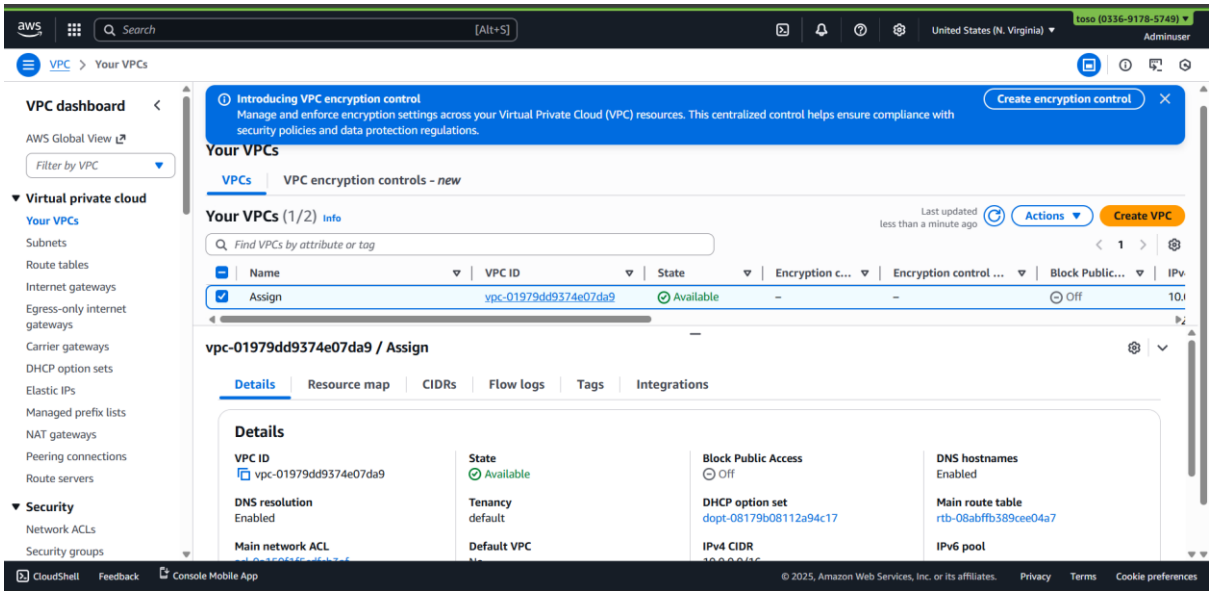
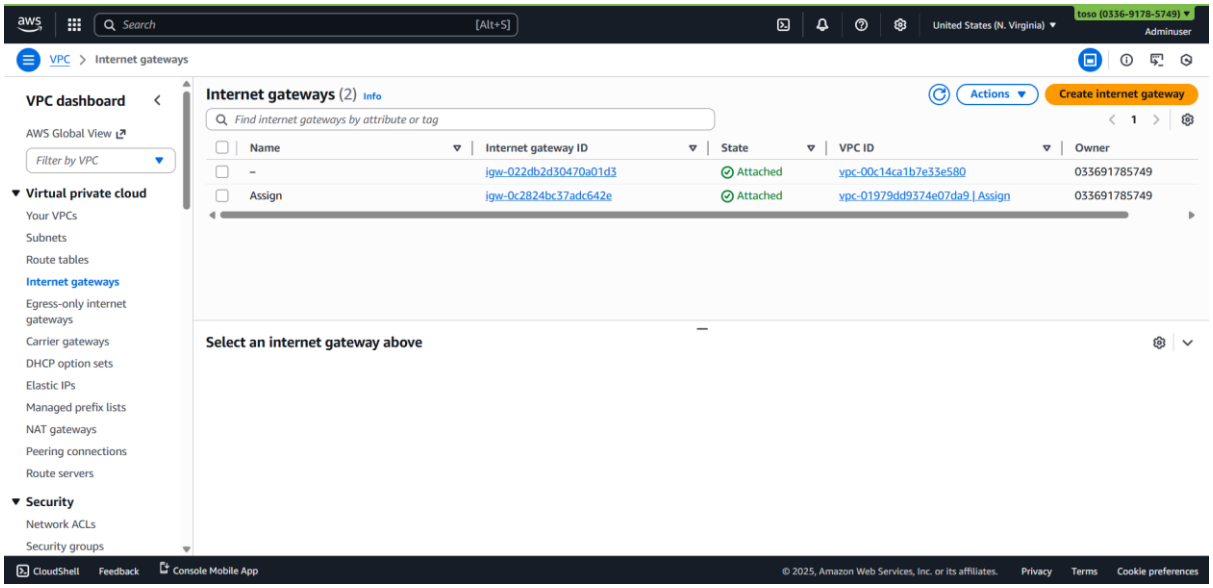
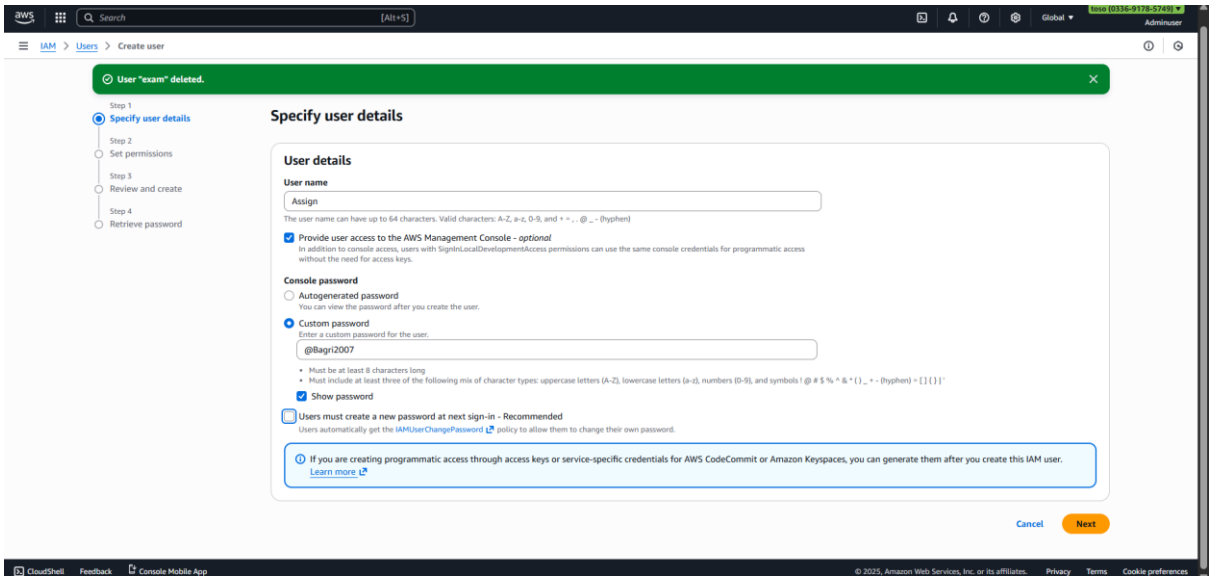
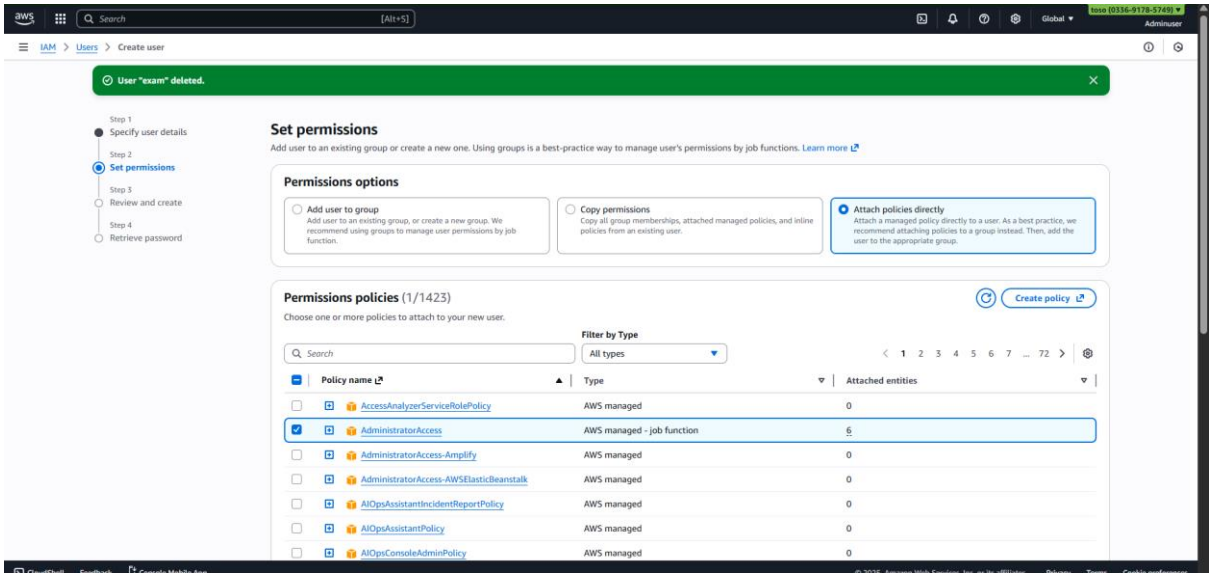
Question 1: (a)Create VPC and add internet gateway to it



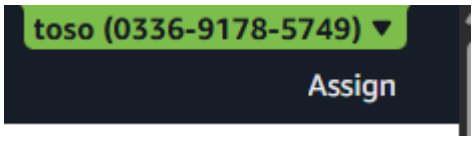


(b) Create a user with administrator access

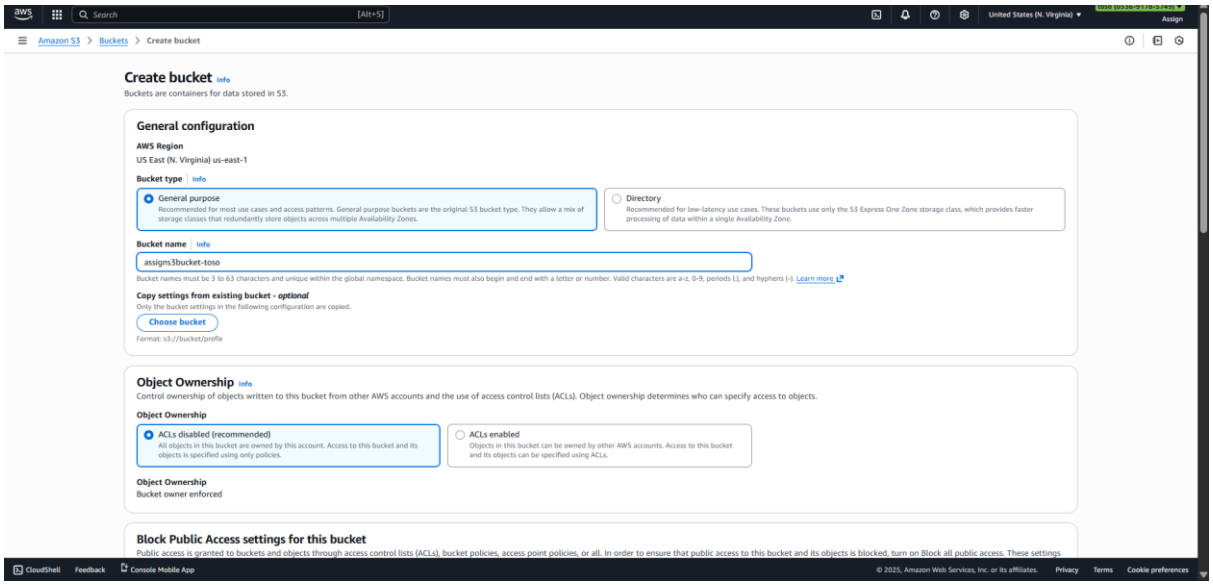


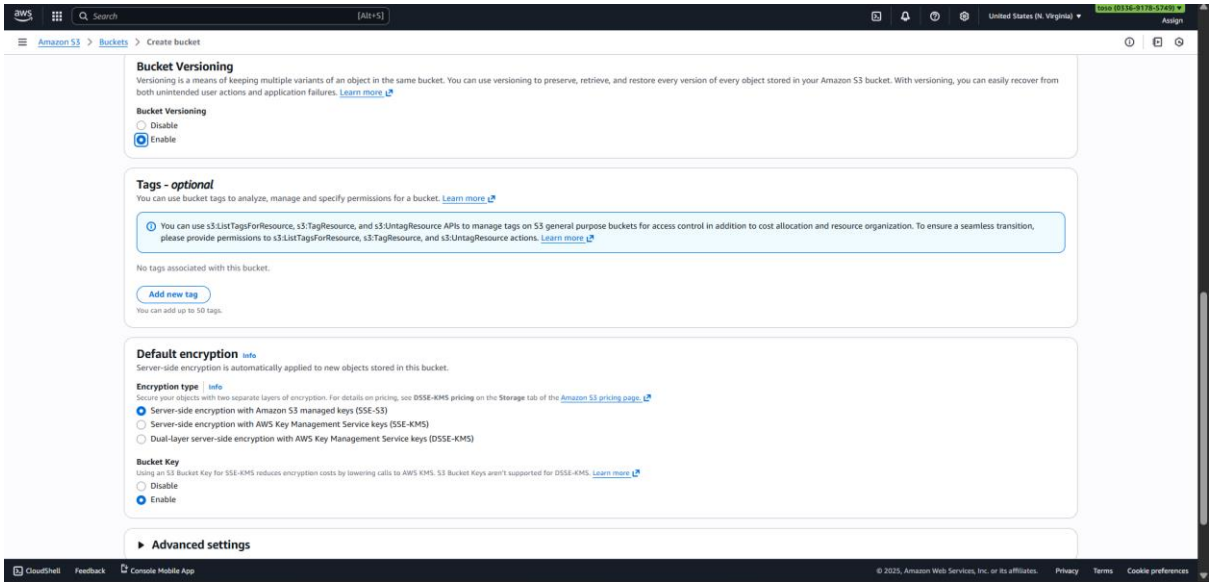


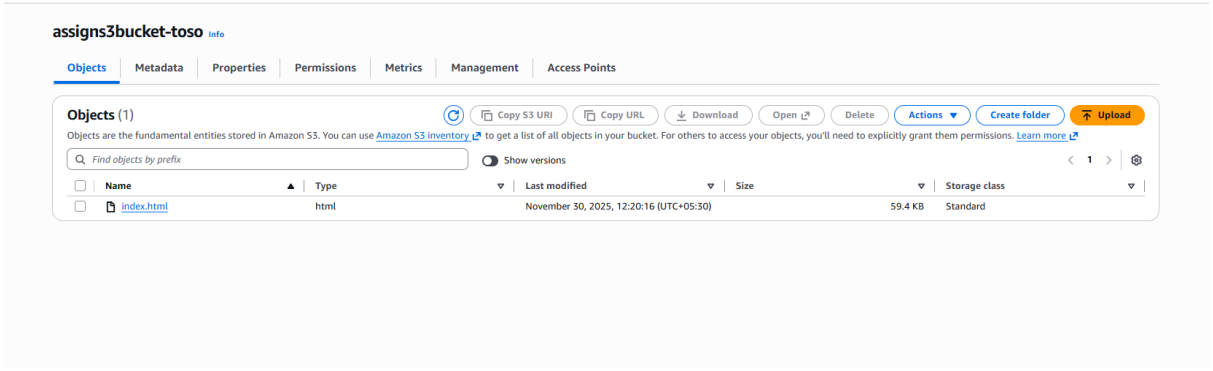
Assign	/	0	-	-	Now	-	-	-	-	-



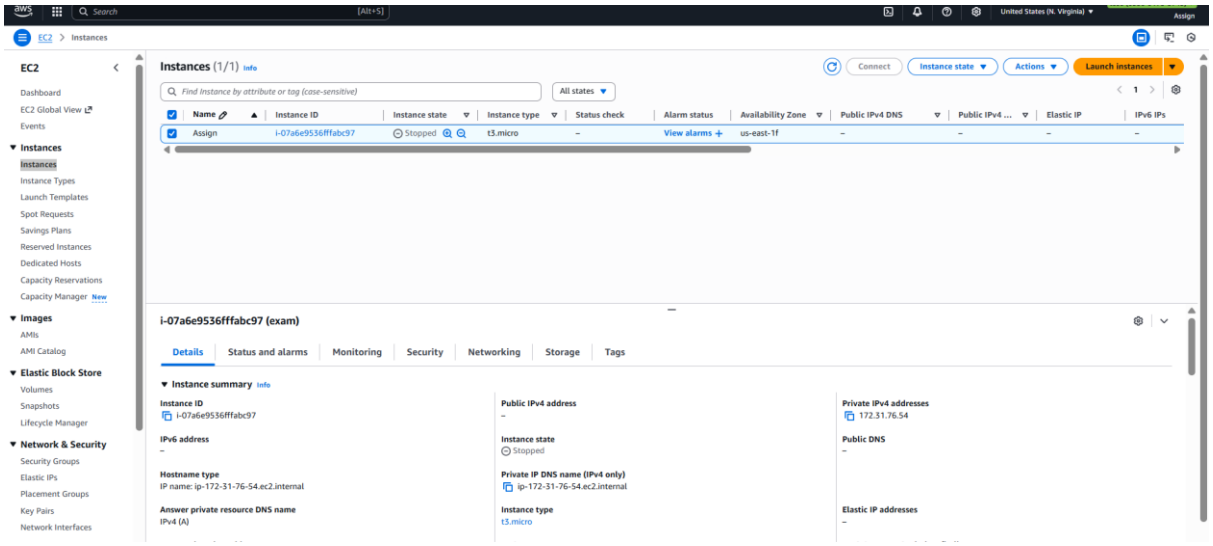
(c)Create a S3 Bucket by enable versioning and have one file



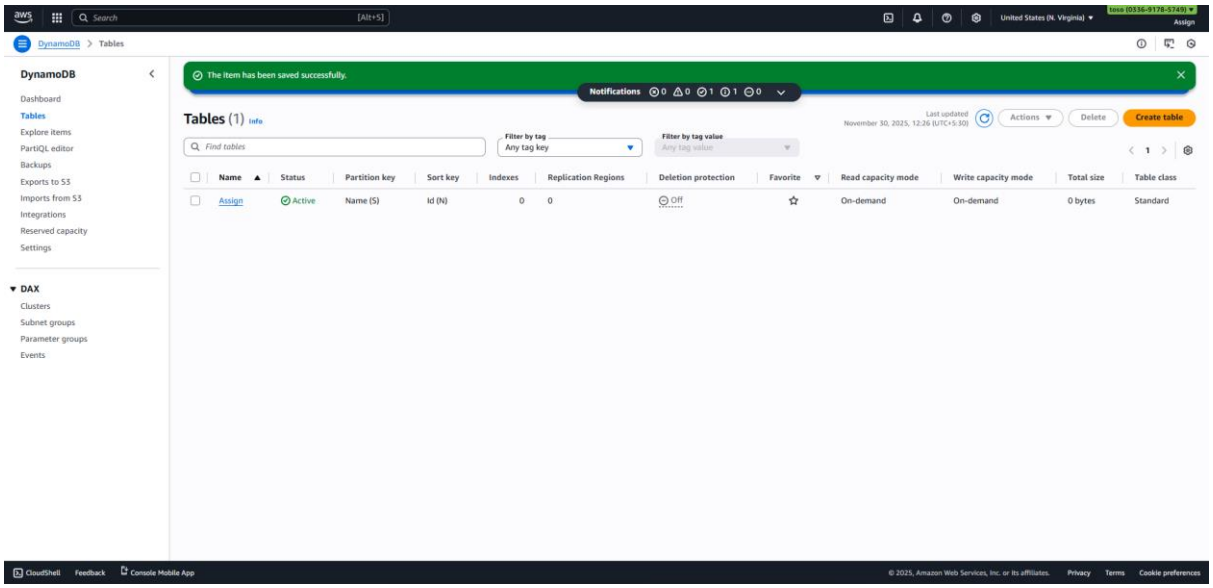


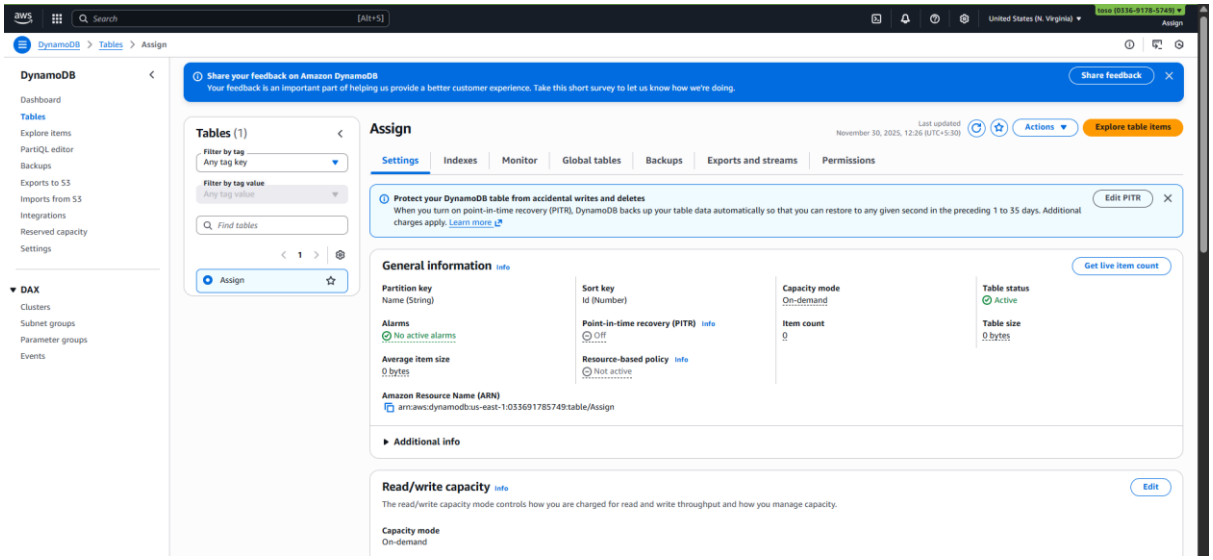


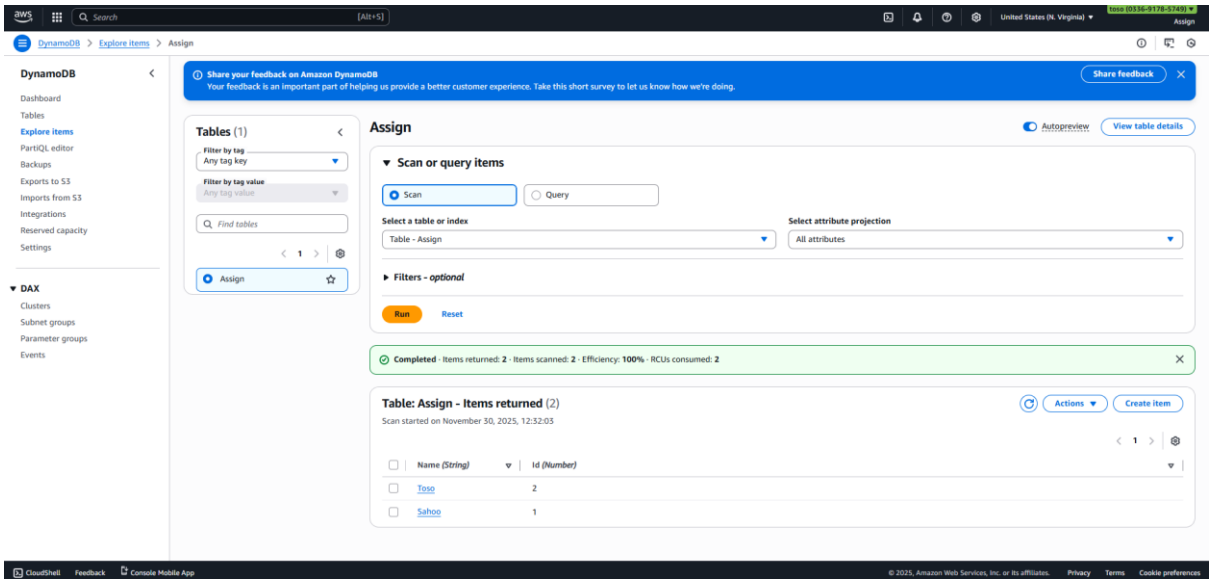
(d) Create a Ec2 instance

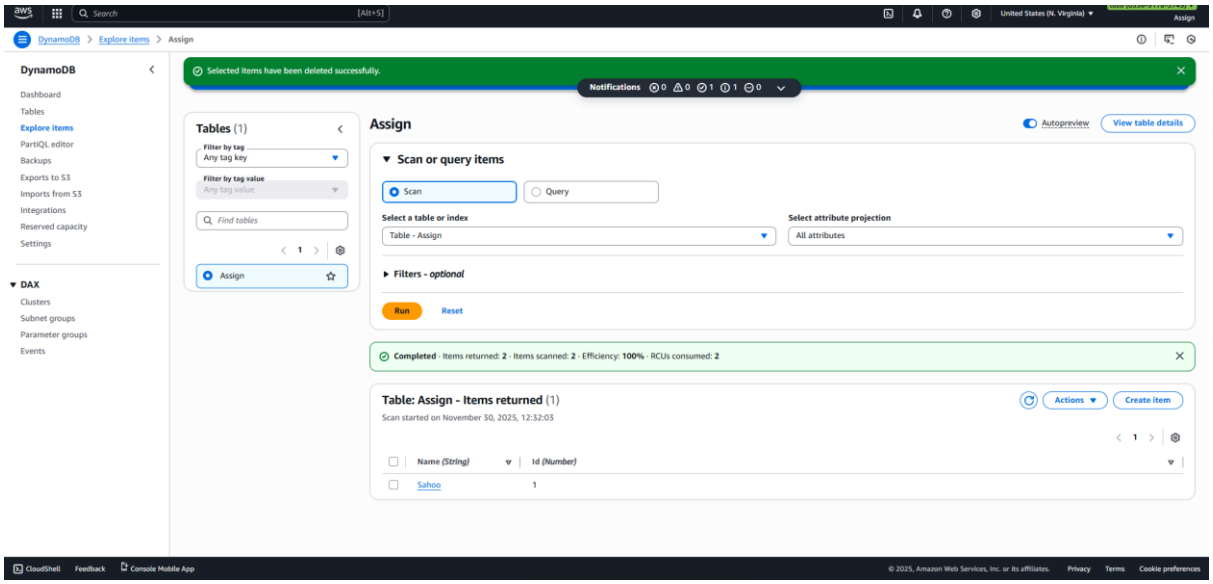


(e) Create a Dynamodb table and add some entries in it and then delete a entry from it

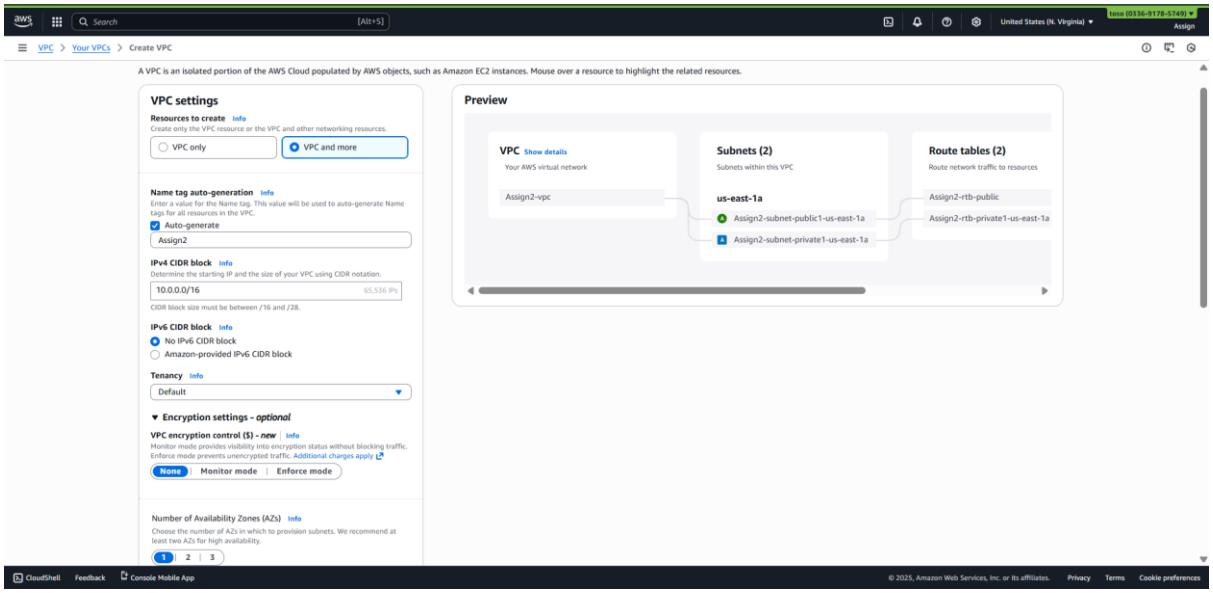


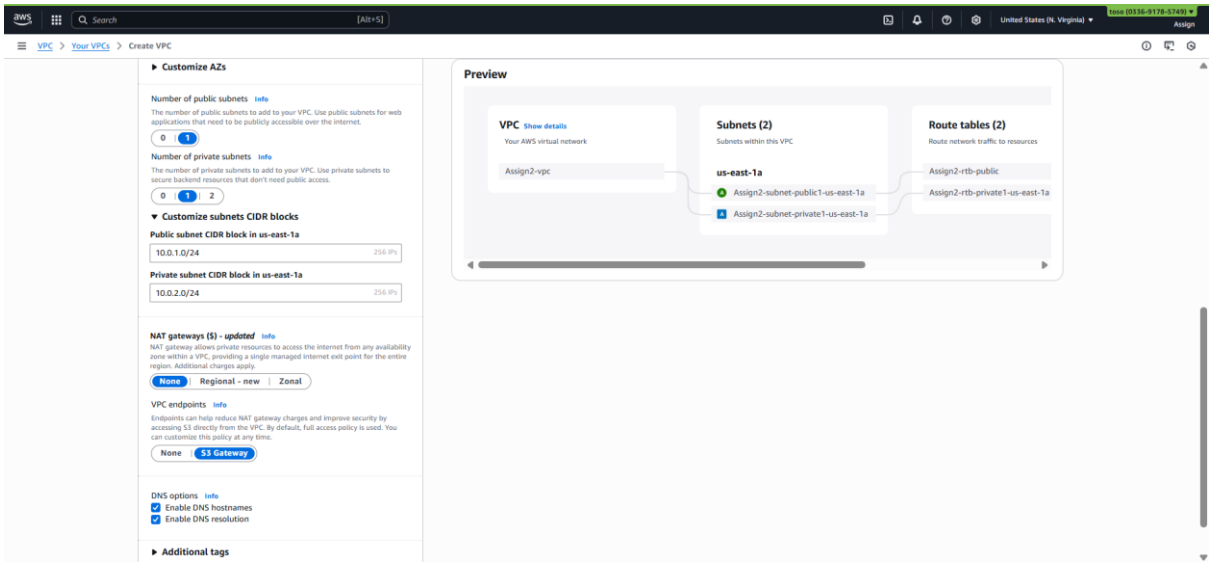

DynamoDB
Tables
Assign
Share your feedback on Amazon DynamoDB
Your feedback is an important part of helping us provide a better customer experience. Take this short survey to let us know how we're doing.
Share feedback
Tables (1)
Assign
Actions
Explore table items
Settings
Indexes
Monitor
Global tables
Backups
Exports and streams
Permissions
Protect your DynamoDB table from accidental writes and deletes
When you turn on point-in-time recovery (PITR), DynamoDB backs up your table data automatically so that you can restore to any given second in the preceding 1 to 35 days. Additional charges apply. Learn more
Edit PITR
General information
Get live item count
Partition key
Name (String)
Sort key
Id (Number)
Capacity mode
On-demand
Table status
Active
Alarms
No active alarms
Point-in-time recovery (PITR)
Off
Item count
0
Table size
0 bytes
Average item size
0 bytes
Resource-based policy
Not active
Amazon Resource Name (ARN)
arn:aws:dynamodb:us-east-1:033691785749:table/Assign
Additional info
Read/write capacity
Edit
The read/write capacity mode controls how you are charged for read and write throughput and how you manage capacity.
Capacity mode
On-demand

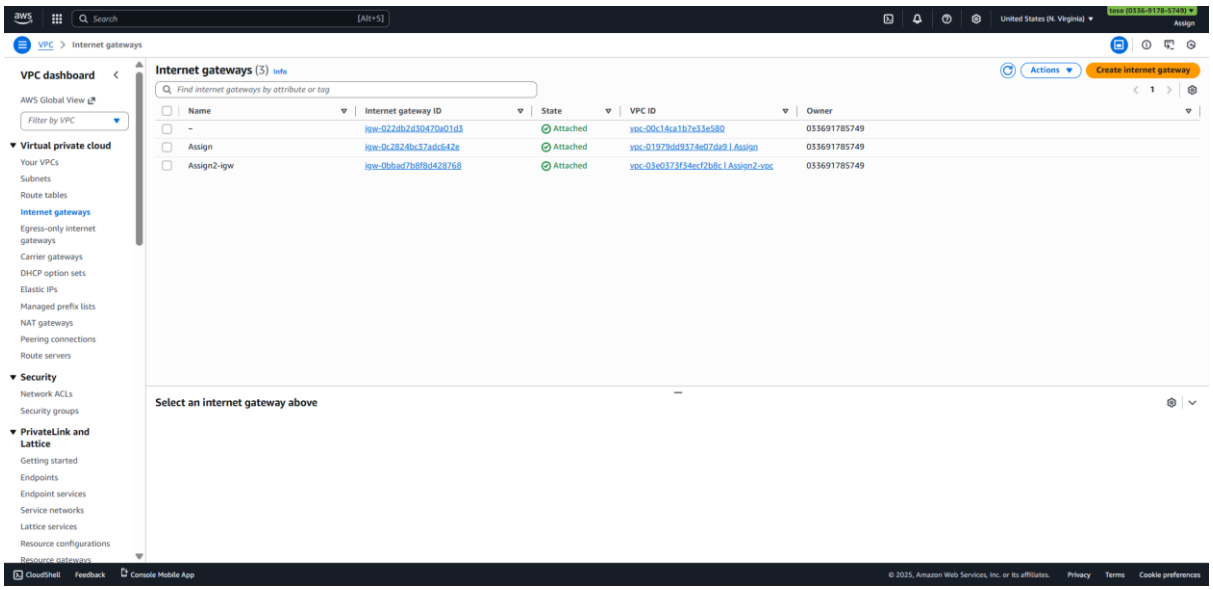

DynamoDB
Explore items
Assign
Share your feedback on Amazon DynamoDB
Your feedback is an important part of helping us provide a better customer experience. Take this short survey to let us know how we're doing.
Share feedback
Tables (1)
Assign
Autopreview
View table details
Scan or query items
Scan
Query
Select a table or index
Table - Assign
Select attribute projection
All attributes
Filters - optional
Run
Reset
Completed · Items returned: 2 · Items scanned: 2 · Efficiency: 100% · RCUs consumed: 2
Table: Assign - Items returned (2)
Actions
Create item
Scan started on November 30, 2025, 12:32:03
Name (String)
Id (Number)
Toso
2
Sahoo
1

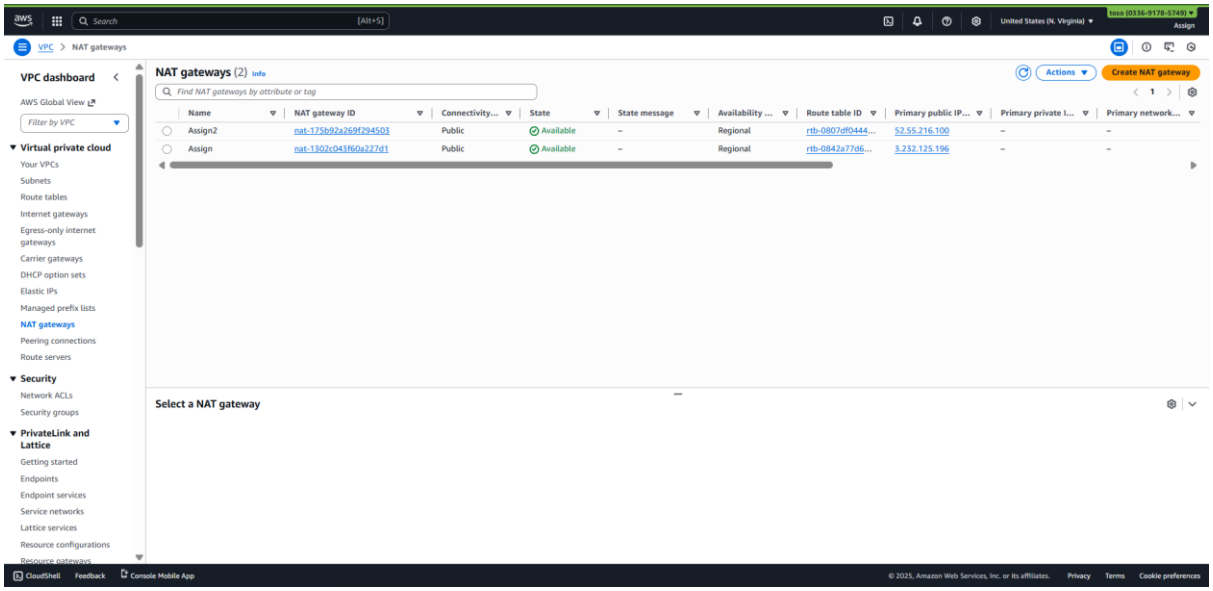

DynamoDB
Explore items
Assign
Selected items have been deleted successfully.
Notifications
Tables (1)
Assign
Autopreview
View table details
Scan or query items
Scan
Query
Select a table or index
Table - Assign
Select attribute projection
All attributes
Filters - optional
Run
Reset
Completed · Items returned: 2 · Items scanned: 2 · Efficiency: 100% · RCUs consumed: 2
Table: Assign - Items returned (1)
Actions
Create item
Scan started on November 30, 2025, 12:32:03
Name (String)
Id (Number)
Sahoo
1

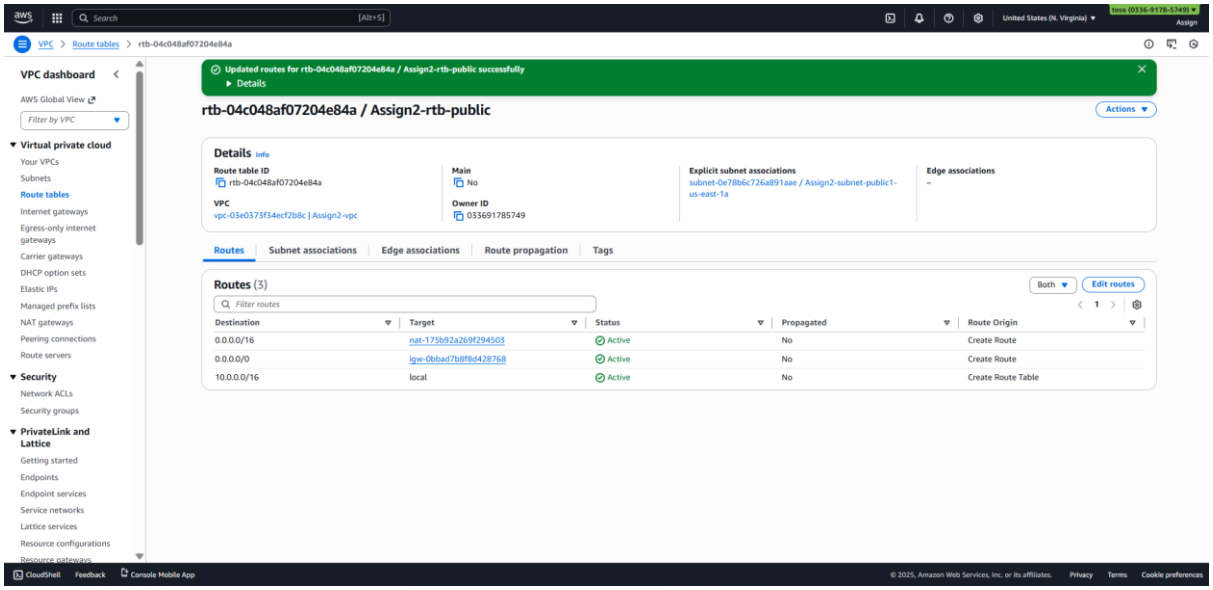
Question 2: Secure ML Pipeline Network Architecture



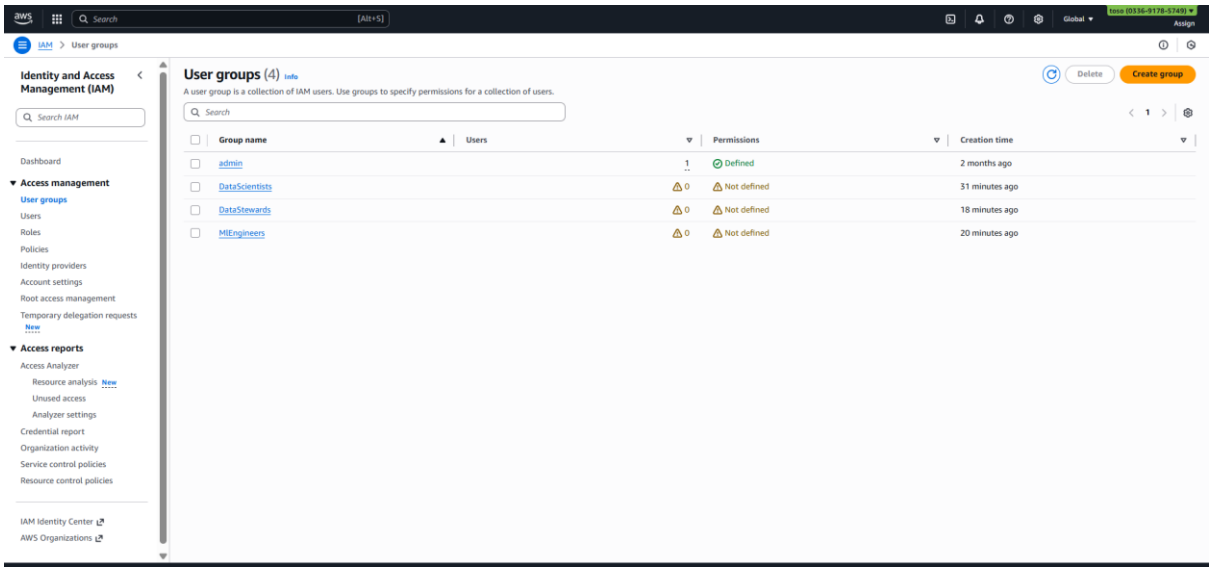


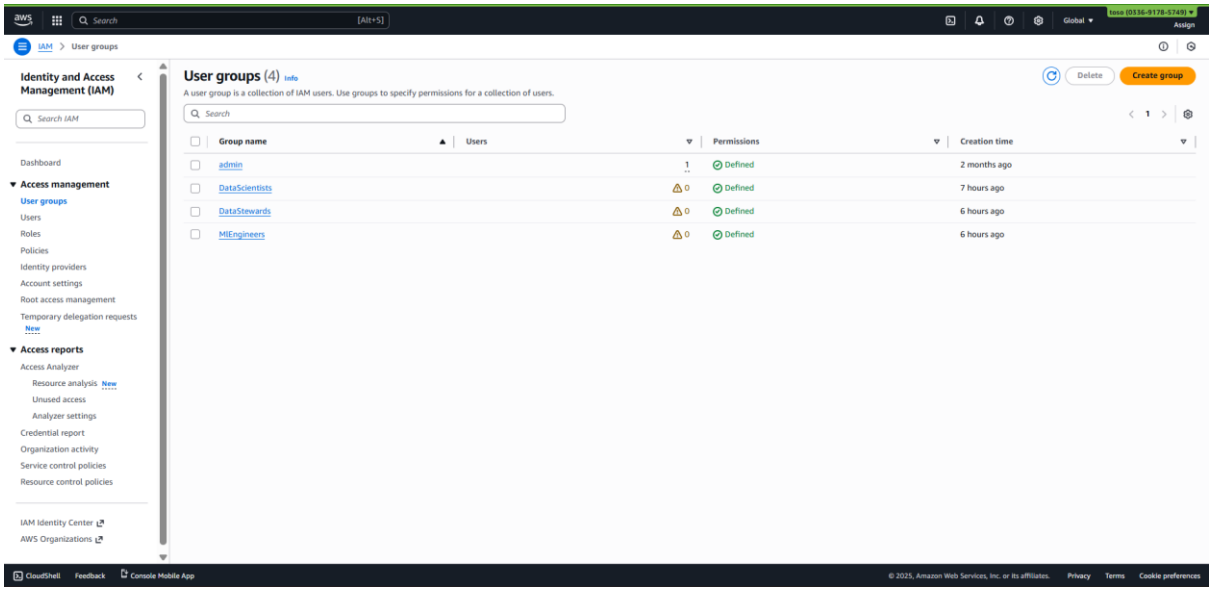


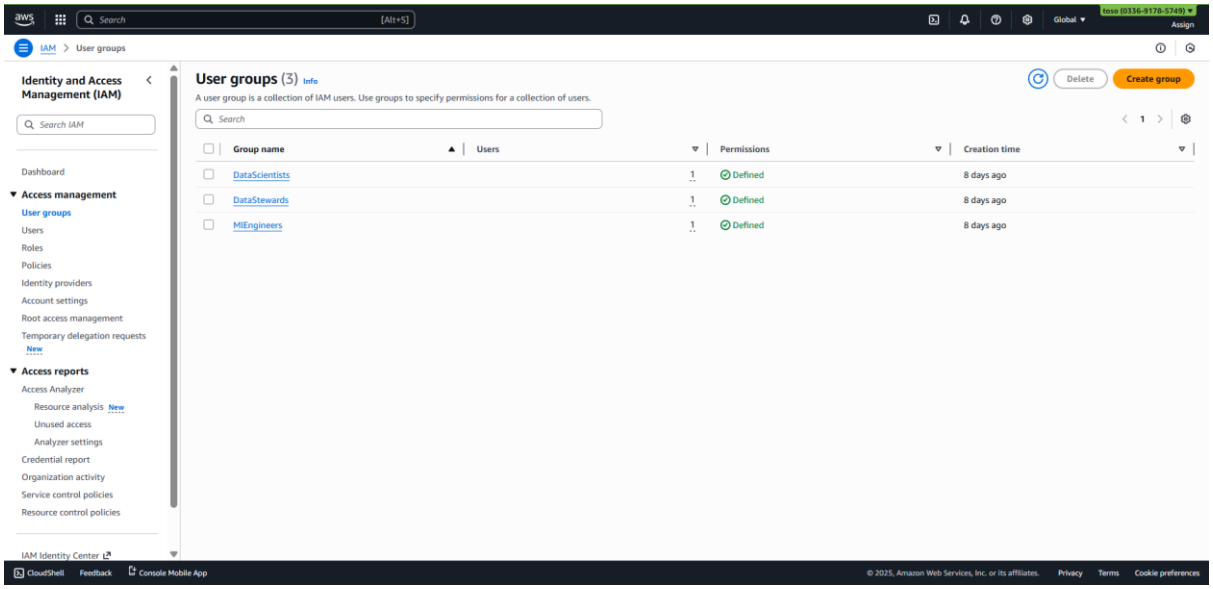


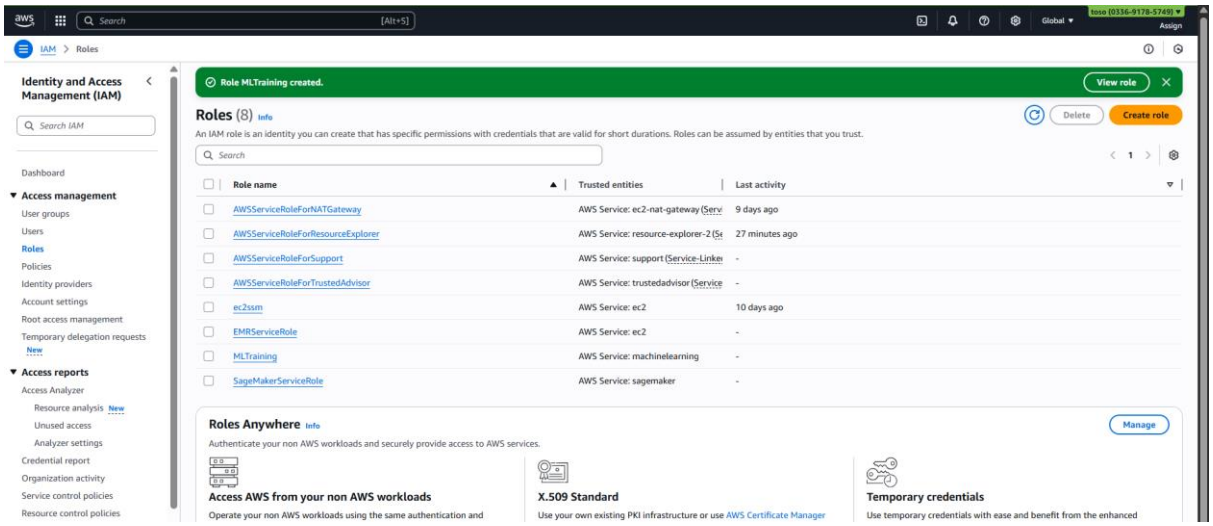


Question 3: ML Team Access Control & Data Governance




Search [Alt+S]
Global
IAM > User groups
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
AWS Organizations
User groups (4) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Group name
Users
Permissions
Creation time
admin
1
Defined
2 months ago
DataScientists
0
Defined
7 hours ago
DataStewards
0
Defined
6 hours ago
MlEngineers
0
Defined
6 hours ago
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Global
IAM > User groups
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
IAM Identity Center
User groups (3) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Group name
Users
Permissions
Creation time
DataScientists
1
Defined
8 days ago
DataStewards
1
Defined
8 days ago
MlEngineers
1
Defined
8 days ago
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Global
IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Temporary delegation requests
New
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Resource control policies
Role MLTraining created.
View role
Roles (8) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Role name
Trusted entities
Last activity
AWSServiceRoleForNATGateway
AWS Service: ec2-nat-gateway (Serv
9 days ago
AWSServiceRoleForResourceExplorer
AWS Service: resource-explorer-2 (Se
27 minutes ago
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
-
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
-
ec2ssm
AWS Service: ec2
10 days ago
EMRServiceRole
AWS Service: ec2
-
MLTraining
AWS Service: machinelearning
-
SageMakerServiceRole
AWS Service: sagemaker
-
Roles Anywhere Info
Manage
Authenticate your non AWS workloads and securely provide access to AWS services.
Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and
X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager
Temporary credentials
Use temporary credentials with ease and benefit from the enhanced