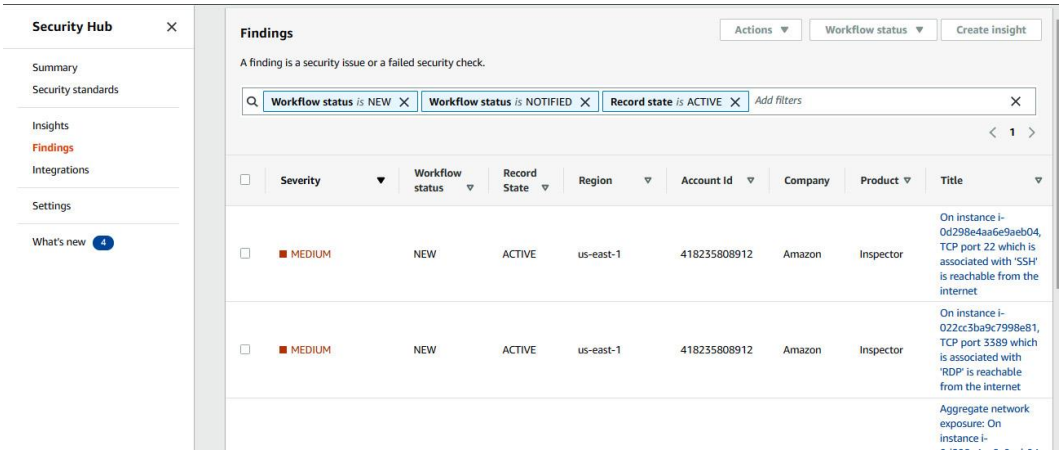

Figure 7.15 – Integration with AWS Security Hub

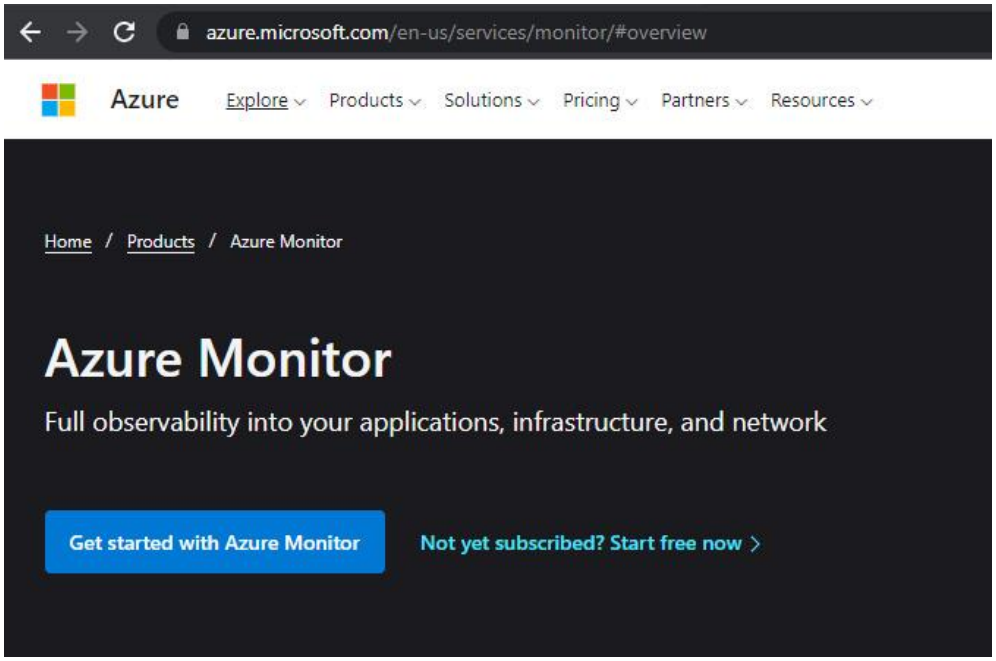

Figure 7.16 – Azure Monitor

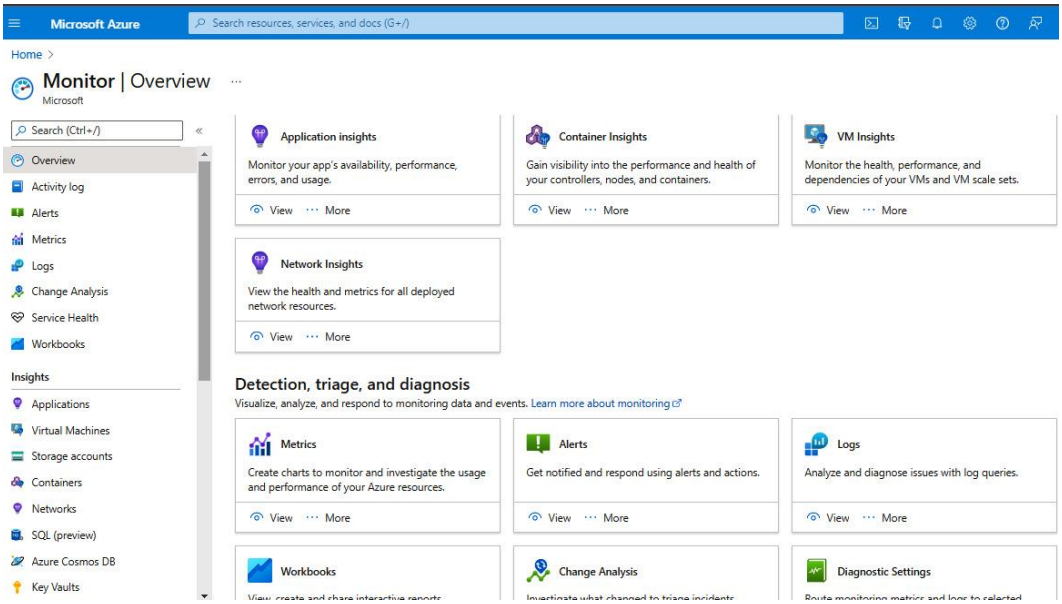

Figure 7.17 – Azure Monitor Overview

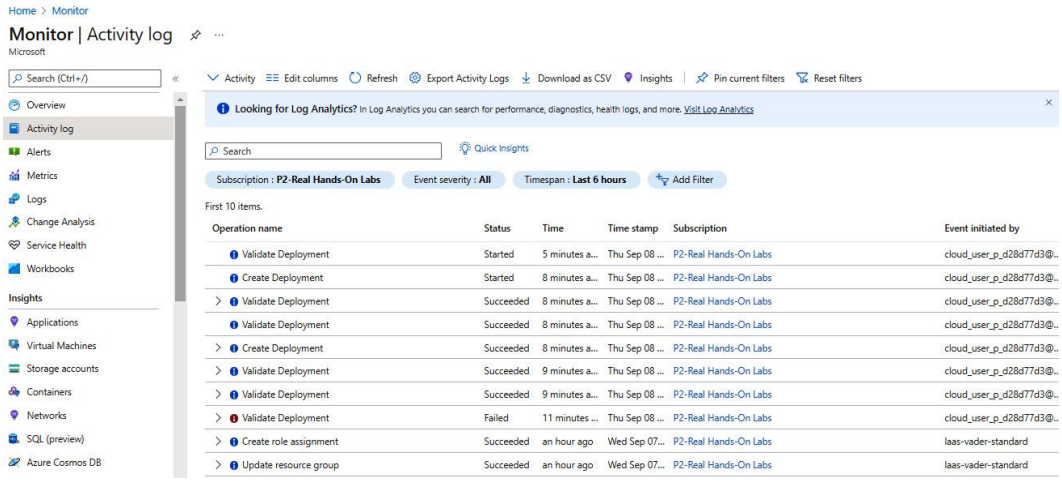

Figure 7.18 – Azure Monitor Activity log

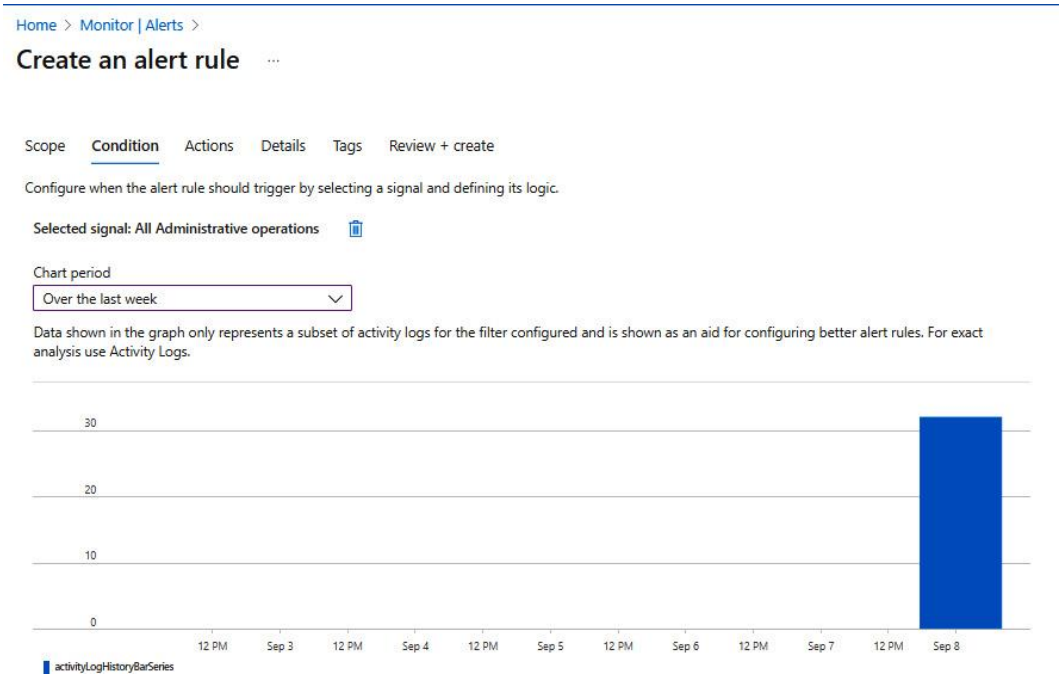

Figure 7.19 – Creating an alert rule

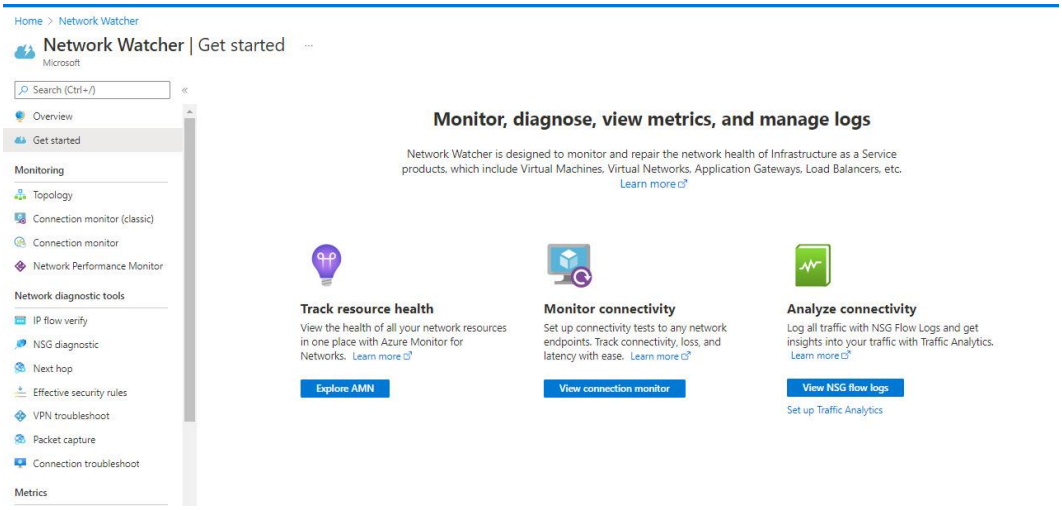

Figure 7.20 – Azure Network Watcher

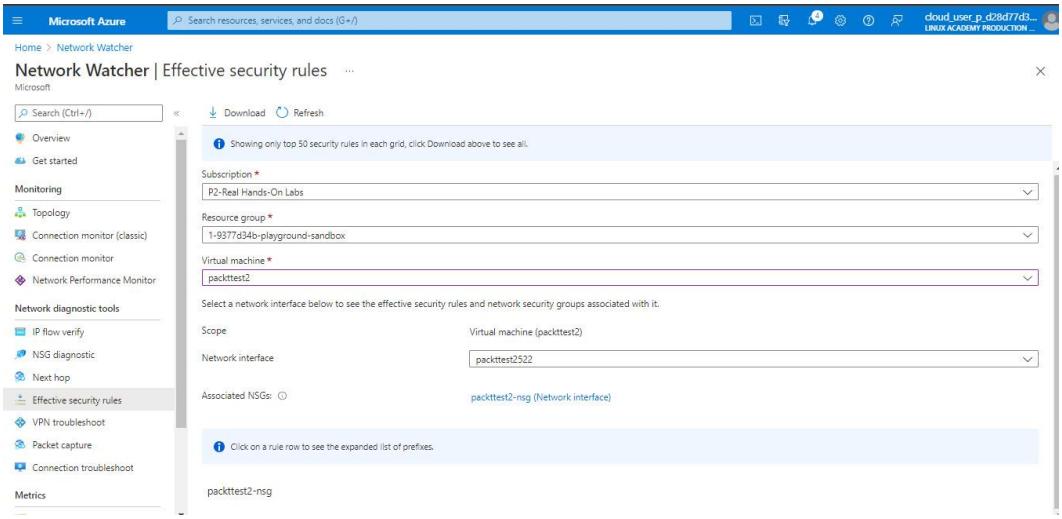

Figure 7.21 – Effective security rules

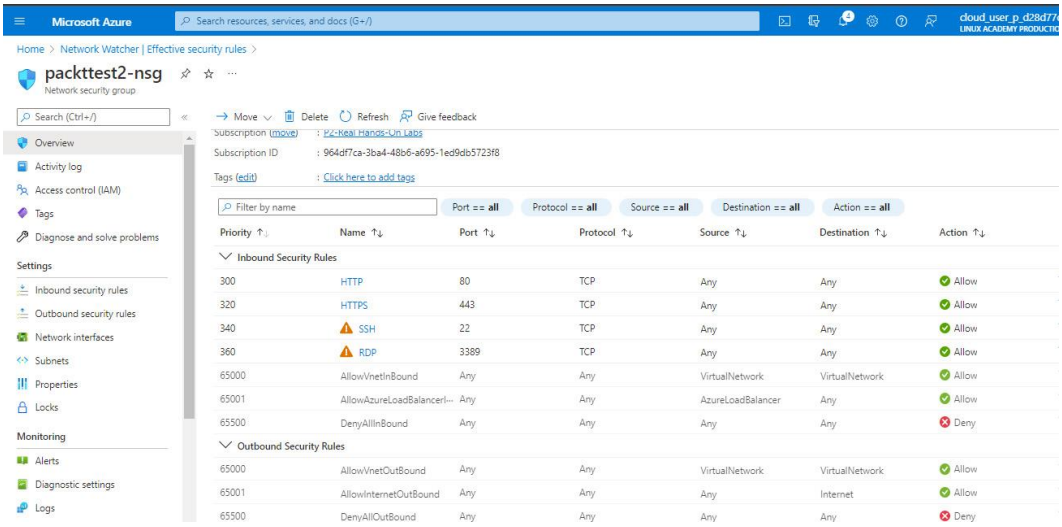

Figure 7.22 – packttest2-nsg

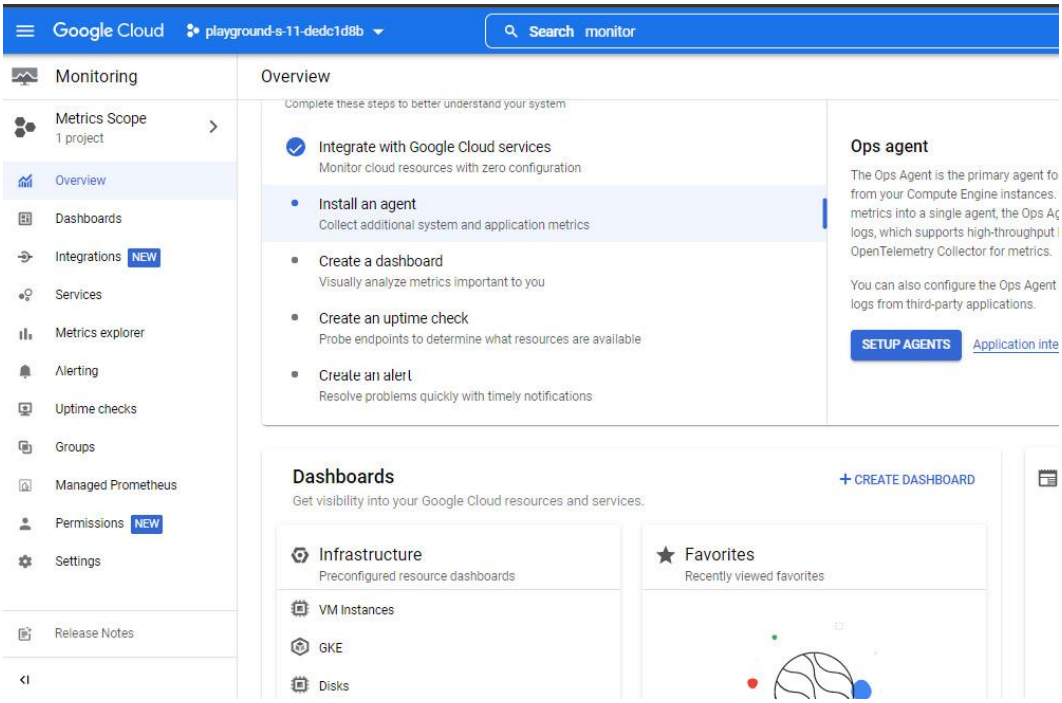

Figure 7.23 – Google Cloud Monitoring Overview

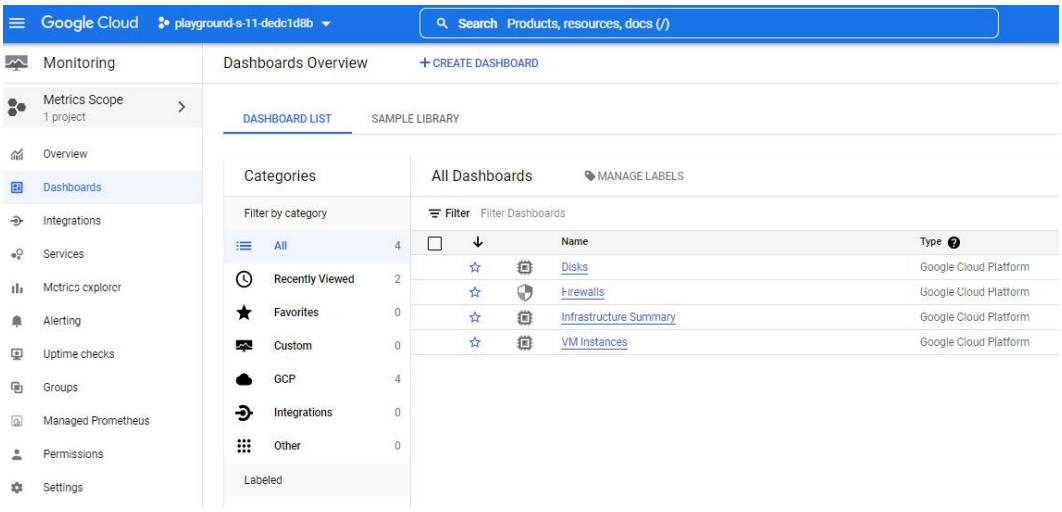

Figure 7.24 – Dashboards Overview

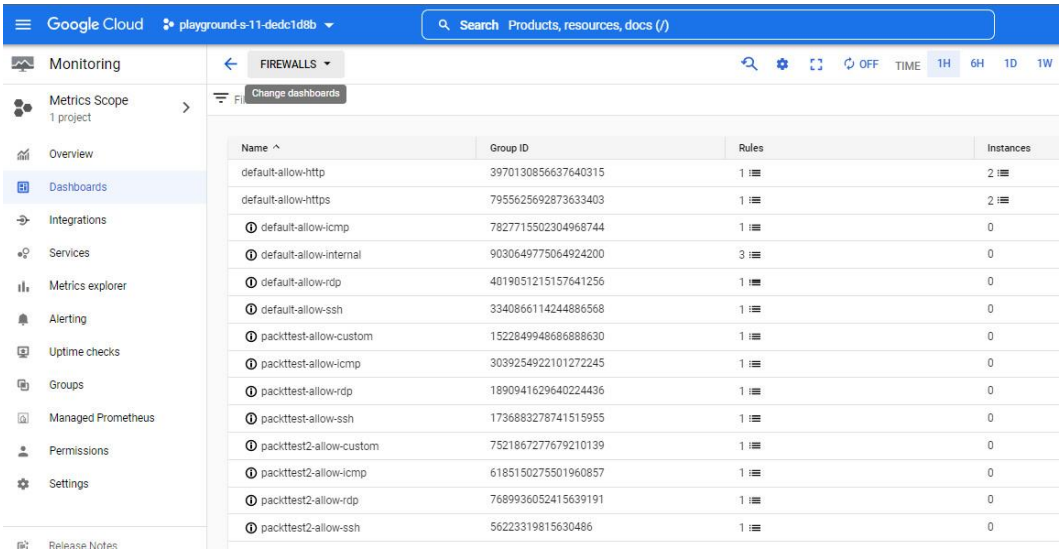

Figure 7.25 – The Firewalls dashboard

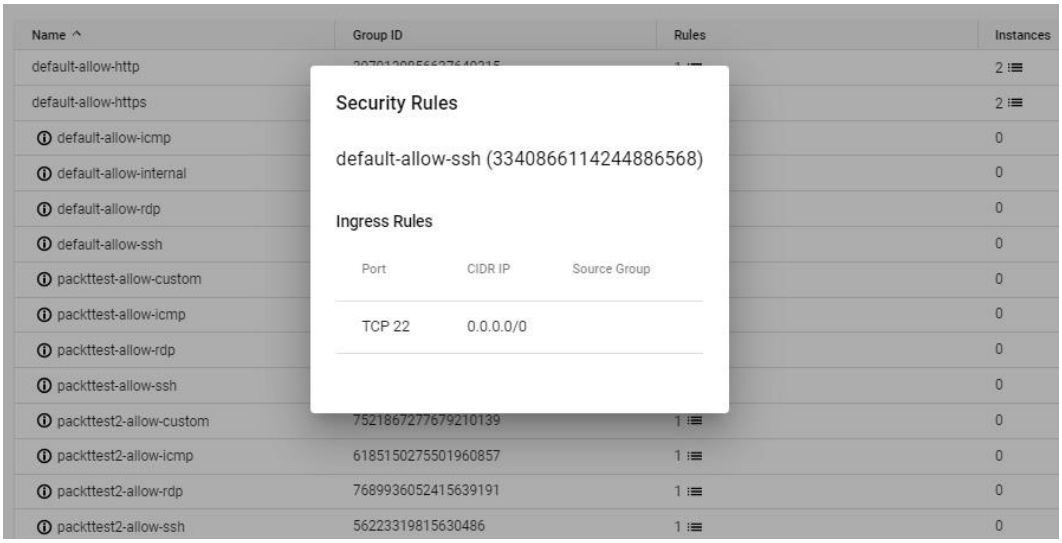

Figure 7.26 – Security Rules

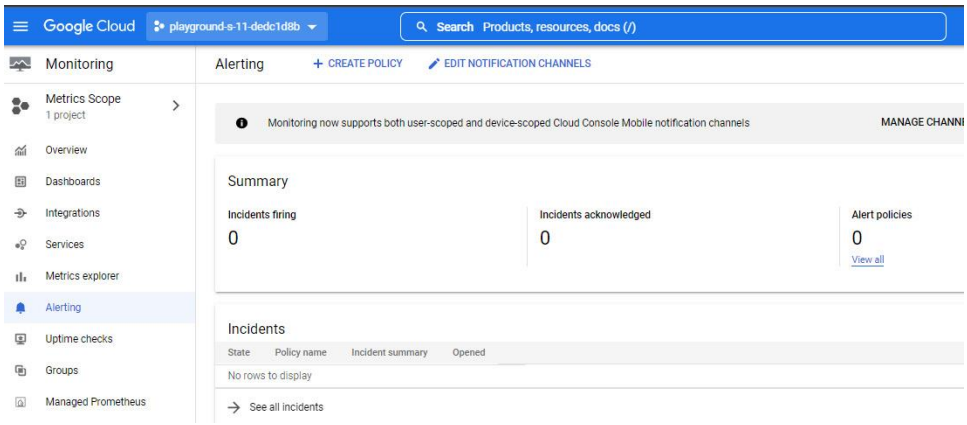

Figure 7.27 – Alerts

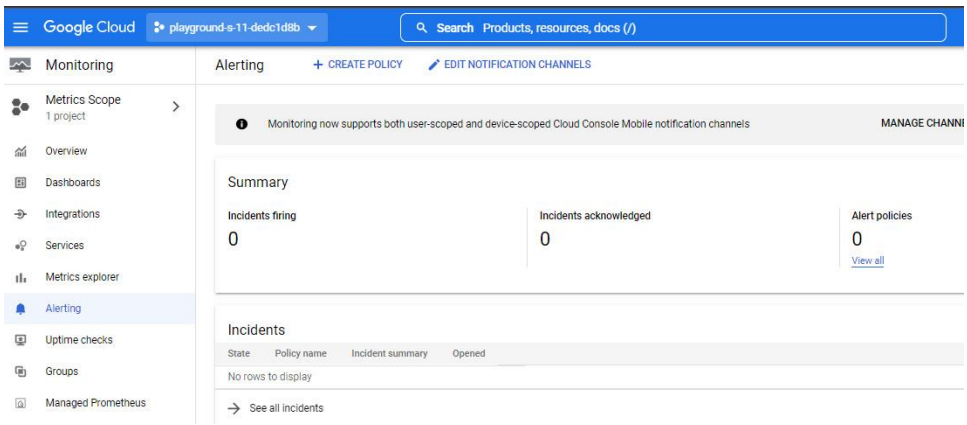

Figure 7.27 – Alerts

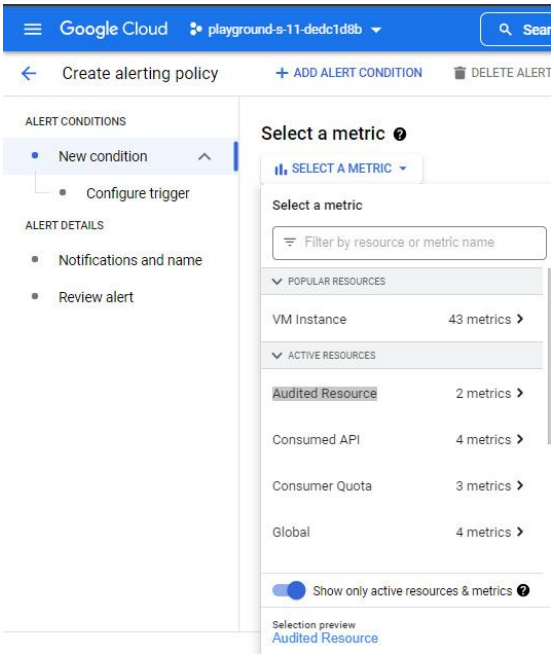

Figure 7.28 – Selecting a metric

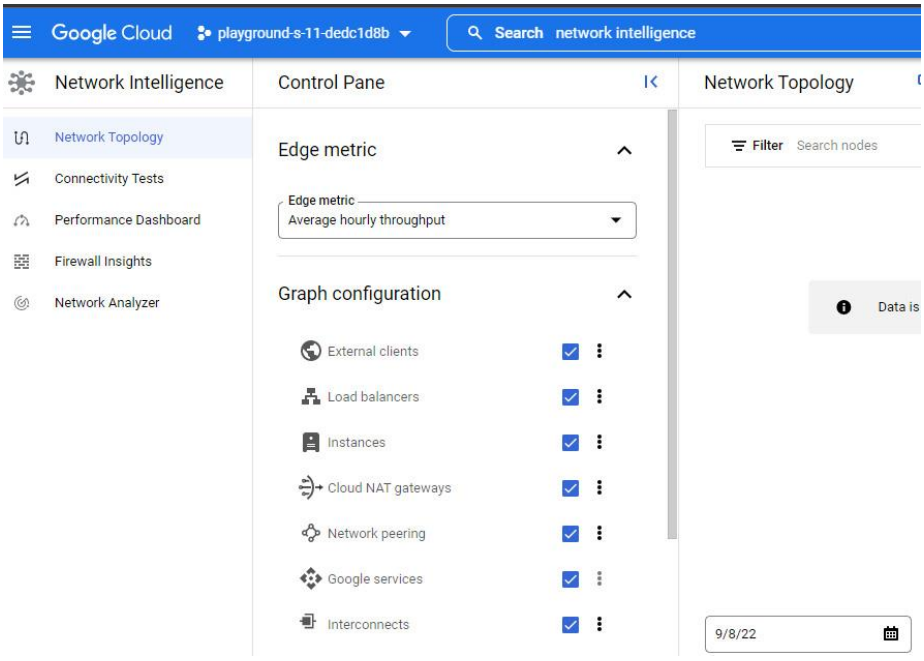

Figure 7.29 – Network Intelligence

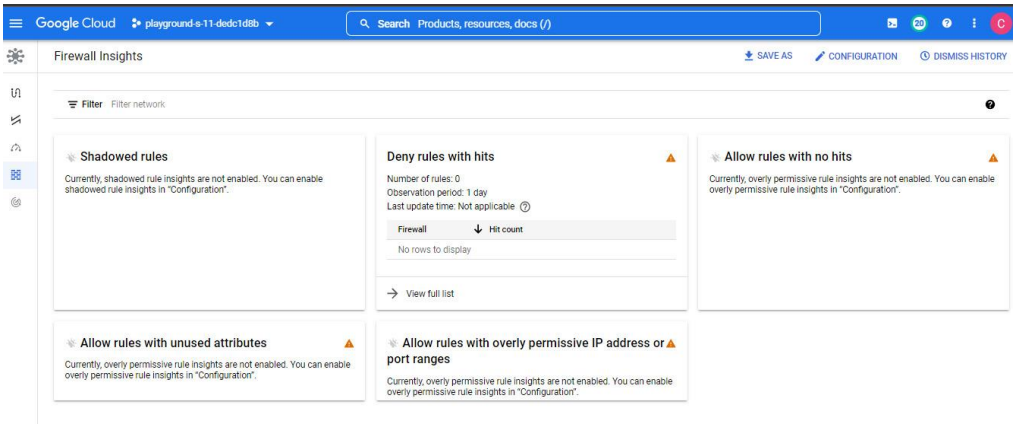

Figure 7.30 – Firewall Insights

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.

SMTP port 25 disallowed in this project

REFRESH CONFIGURE LOGS DELETE

Filter Enter property name or value

Name	Type	Targets	Filters	Protocols / ports	Action	Network
default-allow-https	Ingress	https-server	IP ranges: 0.(	tcp:443	Allow	default
default-allow-http	Ingress	http-server	IP ranges: 0.(	tcp:80	Allow	default
default-allow-icmp	Ingress	Apply to all	IP ranges: 0.(	icmp	Allow	default
default-allow-internal	Ingress	Apply to all	IP ranges: 10	tcp:0-65535 udp:0-65535 icmp	Allow	default
default-allow-rdp	Ingress	Apply to all	IP ranges: 0.(	tcp:3389	Allow	default
default-allow-ssh	Ingress	Apply to all	IP ranges: 0.(	tcp:22	Allow	default

Figure 7.31 – VPC firewalls rules

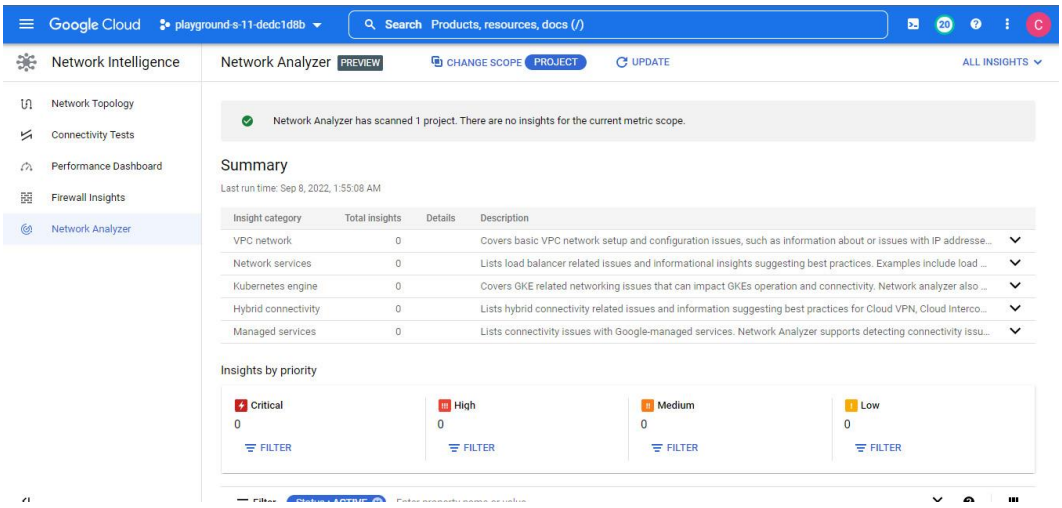

Figure 7.32 – Network Analyzer

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

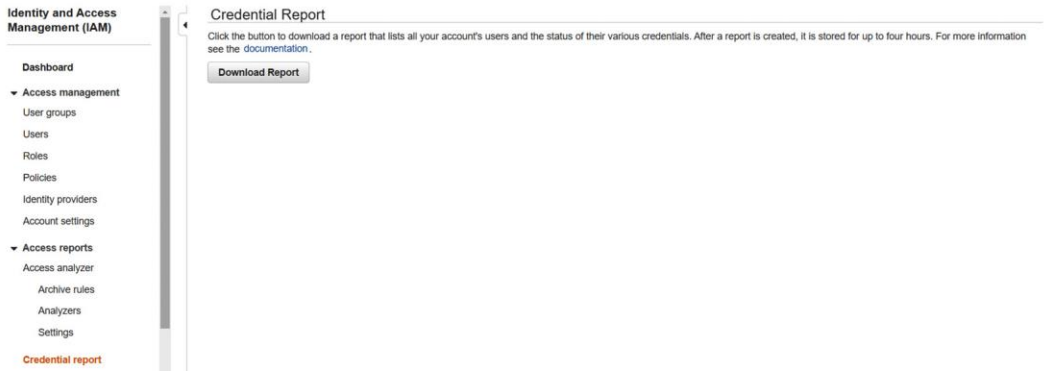

Figure 8.1 – AWS IAM Credential Report

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

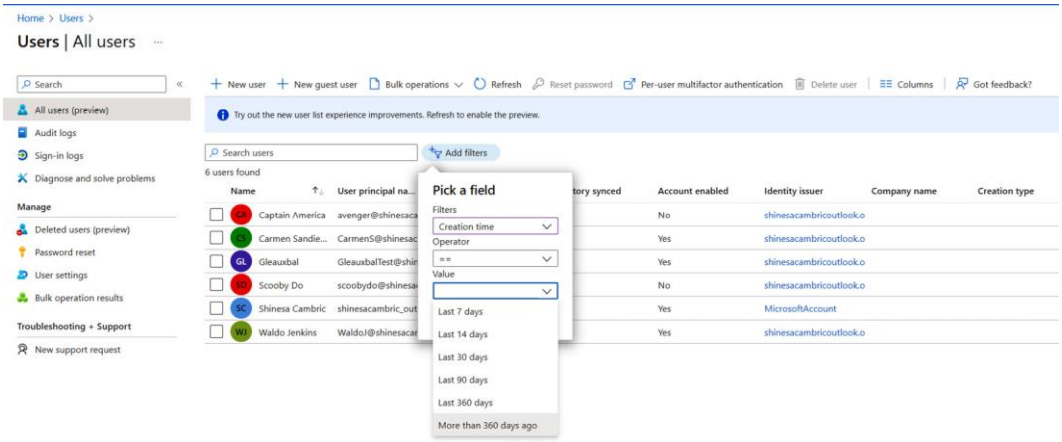

Figure 8.3 – Microsoft Azure user list

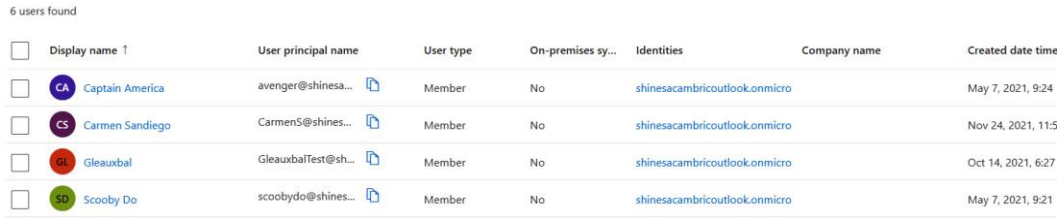

Figure 8.4 – Microsoft Azure filtered user list

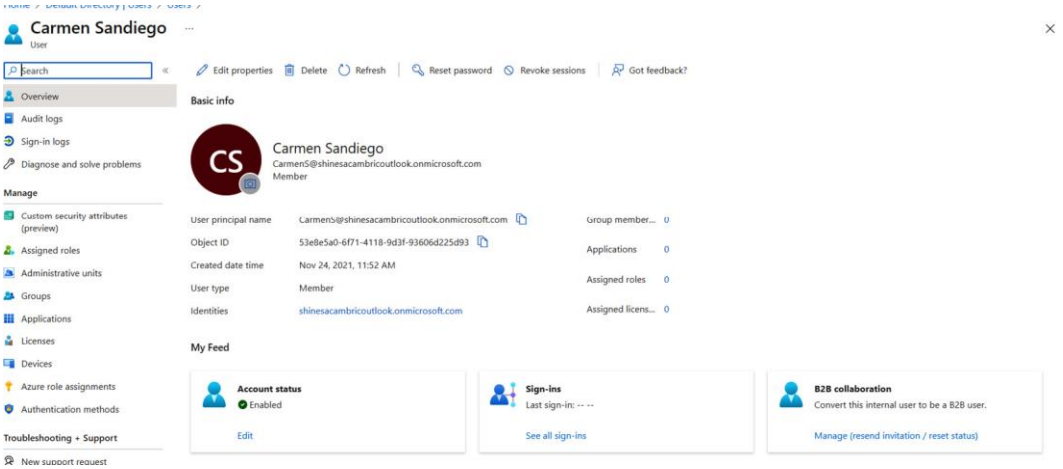

Figure 8.5 – Microsoft Azure selected user with sign-in details

Figure 8.6 – Microsoft Azure user sign-in history

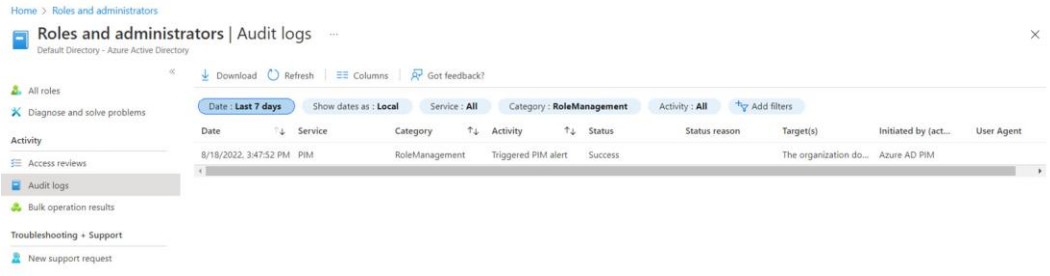

Figure 8.7 – Microsoft Azure role management audit logs

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

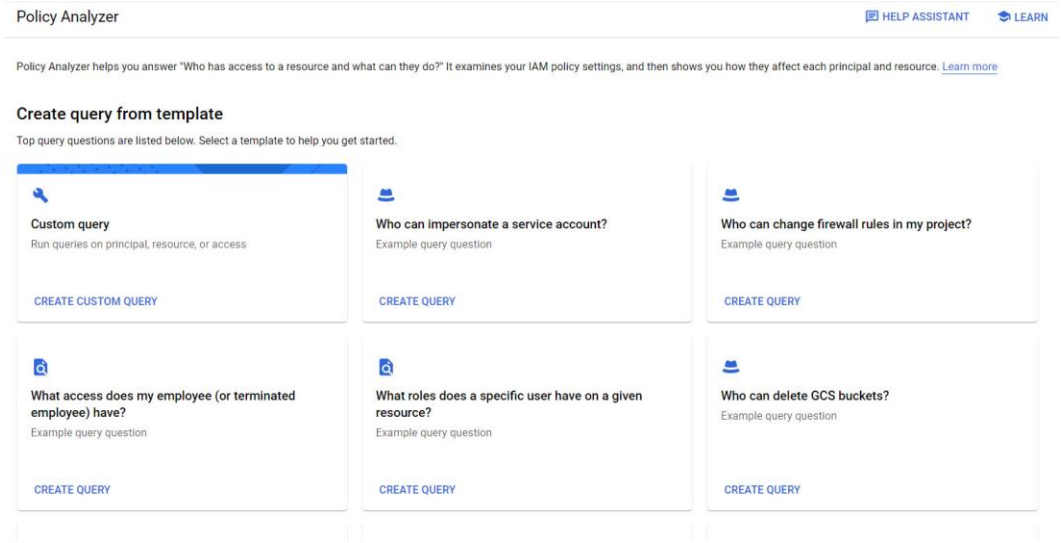

Figure 8.9 – GCP Policy Analyzer custom query

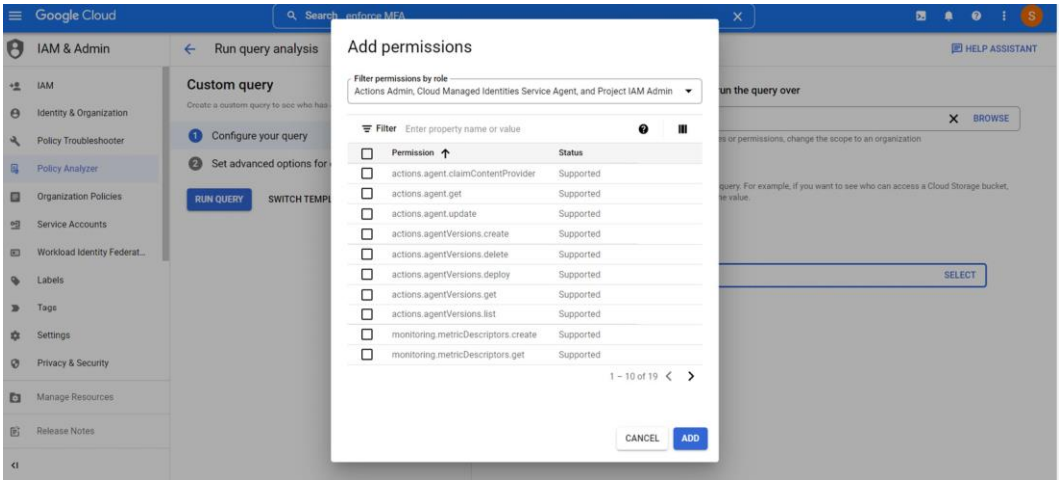

Figure 8.10 – GCP Policy Analyzer custom query filter

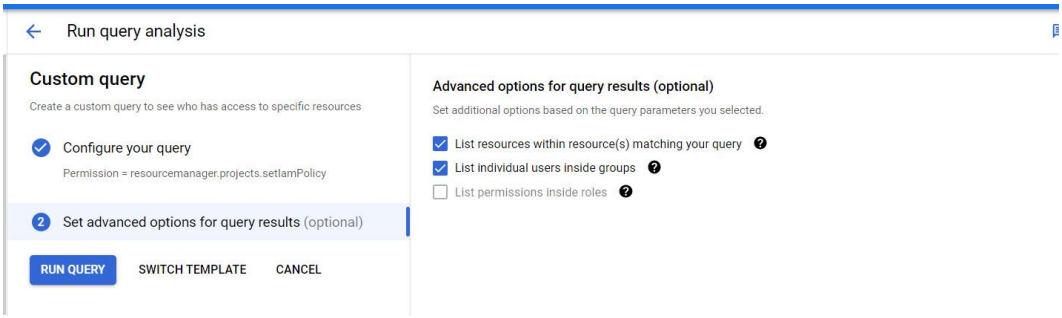

Figure 8.11 – GCP Policy Analyzer custom query and inheritance options

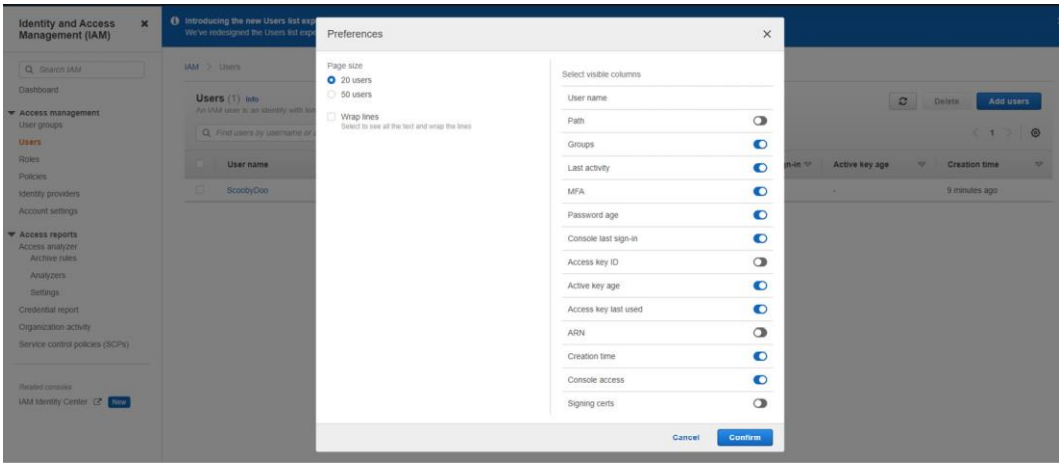

Figure 8.12 – AWS EC2 Users report column selection

Figure 8.13 – The Microsoft Azure Roles and administrators blade

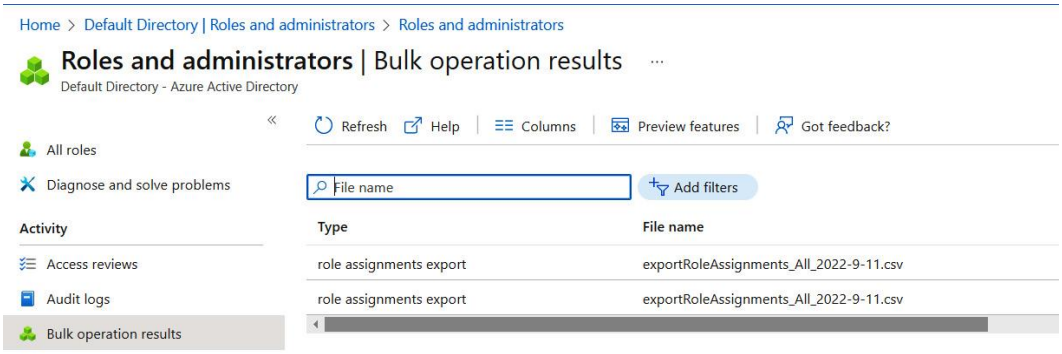

Figure 8.14 – Microsoft Azure Roles and administrators bulk operation reports

roleDisplayName	isBuiltIn	principalI	userPrincipalName	displayNa	objectType
Application Administrator	TRUE	d965573e-	scoobydo@shinesac	Scooby Do	user
Conditional Access Administrator	TRUE	a0b2c84e-	avenger@shinesaca	Captain A	user
Directory Readers	TRUE	9ae2fe0d-	00000014-0000-0000	Microsoft.	servicePrincipal
Global Administrator	TRUE	8aa2ca2b-	shinesacambric_out	Shinesa C	user
Global Administrator	TRUE	811ec4a9-	WaldoJ@shinesacar	Waldo Jer	user
Groups Administrator	TRUE	a0b2c84e-	avenger@shinesaca	Captain A	user

Figure 8.15 – The AWS EC2 Users report column selection

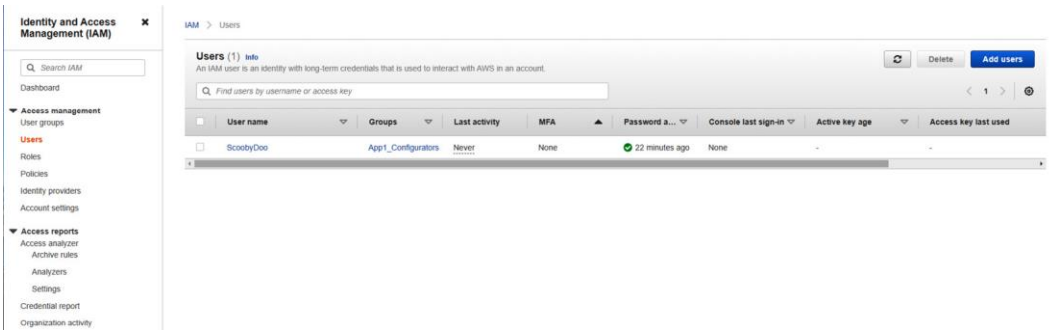

Figure 8.16 – The AWS IAM Users report column selection

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_suppo	TRUE
2022-09-11T22:05:13+00:00	TRUE	no_information	2022-09-11T22:05:13+00:00	N/A	FALSE

Figure 8.17 – The AWS IAM Users report column selection

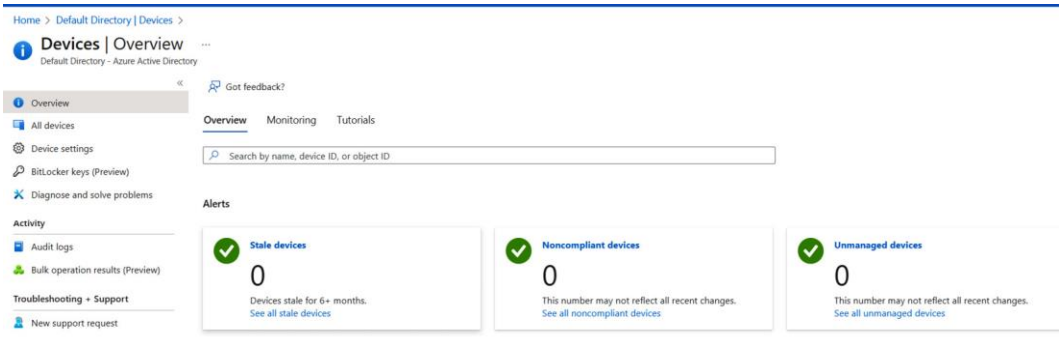

Figure 8.18 – Microsoft Azure Devices | Overview

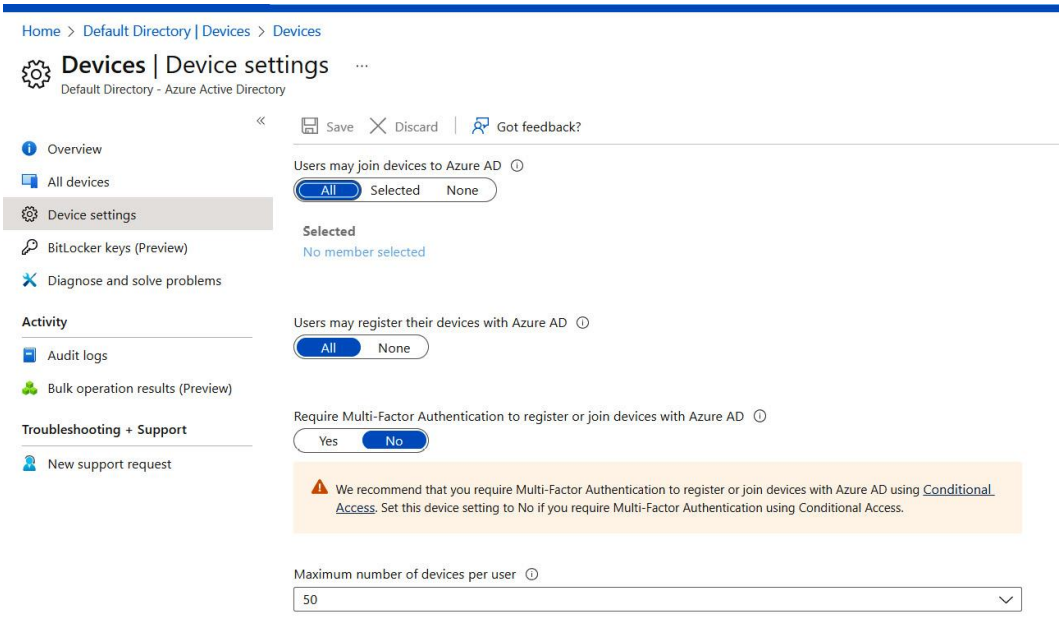

Figure 8.19 – Microsoft Azure Device settings

Chapter 9

Figures

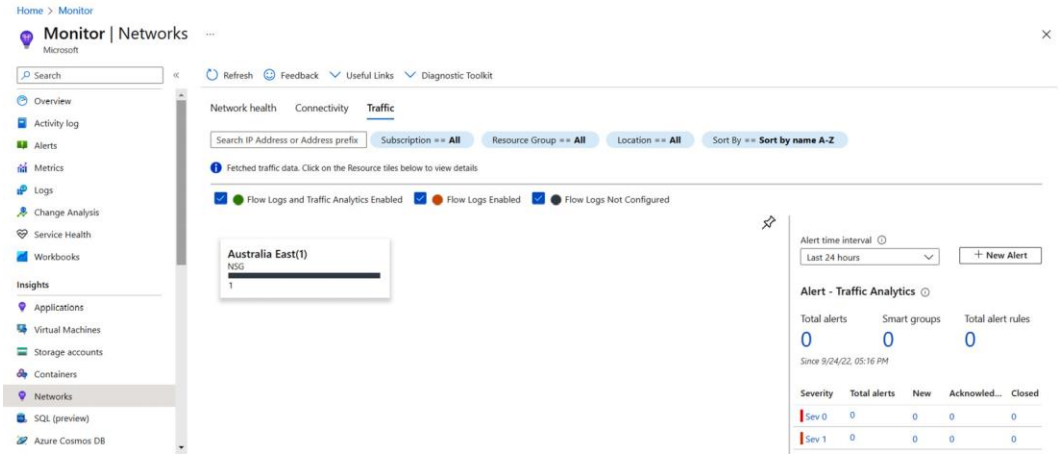

Figure 9.1 – Microsoft Azure network traffic logging

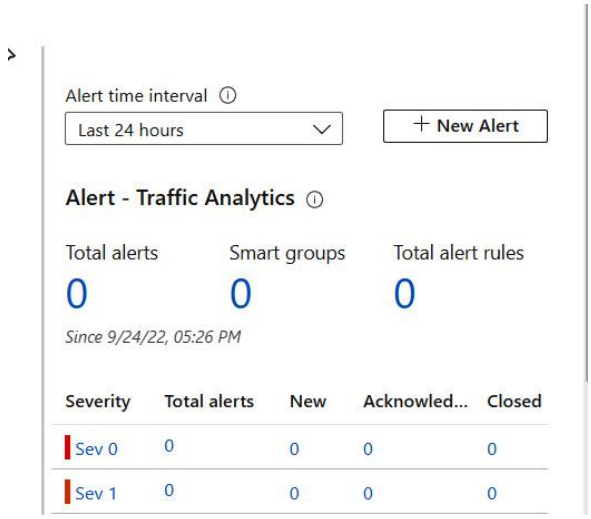

Figure 9.2 – Microsoft Azure network traffic alerts

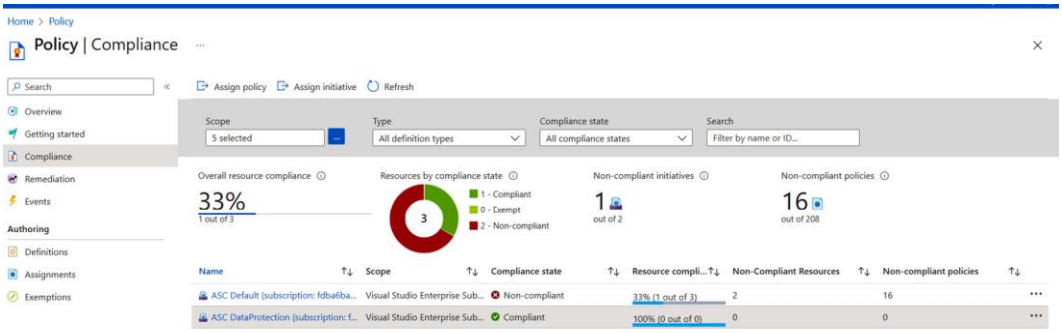

Figure 9.3 – Microsoft Azure compliance policies

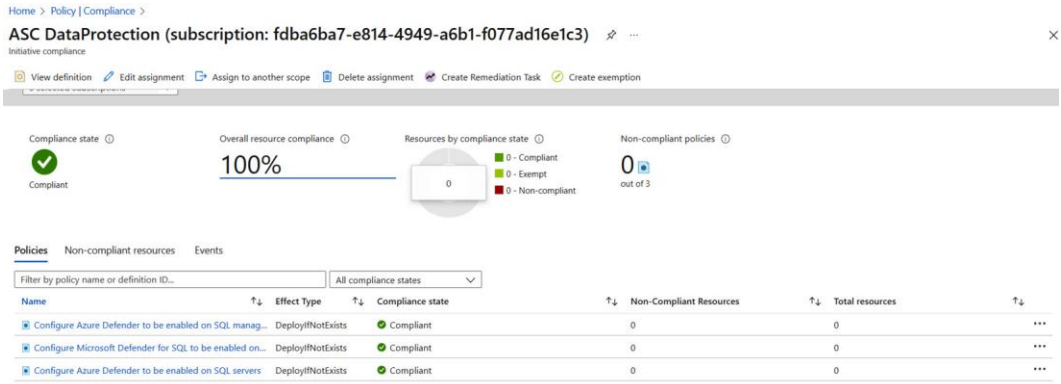

Figure 9.4 – Microsoft Azure compliance, no policies applied

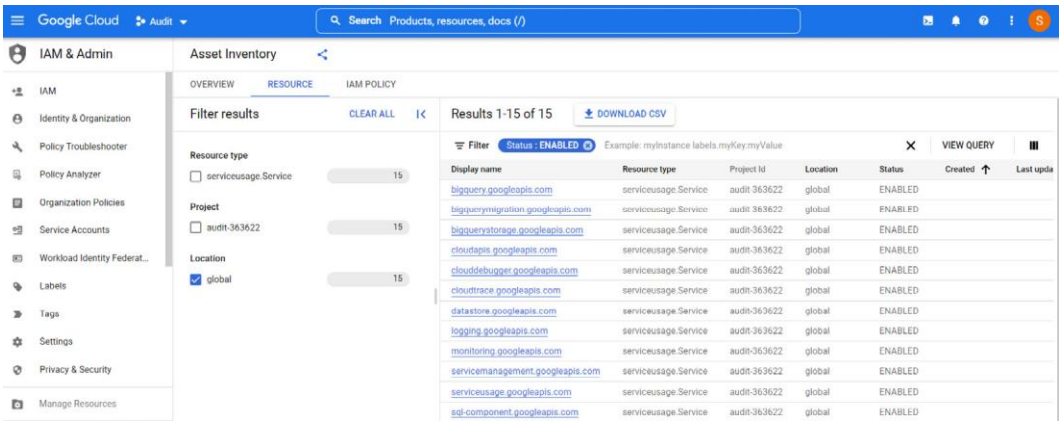

Figure 9.5 – GCP Asset Inventory

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

Figure 9.6 – GCP Asset Inventory labels and network tags

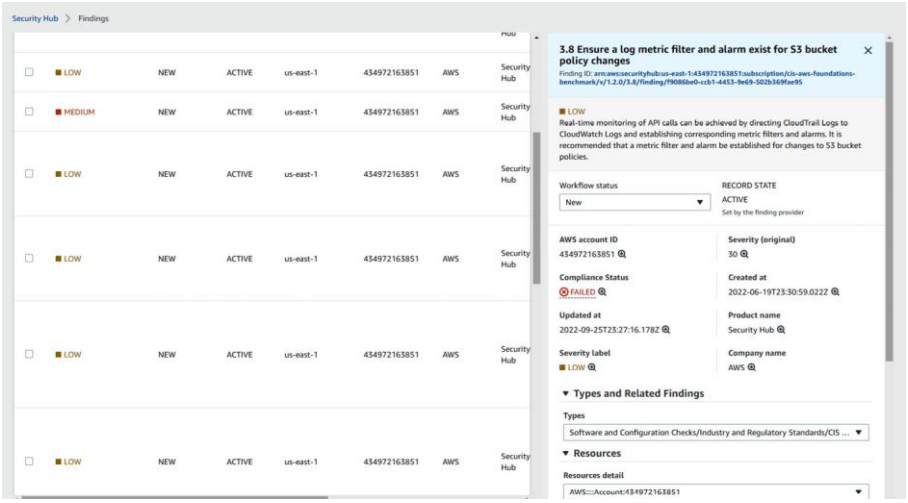

Figure 9.7 – AWS EC2 data security findings

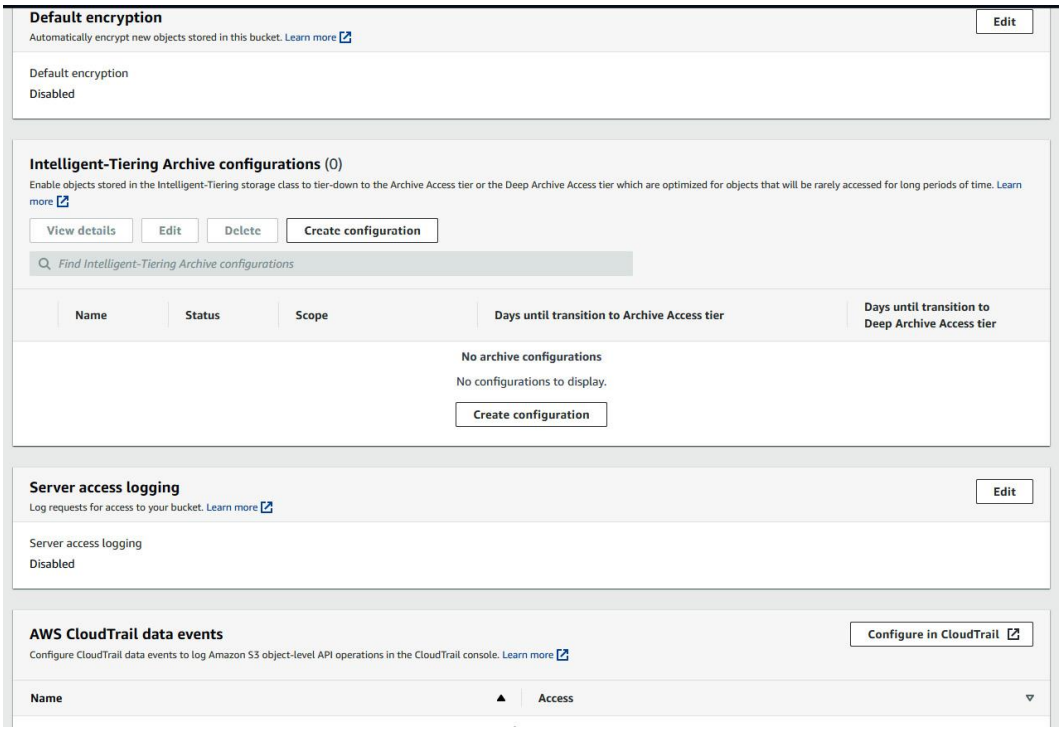

Figure 9.8 – AWS S3 bucket properties

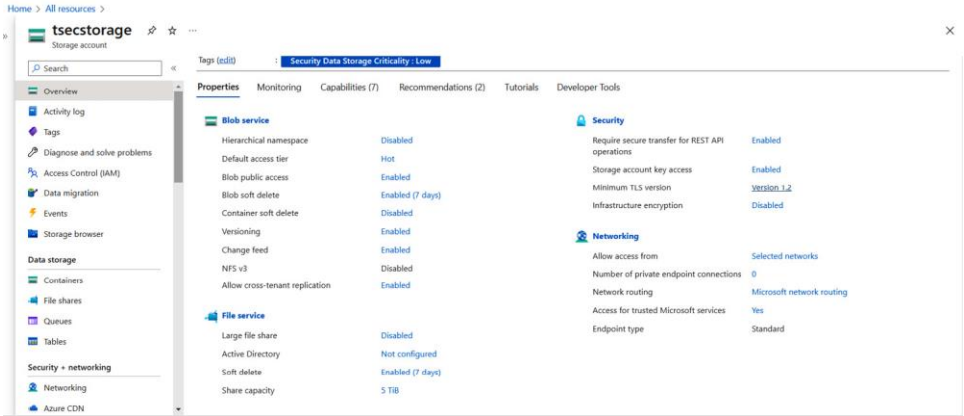

Figure 9.9 – Microsoft Azure Storage account overview

Figure 9.10 – Azure data security

Figure 9.11 – Azure encryption settings and scopes

Chapter 10

Figures

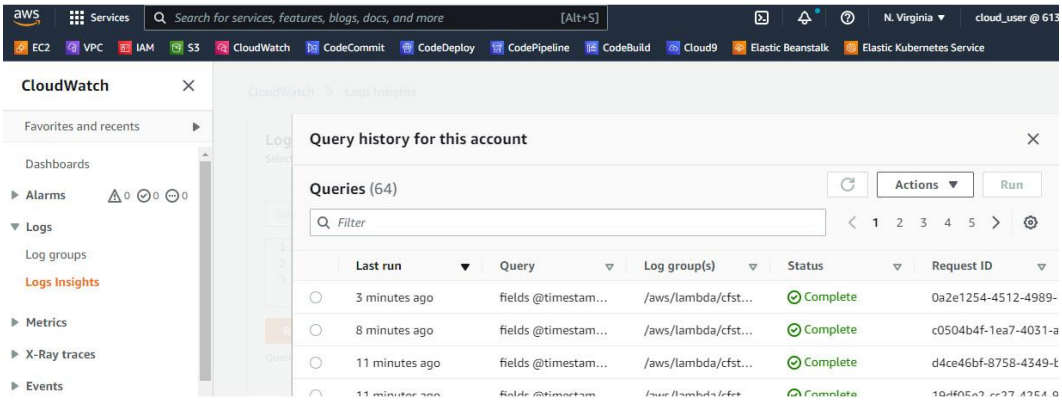

Figure 10.1 – Amazon CloudWatch Logs | Logs Insights

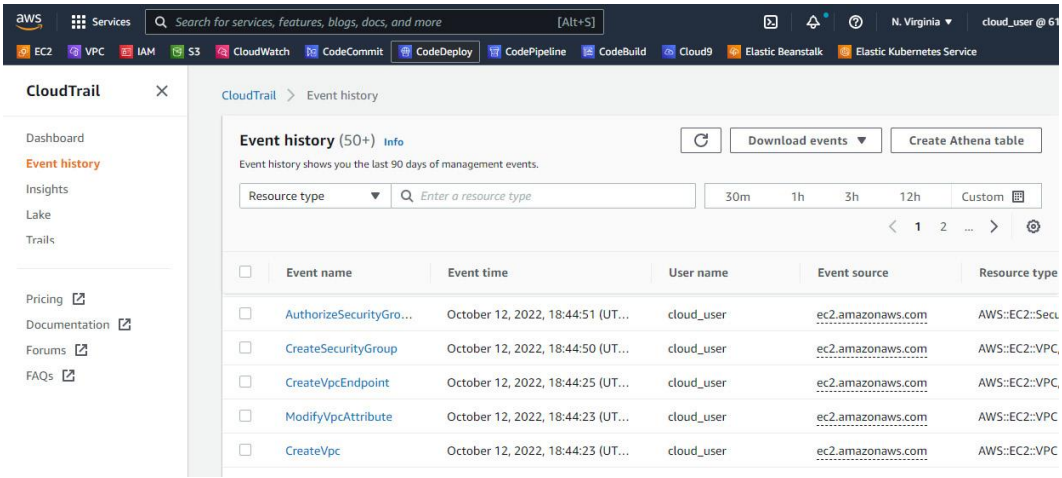

Figure 10.2 – AWS CloudWatch Logs | Event history

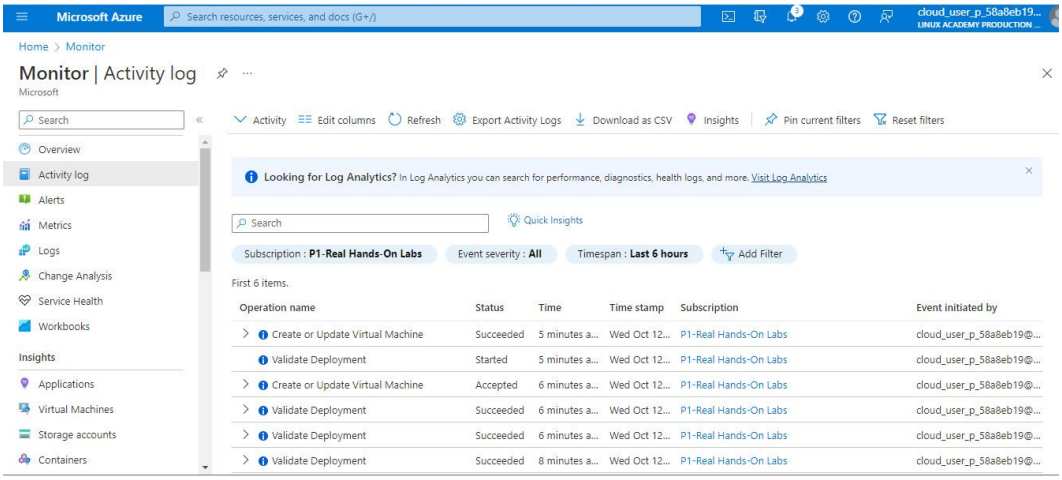

Figure 10.3 – Azure Monitor | Activity log

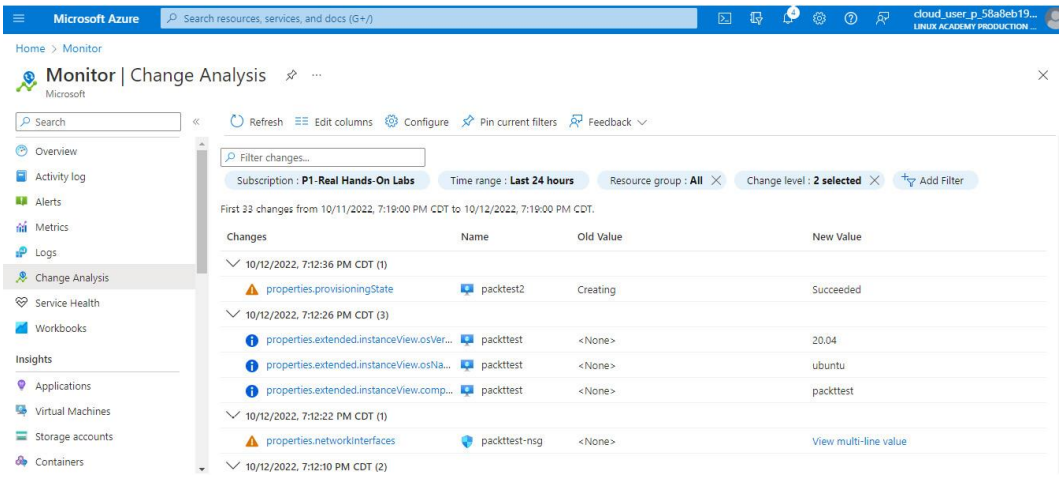

Figure 10.4 – Azure Monitor | Change Analysis

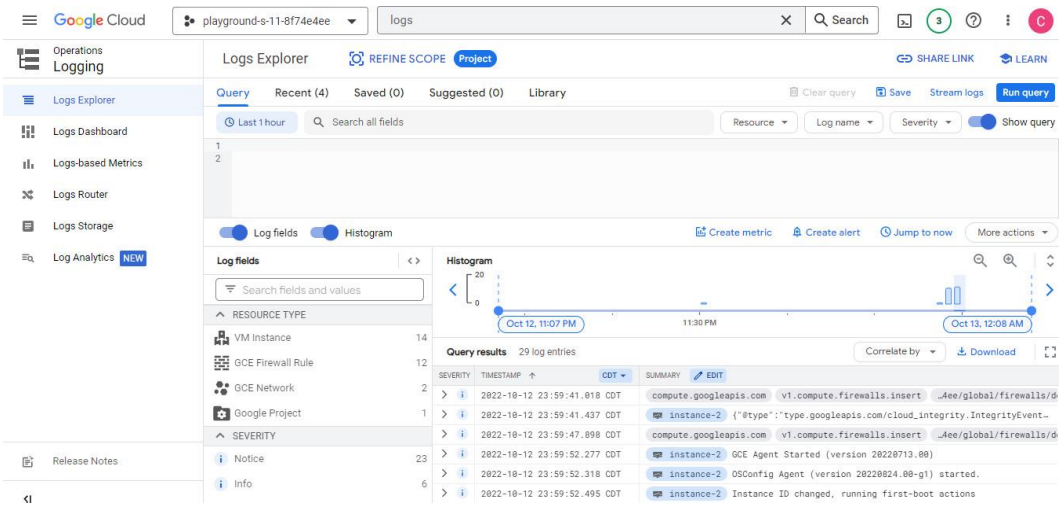

Figure 10.5 – GCP Logs Explorer

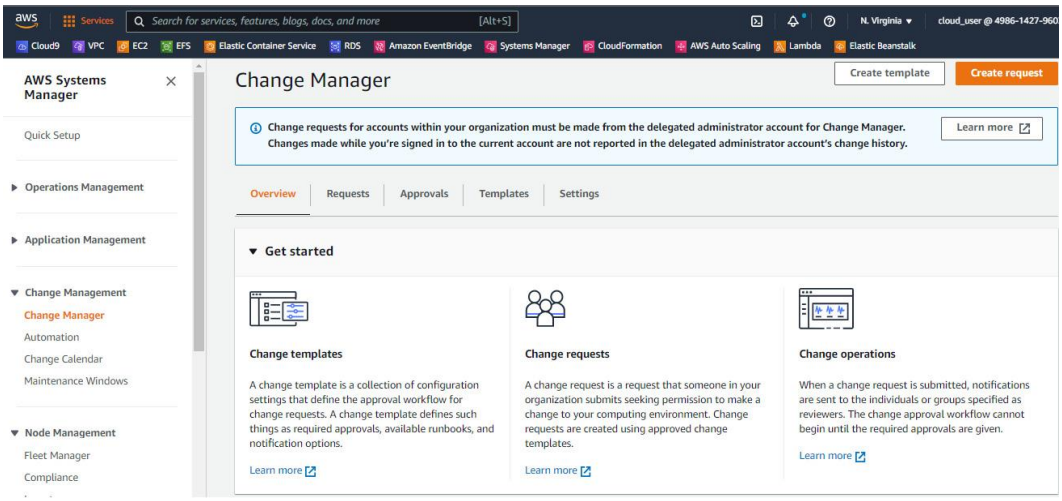

Figure 10.6 – AWS Systems Manager | Change Manager

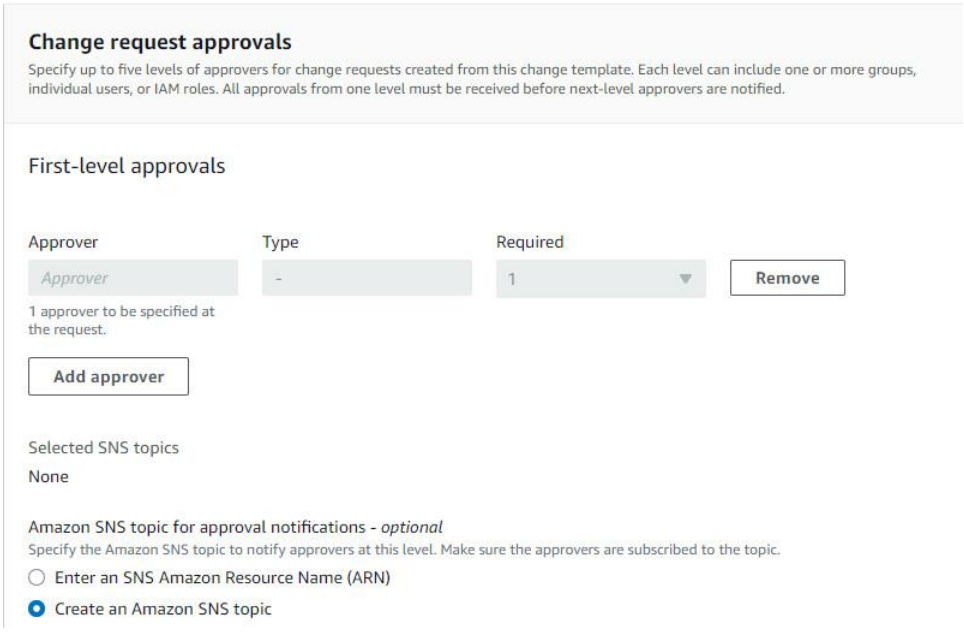

Figure 10.7 – Change Manager | Change request approvals

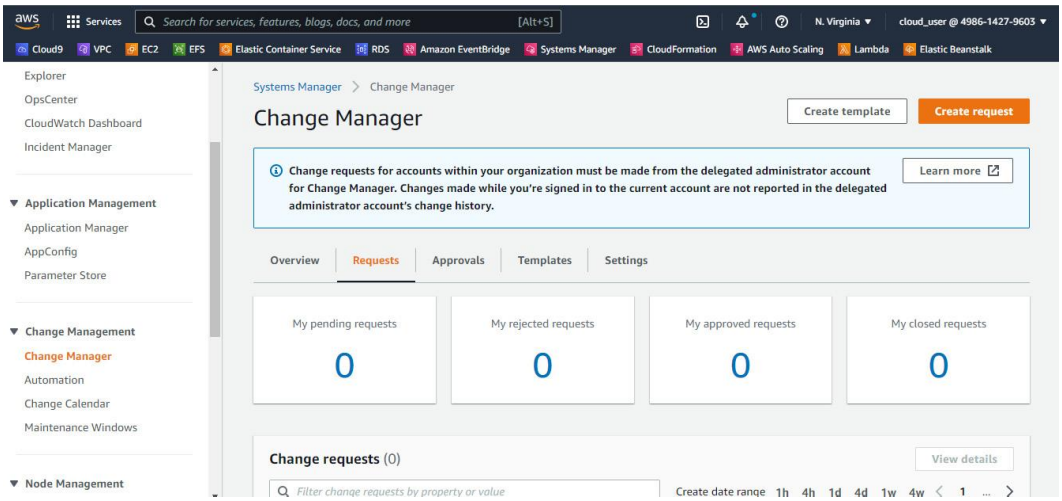

Figure 10.8 – Change Manager | Requests

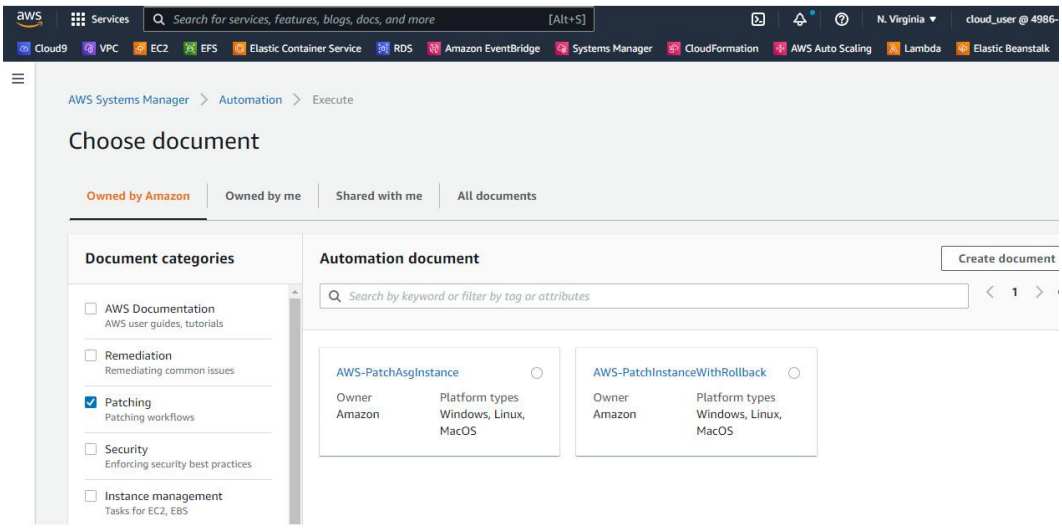

Figure 10.9 – AWS Systems Manager | Automation

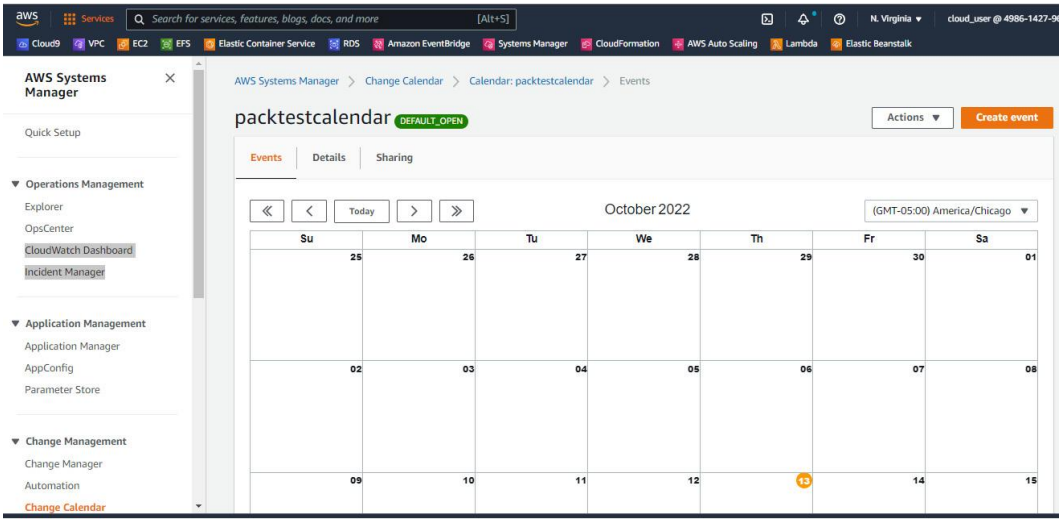

Figure 10.10 – AWS Systems Manager | Change Calendar

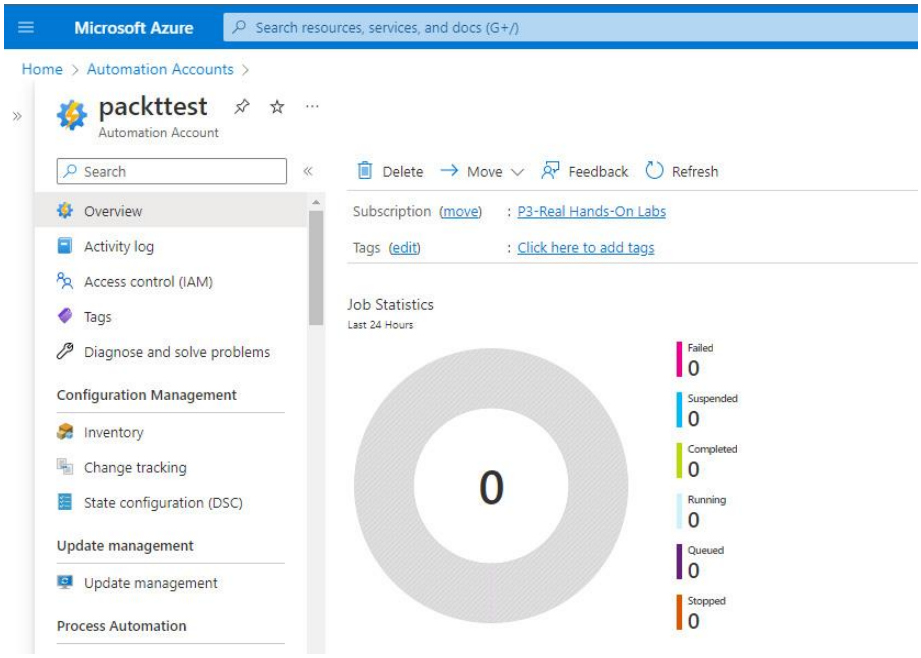

Figure 10.11 – Azure Automation Configuration Management | Change tracking

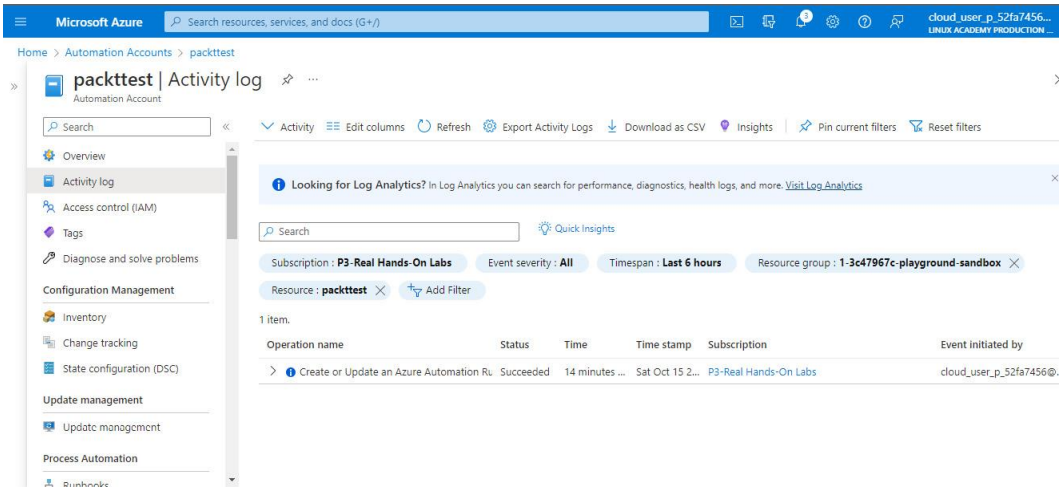

Figure 10.12 – Azure Automation | Activity log

```
# 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
digraph {
        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

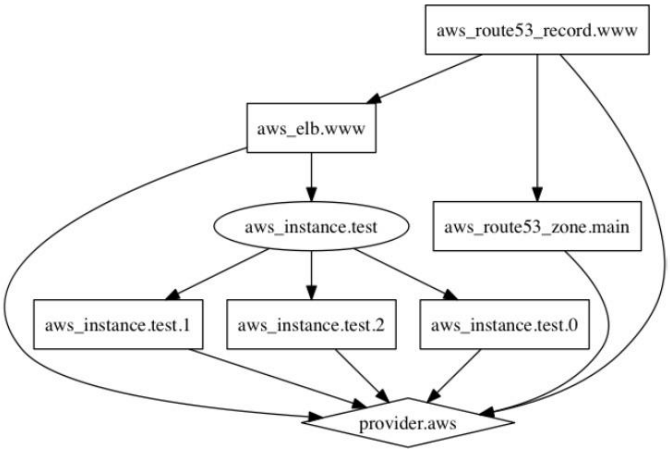

Figure 10.19 – Example of a Terraform graph output

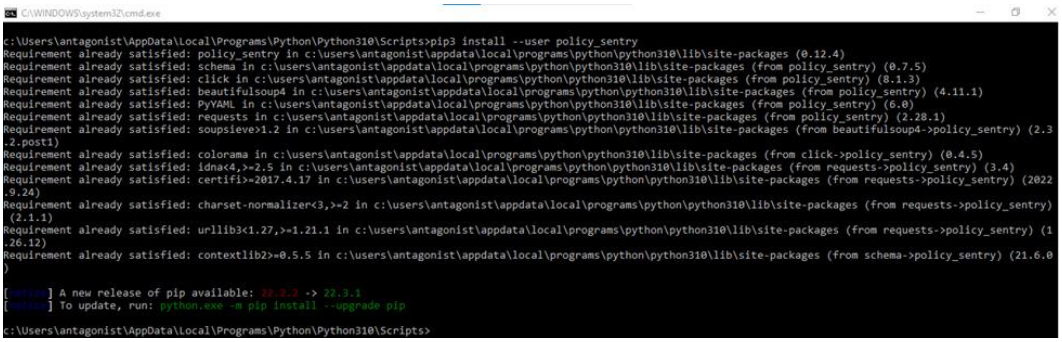

Figure 10.20 – Policy Sentry installation on the command line

```
Requirement already satisfied: contextlib2>=0.5.5 in c:\users\antagonist\appdata\local\prograr
)

[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

```
c:\Users\antagonist\AppData\Local\Programs\Python\Python310\Scripts>policy_sentry query action-table --service all --access-level permissions-management
permissions-management actions across ALL services:

acm-pca:CreatePermission
acm-pca:DeletePermission
acm-pca:DeletePolicy
acm-pca:PutPolicy
apigateway:AddCertificateToDomain
apigateway:RemoveCertificateFromDomain
apigateway:SetWebACL
apigateway:UpdateRestApiPolicy
backup:DeleteBackupVaultAccessPolicy
backup:PutBackupVaultAccessPolicy
chime:DeleteVoiceConnectorTerminationCredentials
chime:PutVoiceConnectorTerminationCredentials
cloudformation:SetStackPolicy
cloudsearch:UpdateServiceAccessPolicies
codeartifact:DeleteDomainPermissionsPolicy
codeartifact:DeleteRepositoryPermissionsPolicy
codebuild:DeleteResourcePolicy
codebuild:DeleteSourceCredentials
codebuild:ImportSourceCredentials
codebuild:PutResourcePolicy
codeguru-profiler:PutPermission
codeguru-profiler:RemovePermission
codestar:AssociateTeamMember
codestar:CreateProject
codestar:DeleteProject
codestar:DisassociateTeamMember
codestar:UpdateTeamMember
cognito-identity:CreateIdentityPool
cognito-identity:DeleteIdentities
cognito-identity:DeleteIdentityPool
cognito-identity:GetId
cognito-identity:MergeDeveloperIdentities
cognito-identity:SetIdentityPoolRoles
cognito-identity:UnlinkDeveloperIdentity
cognito-identity:UnlinkIdentity
cognito-identity:UpdateIdentityPool
deeplens:AssociateServiceRoleToAccount
```

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

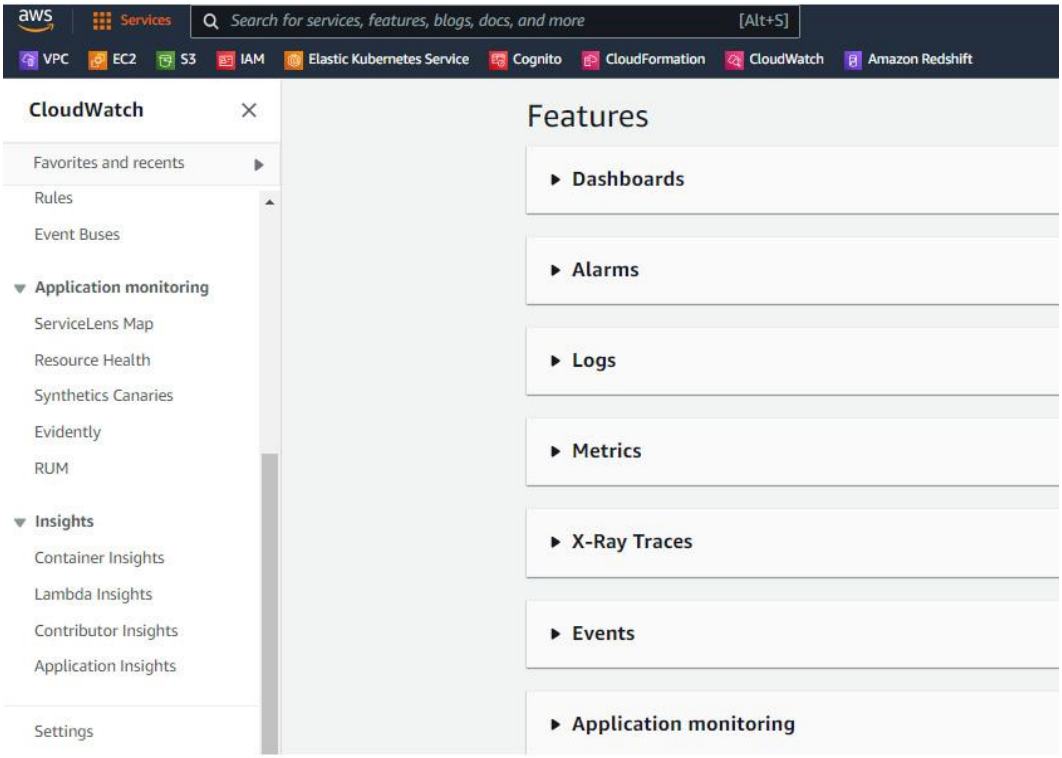

Figure 10.24 – Amazon CloudWatch

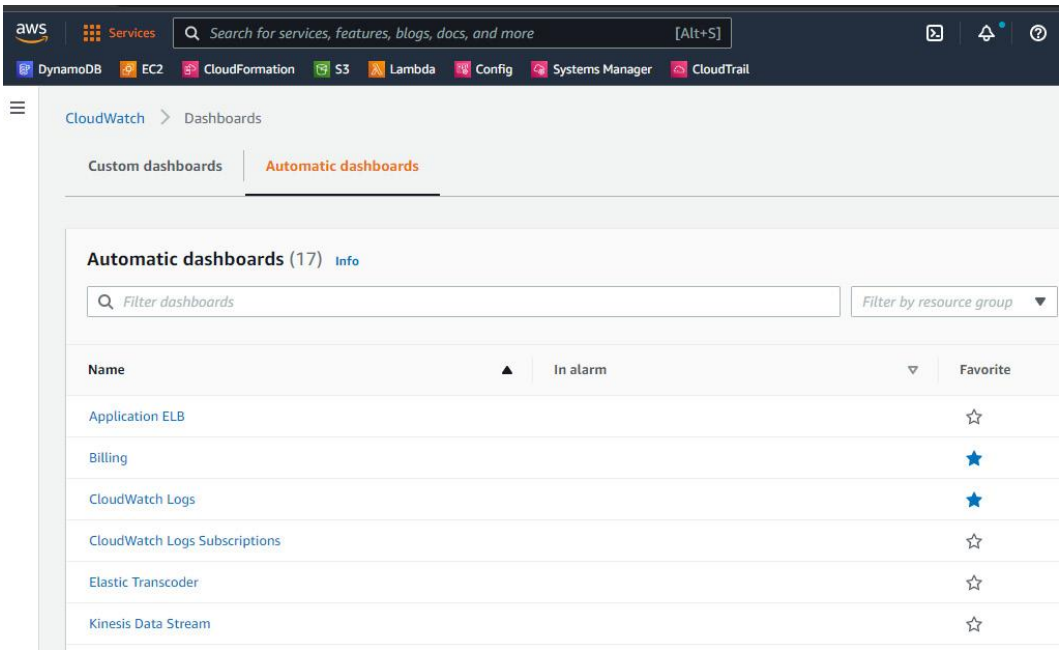

Figure 10.25 – CloudWatch | Dashboards

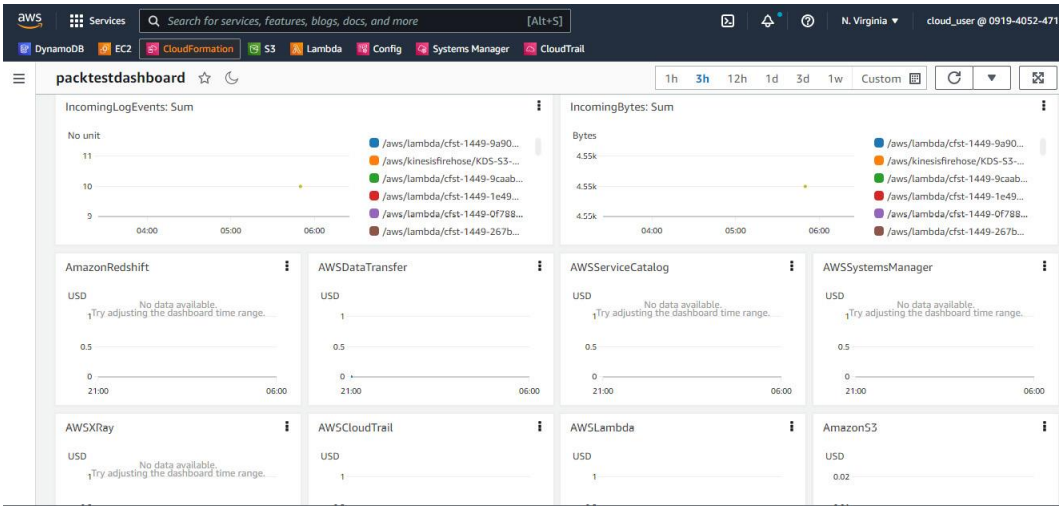

Figure 10.26 – CloudWatch | packtestdashboard

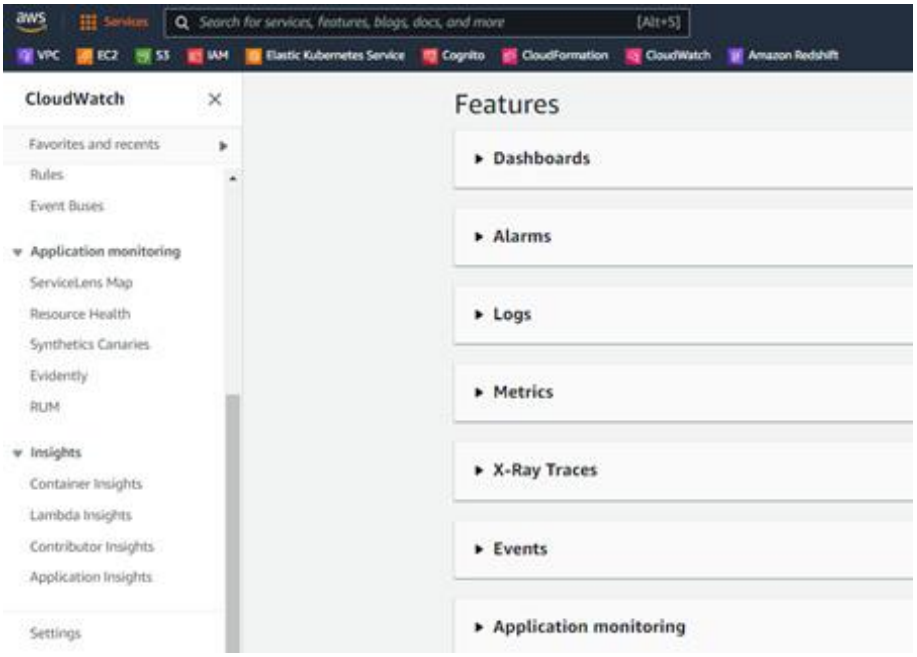

Figure 10.27 – CloudWatch | Alarms

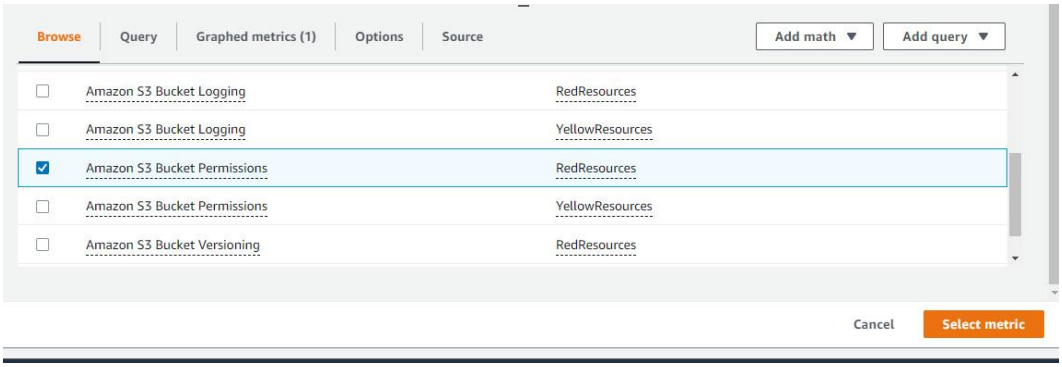

Figure 10.28 – Amazon S3 Bucket Permissions metric

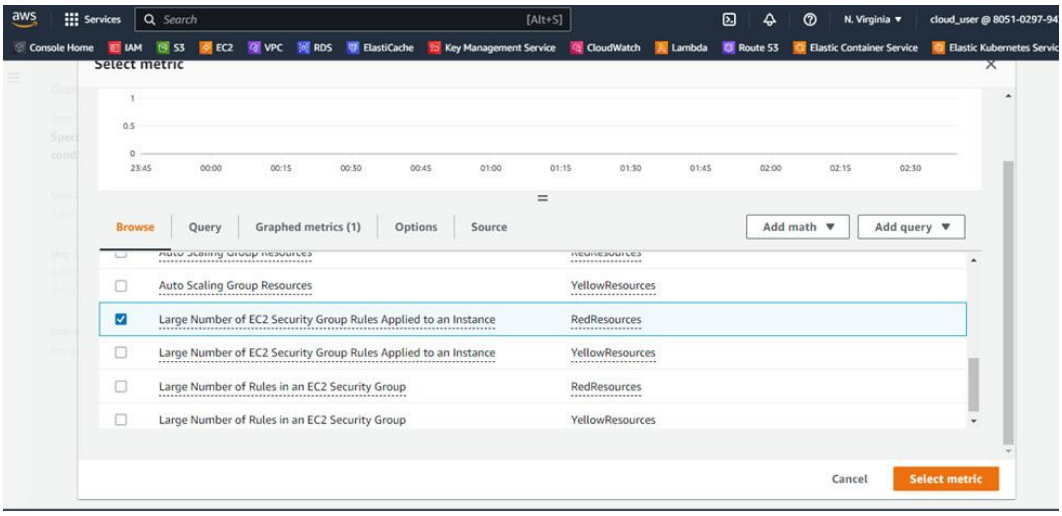

Figure 10.29 – The Large Number of EC2 Security Group Rules Applied to an Instance metric

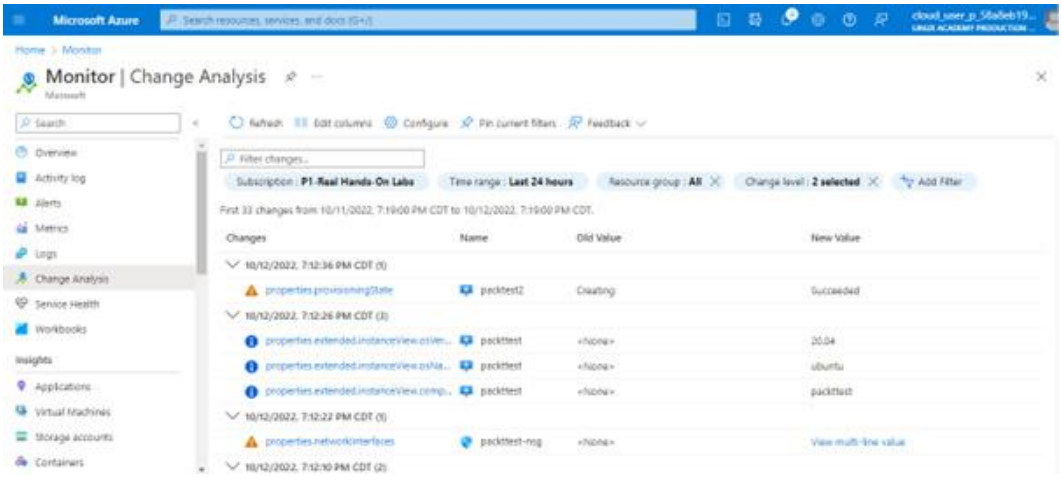

Figure 10.30 – Azure Monitor | Change Analysis

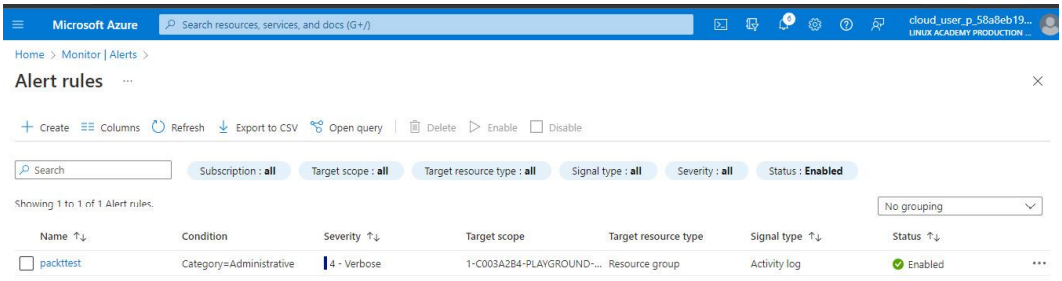

Figure 10.31 – Azure Monitor | Alert rules

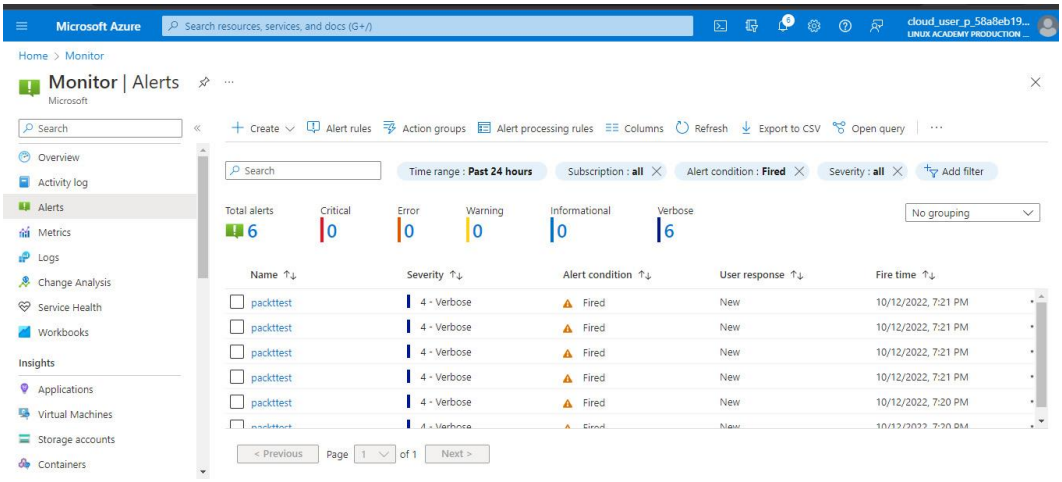

Figure 10.32 – Azure Monitor | Alerts

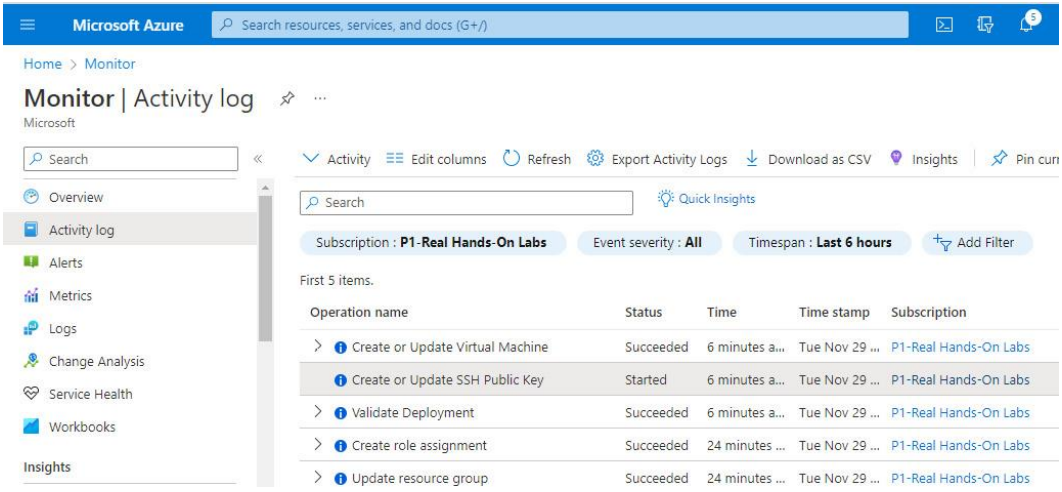

Figure 10.33 – Azure Monitor | Activity log

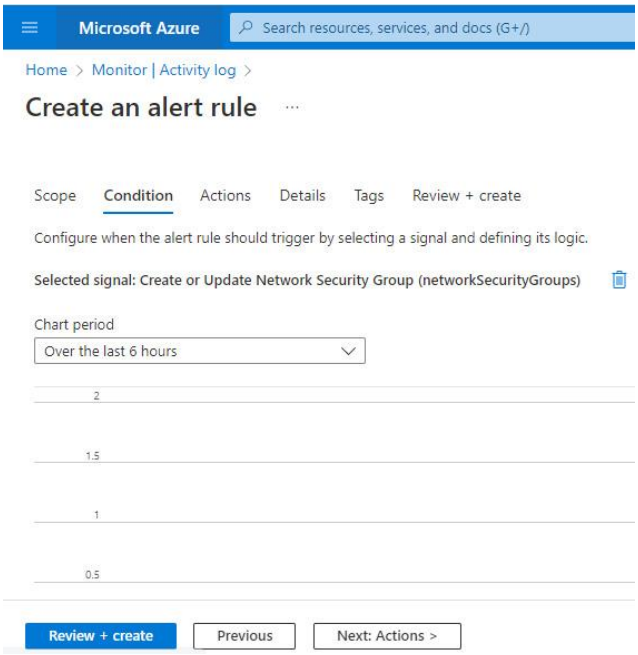

Figure 10.34 – Alert Rule: Create or Update Network Security Group

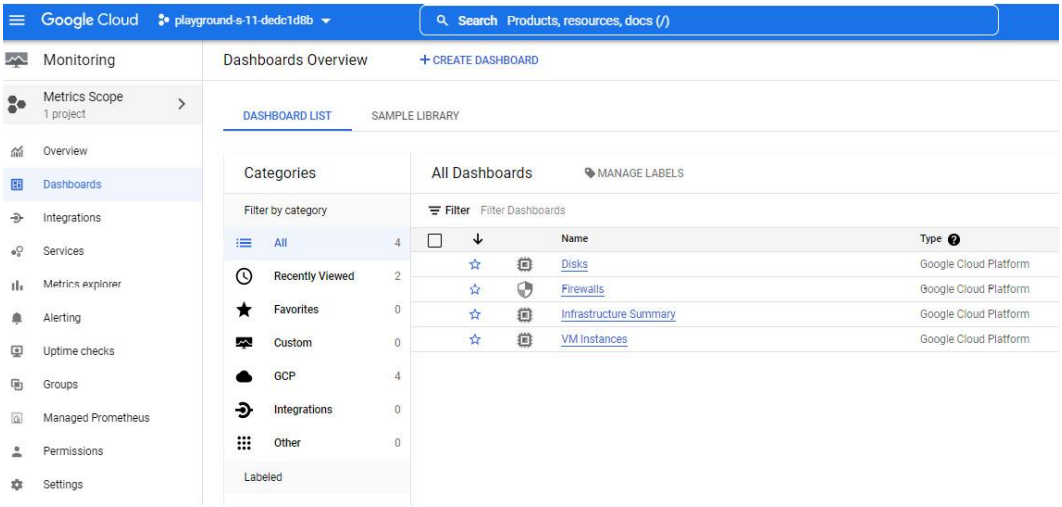

Figure 10.35 – Google Cloud Monitoring

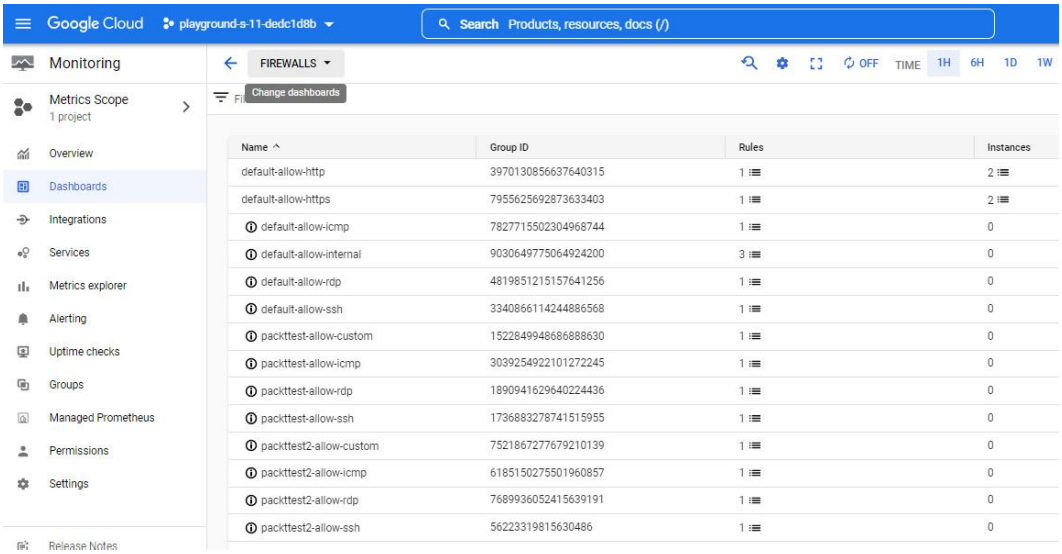

Figure 10.36 – Google Cloud Monitoring | Dashboards

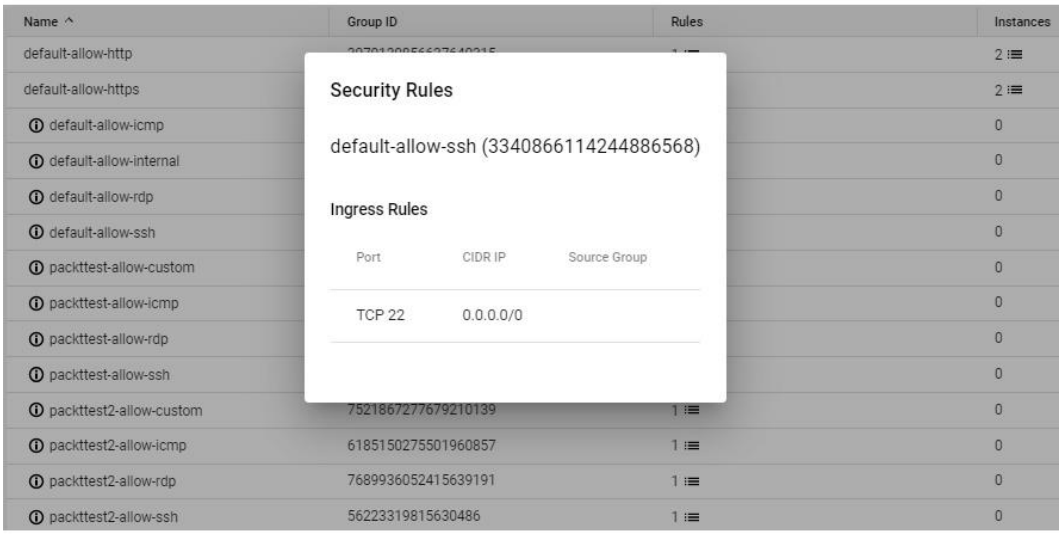

Figure 10.37 – Security Rules

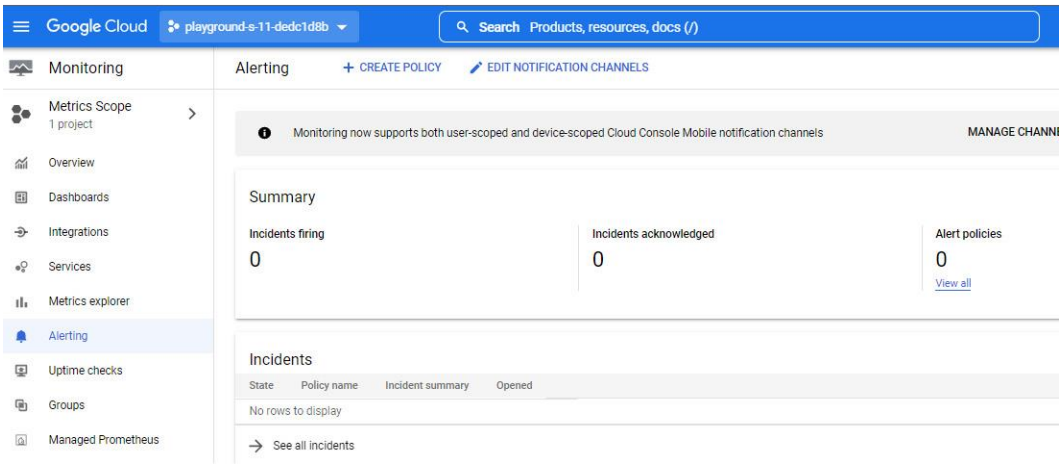

Figure 10.38 – Google Cloud Monitoring | Alerting

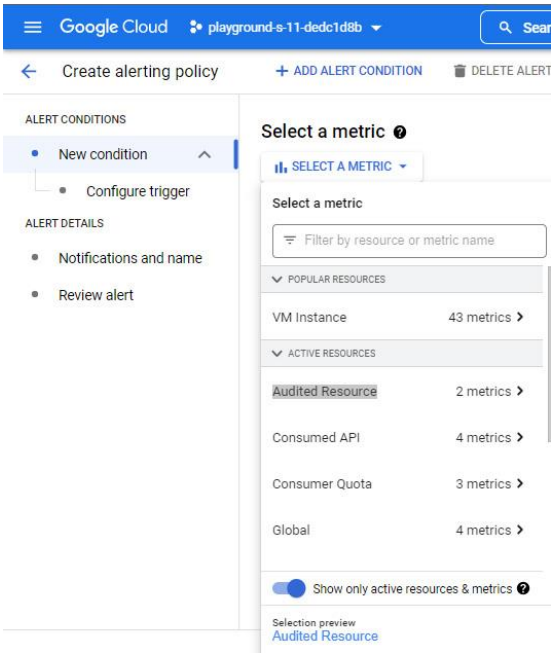

Figure 10.39 – Create alerting policy | Audited Resource metric

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.