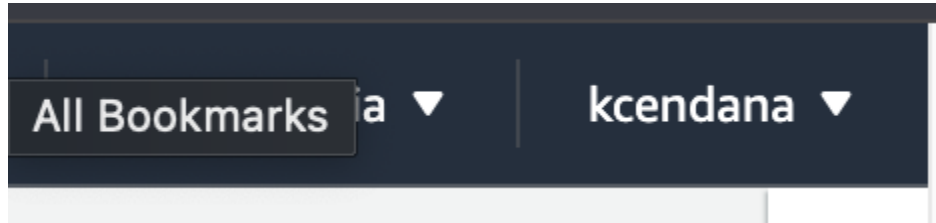


Task 1

1) I already had an AWS account, so I just logged into my existing one.



2) Set up Multi-Factor Authentication (MFA) for the root user by choosing an authenticator app and scanning a QR code to link my account for additional security.

Sign in

☒ **Root user**

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**

User within an account that performs daily tasks. [Learn more](#)

Root user email address

kevincendana@outlook.com

Next



N. California ▼

kcendana ▲

Account ID: 9876-4370-2368 

Account

Organization

Service Quotas

Billing and Cost Management

Security credentials

Sign out

Step 1 of 2

Select MFA device [Info](#)

MFA device name

Device name

Enter a meaningful name to identify this device.

Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.



Authenticator app

Authenticate using a code generated by an app installed on your mobile device or computer.

Step 2 of 2

Set up device [Info](#)

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1



Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#) [↗](#)



Open your authenticator app, choose **Show QR code** on this page,

My security credentials

 **MFA device assigned** 

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

Account details

Edit account name, email, and password

Account name

kcendana

Email address

kevincendana@outlook.com

AWS account ID

3) Created an IAM administrator user to avoid using the root user for everyday tasks. Configured the user with administrative privileges and set up MFA for this account as well.

User details

User name

kevin

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☒ **Provide user access to the AWS Management Console - *optional***

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.



Are you providing console access to a person?

User type

☐ **Specify a user in Identity Center - Recommended**

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ **I want to create an IAM user**

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☐ **Autogenerated password**

You can view the password after you create the user.

☒ **Custom password**

Enter a custom password for the user.

.....

☐ Show password

☒ **Users must create a new password at next sign-in - Recommended**

Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.



If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details


User name
kevin

Console password type
Custom password

Require password reset
Yes

Permissions summary

< 1 >

Name 	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.


Console sign-in details

Email sign-in instructions 

Console sign-in URL

 <https://987643702368.signin.aws.amazon.com/console>

User name

 kevin

Console password

Users (2) [Info](#)

[Delete](#)[Create user](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

[< 1 >](#) [Settings](#)

<input type="checkbox"/>	User name ▲	Path ▼	Group: ▼	Last activity ▼	MFA ▼	Permissions ▼
<input type="checkbox"/>	kcendana	/	0	⚠ 184 days ago	-	-
<input type="checkbox"/>	kevin	/	0	✅ 4 minutes ago	-	✅

Select MFA device [Info](#)

MFA device name

Device name

Enter a meaningful name to identify this device.

Maximum 64 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.







Authenticator app

Authenticate using a code generated by an app installed on your mobile device or computer.

Task 2

- 1) Logged in with new AWS account (not the root user). Created a new IAM user named "auditor" with limited permissions for security auditing purposes, ensuring it has access to AWS services in a read-only and secure audit capacity.

[Option+S]




Global ▾

kevin @ 9876-4370-2368 ▾

[IAM](#) > Users

▼ Ready to streamline human access to AWS and cloud apps?




Dismiss

Manage workforce users 


Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.


[Learn more !\[\]\(9b8c673b0d75e72caabf3ca9944ef845_img.jpg\)](#) | [Watch how it works !\[\]\(18f23ec37a471f851e2e8a40dc8f10ea_img.jpg\)](#)




Users (2) [Info](#)



An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

 Search

< 1 > 

<input type="checkbox"/>	User name ▲	Path ▼	Group: ▼	Last activity ▼	MFA ▼	Pe
<input type="checkbox"/>	kcendana	/	0	 184 days ago	-	-
<input type="checkbox"/>	kevin	/	0	 1 minute ago	Virtual	

User details


User name

auditor

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

 If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel

Next

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name

auditor

Console password type

None

Require password reset

No

Permissions summary

< 1 >

Name 



Type



Used a

[ReadOnlyAccess](#)

AWS managed - job function

Permis

[SecurityAudit](#)

AWS managed - job function

Permis

Users (3) Info

Delete

Create user

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

< 1 >

<input type="checkbox"/>	User name ▲	Path ▼
<input type="checkbox"/>	auditor	/
<input type="checkbox"/>	kcendana	/
<input type="checkbox"/>	kevin	/

Use case

Command Line Interface (CLI)

You plan to use this access key to enable the AWS CLI to access your AWS account.

2) Installed and configured AWS CLI on my Ubuntu VM, updating the system first, then installing the CLI tool, and finally configuring it with the "auditor" profile.

```
update-alternatives: using /usr/bin/montage-im6.q16 to provide /usr/bin/montage-  
im6 (montage-im6) in auto mode  
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify  
(mogrify) in auto mode  
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify-  
im6 (mogrify-im6) in auto mode  
Setting up imagemagick (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.3) ...  
Processing triggers for man-db (2.10.2-1) ...  
Processing triggers for shared-mime-info (2.1-2) ...  
Processing triggers for sgml-base (1.30) ...  
Setting up python3-docutils (0.17.1+dfsg-2) ...  
Processing triggers for install-info (6.8-4build1) ...  
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...  
Processing triggers for fontconfig (2.13.1-4.2ubuntu5) ...  
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...  
Processing triggers for hicolor-icon-theme (0.17-2) ...  
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...  
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...  
Setting up awscli (1.22.34-1) ...  
kevin@ubuntu:~$
```

```
Setting up imagemagick (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.3) ...  
Processing triggers for man-db (2.10.2-1) ...  
Processing triggers for shared-mime-info (2.1-2) ...  
Processing triggers for sgml-base (1.30) ...  
Setting up python3-docutils (0.17.1+dfsg-2) ...  
Processing triggers for install-info (6.8-4build1) ...  
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...  
Processing triggers for fontconfig (2.13.1-4.2ubuntu5) ...  
Processing triggers for desktop-file-utils (0.26-1ubuntu3) ...  
Processing triggers for hicolor-icon-theme (0.17-2) ...  
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...  
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...  
Setting up awscli (1.22.34-1) ...  
kevin@ubuntu:~$ aws --version  
aws-cli/1.22.34 Python/3.10.12 Linux/6.5.0-15-generic botocore/1.23.34  
kevin@ubuntu:~$ aws configure --profile auditor  
AWS Access Key ID [None]: dDV4V79gh2t+86nRKIvBlyIRO5JXm5kvwAagGLYW  
AWS Secret Access Key [None]: ^C  
kevin@ubuntu:~$ aws configure --profile auditor  
AWS Access Key ID [None]: AKIA6L5BG5RQJN5LEPXP  
AWS Secret Access Key [None]: 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  
[Help] t region name [None]: us-west-1  
t output format [None]: json  
kevin@ubuntu:~$
```

3) Set up and ran ScoutSuite in a Python virtual environment to scan my AWS environment for security misconfigurations, then reviewed the generated HTML report for vulnerabilities.

```
Selecting previously unselected package python3-platformdirs.  
Preparing to unpack .../3-python3-platformdirs_2.5.1-1_all.deb ...  
Unpacking python3-platformdirs (2.5.1-1) ...  
Selecting previously unselected package python3-setuptools-whl.  
Preparing to unpack .../4-python3-setuptools-whl_59.6.0-1.2ubuntu0.22.04.1_all.d  
eb ...  
Unpacking python3-setuptools-whl (59.6.0-1.2ubuntu0.22.04.1) ...  
Selecting previously unselected package python3-wheel-whl.  
Preparing to unpack .../5-python3-wheel-whl_0.37.1-2ubuntu0.22.04.1_all.deb ...  
Unpacking python3-wheel-whl (0.37.1-2ubuntu0.22.04.1) ...  
Selecting previously unselected package python3-virtualenv.  
Preparing to unpack .../6-python3-virtualenv_20.13.0+ds-2_all.deb ...  
Unpacking python3-virtualenv (20.13.0+ds-2) ...  
Setting up python3-setuptools-whl (59.6.0-1.2ubuntu0.22.04.1) ...  
Setting up python3-filelock (3.6.0-1) ...  
Setting up python3-pip-whl (22.0.2+dfsg-1ubuntu0.4) ...  
Setting up python3-distlib (0.3.4-1) ...  
Setting up python3-platformdirs (2.5.1-1) ...  
Setting up python3-wheel-whl (0.37.1-2ubuntu0.22.04.1) ...  
Setting up python3-virtualenv (20.13.0+ds-2) ...  
Processing triggers for man-db (2.10.2-1) ...  
kevin@ubuntu:~$
```

```
kevin@ubuntu: ~  
1.20231109 portalocker-2.8.2 portend-3.2.0 proto-plus-1.23.0 protobuf-3.20.3 pyO  
penSSL-24.1.0 pyasn1-0.6.0 pyasn1-modules-0.4.0 pycparser-2.22 pycryptodome-3.20  
.0 pyparsing-3.1.2 python-dateutil-2.8.0 pytz-2024.1 pyyaml-6.0.1 requests-2.31.  
0 requests-oauthlib-2.0.0 rsa-4.9 s3transfer-0.10.1 scoutsuite-5.13.0 six-1.16.0  
sqlitedict-2.1.0 tempora-5.5.1 typeguard-4.2.1 typing-extensions-4.11.0 uritemp  
late-4.1.1 urllib3-2.2.1 websocket-client-1.8.0 zc.lockfile-3.0.post1  
usage: scout [-h] [-v] {aws,gcp,azure,aliyun,oci,kubernetes} ...  
  
options:  
  -h, --help            show this help message and exit  
  -v, --version          show program's version number and exit  
  
The provider you want to run scout against:  
{aws,gcp,azure,aliyun,oci,kubernetes}  
  aws                  Run Scout against an Amazon Web Services account  
  gcp                  Run Scout against a Google Cloud Platform account  
  azure                Run Scout against a Microsoft Azure account  
  aliyun               Run Scout against an Alibaba Cloud account  
  oci                  Run Scout against an Oracle Cloud Infrastructure  
                      account  
  kubernetes           Run Scout against a Kubernetes cluster  
  
To get additional help on a specific provider run: scout.py {provider} -h  
(venv) kevin@ubuntu:~$
```


ce

2024-05-03 22:40:20 ubuntu scout[6868] INFO Fetching resources for the IAM service

2024-05-03 22:40:20 ubuntu scout[6868] INFO Fetching resources for the KMS service

2024-05-03 22:40:21 ubuntu scout[6868] INFO Fetching resources for the RDS service

2024-05-03 22:40:21 ubuntu scout[6868] INFO Fetching resources for the RedShift service

2024-05-03 22:40:22 ubuntu scout[6868] INFO Fetching resources for the Route53 service

2024-05-03 22:40:22 ubuntu scout[6868] INFO Fetching resources for the S3 service

2024-05-03 22:40:30 ubuntu scout[6868] INFO Fetching resources for the SES service

2024-05-03 22:40:30 ubuntu scout[6868] INFO Fetching resources for the SNS service

2024-05-03 22:40:31 ubuntu scout[6868] INFO Fetching resources for the SQS service

2024-05-03 22:40:31 ubuntu scout[6868] INFO Fetching resources for the VPC service

2024-05-03 22:40:32 ubuntu scout[6868] INFO Fetching resources for the Secrets Manager service

The screenshot shows the Scout Suite AWS Auditor interface. The top navigation bar includes the Scout logo and various category dropdowns: Analytics, Compute, Containers, Database, Management, Messaging, Network, Security, Storage, and Filters. Below the navigation bar, the page title is "Amazon Web Services > 987643702368". A "Dashboard" tab is selected. The main content is a table with the following columns: Service, Resources, Rules, Findings, and Checks. The table lists various AWS services with their respective counts. Notable findings are highlighted with red exclamation marks for CloudTrail, Config, and EC2.

Service	Resources	Rules	Findings	Checks
ACM	0	2	0	0
Lambda	0	0	0	0
CloudFormation	0	1	0	0
CloudFront	0	3	0	0
CloudTrail	0	9	17	17
CloudWatch	0	1	0	0
Codebuild	0	0	0	0
Config	0	1	17	17
Directconnect	0	0	0	0
DynamoDB	0	0	0	0
EC2	26	28	73	662
EFS	0	0	0	0
ElastiCache	0	0	0	0
ELB	0	3	0	0

4) Analyzed a specific vulnerability identified by ScoutSuite, here is the documentation of its impact and the steps needed for remediation.

1) Description of the Vulnerable AWS Service:

EC2 Dashboard -> "EB5 Volume Not Encrypted"

EBS volumes are storage devices for EC2 instances. Basically, the data on these storage devices aren't protected by encryption.

2) How is security impacted by the vulnerability/misconfiguration:

Without encryption, data stored on the EBS volume could be intercepted or accessed by unauthorized parties, which could lead to data breaches or compliance violations.

3) How can the service be fixed (what steps are needed):

Searching the internet gave these results:







- EC2 Dashboard -> Volumes Section in Elastic Block Store category
- Identify the non encrypted EBS volume
- Select with Actions->Modify Volume
- Check "Encrypt" and follow prompts

But this didn't work (I couldn't encrypt an existing one) so I made another:

▼ Elastic Block Store

Volumes

Volume ID: vol-04e4de1459293796f =

<div>Volume ID</div> <div> vol-04e4de1459293796f</div>	<div>Size</div> <div> 8 GiB</div>	<div>Type</div> <div>gp3</div>
<div>AWS Compute Optimizer finding</div> <div> Opt-in to AWS Compute Optimizer for recommendations. Learn more </div>	<div>Volume state</div> <div> In-use</div>	<div>IOPS</div> <div>3000</div>
<div>Encryption</div> <div>Not encrypted</div>	<div>KMS key ID</div> <div>-</div>	<div>KMS key alias</div> <div>-</div>
<div><div>vol-04e4de1459293796f</div><div></div><div>Actions ▼</div><div>Delete</div><div>Modify</div></div>		

No option to encrypt an existing one, but making another allows encryption.

Modify volume [Info](#)

Modify the type, size, and performance of an EBS volume.

Volume details

Volume ID

 `vol-04e4de1459293796f`

Volume type [Info](#)

General Purpose SSD (gp3) ▼

Size (GiB) [Info](#)

8 ▼

Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS [Info](#)

3000

Min: 3000 IOPS, Max: 16000 IOPS. The value must be an integer.

Throughput (MiB/s) [Info](#)

125

Min: 125 MiB, Max: 1000 MiB. Baseline: 125 MiB/s.

Cancel

Modify

Size (GiB) | [Info](#)

Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS | [Info](#)

Min: 3000 IOPS, Max: 16000 IOPS. The value must be an integer.

Throughput (MiB/s) | [Info](#)

Min: 125 MiB, Max: 1000 MiB. Baseline: 125 MiB/s.

Availability Zone | [Info](#)

Snapshot ID - *optional* | [Info](#)



Encryption | [Info](#)

Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.



Encrypt this volume