Performing a Basic Audit of your AWS Environment

Lab overview

In this lab, you perform basic audits of core AWS resources. You use the AWS Management Console to understand how to audit the use of multiple AWS services, such as Amazon EC2, Amazon VPC, Amazon IAM, Amazon Security Groups, AWS CloudTrail, and Amazon CloudWatch. This lab teaches you how to extend your existing auditing objectives related to organizational Governance, Asset Configuration, Logical Access Controls, Operating Systems, Databases, and Applications security configurations within AWS.

Objectives

By the end of this lab, you will be able to do the following:

- Review user permissions in AWS IAM.
- Capture audit evidence using AWS IAM Policy Simulator.
- Review Inbound and Outbound networking rules for Amazon EC2 Security Groups.
- Review Amazon VPC configurations, subnets, and Network ACLs.
- Review Amazon CloudWatch performance metrics.
- Review raw Amazon CloudTrail logs within Amazon S3.

Technical knowledge prerequisites

To successfully complete this lab, you should be familiar with basic AWS services.

Start lab

1. To launch the lab, at the top of the page, choose **Start Lab**.

Caution: You must wait for the provisioned AWS services to be ready before you can continue.

2. To open the lab, choose **Open Console** .

You are automatically signed in to the AWS Management Console in a new web browser tab.

Warning: Do not change the **Region** unless instructed.

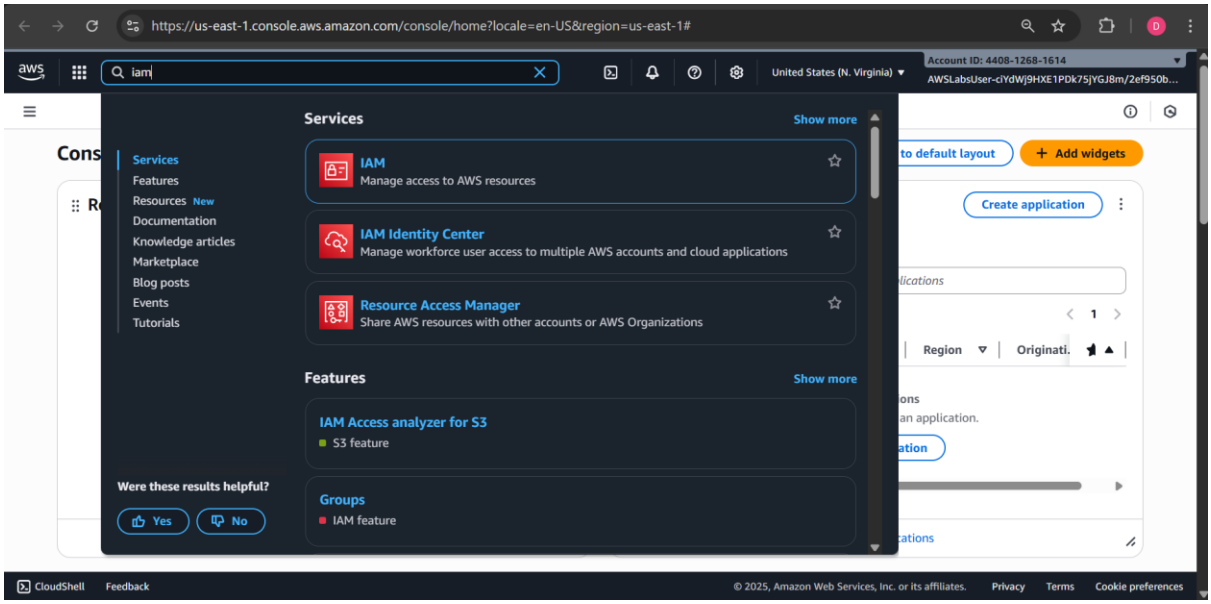
Task 1: Audit user permissions in IAM

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

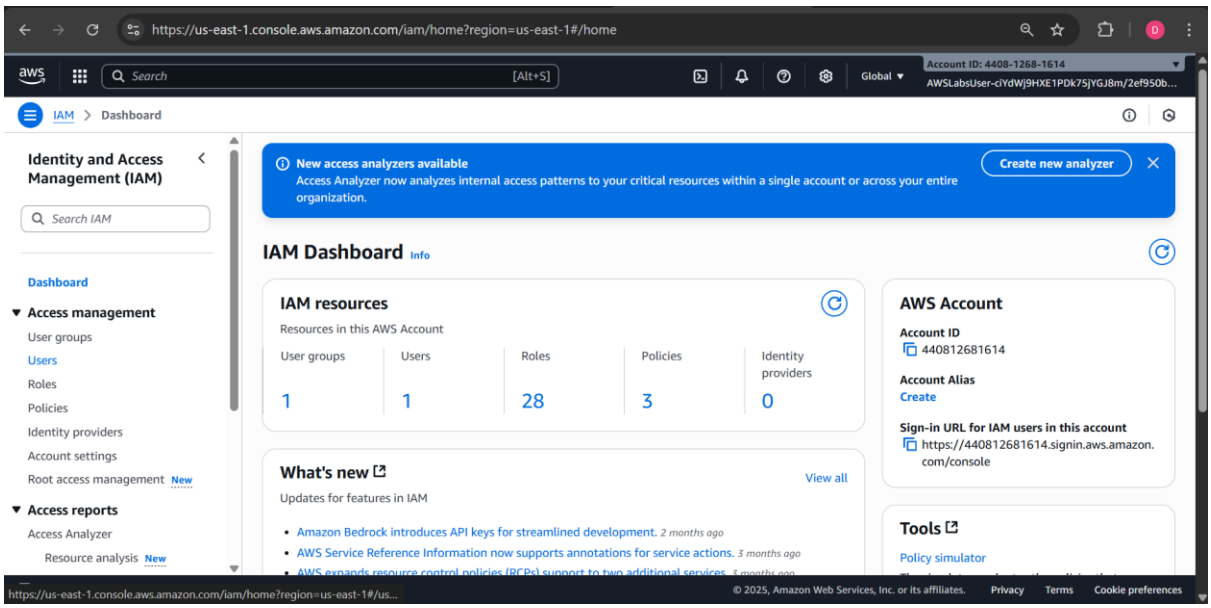
In this lab, you launch IAM secure AWS Access Control in order to review permissions, group assignments and roles associated with the auditing instance:

Review your permissions

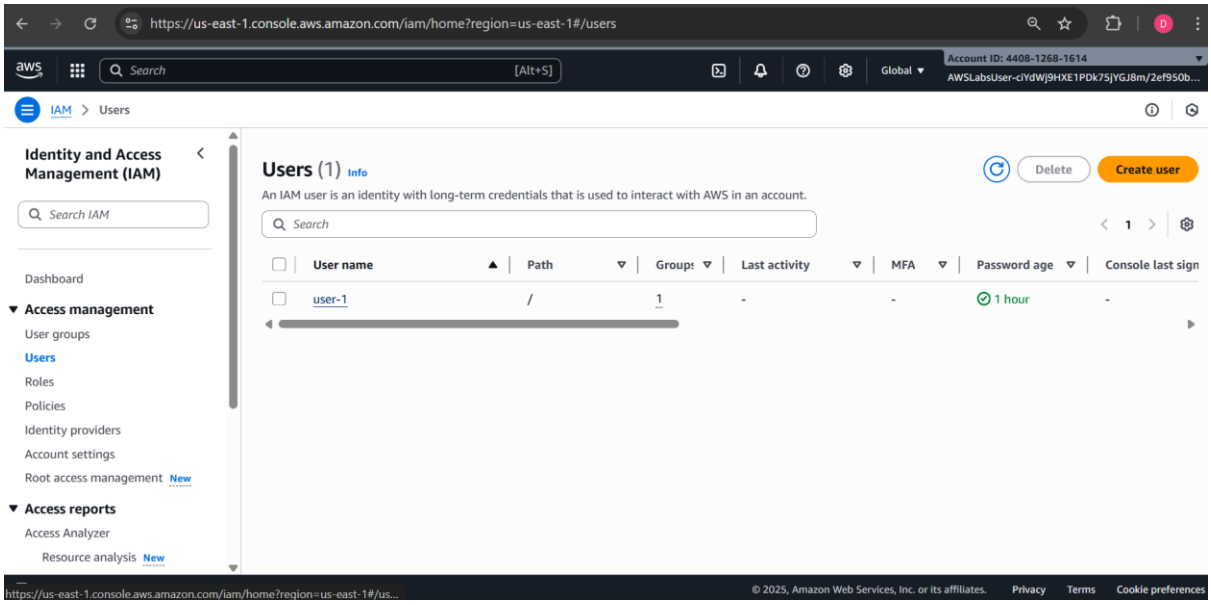
3. At the top of the AWS Management Console, in the search bar, search for and choose IAM



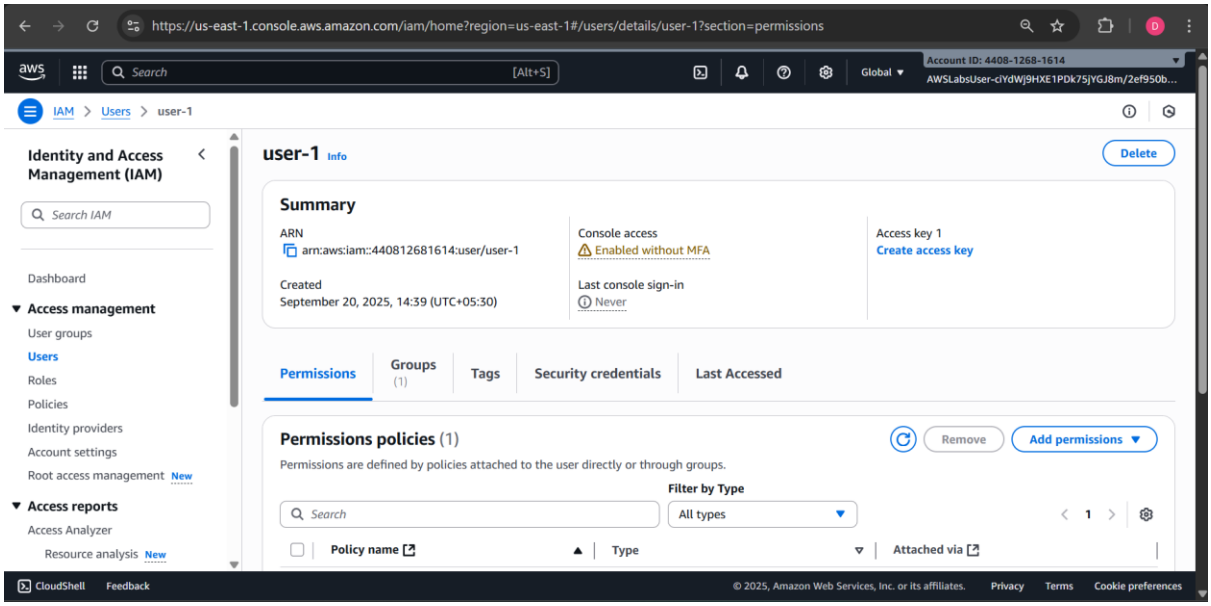
4. In the navigation pane at the left of the page, under **Access management**, choose **Users**.



5. On the **Users** page, choose the link for **user-1** to view its details.



6. Review the **Summary** section for information about your user.

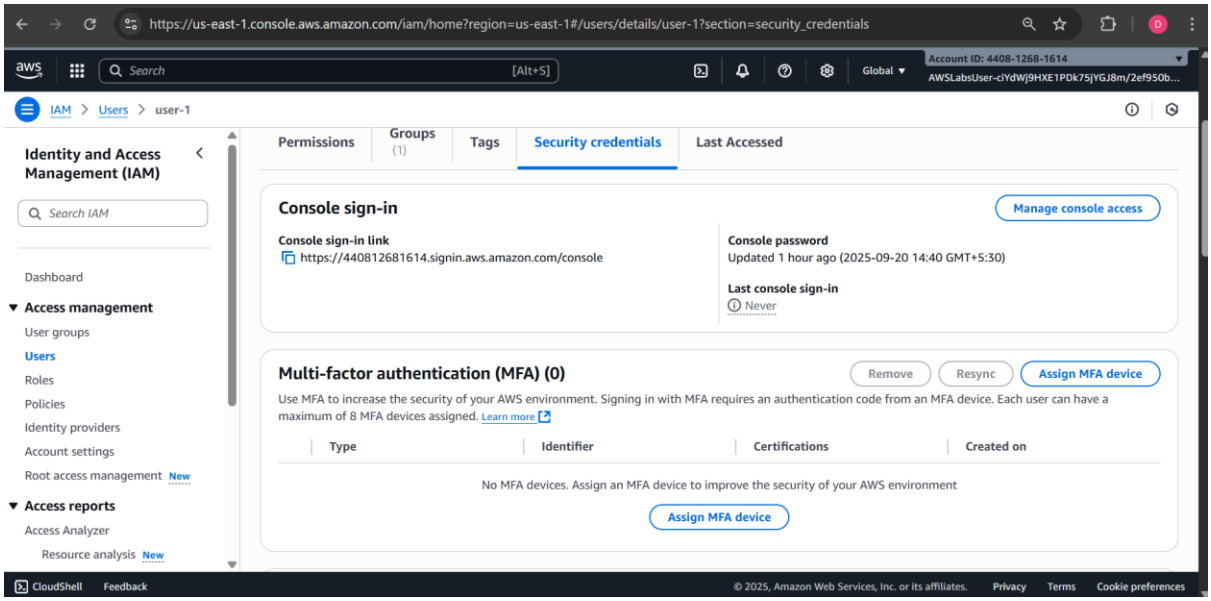


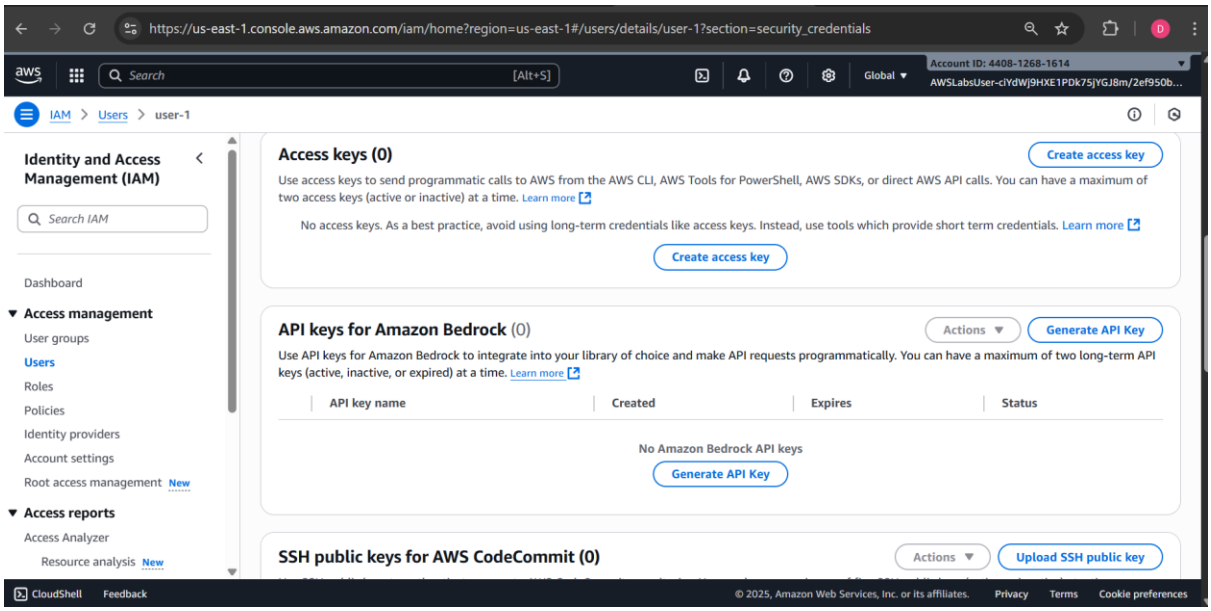
7. Select the **Security credentials** tab to review it.

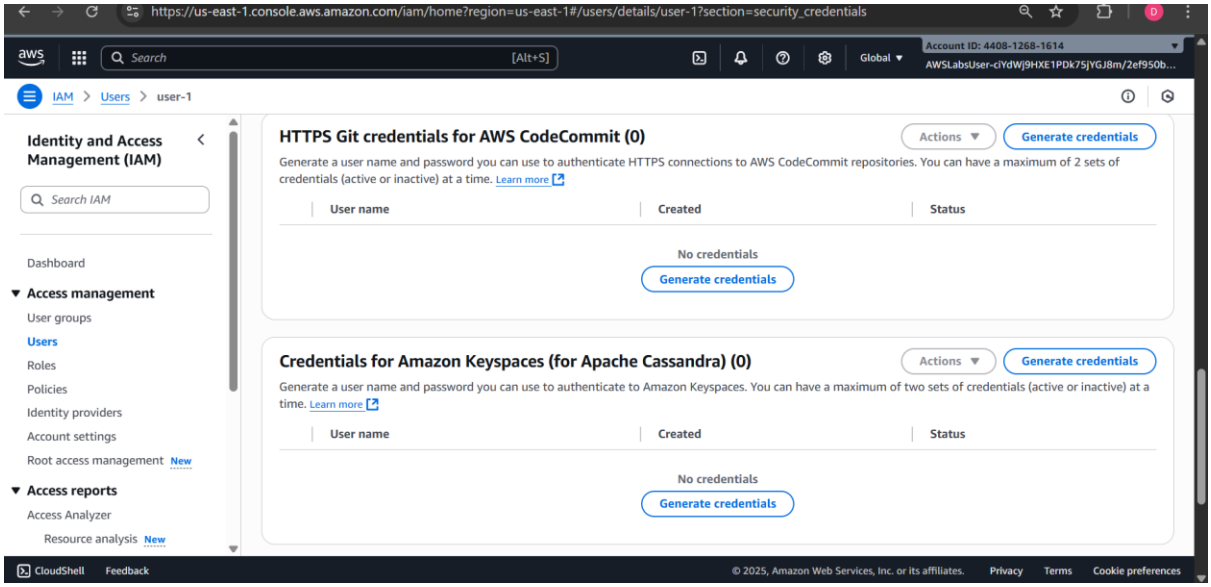
Here, you can see how many access keys a user has, when an access key was created, whether a Multi-Factor Authentication (MFA) device is assigned, and more.

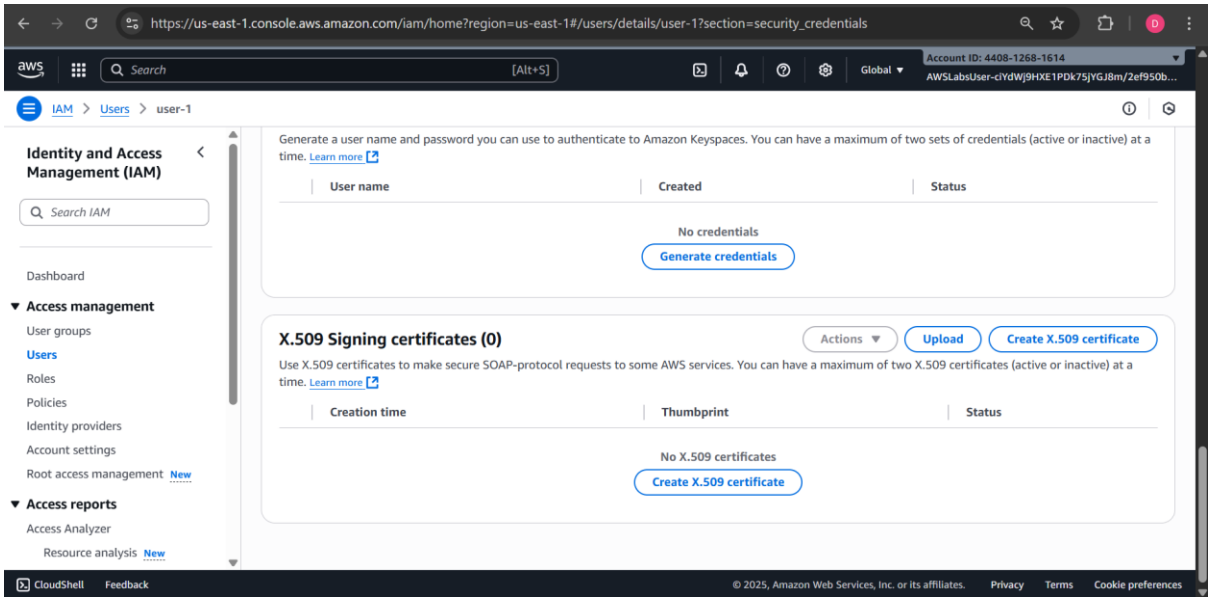
- **Access Keys:** Keys can be active or inactive and only administrators have the ability to inactivate or delete keys. If a user with limited permissions tried to deactivate or delete an access key, they would receive a message similar to the following:
    - *We encountered the following errors while processing your request: User:arn:aws:iam::111122223333:user/user-1_01 is not authorized to perform: iam:UpdateAccessKey on resource: user user-1_01*
- **Signing Certificates:** Can be signed certificates, X.509 Certificate and/or third party tools (e.g. OpenSSL).

- **Console password:** Users with access to the AWS Management Console require a password. Passwords can be generated and/or changed by administrators within the IAM dashboard. Passwords can be auto-generated or custom-generated based on organization preferences.
- **Assigned MFA (Multi-Factor Authentication) Device:** Multi-Factor Authentication is a simple best practice that adds an extra layer of protection on top of your username and password.
- **Virtual:** Use your existing smartphone, tablet, or computer running any application that supports the open TOTP standard.
- **Hardware Keyfob:** Tamper-evident hardware keyfob device provided by Gemalto, a 3rd-party provider.
- **Hardware Display Card:** Tamper-evident hardware display card device provided by Gemalto, a 3rd-party provider.





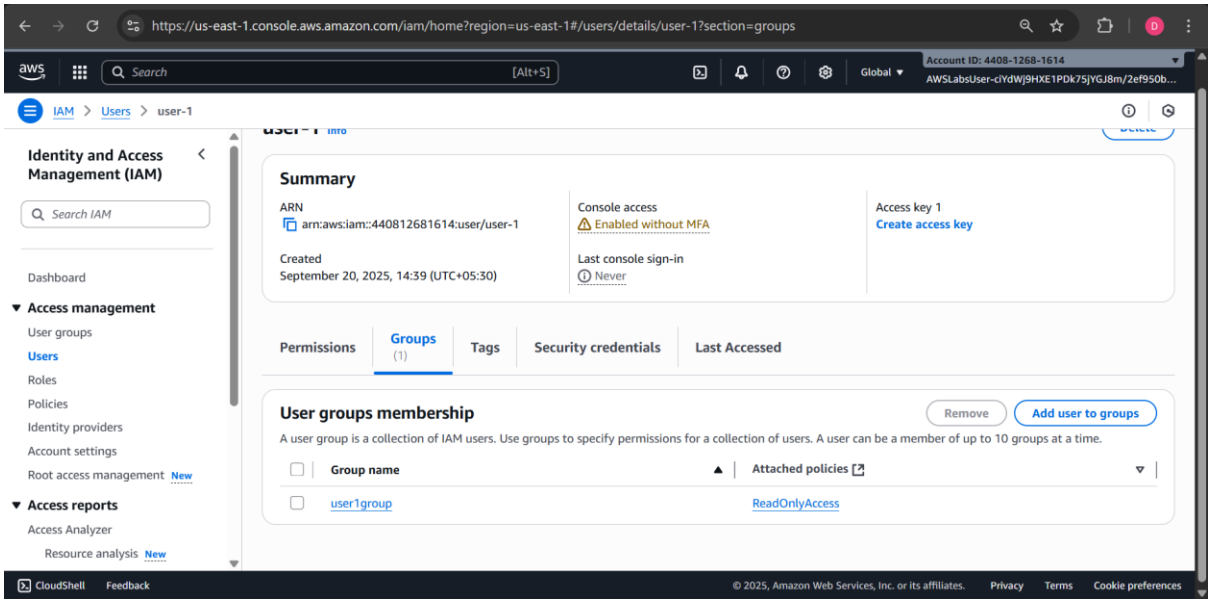




8. Choose the **Groups** tab.

Consider: Which groups is *user-1* associated with?

Notice that *user-1* is a member of the *user1group* group. Groups are a collection of IAM users. Administrators use groups to specify permissions for a collection of users to manage those permissions more efficiently.

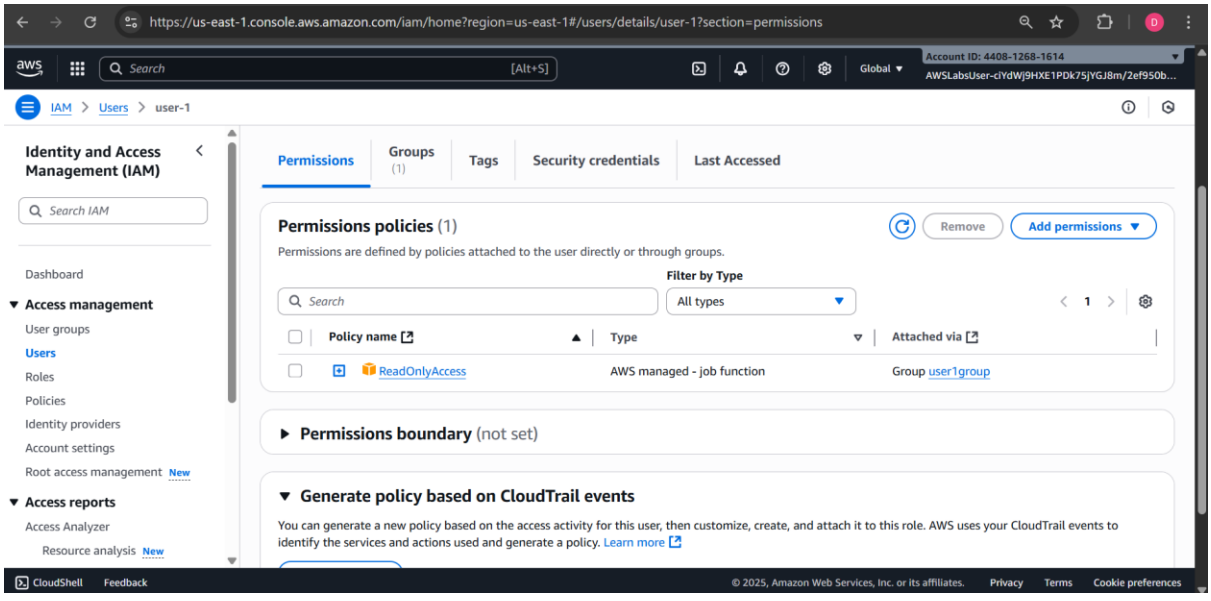


Run the IAM Policy Simulator

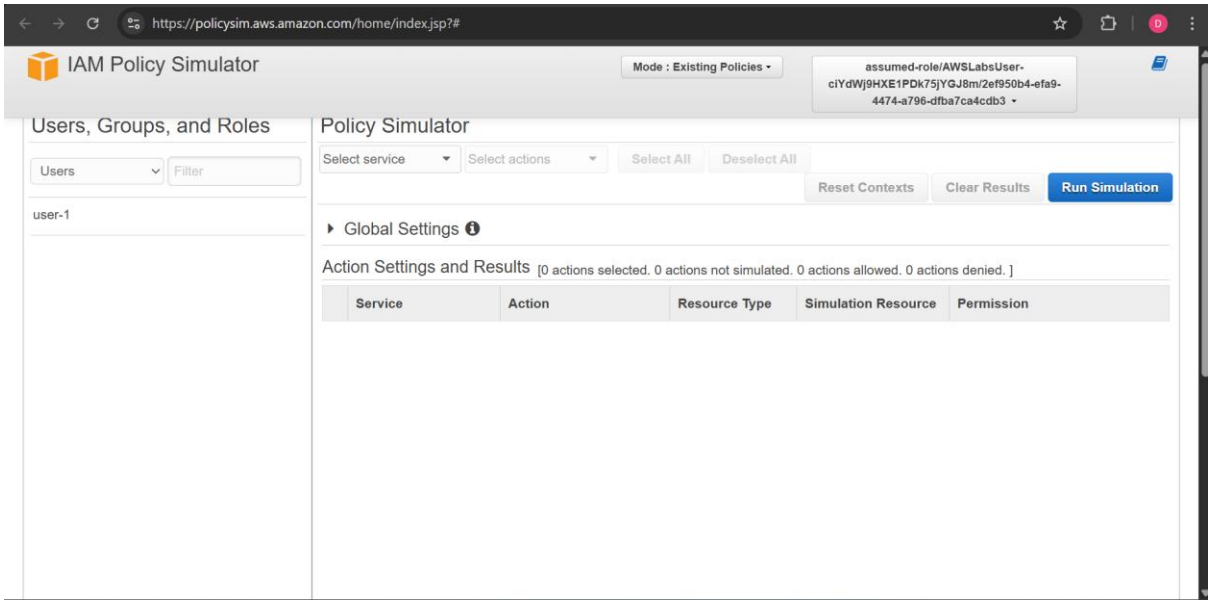
You can use the IAM Policy Simulator to test the effects of AWS IAM policies to test your existing IAM policies to verify that they have the intended effect and capture the Policy Simulator output to use as supporting evidence in user access reviews.

9. Choose the **Permissions** tab.

In the **Permissions policies** section, notice there is one policy attached to the user. The **Attached via** column shows that the *ReadOnlyAccess* policy is attached to *user-1* via the *user1group* IAM group.

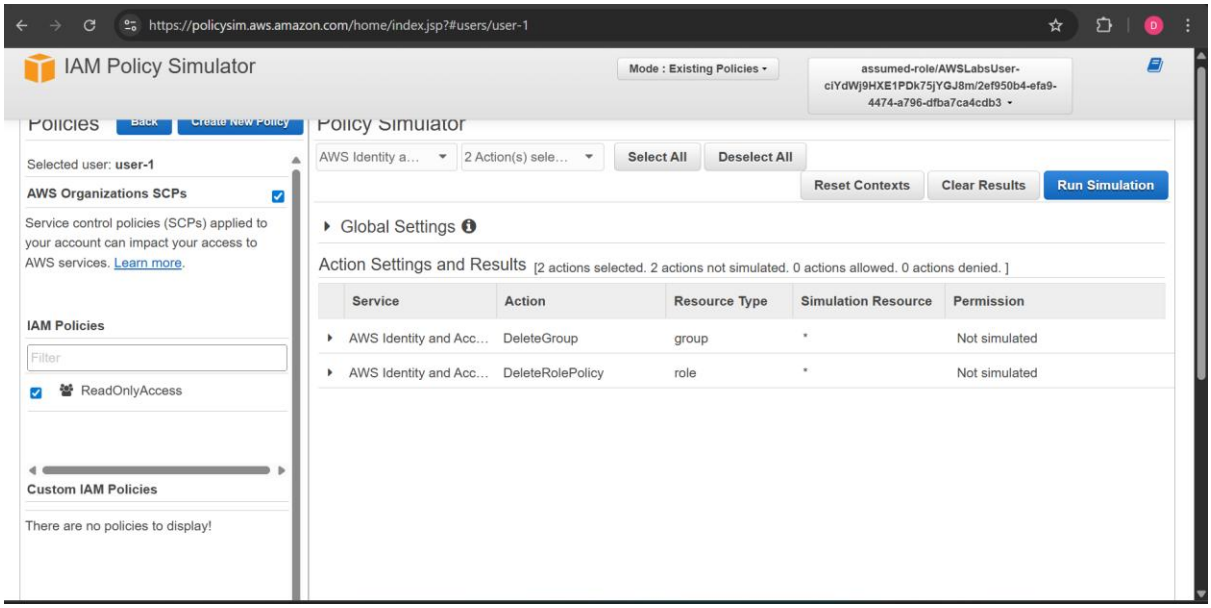


10. To run the IAM Policy Simulator, open the following link in a new web browser tab: [IAM Policy Simulator](#).



11. On the **IAM Policy Simulator** page, in the **Users, Groups, and Roles** pane, choose **user-1**.
12. In the **Policy Simulator** pane, on the **Select service** drop-down menu, choose **Identity and Access Management**.
13. On the **Select actions** drop-down menu, select the following options:

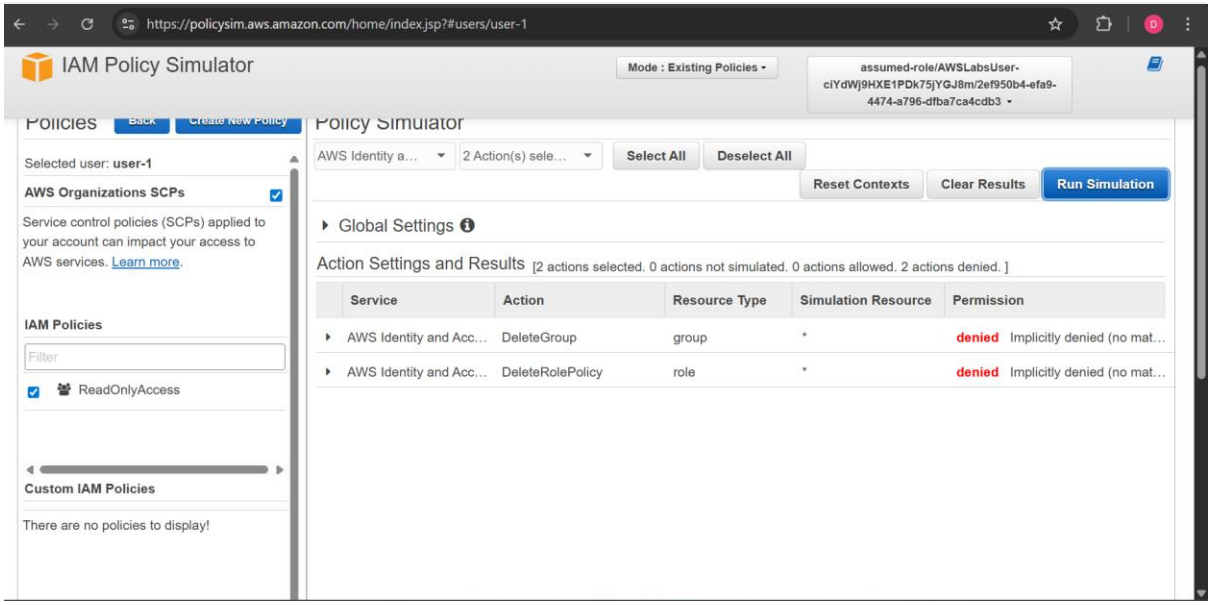
- **DeleteGroup**
- **DeleteRolePolicy**



14. Choose **Run Simulation**.

Expected output: The **Action Settings and Results** section displays the effective permissions for *user-1*, similar to this:

Service	Action	Resource Type	Simulation Resource	Permission
AWS Identity and Access Management	DeleteGroup	group	*	**denied** Implicitly denied (no matching statements).
AWS Identity and Access Management	DeleteRolePolicy	role	*	**denied** Implicitly denied (no matching statements).



Consider: Why do you think think both actions were denied?

Recall that the policy attached to *user-1* is a *read-only* policy. Any actions that could allow changes to a service or resource are *denied*.

15. Close the **IAM Policy Simulator** web browser tab.

Learn more: For more information about the IAM Policy Simulator, refer to *Testing IAM policies with the IAM policy simulator* in the **Additional resources** section.

Collecting audit evidence

From an audit evidence standpoint, you can capture the IAM settings and the IAM Policy Simulator output to be used as support evidence in user access reviews.

Congratulations! You have successfully audited the permissions assigned to an IAM user.

Task 2: Review the security configuration of Amazon EC2 instances

What is Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. Amazon EC2 presents a true virtual computing environment, allowing you to use web service interfaces to launch instances with a variety of operating systems, load them with your custom application environment, manage your network's access permissions, and run your image using as many or few systems as you desire.

What is a security group?

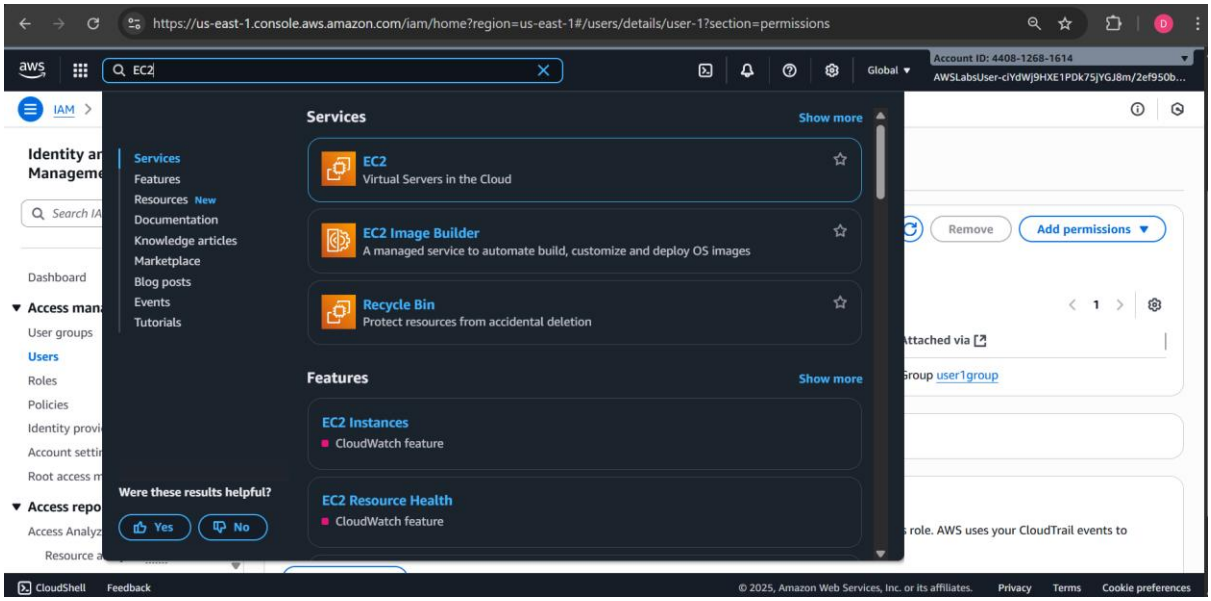
A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. Security groups act at the instance level, not the subnet level. For each security group, you add rules that control the inbound traffic to instances and a separate set of rules that control the outbound traffic.

The following are basic characteristics of security groups:

- You can specify allow rules, but not deny rules.
- You can specify separate rules for inbound and outbound traffic.
- By default, no inbound traffic is allowed until you add inbound rules to the security group.
- By default, all outbound traffic is allowed until you add outbound rules to the group. Then, you specify the outbound traffic that is allowed.
- Responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules and vice versa, as security groups are therefore stateful.
- Instances associated with a security group can't talk to each other unless you add rules allowing it.
    - **Exception:** The default security group has these rules by default.
- After you launch an instance, you can change which security groups the instance is associated with.

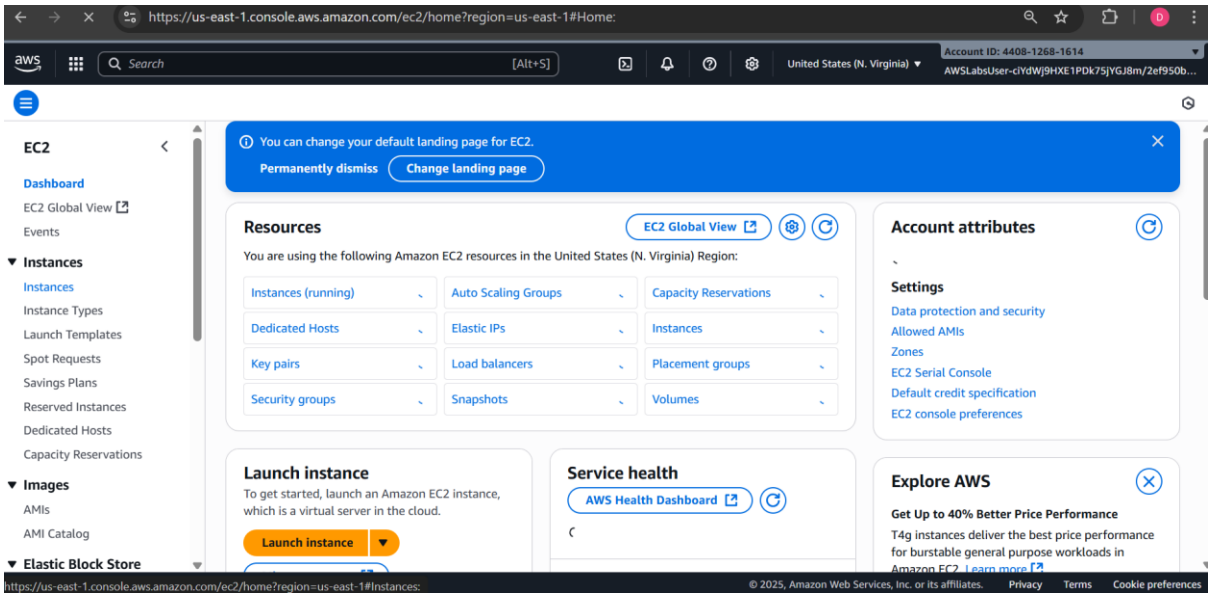
Review running Amazon EC2 instances

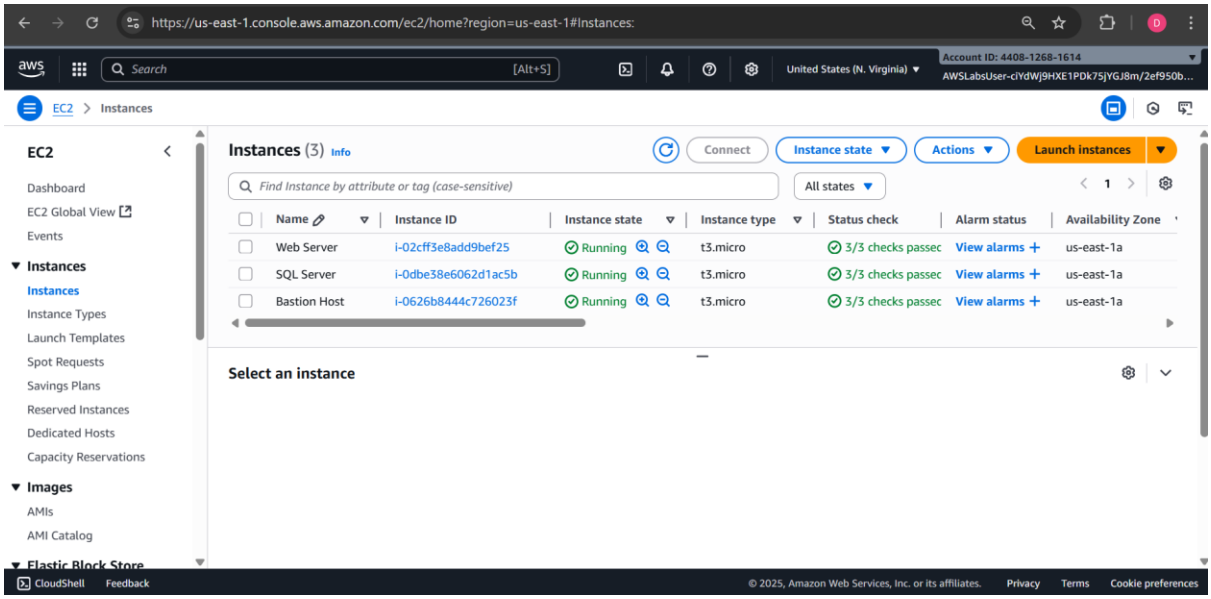
16. At the top of the AWS Management Console, in the search bar, search for and choose EC2



17. In the navigation pane at the left of the page, under **Instances**, choose **Instances**.

In this lab environment, there are three running instances: *Web Server*, *Bastion Host*, and *SQL Server*.

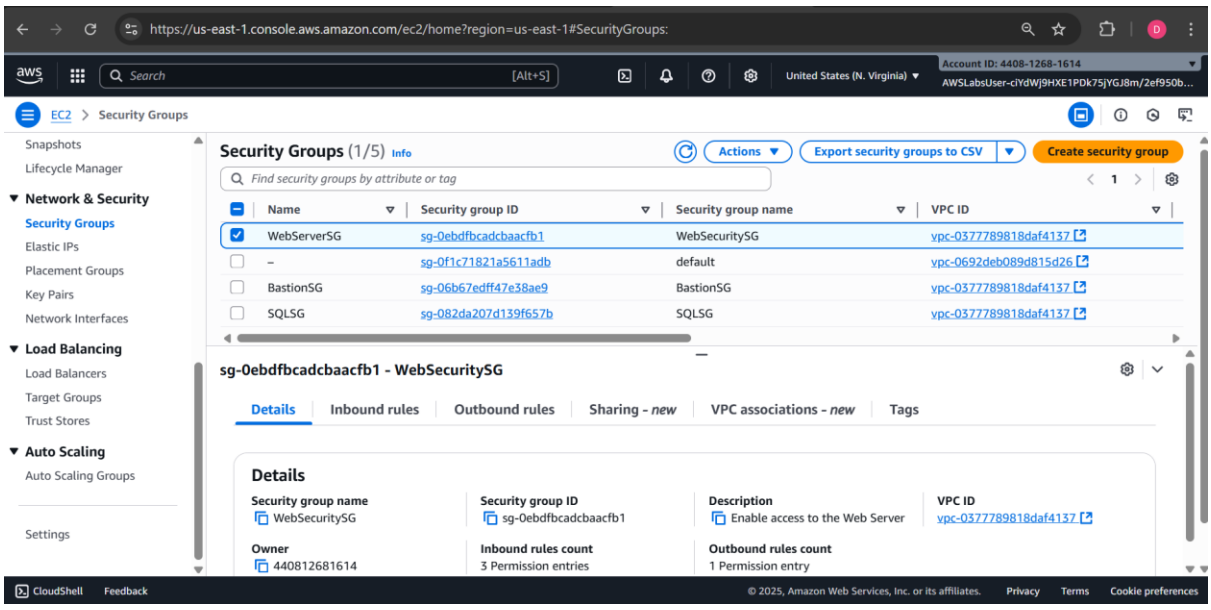




Review the web server security group

18. In the navigation pane at the left of the page, under **Network & Security**, choose **Security Groups**.

19. Select **WebServerSG**.



20. In the details pane at the bottom of the page, choose the **Inbound rules** tab.

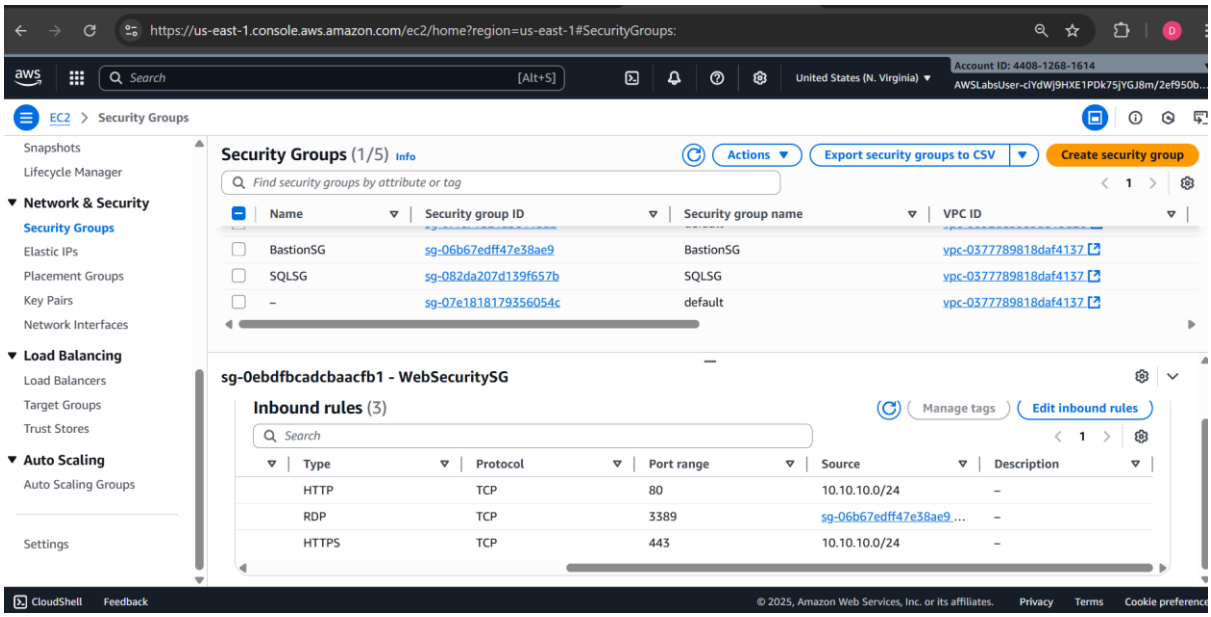
21. Review the **Inbound rules**.

Consider: Are the inbound rules what you would expect for a web server in a restricted access environment?

The *WebServerSG* security group demonstrates a security-focused configuration. Unlike typical public-facing web servers that allow HTTP/HTTPS access from anywhere, this configuration implements a more restrictive security posture by:

- Limiting web traffic (ports 80/443) to a specific IP range (10.10.10.0/24) Restricting RDP access (port 3389) to connections from the BastionSG security group only
- This restricted configuration is typical for internal web applications, development environments, or services requiring controlled access. Even if an EC2 instance in the same subnet as the Web Server attempts to connect via RDP, it is only allowed if the *BastionSG* security group is associated with it.

Note: When configuring security group rules, you can specify sources such as specific CIDR ranges, *My IP*, or security group IDs. While *anywhere* (0.0.0.0/0) access is common for public web servers, using more restrictive sources aligns with security best practices and the principle of least privilege.



Review the bastion host security group

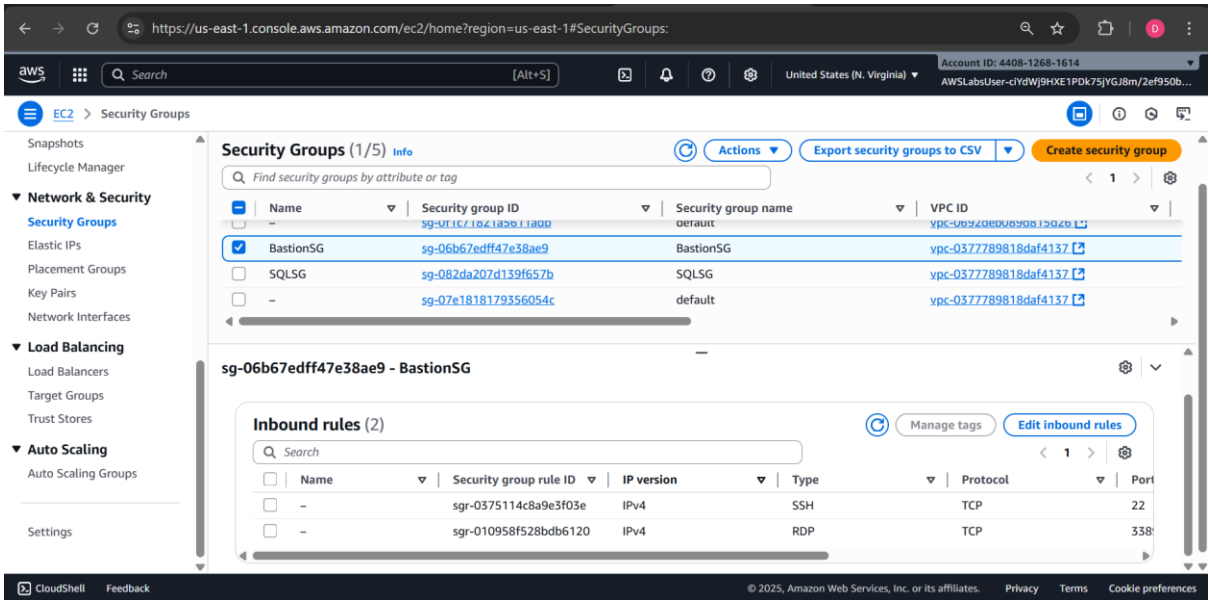
22. Clear **WebServerSG**.
23. Select **BastionSG**.

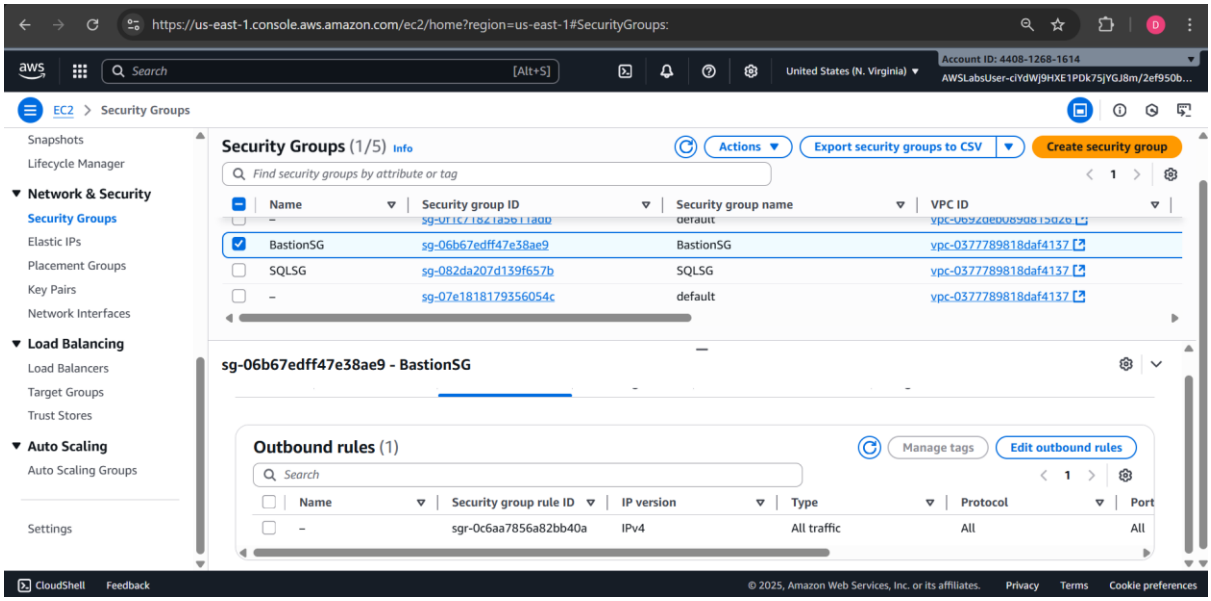
A bastion host is a special purpose server on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application (such as a proxy server) and all other services are removed or limited to reduce threats to the computer. It is hardened in this manner primarily due to its location and purpose, which is typically on the outside of the firewall and usually involves access from untrusted networks or computers.

24. To review the inbound and outbound rules, choose the **Inbound rules** and **Outbound rules** tabs respectively.

Consider: Are the Inbound and Outbound rules what you would expect for the bastion host?

The Bastion host should be set to accept traffic from your management network. Notice that the Bastion host instance is specifically set up to allow TCP port 22 (SSH) and TCP port 3389 (RDP) from an IP range of 10.10.10.0/24. Think of this IP range as your data center management network which can be reached via a private network.





Review the SQL server security group

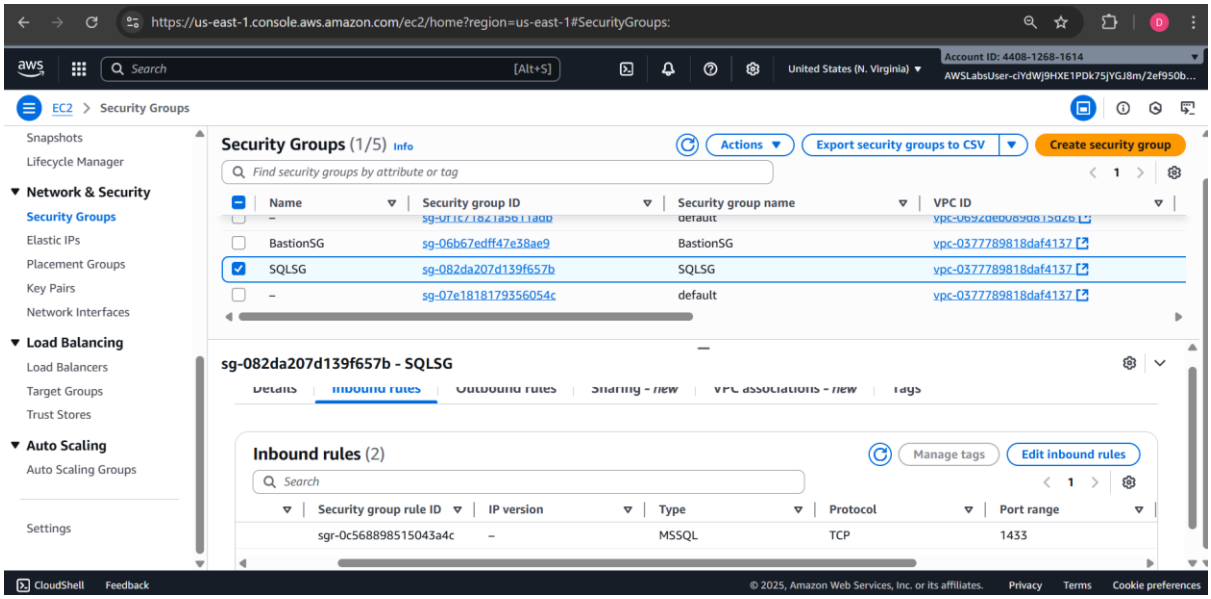
25. Clear **BastionSG**.
26. Select **SQLSG**.
27. To review the inbound rules, choose the **Inbound rules** tab.

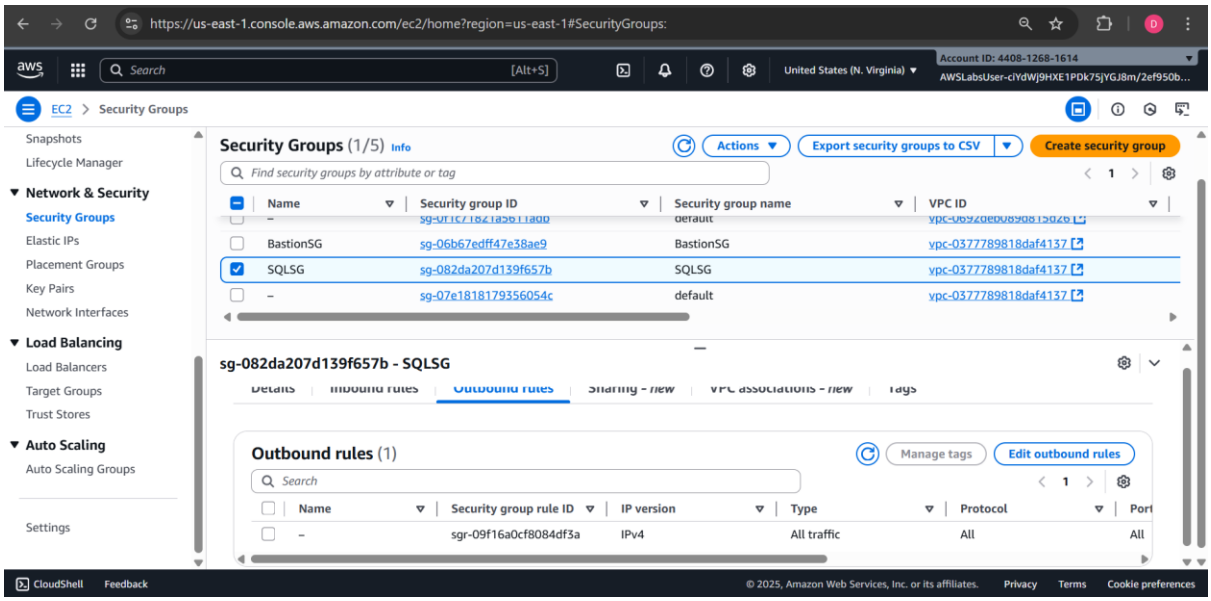
Consider: Are the inbound rules what you would expect for the SQL Server?

Notice that the inbound rules are configured with a custom source—a security group ID from this account.

28. To review the outbound rules, choose the **Outbound rules** tab.

Consider: Are the Outbound Rules what you would expect for the SQL Server?





Collecting audit evidence

From an audit evidence standpoint, these findings can support your resource access isolation and data protection from internal or external threats. All access to the *SQL Server* instance is restricted via a jump box (Bastion Host); therefore, no internal user has direct access to it. Externally, the SQL Server only communicates with the web service via the *WebServerSG* and *SQLSG* security groups.

Congratulations! You have successfully reviewed the security group configuration for each EC2 instance in the environment.

Task 3: Review Amazon VPC security configurations

What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) permits you to launch AWS resources into a virtual network that you have defined. This virtual network closely resembles a traditional network that you would operate in your own data center, with the benefits of using the scalable infrastructure of AWS. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

Amazon VPC provides two features that you can use to increase security for your VPC:

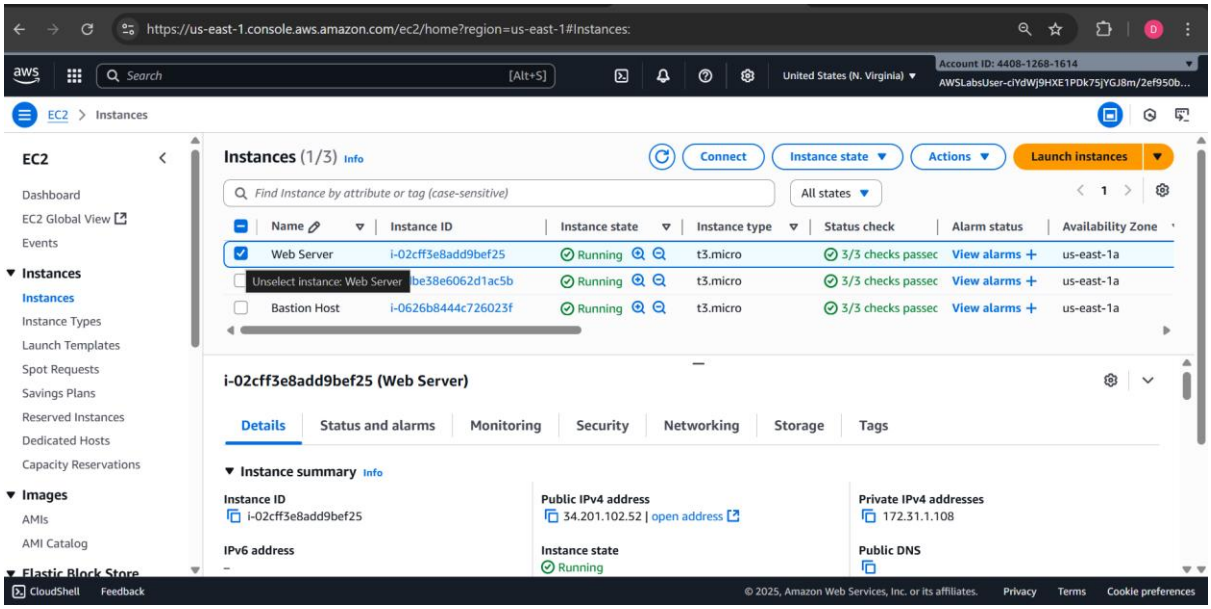
- **Security Groups:** Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.
- **Network Access Control Lists (ACLs):** Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.

When you launch an instance in a VPC, you can associate one or more security groups that you have created. Each instance in your VPC could belong to a different set of security groups. If you do not specify a security group when you launch an instance, the instance automatically belongs to the default security group for the VPC.

Locate Amazon EC2 instance VPC configurations

29. In the navigation pane at the left of the page, under **Instances**, choose **Instances**.
30. Select **Web Server**.

The *Details* pane appears below the list of instances that shows information about the instance you selected.



31. In the **Instance summary** section, locate the **VPC ID** value and copy it to your favorite text editor.

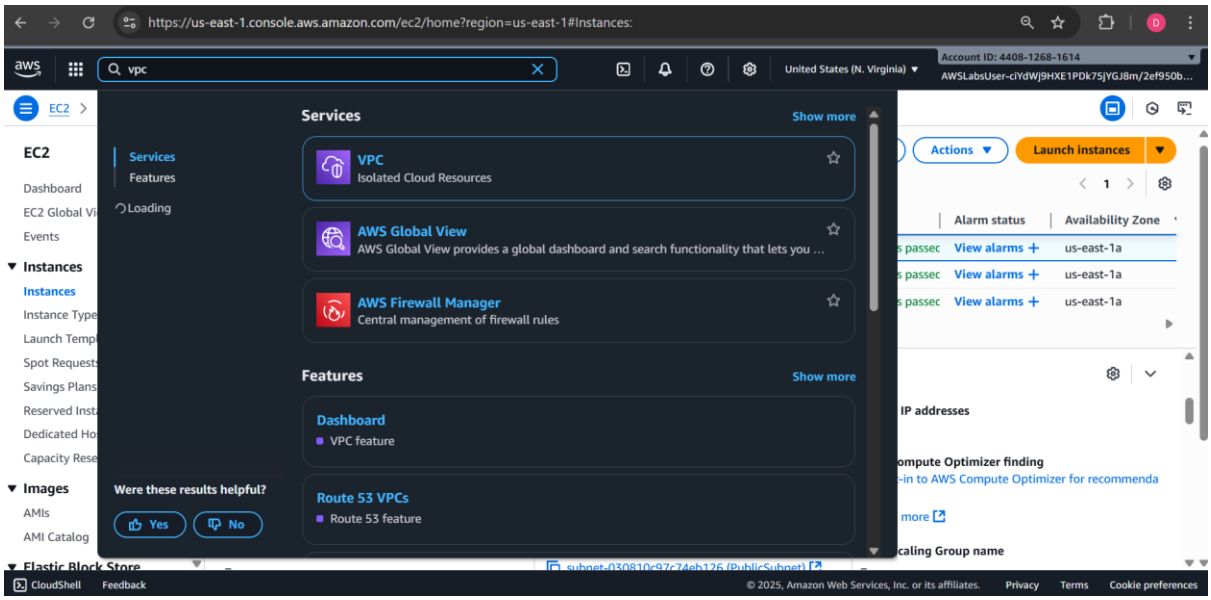
Note: The VPC ID should look similar to: *vpc-0586914dd2bce2335*.

Every VPC is associated with a VPC ID. In the next section, you identify the VPC that is associated with this VPC ID.

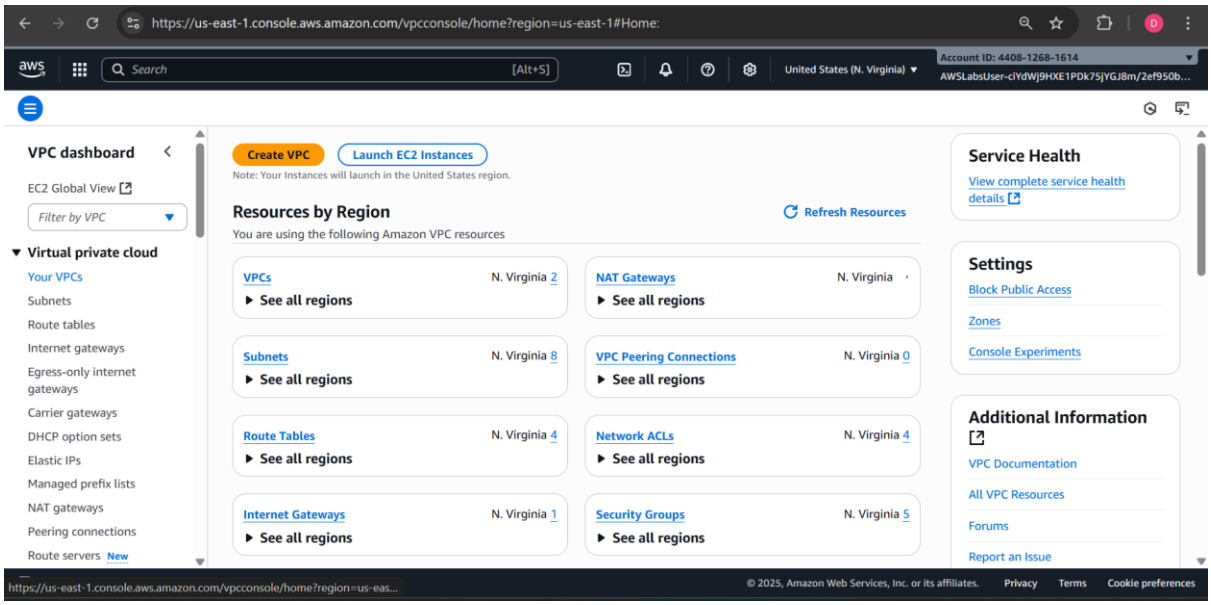
Review existing VPCs, subnets, and NACLs

In this section, you review your existing VPCs, subnets, and Network ACL capabilities within a Virtual Private Cloud.

32. At the top of the AWS Management Console, in the search bar, search for and choose VPC

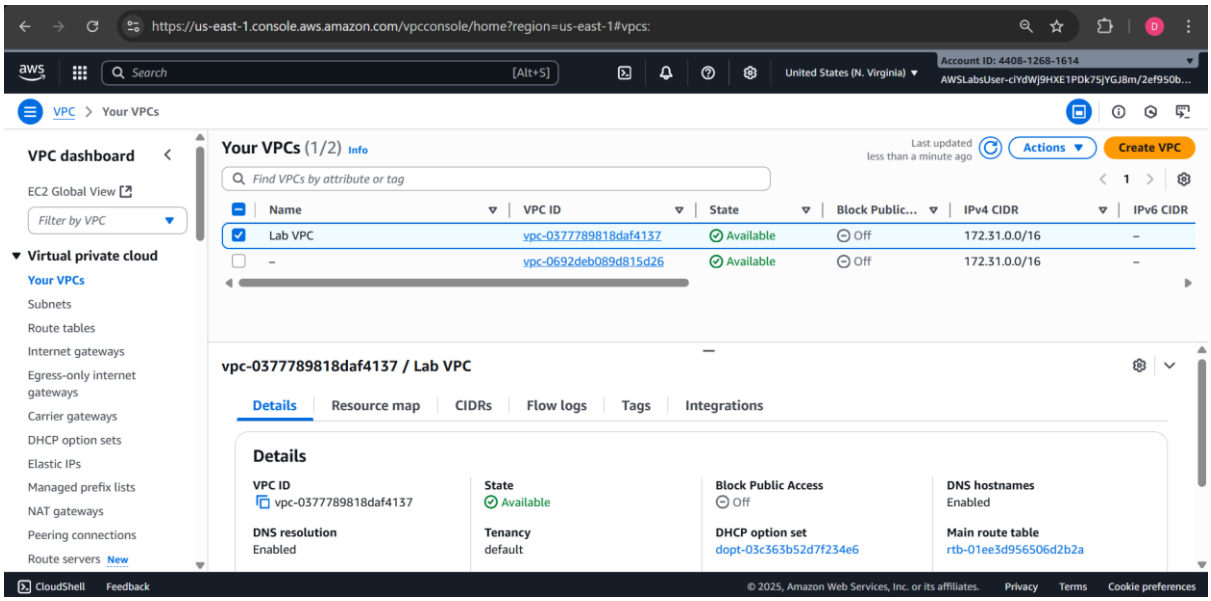


33. In the navigation pane at the left of the page, under **Virtual private cloud**, choose **Your VPCs**.



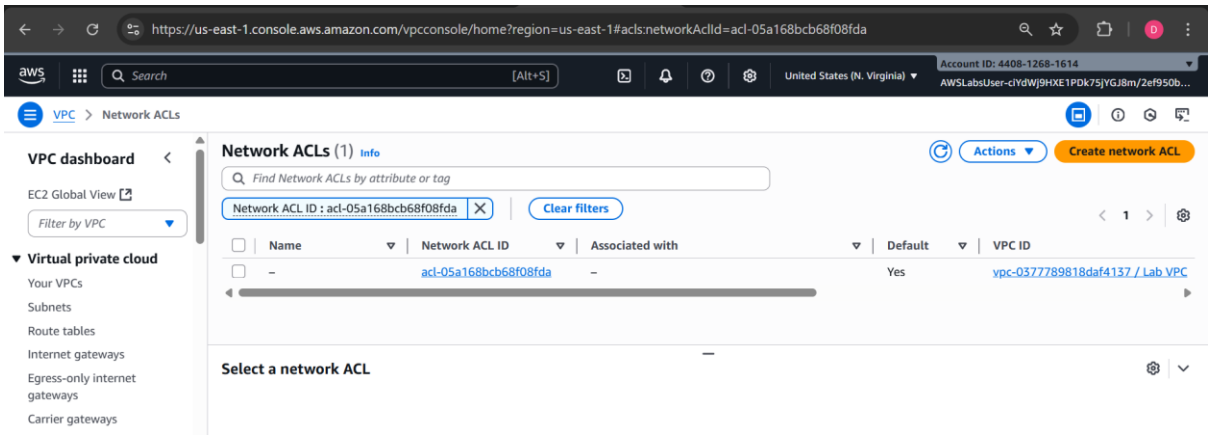
34. Select **Lab VPC**.

The *Details* pane appears below the list of VPCs that shows the configuration elements for the selected VPC.



35. Notice that the **VPC ID** value is the same **VPC ID** value that you copied to your text editor.

36. In the **Details** section, choose the **Main network ACL** link.

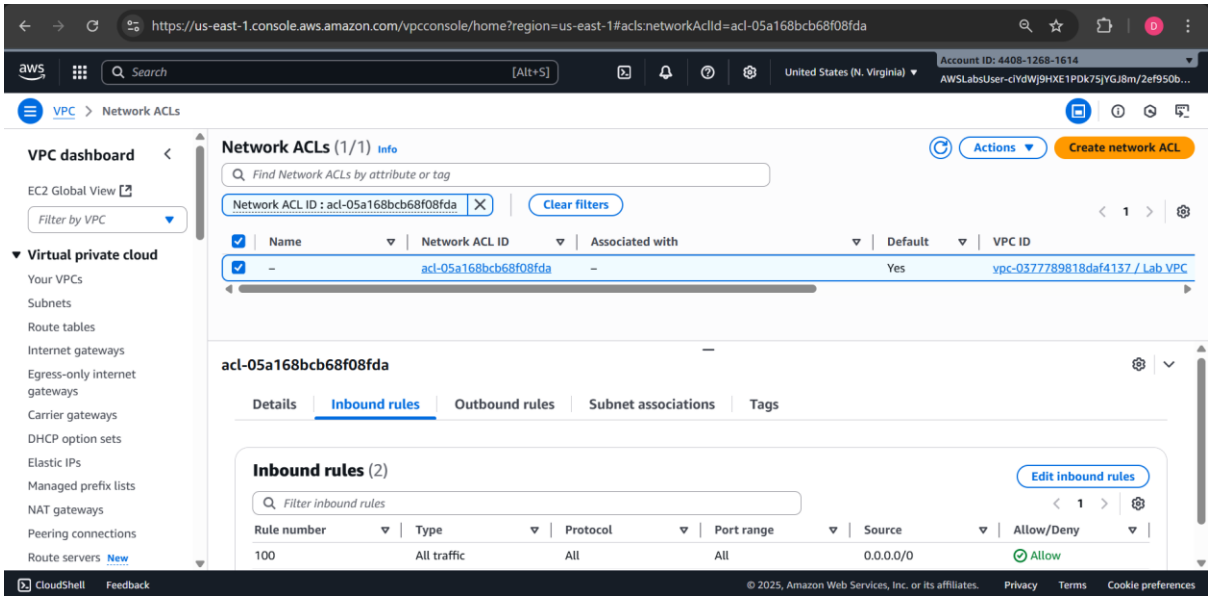


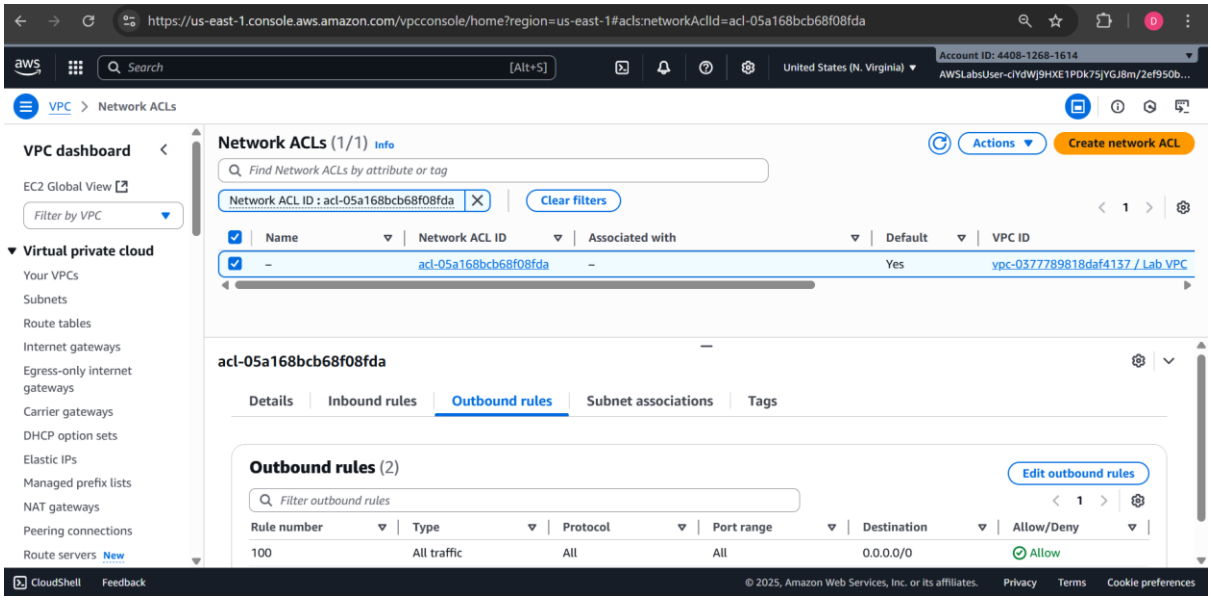
37. On the **Network ACLs** page, select the Network ACL which has a **Default** parameter value of **Yes**.

Note: There should only be one choice.

38. To review the inbound and outbound rules, in the **Details** pane at the bottom of the page, choose the **Inbound rules** and **Outbound rules** tabs respectively.

Note: As audit evidence, you can see how the VPC is using ACLs to communicate with an external network via explicit protocols.





Congratulations! You have successfully reviewed the details of the lab VPC.

Task 4: Audit CloudWatch metrics and alarms

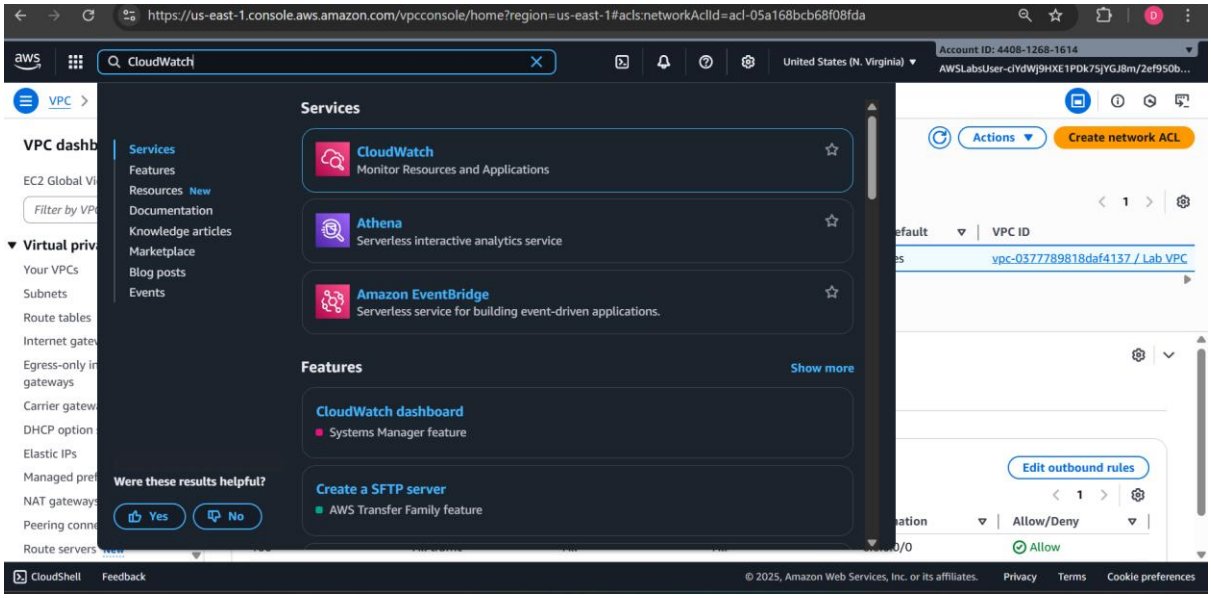
In this task, you review built-in CloudWatch metrics, alarms, and service health associated with running instances, storage volumes, and data services within the auditing instance.

What is Amazon CloudWatch?

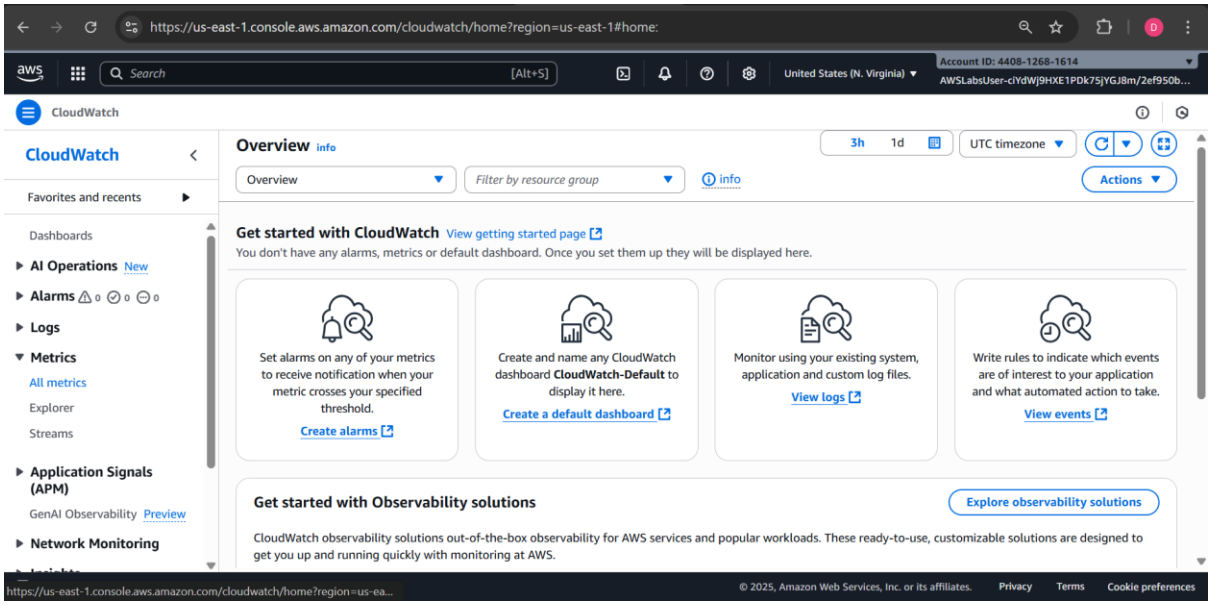
Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SREs), and IT managers. CloudWatch provides you with data and actionable insights to monitor your applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing you with a unified view of AWS resources, applications and services that run on AWS, and on-premises servers. You can use CloudWatch to set high resolution alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to optimize your applications, and ensure they are running smoothly.

Audit CloudWatch metrics and alarms

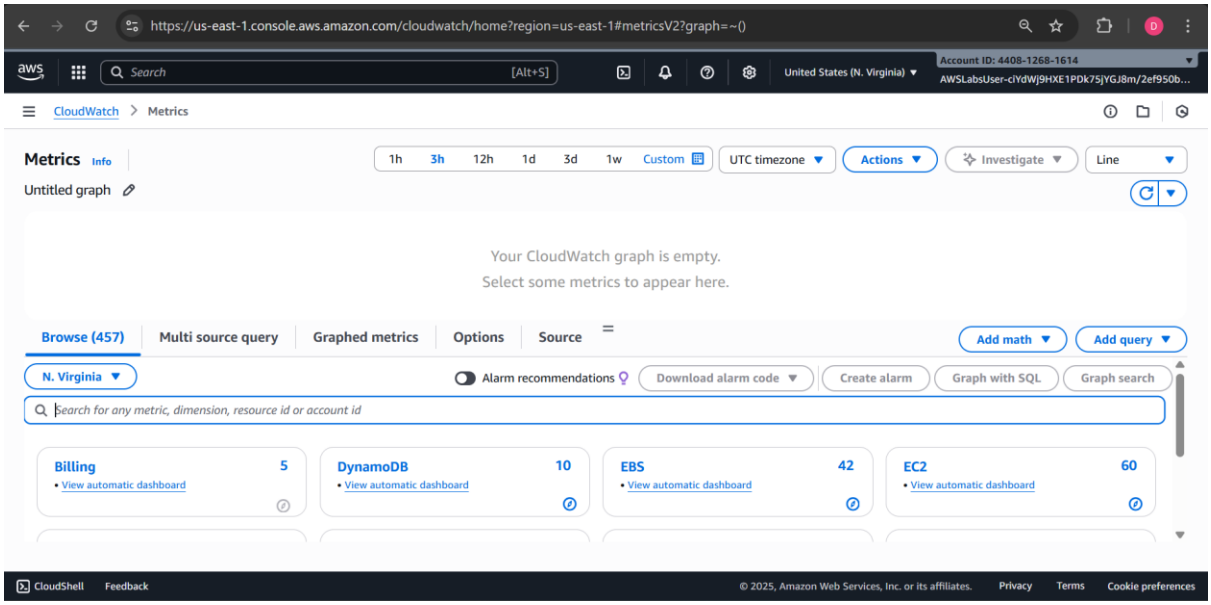
39. At the top of the AWS Management Console, in the search bar, search for and choose CloudWatch



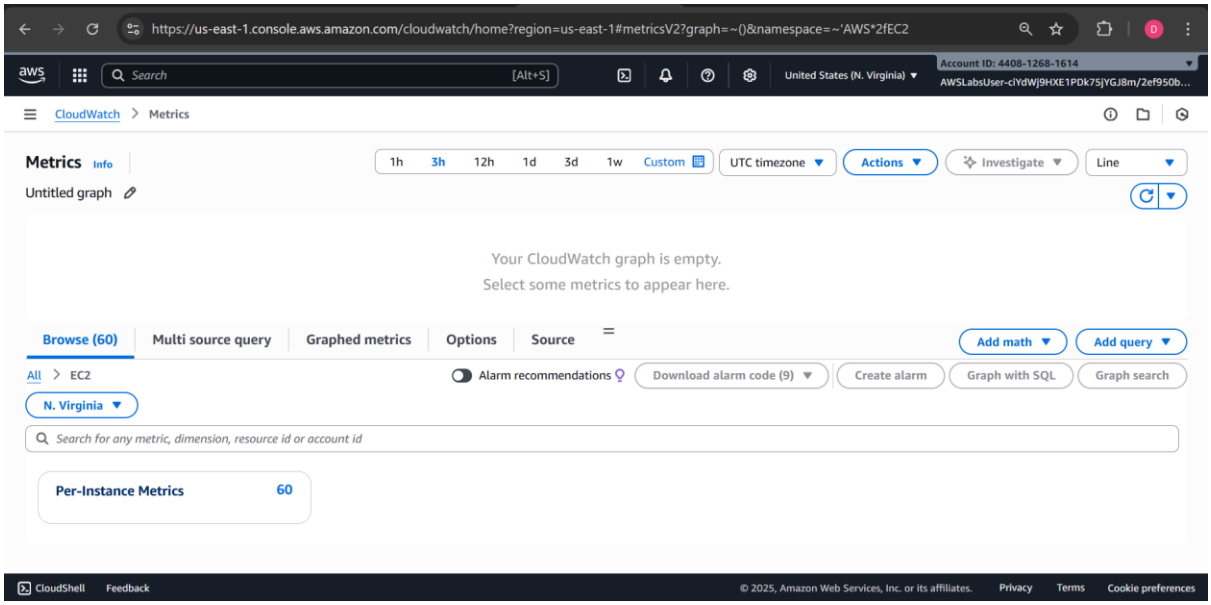
40. In the navigation pane at the left of the page, in the **Metrics** section, choose **All metrics**.



41. On the **Browse** tab, choose **EC2**.

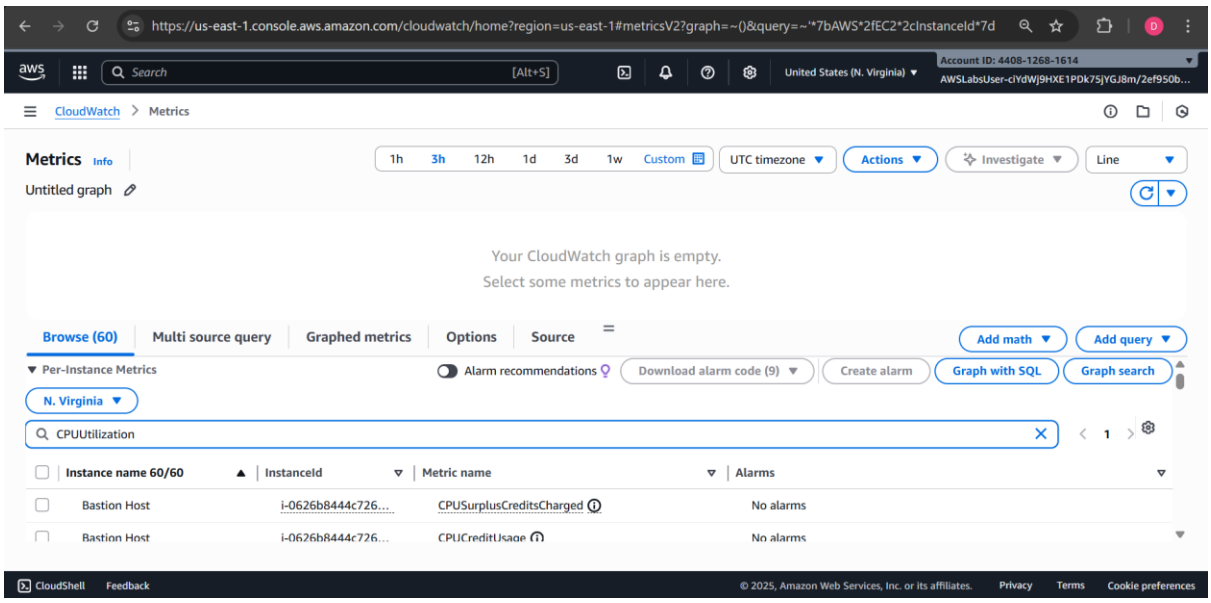


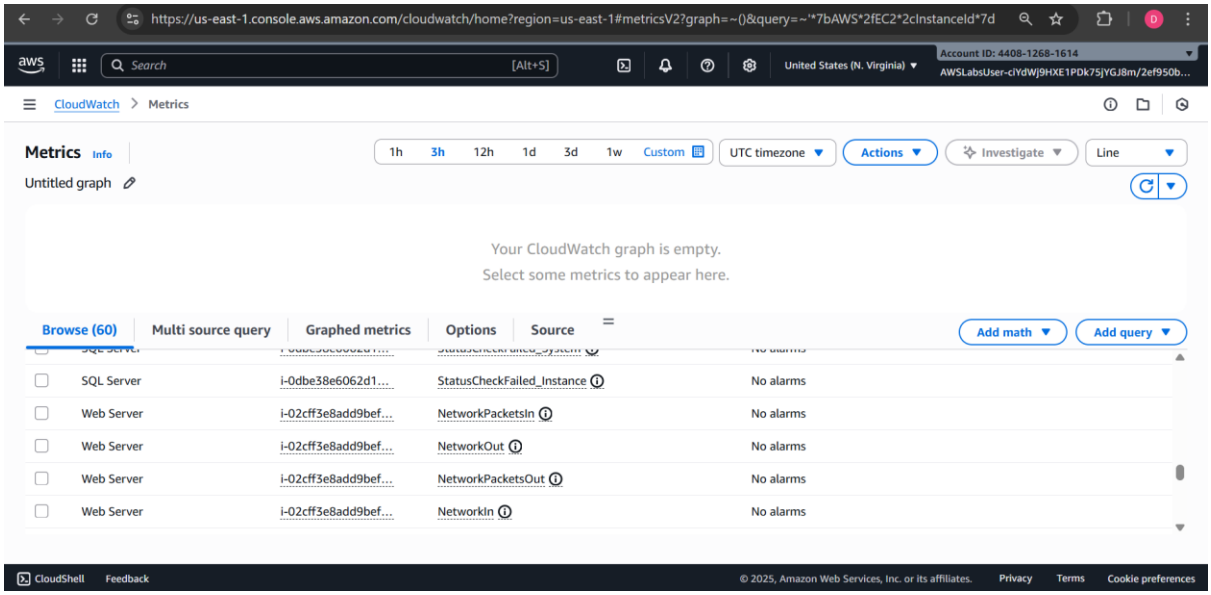
42. Choose **Per-Instance Metrics**.



43. In the **Search** box, search for CPUUtilization

Expected output: The search results should display the three EC2 instance that you reviewed previously.

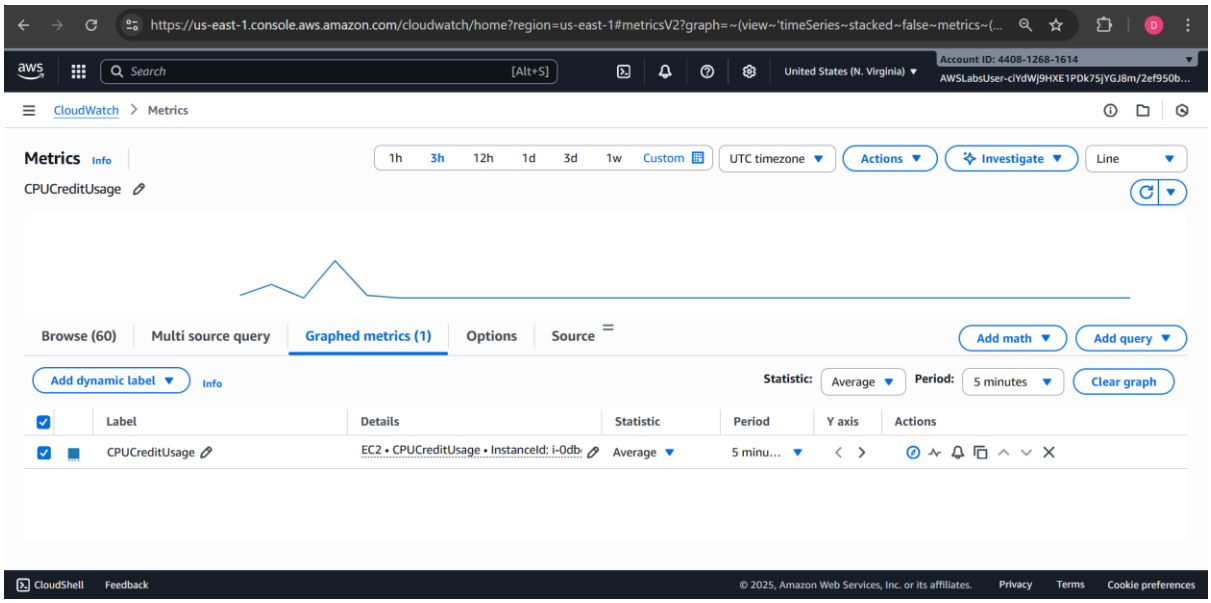




44. Select **SQL Server**.

45. Choose the **Graphed metrics** tab.

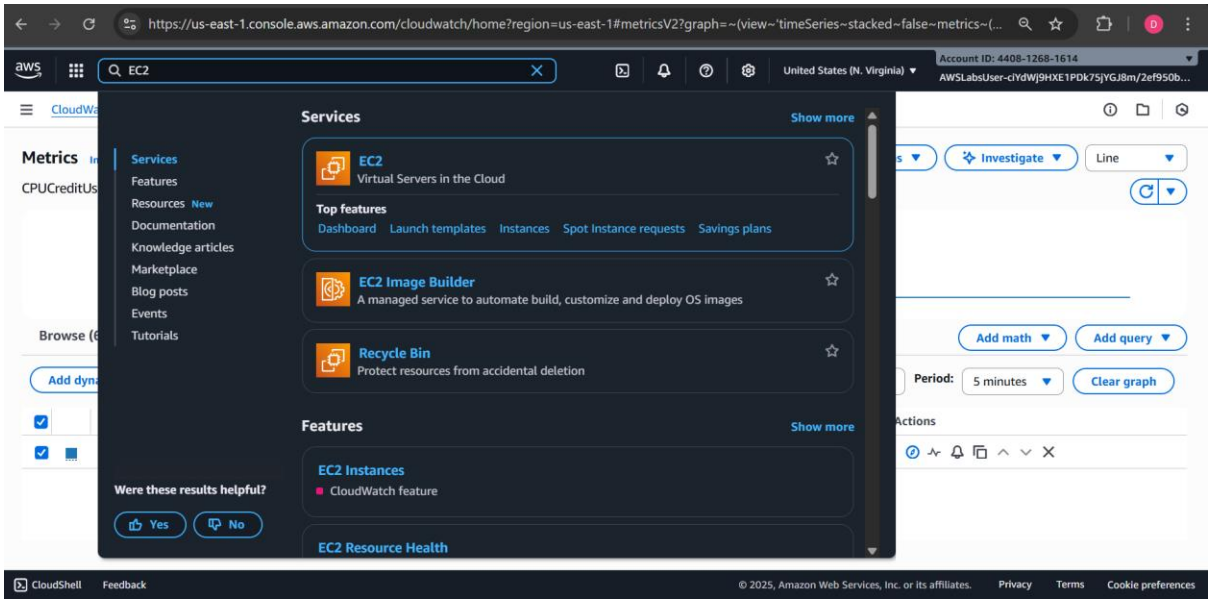
Note: You can change the *Statistic* and the *Period* settings to customize the view to your liking.



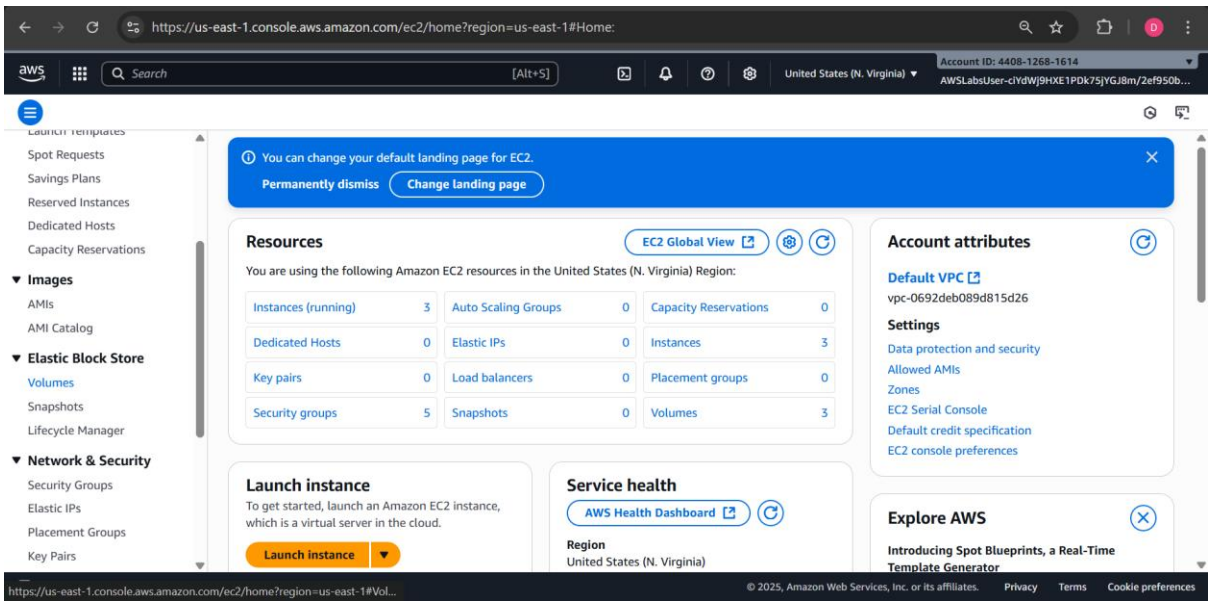
Review CloudWatch data for EBS volumes

In addition to viewing Amazon CloudWatch metrics and alarms via the CloudWatch dashboard, you can also view the data in other locations. In this section, you review Amazon CloudWatch data for your Amazon EBS volumes.

46. At the top of the AWS Management Console, in the search bar, search for and choose EC2



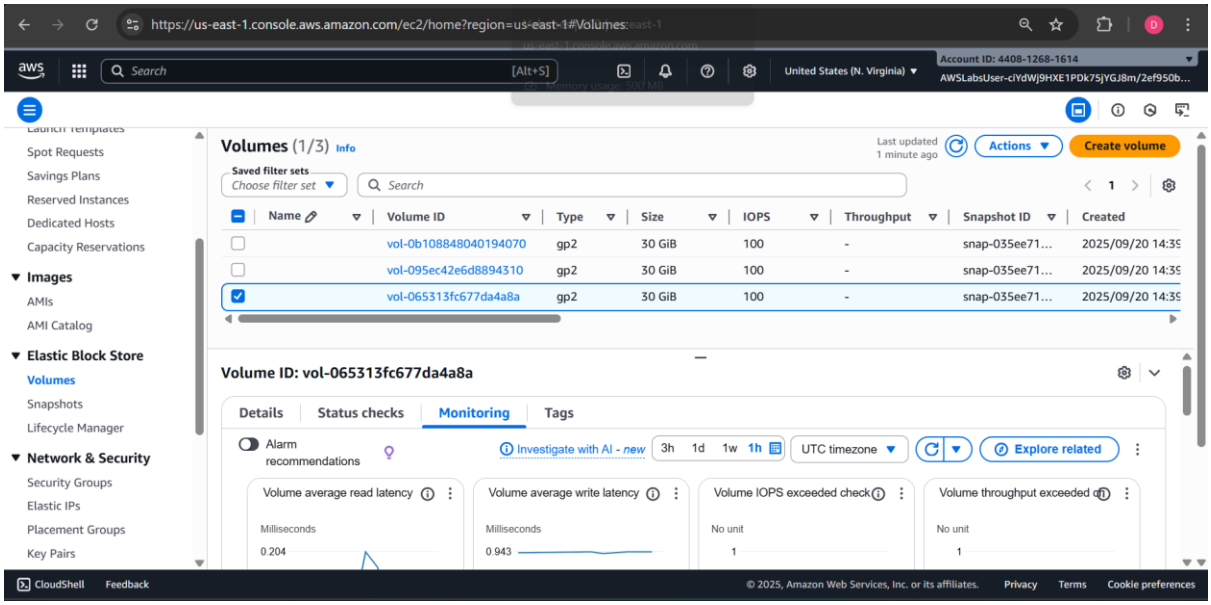
47. In the navigation pane at the left of the page, under **Elastic Block Store**, choose **Volumes**.



48. Select the **Volume** that is attached to the **Web Server** instance.

Note: To review the volume names and their attached instances, you might need to scroll to the right until you see the **Attached Instances** column header.

49. In the details pane at the bottom of the page, choose the **Monitoring** tab.



49. Review the CloudWatch metrics and any configured CloudWatch alarms.

Note: Amazon CloudWatch metrics can directly support several auditing elements and provide real-time audit evidence based on pre-defined criterion and custom criterion related to organization processes.

You have successfully reviewed where to locate CloudWatch metrics and alarms related to an EC2 instance.

Task 5: Audit CloudTrail logs

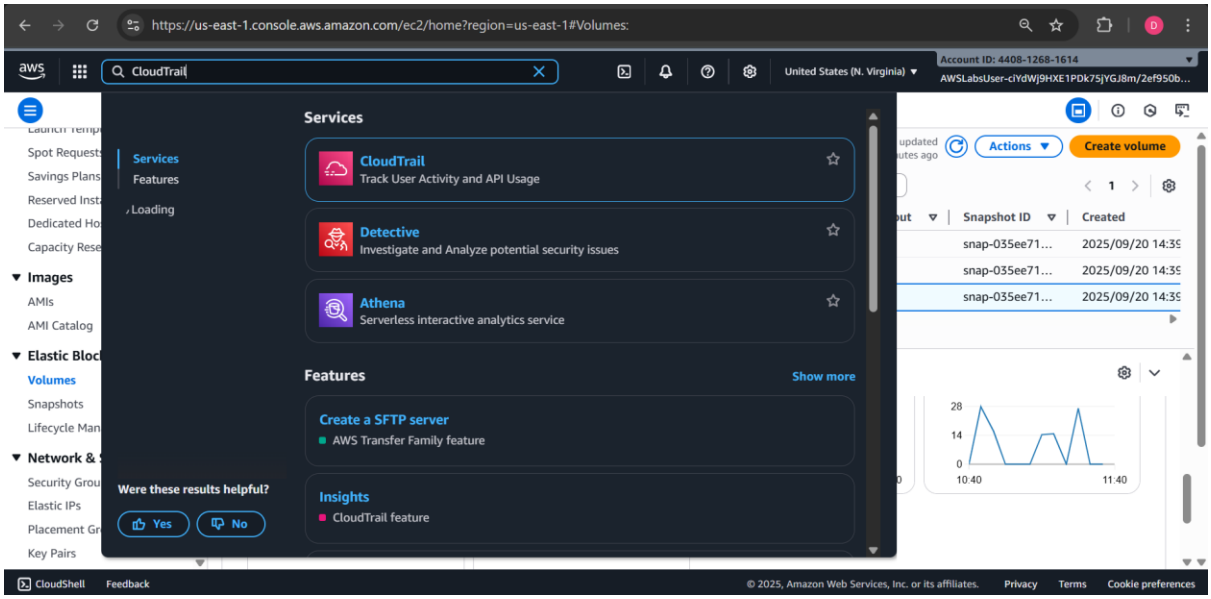
In this task, you use AWS CloudTrail to review configuration details and S3 storage locations.

What is AWS CloudTrail?

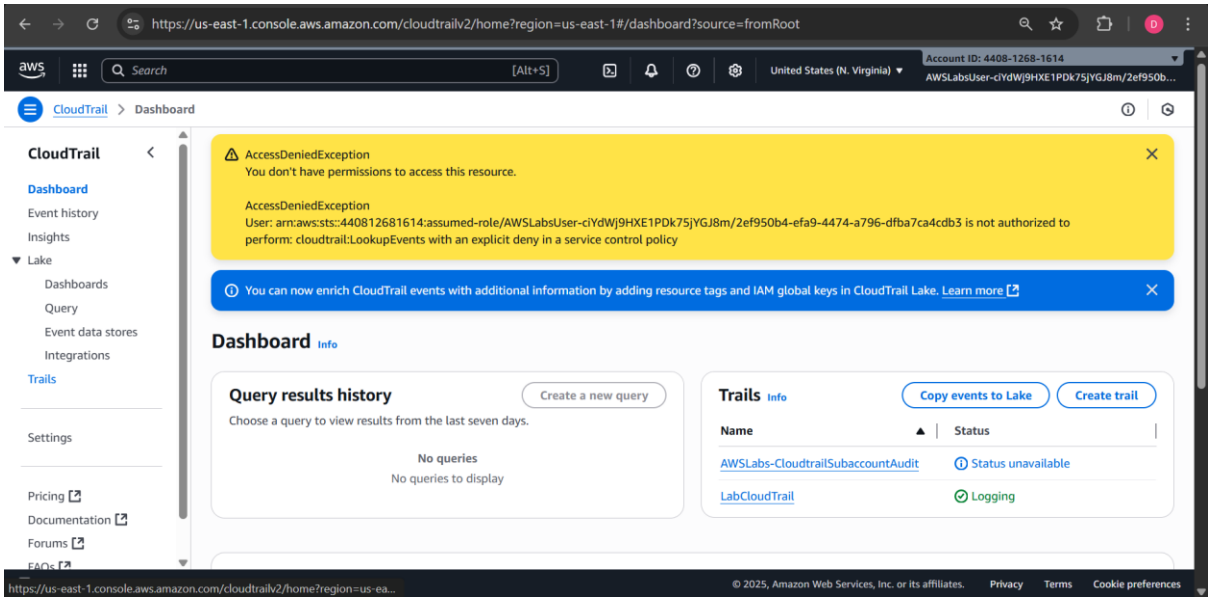
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.

Find CloudTrail logs

51. At the top of the AWS Management Console, in the search bar, search for and choose CloudTrail



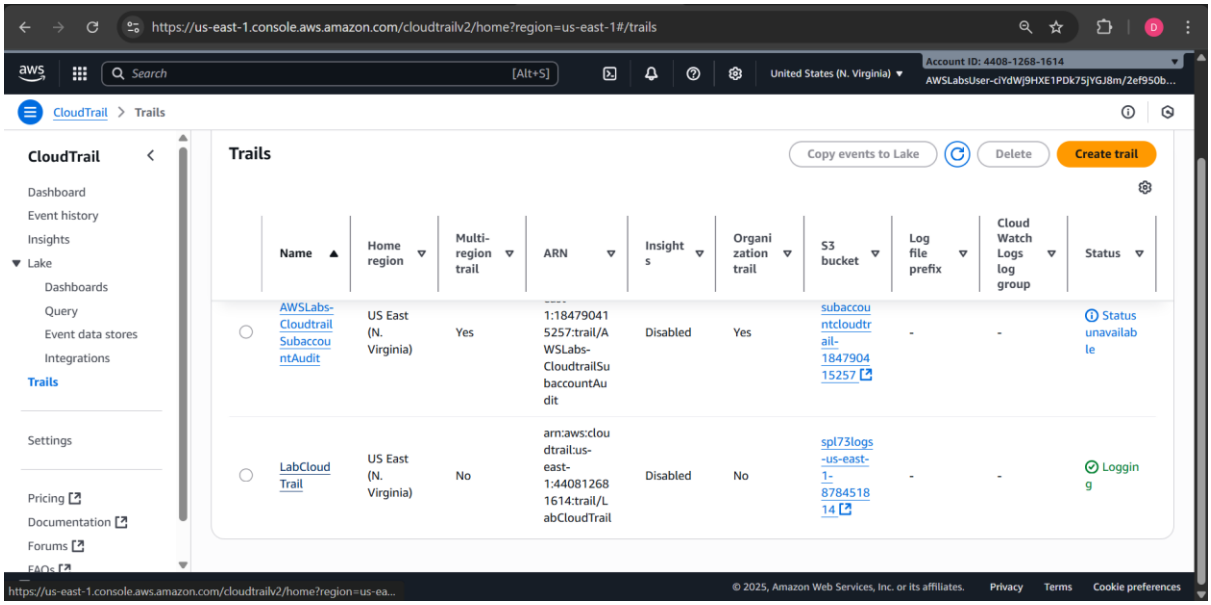
52. In the navigation pane at the left of the page, choose **Trails**.

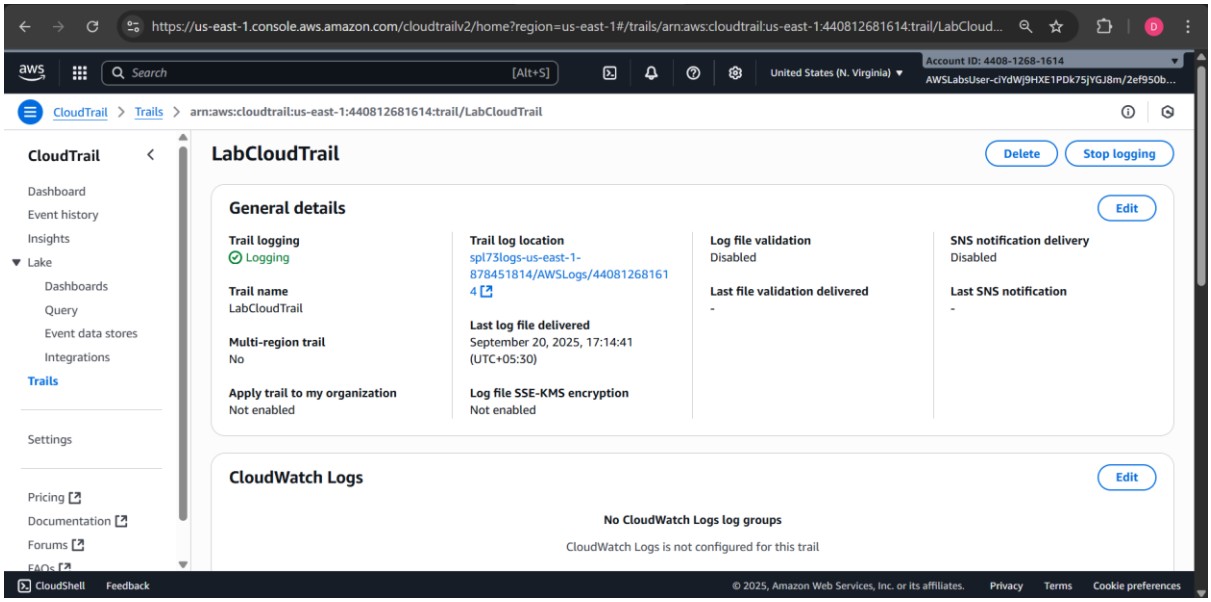


53. Choose the **LabCloudTrail** link to view its details.

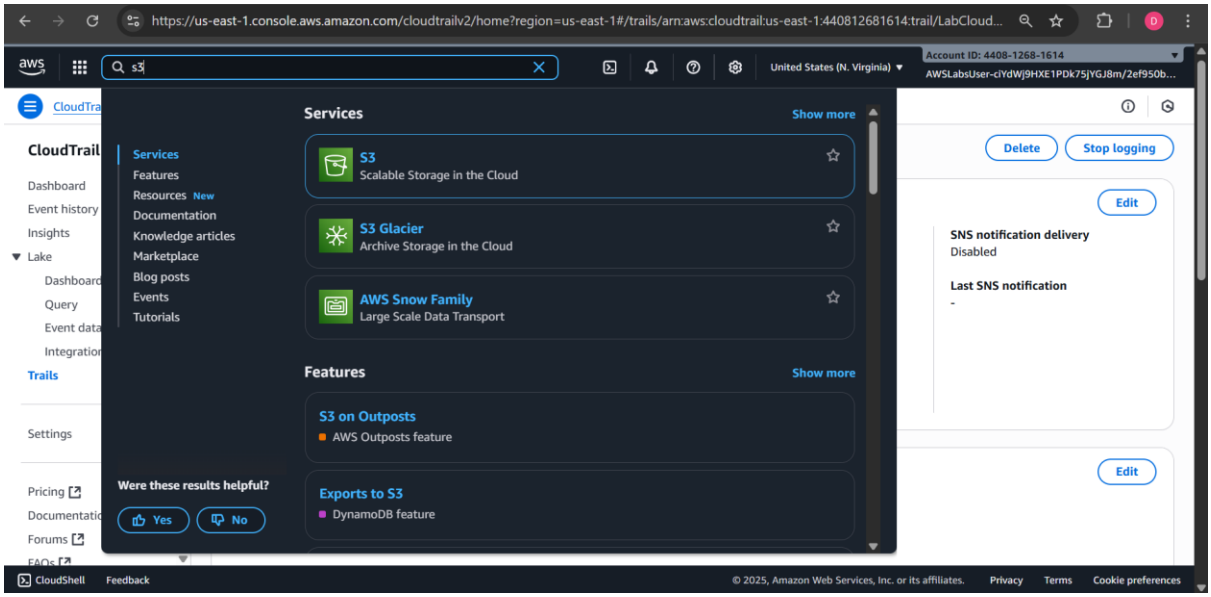
54. Review the CloudTrail configuration details.

Note: The *LabCloudTrail* trail was created using AWS CloudFormation when you started the lab. It's configured to store logs in the Amazon S3 bucket with a name that starts with *SPL73Logs*, as defined by the *Trail log location* property.

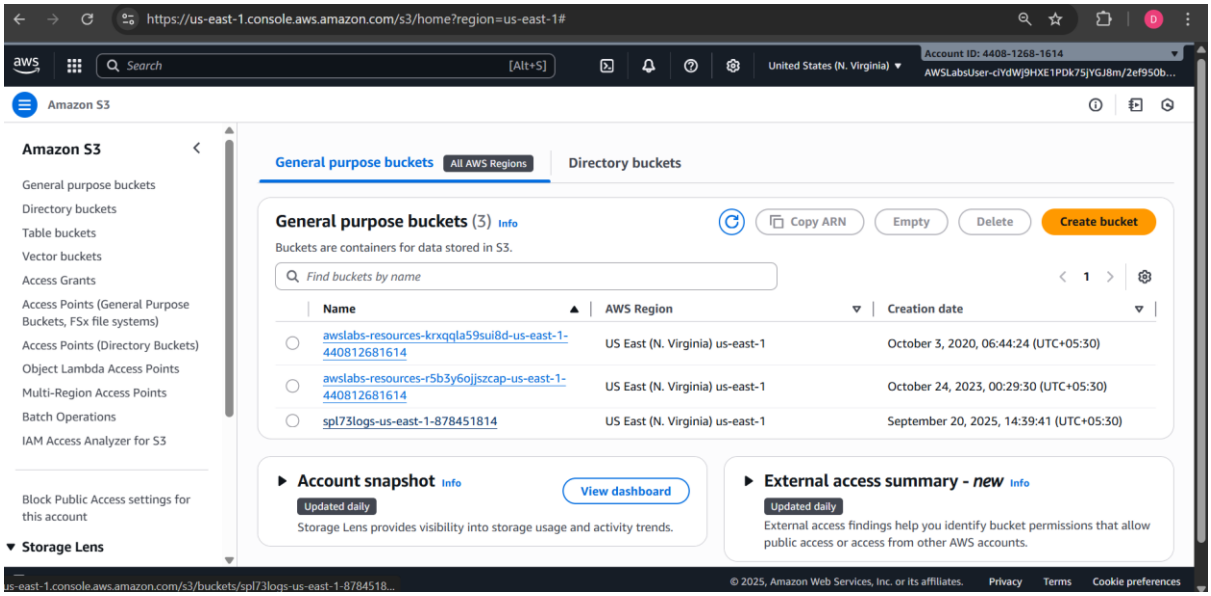




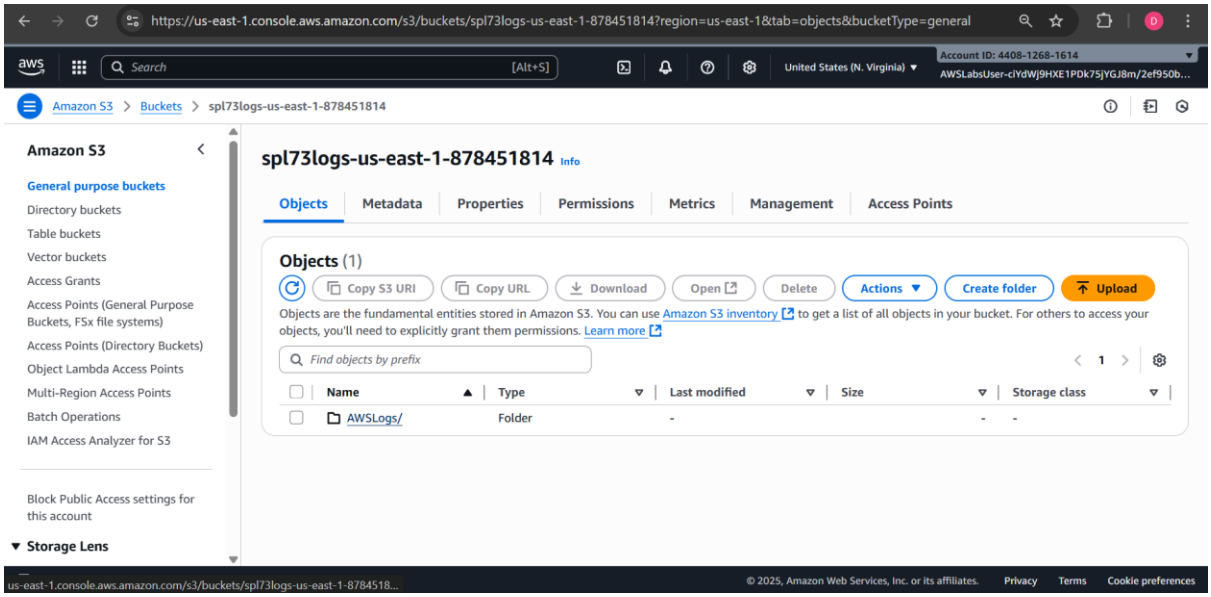
55. At the top of the AWS Management Console, in the search bar, search for and choose S3



56. Choose the link for the bucket name that starts with **spl73logs**.

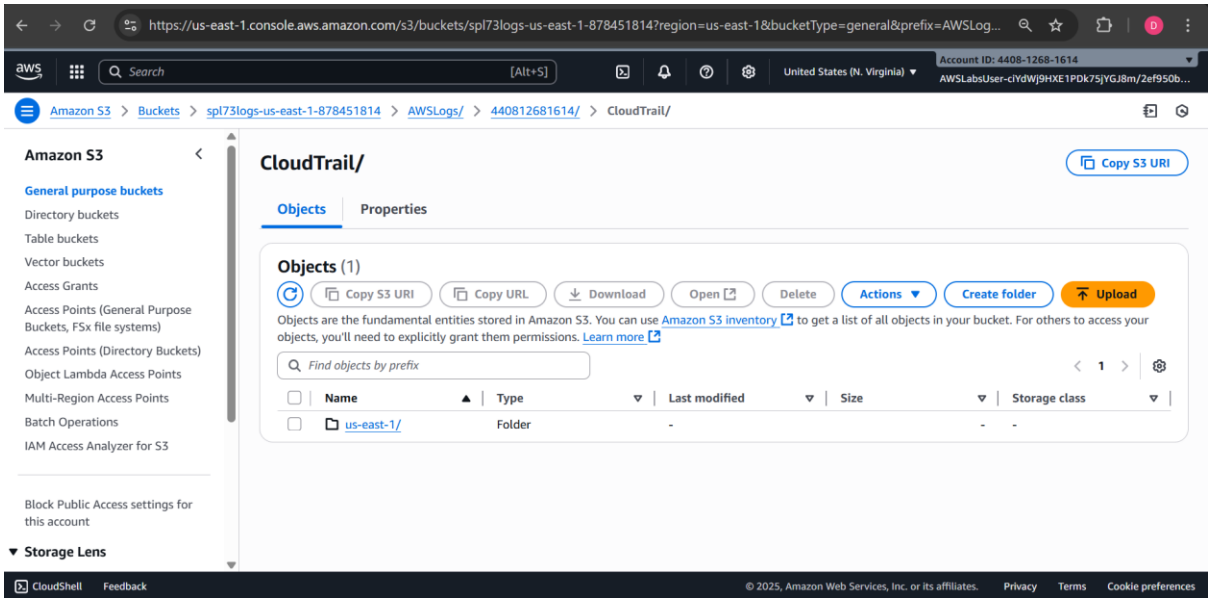


57. Choose the **AWSLogs/** link.



58. Continue selecting the links for the various folders until you get to a folder that represents the region your lab was launched in.

Note: The **Region** value is listed to the left of these instructions.

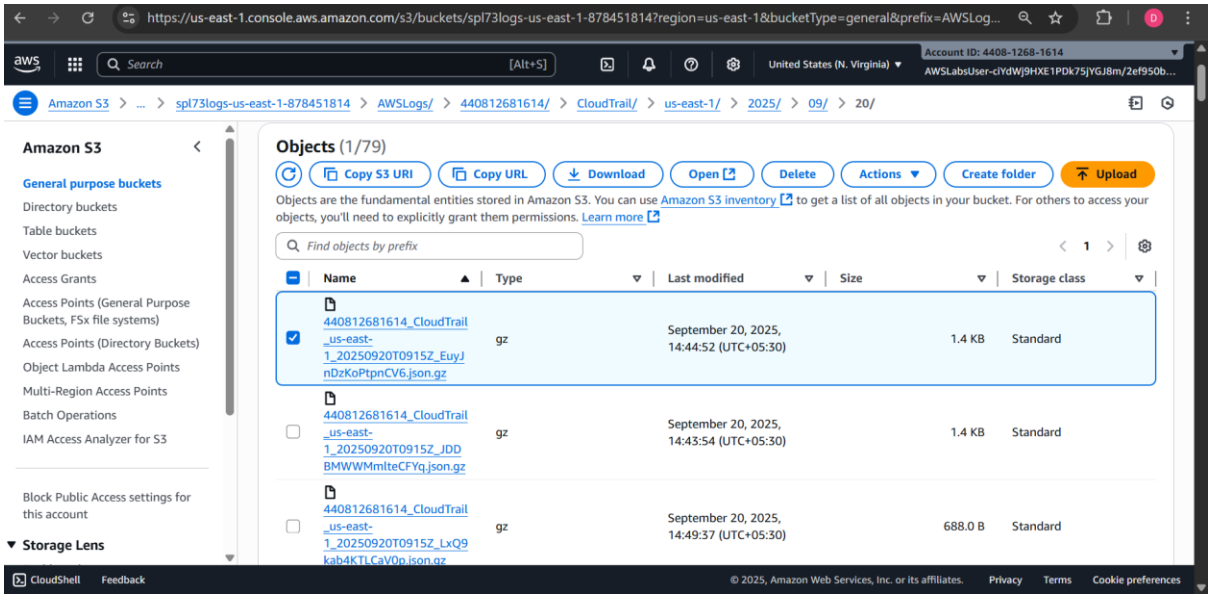


59. Continue selecting the links for the various folders, which represent today's date, until you see a log file.

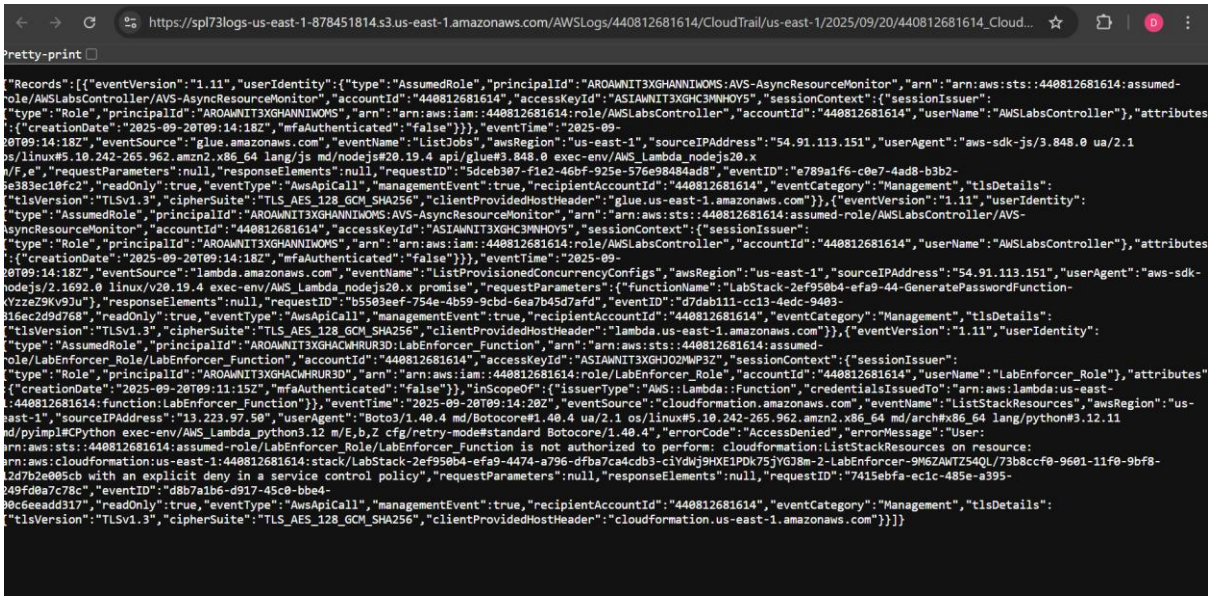
The log file name contains the AWS account number, AWS region, a numeric representation of the day's date and time, and a unique identifier, similar to this: *111122223333_CloudTrail_us-east-1_20230314T1535Z_MArnLpySt8ZdwFnQ.json.gz*

60. Choose the link for one of the log files, with a file name that ends in **json.gz**.

61. Choose **Open**.



Expected output: Depending on your web browser settings, a new window or a new tab opens that displays the contents of the log file. It is in JSON format.



An alternate approach to viewing your Amazon CloudTrail logs is to download them locally and use a text editor along with the JSON Viewer plug-in.

3rd Party Solutions: AWS partners with third-party specialists in logging and analysis to provide solutions that leverage Amazon CloudTrail output, such as Splunk or Alert Logic.

Congratulations! You have successfully reviewed the CloudTrail logs for an EC2 instance.

Conclusion

Congratulations! You have now successfully:

- Reviewed user permissions in AWS IAM.
- Captured audit evidence using AWS IAM Policy Simulator.

- Reviewed Inbound and Outbound networking rules for Amazon EC2 Security Groups.
- Reviewed Amazon VPC configurations, subnets, and Network ACLs.
- Reviewed Amazon CloudWatch performance metrics.
- Reviewed raw Amazon CloudTrail logs within Amazon S3.

End lab

Follow these steps to close the console and end your lab.

62. Return to the **AWS Management Console**.
63. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
64. Choose **End Lab** and then confirm that you want to end your lab.

Additional Resources

- Testing IAM policies with the IAM policy simulator
- AWS Security Center