

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

The screenshot shows the AWS search results for the query 'iam'. The results are categorized into 'Services' and 'Features'. Under 'Services', there are links to IAM, IAM Identity Center, and Resource Access Manager. Under 'Features', there is a link to 'IAM Access analyzer for S3'. A sidebar on the left lists various AWS services like CloudShell and Feedback. On the right, there is a 'Create application' button and a 'to default layout' button. The bottom of the page includes standard AWS navigation links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

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

The screenshot shows the IAM Dashboard. On the left, a navigation pane includes 'Identity and Access Management (IAM)' and sections for 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), 'Access reports' (Access Analyzer, Resource analysis), and 'AWS Lambda' (New). The main area displays 'IAM resources' with counts: User groups (1), Users (1), Roles (28), Policies (3), and Identity providers (0). A 'What's new' section lists recent changes. To the right, there are boxes for 'AWS Account' (Account ID: 440812681614, Account Alias Create, Sign-in URL) and 'Tools' (Policy simulator). The bottom of the page includes standard AWS navigation links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

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

The screenshot shows the AWS IAM 'Users' page. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main area displays a table titled 'Users (1)'. The table has one row for 'user-1'. The columns include 'User name' (user-1), 'Path' (/), 'Groups' (1), 'Last activity' (1 hour ago), 'MFA' (none), 'Password age' (never), and 'Console last sign-in' (never). There are 'Delete' and 'Create user' buttons at the top right of the table.

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

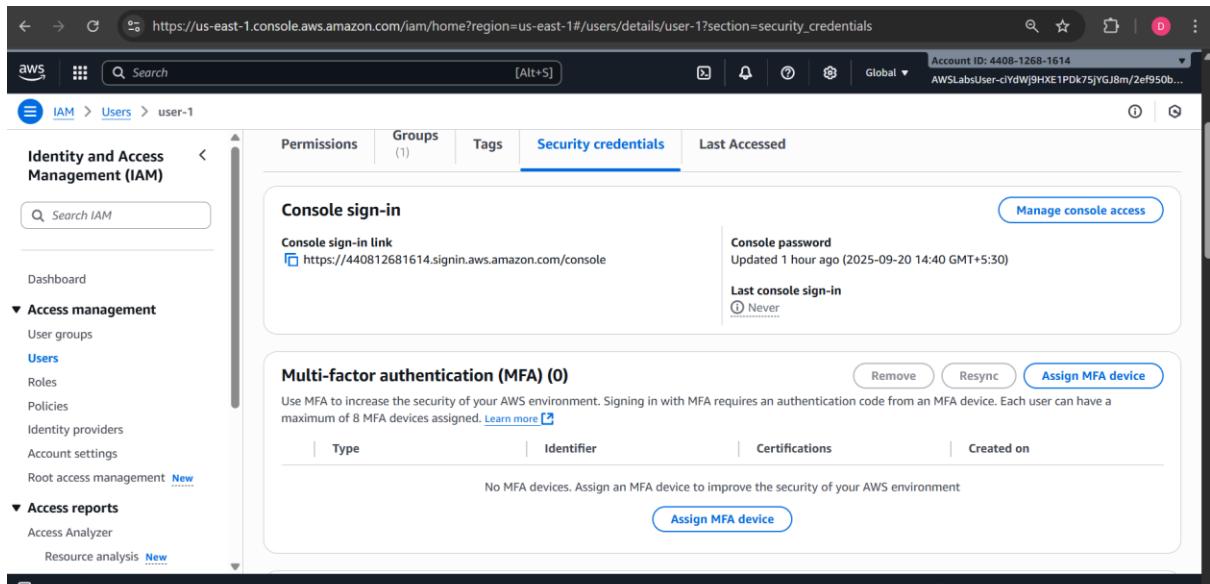
The screenshot shows the 'user-1' details page. The left sidebar is identical to the previous screenshot. The main area has a 'Summary' section with details: ARN (arn:aws:iam::440812681614:user/user-1), Console access (Enabled without MFA), and Last console sign-in (Never). Below this is a 'Permissions' tab, which is currently selected, showing 'Permissions policies (1)'. A table lists the policy: Policy name (aws:iam:UpdateAccessKey), Type (AWS Lambda), and Attached via (user user-1_01). There are 'Remove' and 'Add permissions' buttons at the top of this section.

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

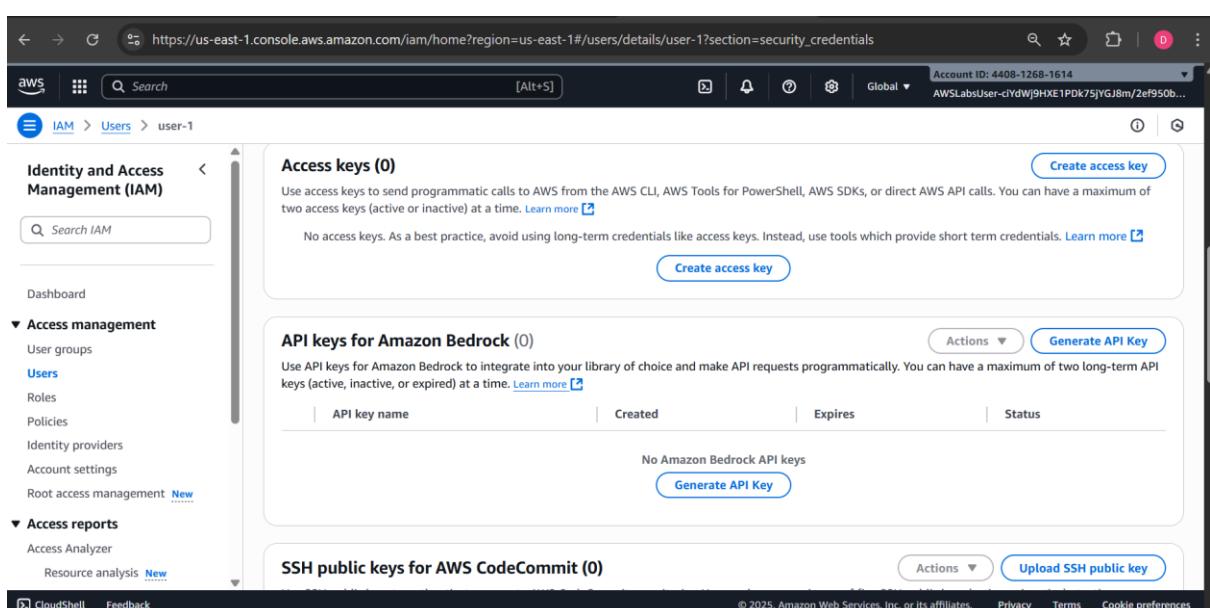
Here, you can see how many access keys a user has, when an access key was created, whether a Multi-Factor Authentication (MFA) device is assigned, and more.

- Access Keys:** Keys can be active or inactive and only administrators have the ability to deactivate 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.



The screenshot shows the AWS IAM Security Credentials page for a user named 'user-1'. The 'Security credentials' tab is selected. Under 'Console sign-in', there is a 'Console sign-in link' to https://440812681614.signin.aws.amazon.com/console. A 'Console password' was updated 1 hour ago. Under 'Multi-factor authentication (MFA)', it says '0' assigned MFA devices. There is a 'Assign MFA device' button. The bottom of the page includes links for CloudShell and Feedback, and standard footer links for Privacy, Terms, and Cookie preferences.



The screenshot shows the AWS IAM Security Credentials page for the same user 'user-1'. The 'Access keys (0)' section has a 'Create access key' button. The 'API keys for Amazon Bedrock (0)' section has a 'Generate API Key' button. The 'SSH public keys for AWS CodeCommit (0)' section has an 'Upload SSH public key' button. The bottom of the page includes links for CloudShell and Feedback, and standard footer links for Privacy, Terms, and Cookie preferences.

Identity and Access Management (IAM)

HTTPS Git credentials for AWS CodeCommit (0)
Generate a user name and password you can use to authenticate HTTPS connections to AWS CodeCommit repositories. You can have a maximum of 2 sets of credentials (active or inactive) at a time. [Learn more](#)

User name	Created	Status
No credentials		

Credentials for Amazon Keyspaces (for Apache Cassandra) (0)
Generate a user name and password you can use to authenticate to Amazon Keyspaces. You can have a maximum of two sets of credentials (active or inactive) at a time. [Learn more](#)

User name	Created	Status
No credentials		

CloudShell Feedback

Identity and Access Management (IAM)

X.509 Signing certificates (0)
Use X.509 certificates to make secure SOAP-protocol requests to some AWS services. You can have a maximum of two X.509 certificates (active or inactive) at a time. [Learn more](#)

Creation time	Thumbprint	Status
No X.509 certificates		

AWS Lambda functions (0)
AWS Lambda functions are serverless compute functions that run in response to events. You can have a maximum of 100 Lambda functions per user account.

Name	Last modified	Size	Actions
No Lambda functions found			

CloudShell Feedback

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.

The screenshot shows the AWS IAM User Details page for a user named 'user-1'. The 'Groups' tab is selected, displaying the user's group membership. The 'Attached policies' column indicates that the 'ReadOnlyAccess' policy is attached to the user via the 'user1group' group.

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.

The screenshot shows the AWS IAM User Details page for a user named 'user-1'. The 'Permissions' tab is selected, displaying the attached policies. The 'Attached via' column shows that the 'ReadOnlyAccess' policy is attached to the user via the 'user1group' group.

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

The screenshot shows the IAM Policy Simulator interface. On the left, the 'Users, Groups, and Roles' pane displays a list of users, with 'user-1' selected. On the right, the 'Policy Simulator' pane has 'Mode : Existing Policies' selected. The 'Select service' dropdown is set to 'AWS Identity and Access Management'. The 'Action Settings and Results' section shows 0 actions selected, 0 actions not simulated, 0 actions allowed, and 0 actions denied. A table at the bottom lists actions for 'user-1':

Service	Action	Resource Type	Simulation Resource	Permission
AWS Identity and Acc...				

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**

The screenshot shows the IAM Policy Simulator interface. On the left, the 'Policies' pane shows 'Selected user: user-1' and 'AWS Organizations SCPs'. Under 'IAM Policies', there is a checkbox for 'ReadOnlyAccess' which is checked. On the right, the 'Policy Simulator' pane shows 'Mode : Existing Policies' selected. The 'Select service' dropdown is set to 'AWS Identity and Access Management'. The 'Action Settings and Results' section shows 2 actions selected, 2 actions not simulated, 0 actions allowed, and 0 actions denied. A table at the bottom lists actions for 'user-1':

Service	Action	Resource Type	Simulation Resource	Permission
AWS Identity and Acc...	DeleteGroup	group	*	Not simulated
AWS Identity and Acc...	DeleteRolePolicy	role	*	Not simulated

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).

The screenshot shows the IAM Policy Simulator interface. On the left, there's a sidebar with tabs for 'Policies' (selected), 'Back', and 'Create New Policy'. It shows the selected user is 'user-1' and lists 'AWS Organizations SCPs' and 'IAM Policies'. Under 'IAM Policies', there is a single policy named 'ReadOnlyAccess' with a checkmark. The main panel is titled 'Policy Simulator' and has a 'Mode : Existing Policies' dropdown set to 'assumed-role/AWSLabsUser-...'. Below this, there are buttons for 'Run Simulation', 'Reset Contexts', and 'Clear Results'. A section titled 'Global Settings' is expanded, showing 'Action Settings and Results' with two entries. Both entries show 'AWS Identity and Acc...' as the service, 'DeleteGroup' and 'DeleteRolePolicy' as actions, 'group' and 'role' as resource types, and '*' as simulation resources. Both entries have a permission status of 'denied' and the note 'Implicitly denied (no matching statements)'.

Consider: Why do you 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

The screenshot shows the AWS IAM console with a search result for 'EC2'. The left navigation pane includes 'Identity and Management', 'Access management', 'Users', and 'Access reporting'. The main content area displays 'Services' and 'Features' related to EC2. The 'Services' section lists 'EC2' (Virtual Servers in the Cloud), 'EC2 Image Builder' (A managed service to automate build, customize and deploy OS images), and 'Recycle Bin' (Protect resources from accidental deletion). The 'Features' section lists 'EC2 Instances' (CloudWatch feature) and 'EC2 Resource Health' (CloudWatch feature). A sidebar on the right shows permission management for a group named 'user1group'.

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*.

The screenshot shows the AWS EC2 home page. The left navigation pane is expanded to show 'Instances' selected. The main content area includes sections for 'Resources' (listing various EC2 components like Instances, Auto Scaling Groups, and Snapshots), 'Launch instance' (with a prominent orange 'Launch instance' button), 'Service health' (with a 'AWS Health Dashboard' button), and 'Explore AWS' (with a callout about getting up to 40% better price performance). A blue banner at the top of the main content area says 'You can change your default landing page for EC2.'

The screenshot shows the AWS EC2 Instances page. In the left navigation pane, under the 'Instances' section, 'Instances' is selected. The main content area displays a table titled 'Instances (3) Info' with three rows. The columns are: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Zone. The instances listed are:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Web Server	i-02cff3e8add9bef25	Running	t3.micro	3/3 checks passed	View alarms	us-east-1a
SQL Server	i-0dbe38e6062d1ac5b	Running	t3.micro	3/3 checks passed	View alarms	us-east-1a
Bastion Host	i-0626b8444c726023f	Running	t3.micro	3/3 checks passed	View alarms	us-east-1a

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**.

The screenshot shows the AWS Security Groups page. In the left navigation pane, under the 'Network & Security' section, 'Security Groups' is selected. The main content area displays a table titled 'Security Groups (1/5) Info' with five rows. The columns are: Name, Security group ID, Security group name, and VPC ID. The security groups listed are:

Name	Security group ID	Security group name	VPC ID
WebServerSG	sg-0ebdfbcadcbacfb1	WebSecuritySG	vpc-0377789818daf4137
-	sg-0f1c71821a5611adb	default	vpc-0692deb089d815d26
BastionSG	sg-06b67edff47e38ae9	BastionSG	vpc-0377789818daf4137
SQLSG	sg-082da207d139f657b	SQLSG	vpc-0377789818daf4137

Below the table, a details pane is open for the 'sg-0ebdfbcadcbacfb1 - WebSecuritySG' security group. The tabs in the details pane are: Details, Inbound rules, Outbound rules, Sharing - new, VPC associations - new, and Tags. The 'Details' tab is selected.

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.

Name	Security group ID	Security group name	VPC ID
BastionSG	sg-06b67edff47e38ae9	BastionSG	vpc-0377789818daf4137
SQLSG	sg-082da207d139f657b	SQLSG	vpc-0377789818daf4137
-	sg-07e18179356054c	default	vpc-0377789818daf4137

Type	Protocol	Port range	Source	Description
HTTP	TCP	80	10.10.10.0/24	-
RDP	TCP	3389	sg-06b67edff47e38ae9 ...	-
HTTPS	TCP	443	10.10.10.0/24	-

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.

The screenshot shows the AWS EC2 Security Groups page. The left sidebar includes options for Snapshots, Lifecycle Manager, Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers, Target Groups, Trust Stores), and Auto Scaling (Auto Scaling Groups, Settings). The main content area displays a table of security groups with columns for Name, Security group ID, Security group name, and VPC ID. One row is selected: BastionSG (sg-06b67edff47e38ae9). Below this, a detailed view for BastionSG shows the Inbound rules tab with two entries:

Name	Security group rule ID	IP version	Type	Protocol	Port
sgr-0375114c8a9e3f03e	IPv4	SSH	TCP	22	
sgr-010958f528bdb6120	IPv4	RDP	TCP	3389	

The screenshot shows the AWS EC2 Security Groups page, identical to the previous one but with the Outbound rules tab selected for the BastionSG security group. The table shows one outbound rule:

Name	Security group rule ID	IP version	Type	Protocol	Port
sgr-0c6aa7856a82bb40a	IPv4	All traffic	All	All	

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?

The screenshot shows the AWS EC2 Security Groups page. The left sidebar includes options for Snapshots, Lifecycle Manager, Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers, Target Groups, Trust Stores), Auto Scaling (Auto Scaling Groups, Settings), and CloudShell/Feedback.

The main content displays the Security Groups (1/5) table with the following data:

Name	Security group ID	Security group name	VPC ID
sg-07e1818179356054c	sg-07e1818179356054c	default	vpc-0377789818daf4137
BastionSG	sg-06b67edff47e38ae9	BastionSG	vpc-0377789818daf4137
SQLSG	sg-082da207d139f657b	SQLSG	vpc-0377789818daf4137
-	sg-07e1818179356054c		vpc-0377789818daf4137

Below the table, the details for the SQLSG security group are shown, specifically the Inbound rules section. It contains one rule:

Security group rule ID	IP version	Type	Protocol	Port range
sgr-0c568898515043a4c	-	MSSQL	TCP	1433

The screenshot shows the AWS EC2 Security Groups page, identical to the previous one but with the Outbound rules tab selected for the SQLSG security group.

The main content displays the Outbound rules table with the following data:

Name	Security group rule ID	IP version	Type	Protocol	Port
-	sgr-09f16a0cf8084df3a	IPv4	All traffic	All	All

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.

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed, showing options like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store. The main content area has a header 'Instances (1/3) Info' with filters for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Zone. A table lists three instances: 'Web Server' (i-02cff3e8add9bef25, Running, t3.micro, 3/3 checks passed, us-east-1a), 'Unselect instance: Web Server' (i-be38e6062d1ac5b, Running, t3.micro, 3/3 checks passed, us-east-1a), and 'Bastion Host' (i-0626b8444c726023f, Running, t3.micro, 3/3 checks passed, us-east-1a). Below the table, a details panel for 'i-02cff3e8add9bef25 (Web Server)' is expanded, showing tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. Under 'Details', there's an 'Instance summary' section with fields for Instance ID (i-02cff3e8add9bef25), Public IPv4 address (34.201.102.52), Private IPv4 addresses (172.31.1.108), IPv6 address (-), Instance state (Running), and Public DNS (-).

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

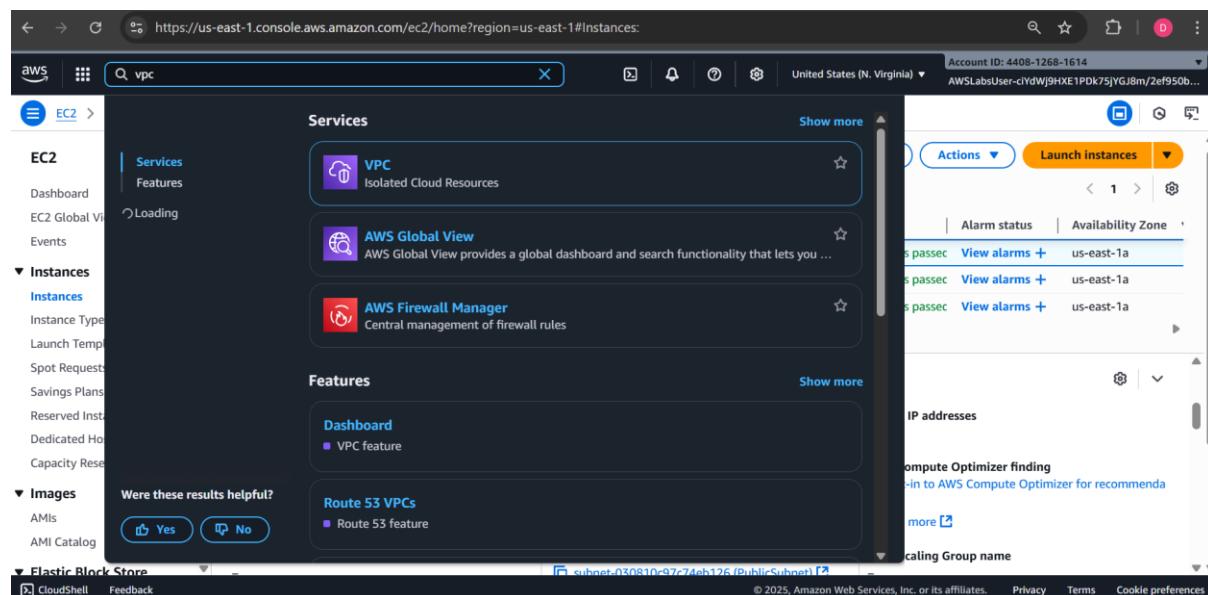
Note: The VPC ID should look similar to: *vpc-0586914dd2bce2335*.

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

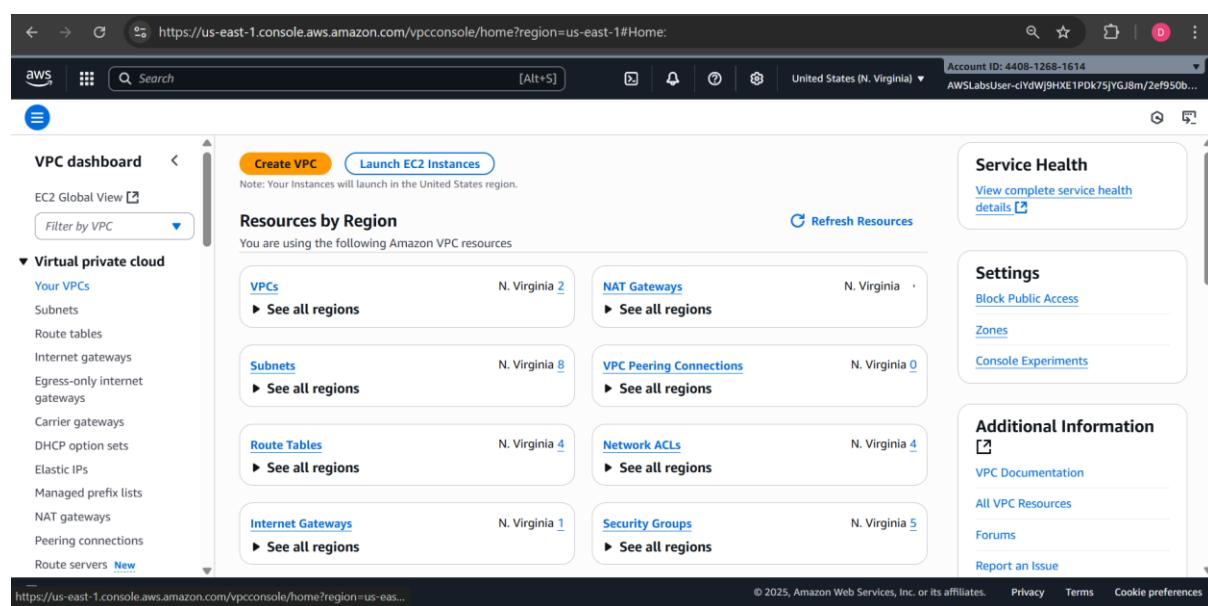
In this section, you review your existing VPCs, subnets, and Network ACL capabilities within a Virtual Private Cloud.

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



The screenshot shows the AWS Management Console EC2 home page. The search bar at the top contains 'vpc'. The left navigation pane is open, showing sections for EC2, Instances, Images, and Elastic Block Store. The main content area displays search results for 'vpc' under 'Services' and 'Features'. The 'VPC' service card is highlighted, showing its description as 'Isolated Cloud Resources'. Other cards include 'AWS Global View' and 'AWS Firewall Manager'. Under 'Features', there are cards for 'Dashboard' (VPC feature) and 'Route 53 VPCs' (Route 53 feature). On the right side, there is a 'Launch Instances' button and a list of alarms for the 'us-east-1a' availability zone. A message at the bottom asks if the results were helpful, with 'Yes' and 'No' buttons.

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



The screenshot shows the AWS Management Console VPC console home page. The left navigation pane is open, showing 'Virtual private cloud' and 'Your VPCs'. The main content area displays 'Resources by Region' for the 'N. Virginia' region. It shows counts for VPCs (2), Subnets (8), Route Tables (4), Internet Gateways (1), NAT Gateways (4), VPC Peering Connections (0), Network ACLs (4), Security Groups (5), and Internet Gateways (1). There are buttons for 'Create VPC' and 'Launch EC2 Instances'. On the right side, there are sections for 'Service Health', 'Settings' (with options for 'Block Public Access', 'Zones', and 'Console Experiments'), and 'Additional Information' (with links for 'VPC Documentation', 'All VPC Resources', 'Forums', and 'Report an Issue').

34. Select **Lab VPC**.

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

The screenshot shows the AWS VPC console interface. On the left, there's a navigation sidebar with options like 'VPC dashboard', 'EC2 Global View', and 'Virtual private cloud'. Under 'Virtual private cloud', 'Your VPCs' is selected. The main area displays a table titled 'Your VPCs (1/2)'. It lists two VPCs: 'Lab VPC' (selected with a checkbox) and another entry. The 'Lab VPC' row contains the following details:

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
Lab VPC	vpc-0377789818daf4137	Available	Off	172.31.0.0/16	-
-	vpc-0692deb089d815d26	Available	Off	172.31.0.0/16	-

Below the table, a detailed view for 'vpc-0377789818daf4137 / Lab VPC' is shown. The 'Details' tab is selected, displaying the following configuration:

Details	Resource map	CIDRs	Flow logs	Tags	Integrations
<p>VPC ID vpc-0377789818daf4137</p> <p>DNS resolution Enabled</p>	<p>State Available</p> <p>Tenancy default</p>	<p>Block Public Access Off</p> <p>DHCP option set dopt-03c363b52d7f234e6</p>	<p>DNS hostnames Enabled</p> <p>Main route table rtb-01ee3d956506d2b2a</p>		

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.

The screenshot shows the AWS VPC Network ACLs page. The left sidebar includes 'VPC dashboard', 'EC2 Global View', and 'Virtual private cloud' sections. The 'Virtual private cloud' section has 'Your VPCs' selected. The main content area is titled 'Network ACLs (1) Info'. It shows a single Network ACL entry:

Name	Network ACL ID	Associated with	Default	VPC ID
acl-05a168bcb68f08fd	-	-	Yes	vpc-0377789818daf4137 / Lab_VPC

At the bottom of the page, there's a section titled 'Select a network ACL'.

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.

The screenshot shows the AWS VPC Network ACLs page. The URL is https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#acls.networkAclId=acl-05a168bcb68f08fda. The page displays a list of Network ACLs with one item: acl-05a168bcb68f08fda. The Inbound rules tab is selected, showing a single rule (Rule number 100) allowing all traffic from 0.0.0.0/0.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow

The screenshot shows the AWS VPC Network ACLs page. The URL is https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#acls.networkAclId=acl-05a168bcb68f08fda. The page displays a list of Network ACLs with one item: acl-05a168bcb68f08fda. The Outbound rules tab is selected, showing a single rule (Rule number 100) allowing all traffic to 0.0.0.0/0.

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow

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

The screenshot shows the AWS Management Console interface. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#acl:networkAclId=acl-05a168bcb68f08fd>. The top navigation bar includes the AWS logo, a search bar with 'CloudWatch', and account information: Account ID: 4408-1268-1614, AWSLabsUser-c1YdWj9HXE1Pdk75jYGJ8m/2ef950b...'. The left sidebar has a 'VPC' section expanded, showing 'VPC dashboard', 'EC2 Global View', and 'Virtual private clouds' with sub-options like 'Your VPCs', 'Subnets', 'Route tables', 'Internet gateways', 'Egress-only internet gateways', 'Carrier gateways', 'DHCP options', 'Elastic IPs', 'Managed prefixes', 'NAT gateways', 'Peering connections', and 'Route servers'. A 'Were these results helpful?' button with 'Yes' and 'No' options is present. The main content area is titled 'Services' and lists 'CloudWatch' (Monitor Resources and Applications), 'Athena' (Serverless interactive analytics service), and 'Amazon EventBridge' (Serverless service for building event-driven applications). To the right, there's a 'Network ACLs' section for a 'default' VPC ID 'vpc-0377789818daf4137 / Lab VPC', showing an 'Edit outbound rules' button and an 'Allow' rule.

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

The screenshot shows the AWS CloudWatch home page for the US East (N. Virginia) region. The left sidebar includes sections for Dashboards, AI Operations, Alarms, Logs, Metrics (with sub-options for All metrics, Explorer, and Streams), Application Signals (APM), GenAI Observability (Preview), and Network Monitoring. The main content area displays the 'Get started with CloudWatch' section, which includes four cards: 'Create alarms' (Set alarms on any of your metrics to receive notification when your metric crosses your specified threshold), 'Create a default dashboard' (Create and name any CloudWatch dashboard CloudWatch-Default to display it here), 'View logs' (Monitor using your existing system, application and custom log files), and 'View events' (Write rules to indicate which events are of interest to your application and what automated action to take). Below this is a 'Get started with Observability solutions' section, which links to 'Explore observability solutions'. The top right corner shows account information: Account ID: 4408-1268-1614, AWSLabsUser-c1YdWj9HXE1PDK75jYGJ8m/2ef950b..., and the current UTC timezone.

41. On the Browse tab, choose EC2.

The screenshot shows the 'Metrics' section of the CloudWatch console. The top navigation bar includes tabs for Metrics (selected), Multi source query, Graphed metrics, Options, Source, and a search bar. Below this is a list of metrics grouped by service: Billing (5), DynamoDB (10), EBS (42), and EC2 (60). Each group has a link to 'View automatic dashboard'. The bottom right corner shows copyright information: © 2025, Amazon Web Services, Inc. or its affiliates.

42. Choose Per-Instance Metrics.

The screenshot shows the AWS CloudWatch Metrics console at the URL [https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?graph=~\(\)&namespace=~'AWS*2fEC2](https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricsV2?graph=~()&namespace=~'AWS*2fEC2). The interface includes a top navigation bar with account information (Account ID: 4408-1268-1614, AWSLabsUser-c1YdWj9HXE1PDK75jYGJ8m/2ef950b...), a search bar, and various navigation and configuration buttons. Below the header, the main area displays a message: "Your CloudWatch graph is empty. Select some metrics to appear here." A search bar at the bottom allows users to "Search for any metric, dimension, resource id or account id". The central panel shows a list of metrics under "Per-Instance Metrics" with a count of 60.

43. In the Search box, search for CPUUtilization

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

The screenshot shows the AWS CloudWatch Metrics console after searching for "CPUUtilization". The search results table lists two EC2 instances: "Bastion Host" and "Bastion Host". The table has columns for Instance name, InstanceId, Metric name, and Alarms. Both instances show "No alarms". The search bar at the bottom of the table is still active with "CPUUtilization".

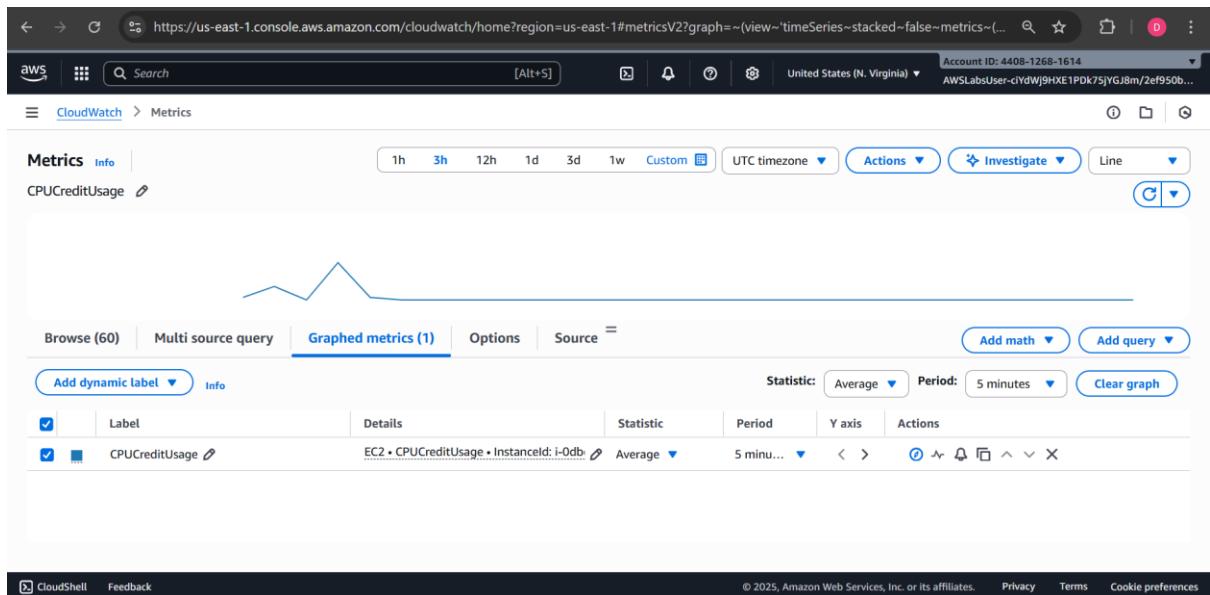
Instance name	InstanceId	Metric name	Alarms
Bastion Host	i-0626b8444c726...	CPUSurplusCreditsCharged ⓘ	No alarms
Bastion Host	i-0626b8444c726...	CPUCreditUsage ⓘ	No alarms

The screenshot shows the AWS CloudWatch Metrics dashboard. At the top, there are navigation links for 'Metrics' and 'Info'. Below this is a search bar and a time range selector from '1h' to 'Custom'. A 'Actions' button and an 'Investigate' button are also present. The main area displays a message: 'Your CloudWatch graph is empty. Select some metrics to appear here.' Below this is a table titled 'Browse (60)' showing various metrics for 'SQL Server' and 'Web Server' instances. The table includes columns for metric names like 'StatusCheckFailed_Instance', 'NetworkPacketsIn', etc., and status indicators like 'No alarms'. At the bottom, there are links for 'CloudShell' and 'Feedback', along with copyright information for 2025.

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

The screenshot shows the AWS CloudWatch Metrics search interface. The search bar at the top contains the query "EC2". The results pane on the left lists various services and features under the "Metrics" category, including EC2, EC2 Image Builder, Recycle Bin, and EC2 Instances. The main content area displays a graph titled "CloudWatch Metrics for EC2 Instances". The graph has a single data series named "CPU Credit Usage" over a period of 5 minutes. The graph includes options for "Add math" and "Add query". The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, and links to Privacy, Terms, and Cookie preferences.

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

The screenshot shows the AWS EC2 home page. The left navigation pane is expanded, showing sections for Launch templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs), and Compute (Lambda, Step Functions). The "Volumes" link under "Elastic Block Store" is highlighted. The main content area displays a summary of resources: 3 instances (running), 0 auto scaling groups, 0 capacity reservations, 0 dedicated hosts, 0 elastic IPs, 3 instances, 0 key pairs, 0 load balancers, 0 placement groups, 5 security groups, 0 snapshots, 0 volumes, and 3 volume snapshots. It also shows service health and an explore AWS section. The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, and links to Privacy, Terms, and Cookie preferences.

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

The screenshot shows the AWS CloudTrail service page. In the navigation pane on the left, under the 'CloudTrail' section, the 'Dashboard' link is selected. The main content area displays the 'Services' and 'Features' sections. The 'Services' section lists CloudTrail, Detective, and Athena. The 'Features' section includes 'Create a SFTP server' (AWS Transfer Family feature) and 'Insights' (CloudTrail feature). A sidebar on the right shows a table of snapshots and a line graph.

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

The screenshot shows the AWS CloudTrail Trails dashboard. The left navigation pane has 'CloudTrail' selected, with 'Trails' also highlighted. The main area shows a yellow warning box about AccessDeniedException and a blue info box about enriching CloudTrail events. Below these are sections for 'Query results history' and 'Trails'. The 'Trails' section lists two trails: 'AWSLabs-CloudtrailSubaccountAudit' (Status: unavailable) and 'LabCloudTrail' (Status: Logging).

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.

Screenshot of the AWS CloudTrail console showing the 'Trails' list. The table displays two trails:

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	Cloud Watch Logs log group	Status
AWSLabs-CloudtrailSubaccountAudit	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:184790415257:trail/AWSLabs-CloudtrailSubaccountAudit	Disabled	Yes	subaccountcloudtrail-all-184790415257	-	-	Status unavailable
LabCloudTrail	US East (N. Virginia)	No	arn:aws:cloudtrail:us-east-1:140812681614:trail/LabCloudTrail	Disabled	No	spl73logs-us-east-1-878451814	-	-	Login

Screenshot of the AWS CloudTrail console showing the 'LabCloudTrail' details page.

General details

Trail logging	Trail log location	Log file validation	SNS notification delivery
<input checked="" type="checkbox"/> Logging	spl73logs-us-east-1-878451814/AWSLogs/440812681614	Disabled	Disabled
Trail name	Last log file delivered	Last file validation delivered	Last SNS notification
LabCloudTrail	September 20, 2025, 17:14:41 (UTC+05:30)	-	-
Multi-region trail	Log file SSE-KMS encryption		
No	Not enabled		
Apply trail to my organization			
Not enabled			

CloudWatch Logs

No CloudWatch Logs log groups
CloudWatch Logs is not configured for this trail

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

The screenshot shows the AWS CloudTrail service page. On the left, there's a sidebar with links like Dashboard, Event history, Insights, Lake, Marketplace, and Trail details. The main content area has sections for 'Services' and 'Features'. Under 'Services', there are cards for S3 (Scalable Storage in the Cloud), S3 Glacier (Archive Storage in the Cloud), and AWS Snow Family (Large Scale Data Transport). Under 'Features', there are cards for S3 on Outposts (AWS Outposts feature) and Exports to S3 (DynamoDB feature). At the bottom, there's a feedback section asking if results were helpful, with 'Yes' and 'No' buttons. The top right shows account information: Account ID: 4408-1258-1614, AWSLabsUser-cYdWj9HXE1Pdk75jYGJ8m/2ef950b..., and a link to AWSLabsUser-cYdWj9HXE1Pdk75jYGJ8m/2ef950b... .

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

The screenshot shows the AWS S3 service page. On the left, there's a sidebar with links for General purpose buckets, Directory buckets, Table buckets, Vector buckets, Access Grants, Access Points (General Purpose Buckets, FSx file systems), Access Points (Directory Buckets), Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, and Storage Lens. The main content area shows 'General purpose buckets' (3) and 'Directory buckets'. The 'General purpose buckets' table lists three buckets:

Name	AWS Region	Creation date
awslabs-resources-krxqqla59su18d-us-east-1-440812681614	US East (N. Virginia) us-east-1	October 3, 2020, 06:44:24 (UTC+05:30)
awslabs-resources-r5b3y6ojjszcap-us-east-1-440812681614	US East (N. Virginia) us-east-1	October 24, 2023, 00:29:30 (UTC+05:30)
spl73logs-us-east-1-878451814	US East (N. Virginia) us-east-1	September 20, 2025, 14:39:41 (UTC+05:30)

At the bottom, there are sections for 'Account snapshot' (View dashboard) and 'External access summary - new' (View details). The top right shows account information: Account ID: 4408-1258-1614, AWSLabsUser-cYdWj9HXE1Pdk75jYGJ8m/2ef950b..., and a link to AWSLabsUser-cYdWj9HXE1Pdk75jYGJ8m/2ef950b... .

57. Choose the **AWSLogs** link.

The screenshot shows the AWS S3 console interface. The left sidebar has 'Amazon S3' selected under 'General purpose buckets'. The main area shows the 'spl73logs-us-east-1-878451814' bucket with one object: 'AWSLogs/'. The 'Actions' dropdown menu is open, showing options like Copy S3 URI, Copy URL, Download, Open, Delete, Actions (with a dropdown arrow), Create folder, and Upload.

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.

The screenshot shows the AWS S3 console interface, navigating through the AWSLogs folder. The path in the top navigation bar is 'Amazon S3 > Buckets > spl73logs-us-east-1-878451814 > AWSLogs/ > 440812681614/ > CloudTrail/'. The main area shows the 'CloudTrail/' folder with one object: 'us-east-1/'. The 'Actions' dropdown menu is open, showing options like Copy S3 URI, Copy URL, Download, Open, Delete, Actions (with a dropdown arrow), Create folder, and Upload.

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**.

The screenshot shows the AWS CloudTrail log viewer interface. On the left, there's a sidebar with 'Amazon S3' navigation and a 'General purpose buckets' section listing various bucket types like Directory buckets, Table buckets, Vector buckets, Access Grants, etc. Below that is a 'Storage Lens' section. The main area is titled 'Objects (1/79)' and contains a table of logs. The first log is selected, showing its details: Name is '440812681614_CloudTrail', Type is 'gz', Last modified is 'September 20, 2025, 14:44:52 (UTC+05:30)', Size is '1.4 KB', and Storage class is 'Standard'. The file content is partially visible as 'nDxKoPtpnCV6.json.gz'. There are two other logs listed below it.

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.

This screenshot shows a browser window displaying the raw JSON content of one of the CloudTrail logs. The log is very long and detailed, showing numerous events related to AWS Lambda function executions and CloudFormation stack operations. Key fields visible include 'eventVersion', 'userIdentity', 'principalId', 'awsRegion', 'sourceIPAddress', 'userAgent', and various 'requestParameters' and 'responseElements' sections. The log is presented in a monospaced font, making it difficult to read in full.

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](#)