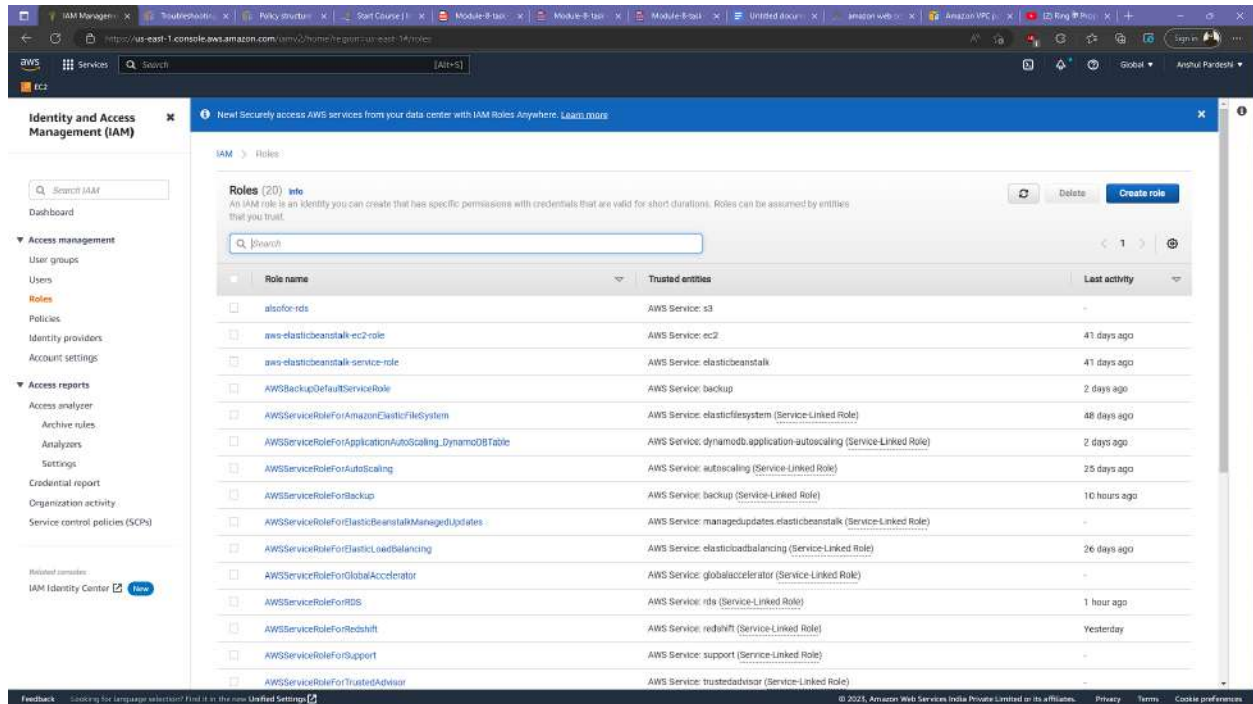


Module-8: IAM Assignment - 3

You have been asked to:

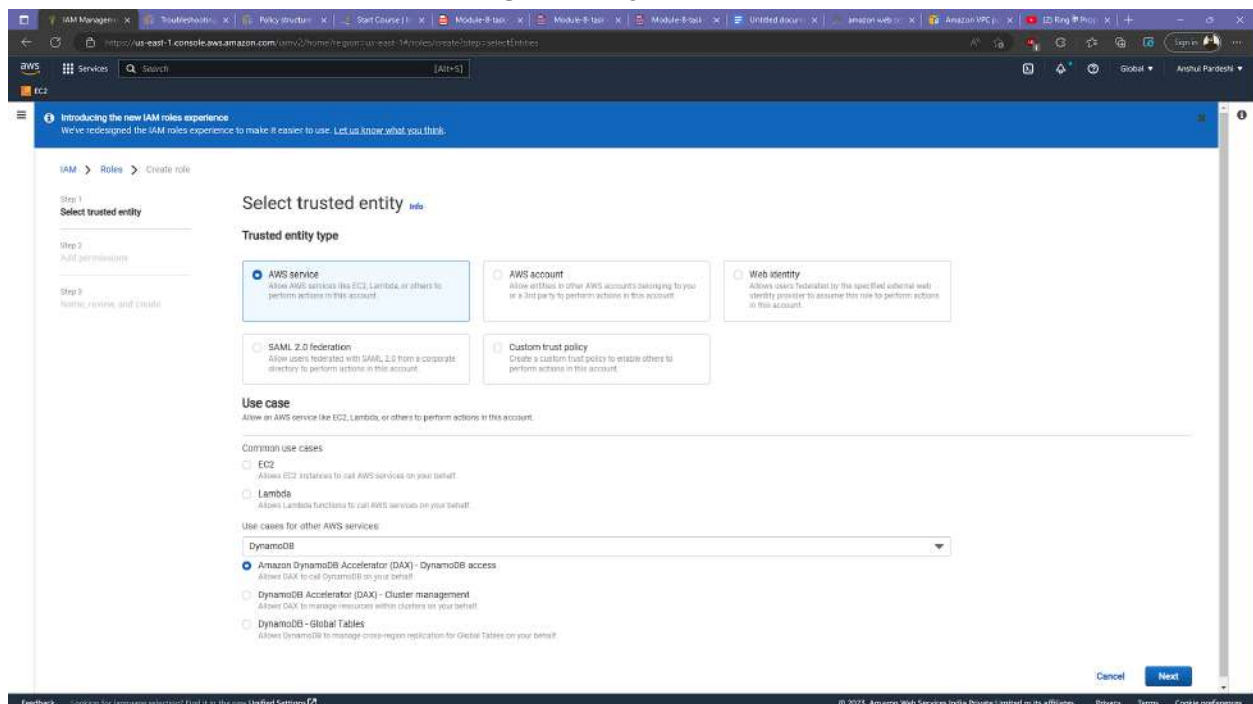
1. Create a Role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.
2. Login into user1 and shift to the role to test out the feature.

Create role



The screenshot shows the AWS IAM console 'Roles' page. A list of 20 roles is displayed, including 'alsofor-ids', 'aws-elasticbeanstalk-ec2-role', 'aws-elasticbeanstalk-service-role', 'AWSBackupDefaultServiceRole', 'AWSServiceRoleForAmazonElasticFileSystem', 'AWSServiceRoleForApplicationAutoScaling-DynamoDBTable', 'AWSServiceRoleForAutoScaling', 'AWSServiceRoleForBackup', 'AWSServiceRoleForElasticBeanstalkManagedUpdates', 'AWSServiceRoleForElasticLoadBalancing', 'AWSServiceRoleForGlobalAccelerator', 'AWSServiceRoleForRDS', 'AWSServiceRoleForRedshift', 'AWSServiceRoleForSupport', and 'AWSServiceRoleForTrustedAdvisor'. Each role entry shows its name, trusted entities, and last activity.

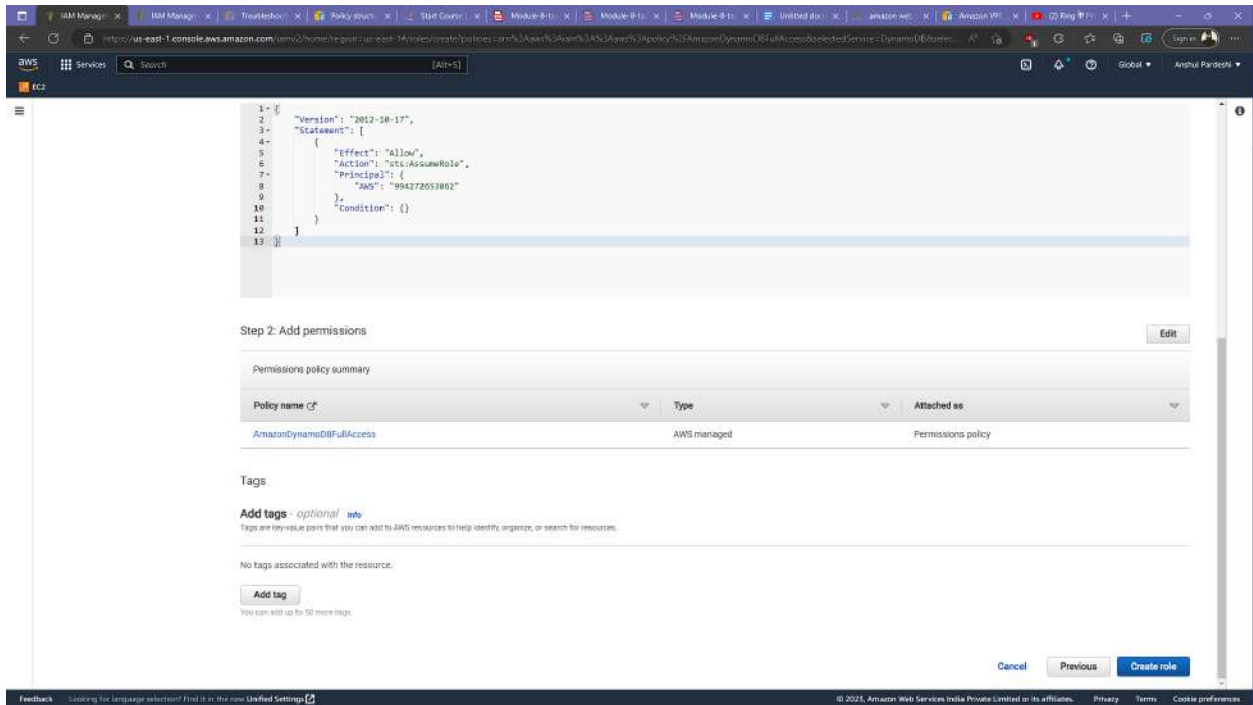
Let's go with dynamodb first.



The screenshot shows the 'Create role' wizard in the AWS IAM console, specifically Step 1: 'Select trusted entity'. The 'Trusted entity type' section has three options: 'AWS service' (selected), 'AWS account', and 'Web identity'. The 'AWS service' option is further detailed with 'Common use cases' (EC2, Lambda) and 'Use cases for other AWS services' (DynamoDB). Under 'DynamoDB', the 'Amazon DynamoDB Accelerator (DAX) - DynamoDB access' option is selected. The 'Next' button is visible at the bottom right.

[illegible][illegible]

Create role.



The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with 'IAM' and 'Roles' tabs. The main content area is titled 'Create role' and shows the 'Step 1: Select an AWS managed policy' screen. A search bar at the top of the policy list shows 'AmazonDynamoDBFullAccess'. The policy is listed with 'AWS managed' type and 'Permissions policy' attached. Below the policy list, there's a 'Tags' section with an 'Add tag' button. At the bottom, there are 'Cancel', 'Previous', and 'Create role' buttons.

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": "sts:AssumeRole",
7-       "Principal": {
8-         "AWS": "994272653862"
9-       },
10-      "Condition": {}
11-    }
12-  ]
13- }
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonDynamoDBFullAccess	AWS managed	Permissions policy

Tags

Add tags - optional

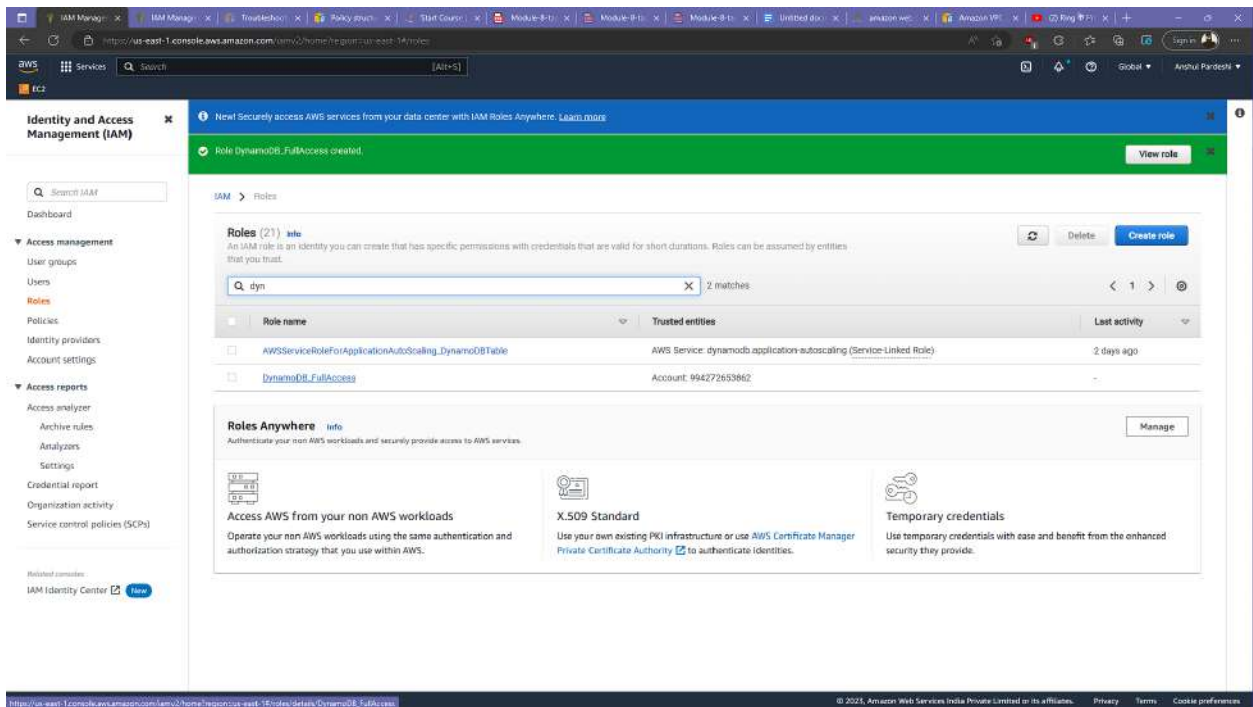
No tags associated with the resource.

Add tag

You can add up to 50 more tags.

Cancel Previous Create role

Role has been created.Open the role.



The screenshot shows the AWS IAM console interface. The left sidebar shows the 'Identity and Access Management (IAM)' section. The main content area is titled 'Roles' and shows a list of roles. The 'DynamoDB_FullAccess' role is highlighted. Below the list, there's a 'Roles Anywhere' section with three cards: 'Access AWS from your non AWS workloads', 'X.509 Standard', and 'Temporary credentials'. The 'DynamoDB_FullAccess' role is listed with 'Account: 994272653862' and 'Last activity'.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analysers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related services

- IAM Identity Center

New! Securely access AWS services from your data center with IAM Roles Anywhere. Learn more

Role DynamoDB_FullAccess created. View role

Roles (21)

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.

Search dyn 2 matches

Role name	Trusted entities	Last activity
AWSServiceRoleForApplicationAutoScaling-DynamoDBTable	AWS Service: dynamodb.applicationautoscaling (Service-Linked Role)	2 days ago
DynamoDB_FullAccess	Account: 994272653862	-

Roles Anywhere

Authenticate your own 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 authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Manage

Edit trust policy.

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 Related services. The main content area displays the 'DynamoDB_FullAccess' role's 'Trust relationships' tab. The 'Summary' section shows the role's creation date, last activity, and ARN. The 'Trusted entities' section displays a JSON policy document for the role.

Summary

Creation date: January 11, 2023, 22:04 (UTC+05:30)

Last activity: None

ARN: arn:aws:iam:994272653862:role/DynamoDB_FullAccess

Maximum session duration: 1 hour

Link to switch roles in console: https://signin.aws.amazon.com/switchrole?roleName=DynamoDB_FullAccess&account=994272653862

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam:994272653862:root"
8       },
9       "Action": "sts:AssumeRole",
10      "Condition": {}
11    }
12  ]
13 }
```

The screenshot shows the 'Edit trust policy' interface for the 'DynamoDB_FullAccess' role. The left sidebar contains navigation links for IAM, Roles, and Edit trust policy. The main content area displays the 'Edit trust policy' form. The 'JSON' tab is selected, showing the policy document. The 'Edit statement' panel on the right allows adding actions for STS, access level, and principal.

Edit trust policy

1 {
2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Effect": "Allow",
6 "Principal": {
7 "AWS": "arn:aws:iam:994272653862:root"
8 },
9 "Action": "sts:AssumeRole",
10 "Condition": {}
11 }
12]
13 }

Edit statement

1. Add actions for STS

Filter actions

Access level - read or write

☒ AssumeRole

☐ AssumeRoleWithSAML

☐ AssumeRoleWithWebIdentity

☐ DecodeAuthorizationMessage

☐ GetAccessKeyInfo

☐ GetCallerIdentity

☐ GetFederationToken

☐ GetServiceBearerToken

☐ GetSessionToken

☐ SetSourceIdentity

2. Add a principal

3. Add a condition (optional)

JSON Ln 7, Col 14

Security Errors Warnings Suggestions: 1

Preview external access

Copy users ARN.

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with options like Dashboard, Access management, User groups, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, and Service control policies (SCPs). The main content area displays the 'Summary' page for 'user1'. It shows the User ARN as 'arn:aws:iam::994272653862:user/user1', Path as '/', and Creation time as '2023-01-11 18:21 UTC+0530'. Under the 'Permissions' tab, it lists 'Permissions policies (5 policies applied)' with an 'Add permissions' button. A table shows 'Attached directly' with 'IAMUserChangePassword' as an 'AWS managed policy'. Below this, it says 'Attached from group' with a 'Show 4 more' link. There is also a section for 'Permissions boundary (not set)' and a 'Generate policy based on CloudTrail events' section with a 'Generate policy' button. A notification banner at the top mentions a new feature to generate a policy based on CloudTrail events.

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID: 994272653862

Summary

User ARN: arn:aws:iam::994272653862:user/user1

Path: /

Creation time: 2023-01-11 18:21 UTC+0530

Permissions

Groups (2)

Tags

Security credentials

Access Advisor

Permissions policies (5 policies applied)

Add permissions

Add inline policy

Policy name	Policy type
IAMUserChangePassword	AWS managed policy

Attached directly

Attached from group

Show 4 more

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

Share your feedback and help us improve the policy generation experience.

Generate policy

No requests to generate a policy in the past 7 days.

This screenshot shows the 'Summary' page for 'user2' in the AWS IAM console. The layout is identical to the first screenshot, but the User ARN is 'arn:aws:iam::994272653862:user/user2' and the 'Permissions policies' section shows '3 policies applied' instead of 5. The 'Attached directly' table still shows 'IAMUserChangePassword' as an 'AWS managed policy'. The 'Generate policy' button is still present, and the notification banner at the top remains the same.

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analysts

Settings

Credential report

Organization activity

Service control policies (SCPs)

Search IAM

AWS account ID: 994272653862

Summary

User ARN: arn:aws:iam::994272653862:user/user2

Path: /

Creation time: 2023-01-11 18:21 UTC+0530

Permissions

Groups (1)

Tags

Security credentials

Access Advisor

Permissions policies (3 policies applied)

Add permissions

Add inline policy

Policy name	Policy type
IAMUserChangePassword	AWS managed policy

Attached directly

Attached from group

Show 2 more

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

Share your feedback and help us improve the policy generation experience.

Generate policy

No requests to generate a policy in the past 7 days.

Paste it in this syntax so that those users are assigned with this role.

The screenshot shows the 'Edit trust policy' page in the AWS IAM console. The left pane displays the JSON policy document with line numbers 1 through 17. The right pane shows the 'Edit statement' interface with a list of actions for STS, including 'AssumeRoleWithWebIdentity', 'AssumeRoleWithSAML', 'DecodeAuthorizationMessage', 'GetAccessKeyInfo', 'GetCallerIdentity', 'GetFederationToken', 'GetServiceBearerToken', 'GetSessionToken', 'SetSourceIdentity', 'TagSession', and 'UntagSession'. The 'Add actions for STS' section is currently empty. Below the list, there are sections for '2. Add a principal' and '3. Add a condition (optional)', each with an 'Add' button. At the bottom, there are 'Cancel' and 'Update policy' buttons.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::994272653862:root",
9           "arn:aws:iam::994272653862:user/user2",
10          "arn:aws:iam::994272653862:user/user1"
11        ]
12      },
13      "Action": "sts:AssumeRole",
14      "Condition": {}
15    }
16  ]
17 }
```

The screenshot shows the 'Roles' page in the AWS IAM console. The left sidebar contains navigation links for 'Identity and Access Management (IAM)', 'Access management', 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Access reports', 'Access analyzer', 'Archive rules', 'Analyzers', 'Settings', 'Credential report', 'Organization activity', and 'Service control policies (SCPs)'. The main content area shows the details for the role 'DynamoDB_FullAccess'. It includes the creation date (January 11, 2023, 22:04 (UTC+05:30)), the ARN (arn:aws:iam::994272653862:role/DynamoDB_FullAccess), and the maximum session duration (1 hour). The 'Trust relationships' tab is selected, showing the 'Trusted entities' section with the JSON policy document. The 'Edit trust policy' button is visible in the top right corner of the 'Trusted entities' section.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": [
8           "arn:aws:iam::994272653862:root",
9           "arn:aws:iam::994272653862:user/user2",
10          "arn:aws:iam::994272653862:user/user1"
11        ]
12      },
13      "Action": "sts:AssumeRole",
14      "Condition": {}
15    }
16  ]
17 }
```


Create another role.

The screenshot shows the AWS IAM console 'Roles' page. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Related services. The main content area displays a list of 21 roles. At the top right, there are buttons for 'Delete' and 'Create role'. A search bar is located above the table.

Role name	Trusted entities	Last activity
alsofor-ids	AWS Service: s3	-
aws-elasticbeanstalk-ec2-role	AWS Service: ec2	41 days ago
aws-elasticbeanstalk-service-role	AWS Service: elasticbeanstalk	41 days ago
AWSBackupDefaultServiceRole	AWS Service: backup	2 days ago
AWSServiceRoleForAmazonElasticFilesystem	AWS Service: elasticfilesystem (Service-Linked Role)	48 days ago
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb application-autoscaling (Service-Linked Role)	2 days ago
AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	25 days ago
AWSServiceRoleForBackup	AWS Service: backup (Service-Linked Role)	10 hours ago
AWSServiceRoleForElasticBeanstalkManagedUpdates	AWS Service: managedupdates elasticbeanstalk (Service-Linked Role)	-
AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	26 days ago
AWSServiceRoleForGlobalAccelerator	AWS Service: globalaccelerator (Service-Linked Role)	-
AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	1 hour ago
AWSServiceRoleForRedshift	AWS Service: redshift (Service-Linked Role)	Yesterday
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

The screenshot shows the 'Create role' wizard in the AWS IAM console, specifically Step 1: Select trusted entity. The left sidebar shows the progress: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). The main content area is titled 'Select trusted entity' and includes a 'Trusted entity type' section with five options: AWS service (selected), AWS account, Web identity, SAML 2.0 federation, and Custom trust policy. Below this is a 'Use case' section with 'Common use cases' (EC2 selected, Lambda) and a dropdown for 'Use cases for other AWS services'. At the bottom right are 'Cancel' and 'Next' buttons.

Choose AmazonVPC FullAccess

The screenshot shows the 'Add permissions' step in the AWS IAM console. The breadcrumb navigation is 'IAM > Roles > Create role'. The left sidebar shows the progress: Step 1: Select trusted entity, Step 2: Add permissions (current), and Step 3: Name, review, and create. The main area is titled 'Add permissions' with a sub-header 'Permissions policies (Selected 1/807)'. Below this is a search bar with the text 'Filter policies by property or policy name and press enter:' and a '7 matches' indicator. A filter 'vpc' is applied, and a 'Clear filters' button is present. A table lists available policies:

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AmazonVPCReadOnlyAccess	AWS ma...	Provides read only access to Amazon VPC via the AWS Management Console.
<input type="checkbox"/>	AmazonVPCDMSAccountN...	AWS ma...	Provides access to create network interfaces and attach them to cross-account resources
<input checked="" type="checkbox"/>	AmazonVPCFullAccess	AWS ma...	Provides full access to Amazon VPC via the AWS Management Console.
<input type="checkbox"/>	AmazonDMSVPCManageme...	AWS ma...	Provides access to manage VPC settings for AWS managed customer configurations
<input type="checkbox"/>	AmazonDRSVPCManagement	AWS ma...	Provides access to manage VPC settings for Amazon managed customer configurations
<input type="checkbox"/>	AWSLambdaVPCAccessExec...	AWS ma...	Provides minimum permissions for a Lambda function to execute while accessing a resource within a VPC: create, describe, delete network interfaces and ...
<input type="checkbox"/>	AmazonEKSVPCResourceCo...	AWS ma...	Policy used by VPC Resource Controller to manage ENI and IPa for worker nodes.

Below the table, there is a section 'Set permissions boundary - optional' with a link to 'info'. It states: 'Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.'

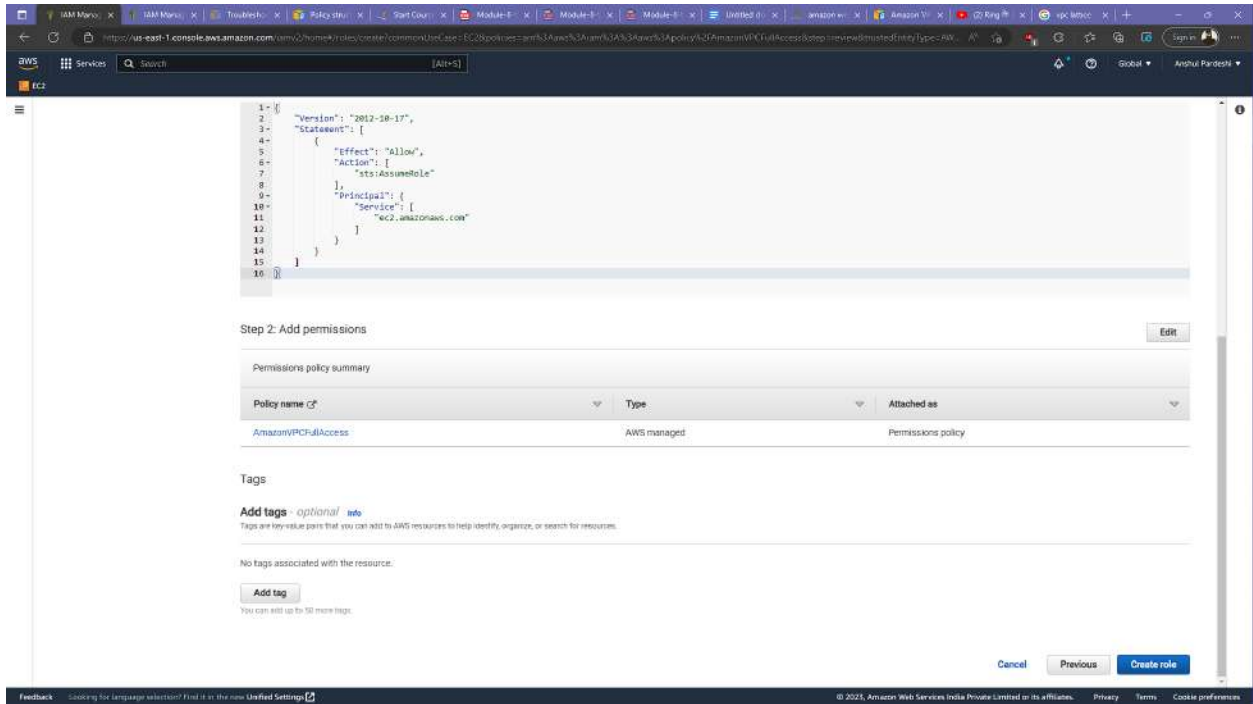
At the bottom right, there are buttons: 'Cancel', 'Previous', and 'Next'.

Create role.

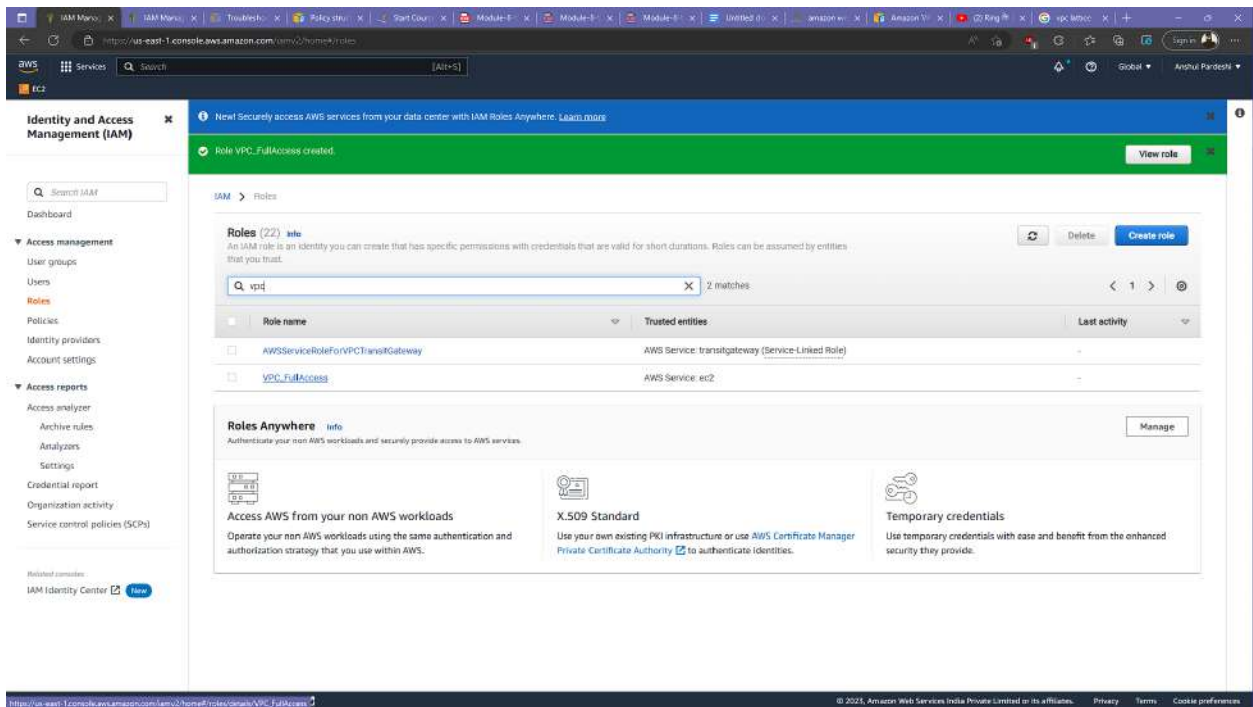
The screenshot shows the 'Step 2: Add permissions' screen in the AWS IAM console. The breadcrumb navigation is 'IAM > Roles > Create role'. The left sidebar shows the progress: Step 1: Select trusted entity, Step 2: Add permissions (current), and Step 3: Name, review, and create. The main area is titled 'Step 2: Add permissions' with an 'Edit' button. Below this is a section 'Permissions policy summary' with a table:

Policy name	Type	Attached as
AmazonVPCFullAccess	AWS managed	Permissions policy

Below the table, there is a section 'Tags' with a sub-header 'Add tags - optional'. It states: 'Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.' Below this, it says 'No tags associated with the resource.' and there is an 'Add tag' button. At the bottom right, there are buttons: 'Cancel', 'Previous', and 'Create role'.



Open the role.



Edit Trust Policy.

The screenshot shows the AWS IAM console with the 'Edit trust policy' page for the 'VPC_FullAccess' role. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Settings. The main content area displays the 'Summary' tab, which includes the role's ARN, creation date, and last activity. Below the summary, the 'Trusted entities' section shows a list of trusted entities, with the first entity being 'ec2.amazonaws.com'. The 'Edit trust policy' button is visible in the top right corner of the trusted entities section.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "allow",
6       "Principal": {
7         "Service": "ec2.amazonaws.com"
8       },
9       "Action": "sts:AssumeRole"
10    }
11  ]
12 }
```

Add both users using the same syntax.

The screenshot shows the AWS IAM console with the 'Edit trust policy' page for the 'VPC_FullAccess' role. The 'Add new statement' dialog is open, showing the '1. Add actions for STS' section. The 'AssumeRole' action is selected. The '2. Add a principal' section is also visible, showing the 'Add' button. The '3. Add a condition (optional)' section is also visible, showing the 'Add' button. The 'Update policy' button is visible at the bottom right of the dialog.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "allow",
6       "Principal": {
7         "Service": "ec2.amazonaws.com",
8         "AWS": [
9           "arn:aws:iam::994272653862:user/user1",
10          "arn:aws:iam::994272653862:user/user2"
11        ]
12      },
13      "Action": "sts:AssumeRole"
14    }
15  ]
16 }
```

Introducing the new IAM roles experience. We've redesigned the IAM roles experience to make it easier to use. [Let us know what you think.](#)

Trust policy updated.

VPC_FullAccess

VPC Full access for assignment.

Summary

Creation date January 11, 2023, 22:14 (UTC+05:30)	ARN <code>arn:aws:iam:994272653862:role/VPC_FullAccess</code>	Link to switch roles in console https://signin.aws.amazon.com/switchrole?roleName=~VPC_FullAccess&account=994272653862	Instance profile ARN <code>arn:aws:iam:994272653862:instance-profile/VPC_FullAccess</code>
Last activity None	Maximum session duration 1 hour		

Permissions | **Trust relationships** | Tags | Access Advisor | Revoke sessions

Trusted entities

Entities that can assume this role under specified conditions.

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "Service": "ec2.amazonaws.com",
8         "AWS": [
9           "arn:aws:iam:994272653862:user/user1",
10          "arn:aws:iam:994272653862:user/user2"
11        ]
12      },
13      "Action": "sts:AssumeRole"
14    }
15  ]
16 }
```

Feedback Loading for language selection? Find it in the new Unified Settings.

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Sign In with IAM User1.

Amazon Web Services Sign-In

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](#)

Account ID (12 digits) or account alias

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

[New to AWS?](#)

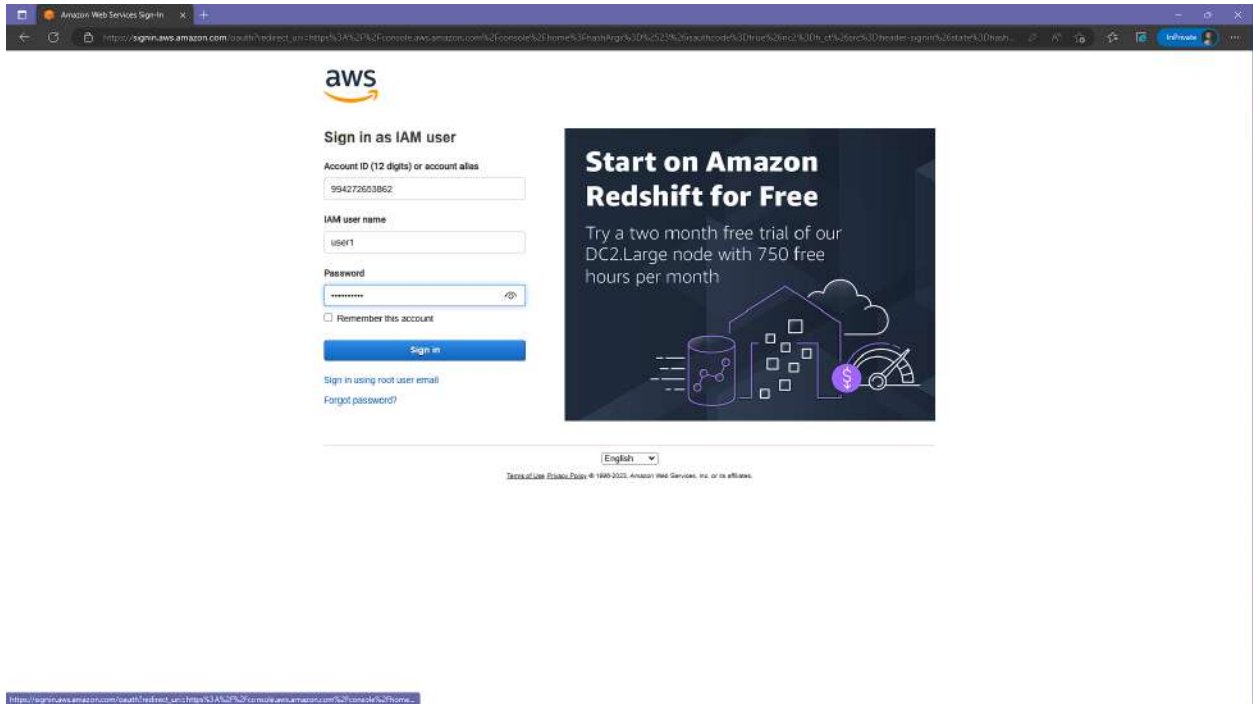
Create a new AWS account

Amazon Lightsail
Lightsail is the easiest way to get started on AWS

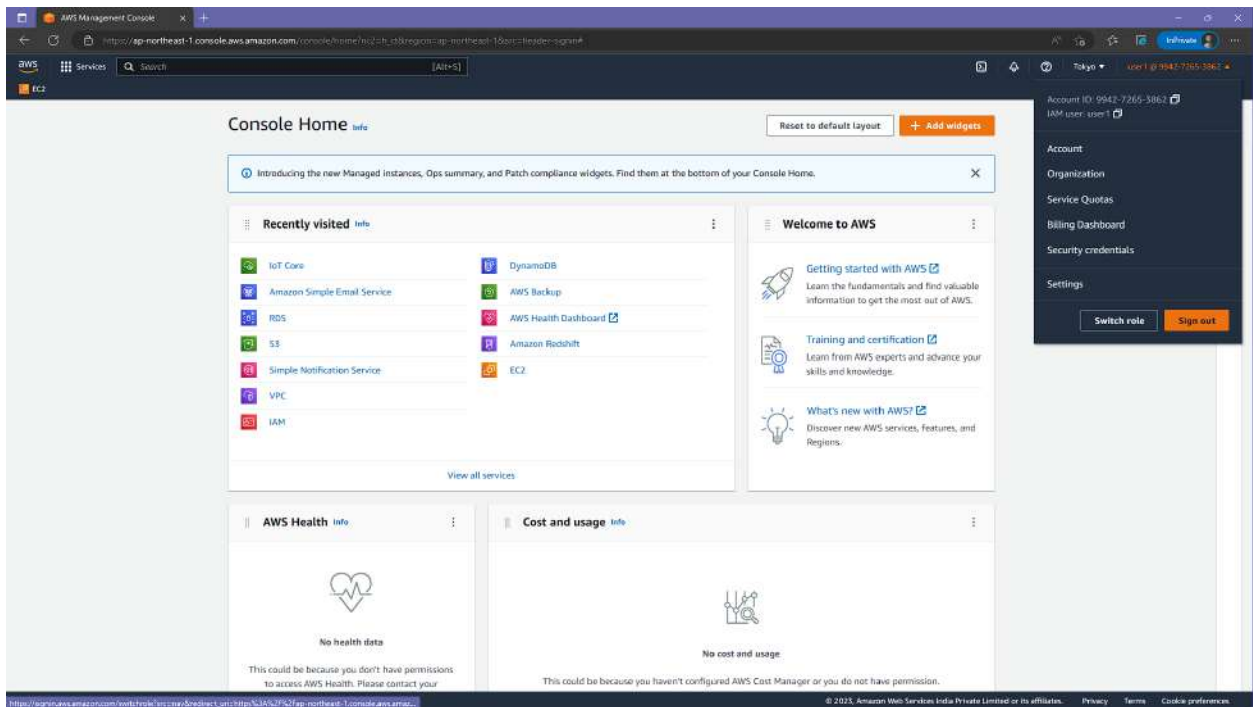
[LEARN MORE](#)

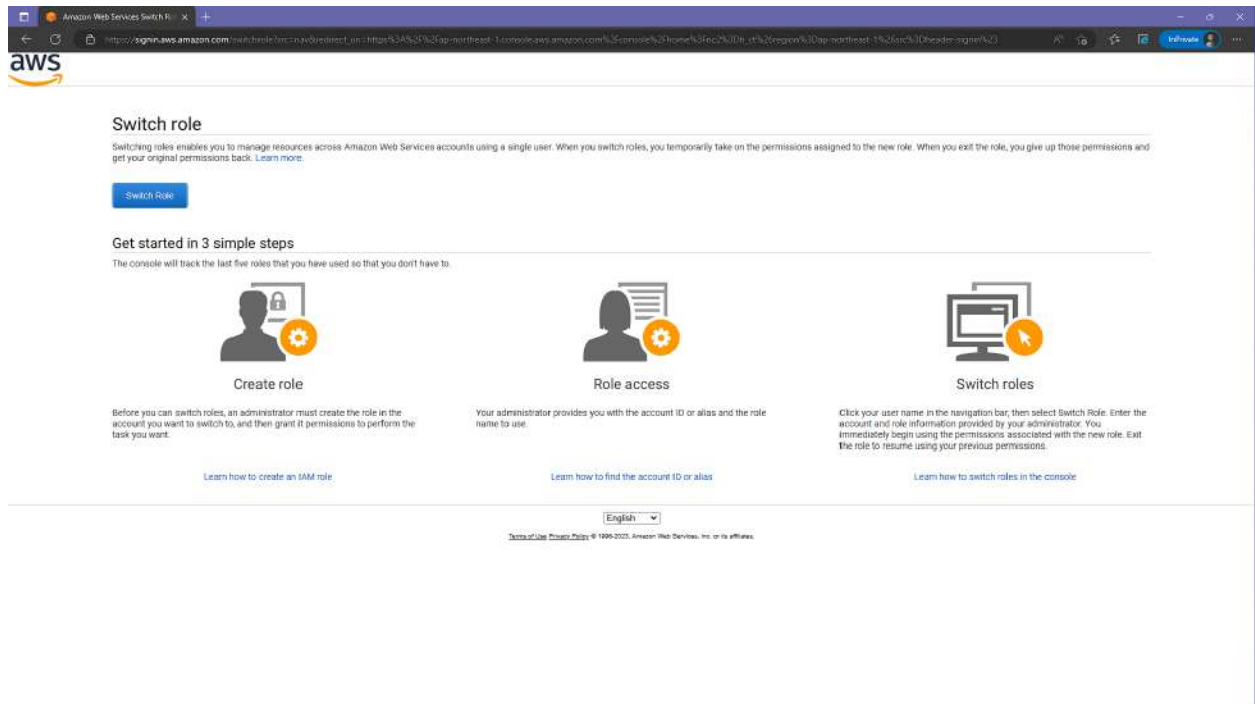
© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

English

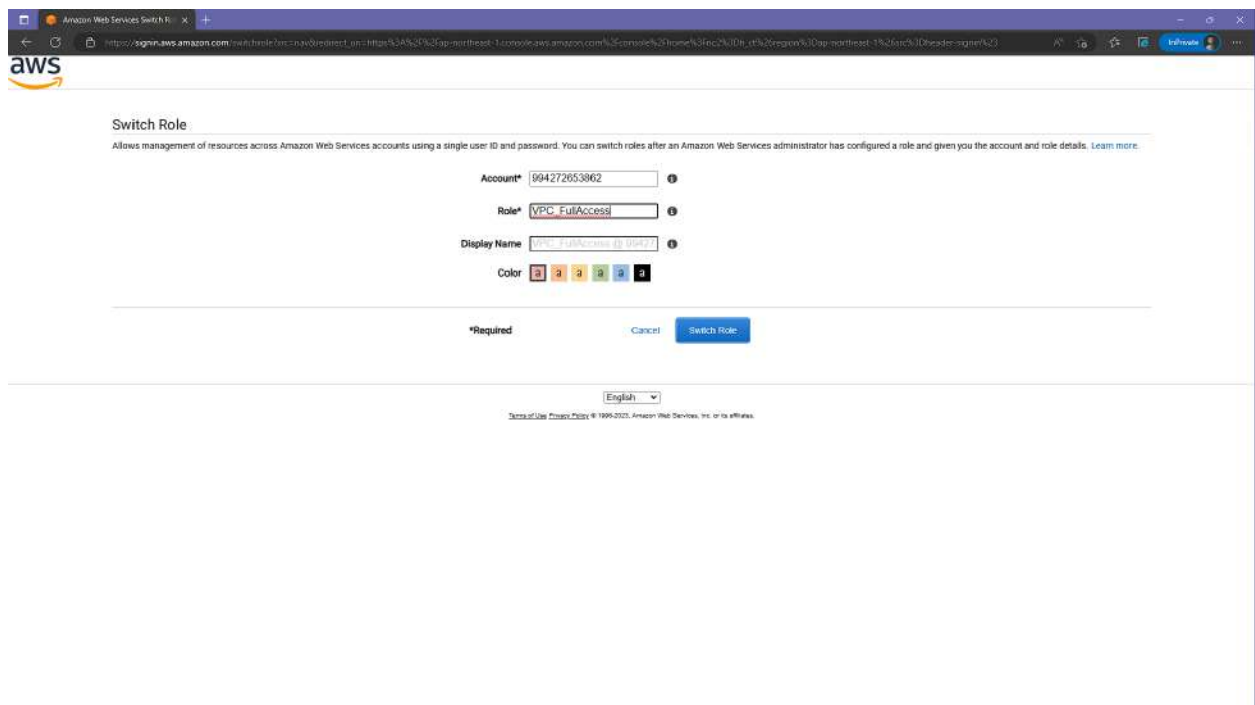


Switch role.

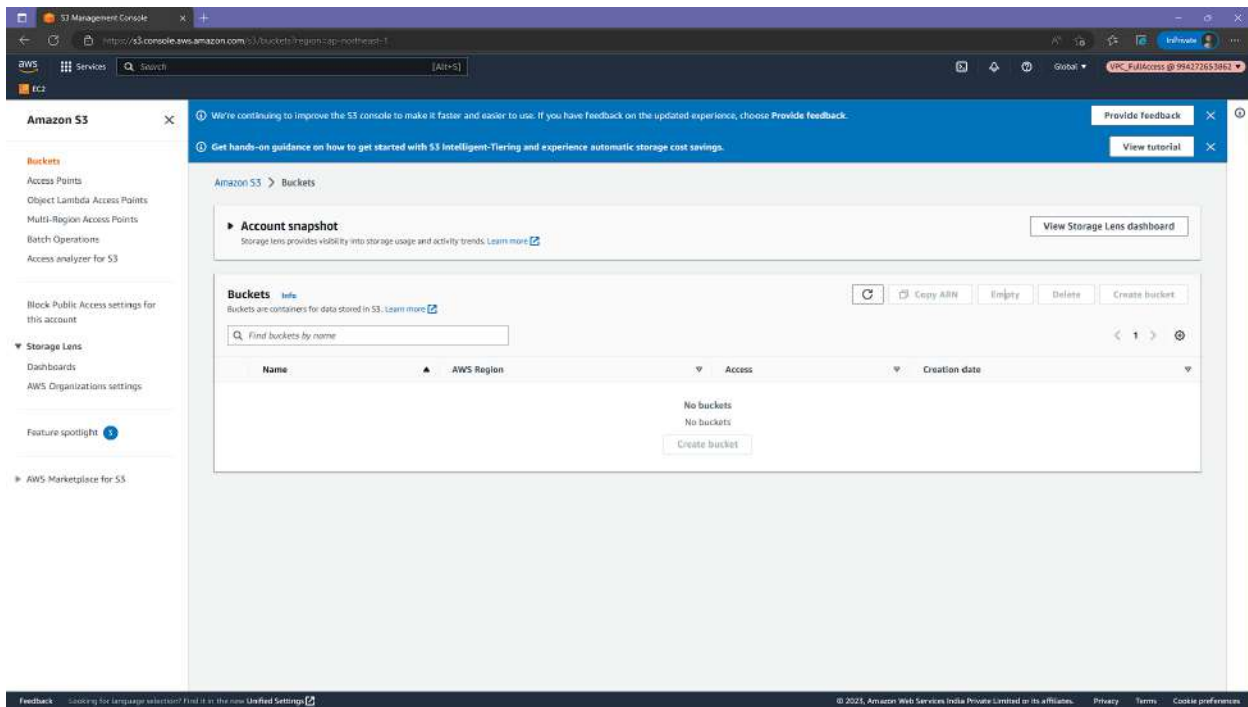




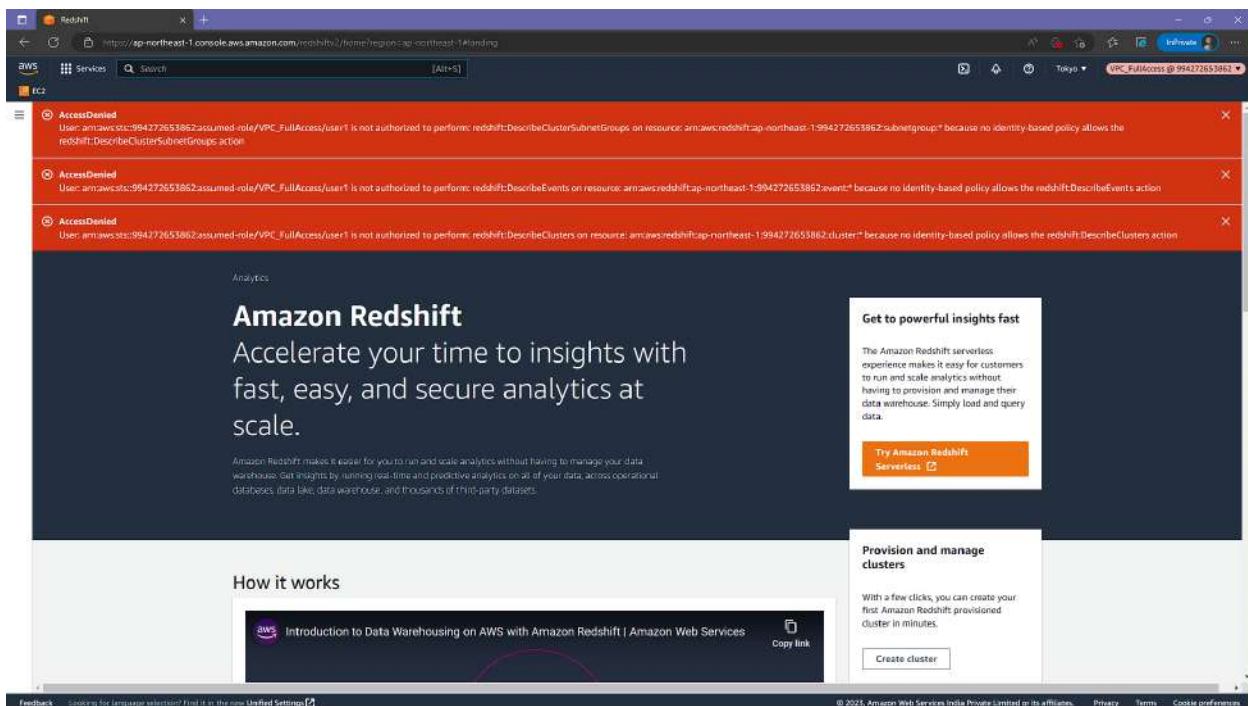
Paste Root user account ID and role name.



Role has been switched. You can't access s3 here.



Nor redshift.



But can access VPC due to the role.

Create VPC

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances. Mouse over a resource to highlight the related resources.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only

☒ VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)
Default

Number of Availability Zones (AZs) [Info](#)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1 2 3

Preview

Introducing the new create VPC experience
We've designed the new create VPC experience to make it easier to use. Now you can visualize the resources that will be created. Let us know what you think.

VPC [Show details](#)
Your AWS virtual network

VPC without Name tag

Subnets (4)
Subnets within this VPC

ap-northeast-1a

subnet-public1-ap-northeast-1a
subnet-private1-ap-northeast-1a

ap-northeast-1c

subnet-public2-ap-northeast-1c
subnet-private2-ap-northeast-1c

Route tables (3)
Route network traffic to resources

rtb-public
rtb-private1-ap-northeast-1a
rtb-private2-ap-northeast-1c

Network connection
Connections to other networks

igw
vpc-gs

Feedback Looking for language selection? Find it in the new [Unified Settings](#)

© 2025, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)