

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
-

https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles

AWS Services Global VAIBHAV VERMA

Identity and Access Management (IAM)

New! Securely access AWS services from your data center with IAM Roles Anywhere [Learn more](#)

IAM > Roles

Roles (13) 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.

Create role

Role name	Trusted entities	Last activity
AWSBackupDefaultServiceRole	AWS Service backup	9 days ago
AWSServiceRoleForAmazonElasticFileSystem	AWS Service elasticfilesystem (Service-Linked Role)	59 days ago
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service dynamodb application autoscaling (Service-Linked Role)	9 days ago
AWSServiceRoleForAutoScaling	AWS Service autoscaling (Service-Linked Role)	12 days ago
AWSServiceRoleForBackup	AWS Service backup (Service-Linked Role)	11 hours ago
AWSServiceRoleForCloudWatchEvents	AWS Service events (Service-Linked Role)	-
AWSServiceRoleForRDS	AWS Service rds (Service-Linked Role)	40 minutes ago
AWSServiceRoleForRedshift	AWS Service redshift (Service-Linked Role)	7 days ago
AWSServiceRoleForSupport	AWS Service support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service trustedadvisor (Service-Linked Role)	-
demo-role-lambda-ec2-cloudwatch-01-10-2022	AWS Service lambda	19 days ago
demo-role-s3-lambda1-29-09-2022	AWS Service lambda	20 days ago

Search

1 / 1

Access management

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

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings

Credential report

Organization activity

Service control policies (SCPs)

Related consoles

IAM Identity Center [New](#)

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

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

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.](#)

IAM > Roles > Create role

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

Select trusted entity Info

Trusted entity type

AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account

AWS account

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

Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account

SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

```
1 = {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Principal": {},  
8       "Action": "sts:AssumeRole"  
9     }  
10   ]  
11 }
```

Edit statement
Statement1

Remove

1. Add actions for STS

Filter actions

All actions (sts *)

Access level - read or write

AssumeRole ?

Services [Alt+S] Global ▾ VAIBHAV VERMA ▾

Identity and Access Management (IAM)

Users > user1

Summary

User ARN: arn:aws:iam::111952067877:user/user1

Path: /

Creation time: 2022-10-19 14:35 UTC+0530

Permissions Groups (2) Tags Security credentials Access Advisor

▼ Permissions policies (2 policies applied)

Add permissions

Policy name	Policy type
Attached from group	Managed policy from group DevTeam
▶ PolicyNumber1	
▶ PolicyNumber2	
▶ 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 activities to generate a policy in the last 7 days.

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

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Identity and Access Management (IAM)

Users > user2

Summary

[Delete user](#)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

User ARN arn:aws:iam::111952067877:user/user2

Path



Creation time 2022-10-19 14:35 UTC+0530

[Permissions](#) [Groups \(1\)](#) [Tags](#) [Security credentials](#) [Access Advisor](#)

▼ Permissions policies (1 policy applied)

[Add permissions](#)[Add inline policy](#)

Policy name ▾

Policy type ▾

Attached from group

▶ PolicyNumber1

Managed policy from group DevTeam



▶ 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

```
1 {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "Statement1",
6             "Effect": "Allow",
7             "Principal": {
8                 "AWS": [
9                     "arn:aws:iam::111952067877:user/user1",
10                    "arn:aws:iam::111952067877:user/user2"
11                ]
12            },
13            "Action": "sts:AssumeRole"
14        }
15    ]
16 }
17 }
```

[+ Add new statement](#)

JSON Ln 10. Col 48

Edit statement
Statement1 Remove

1. Add actions for STS

 Filter actions All actions (sts:*)

Access level - read or write

 AssumeRole i AssumeRoleWithSAML i AssumeRoleWithWebIdentity i DecodeAuthorizationMessage i GetAccessKeyInfo i GetCallerIdentity i GetFederationToken i GetServiceBearerToken i GetSessionToken i SetSourceIdentity i

2. Add a principal

[Add](#)

3. Add a condition (optional)

[Add](#)[Preview external access](#)

s experience

s experience to make it easier to use. [Let us know what you think.](#)

Add permissions Info

Permissions policies (Selected 2/776) Info

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

[Create policy](#)

< 1 >

Filter policies by property or policy name and press enter

4 matches

"Dynamodb"

[Clear filters](#)

<input type="checkbox"/>	Policy name	Type	Description
<input checked="" type="checkbox"/>	AmazonDynamoDBFullAccess	AWS managed policy	Provides full access to Amazon DynamoDB via the AWS Management Console.
<input type="checkbox"/>	AWSLambdaDynamoDBExecutionRole	AWS managed policy	Provides list and read access to DynamoDB streams and write permissions to CloudWatch logs.
<input type="checkbox"/>	AmazonDynamoDBReadOnlyAccess	AWS managed policy	Provides read only access to Amazon DynamoDB via the AWS Management Console.
<input type="checkbox"/>	AWSLambdaInvocation-DynamoDB	AWS managed policy	Provides read access to DynamoDB Streams.

► Set permissions boundary - optional Info

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.

[Cancel](#)

[Previous](#)

[Next](#)

AM roles experience

AM roles experience to make it easier to use. [Let us know what you think.](#)

Create role

Add permissions [Info](#)Permissions policies (Selected 2/776) [Info](#)

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

Create policy [Edit](#) Filter policies by property or policy name and press enter.

7 matches

< 1 >

 "vpc" [Clear filters](#)

Policy name	Type	Description
AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon VPC via the AWS Management Console.
AmazonVPCCrossAccountNetworkInterfaceOperat...	AWS managed	Provides access to create network interfaces and attach them to cross-account resources
<input checked="" type="checkbox"/> AmazonVPCFullAccess	AWS managed	Provides full access to Amazon VPC via the AWS Management Console
AmazonDMSVPCManagementRole	AWS managed	Provides access to manage VPC settings for AWS managed customer configurations
AmazonDRSVPCTManagement	AWS managed	Provides access to manage VPC settings for Amazon managed customer configurations
AWSLambdaVPCAccessExecutionRole	AWS managed	Provides minimum permissions for a Lambda function to execute while accessing a resource within a VPC
AmazonEKSVPCResourceController	AWS managed	Policy used by VPC Resource Controller to manage ENI and IPs for worker nodes.

▶ Set permissions boundary - optional [Info](#)

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.

<input type="checkbox"/>	PolicyNumber1	Custom...	
<input type="checkbox"/>	PolicyNumber2	Custom...	
<input type="checkbox"/>	AWSDirectConnectReadOnlyAccess	AWS m	Provides read only access to AWS Direct Connect via the AWS Management Console.
<input type="checkbox"/>	AmazonGlacierReadOnlyAccess	AWS m	Provides read only access to Amazon Glacier via the AWS Management Console.
<input type="checkbox"/>	AWSMarketplaceFullAccess	AWS m	Provides the ability to subscribe and unsubscribe to AWS Marketplace software, allows users to manage...
<input type="checkbox"/>	AWSSSOAdministrator	AWS m	Administrator access for SSO Directory
<input checked="" type="checkbox"/>	AWSIoT1ClickReadOnlyAccess	AWS m	Provides read only access to AWS IoT 1-Click
<input type="checkbox"/>	AutoScalingConsoleReadOnlyAccess	AWS m	Provides read-only access to Auto Scaling via the AWS Management Console.
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS m	Provides access to manage S3 settings for Redshift endpoints for DMS.
<input type="checkbox"/>	AWSQuickSightListIAM	AWS m	Allow QuickSight to list IAM entities
<input type="checkbox"/>	AWSHealthFullAccess	AWS m	Allows full access to the AWS Health APIs and Notifications and the Personal Health Dashboard
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS m	Provide gateway execution access to AlexaForBusiness services
<input type="checkbox"/>	AmazonElasticTranscoder_ReadOnlyAccess	AWS m	Grants users read-only access to Elastic Transcoder and list access to related services
<input type="checkbox"/>	AmazonRDSFullAccess	AWS m	Provides full access to Amazon RDS via the AWS Management Console.

▶ Set permissions boundary - optional Info

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.

Cancel

Previous

Next

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role

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

Description

Add a short explanation for this role

Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters

Step 1: Select trusted entities

[Edit](#)

```
1+ {
2+     "Version": "2012-10-17",
3+     "Statement": [
4+         {
5+             "Sid": "Statement1",
6+             "Effect": "Allow",
7+             "Principal": {
8+                 "AWS": [
9+                     "arn:aws:iam::111952067877:user/user1",
10+                    "arn:aws:iam::111952067877:user/user2"
11+                ]
12+            },
13+            "Action": "sts:AssumeRole"
14+        }
15+    ]
}
```

```
11      ]
12      },
13      "Action": "sts:AssumeRole"
14    }
15  ]
16 }
```

Step 2: Add permissions

[Edit](#)

Permissions policy summary

Policy name	Type	Attached as
AmazonVPCFullAccess	AWS managed	Permissions policy
AmazonDynamoDBFullAccess	AWS managed	Permissions policy

Tags

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource

[Add tag](#)

You can add up to 50 more tags

[Cancel](#)[Previous](#)[Create role](#)

New! Securely access AWS services from your data center with IAM Roles Anywhere. [Learn more](#)

✓ Role VPC+DynamoDB created.

[View role](#)

IAM > Roles

Roles (14) 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

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSBackupDefaultServiceRole	AWS Service: backup	9 days ago
<input type="checkbox"/>	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Service-Linked Role)	59 days ago
<input type="checkbox"/>	AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb application-autoscaling (Service-Linked Role)	9 days ago
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	12 days ago
<input type="checkbox"/>	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked Role)	12 hours ago
<input type="checkbox"/>	AWSServiceRoleForCloudWatchEvents	AWS Service: events (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	1 hour ago
<input type="checkbox"/>	AWSServiceRoleForRedshift	AWS Service: redshift (Service-Linked Role)	7 days ago
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-



...



Global ▾

VAIBHAV VERMA ▾

Account ID: 1119-5206-7877

Account

Organization

Service Quotas

Billing Dashboard

Security credentials

Settings



AWS Account

Account ID

1119520678



Account Alias

111952067877

Sign-in URL for

https://1119

m/console

Identity providers

0

Quick Links

[My security credentials](#)

Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

[Policy simulator](#)

The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify

[Web Identity federation playground](#)

Authenticate yourself to any of the supported web identity providers, see the requests and



[Sign in](#)

Root user

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

IAM user

User within an account that performs daily tasks

Account ID (12 digits) or account alias

111952067877

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

© 2022 Amazon Web Services, Inc. or its affiliates. All rights reserved.

English





Sign in as IAM user

Account ID (12 digits) or account alias

111952067877

IAM user name

user1

Password

.....

Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Build event-driven architectures on AWS

Take a deep dive into how EDAs help organizations increase agility and build reliable, scalable applications

[Download the guide >](#)



English ▾

[Terms of Use](#) [Privacy Policy](#) © 1996-2022 Amazon Web Services, Inc. or its affiliates.

Console Home Info

[Reset to default layout](#)

[+ Add widgets](#)



Recently visited Info

- [VPC](#)
- [Lambda](#)
- [Support](#)
- [RDS](#)
- [CloudWatch](#)
- [AWS Backup](#)
- [DynamoDB](#)

- [Amazon Redshift](#)
- [S3](#)
- [EC2](#)
- [CloudFormation](#)
- [AWS Budgets](#)
- [IAM](#)

[View all services](#)

Welcome to AWS



Getting started with AWS

Learn the fundamentals and find valuable information to get the most out of AWS.



Training and certification

Learn from AWS experts and advance your skills and knowledge.



What's new with AWS?

Discover new AWS services, features, and Regions.

AWS Health Info



No health data

Cost and usage Info



No cost and usage

This could be because you don't have permission.

Create VPC

Launch EC2 Instances

Note: Your Instances will launch in the US East region.

Resources by Region Refresh Resources

You are using the following Amazon VPC resources

VPCs See all regions ▾	US East 1	NAT Gateways See all regions ▾	US East 0
Subnets See all regions ▾	US East 6	VPC Peering Connections See all regions ▾	US East 0
Route Tables See all regions ▾	US East 1	Network ACLs See all regions ▾	US East 1
Internet Gateways See all regions ▾	US East 1	Security Groups See all regions ▾	US East 7
Egress-only Internet Gateways See all regions ▾	US East 0	Customer Gateways See all regions ▾	US East 0
DHCP option sets See all regions ▾	US East 1	Virtual Private Gateways See all regions ▾	US East 0
Elastic IPs See all regions ▾	US East 0	Site-to-Site VPN Connections See all regions ▾	US East 0
Endpoints See all regions ▾	US East 0	Running Instances See all regions ▾	US East 0

Service Health

Current Status	Details
 Amazon EC2 - US East	Service is operating normally

Settings

Zones

Console Experiments

Additional Information

VPC Documentation
All VPC Resources
Forums
Report an Issue

AWS Network Manager

AWS Network Manager centrally manages your Cloud WAN core network and your Transit Gateway network across AWS and on-premises locations. [Learn more](#)

Get started with Network Manager

Site-to-Site VPN Connections

Amazon VPC enables you to use your own isolated resources within the AWS Cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted Psec VPN connections.

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

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 - optional

Creates a tag with a key of 'Name' and a value that you specify.

MyVPC

IPv4 CIDR block Info

IPv4 CIDR manual input

IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

IPv6 CIDR block Info

No IPv6 CIDR block

IPAM-allocated IPv6 CIDR block

Amazon-provided IPv6 CIDR block

IPv6 CIDR owned by me

Tenancy Info

Default

aws

Services



MyVPC

IPv4 CIDR block [Info](#)

- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

IPv6 CIDR block [Info](#)

- No IPv6 CIDR block
- IPAM-allocated IPv6 CIDR block
- Amazon-provided IPv6 CIDR block
- IPv6 CIDR owned by me

Tenancy [Info](#)

Default

Tags

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.

Key

Value - optional

 Name X MyVPC XRemoveAdd new tag

You can add 49 more tags.

CancelCreate VPC

There was an error creating your VPC

You are not authorized to perform this operation. Encoded authorization failure message: e5W_gqLJDcj-SzTbVDLNPI8XeZ7ZWfedvYQpTv-kD7kirObLqF99gLfadE2BW1GdJpbCfPjOfjf3ElkPq93Fy0vdD5SXn64CAAQP8QornCQo2NX673aj0V7zpGuTwMWStEfmycBMSeFe7-W6MfNVEBBKbHG7VqGmIn-9b0nvUugiSpXYIIAOagVVFFxYv689ADqg01NpxWOgfwe7oH6Y_-PlvN87AQ6qVZjQT5PeMcvQS3YY22DCMZ4gQwYKNN-Eb-9WICOOQoz67fNv-X11VIY-bfls3jL7FdTZqOYHWT_qBbCfUAQ7kG8k1Xy1dQy2v4oHGYHm_O7AVuIYxltz17oTWLqjFZAYSELWFpgdcBVSBXM86-IlbgTHbA0A1mCElj42RdwQtJYBkOPTZ1JJ8yQmfZGLjmISm41tqYFYRAAnKwGyOUjM6ckn1_go_awcJJGA9WaLnYGSZqrWatMNsyRezu7yyHxuad6obml3XbfaA5-uUQBmVQ

[VPC](#) > [Your VPCs](#) > [Create VPC](#)

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

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 - optional

Creates a tag with a key of 'Name' and a value that you specify.

 MyVPC

IPv4 CIDR block Info

 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

IPv4 CIDR

 10.0.0.0/16

IPv6 CIDR block Info

 No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block



N. Virginia ▾

user1 @ 1119-5206-7877 ▾

Account ID: 1119-5206-7877

IAM user: user1

XYlIAOagVVFfxYv689ADqg01NpxWOGfv
AYSELWFpgdcBVSbXM86-

Account

Organization

Service Quotas

Billing Dashboard

Security credentials

Settings

[Switch role](#)



[Sign out](#)



Switch role

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

[Switch Role](#)

Get started in 3 simple steps

The console will track the last five roles that you have used so that you don't have to.



Create role

Before you can switch roles, an administrator must create the role in the account you want to switch to, and then grant it permissions to perform the task you want.

[Learn how to create an IAM role](#)



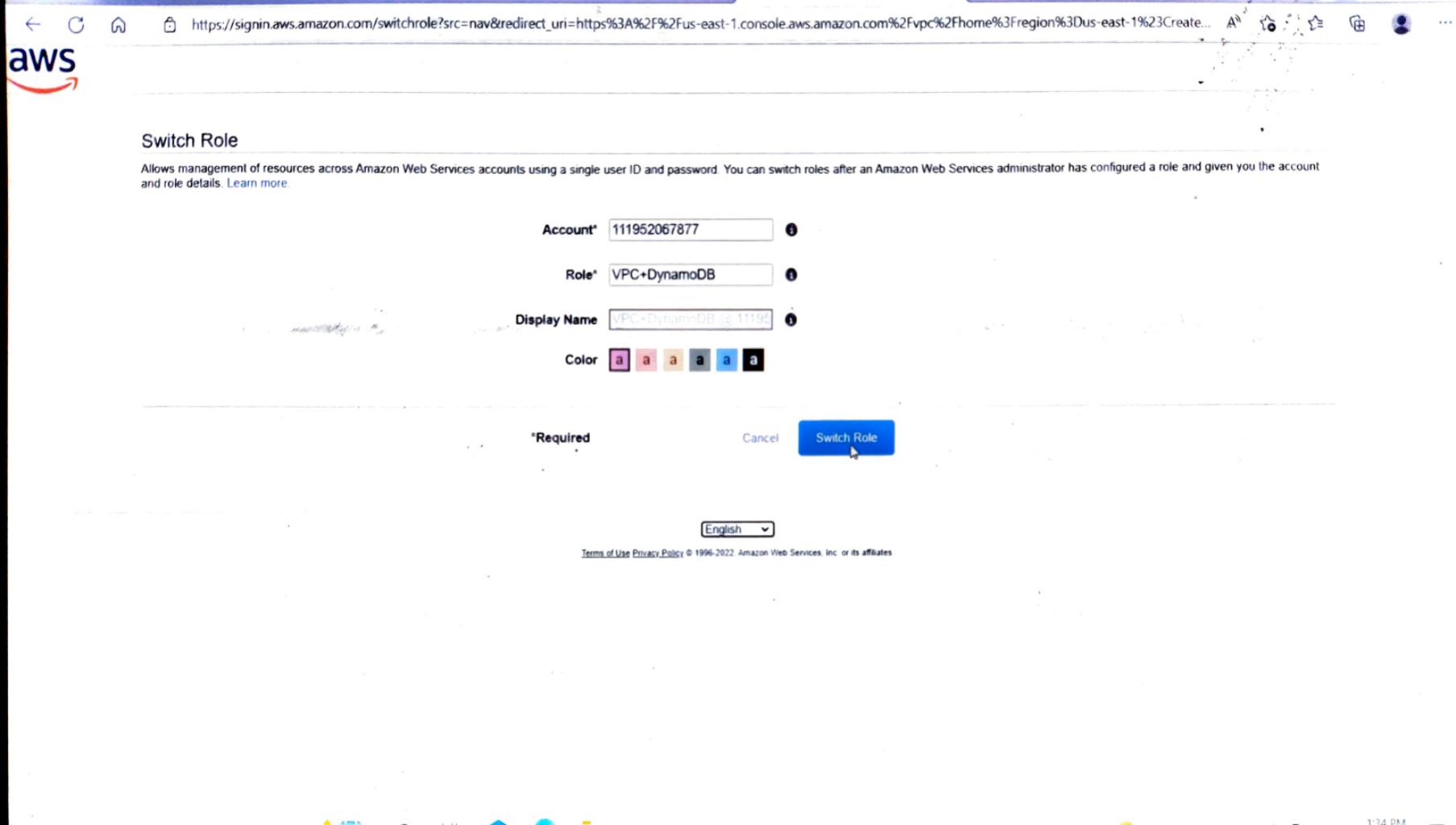
Role access

Your administrator provides you with the account ID or alias and the role name to use.

[Learn how to find the account ID or alias](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2022 Amazon Web Services, Inc. or its affiliates.



Create VPC

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

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 - optional

Creates a tag with a key of 'Name' and a value that you specify.

my-voc-01

IPv4 CIDR block Info

- IPv4 CIDR manual input
 - IPAM-allocated IPv4 CIDR block

IPv4 CIDR

Py6 CIDR block info

- No IPv6 CIDR block
 - IPAM-allocated IPv6 CIDR block
 - Amazon-provided IPv6 CIDR block
 - IPv6 CIDR owned by me

Tenancy info

Default

VPC > Your VPCs > Create VPC

Create VPC

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

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 - optional

Creates a tag with a key of 'Name' and a value that you specify.

MyVPC-01

IPv4 CIDR block [Info](#)

- IPv4 CIDR manual input
- IPAM allocated IPv4 CIDR

IPv4 CIDR

10.000/15

IPv6 CIDR block info

- No IPv6 CIDR block
- IPAM-allocated IPv6 CIDR block
- Amazon-provided IPv6 CIDR block
- IPv6 CIDR owned by me

Tenancy Info

Default

MyVPC-01

IPv4 CIDR block

- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

IPv6 CIDR block

- No IPv6 CIDR block
- IPAM-allocated IPv6 CIDR block
- Amazon-provided IPv6 CIDR block
- IPv6 CIDR owned by me

Tenancy

Default

Tags

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.

Key

Name

Value - optional

MyVPC-01

Remove

Add new tag

You can add 49 more tags.

Cancel

Create VPC

✓ You successfully created **vpc-076633a58c26259dc / MyVPC-01**

VPC > Your VPCs > vpc-076633a58c26259dc

vpc-076633a58c26259dc / MyVPC-01

Actions ▾

Details Info

VPC ID	vpc-076633a58c26259dc	State	Available	DNS hostnames	Disabled	DNS resolution	Enabled
Tenancy		DHCP option set	dopt-05eb69ee65ff0b1cf	Main route table	rtb-0f88881706df42ad2	Main network ACL	acl-009223c6f07bfca03
Default	No	Default VPC	IPv4 CIDR 10.0.0.0/16	IPv6 pool	-	IPv6 CIDR (Network border group)	-
Network mapping unit metrics	Disabled	Route 53 Resolver DNS Firewall rule groups	Failed to load rule groups	Owner ID	111952067877		

CIDRs Flow logs Tags

CIDRs Info

Address type	CIDR	Network Border Group	Pool	Status
IPv4	10.0.0.0/16	-	-	Associated

✓ You successfully created **vpc-076633a58c26259dc / MyVPC-01**

VPC > Your VPCs > **vpc-076633a58c26259dc**

vpc-076633a58c26259dc / MyVPC-01

Actions ▾

Details Info

VPC ID	<input checked="" type="checkbox"/> vpc-076633a58c26259dc	State	<input checked="" type="checkbox"/> Available	DNS hostnames	Disabled	DNS resolution	Enabled
Tenancy		DHCP option set		Main route table		Main network ACL	
Default		dopt-05eb69ee65ff0b1cf		rtb-0f88881706df42ad2		acl-009223c6f07bfca03	
Default VPC		IPv4 CIDR		IPv6 pool		IPv6 CIDR (Network border group)	
No		10.0.0.0/16		—		—	
Network mapping unit metrics		Route 53 Resolver DNS Firewall rule groups		Owner ID			
Disabled		✗ Failed to load rule groups		<input checked="" type="checkbox"/> 111952067877			

CIDRs Flow logs Tags

CIDRs Info

Address type	CIDR	Network Border Group	Pool	Status
IPv4	10.0.0.0/16	—	—	✓ Associated

Your VPCs (2) [Info](#)

Actions ▾

Create VPC



Filter VPCs

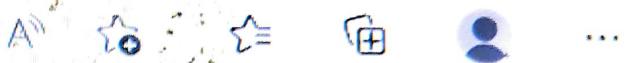
< 1 >



<input type="checkbox"/> Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table
<input type="checkbox"/> MyVPC-01	vpc-076633a58c26259dc	<input checked="" type="radio"/> Available	10.0.0.0/16	-	dopt-05eb69ee65ff0b...	rtb-0f8e...
<input type="checkbox"/> -	vpc-0b03f01cba75ff067	<input checked="" type="radio"/> Available	172.31.0.0/16	-	dopt-05eb69ee65ff0b...	rtb-090...

Select a VPC above





N. Virginia

VPC+DynamoDB @ 111952067877



...

v4 CIDR

0.0.0.0/16

72.31.0.0/16

IPv6 CIDR

-

-

Currently active as: VPC+DynamoDB

Account ID: 1119-5206-7877

Account

Organization

Service Quotas

Billing Dashboard

Settings

Signed in as: user1

Account ID: 1119-5206-7877

[Switch back](#)

Role histo

user1 @ 1119-5206-7877

 VPC+DynamoDB @ 111952067877[Switch role](#)[Sign out](#)