

## AWS LAB Secure Architecture | Monarch Nigam

### EXERCISE 12.1

#### Create a Limited Administrative User

In this exercise We will create an IAM user with limited administrative privileges. You'll use policy boundary permissions to allow the user to perform only actions in the EC2 service.

1. Create a customer-managed policy called LimitedAdminPolicyBoundary. Populate the policy document with the following content:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "ec2:*",  
      "Resource": "*"  
    }  
  ]  
}
```

The screenshot shows the AWS IAM 'Create policy' interface. It's Step 1: Specify permissions. The title is 'Specify permissions' with an info link. Below it says 'Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.' A 'Policy editor' pane contains the JSON code from the previous step. To the right are tabs for 'Visual', 'JSON' (which is selected), and 'Actions'. Below the editor is a section titled 'Edit statement' with a 'Select a statement' button and a note: 'Select an existing statement in the policy or add a new statement.'

2. Create an IAM user with the name of your choice, such as LimitedAdmin.

The screenshot shows the AWS IAM 'Policies' page. It displays a green success message: 'Policy LimitedAdminPolicyBoundary\_monarch created.' Below it is a table of policies. One row is highlighted with a blue border, showing the policy name 'LimitedAdminPolicyBoundary\_monarch', type 'Customer managed', and usage status 'None'. The table has columns for 'Policy name', 'Type', 'Used as', and 'Description'. There are also 'Actions' and 'Delete' buttons for each row. A search bar at the top is set to 'LimitedAdminPolicyBoundary\_monarch'.

3. In the IAM Dashboard, click the Users option and then click the username you created.

The screenshot shows the AWS IAM Users page. A green success message at the top states "User created successfully" and "You can view and download the user's password and email instructions for signing in to the AWS Management Console." Below this, the "Users (1) Info" section shows one user named "LimitedAdmin\_monarch". The user has a path of "/", 0 groups, and 0 last activities. There are buttons for "View user", "Delete", and "Create user".

4. Under Permissions Boundary, click the Set Boundary button.
5. Select the LimitedAdminPolicyBoundary option and click the Set Boundary button.

The screenshot shows the "Permissions boundary" section for the user "LimitedAdmin\_monarch". It displays a message "Permissions boundary LimitedAdminPolicyBoundary\_monarch added." and a note that permissions are defined by policies attached to the user directly or through groups. A table titled "Permissions boundary (set)" shows one policy: "LimitedAdminPolicyBoundary\_monarch" (Customer managed). Buttons for "Change boundary" and "Remove boundary" are visible.

6. Under Permissions Policy, click Add Permissions.
7. Click the Attach Existing Policies Directly button.

The screenshot shows the "Add permissions" step 1. It includes a sidebar with "Step 1 Add permissions", "Step 2 Review", and "Add permissions" selected. The main area is titled "Add permissions" and describes adding users to existing groups or creating new ones. It features "Permissions options" with three choices: "Add user to group" (selected), "Copy permissions", and "Attach policies directly". The "Permissions policies (1338)" section lists two policies: "AccessAnalyzerServiceRolePolicy" (AWS managed, 0 attached entities) and "AdministratorAccess" (AWS managed - job function, 0 attached entities).

8. Select the AdministratorAccess policy and click the Next: Review button.
9. Click the Add Permissions button.

**LimitedAdmin\_monarch** [Info](#)

**Summary**

ARN: arn:aws:iam::160885292183:user/LimitedAdmin\_monarch

Created: April 13, 2025, 20:32 (UTC-05:00)

Last console sign-in: Never

Console access: Enabled without MFA

Access key 1: Create access key

**Permissions** Groups Tags Security credentials Last Accessed

**Permissions policies (1)**

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Directly

## EXERCISE 12.2

In this exercise, we will create a role and assume it.

- While logged in as an administrative IAM user, click Roles on the menu on the left side of the IAM Dashboard screen and then click the Create Role button.

**Console Home** [Info](#)

**Recently visited** [Info](#)

No recently visited services

Explore one of these commonly visited AWS services.

[EC2](#) [S3](#) [Aurora and RDS](#) [Lambda](#)

**Applications (0)** [Info](#)

Region: US East (Ohio)

Select Region: us-east-2 (Current Region) [Find applications](#)

**Access denied to servicecatalog>ListApplications**

[Diagnose with Amazon Q](#)

- Under Select Type Of Trusted Entity, click the Another AWS Account button.
- Under Account ID, enter your AWS account number. Click the Next: Permissions button.

**Select trusted entity**

**Trusted entity type**

- AWS service
- AWS account
- SAML 2.0 federation
- Custom trust policy

**An AWS account**

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

This account (160885292183)

Another AWS account

Account ID

160885292183

Account ID is a 12-digit number.

- Select the AmazonEC2ReadOnlyAccess AWS managed policy and click the Next: Tags button.

**Add permissions**

**Permissions policies (1/1040)**

Choose one or more policies to attach to your new role.

Filter by Type
AmazonEC2ReadOnlyAccess
All types
1 match
Policy name
AmazonEC2ReadOnlyAccess
AWS managed
Provides read only access to Amazon E...

**Set permissions boundary - optional**

- Click the Next: Review button.
- Enter a name for the role, such as EC2ReadOnlyRole

aws Search [Option+S] Global LimitedAdmin\_monarch @ 1608-8529-2183

IAM > Roles > Create role

Step 1  
Select trusted entity  
Step 2  
Add permissions  
Step 3  
**Name, review, and create**

### Name, review, and create

**Role details**

**Role name**  
Enter a meaningful name to identify this role.  
**EC2ReadOnlyRole\_monarch**  
Maximum 64 characters. Use alphanumeric and '+,-,@,\_' characters.

**Description**  
Add a short explanation for this role.  
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: '\_+=,. @-/\[\]!#\$%^&`~`-

**Step 1: Select trusted entities** Edit

**Trust policy**

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": "sts:AssumeRole",
7-       "Principal": {
8-         "AWS": "160885292183"
9-       },
10-      "Condition": {}
11-    }
12-  ]
13- }
```

- Click the Create Role button.

aws Search [Option+S] Global LimitedAdmin\_monarch @ 1608-8529-2183

IAM > Roles

Identity and Access Management (IAM)

Roles (7) Info

Role EC2ReadOnlyRole\_monarch created. View role X

<input type="checkbox"/> Role name	Trusted entities	Last activity
<a href="#">AWSServiceRoleForRDS</a>	AWS Service: rds (Service-Linked Rol)	27 days ago
<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linker)	-
<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service)	-
<a href="#">AWSServiceRoleForVPCTransitGateway</a>	AWS Service: transitgateway (Service)	21 days ago
<a href="#">EC2ReadOnlyRole_monarch</a>	Account: 160885292183	-
<a href="#">monarch-cloudtrail-role</a>	AWS Service: cloudtrail	7 days ago
<a href="#">rds-monitoring-role</a>	AWS Service: monitoring.rds	41 days ago

- On the navigation bar at the top of the AWS Management Console, click your IAM account name. A drop-down menu will appear.
- Click the Switch Role link in the drop-down menu, as shown here.
- Snapshot of entering the fields.
- Click the Switch Role button.
- Enter your 12-digit AWS account number or alias and the name of the role you created in step 6. The following shows an example of a Switch Role screen with the account and role specified.
- Snapshot of entering the fields.

## Switch Role

Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. [Learn more](#)

**Account ID**  
The 12-digit account number or the alias of the account in which the role exists.

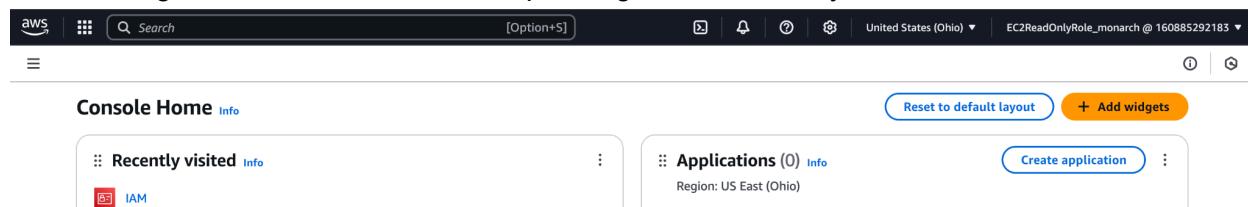
**IAM role name**  
The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the **TestRole** role name from the following role ARN: `arn:aws:iam::123456789012:role/TestRole`.

**Display name - optional**  
This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.

**Display color - optional**  
The selected color displays in the console navigation when this role is active

None

- Click the Switch Role button. The name of the role followed will appear in the top navigation bar. You will now be operating under the role you created.



- Try to launch an EC2 instance. It will fail because the assumed role doesn't have the RunInstances permission. As we can see in the below snapshot we are not able to create the EC2 instance

aws Search [Option+S]

EC2 > Instances > Launch an instance

**Instance launch failed**

You are not authorized to perform this operation. User: arn:aws:sts::160885292183:assumed-role/EC2ReadOnlyRole\_monarch/LimitedAdmin\_monarch is not authorized to perform: ec2:RunInstances on resource: arn:aws:ec2:us-east-1:160885292183:instance/\* because no identity-based policy allows the ec2:RunInstances action. Encoded authorization failure message: bnzokh1TPeQdTeGKApxFutlMPluhYUdu7HlLBzqLuloiuHvHa7EuJjigU3ldtw1hZwSPtUfYomam6gQvLBbQdvnhjbXuzlKElkSeQHwq6s675R1rl4AFix4GlxxtbsL4PhOb\_vQA1DA2L6DGZqe6CaQInL\_J\_RAxIUOp5y9ElUWz2uJthQbfSPASy617XSmfpLpJGgaXzUjT3QJUoelDLV1TwAl\_VznfnhuvLXje6CMUJ\_In0MVLSojYIA2asftH0eTurg-rK\_3hniZisNxbzol3BGv7u9jCvnZ-IGSqliKK6BPjMOHUltC24T7oIu2zclanicC2JrDSC3UoqBvMSGMNOMyGhWRH70n-WNW\_e0GU75LG5JwPb5WsuWwMx125ip596FAHD53ZwrSRR0t0d7FLBL-BlaGWZ-98gc9WaMKzHZtn-XUJwmU7gQO0wcoC2f12mX3HYCommfb6vdV3KG45xhILBSULXbzVky8412Njd\_2nHz4xqAq-S8gGAK0L-Ytbrg8VipB3XqonlCauGg485r9wGGMu3lemt3QlRe2mJpKL85JN\_D\_2uK37w9-P2qJ\_5cCFR51-S5\_G0lhWH0dHhwgh5rjKQkaHTDv10zyAD9ehfOzXn1CgbXSM2teEgsGf58H1WJdtcs0BPsT2xUJD8ses16cgGnXvFdFb4Z8eqCMAmReGpcnoTcJw1nNBEXWvQpGsVjgUjf2PaP1JEgl\_kXC6UPkaRarh-lv0TwTpzbDoNPEnGoie5dX83m2XOPW618

**Diagnose with Amazon Q**

▼ Launch log

Initializing requests	Succeeded
Launch initiation	Failed

Cancel Edit instance config Retry failed tasks

- To switch back to your IAM user, click the upper-right menu bar where the name of the role followed by your AWS account number is. Then click the link that reads Back To [your IAM username].

United States (N. Virginia) ▾ EC2ReadOnlyRole\_monarch @ 160885292183 ▾

Currently active as  EC2ReadOnlyRole\_monarch

Account ID  1608-8529-2183

Account Organization Service Quotas Billing and Cost Management

Signed in as  LimitedAdmin\_monarch

Account ID  1608-8529-2183

[Switch back](#)

R LimitedAdmin\_monarch @ 1608-8529-2183  
EC2ReadOnlyRole\_monarch @ 160...

[Turn on multi-session support](#)

[Switch role](#) [Sign out](#)

### EXERCISE 12.3

#### Configure VPC Flow Logging

In this exercise, we will configure VPC flow logging to deliver flow logs to a CloudWatch Logs log group.

1. In the VPC Dashboard, select a VPC you want to log traffic for. Click the Flow Logs tab.

The screenshot shows the AWS VPC Dashboard. At the top, there's a search bar and a 'Your VPCs (1) Info' section. Below it is a table with columns: Name, VPC ID, State, Block Public..., IPv4 CIDR, and IPv6 CIDR. One row is visible, showing 'vpc-0e92ca1c7be9b22ad' with 'Available' status and 'Off' for Block Public. The IPv4 CIDR is listed as '172.31.0.0/16'. On the right side of the table, there are 'Actions' and 'Create VPC' buttons. The top right corner shows 'United States (N. Virginia)' and 'monarch.smiclass.2025'.

2. Click the Create Flow Log button.

The screenshot shows the 'Create flow log' configuration page. At the top, it says 'Selected resources' with one item: 'Name' (vpc-0e92ca1c7be9b22ad) and 'State' (Available). Below this is the 'Flow log settings' section. It has a 'Name - optional' field containing 'monarch-flow-log'. Under 'Filter', there are three radio buttons: 'Accept', 'Reject', and 'All', with 'All' selected. The 'Maximum aggregation interval' is set to '10 minutes'. The 'Destination' section shows four options: 'Send to CloudWatch Logs' (selected), 'Send to an Amazon S3 bucket', 'Send to Amazon Data Firehose in the same account', and 'Send to Amazon Data Firehose in a different account'. At the bottom, there's a 'Destination log group' field with a placeholder 'The name of an existing log group or the name of a new log group that will be created when you create this flow log.' A 'Create' button is located to the right of the destination log group input field. The footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

3. In the Destination Log Group field, enter a name of your choice, such as **FlowLogs**.

**Service access**  
VPC flow logs require permissions to create log groups and publish events in CloudWatch.

Use an existing service role  
 Create and use a new service role

**Service role** [Info](#)  
The IAM role that has permission to publish to the Amazon CloudWatch log group.

FlowlogsRole

[View this service role in the IAM console](#)

4. You'll need to specify a role, which AWS can create for you. Click the Set Up Permissions link.
5. A new browser tab will open. Click the Allow button. AWS will create a role called FlowlogsRole.
6. Return to the previous tab with the Create Flow Log Wizard. Select the FlowlogsRole.
7. Click the Create button.

**CloudWatch**

- Favorites and recents
- Dashboard
- AI Operations [Preview](#)
- Alarms [New](#)
- Logs
  - Log groups** [New](#)
  - Log Anomalies
  - Live Tail
  - Logs Insights [New](#)
  - Contributor Insights
- Metrics
  - All metrics
  - Explorer

**monarch-aws-cloudtrail-logs-160885292183-d7c98bb4**

**Log group details**

**Log streams (4)**

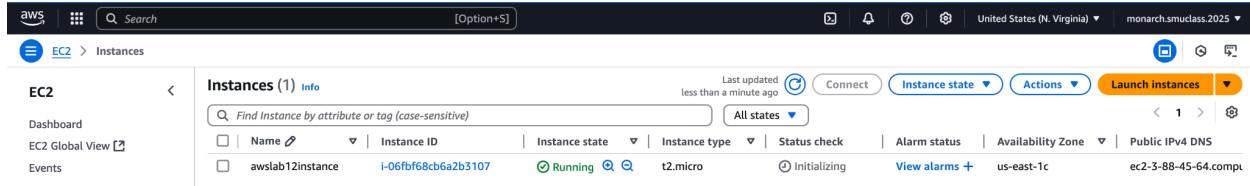
Log stream	Last event time
160885292183_CloudTrail_us-east-1_4	2025-04-06 20:13:23 (UTC)
160885292183_CloudTrail_us-east-1_3	2025-04-06 20:11:13 (UTC)
160885292183_CloudTrail_us-east-1_2	2025-04-06 20:03:52 (UTC)
160885292183_CloudTrail_us-east-1_1	-

## **EXERCISE 12.4**

### **Encrypt an EBS Volume**

For this exercise, we will encrypt an unencrypted volume attached to a running EC2 instance.

1. Create an EC2 instance from an unencrypted snapshot or AMI. If you already have one you can bear to part with, you may use that.



The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation menu with 'EC2' selected. The main area displays a table titled 'Instances (1) Info'. It shows one instance: 'awslab12instance' with ID 'i-06fbf68cb6a2b3107'. The instance is 'Running' and has an 't2.micro' instance type. It is currently 'Initializing'. The table includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. The Public IPv4 DNS is listed as 'ec2-3-88-45-64.com'.

2. At the EC2 Dashboard, click Volumes in the left-side menu.
3. Select the volume attached to your instance.



The screenshot shows the AWS EC2 Volumes page. On the left, there's a navigation menu with 'EC2' selected. The main area displays a table titled 'Volumes (1/1) Info'. It shows one volume: 'vol-0a88fb308068aa4f1'. The volume is a 'gp3' type with 8 GiB of storage, 3000 IOPS, and 125 throughput. It was created from snapshot 'snap-0be675a...' on 2025/04/13 at 22:01 GMT-5. The table includes columns for Name, Volume ID, Type, Size, IOPS, Throughput, Snapshot ID, Created, and Availability Zone.

4. Under the Actions menu, click Create Snapshot. EBS will begin creating an unencrypted snapshot of the volume.

**Create snapshot** Info

Create a point-in-time snapshot to back up the data on an Amazon EBS volume to Amazon S3.

**Source volume**

Volume ID <a href="#">vol-0a88fb308068aa4f1</a>	Availability Zone us-east-1c
--	---------------------------------

**Snapshot details**

Description  
Add a description for your snapshot  
  
255 characters maximum.

Encryption Info  
Not encrypted

**Tags** Info  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.  
No tags associated with the resource.

[Add tag](#)  
You can add 50 more tags.

[Cancel](#) [Create snapshot](#)

5. On the left-side menu, click Snapshots. Wait for the snapshot to complete.

**snap-05ae9421265a71d67**

**Details**

Snapshot ID <a href="#">snap-05ae9421265a71d67</a>	Full snapshot size <a href="#">1.57 GiB</a>	Progress <a href="#">100%</a>	Snapshot status <a href="#">Completed</a>
Owner <a href="#">160885292183</a>	Started <a href="#">Sun Apr 13 2025 22:03:27 GMT-0500 (Central Daylight Time)</a>	Product codes -	Fast snapshot restore -
Description <a href="#">snapshot_monarch</a>			
Source volume			

Last updated less than a minute ago [Copy](#) [Delete](#) [Actions](#)

6. Select the snapshot and under the Actions menu, click Copy.
7. Select the Encrypt This Snapshot check box.
8. Next to the Master Key drop-down, select the KMS key you'd like to use to encrypt the snapshot. You can use your own customer master key or the default AWS/EBS key.

**Source snapshot**  
The original snapshot that is to be copied.

**Snapshot ID**  
snap-05ae9421265a71d67

**Region**  
us-east-1

**Snapshot copy details**

**Description**  
A description for the snapshot copy.  
[Copied snap-05ae9421265a71d67 from us-east-1] snapshot\_monarch  
255 characters maximum.

**Destination Region**  
The Region in which to create the snapshot copy.  
us-east-1

**Time-based copy - new** Info  
Specify a completion duration for the snapshot copy operation. Additional costs apply. [Learn more](#)

Enable time-based copy

**Encryption** Info  
Use Amazon EBS encryption as an encryption solution for your EBS resources.

Encrypt this snapshot

**KMS key** Info  
(default) aws/ebs

9. Click the Copy button. EBS will begin creating an encrypted copy of the snapshot.

The larger the volume, the longer the encryption process takes. A good rule of thumb is about 3 gigabytes per minute.

Snapshots (2) <small>Info</small>							Last updated	<a href="#">Recycle Bin</a>	<a href="#">Actions</a>	<a href="#">Create snapshot</a>
<a href="#">Owned by me</a>		<a href="#">Search</a>								
	Name	Snapshot ID	Full snapshot size	Volume size	Description	Storage tier	Snapshot status	Started		
<input type="checkbox"/>	-	snap-05ae9421265a71d67	1.57 GiB	8 GiB	snapshot_monarch	Standard	Completed	2025/04/		
<input type="checkbox"/>	-	snap-0db17a3acf5173f9f	1.57 GiB	8 GiB	[Copied snap-05ae942126...	Standard	Completed	2025/04/		

10. Select the encrypted snapshot and under the Actions menu, click Create Volume.

11. Choose the volume type, size, and availability zone, which can be different than the original volume.

**Create volume** [Info](#)

Create an Amazon EBS volume to attach to any EC2 instance in the same Availability Zone.

**Volume settings**

Snapshot ID: [snap-0db17a3acf5173f9f](#)

Volume type: [General Purpose SSD \(gp3\)](#)

Size (GiB): 8

IOPS: 3000

Throughput (MiB/s): 125

Availability Zone: us-east-1a

Fast snapshot restore: Not enabled for selected snapshot

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

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

12. Click the Create Volume button. The new volume will be encrypted using the same key that was used to encrypt the snapshot.

Details	Value	Details	Value
Volume ID	<a href="#">vol-07e5208dc808e6803</a>	Size	8 GiB
AWS Compute Optimizer finding	(?) Opt-in to AWS Compute Optimizer for recommendations.   Learn more	Type	gp3
Fast snapshot restored	No	Volume state	<a href="#">Available</a>
Attached resources	-	Availability Zone	us-east-1a
Source	Snapshot ID: <a href="#">snap-0db17a3acf5173f9f</a>	Outposts ARN	-
Encryption	Encryption: Encrypted	KMS key ID	<a href="#">3ec63459-9411-48c0-8fc0-0dc56633c86</a>
		KMS key alias	<a href="#">aws/ebs</a>
Status checks	Status check: <a href="#">OK</a>	I/O status	<a href="#">OK</a>
Monitoring		I/O performance	<a href="#">Not available</a>
Tags			