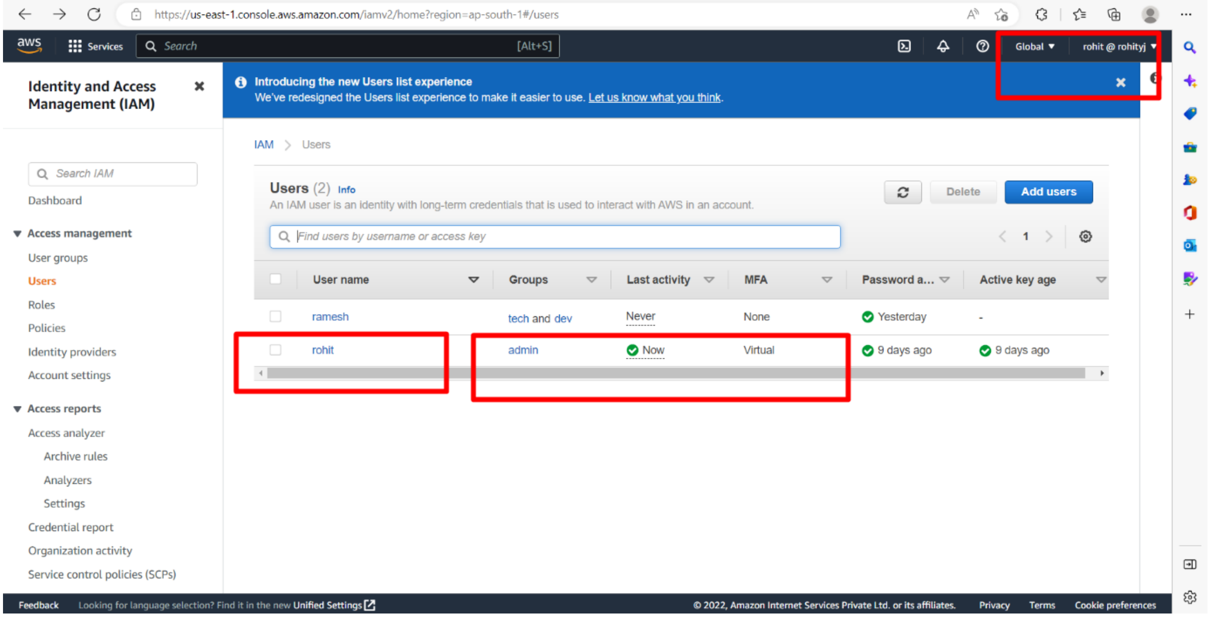
Assignment sheet for IAM

Assignment 1: -

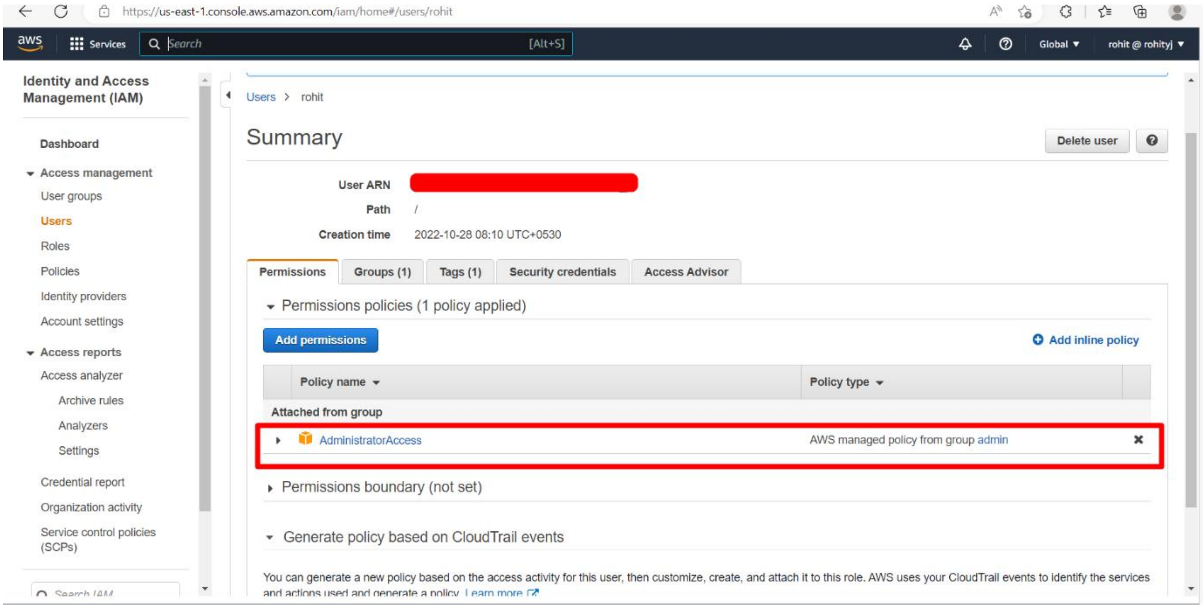
Create an IAM user with username of your own wish and grant administrator policy.


https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users
aws
Services
Search
[Alt+S]
Global
rohit @ rohityj
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
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > Users
Delete
Add users
Find users by username or access key
1
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 Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.

Users (2) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Groups	Last activity	MFA	Password a...	Active key age
ramesh	tech and dev	Never	None	✓ Yesterday	-
rohit	admin	✓ Now	Virtual	✓ 9 days ago	✓ 9 days ago



Summary

User ARN [redacted]
Path /
Creation time 2022-10-28 08:10 UTC+0530

Permissions policies (1 policy applied)

Policy name	Policy type
Attached from group	
AdministratorAccess	AWS managed policy from group admin

Permissions boundary (not set)

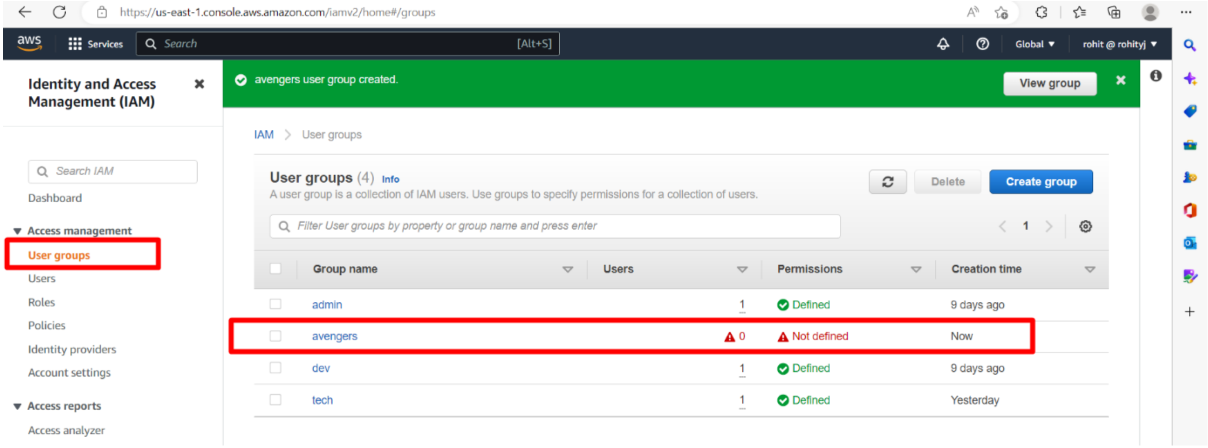
Generate policy based on CloudTrail events

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

Assignment 2: -

Hello students, in this assignment you need to prepare a developer's team of avengers.

- Create 3 IAM users of avengers and assign them in developer's groups with IAM policy.



https://us-east-1.console.aws.amazon.com/iamv2/home#/groups

Identity and Access Management (IAM)

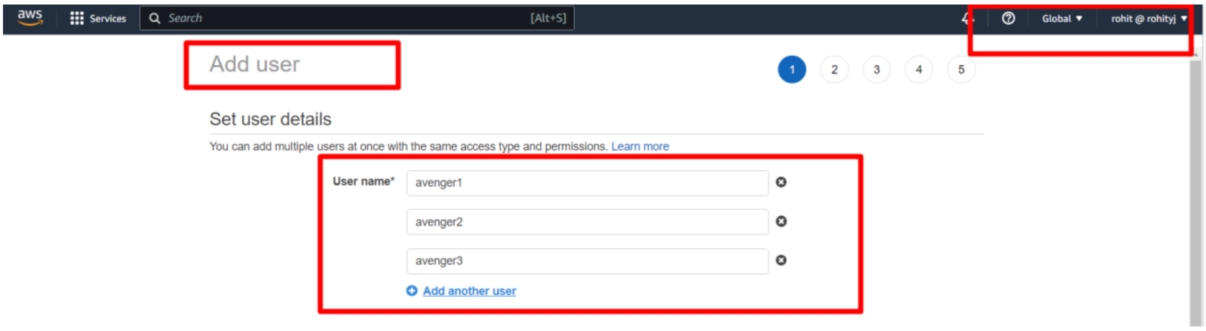
avengers user group created.

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
Filter User groups by property or group name and press enter

□	Group name	Users	Permissions	Creation time
□	admin	1	✓ Defined	9 days ago
□	avengers	⚠ 0	⚠ Not defined	Now
□	dev	1	✓ Defined	9 days ago
□	tech	1	✓ Defined	Yesterday

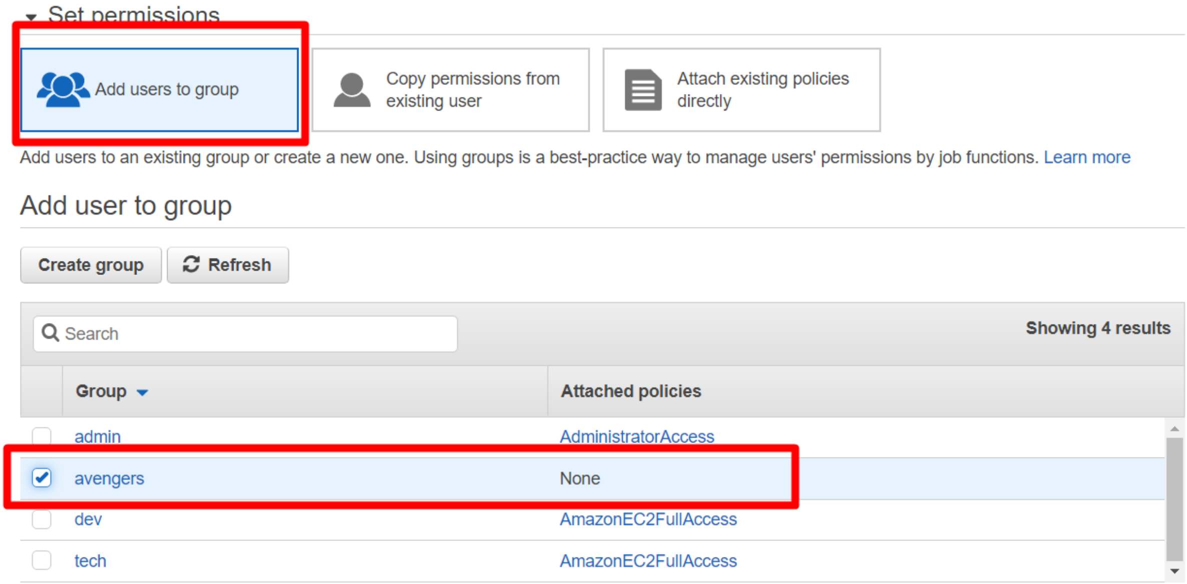


Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name*: avenger1
avenger2
avenger3



▾ Set permissions

Add users to group
Copy permissions from existing user
Attach existing policies directly

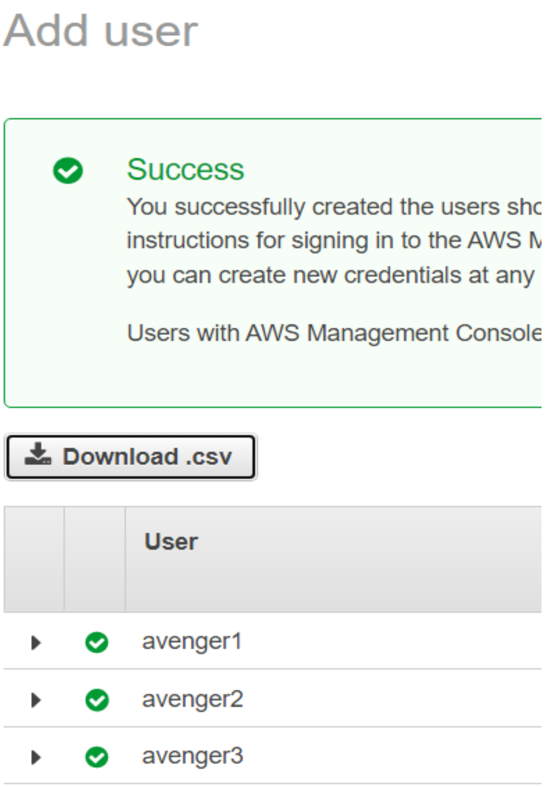
Add users to an existing group or create a new one. Using groups is a best-practice way to manage users' permissions by job functions. Learn more

Add user to group

Create group
Refresh
Search

Showing 4 results

	Group ▾	Attached policies
□	admin	AdministratorAccess
☑	avengers	None
□	dev	AmazonEC2FullAccess
□	tech	AmazonEC2FullAccess



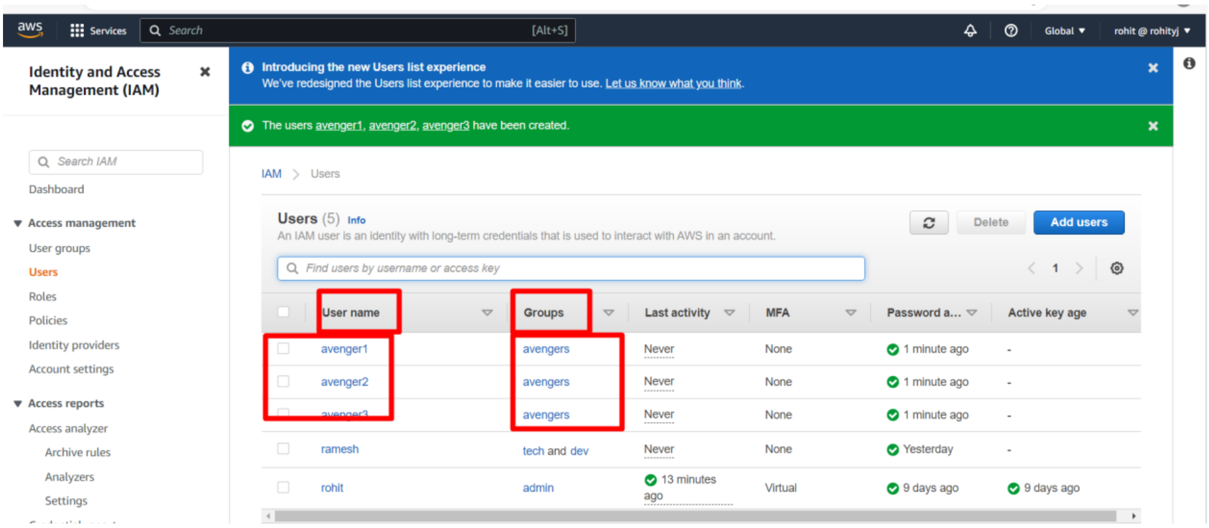
Add user

Success

You successfully created the users sho
instructions for signing in to the AWS M
you can create new credentials at any

Users with AWS Management Console

		User
▶	✓	avenger1
▶	✓	avenger2
▶	✓	avenger3



Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.

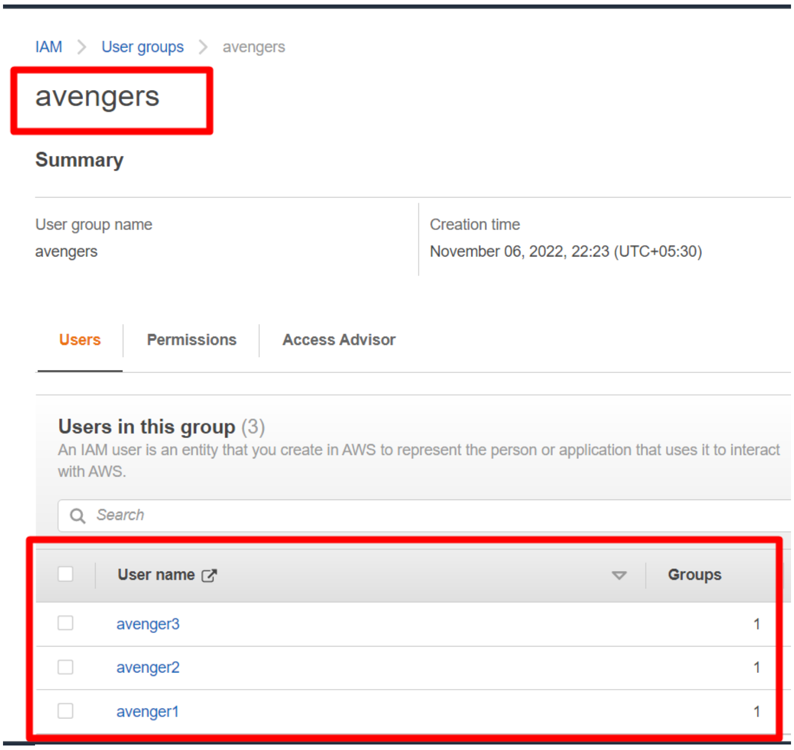
The users avenger1, avenger2, avenger3 have been created.

IAM > Users

Users (5) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Groups	Last activity	MFA	Password a...	Active key age
□	avenger1	avengers	Never	None	✓ 1 minute ago	-
□	avenger2	avengers	Never	None	✓ 1 minute ago	-
□	avenger3	avengers	Never	None	✓ 1 minute ago	-
□	ramesh	tech and dev	Never	None	✓ Yesterday	-
□	rohit	admin	✓ 13 minutes ago	Virtual	✓ 9 days ago	✓ 9 days ago



IAM > User groups > avengers

avengers

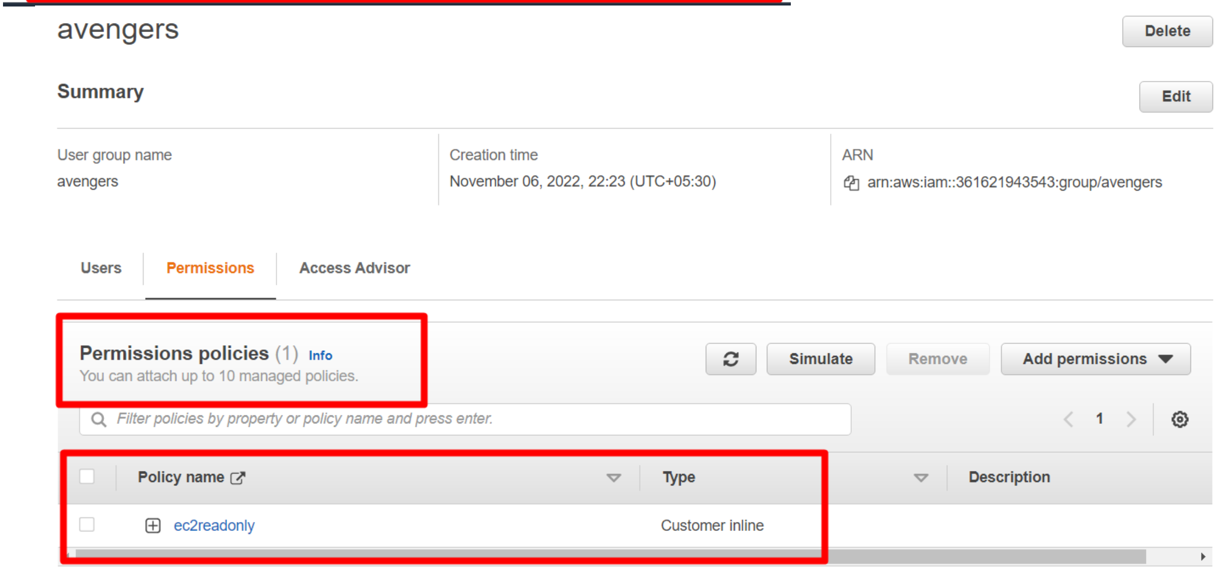
Summary

User group name
avengers

Creation time
November 06, 2022, 22:23 (UTC+05:30)

Users in this group (3)
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups
□	avenger3	1
□	avenger2	1
□	avenger1	1



avengers

Summary

User group name
avengers

Creation time
November 06, 2022, 22:23 (UTC+05:30)

ARN
arn:aws:iam::361621943543:group/avengers

Permissions policies (1) Info
You can attach up to 10 managed policies.

□	Policy name	Type	Description
□	⊞ ec2readonly	Customer inline	

Assignment 3: - Define a condition in policy for expiration like

"DateGreaterThan":

{"aws:CurrentTime":

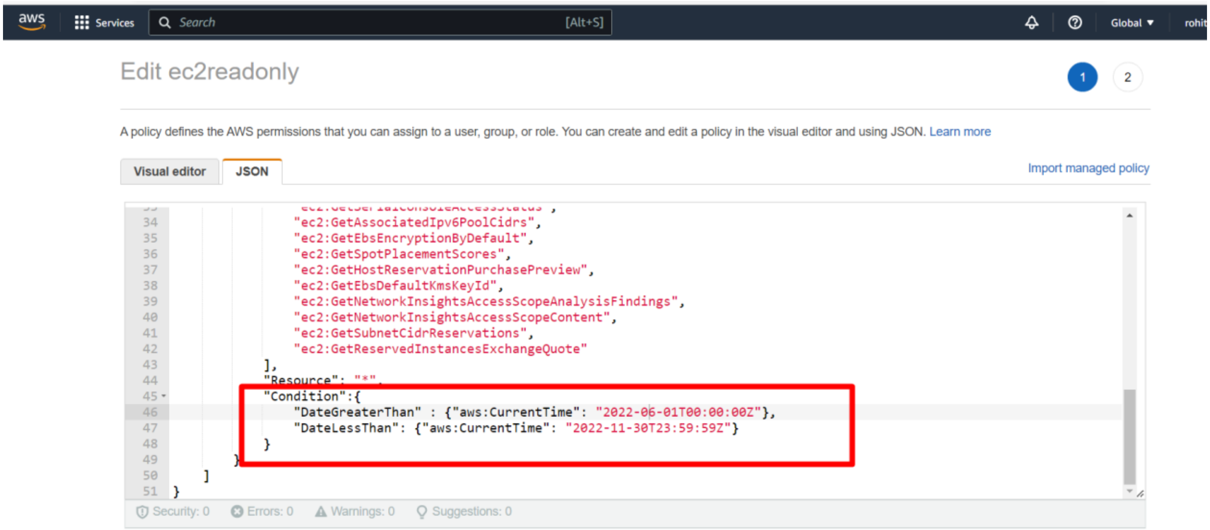
"2020-04-01T00:00:00Z"},

"DateLessThan":

{"aws:CurrentTime":

"2020-06-30T23:59:59Z"}

Define the span of 4 months as per your wish



Edit ec2readonly

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

```
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:GetAssociatedIpv6PoolCidrs",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:GetSpotPlacementScores",
                "ec2:GetHostReservationPurchasePreview",
                "ec2:GetEbsDefaultKmsKeyId",
                "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
                "ec2:GetNetworkInsightsAccessScopeContent",
                "ec2:GetSubnetCidrReservations",
                "ec2:GetReservedInstancesExchangeQuote"
            ],
            "Resource": "*",
            "Condition":{
                "DateGreaterThan" : {"aws:CurrentTime": "2022-06-01T00:00:00Z"},
                "DateLessThan": {"aws:CurrentTime": "2022-11-30T23:59:59Z"}
            }
        }
    ]
}
```

Assignment 3: - Prepare 15 authentic MCQ questions related to IAM.

1. A Solutions Architect is designing a shared service for hosting containers from several customers on Amazon ECS. These containers will use several AWS services. A container from one customer should not be able access data from another customer. Which of the below solutions should the architect use to meet these requirements?

A. IAMroles for tasks

B. IAMroles for EC2 Instances

C. IAMInstance profile for EC2 Instances

D. SecurityGroup rules

A. IAMroles for tasks

With IAM roles for Amazon ECS tasks, you can specify an IAM role to be used by the containers in a task. Applications are required to sign their AWS API requests with AWS credentials, and this feature provides a strategy to manage credentials for your application's use. This is similar to how Amazon EC2 instance profiles provide credentials to EC2 instances. For more information on configuring IAM Roles for tasks in ECS, please visit the following URL: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task-iam-roles.html

2. An EC2 Instance hosts a Java based application that accesses a DynamoDB table. This EC2 Instance is currently serving production users. Which of the following is a secure way for the EC2 Instance to access the DynamoDB table?

A. UseIAM Roles with permissions to interact with DynamoDB and assign it to the EC2Instance.

B. UseKMS Keys with the right permissions to interact with DynamoDB and assign it tothe EC2 Instance.

C. UseIAM Access Keys with the right permissions to interact with DynamoDB and assignit to the EC2 Instance.

D. UseIAM Access Groups with the right permissions to interact with DynamoDB andassign it to the EC2 Instance.

Answer

A. UseIAM Roles with permissions to interact with DynamoDB and assign it to the EC2Instance.

To ensure secure access to AWS resources from EC2 Instances, always assign a role to the EC2 Instance. For more information on IAM Roles, please refer to the below URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html An IAM role is similar to a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it. Also, a role does not have standard long-term credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user. You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. Note: You can attach IAM role to the existing EC2 instance. https://aws.amazon.com/about-aws/whats-new/2017/02/new-attach-an-iam-role-to-your-existing-amazon-ec2-instance/

3. An EC2 Instance setup in AWS will host an application which will make API calls to the Simple Storage Service. What is an ideal way for the application to access the Simple Storage Service?

A. Pass API credentials to the instance using instance user data.

B. Store API credentials as an object in a separate Amazon S3 bucket.

C. Embed the API credentials into your application.

D. Create and Assign an IAM role to the EC2 Instance.

Answer

D. Create and Assign an IAM role to the EC2 Instance.

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. It is not a good practice to use IAM credentials for a production-based application. It is always a good practice to use IAM Roles.

For more information on IAM Roles, please visit the following URL:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

4. Which of the following is not a feature of AWS Security Token Service?

A. STS enables you to request temporary, limited-privilege credentials.

B. STS enables users to assume role.

C. STS generates Git Credentials for IAM users.

D. STS generates Federated Credentials for IAM users.

Answer

C. STS generates Git Credentials for IAM users.

The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users that you authenticate (federated users). This guide provides descriptions of the STS API.
https://docs.aws.amazon.com/STS/latest/APIReference/Welcome.html

5. You are deploying an application on Amazon EC2, which must call AWS APIs. What method should you use to securely pass credentials to the application?

A. PassAPI credentials to the instance using Instance userdata.

B. StoreAPI credentials as an object in Amazon S3.

C. Embedthe API credentials into your application.

D. AssignIAM roles to the EC2 Instances.

Answer

D. AssignIAM roles to the EC2 Instances.

You can use roles to delegate access to users, applications, or services that don't normally have access to your AWS resources. It is not a good practice to use IAM credentials for a production-based application. A good practice however, is to use IAM Roles. For more information on IAM Roles, please visit the following URL: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

6. You have created an AWS Lambda function that will write data to a DynamoDB table. Which of the following must be in place to ensure that the Lambda function can interact with the DynamoDB table?

A. Ensure an IAM Role is attached to the Lambda function which has the required DynamoDBprivileges.

B. Ensure an IAM User is attached to the Lambda function which has the required DynamoDB privileges.

C. Ensure the Access keys are embedded in the AWS Lambda function.

D. Ensure the IAM user password is embedded in the AWS Lambda function.

Answer

A. Ensure an IAM Role is attached to the Lambda function which has the required DynamoDB privileges.

Each Lambda function has an IAM role (execution role) associated with it. You specify the IAM role when you create your Lambda function. Permissions you grant to this role determine what AWS Lambda can do when it assumes the role. There are two types of permissions that you grant to the IAM role:

If your Lambda function code accesses other AWS resources, such as to read an object from an S3 bucket or write logs to CloudWatch Logs, you need to grant permissions for relevant Amazon S3 and CloudWatch actions to the role. If the event source is stream-based (Amazon Kinesis Data Streams and DynamoDB streams), AWS Lambda polls these streams on your behalf. AWS Lambda needs permissions to poll the stream and read new records on the stream so you need to grant the relevant permissions to this role. For more information on the Permission Role model for AWS Lambda, please refer to the URL below.

https://docs.aws.amazon.com/lambda/latest/dg/intro-permission-model.html

7. You have currently contacted an AWS partner to carry out an audit for your AWS account. You need to ensure that the partner can carry out an audit on your resources. Which one of the following steps would you ideally carry out?

A. Create an IAM user for the partner account for login purposes

B. Create a cross account IAM Role

C. Create an IAM group for the partner account for login purposes

D. Create an IAM profile for the partner account for login purposes

Answer

B. Create a cross account IAM Role.

Cross-account IAM roles allow customers to securely grant access to AWS resources in their account to a third party, like an APN Partner, while retaining the ability to control and audit who is accessing their AWS account. Cross-account roles reduce the amount of sensitive information APN Partners need to store for their customers, so that they can focus on their product instead of managing keys. In this blog post, I explain some of the risks of sharing IAM keys, how you can implement cross-account IAM roles, and how cross-account IAM roles mitigate risks for customers and for APN Partners, particularly those who are software as a service (SaaS) provider.

Because this is clearly mentioned in the AWS Documentation, all other options are invalid

For more information on cross account roles, please refer to the below URL

https://aws.amazon.com/blogs/apn/securely-accessing-customer-aws-accounts-with-cross-account-iam-roles/

8. You work in the media industry and have created a web application where users will be able to upload photos they create to your website. This web application must be able to call the S3 API in order to be able to function. Where should you store your API credentials whilst maintaining the maximum level of security?

A. Save the API credentials to your PHP files.

B. Don't save your API credentials. Instead create a role in IAM and assign this role toan EC2 instance when you first create it.

C. Save your API credentials in a public Github repository.

D. Pass API credentials to the instance using instance user data.

Answer

B. Don't save your API credentials. Instead create a role in IAM and assign this role toan EC2 instance when you first create it.

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

9. Your application consists of a set of EC2 Instances which are spun up as part of an Autoscaling Group. These Instances need to access objects in an S3 bucket. Which of the following is the ideal approach to ensure this access is set in place?

A. Ensure that the Access Keys are picked up from another S3 bucket. The Access Keys can be embedded in the User data during Instance Launch.

B. Ensure that the Autoscaling Group attaches an IAM Role attached to the underlying EC2 Instances.

C. Ensure that an IAM policy is attached to the S3 bucket which allows access to the S3 buckets.

D. Ensure that the Autoscaling Group attaches an IAM User attached to the underlying EC2 Instances.

Answer

B. Ensure that the Autoscaling Group attaches an IAM Role attached to the underlying EC2 Instances.

Applications must sign their API requests with AWS credentials. Therefore, if you are an application developer, you need a strategy for managing credentials for your applications that run on EC2 instances. For example, you can securely distribute your AWS credentials to the instances, enabling the applications on those instances to use your credentials to sign requests, while protecting your credentials from other users. However, it's challenging to securely distribute credentials to each instance, especially those that AWS creates on your behalf, such as Spot Instances or instances in Auto Scaling groups. You must also be able to update the credentials on each instance when you rotate your AWS credentials.

We designed IAM roles so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html

10. Your company has a set of EC2 Instances that access data objects stored in an S3 bucket. Your IT Security department is concerned about the security of this architecture and wants you to implement the following:

Ensure that the EC2 Instance securely accesses the data objects stored in the S3 bucket

Prevent accidental deletion of objects Which of the following would help fulfil the requirements of the IT Security department? Choose 2 answers from the options given below.

A. Create an IAM user and ensure the EC2 Instances use the IAM user credentials to access the data in the bucket.

B. Create an IAM Role and ensure the EC2 Instances use the IAM Role to access the data in the bucket.

C. Use S3 Cross-Region Replication to replicate the objects so that the integrity of data is maintained.

D. Use an S3 bucket policy that ensures that MFA Delete is set on the objects in the bucket.

Answer

B. & D.

IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles

For more information on IAM Roles, please refer to the below link:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html MFA Delete can be used to add another layer of security to S3 Objects to prevent accidental deletion of objects.

For more information on MFA Delete, please refer to the below link:

https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/

11. Your company is planning on hosting their development, test and production applications on EC2 Instances in AWS. They are worried about how access control would be given to relevant IT Admins for each of the above environments. As an architect, what would you suggest for managing the relevant accesses?

A. Add tags to the instances marking each environment and then segregate access using IAM Policies.

B. Add Userdata to the underlying instances to mark each environment.

C. Add Metadata to the underlying instances to mark each environment.

D. Add each environment to a separate Auto Scaling Group.

Answer

A. Add tags to the instances marking each environment and then segregate access using IAM Policies.

Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type — you can quickly identify a specific resource based on the tags you've assigned to it. Each tag consists of a key and an optional value, both of which you define. For example, you could define a set of tags for your account's Amazon EC2 instances that helps you track each instance's owner and stack level. We recommend that you devise a set of tag keys that meets your needs for each resource type. Using a consistent set of tag keys makes it easier for you to manage your resources. You can search and filter the resources based on the tags you add.

For more information on using tags, please see the below link:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

12. Your company is planning on using the API Gateway service to manage APIs for developers and users. There is a need to segregate the access rights for both developers and users. How can this be accomplished?

A. Use IAM permissions to control the access.

B. Use AWS Access keys to manage the access.

C. Use AWS KMS service to manage the access.

D. Use AWS Config Service to control the access.

Answer

A. Use IAM permissions to control the access.

You control access to Amazon API Gateway with IAM permissions by controlling access to the following two API Gateway component processes:

To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway. To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway. For more information on permissions for the API gateway, please visit the URL:

https://docs.aws.amazon.com/apigateway/latest/developerguide/permissions.html

13. Your organization AWS Setup has an AWS S3 bucket which stores confidential documents which can be only downloaded by users authenticated and authorized via your application. You do not want to create IAM users for each of these users and as a best practice you have decided to generate AWS STS Federated User temporary credentials each time when a download request is made and then use the credentials to generate preassigned URL and redirect user for download. However, when user is trying to access the preassigned URL, they are getting Access Denied Error. What could be the reason?

A. AWS STS service must be given access in S3 bucket ACL.

B. IAM User used to generate Federated User credentials does not have access on S3 bucket

C. IAM Role used to generate Federated User credentials does not have access on S3 bucket.

D. Your application must be whitelisted in AWS STS service to perform Federated User action.

Answer

B. IAM User used to generate Federated User credentials does not have access on S3 bucket.

Returns a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) for a federated user. A typical use is in a proxy application that gets temporary security credentials on behalf of distributed applications inside a corporate network. You must call the GetFederationToken operation using the long-term security credentials of an IAM user. As a result, this call is appropriate in contexts where those credentials can be safely stored, usually in a server-based application. For a comparison of GetFederationToken with the other API operations that produce temporary credentials https://docs.aws.amazon.com/STS/latest/APIReference/API_GetFederationToken.html

14. Your organization has an AWS setup and planning to build Single Sign On for users to authenticate with on-premise Microsoft Active Directory Federation Services (ADFS) and let user's login to AWS console using AWS STS Enterprise Identity Federation. Which of the following service you need to call from AWS STS service after you authenticate with your on-premise?

A. AssumeRoleWithSAML

B. GetFederationToken

C. AssumeRoleWithWebIdentity

D. GetCallerIdentity

Answer

A. AssumeRoleWithSAML.

Returns a set of temporary security credentials for users who have been authenticated via a SAML authentication response. This operation provides a mechanism for tying an enterprise identity store or directory to role-based AWS access without user-specific credentials or configuration. For a comparison of AssumeRoleWithSAML with the other API operations that produce temporary credentials https://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRoleWithSAML.html

15. Which of the following is the most secure way of giving access to AWS services to applications running on Ec2 instances?

A. Creating Service users

B. Creating Service groups

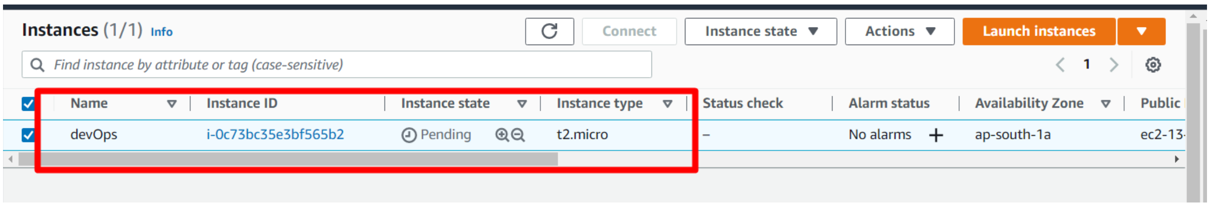
C. Roles

D. Attaching policies to applications

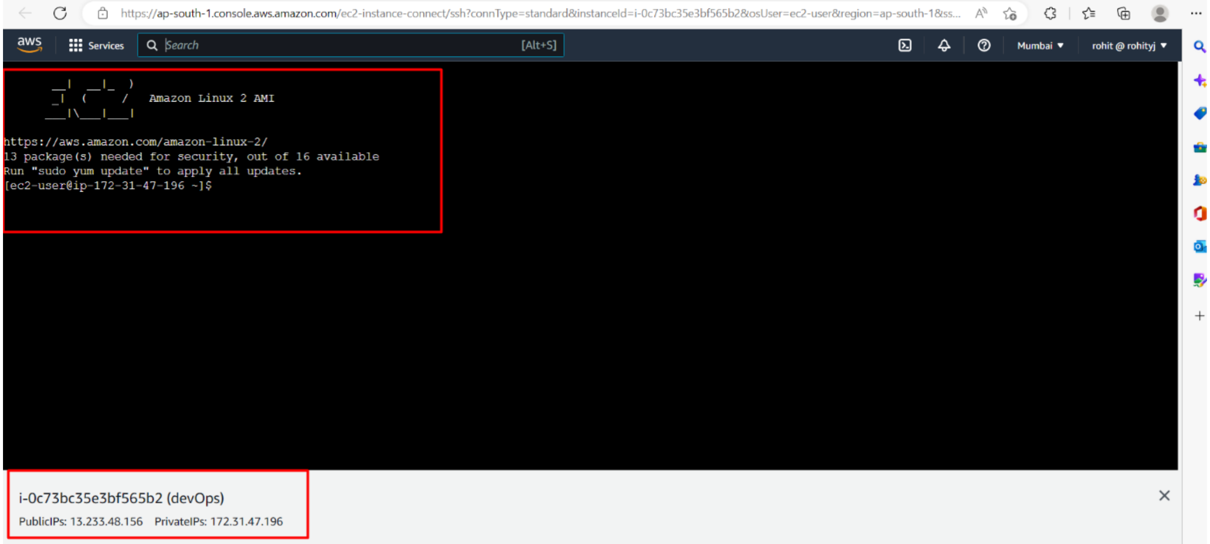
Answer

C. Roles

Assignment 4: - Launch your Linux instance in IAM and update your machine.



☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
☑	devOps	i-0c73bc35e3bf565b2	Pending	t2.micro	–	No alarms	ap-south-1a	ec2-13-



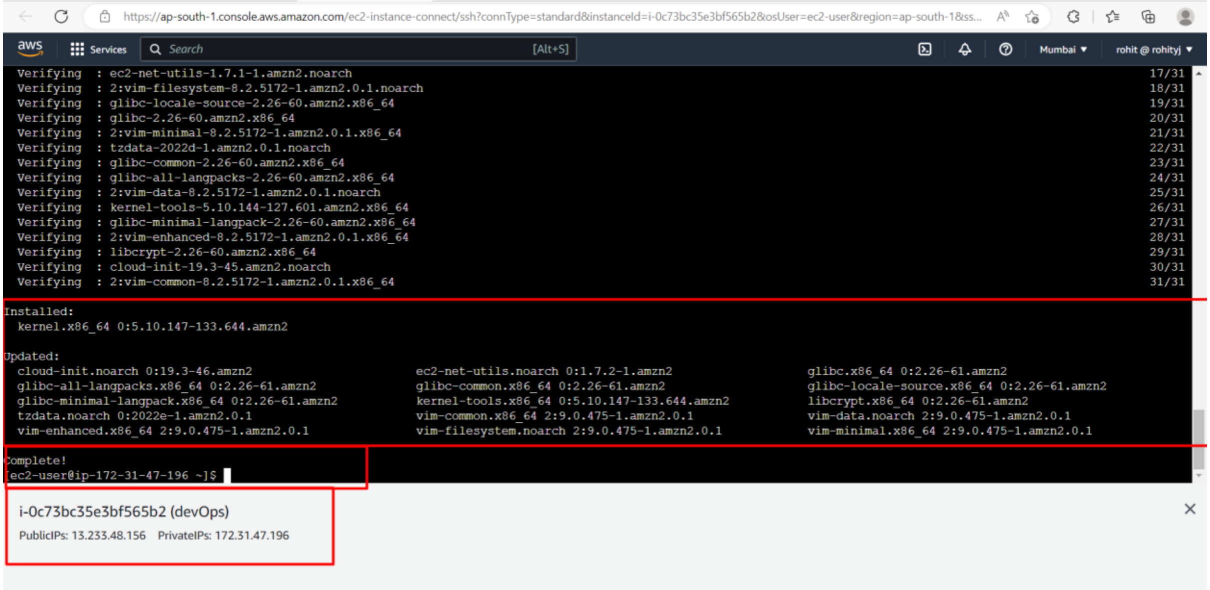
https://ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0c73bc35e3bf565b2&osUser=ec2-user&region=ap-south-1&ss...
aws
Services
Search
[Alt+S]
Mumbai ▼
rohit @ rohityj ▼

```
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
13 package(s) needed for security, out of 16 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-47-196 ~]$
```

i-0c73bc35e3bf565b2 (devOps)

PublicIPs: 13.233.48.156 PrivateIPs: 172.31.47.196



https://ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?connType=standard&instanceId=i-0c73bc35e3bf565b2&osUser=ec2-user&region=ap-south-1&ss...
aws
Services
Search
[Alt+S]
Mumbai ▼
rohit @ rohityj ▼

```
  Verifying  : ec2-net-utils-1.7.1-1.amzn2.noarch                                                                                    17/31
  Verifying  : 2:vim-filesystem-8.2.5172-1.amzn2.0.1.noarch                                                                          18/31
  Verifying  : glibc-locale-source-2.26-60.amzn2.x86_64                                                                              19/31
  Verifying  : glibc-2.26-60.amzn2.x86_64                                                                                            20/31
  Verifying  : 2:vim-minimal-8.2.5172-1.amzn2.0.1.x86_64                                                                             21/31
  Verifying  : tzdata-2022d-1.amzn2.0.1.noarch                                                                                       22/31
  Verifying  : glibc-common-2.26-60.amzn2.x86_64                                                                                     23/31
  Verifying  : glibc-all-langpacks-2.26-60.amzn2.x86_64                                                                              24/31
  Verifying  : 2:vim-data-8.2.5172-1.amzn2.0.1.noarch                                                                                25/31
  Verifying  : kernel-tools-5.10.144-127.601.amzn2.x86_64                                                                            26/31
  Verifying  : glibc-minimal-langpack-2.26-60.amzn2.x86_64                                                                           27/31
  Verifying  : 2:vim-enhanced-8.2.5172-1.amzn2.0.1.x86_64                                                                            28/31
  Verifying  : libcrypt-2.26-60.amzn2.x86_64                                                                                         29/31
  Verifying  : cloud-init-19.3-45.amzn2.noarch                                                                                       30/31
  Verifying  : 2:vim-common-8.2.5172-1.amzn2.0.1.x86_64                                                                              31/31

Installed:
  kernel.x86_64 0:5.10.147-133.644.amzn2

Updated:
  cloud-init.noarch 0:19.3-46.amzn2                  ec2-net-utils.noarch 0:1.7.2-1.amzn2               glibc.x86_64 0:2.26-61.amzn2
  glibc-all-langpacks.x86_64 0:2.26-61.amzn2         glibc-common.x86_64 0:2.26-61.amzn2                glibc-locale-source.x86_64 0:2.26-61.amzn2
  glibc-minimal-langpack.x86_64 0:2.26-61.amzn2      kernel-tools.x86_64 0:5.10.147-133.644.amzn2       libcrypt.x86_64 0:2.26-61.amzn2
  tzdata.noarch 0:2022e-1.amzn2.0.1                  vim-common.x86_64 2:9.0.475-1.amzn2.0.1            vim-data.noarch 2:9.0.475-1.amzn2.0.1
  vim-enhanced.x86_64 2:9.0.475-1.amzn2.0.1          vim-filesystem.noarch 2:9.0.475-1.amzn2.0.1        vim-minimal.x86_64 2:9.0.475-1.amzn2.0.1

Complete!
[ec2-user@ip-172-31-47-196 ~]$
```

i-0c73bc35e3bf565b2 (devOps)

PublicIPs: 13.233.48.156 PrivateIPs: 172.31.47.196