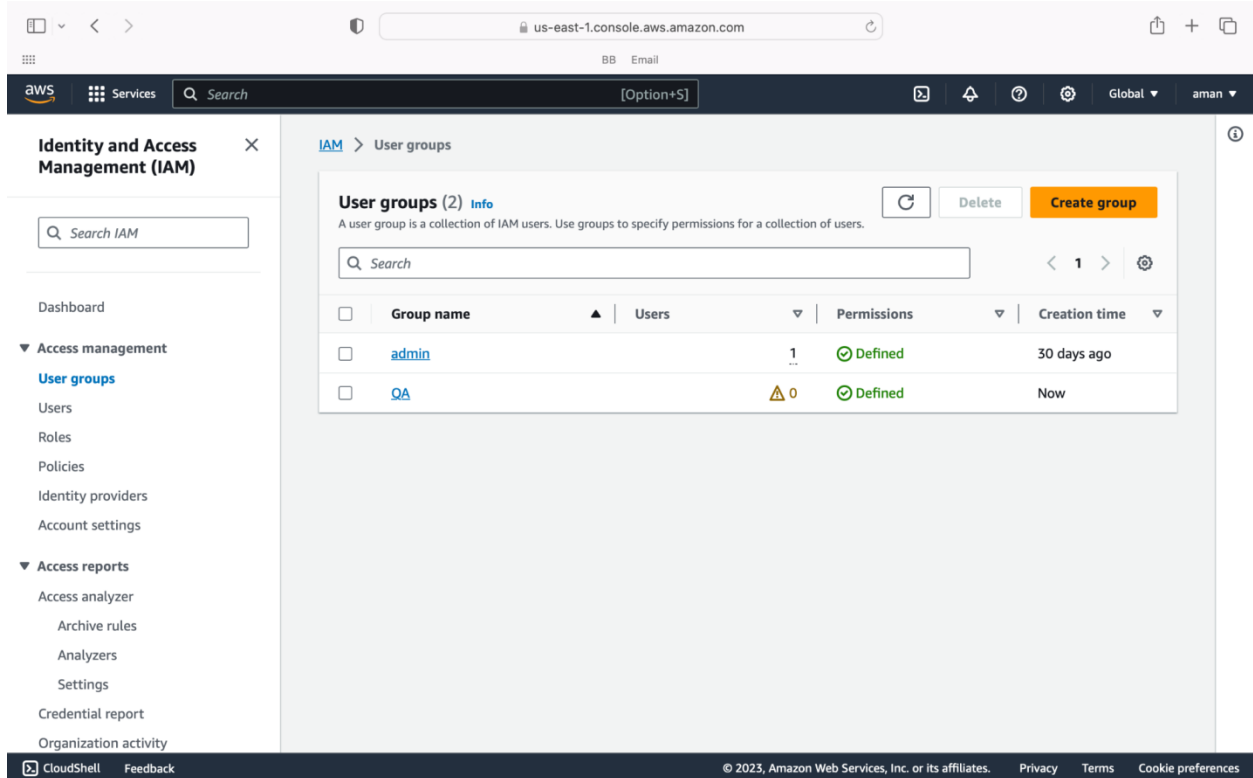


Identity and Access Management

Follow the steps in Section 13 'Security Best Practices', section 'Identity and Access Management', to create a group, create users, and assign the users to a group. Submit a screenshot of step 3, with the new group visible.



Follow the steps to attach a policy to the group. Submit a screenshot of step 2, with the selected policy visible.

The screenshot shows the AWS IAM console for the 'QA' user group. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Organization activity. The main content area shows the 'QA' user group details, including its name, creation time, and ARN. The 'Permissions policies' tab is selected, displaying a table with one policy: 'AmazonEC2FullAccess' (AWS managed) attached to the group.

Policy name	Type	Attached entities
AmazonEC2FullAccess	AWS managed	1

Follow the steps to create the Developers Group. Submit a screenshot of step 5, with the two groups visible.

The screenshot shows the AWS IAM console for the 'User groups' list. A green notification banner at the top states 'Developers user group created.' The main content area shows the 'User groups (3)' list, including a search bar and a table with columns for Group name, Users, Permissions, and Creation time. The table lists three groups: 'admin', 'Developers', and 'QA'.

Group name	Users	Permissions	Creation time
admin	1	Defined	30 days ago
Developers	0	Defined	Now
QA	0	Defined	1 minute ago

Follow the steps to create a user, and add the user to the Developers Group. Submit a screenshot of step 4 in which the user was successfully created.

The screenshot shows the AWS IAM console for a user named 'dev-user'. The user's ARN is 'arn:aws:iam::692215778807:user/dev-user', created on October 27, 2023, at 14:07 UTC-04:00. The console access is 'Enabled without MFA'. The user is a member of the 'Developers' group, which has the 'AmazonEC2FullAccess' policy attached. The 'Summary' tab is selected, showing the user's details and group membership.

Summary

ARN arn:aws:iam::692215778807:user/dev-user	Console access Enabled without MFA	Access key 1 Create access key
Created October 27, 2023, 14:07 (UTC-04:00)	Last console sign-in Never	

User groups membership (1)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

Group name	Attached policies
Developers	AmazonEC2FullAccess

Follow the steps to delete the root access keys. Submit a screenshot of step 4 in which the security status verifies the root access keys were deleted.

The screenshot shows the AWS IAM Dashboard in the us-east-1 console. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Account settings. The main content area displays the 'IAM Dashboard' with a 'Security recommendations' section showing one recommendation to 'Add MFA for root user'. Below this is the 'IAM resources' section, which lists the following counts: 3 User groups, 2 Users, 17 Roles, 1 Policies, and 0 Identity providers. A 'What's new' section at the bottom indicates updates for features in IAM.

Resource Type	Count
User groups	3
Users	2
Roles	17
Policies	1
Identity providers	0

Follow the steps to apply an IAM password policy. Submit a screenshot of step 5 in which it verifies a password policy has been successfully set.

The screenshot shows the 'Password policy' page in the AWS IAM console. A green notification banner at the top states 'Password requirements for IAM users are updated.' The page title is 'Password policy' with an 'Info' link and an 'Edit' button. The main content area describes the current custom password policy for the AWS account, listing the following requirements:

- Password minimum length:** 8 characters
- Password strength:**
 - Require at least one uppercase letter from the Latin alphabet (A-Z)
 - Require at least one lowercase letter from the Latin alphabet (a-z)
 - Require at least one number
 - Require at least one non-alphanumeric character
- Other requirements:**
 - Never expire password
 - Allow users to change their own password

Below the password policy section, the 'Security Token Service (STS)' section is visible, explaining that STS is used to create and provide trusted users with temporary security credentials.

Follow the steps to enable MFA, and try out a virtual MFA Device. Submit a screenshot of step 3, in which the IAM dashboard displays Security Status 5 out of 5.

The screenshot shows the AWS IAM console interface. At the top, a green notification banner states "MFA device assigned" with a checkmark icon. Below this, the "Multi-factor authentication (MFA) (2)" section is visible, indicating that two MFA devices are assigned. A table lists these devices:

	Device type	Identifier	Certifications	Created on
<input type="radio"/>	Virtual	arn:aws:iam::692215778807:mfa/dev-2	Not Applicable	Now
<input type="radio"/>	Virtual	arn:aws:iam::692215778807:mfa/device-1	Not Applicable	14 minutes ago

Below the MFA section, the "Access keys (0)" section is shown, indicating no access keys are currently assigned. The left sidebar contains navigation links for "Identity and Access Management (IAM)", "Access management", "Access reports", and "Organization activity". The bottom of the console shows the footer with copyright information and links for Privacy, Terms, and Cookie preferences.

IAM Policies

Follow the steps to create a policy related to S3. Submit a screenshot of step 9, displaying that the policy has been successfully created.

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and CloudShell. The main content area is titled 'policy' and shows details for a policy named 'securityLAKE'. The policy details include Type (Customer managed), Creation time (October 27, 2023, 14:51 UTC-04:00), Edited time (October 27, 2023, 14:51 UTC-04:00), and ARN (arn:aws:iam::6922157788:07:policy/policy). The 'Permissions' tab is selected, showing 'Permissions defined in this policy' and a table of explicit deny services.

Service	Access level	Resource	Request condition
EC2	Full access	All resources	None

Follow the steps to create a user and assign a policy to it. Submit a screenshot of step 8 in which the user successfully creates a bucket.

The screenshot shows the AWS S3 console interface. A green banner at the top indicates 'Successfully created bucket "networking-lab"'. Below the banner, the 'Buckets (4)' section is displayed, showing a table of buckets. The 'networking-lab' bucket is highlighted, showing its name, AWS Region (US East (Ohio) us-east-2), Access (Error), and Creation date (October 27, 2023, 15:10:23 UTC-04:00).

Name	AWS Region	Access	Creation date
amanz-bucket	US East (N. Virginia) us-east-1	Error	October 26, 2023, 20:04:43 (UTC-04:00)
demo-amanz-v3-event-notifications	US East (N. Virginia) us-east-1	Error	October 26, 2023, 21:28:30 (UTC-04:00)
elasticbeanstalk-us-east-1-692215778807	US East (N. Virginia) us-east-1	Error	September 17, 2023, 16:01:33 (UTC-04:00)
networking-lab	US East (Ohio) us-east-2	Error	October 27, 2023, 15:10:23 (UTC-04:00)

Security Groups

Follow the steps to create a Security Group. Submit a screenshot of step 3 with the new security group visible.

The screenshot displays the AWS Management Console interface. At the top, a green notification bar states: "Security group (sg-0482c1a55fe5dffff | LAB-NET) was created successfully". Below this, the breadcrumb navigation shows "EC2 > Security Groups > sg-0482c1a55fe5dffff - LAB-NET". The main heading is "sg-0482c1a55fe5dffff - LAB-NET".

The "Details" tab is active, showing the following information:

Security group name LAB-NET	Security group ID sg-0482c1a55fe5dffff	Description sg-aws-networking	VPC ID vpc-0da63d8e53796a2f5
Owner 692215778807	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Below the details, there are tabs for "Inbound rules", "Outbound rules", and "Tags". The "Inbound rules" tab is selected, showing "Inbound rules (3)". There is a search bar with the placeholder "Filter security group rules" and buttons for "Manage tags" and "Edit inbound rules".

The footer of the console includes "CloudShell", "Feedback", "© 2023, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", and "Cookie preferences".

us-east-1.console.aws.amazon.com

Services Search [Option+S]

N. Virginia aman

sg-0482c1a55fe5dfff - LAB-NET

Actions

Details

Security group name LAB-NET	Security group ID sg-0482c1a55fe5dfff	Description sg-aws-networking	VPC ID vpc-0da63d8e53796a2f5
Owner 692215778807	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

Inbound rules (3)

Filter security group rules

Security group rule...	IP version	Type	Protocol	Port range	Source
sgr-0121e275824404...	IPv4	SSH	TCP	22	0.0.0.0/0
sgr-05fc7348178b2122f	IPv4	HTTP	TCP	80	0.0.0.0/0
sgr-074c54c731feedc74	IPv4	HTTPS	TCP	443	0.0.0.0/0

CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Network ACLs

Follow the steps to view the Network ACLs in the AWS Management Portal, and create a new Network ACL. Submit a screenshot of step 15 in which you verify the Subnet Association of the new Network ACL.

us-east-1.console.aws.amazon.com

BB Email

aws

Services

Search

[Option+S]

N. Virginia

aman

VPC dashboard

EC2 Global View

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Network ACLs

You have successfully updated subnet associations for acl-01971f3a80f3bc3ea / my-acl-1.

Details

Network ACLs (1/3)

Info

Find resources by attribute or tag

1

	Name	Network ACL ID	Associated with	Default	VPC ID
<input type="checkbox"/>	-	acl-0c5d1568cb7013823	subnet-07d3ef192448955cb	Yes	vpc-0b75f3...
<input type="checkbox"/>	-	acl-000b826c594143ca4	3 Subnets	Yes	vpc-0da63d...
<input checked="" type="checkbox"/>	my-acl-1	acl-01971f3a80f3bc3ea	subnet-02cc32c1e98b96558 / LAB VPC-subnet...	No	vpc-0da63d...

acl-01971f3a80f3bc3ea / my-acl-1

DetailsInbound rulesOutbound rulesSubnet associationsTags

Subnet associations (1)

Filter subnet associations

1

Name	Subnet ID	Associated with	Availability Zo...	IPv4 CIDR
LAB VPC-subnet-public...	subnet-02cc32c1e98b9...	acl-01971f3a80f3bc3ea / my-acl-1	us-east-1a	10.0.0.0/20

CloudShell

Feedback

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences