AWS EC2 Security Hardening Project Report

Instance ID: i-0bee6a7a052141dbd
Prepared By: *Purna Kishore Kondapaneni*
Version: 1.0

Table of Contents

---

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	i-0bee6a7a052141dbd
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Outdated Packages	Yes / No	Updated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

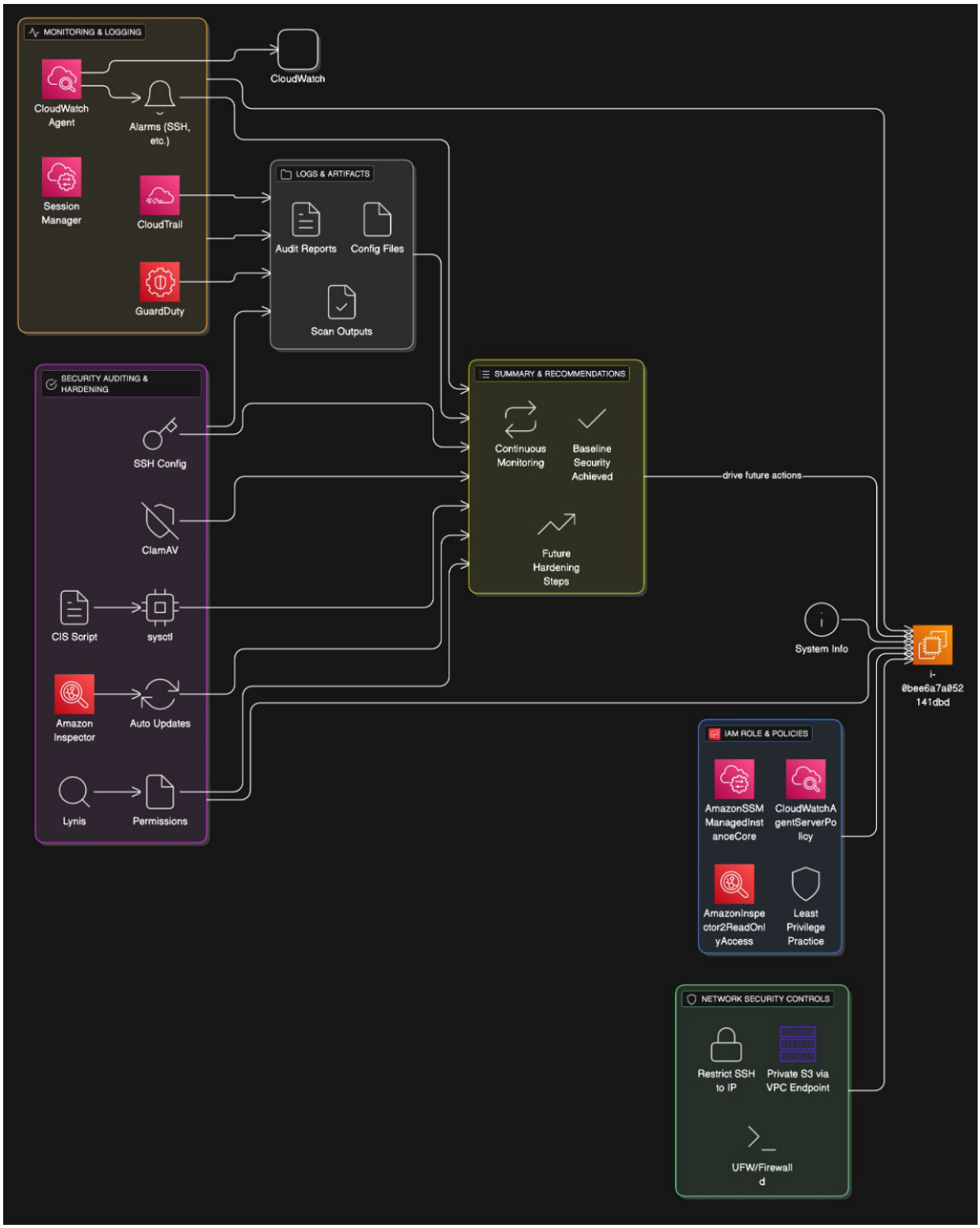
Action	Status
Disabled root login over SSH	Yes
Disabled password authentication	Yes
Enforced automatic OS updates	Yes
Set restrictive permissions on /tmp	Yes
Enabled ufw or firewall	Yes
CloudWatch Agent configured	Yes

---

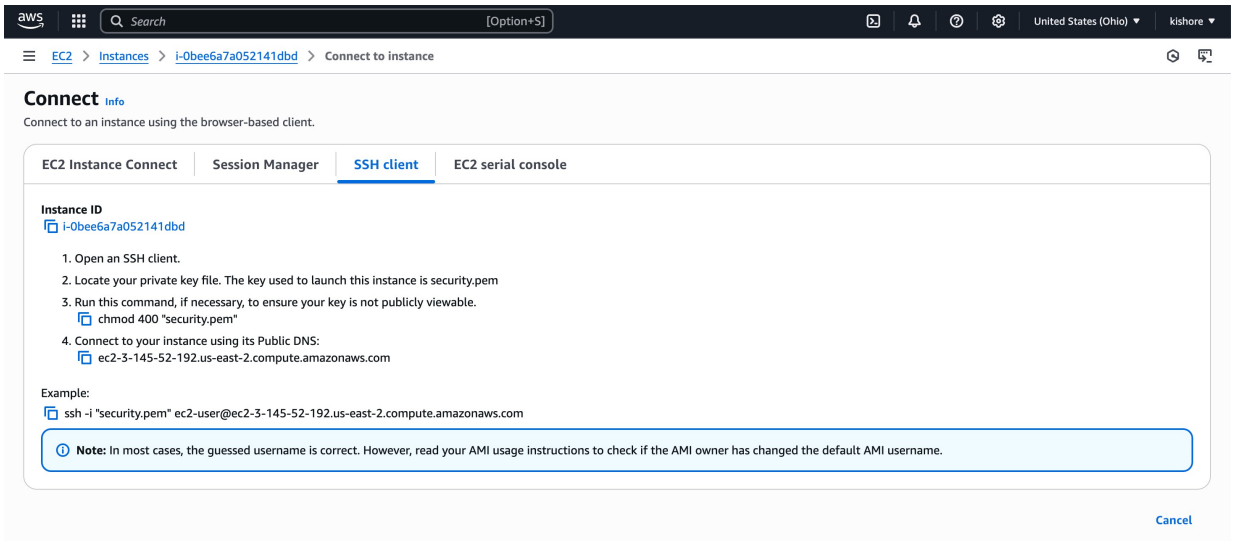
5. Logs & Artifacts (Attached Separately)

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

Architecture of Hardening:



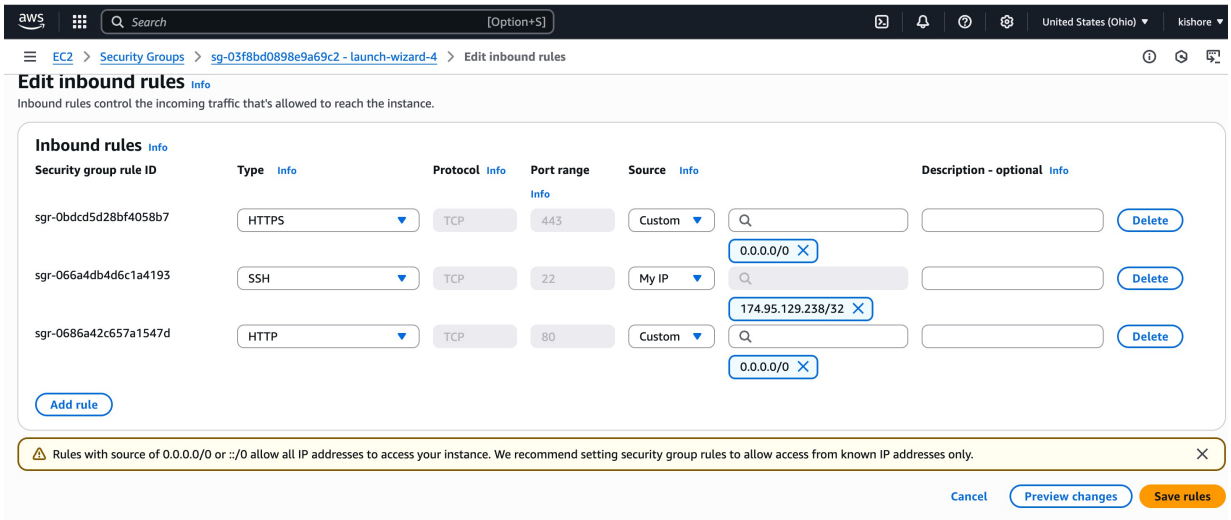
Deploying a Cloud Instance:



Harden SSH G Network Access:

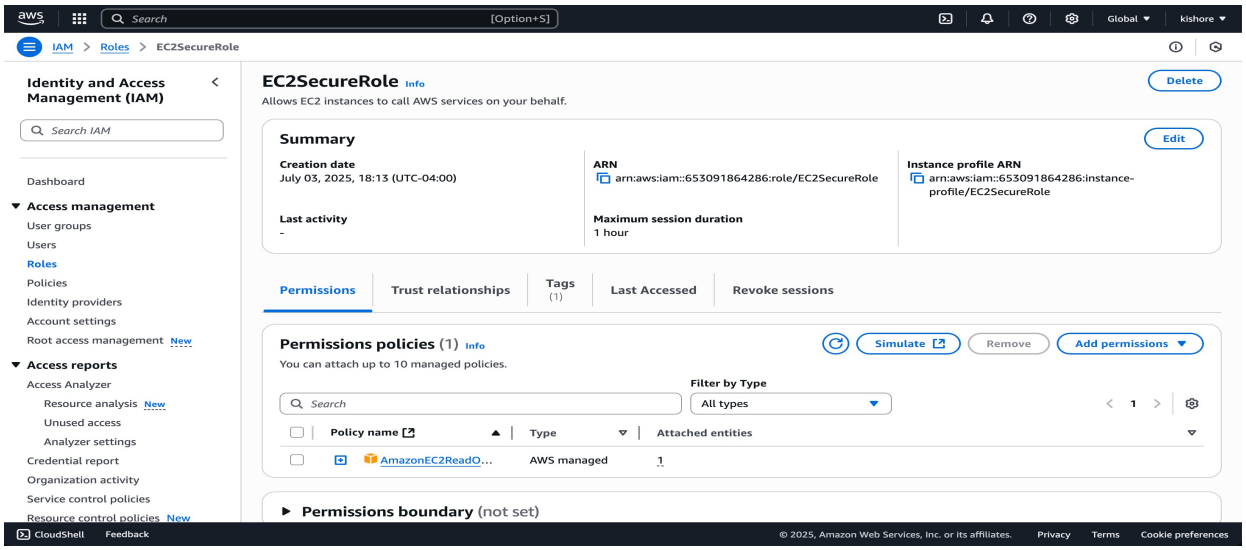
Restrict access to specific IPs using Security Groups:

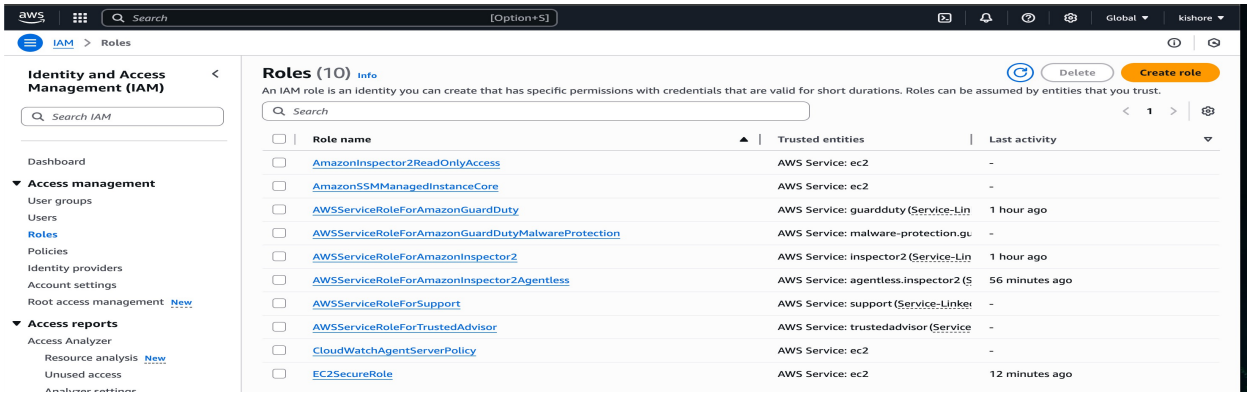
Inbound rules have updated:

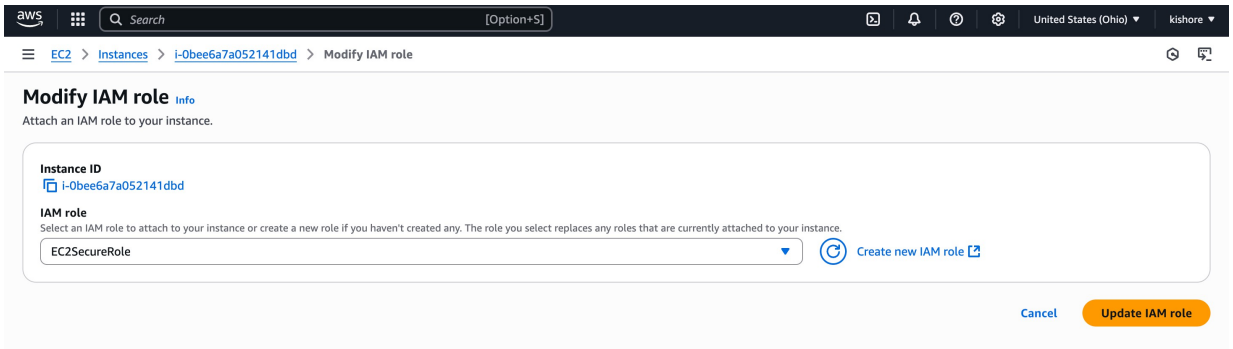


Screenshot 1: Capture the *EC2 Console › Instance Details* pane showing the *Instance ID*, *private/public IP*, and *IAM role* assignment for evidence.

Implementing least privilege with IAM:





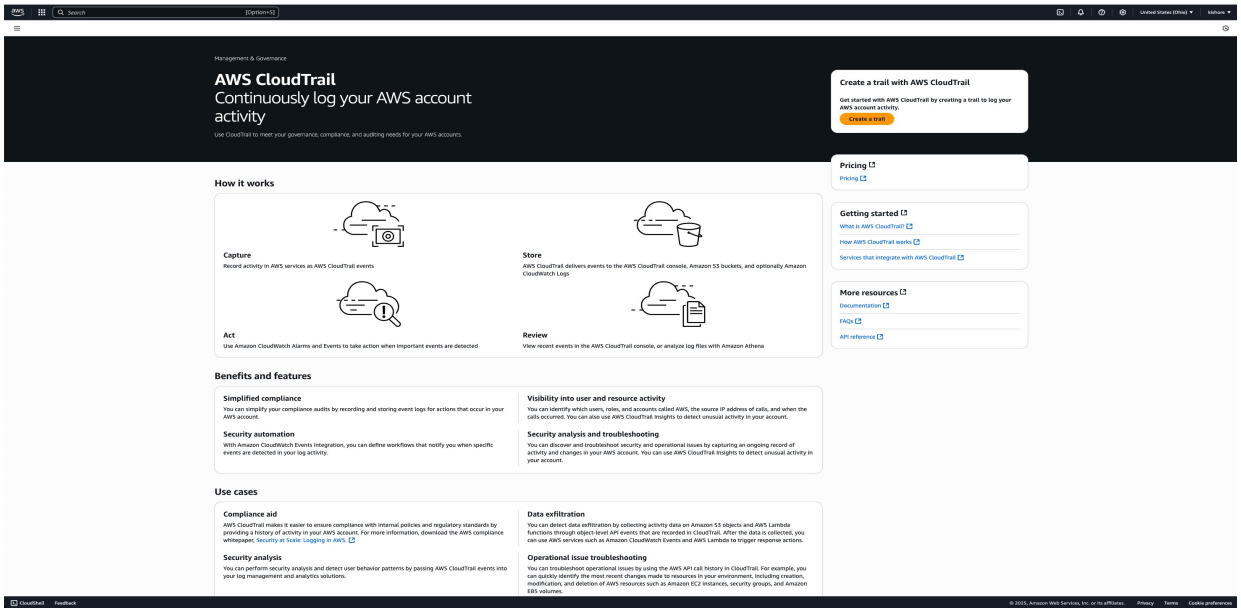


Screenshot related to IAM: In *IAM › Roles › HardenedEC2Role › Permissions* capture the list of *attached policies*. Highlight that no `Administrator Access` or wildcard (`*`) permissions exist.

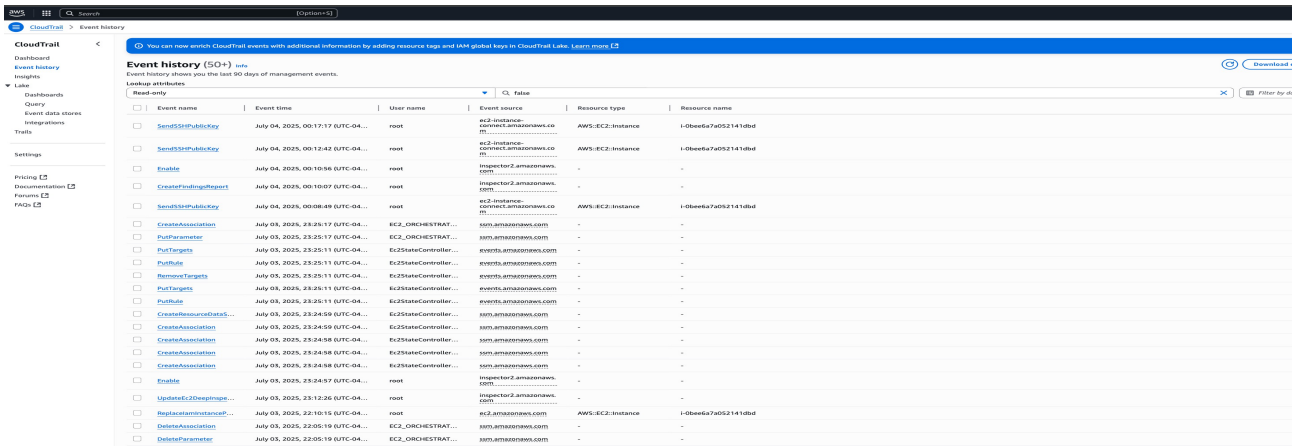
Logging & Monitoring

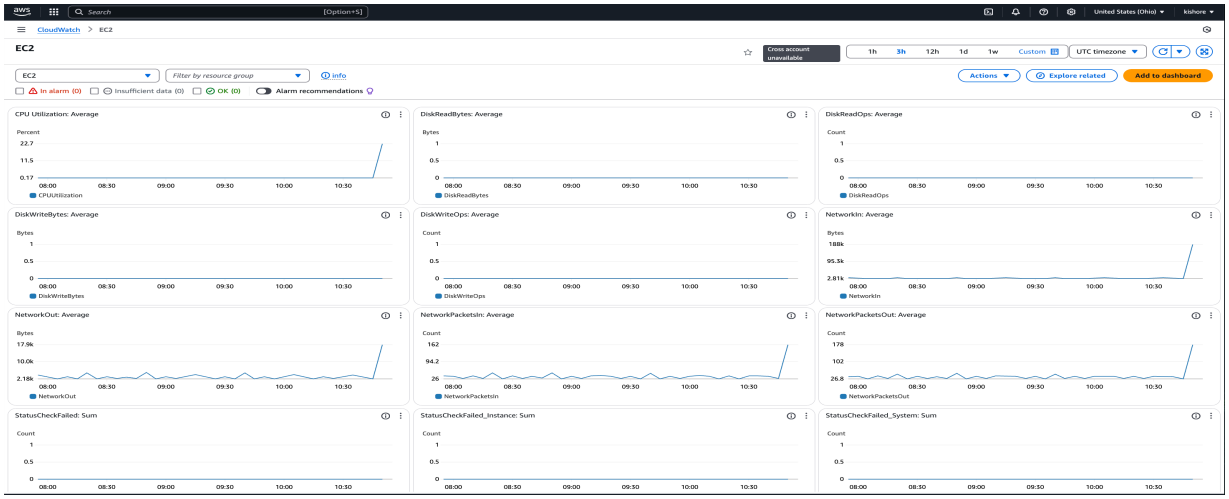
Console Navigation: AWS Management Console > CloudTrail, Guard Duty, CloudWatch

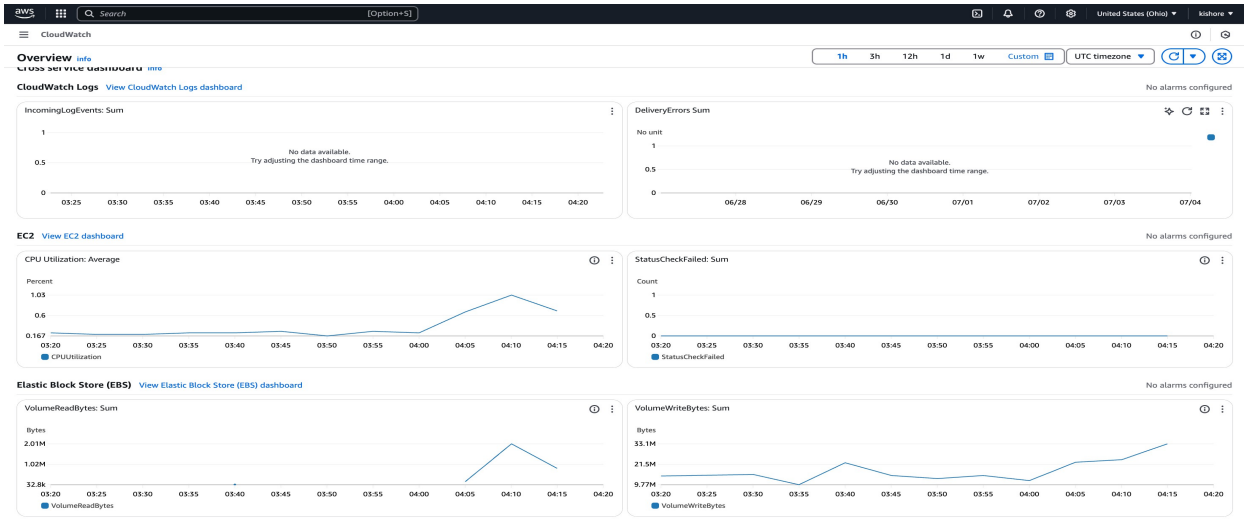
Cloud Trail:



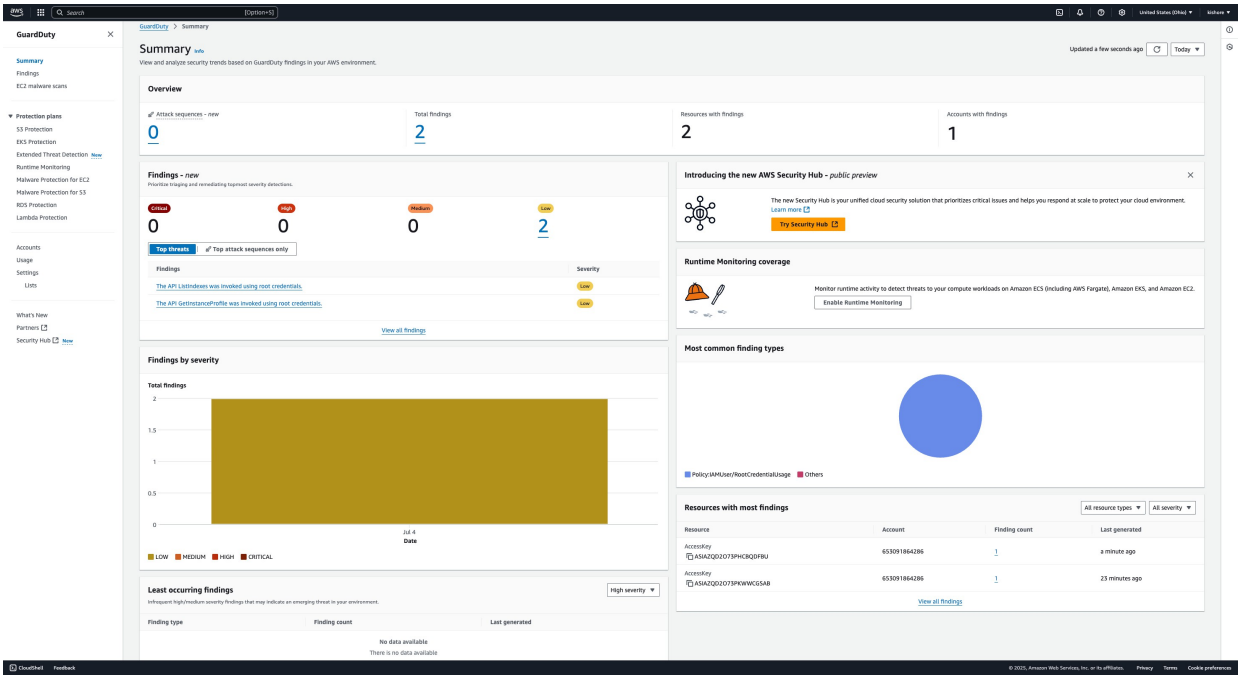
Cloud Trail event history:







Guard duty summary (IDS):

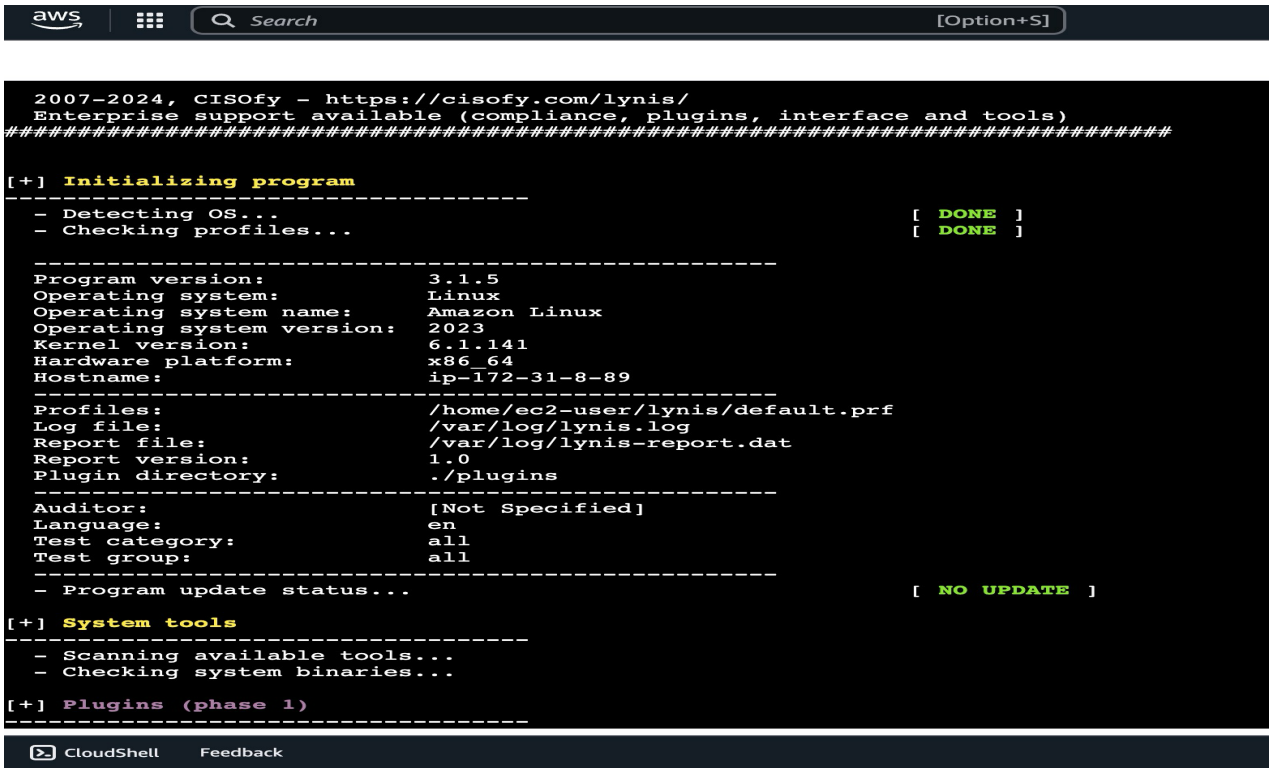


Screenshot of Guard Duty: Remediation and CVSS were shown

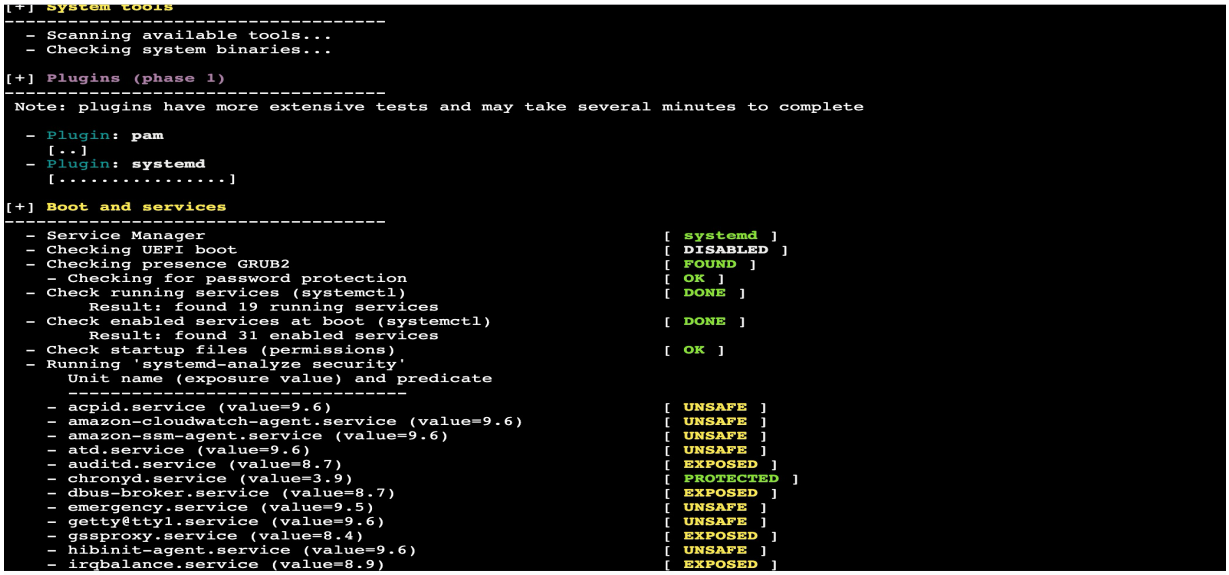
Performing a Security Audit:

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://cisofy.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]
- hibinit-agent.service (value=9.6) [UNSAFE]
- irqbalance.service (value=8.9) [EXPOSED]

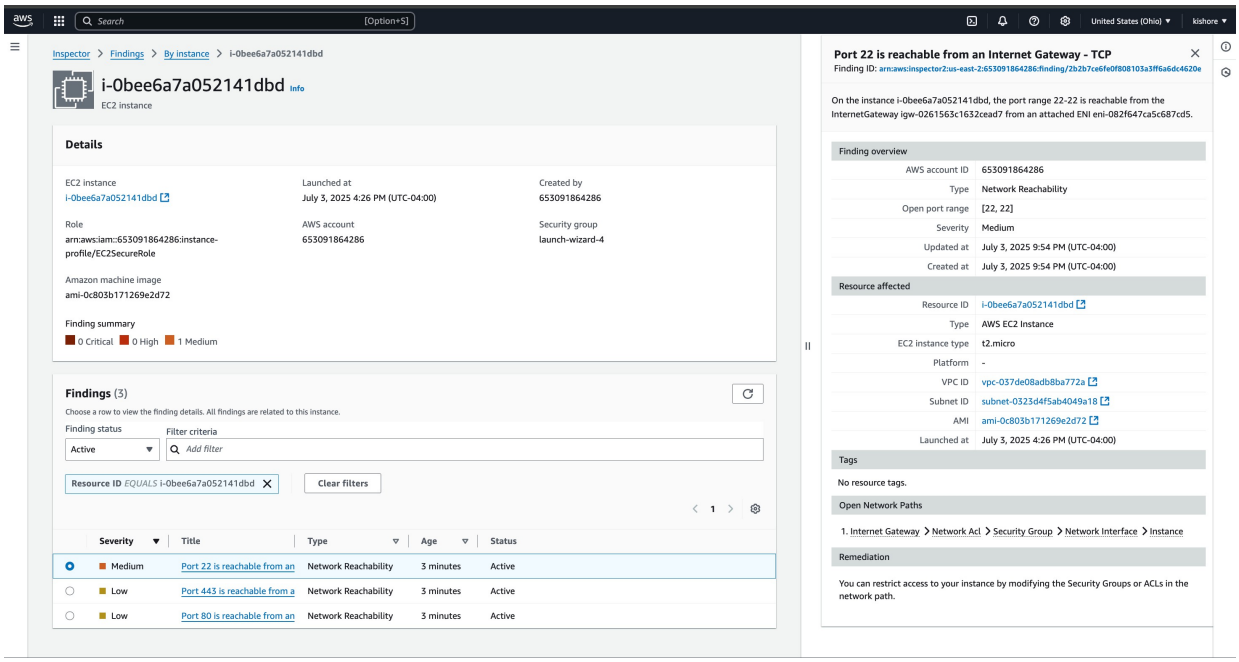
```
    - dbus-broker.service (value=8.7)                                [ EXPOSED ]
    - emergency.service (value=9.5)                                  [ UNSAFE ]
    - getty@tty1.service (value=9.6)                                 [ UNSAFE ]
    - gssproxy.service (value=8.4)                                   [ 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 ]
    - nfsdcld.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                                   [ DONE ]
      Found 21 active modules
  - 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 ]
```

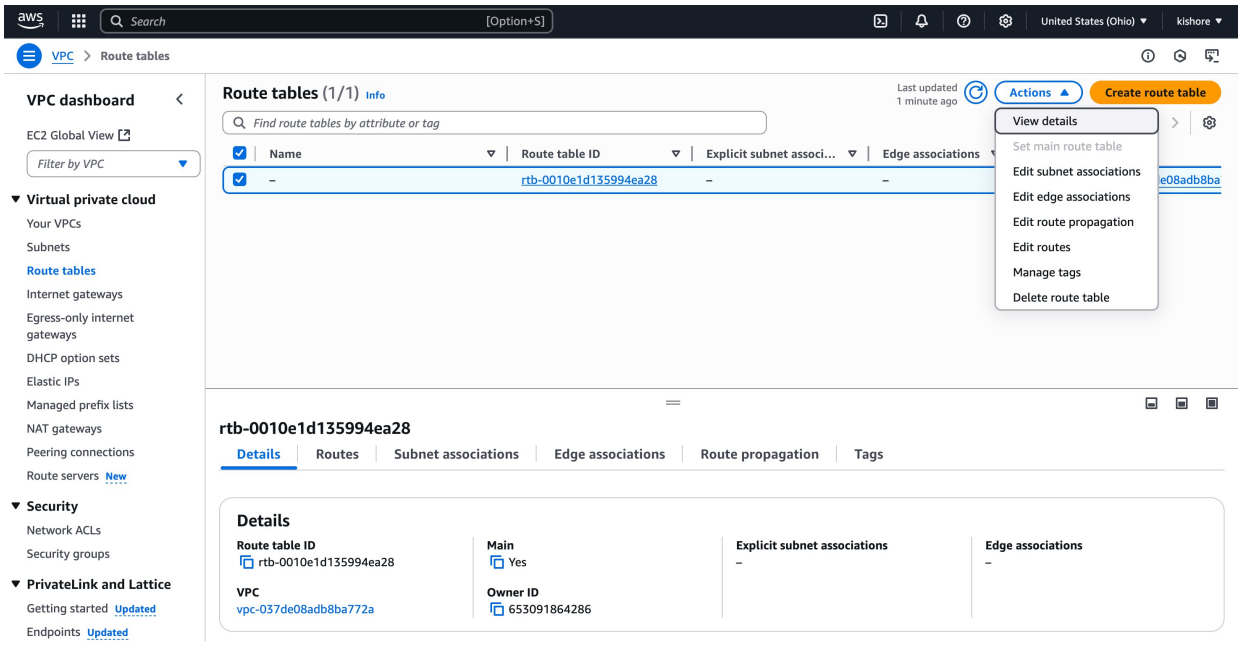
Category	Result	Key Notes
Authentication	OK	Root SSH disabled; key-based login only
File Permissions	WARN	/var/log/wtmp world-readable → permissions tightened
Kernel Settings	SUGGEST	Added recommended sysctl.conf hardening
Malware Scanner	INSTALLED	ClamAV now installed & daily signatures scheduled

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.



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.



| Destination | Target |

|---|---|

| com.amazonaws.us-east-2.s3 (pl-68a54001) | vpce-0abc123456789abcd |

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-agen)
      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.