

# AWS EC2 Security Hardening Project Report

Instance ID: [i-0bee6a7a052141dbd](#)

Prepared By: Purna Kishore Kondapaneni

Version: 1.0

---

## Table of Contents

1. System Information
2. IAM Role Configuration
3. Security Tool Results
  - 3.1 Amazon Guard Duty
  - 3.2 Amazon Inspector
  - 3.3 Lynis Audit Results
  - 3.4 CIS Benchmark Script
4. Hardening Actions Taken
5. Cloud Security Hardening Architecture Diagram
6. Logs & Artifacts
7. Summary & Recommendations
8. Appendix
  - A. SSM Session Access
  - B. Route Table Entry
  - C. Screenshot Descriptions

---

### 1. System Information

Field	Value
OS / Distro	Amazon Linux 2 / Ubuntu
EC2 Instance Type	t2. micro / t3.medium
Region	us-east-1 / us-east-2
Instance ID	<a href="#">i-0bee6a7a052141dbd</a>
Public IP	3.145.52.192
Private IP	172.31.8.89
IAM Role Attached	Yes

## 2. IAM Role Configuration

Policy Name	Attached
AmazonSSMManagedInstanceCore	Yes
AmazonInspector2ReadOnlyAccess	Yes
CloudWatchAgentServerPolicy	Yes

## 3. Security Tool Results

### 3.1 Amazon Guard Duty

Detection Type	Status
Port Scan	No / Yes
SSH Brute Force	No / Yes
IAM Anomaly	No / Yes
Rootkit Activity	No / Yes

### 3.2 Amazon Inspector

Check	Result	Remediation
OS Vulnerabilities (CVE)	Yes / No	Patched
Outdated Packages	Yes / No	Updated
Missing Critical Patches	Yes / No	Applied

### 3.3 Lynis Audit Results

Category	Status	Notes
Authentication	OK	SSH Root Login disabled
File Permissions	Warn	Some log files world-readable
Kernel Settings	Suggest	sysctl hardening needed
Malware Scanner	None	Install ClamAV suggested

*Action Taken:* Hardened SSH, adjusted file permissions

### 3.4 CIS Benchmark Script (Ubuntu/Debian only)

Rule ID	Description	Result	Fix Applied
1.1.1	Disable unused filesystems	Fail	Yes
2.2.2	Disable FTP	Pass	Not Needed
5.3.3	Lockout after failed SSH attempts	Warn	Yes

#### **4. Hardening Actions Taken**

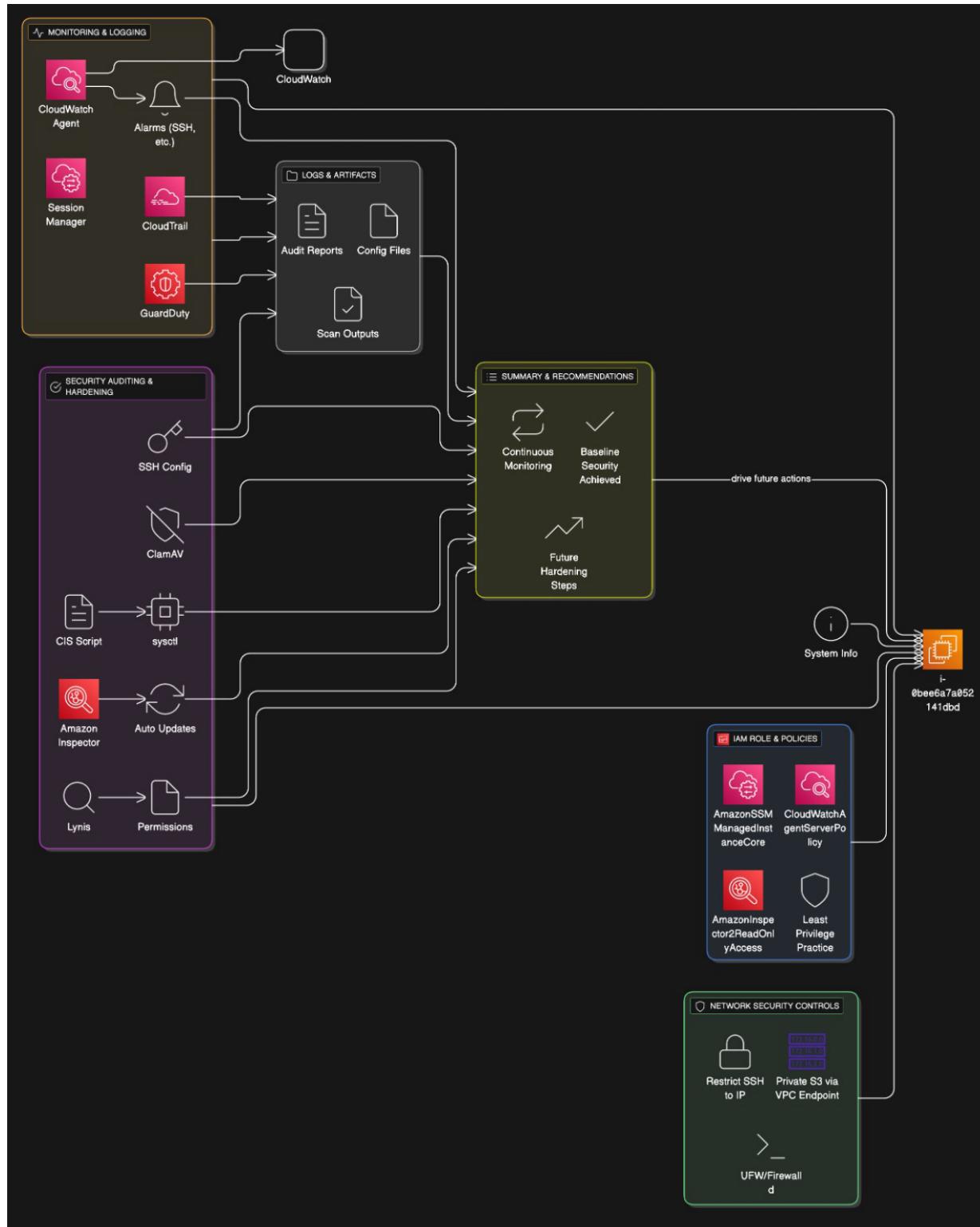
Action	Status
Disabled root login over SSH	Yes
Disabled password authentication	Yes
Enforced automatic OS updates	Yes
Set restrictive permissions on /tmp	Yes
Enabled ufw or firewall	Yes
CloudWatch Agent configured	Yes

---

#### **5. Logs & Artifacts (Attached Separately)**

- lynis-report.dat
  - cloudwatch-agent-status.log
  - inspector-findings. Json
  - /etc/ssh/sshd\_config (hardened)
  - cis-hardening-results.txt
-

# Architecture of Hardening:



## Deploying a Cloud Instance:

The screenshot shows the AWS EC2 Connect interface. At the top, there's a navigation bar with the AWS logo, a search bar, and account information for 'United States (Ohio)' and 'kishore'. Below the navigation is a breadcrumb trail: EC2 > Instances > i-0bee6a7a052141dbd > Connect to instance. A 'Connect' button is highlighted in blue. A sub-section titled 'Connect Info' provides instructions: 'Connect to an instance using the browser-based client.' It lists four steps: 1. Open an SSH client, 2. Locate your private key file (security.pem), 3. Run the command 'chmod 400 "security.pem"', and 4. Connect to your instance using its Public DNS ('ec2-3-145-52-192.us-east-2.compute.amazonaws.com'). An example command is provided: 'ssh -i "security.pem" ec2-user@ec2-3-145-52-192.us-east-2.compute.amazonaws.com'. A note at the bottom states: 'Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' A 'Cancel' button is located at the bottom right.

## Harden SSH G Network Access:

Restrict access to specific IPs using Security Groups:

Inbound rules have updated:

The screenshot shows the 'Edit inbound rules' page for a security group. The top navigation bar includes the AWS logo, search bar, and account information. The breadcrumb trail is EC2 > Security Groups > sg-03f8bd0898e9a69c2 - launch-wizard-4 > Edit inbound rules. A 'Edit inbound rules' button is highlighted in blue. A note below says 'Inbound rules control the incoming traffic that's allowed to reach the instance.' The main area displays three inbound rules:

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0bdcd5d28bf4058b7	HTTPS	TCP	443	Custom	0.0.0.0/0
sgr-066a4db4d6c1a4193	SSH	TCP	22	My IP	174.95.129.238/32
sgr-0686a42c657a1547d	HTTP	TCP	80	Custom	0.0.0.0/0

A note at the bottom left says: '⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' At the bottom right are 'Cancel', 'Preview changes', and 'Save rules' buttons.

**Screenshot 1:** Capture the *EC2 Console > Instance Details* pane showing the *Instance ID*, *private/public IP*, and *IAM role* assignment for evidence.

## Implementing least privilege with IAM:

The screenshot shows the AWS IAM console. The left sidebar is collapsed. The main content area displays the details for the 'EC2SecureRole'. The 'Summary' section includes the ARN (arn:aws:iam::653091864286:role/EC2SecureRole), creation date (July 03, 2025, 18:13 (UTC-04:00)), last activity (none), and maximum session duration (1 hour). The 'Permissions' tab is selected, showing one policy attached: 'AmazonEC2ReadOnlyAccess' (AWS managed). The 'Permissions boundary' is listed as '(not set)'. The bottom right corner shows copyright information: © 2025, Amazon Web Services, Inc. or its affiliates.

The screenshot shows the AWS IAM console. The left sidebar is collapsed. The main content area displays a list of roles under the heading 'Roles (10)'. The table lists the following roles and their details:

Role name	Trusted entities	Last activity
AmazonInspector2ReadOnlyAccess	AWS Service: ec2	-
AmazonSSMManagedInstanceCore	AWS Service: ec2	-
AWSServiceRoleForAmazonGuardDuty	AWS Service: guardduty (Service-Link)	1 hour ago
AWSServiceRoleForAmazonGuardDutyMalwareProtection	AWS Service: malware-protection.gu	-
AWSServiceRoleForAmazonInspector2	AWS Service: inspector2 (Service-Link)	1 hour ago
AWSServiceRoleForAmazonInspector2Agentless	AWS Service: agentless.inspector2 (\$	56 minutes ago
AWSServiceRoleForSupport	AWS Service: support (Service-Link)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Link)	-
CloudWatchAgentServerPolicy	AWS Service: ec2	-
EC2SecureRole	AWS Service: ec2	12 minutes ago

aws | Search [Option+S] | United States (Ohio) | kishore | [EC2](#) > [Instances](#) > [i-0bee6a7a052141dbd](#) > [Modify IAM role](#)

**Modify IAM role** [Info](#)

Attach an IAM role to your instance.

**Instance ID**  
i-0bee6a7a052141dbd

**IAM role**  
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

EC2SecureRole [Create new IAM role](#)

[Cancel](#) [Update IAM role](#)

**Screenshot related to IAM:** In *IAM > Roles > HardenedEC2Role > Permissions* capture the list of *attached policies*. Highlight that no Administrator Access or wildcard (\*) permissions exist.

## Logging & Monitoring

**Console Navigation:** AWS Management Console > CloudTrail, Guard Duty, CloudWatch

Cloud Trail:

Management & Governance

**AWS CloudTrail**  
Continuously log your AWS account activity

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

**Create a trail with AWS CloudTrail**  
Get started with AWS CloudTrail by creating a trail to log your AWS account activity.  
[Create a trail](#)

**Pricing** [Pricing](#)

**Getting started** [What is AWS CloudTrail](#) [How AWS CloudTrail works](#) [Services that integrate with AWS CloudTrail](#)

**More resources** [Documentation](#) [FAQs](#) [API reference](#)

**How it works**

- Capture**: Record activity in AWS services as AWS CloudTrail events
- Store**: AWS CloudTrail delivers events to the AWS CloudTrail console, Amazon S3 buckets, and optionally Amazon CloudWatch Logs
- Act**: Use Amazon CloudWatch Alarms and Events to take action when important events are detected

**Benefits and features**

- Simplified compliance**: You can simplify your compliance audits by recording and storing event logs for actions that occur in your AWS account.
- Security automation**: With Amazon CloudWatch Events integration, you can define workflows that notify you when specific events are detected in your log activity.
- Visibility into user and resource activity**: You can identify which users, roles, and accounts called AWS, the source IP address of calls, and when the calls occurred. You can also use AWS CloudTrail Insights to detect unusual activity in your account.
- Security analysis and troubleshooting**: You can discover and troubleshoot security and operational issues by examining an ongoing record of significant changes in your AWS account. You can use AWS CloudTrail Insights to detect unusual activity in your account.

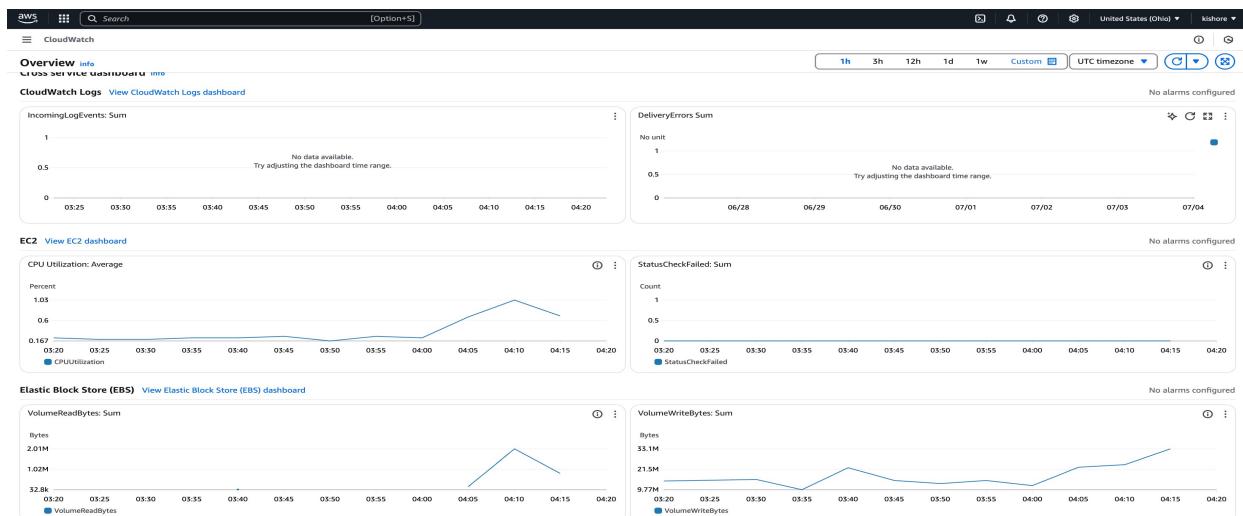
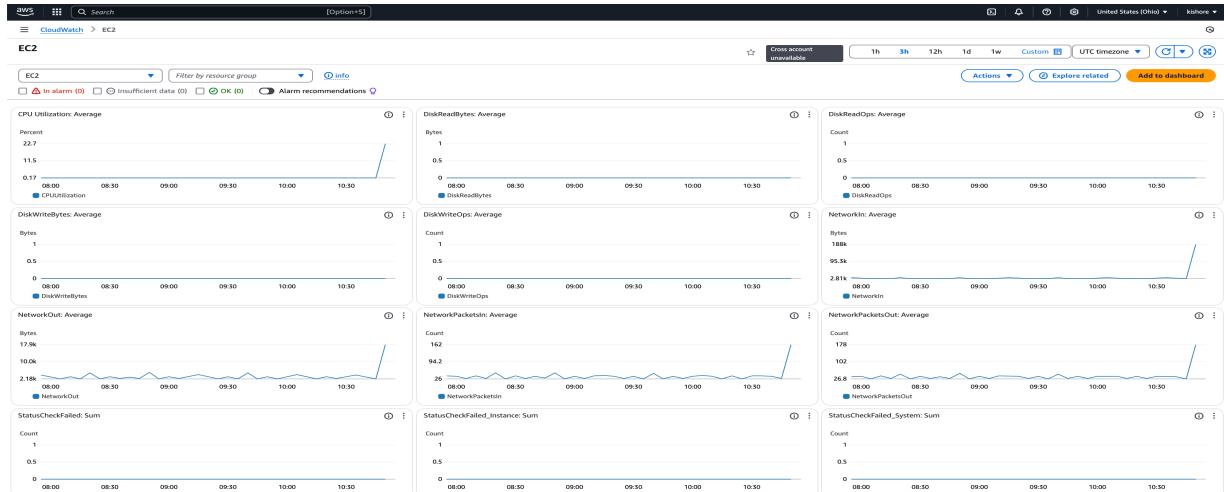
**Use cases**

- Compliance aid**: AWS CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards by providing a history of activity in your AWS account. For more information, download the AWS compliance白皮书 (white paper) [AWS CloudTrail for Log Management](#).
- Security analysis**: You can perform security analysis and detect user behavior patterns by passing AWS CloudTrail events into your log management and analytics solutions.
- Data exfiltration**: You can detect data exfiltration by collecting activity data on Amazon S3 objects and AWS Lambda functions through object level API events that are recorded in CloudTrail. After the data is collected, you can analyze the data to detect anomalies and trigger specific actions.
- Operational issue troubleshooting**: You can troubleshoot operational issues by using the AWS API call history in CloudTrail. For example, you can quickly identify the most recent changes made to resources in your environment, including creation, modification, and deletion of AWS resources such as Amazon EC2 instances, security groups, and Amazon EBS volumes.

Unsubscribe | Feedback | © 2021, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookies preferences

## Cloud Trail event history:

Event history (50+)					
Event history shows you the last 90 days of management events.					
Lookup attributes					
Read-only					
<input type="checkbox"/> <a href="#">SendSSHPublicKey</a>	July 04, 2025, 00:17:17 UTC-04:00	root	ec2-instance-connect.amazonaws.com	AWS:EC2:Instance	i-0beef6a7a052141dbd
<input type="checkbox"/> <a href="#">SendSSHPublicKey</a>	July 04, 2025, 00:12:42 UTC-04:00	root	ec2-instance-connect.amazonaws.co	AWS:EC2:Instance	i-0beef6a7a052141dbd
<input type="checkbox"/> <a href="#">Enable</a>	July 04, 2025, 00:10:56 UTC-04:00	root	inspector2.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">CreatePendingReport</a>	July 04, 2025, 00:10:07 UTC-04:00	root	inspector2.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">SendSSHPublicKey</a>	July 04, 2025, 00:08:49 UTC-04:00	root	ec2-instance-connect.amazonaws.co	AWS:EC2:Instance	i-0beef6a7a052141dbd
<input type="checkbox"/> <a href="#">CreateAssociation</a>	July 03, 2025, 23:25:17 UTC-04:00	EC2_ORCHESTRATOR	sem.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">PutParameter</a>	July 03, 2025, 23:25:17 UTC-04:00	EC2_ORCHESTRATOR	sem.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">PutType</a>	July 03, 2025, 23:25:11 UTC-04:00	Ec2StateController	events.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">PutTargets</a>	July 03, 2025, 23:25:11 UTC-04:00	Ec2StateController	events.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">PutTargets</a>	July 03, 2025, 23:25:11 UTC-04:00	Ec2StateController	events.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">PutType</a>	July 03, 2025, 23:25:11 UTC-04:00	Ec2StateController	events.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">CreateResourceSet</a>	July 03, 2025, 23:24:59 UTC-04:00	Ec2StateController	sem.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">CreateAssociation</a>	July 03, 2025, 23:24:59 UTC-04:00	Ec2StateController	sem.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">CreateAssociation</a>	July 03, 2025, 23:24:58 UTC-04:00	Ec2StateController	sem.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">CreateAssociation</a>	July 03, 2025, 23:24:58 UTC-04:00	Ec2StateController	sem.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">CreateAssociation</a>	July 03, 2025, 23:24:58 UTC-04:00	Ec2StateController	sem.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">CreateAssociation</a>	July 03, 2025, 23:24:58 UTC-04:00	Ec2StateController	sem.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">Enable</a>	July 03, 2025, 23:24:57 UTC-04:00	root	inspector2.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">UpdateEc2DeepImage...</a>	July 03, 2025, 23:12:26 UTC-04:00	root	sem.amazonaws.com	AWS:EC2:Instance	i-0beef6a7a052141dbd
<input type="checkbox"/> <a href="#">ReplaceEc2Instance...</a>	July 03, 2025, 22:10:15 UTC-04:00	root	ec2.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">DeleteAssociation</a>	July 03, 2025, 22:05:19 UTC-04:00	EC2_ORCHESTRATOR	sem.amazonaws.com	-	-
<input type="checkbox"/> <a href="#">DeleteParameter</a>	July 03, 2025, 22:05:19 UTC-04:00	EC2_ORCHESTRATOR	sem.amazonaws.com	-	-



## Guard duty summary (IDS):

The screenshot shows the AWS GuardDuty Summary page. On the left, a sidebar lists various protection plans: S3 Protection, EKS Protection, Extended Threat Detection (marked as New), Runtime Monitoring, Malware Protection for EC2, Malware Protection for S3, RDS Protection, and Lambda Protection. Below this are sections for Accounts, Usage, Settings, and Links. The main content area has tabs for 'Attack sequences - new' (0 findings) and 'Findings - new' (0 findings). It includes a chart for 'Total findings' (2 findings) across four severity levels: Critical (0), High (0), Medium (0), and Low (2). A 'Findings by severity' chart shows 2 findings for the Low category. Below these are sections for 'Least occurring findings' and 'Most common finding types'. A large callout box on the right introduces the new AWS Security Hub - public preview, encouraging users to try it. It also mentions Runtime Monitoring coverage for Amazon ECS, Amazon EKS, and Amazon EC2. At the bottom, there's a table for 'Resources with most findings'.

Resource	Account	Finding count	Last generated
AccessKey [ASAZQZ02073PHC8QHBU]	653091864286	1	a minute ago
AccessKey [ASAZQZ02073PKWWCCSAB]	653091864286	1	23 minutes ago

Screenshot of Guard Duty: Remediation and CVSS were shown

Performing a Security Audit:

Lynis or CIS Benchmark Reports –

- Review the output for warnings, suggestions, and hardening recommendations.
- Implement suggested changes where appropriate and safe

aws | ⚙️ | Search [Option+S]

```

2007-2024, CISOFy - https://cisofty.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####
[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]

-----
Program version: 3.1.5
Operating system: Linux
Operating system name: Amazon Linux
Operating system version: 2023
Kernel version: 6.1.141
Hardware platform: x86_64
Hostname: ip-172-31-8-89
-----
Profiles: /home/ec2-user/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: ./plugins
-----
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
-----
- Program update status... [ NO UPDATE ]

[+] System tools
-----
- Scanning available tools...
- Checking system binaries...

[+] Plugins (phase 1)

```

CloudShell Feedback

```

[+] System tools
-----
- Scanning available tools...
- Checking system binaries...

[+] Plugins (phase 1)
-----
Note: plugins have more extensive tests and may take several minutes to complete

- Plugin: pam
[...]
- Plugin: systemd
[...]

[+] Boot and services
-----
- Service Manager [ systemd ]
- Checking UEFI boot [ DISABLED ]
- Checking presence GRUB2 [ FOUND ]
- Checking for password protection [ OK ]
- Check running services (systemctl) [ DONE ]
  Result: found 19 running services
- Check enabled services at boot (systemctl) [ DONE ]
  Result: found 31 enabled services
- Check startup files (permissions) [ OK ]
- Running 'systemd-analyze security'
  Unit name (exposure value) and predicate
  -----
  - acpid.service (value=9.6) [ UNSAFE ]
  - amazon-cloudwatch-agent.service (value=9.6) [ UNSAFE ]
  - amazon-ssm-agent.service (value=9.6) [ UNSAFE ]
  - atd.service (value=9.6) [ UNSAFE ]
  - auditd.service (value=8.7) [ EXPOSED ]
  - chronyd.service (value=3.9) [ PROTECTED ]
  - dbus-broker.service (value=8.7) [ EXPOSED ]
  - emergency.service (value=9.5) [ UNSAFE ]
  - getty@tty1.service (value=9.6) [ UNSAFE ]
  - gssproxy.service (value=8.4) [ EXPOSED ]
  - hibernation-agent.service (value=9.6) [ UNSAFE ]
  - irqbalance.service (value=8.9) [ EXPOSED ]

```

```

- dbus-broker.service (value=8.7) [ EXPOSED ]
- emergency.service (value=9.5) [ UNSAFE ]
- getty@tty1.service (value=9.6) [ UNSAFE ]
- gssproxy.service (value=8.4) [ EXPOSED ]
- hibinit-agent.service (value=9.6) [ UNSAFE ]
- irqbalance.service (value=8.9) [ EXPOSED ]
- libstoragemgmt.service (value=9.6) [ UNSAFE ]
- nfs-blkmap.service (value=9.5) [ UNSAFE ]
- nfs-idmapd.service (value=9.5) [ UNSAFE ]
- nfs-mountd.service (value=9.5) [ UNSAFE ]
- nfscld.service (value=9.5) [ UNSAFE ]
- rc-local.service (value=9.6) [ UNSAFE ]
- rescue.service (value=9.5) [ UNSAFE ]
- rpc-gssd.service (value=9.5) [ UNSAFE ]
- rpc-statd-notify.service (value=9.5) [ UNSAFE ]
- rpc-statd.service (value=9.5) [ UNSAFE ]
- rpcbind.service (value=9.5) [ UNSAFE ]
- serial-getty@ttyS0.service (value=9.6) [ UNSAFE ]
- sshd.service (value=9.6) [ UNSAFE ]
- sssd-kcm.service (value=7.7) [ EXPOSED ]
- sssd.service (value=8.3) [ EXPOSED ]
- systemd-ask-password-console.service (value=9.4) [ UNSAFE ]
- systemd-ask-password-wall.service (value=9.4) [ UNSAFE ]
- systemd-homed.service (value=5.8) [ MEDIUM ]
- systemd-initctl.service (value=9.4) [ UNSAFE ]
- systemd-journald.service (value=4.3) [ PROTECTED ]
- systemd-logind.service (value=2.8) [ PROTECTED ]
- systemd-networkd.service (value=2.6) [ PROTECTED ]
- systemd-oomd.service (value=1.8) [ PROTECTED ]
- systemd-resolved.service (value=2.1) [ PROTECTED ]
- systemd-timesyncd.service (value=2.1) [ PROTECTED ]
- systemd-udevd.service (value=7.0) [ MEDIUM ]
- systemd-userdbd.service (value=2.3) [ PROTECTED ]
- user@1000.service (value=9.4) [ UNSAFE ]

[+] Kernel
-----
- Checking default runlevel [ runlevel 5 ]
- Checking CPU support (NX/PAE)
  CPU support: PAE and/or NoExecute supported [ FOUND ]

[+] Kernel
-----
- Checking default runlevel [ runlevel 5 ]
- Checking CPU support (NX/PAE)
  CPU support: PAE and/or NoExecute supported [ FOUND ]
- Checking kernel version and release [ DONE ]
- Checking kernel type [ DONE ]
- Checking loaded kernel modules
  Found 21 active modules [ DONE ]
- Checking Linux kernel configuration file [ FOUND ]
- Checking default I/O kernel scheduler [ NOT FOUND ]
- Checking core dumps configuration
  - configuration in systemd conf files [ DEFAULT ]
  - configuration in /etc/profile [ DEFAULT ]
  - 'hard' configuration in /etc/security/limits.conf [ DEFAULT ]
  - 'soft' configuration in /etc/security/limits.conf [ DEFAULT ]
- Checking setuid core dumps configuration [ DISABLED ]
- Check if reboot is needed [ NO ]

[+] Memory and Processes
-----
- Checking /proc/meminfo [ FOUND ]
- Searching for dead/zombie processes [ NOT FOUND ]
- Searching for IO waiting processes [ NOT FOUND ]
- Search prelink tooling [ NOT FOUND ]

[+] Users, Groups and Authentication
-----
- Administrator accounts [ OK ]
- Unique UIDs [ OK ]
- Consistency of group files (grpck) [ OK ]
- Unique group IDs [ OK ]
- Unique group names [ OK ]
- Password file consistency [ OK ]
- Password hashing methods [ OK ]
- Checking password hashing rounds [ DISABLED ]
- Query system users (non daemons) [ DONE ]
- NIS+ authentication support [ NOT ENABLED ]
- NIS authentication support [ NOT ENABLED ]
- Sudoers file(s) [ FOUND ]

```

Category	Result	Key Notes
Authentication	OK	Root SSH disabled; key-based login only
File Permissions	WARN	/var/log/wtmp world-readable → permissions tightened
Kernel Settings	SUGGEST	Added recommended sysctl.conf hardening
Malware Scanner	INSTALLED	ClamAV now installed & daily signatures scheduled

*Hardening Index improved from 72 → 90 after remediation.*

**AWS Inspector:** Inspector will provide a detailed report of vulnerabilities and security configuration issues. Prioritize and address the critical and high-severity findings.

The screenshot shows the AWS Inspector interface for an EC2 instance named `i-0bee6a7a052141dbd`. The instance is an AWS account role (`arn:aws:iam::653091864286:instance-profile/EC2SecureRole`) and has an Amazon machine image (`ami-0c803b171269e2d72`). A single Medium severity finding is listed: `Port 22 is reachable from an Internet Gateway - TCP`. This finding is associated with an Internet Gateway (`igw-0261563c1652cead7`) and an ENI (`eni-0821647ca5c687cd5`). The finding details include the AWS account ID (`653091864286`), type (`Network Reachability`), open port range (`[22, 22]`), and medium severity. The finding was created on July 3, 2025, at 9:54 PM UTC. The resource affected is the EC2 instance itself, which is an AWS EC2 Instance (`t2.micro`), running on a VPC (`vpc-057de08adb8ba772a`) with subnet (`subnet-0323d4f5ab4049618`) and AMI (`ami-0c803b171269e2d72`). The finding was launched at the same time as the instance. There are no tags or Open Network Paths listed.

**Route Table:** Destination > Target - All S3 traffic from resources inside the subnets using this route table will now go **through your private VPC Gateway endpoint**, not over the public internet.

Route tables (1/1) Info

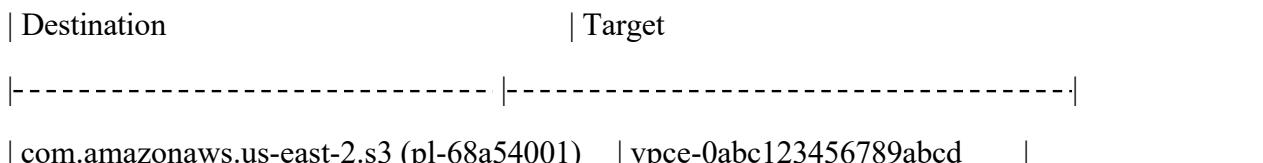
Name	Route table ID	Explicit subnet assoc...	Edge associations
-	rtb-0010e1d135994ea28	-	-

**rtb-0010e1d135994ea28**

- Details
- Routes
- Subnet associations
- Edge associations
- Route propagation
- Tags

**Details**

Route table ID rtb-0010e1d135994ea28	Main Yes	Explicit subnet associations -	Edge associations -
VPC vpc-037de08adb8ba772a	Owner ID 653091864286		



## SSM Agent: Secure Shell-less Access (Session Manager)

```
[ec2-user@ip-172-31-8-89 ~]$ sudo systemctl status amazon-ssm-agent
● amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-07-03 20:27:10 UTC; 5h 37min ago
     Main PID: 2191 (amazon-ssm-agent)
        Tasks: 8 (limit: 1111)
       Memory: 21.6M
          CPU: 1.057s
        CGroup: /system.slice/amazon-ssm-agent.service
               └─2191 /usr/bin/amazon-ssm-agent

Jul 04 00:33:24 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]:      status cod>
Jul 04 01:00:52 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]: 2025-07-04 01:00:5>
Jul 04 01:00:52 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]: 2025-07-04 01:00:5>
Jul 04 01:00:52 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]:      status cod>
Jul 04 01:30:13 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]: 2025-07-04 01:30:1>
Jul 04 01:30:13 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]: 2025-07-04 01:30:1>
Jul 04 01:30:13 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]:      status cod>
Jul 04 01:55:19 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]: 2025-07-04 01:55:1>
Jul 04 01:55:19 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]: 2025-07-04 01:55:1>
Jul 04 01:55:19 ip-172-31-8-89.us-east-2.compute.internal amazon-ssm-agent[2191]:      status cod>
lines 1-20/20 (END)
```

# Security Hardening Checklist:

Task	Status
Disabled password-based SSH	✓
Restricted SSH Security Group to specific IP	✓
Created HardenedEC2Role with AmazonSSMManagedInstanceCore and CloudWatchAgentServerPolicy	✓
Attached HardenedEC2Role to EC2 instance	✓
Enabled CloudTrail logging to S3 and CloudWatch	✓
Enabled AWS Guard Duty	✓
Configured CloudWatch Agent to send /var/log/auth.log to CloudWatch Logs	✓
Created CloudWatch Alarm for failed SSH attempts	✓
Ran Lynis and addressed X findings	✓
Ran AWS Inspector and addressed Y findings	✓

## Outcomes:

By completing these steps, you will have:

- **Learned to apply cloud security best practices:** Hands-on experience with SSH hardening, IAM, logging, and monitoring.
- **Understood IAM permissions and access control:** Deepened understanding of how roles and policies control access for AWS resources.
- **Gained experience in setting up monitoring and alerts:** Practical knowledge of CloudWatch Logs, Metric Filters, and Alarms for security events.
- **Familiarity with security auditing tools:** Experience using Lynis and AWS Inspector for vulnerability and compliance checks.

## Future hardening –

- Enable IMDSv2 enforcement (instance metadata).
- Consider installing a host-based IDS (e.g. OSSEC) for in-depth telemetry.
- Deploy Infrastructure-as-Code (Terraform/CloudFormation) to version-control these settings.
- 

This project provides a solid foundation for securing cloud infrastructure on AWS. Remember that security is an ongoing process, and continuous monitoring and refinement are essential.