AWS - IAM

IAM - Identity and Access Management

- You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
- IAM is service that enables you to manage users and group permission in AWS.

Why we go for IAM in AWS

- To avoid a security and logistical headache.
- IAM allows you to limit access as needed and it can create multiple users with individual security credentials and permission.
- It is used to free in AWS service. (no cost for this)
- Using the root user only to create your first IAM user.
- Language is used to create IAM in AWS is JSON,CLI

Identity and Access Management (IAM)

- **Group**
- **User**
- **Policies**
- **Roles**
- **Identity provider**
- **Account settings**
- **Credentials report**

Group:

- An **IAM** group is a collection of **IAM** users.
- Groups let you specify permissions for multiple users
- Any user in that **group** automatically has the permissions that are assigned to the **group**.

User:

- **IAM** enables you to securely control access to AWS services and resources for your users.
- You can create and manage AWS users and groups and use permissions to allow and deny their permissions to AWS resources.

Policies:

- Permissions in the policies determine whether the request is allowed or denied.
- In AWS have already predefined policies
- We can create policies of our own
  e.g.: write, read & list

Roles:

- **IAM** entity that defines a set of permissions for making **AWS** service requests.
- **IAM roles** are not associated with a specific user or group.

Identity provider:

- Identity provider offers user authentication as a service.

Account settings:

- It has the Password policy & Security Token Service (STS) and endpoints with region.

Credentials report:

- In this report have lists of all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices.

IAM Resources:

- **User**
- **Groups**
- **Roles**
- **Identity provider**
- **Customer managed policies**

Customer managed policies:

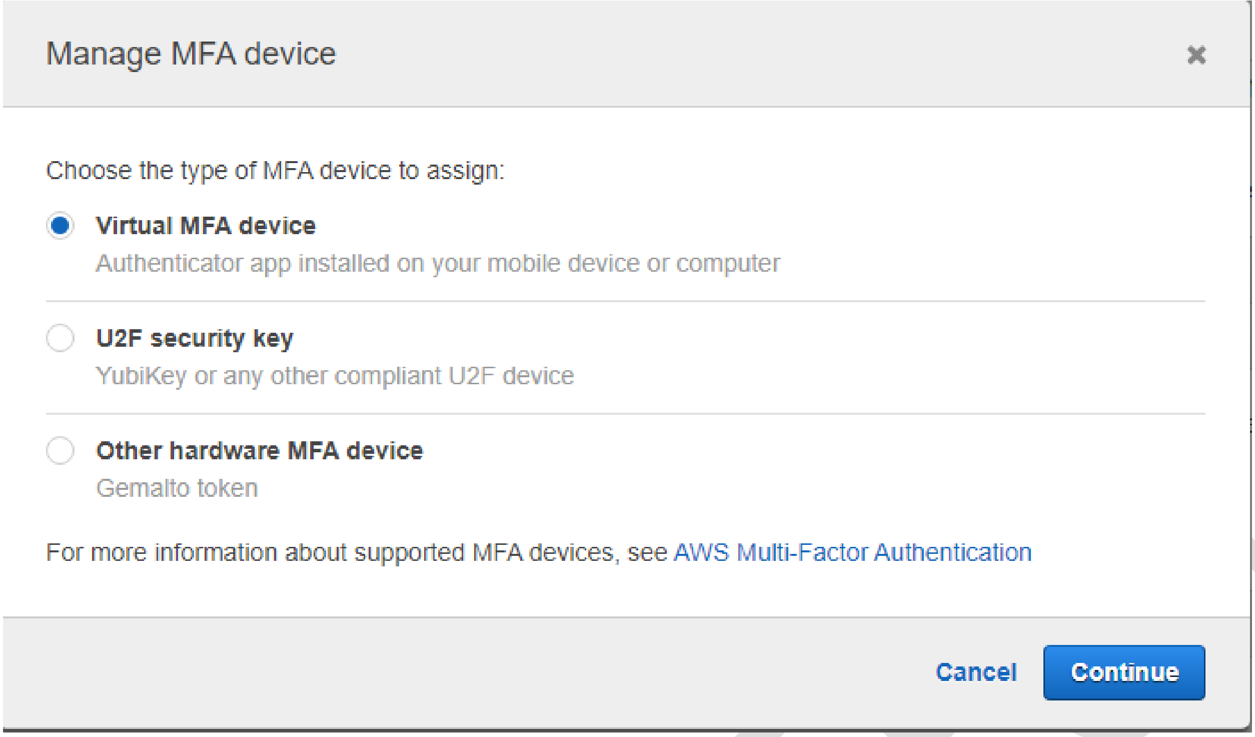
- **https://xxxxxxxxxx.signin.aws.amazon.com/console**
- **It can be changed like this**
- **https://test team.signin.aws.amazon.com/console**

Authentication:

- Two type of authentication in IAM(user logging & MFA)
- In another method we can use the access key and secret key

Multi-factor authentication (MFA):

- In this we have three ways to secure (Virtual MFA device, U2F security key, Other hardware MFA device)
- Virtual MFA device (It is used to scan the Google authentication app for more security purpose .In this every 30sec create one new code)
- U2F security key (If you already use a U2F security key with other services, and it has an AWS supported configuration (for example, the Yubikey 4 or 5 from Yubico), you can also use it with AWS)
- Other hardware MFA device (In the Google we have seen the lock symbol in this we can see the certificate for the organisation.



Manage MFA device ✖

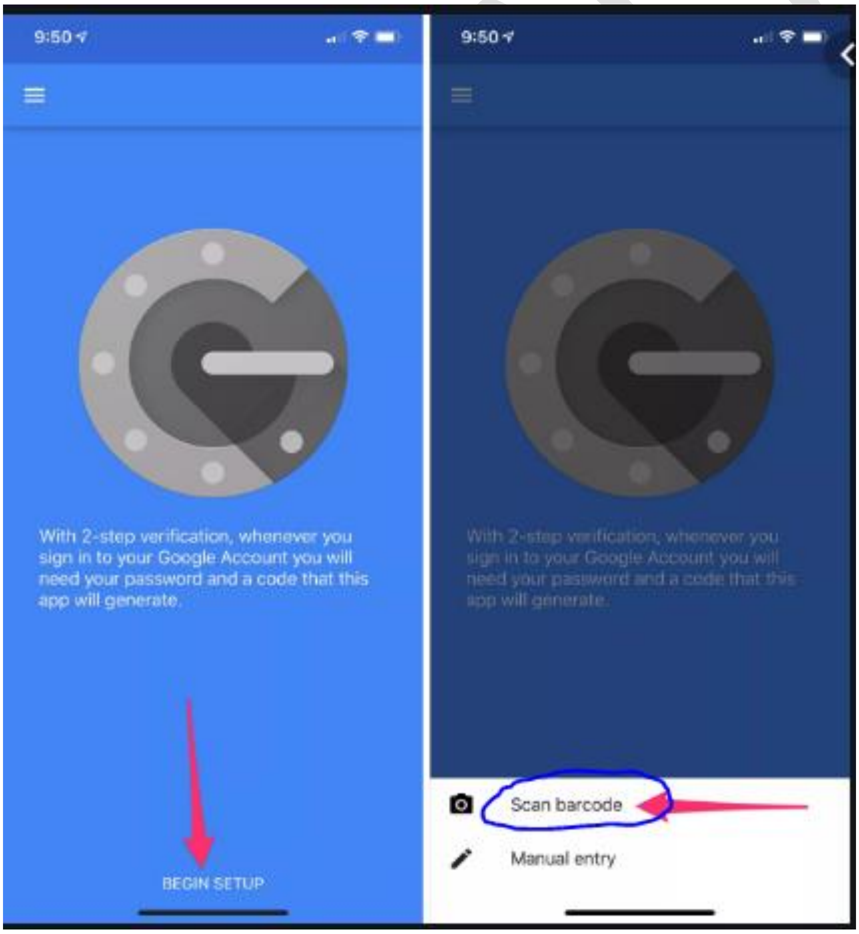
Choose the type of MFA device to assign:

● **Virtual MFA device**
Authenticator app installed on your mobile device or computer

○ **U2F security key**
YubiKey or any other compliant U2F device

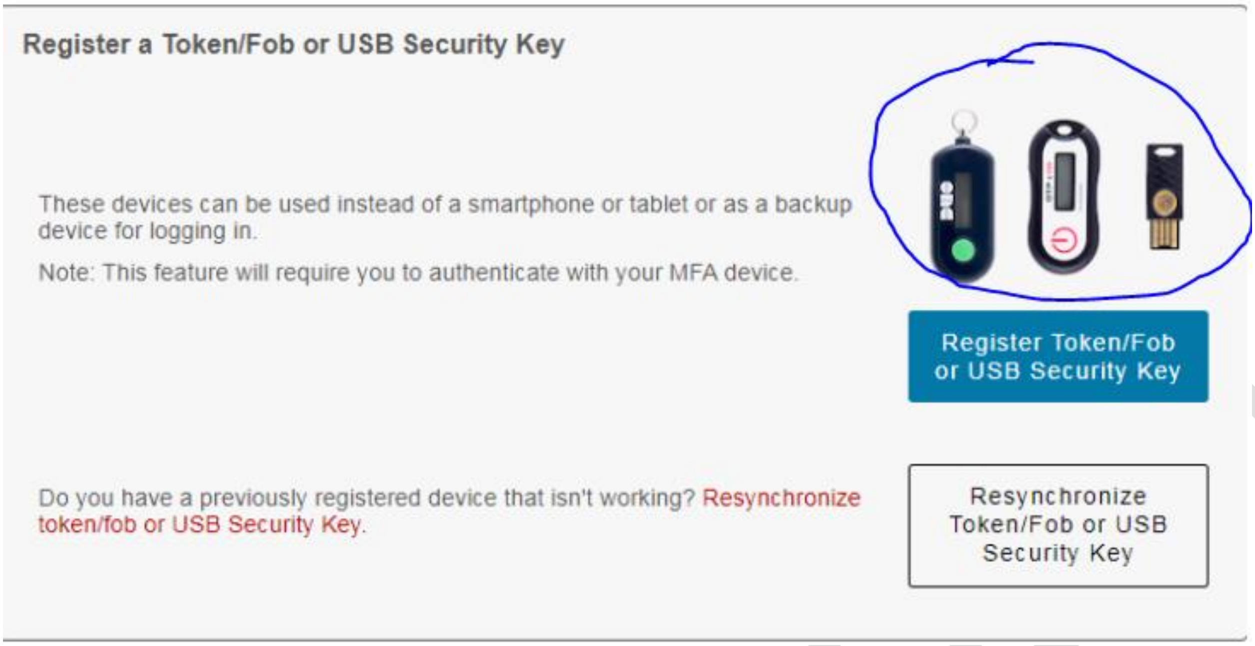
○ **Other hardware MFA device**
Gemalto token

For more information about supported MFA devices, see AWS Multi-Factor Authentication



With 2-step verification, whenever you sign in to your Google Account you will need your password and a code that this app will generate.

With 2-step verification, whenever you sign in to your Google Account you will need your password and a code that this app will generate.



Register a Token/Fob or USB Security Key

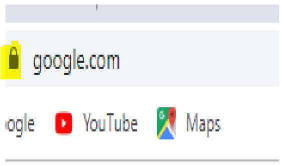
These devices can be used instead of a smartphone or tablet or as a backup device for logging in.

Note: This feature will require you to authenticate with your MFA device.

Register Token/Fob or USB Security Key

Do you have a previously registered device that isn't working? Resynchronize token/fob or USB Security Key.

Resynchronize Token/Fob or USB Security Key



Access key and secret key

- Access key & secret key have for the both root user and user.
- For root users have the full permission for everything and user has the set of permission for them.

In IAM we should follow these steps:

- **Group**
- **User**
- **Policies**
- **Widely role in security concepts**

Task 1:

- Now create the groups
- Create the user and attach to the group

- Now create your own policies to s3 (list, read)
- Then resources (all specific)
- Now go and check the with Customer managed using that link httpd//: team.signin.aws.amazon.com/console
- Only we can see the S3 service and other services we can’t use it

Task 2:

- Now create the groups
- Create the user and attach to the group
- Now create your own policies to EC2 instance (full access)
- Then resources(all specific)
- Now go and check the with Customer managed using that link httpd//: team.signin.aws.amazon.com/console
- Only we can see the EC2 service and other service we can’t use it

Task 3:

- If you lost your access key how can you login

Task 4 (service to service):

- Now create the groups
- Create the user and attach to the group
- Now create your own policies to s3 (list, read)
- Then resources(all specific)
- Now create the role for s3
- Then create EC2 instance and attach the IAM role for s3
- Launch the instance using root user

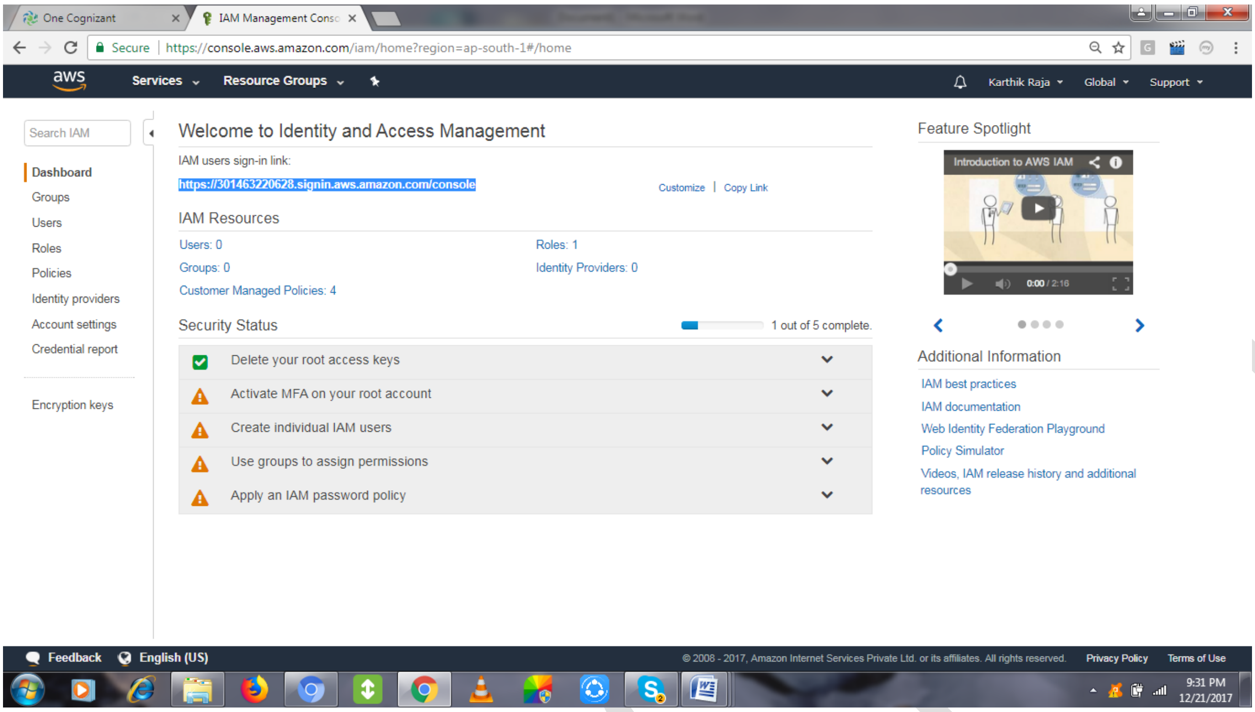
Task 5:

- For the IAM user, How can create own **MFA** authentication for the user

For Example:

Activity 1:

IAM users sign-in link customizable: Instead of the Account ID, the customer name can be updated.



https://console.aws.amazon.com/iam/home?region=ap-south-1#/home

Welcome to Identity and Access Management

IAM users sign-in link:

https://301463220628.signin.aws.amazon.com/console

IAM Resources

Users: 0

Roles: 1

Groups: 0

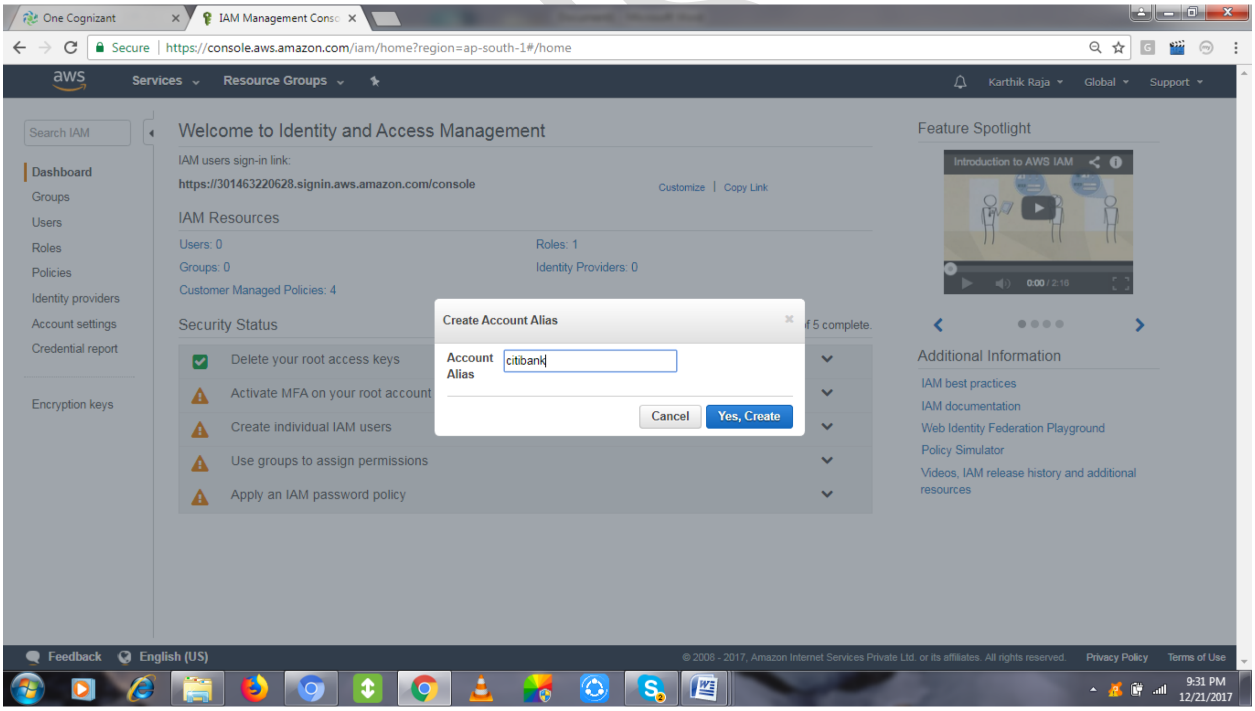
Identity Providers: 0

Customer Managed Policies: 4

Security Status

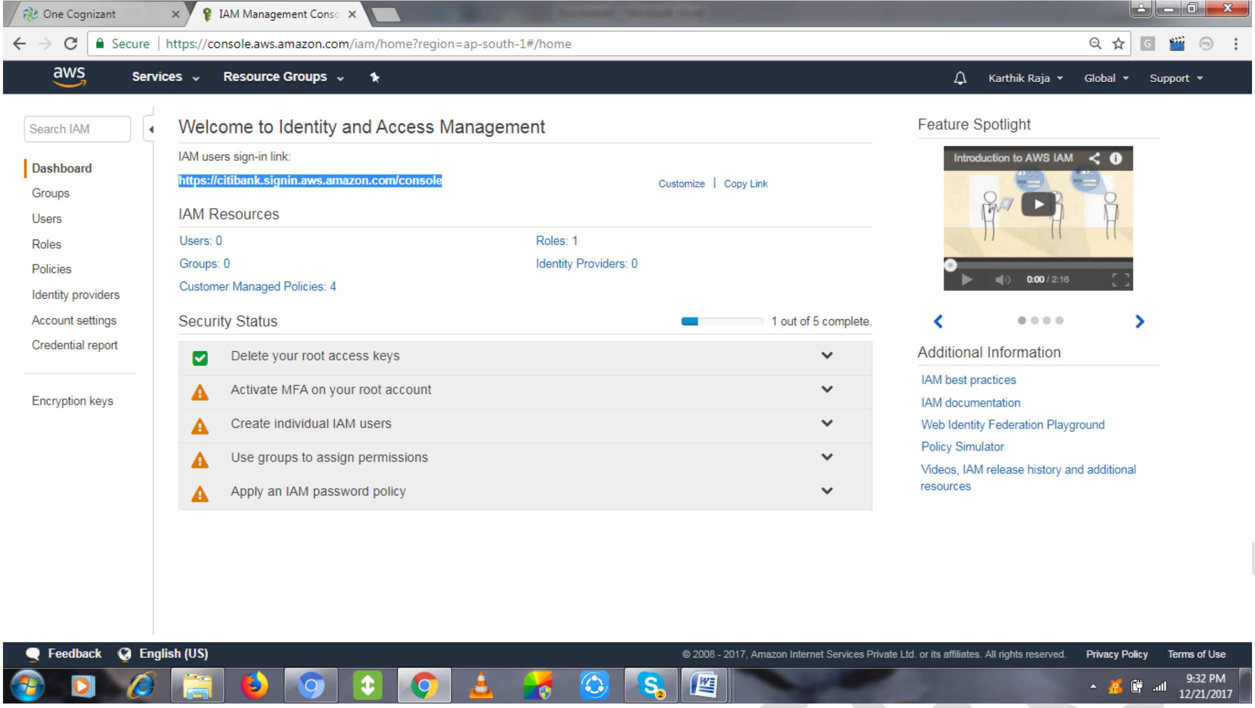
1 out of 5 complete.

- Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy



Create Account Alias

Account Alias: citibank



https://console.aws.amazon.com/iam/home?region=ap-south-1#/home

Welcome to Identity and Access Management

IAM users sign-in link:

https://citibank.signin.aws.amazon.com/console

IAM Resources

Users: 0	Roles: 1
Groups: 0	Identity Providers: 0
Customer Managed Policies: 4	

Security Status — 1 out of 5 complete.

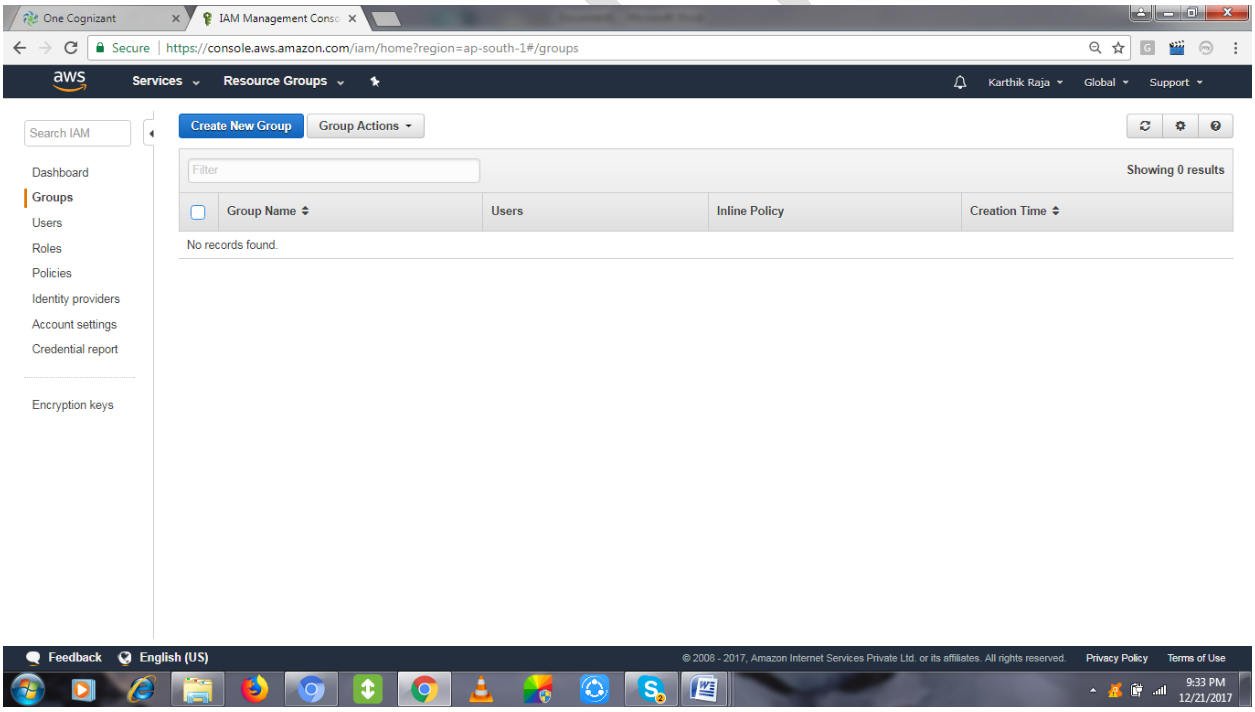
- ✓ Delete your root access keys
- Activate MFA on your root account
- Create individual IAM users
- Use groups to assign permissions
- Apply an IAM password policy

Feature Spotlight: Introduction to AWS IAM

Additional Information: IAM best practices, IAM documentation, Web Identity Federation Playground, Policy Simulator, Videos, IAM release history and additional resources

Activity 2:

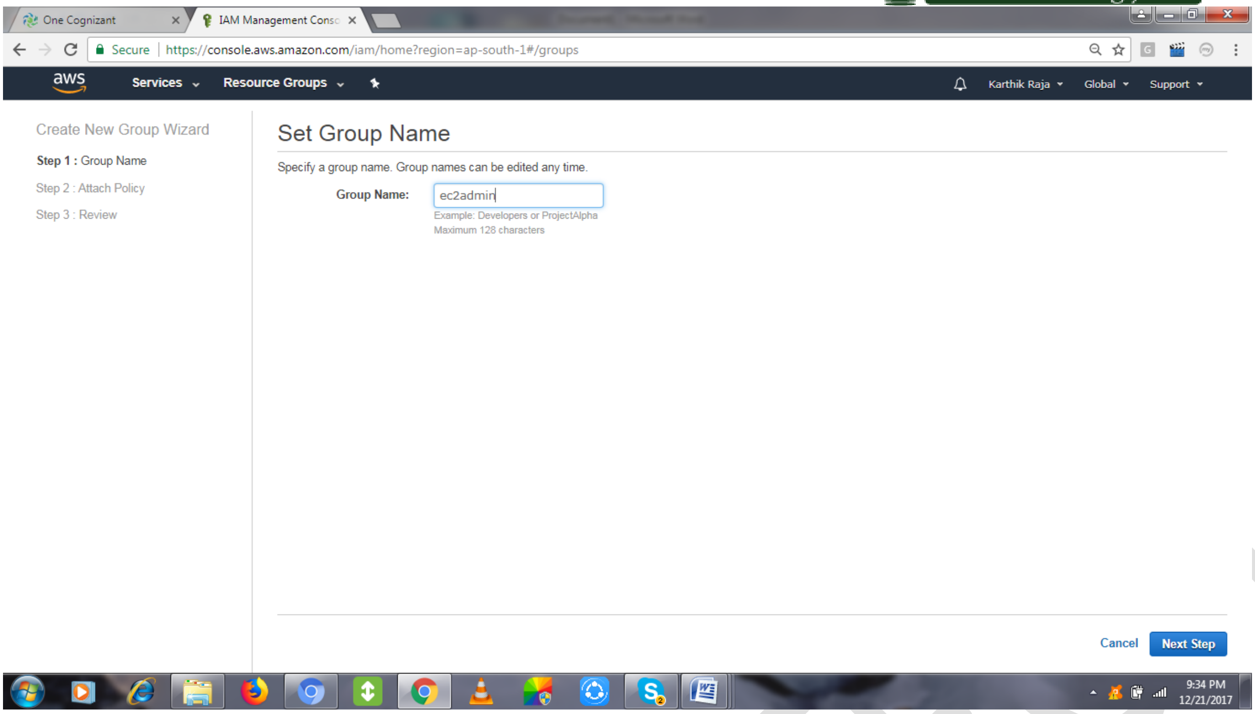
Group Creation: Click Create New Group



https://console.aws.amazon.com/iam/home?region=ap-south-1#/groups

☐	Group Name	Users	Inline Policy	Creation Time
No records found.				

Showing 0 results



Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

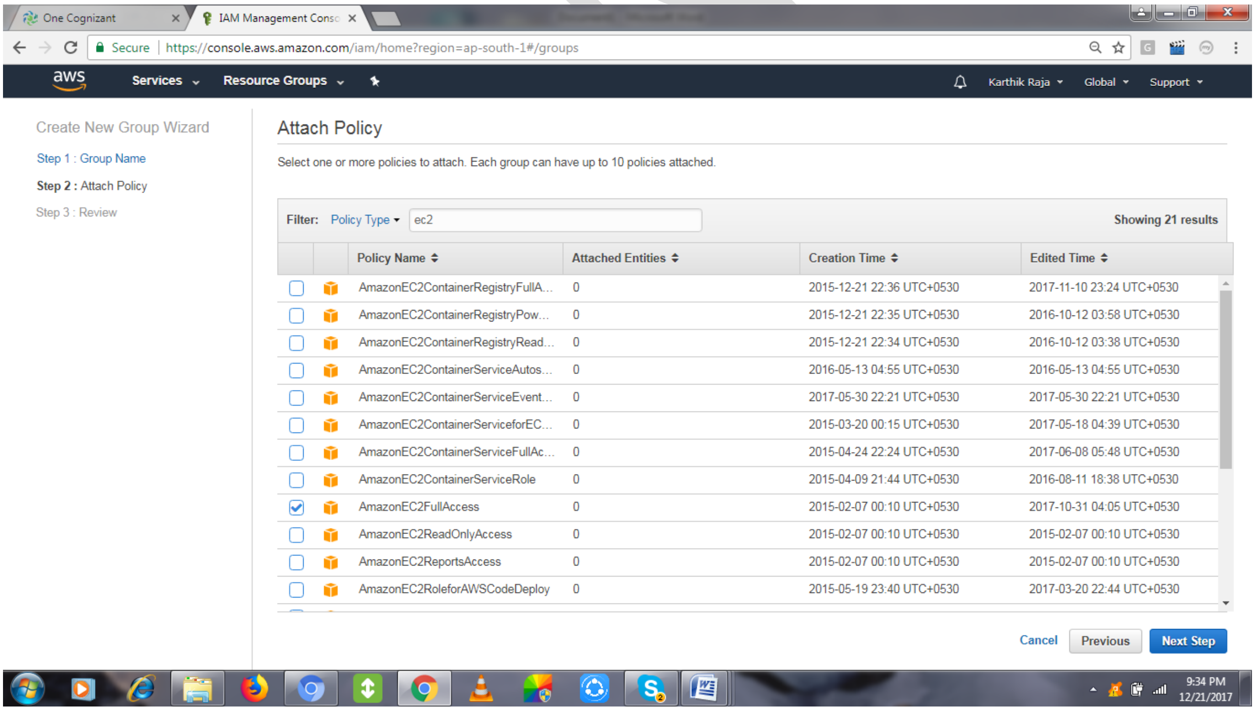
Set Group Name

Specify a group name. Group names can be edited any time.

Group Name: ec2admin

Example: Developers or ProjectAlpha
Maximum 128 characters

Choose the policy related to the group by using the search tab, like ec2, S3 any services.



Create New Group Wizard

Step 1 : Group Name

Step 2 : Attach Policy

Step 3 : Review

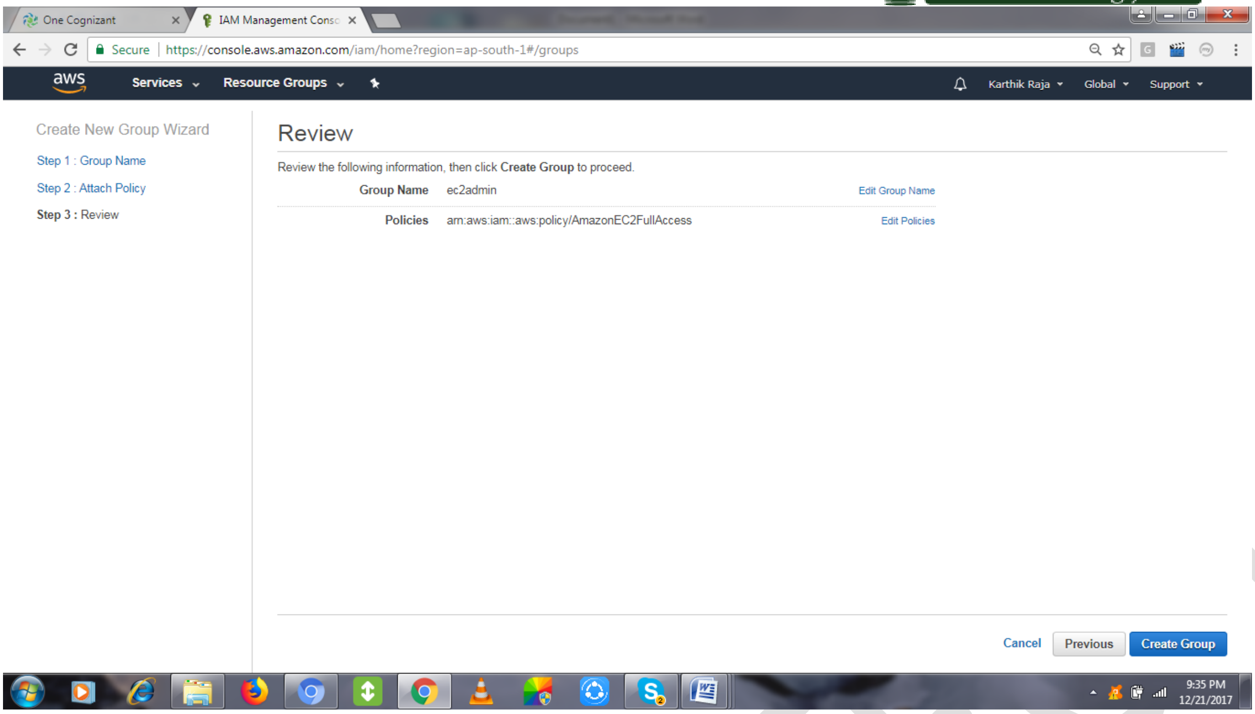
Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾ ec2 **Showing 21 results**

	Policy Name	Attached Entities	Creation Time	Edited Time
□	AmazonEC2ContainerRegistryFullA...	0	2015-12-21 22:36 UTC+0530	2017-11-10 23:24 UTC+0530
□	AmazonEC2ContainerRegistryPow...	0	2015-12-21 22:35 UTC+0530	2016-10-12 03:58 UTC+0530
□	AmazonEC2ContainerRegistryRead...	0	2015-12-21 22:34 UTC+0530	2016-10-12 03:38 UTC+0530
□	AmazonEC2ContainerServiceAutos...	0	2016-05-13 04:55 UTC+0530	2016-05-13 04:55 UTC+0530
□	AmazonEC2ContainerServiceEvent...	0	2017-05-30 22:21 UTC+0530	2017-05-30 22:21 UTC+0530
□	AmazonEC2ContainerServiceforEC...	0	2015-03-20 00:15 UTC+0530	2017-05-18 04:39 UTC+0530
□	AmazonEC2ContainerServiceFullAc...	0	2015-04-24 22:24 UTC+0530	2017-06-08 05:48 UTC+0530
□	AmazonEC2ContainerServiceRole	0	2015-04-09 21:44 UTC+0530	2016-08-11 18:38 UTC+0530
☑	AmazonEC2FullAccess	0	2015-02-07 00:10 UTC+0530	2017-10-31 04:05 UTC+0530
□	AmazonEC2ReadOnlyAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
□	AmazonEC2ReportsAccess	0	2015-02-07 00:10 UTC+0530	2015-02-07 00:10 UTC+0530
□	AmazonEC2RoleforAWSCodeDeploy	0	2015-05-19 23:40 UTC+0530	2017-03-20 22:44 UTC+0530

Review the policy & create the Group.



Create New Group Wizard

Step 1 : Group Name

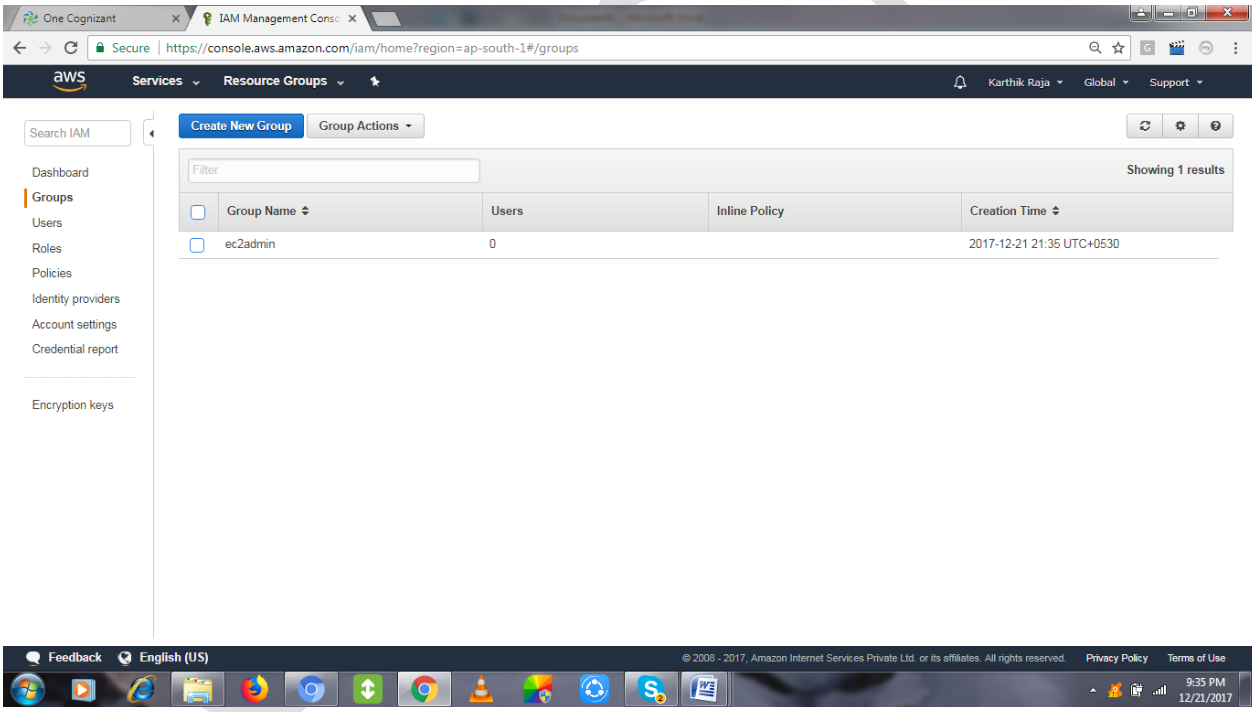
Step 2 : Attach Policy

Step 3 : Review

Review

Review the following information, then click **Create Group** to proceed.

Group Name	ec2admin	Edit Group Name
Policies	arn:aws:iam::aws:policy/AmazonEC2FullAccess	Edit Policies



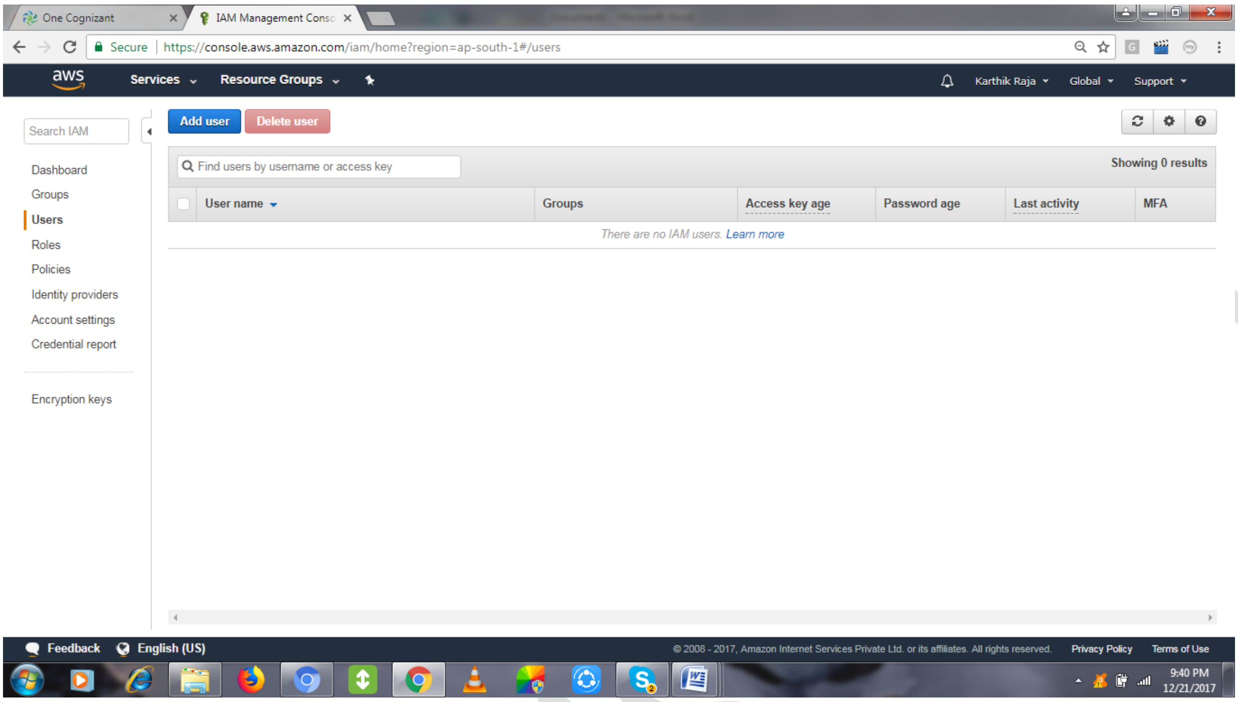
Showing 1 results

☐	Group Name	Users	Inline Policy	Creation Time
☐	ec2admin	0		2017-12-21 21:35 UTC+0530

© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Activity 3:

Creating User by clicking Add User.

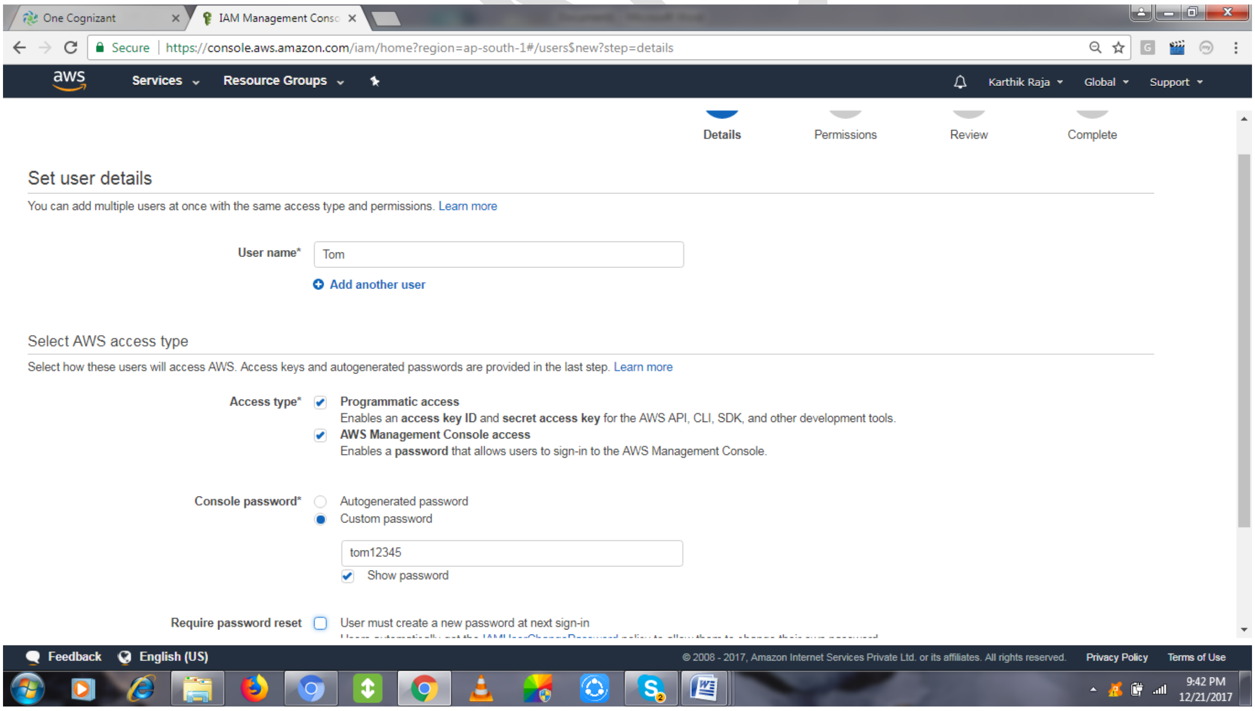


Showing 0 results

□	User name	Groups	Access key age	Password age	Last activity	MFA

There are no IAM users. Learn more

© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.



Set user details

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

User name* Tom

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

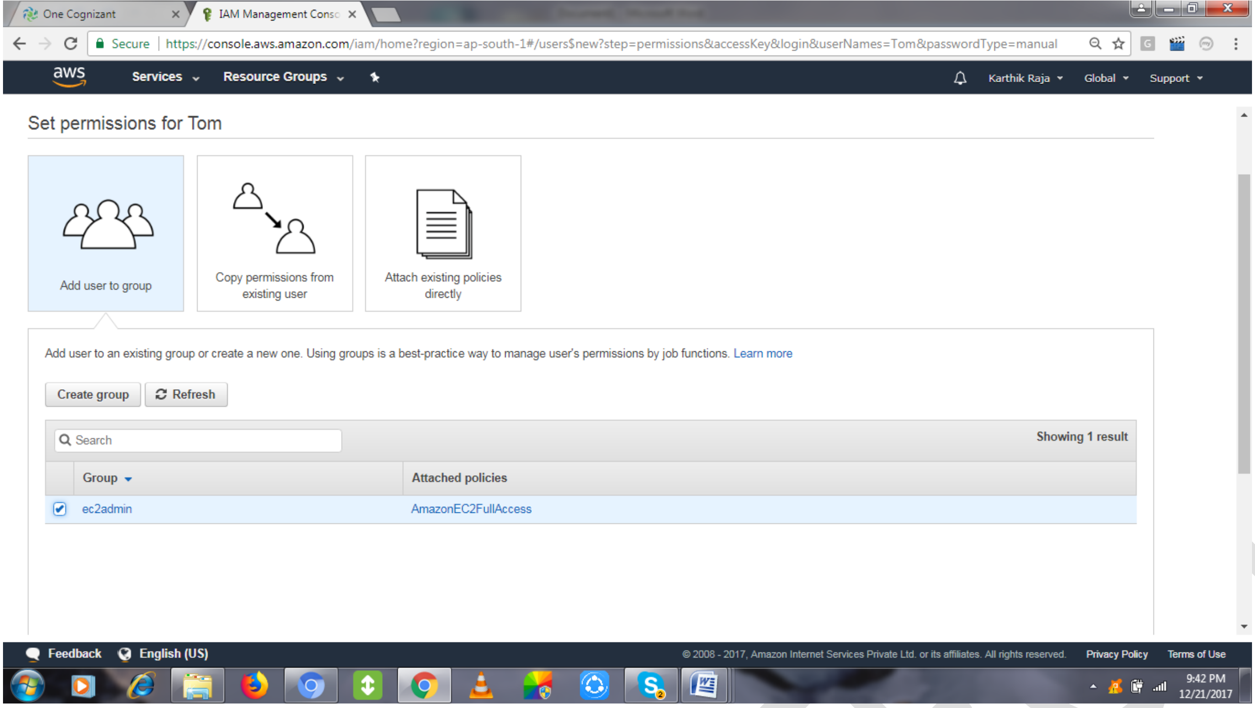
Access type*
☑ Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
☑ AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password*
○ Autogenerated password
● Custom password
tom12345
☑ Show password

Require password reset □ User must create a new password at next sign-in

© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

Add the user to the existing group or create a new group and add the user.



Set permissions for Tom

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

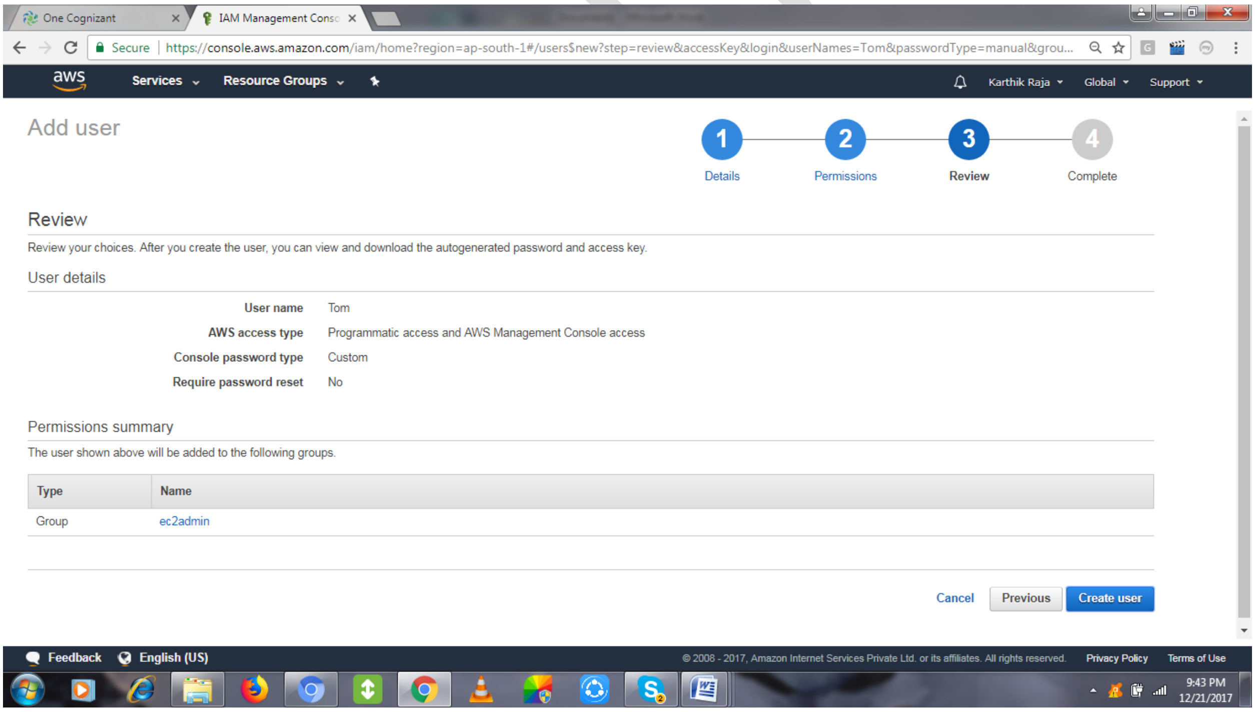
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Create group
Refresh
Search

Showing 1 result

	Group	Attached policies
☑	ec2admin	AmazonEC2FullAccess

Review and create the user finally.



Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

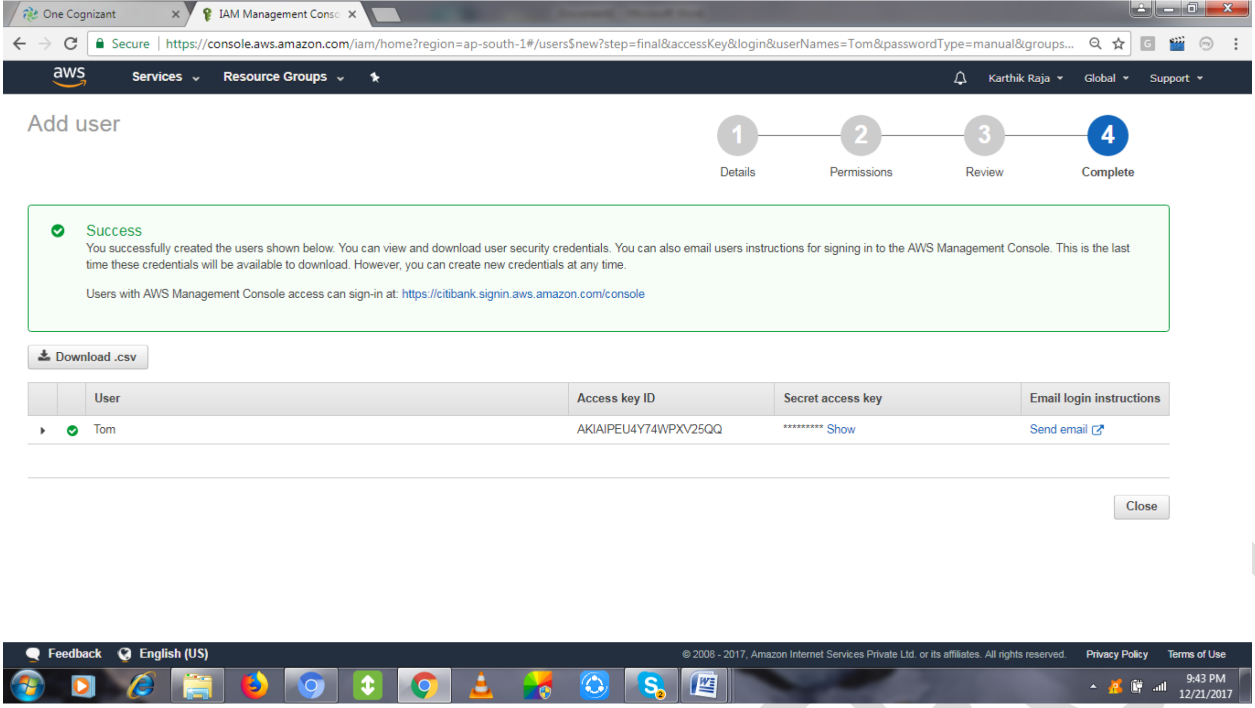
User details

User name	Tom
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	No

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	ec2admin


One Cognizant
IAM Management Conso
Secure | https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=final&accessKey&login&userNames=Tom&passwordType=manual&groups...
aws
Services
Resource Groups
Karthik Raja
Global
Support
1 Details
2 Permissions
3 Review
4 Complete
Download .csv
Close
Feedback
English (US)
© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
9:43 PM
12/21/2017

Add user

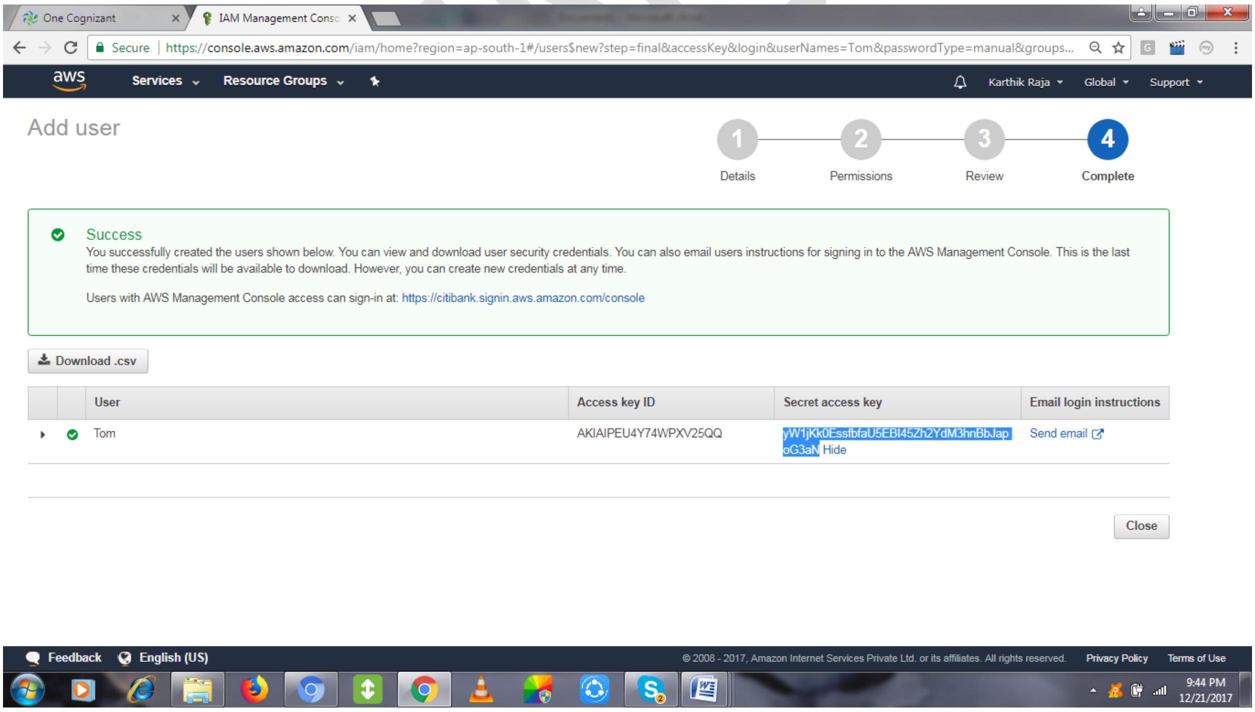
Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://citibank.signin.aws.amazon.com/console

User	Access key ID	Secret access key	Email login instructions
Tom	AKIAIPEU4Y74WPXV25QQ	********* Show	Send email

Collect the Access Key ID & Secret access key and keep it safe for rest of the activities.


One Cognizant
IAM Management Conso
Secure | https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=final&accessKey&login&userNames=Tom&passwordType=manual&groups...
aws
Services
Resource Groups
Karthik Raja
Global
Support
1 Details
2 Permissions
3 Review
4 Complete
Download .csv
Close
Feedback
English (US)
© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
9:44 PM
12/21/2017

Add user

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

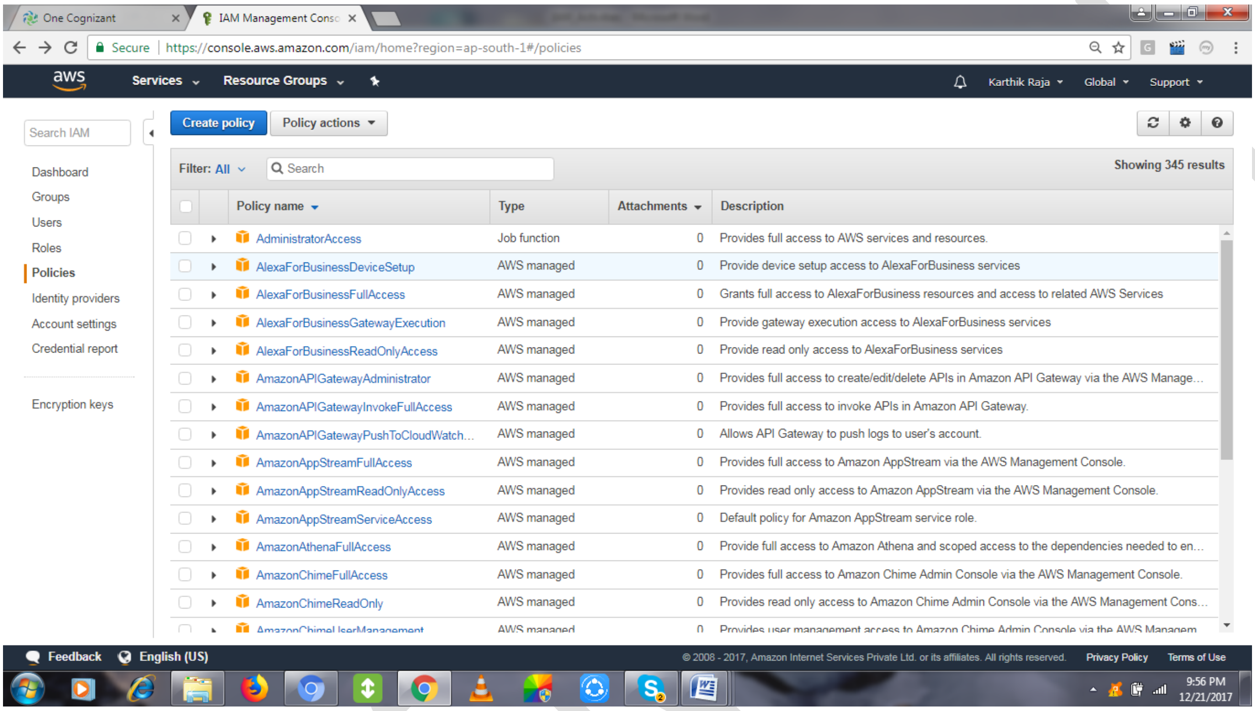
Users with AWS Management Console access can sign-in at: https://citibank.signin.aws.amazon.com/console

User	Access key ID	Secret access key	Email login instructions
Tom	AKIAIPEU4Y74WPXV25QQ	yW1jKk0EssfbfaU5EBI45Zh2YdM3hnBbJapoG3aN Hide	Send email

Activity 4:

Policies are already available have set of permissions, that to be attached for group/user.

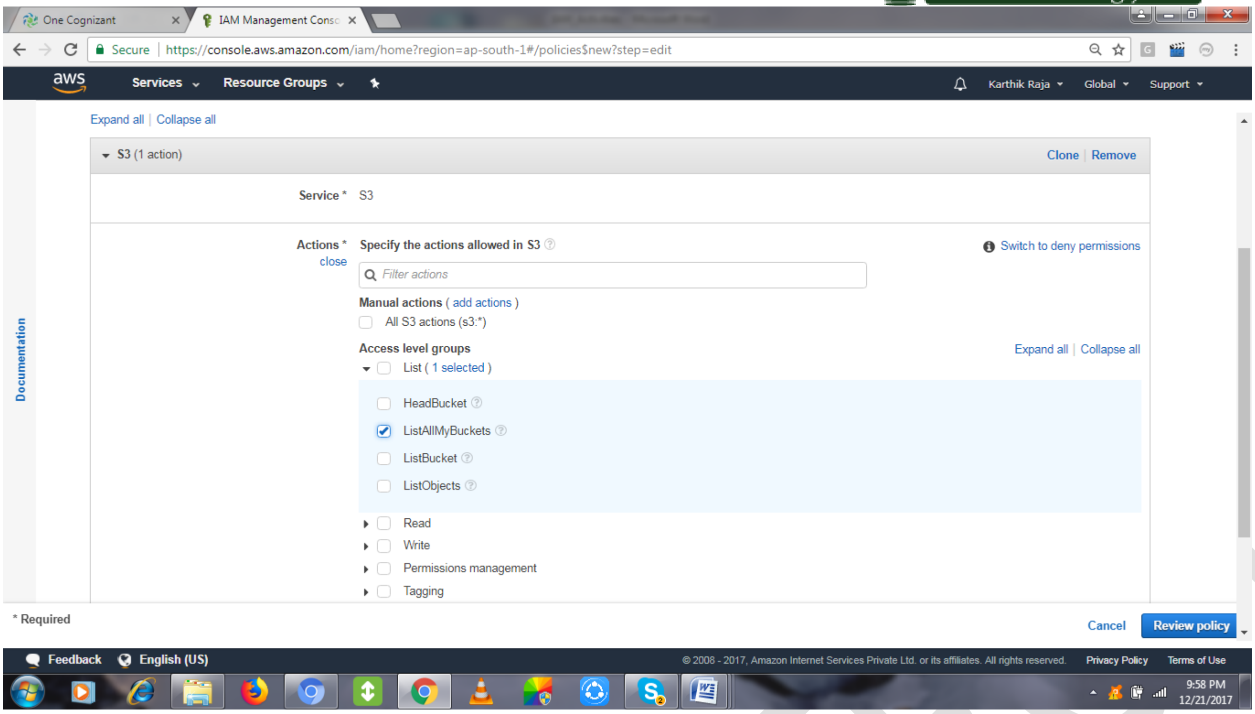
We can create an own Policy too, Click Create Policy.



Policy name	Type	Attachments	Description
AdministratorAccess	Job function	0	Provides full access to AWS services and resources.
AlexaForBusinessDeviceSetup	AWS managed	0	Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS managed	0	Grants full access to AlexaForBusiness resources and access to related AWS Services
AlexaForBusinessGatewayExecution	AWS managed	0	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessReadOnlyAccess	AWS managed	0	Provide read only access to AlexaForBusiness services
AmazonAPIGatewayAdministrator	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Manage...
AmazonAPIGatewayInvokeFullAccess	AWS managed	0	Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewayPushToCloudWatch...	AWS managed	0	Allows API Gateway to push logs to user's account.
AmazonAppStreamFullAccess	AWS managed	0	Provides full access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamReadOnlyAccess	AWS managed	0	Provides read only access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamServiceAccess	AWS managed	0	Default policy for Amazon AppStream service role.
AmazonAthenaFullAccess	AWS managed	0	Provide full access to Amazon Athena and scoped access to the dependencies needed to en...
AmazonChimeFullAccess	AWS managed	0	Provides full access to Amazon Chime Admin Console via the AWS Management Console.
AmazonChimeReadOnly	AWS managed	0	Provides read only access to Amazon Chime Admin Console via the AWS Management Cons...
AmazonChimeUserManagement	AWS managed	0	Provides user management access to Amazon Chime Admin Console via the AWS Managem

Feedback
English (US)
© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
9:56 PM
12/21/2017

Search the service and select a portion of access that needs to be provided as permission.



S3 (1 action)

Service * S3

Actions * Specify the actions allowed in S3

Manual actions (add actions)

□ All S3 actions (s3:*)

Access level groups

□ List (1 selected)

□ HeadBucket

☑ ListAllMyBuckets

□ ListBucket

□ ListObjects

□ Read

□ Write

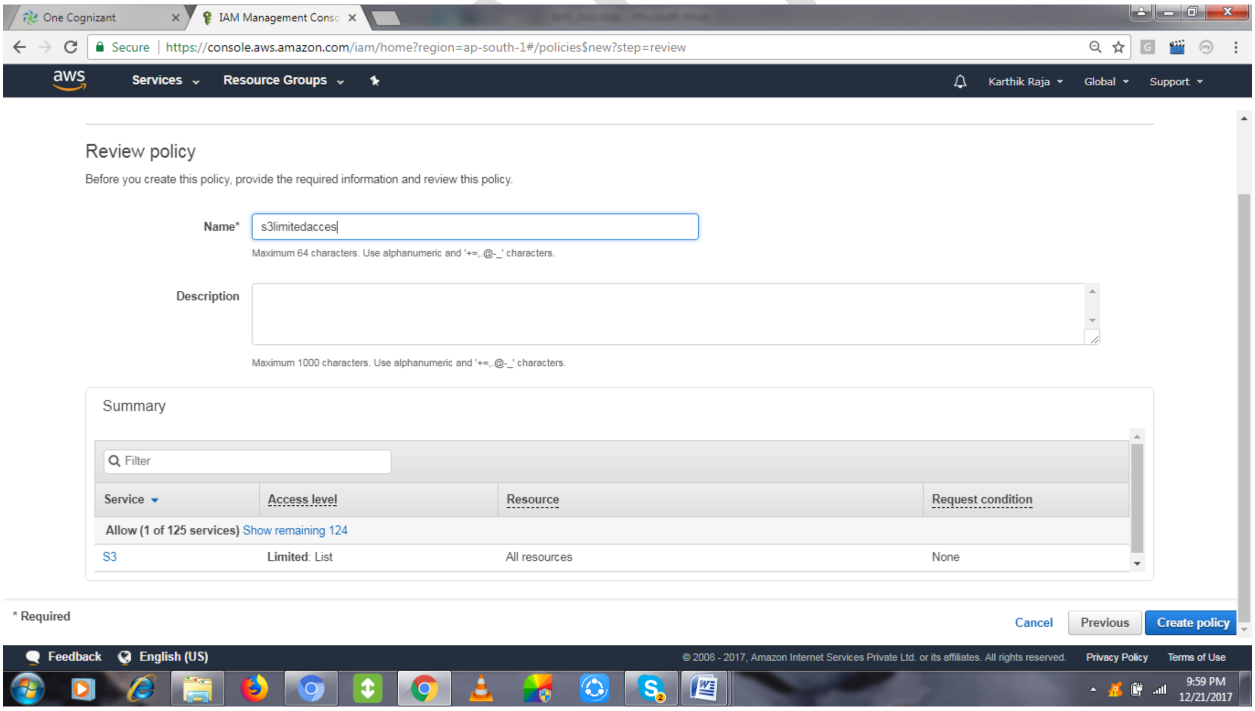
□ Permissions management

□ Tagging

* Required

One Cognizant
IAM Management Consc
Secure
https://console.aws.amazon.com/iam/home?region=ap-south-1#/policies$new?step=edit
aws
Services
Resource Groups
Karthik Raja
Global
Support
Expand all | Collapse all
Documentation
Clone | Remove
close
Filter actions
Switch to deny permissions
Expand all | Collapse all
Cancel
Review policy
Feedback
English (US)
© 2008 - 2017, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
9:58 PM
12/21/2017

Name the policy, review and create it.



Review policy

Before you create this policy, provide the required information and review this policy.

Name* s3limitedacces

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

Description

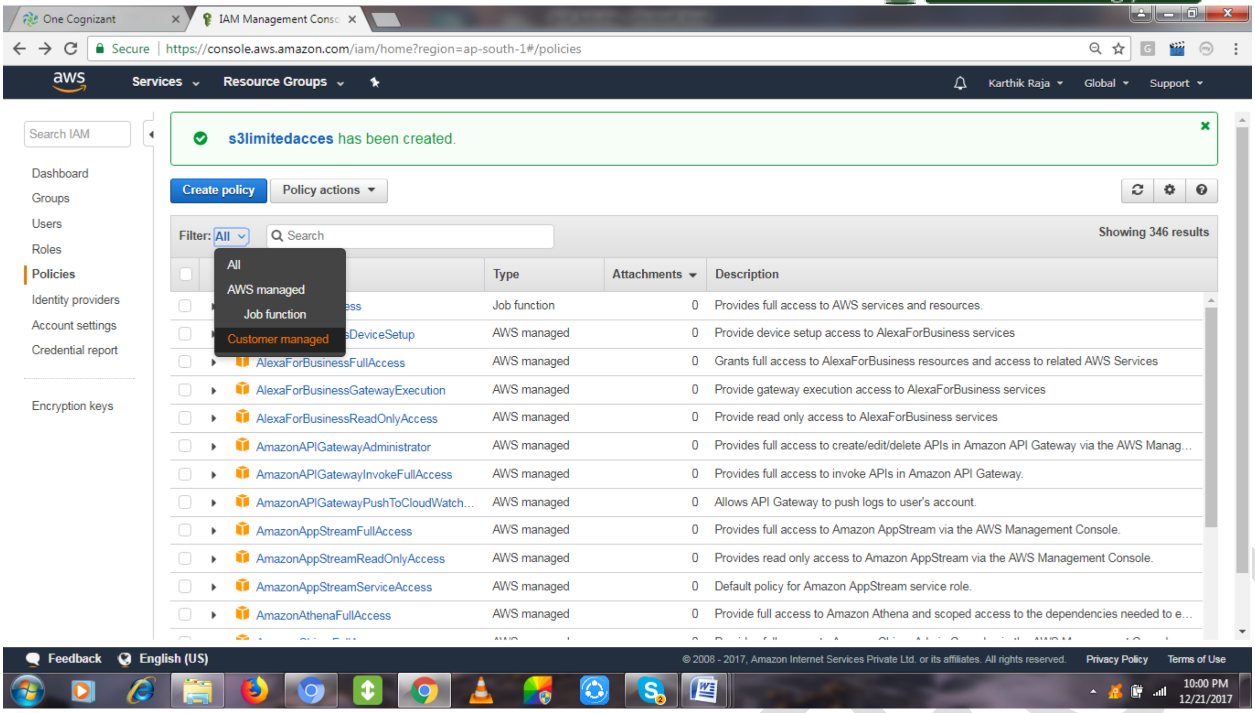
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 125 services) Show remaining 124			
S3	Limited: List	All resources	None

* Required

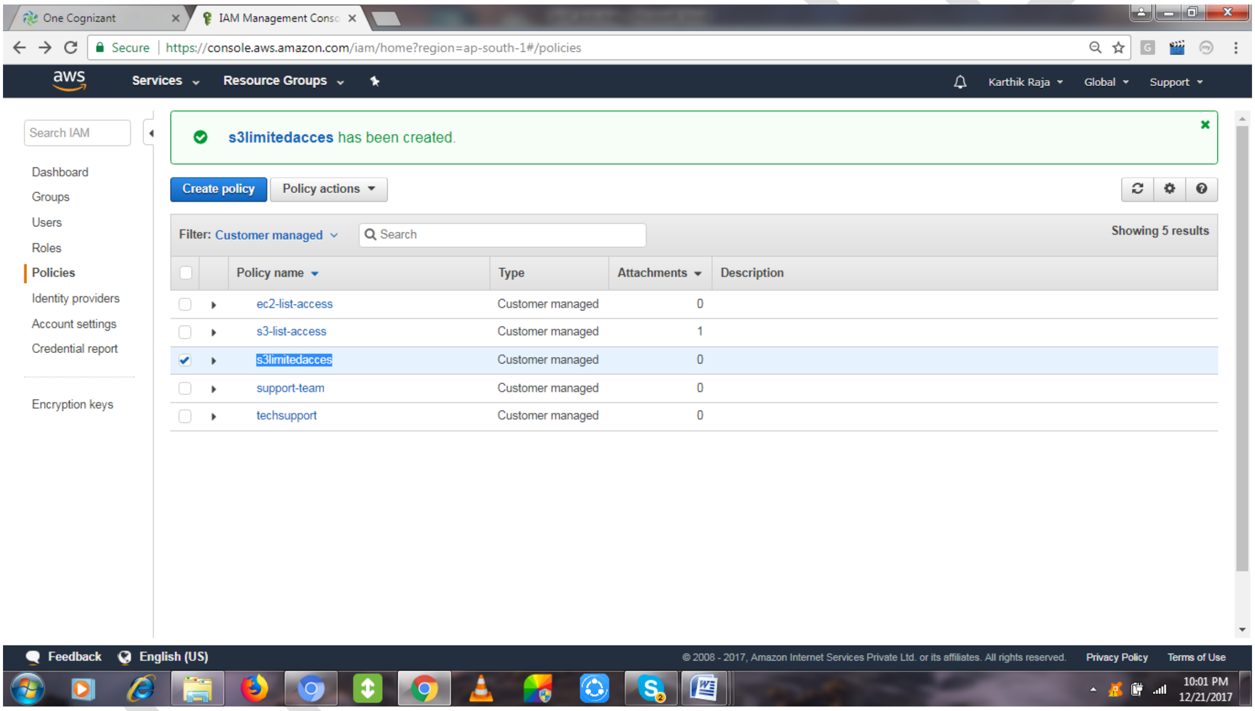
You can check under Customer managed section for the created policy.



s3limitedacces has been created.

Showing 346 results

Policy name	Type	Attachments	Description
…ess	Job function	0	Provides full access to AWS services and resources.
…sDeviceSetup	AWS managed	0	Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS managed	0	Grants full access to AlexaForBusiness resources and access to related AWS Services
AlexaForBusinessGatewayExecution	AWS managed	0	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessReadOnlyAccess	AWS managed	0	Provide read only access to AlexaForBusiness services
AmazonAPIGatewayAdministrator	AWS managed	0	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Manag…
AmazonAPIGatewayInvokeFullAccess	AWS managed	0	Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewayPushToCloudWatch…	AWS managed	0	Allows API Gateway to push logs to user's account.
AmazonAppStreamFullAccess	AWS managed	0	Provides full access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamReadOnlyAccess	AWS managed	0	Provides read only access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamServiceAccess	AWS managed	0	Default policy for Amazon AppStream service role.
AmazonAthenaFullAccess	AWS managed	0	Provide full access to Amazon Athena and scoped access to the dependencies needed to e…



s3limitedacces has been created.

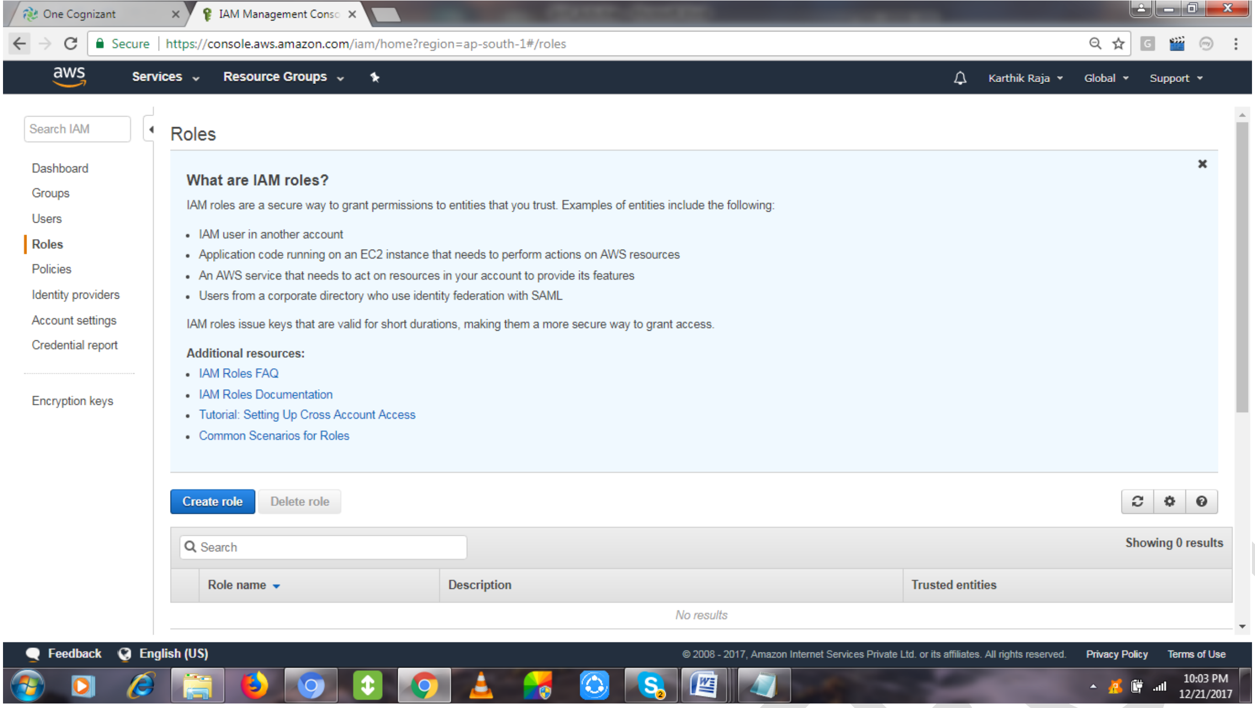
Filter: Customer managed

Showing 5 results

	Policy name	Type	Attachments	Description
□	ec2-list-access	Customer managed	0	
□	s3-list-access	Customer managed	1	
☑	s3limitedacces	Customer managed	0	
□	support-team	Customer managed	0	
□	techsupport	Customer managed	0	

Activity 5:

To create the new role by clicking Create Role.



Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

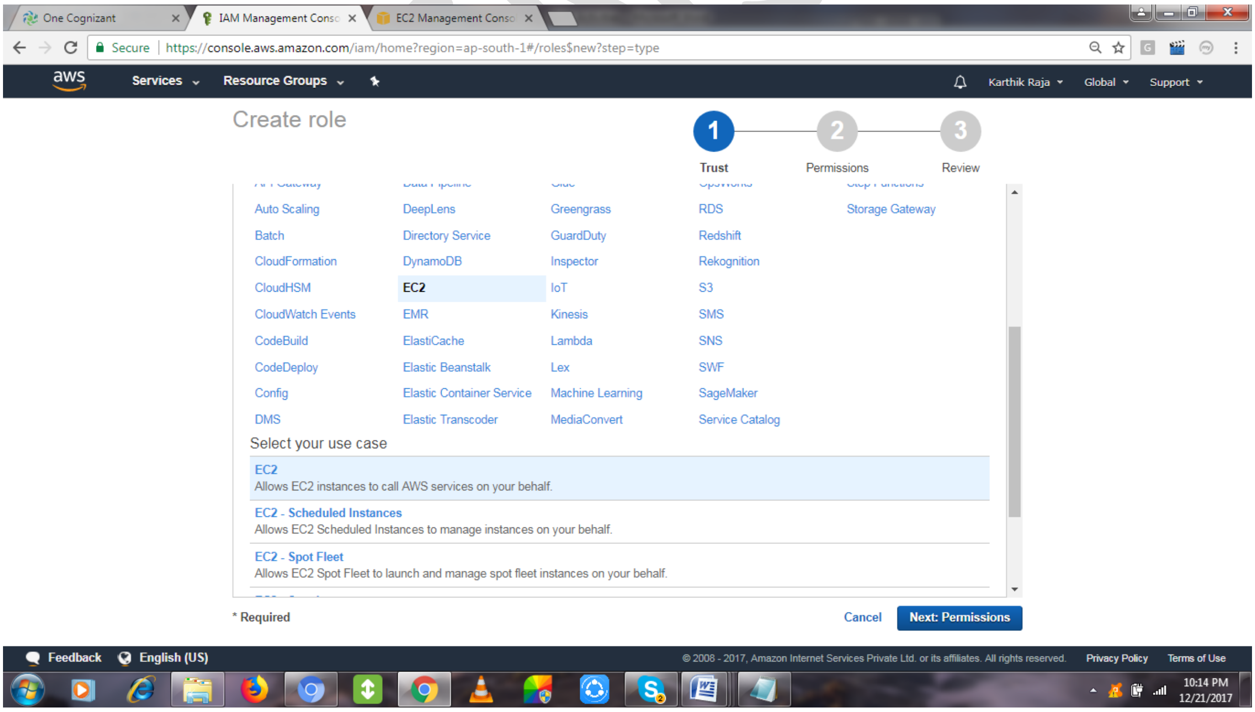
- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

Role name	Description	Trusted entities

Showing 0 results

No results

Choose any AWS Resource for allocating Role level mapping for it, Choosing **S3.**



Create role

Auto Scaling, Batch, CloudFormation, CloudHSM, CloudWatch Events, CodeBuild, CodeDeploy, Config, DMS

DeepLens, Directory Service, DynamoDB, EC2, EMR, ElastiCache, Elastic Beanstalk, Elastic Container Service, Elastic Transcoder

Greengrass, GuardDuty, Inspector, IoT, Kinesis, Lambda, Lex, Machine Learning, MediaConvert

RDS, Redshift, Rekognition, S3, SMS, SNS, SWF, SageMaker, Service Catalog

Storage Gateway

Select your use case

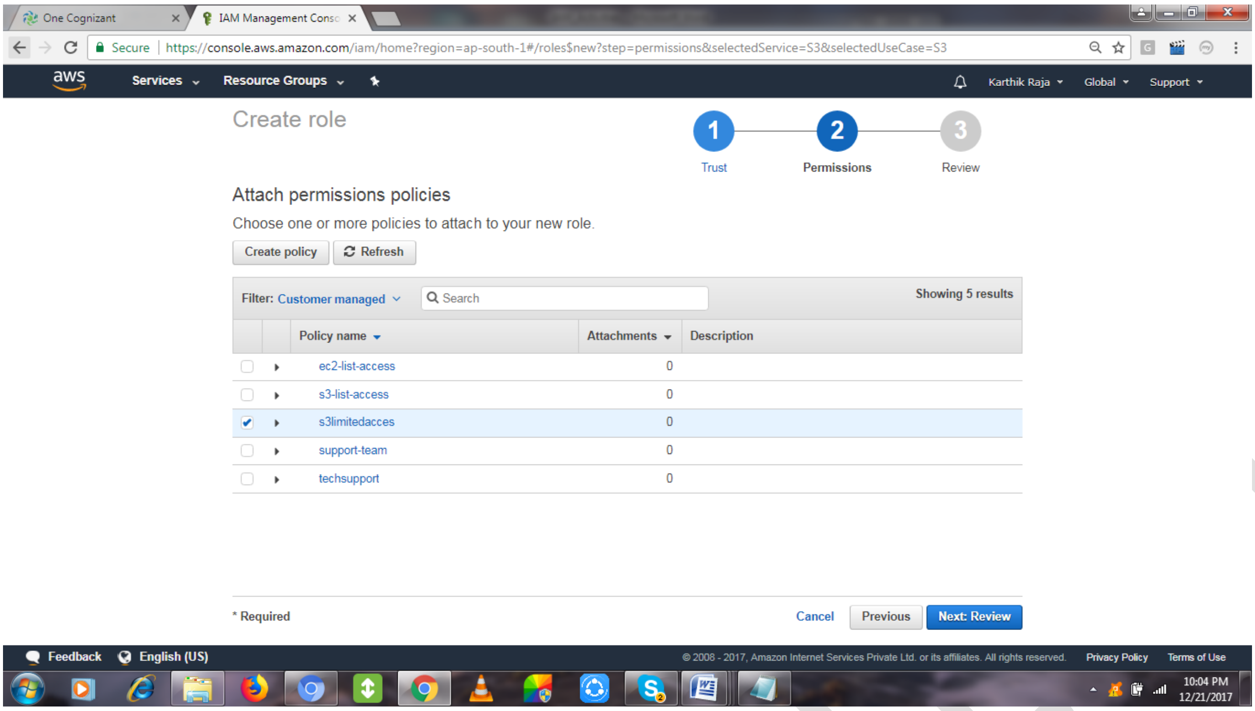
EC2
Allows EC2 instances to call AWS services on your behalf.

EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.

EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

* Required

Choosing the customer managed policy, which we created in the earlier activity.



https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles$new?step=permissions&selectedService=S3&selectedUseCase=S3

Create role

1 Trust — 2 Permissions — 3 Review

Attach permissions policies

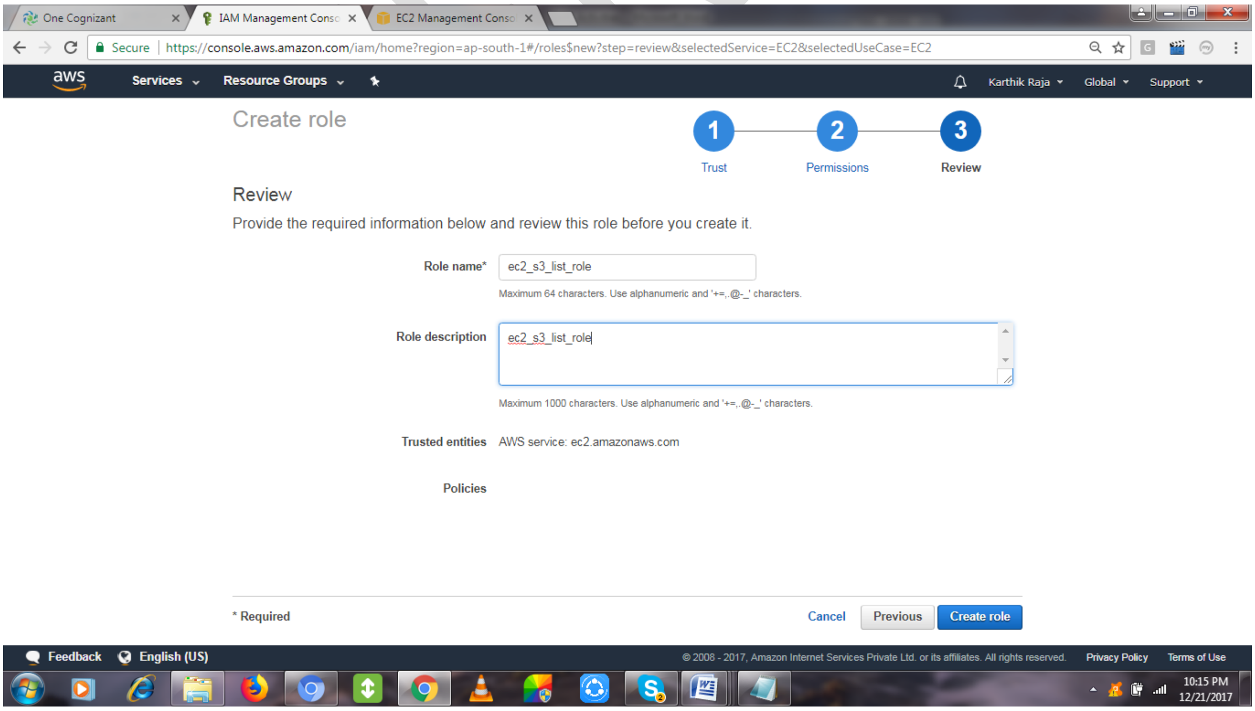
Choose one or more policies to attach to your new role.

Filter: Customer managed   Search   Showing 5 results

		Policy name	Attachments	Description
□	▸	ec2-list-access	0	
□	▸	s3-list-access	0	
☑	▸	s3limitedacces	0	
□	▸	support-team	0	
□	▸	techsupport	0	

* Required

Review and create it with a name for reference to choose this IAM ROLE.



https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles$new?step=review&selectedService=EC2&selectedUseCase=EC2

Create role

1 Trust — 2 Permissions — 3 Review

Review

Provide the required information below and review this role before you create it.

Role name* ec2_s3_list_role

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

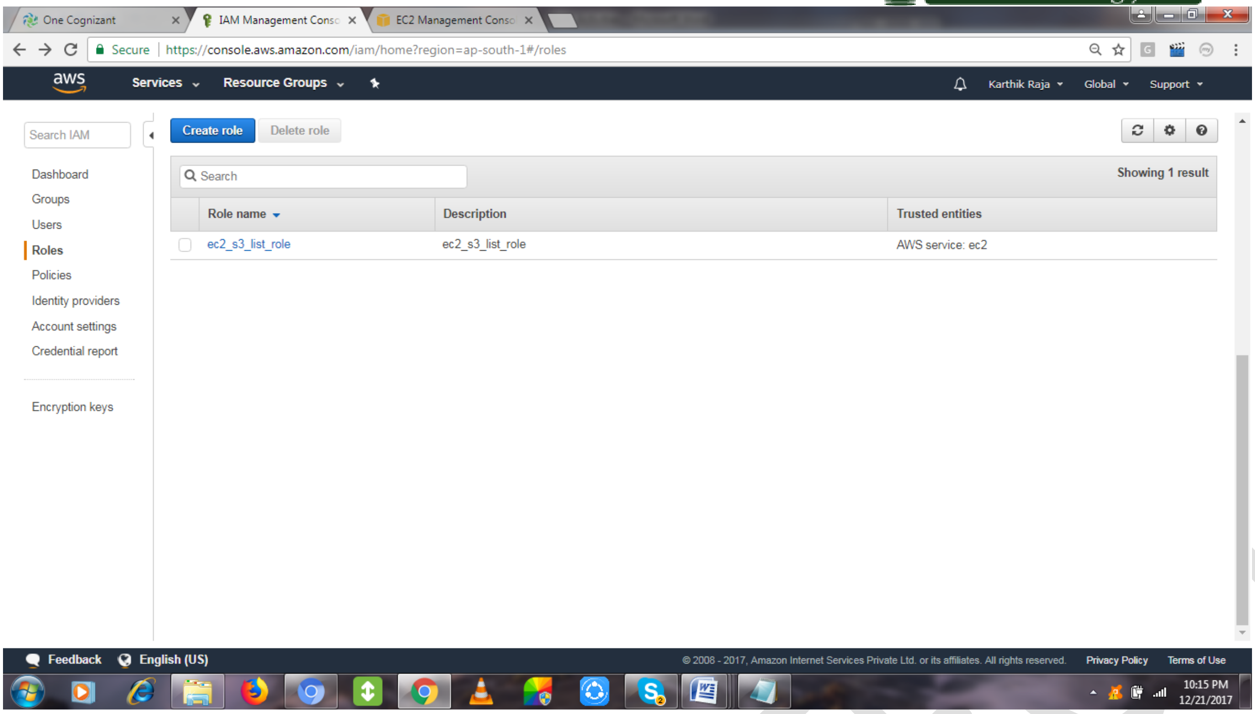
Role description ec2_s3_list_role

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

Trusted entities AWS service: ec2.amazonaws.com

Policies

* Required



https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles

Create role | Delete role

Search IAM

- Dashboard
- Groups
- Users
- **Roles**
- Policies
- Identity providers
- Account settings
- Credential report
- Encryption keys

Showing 1 result

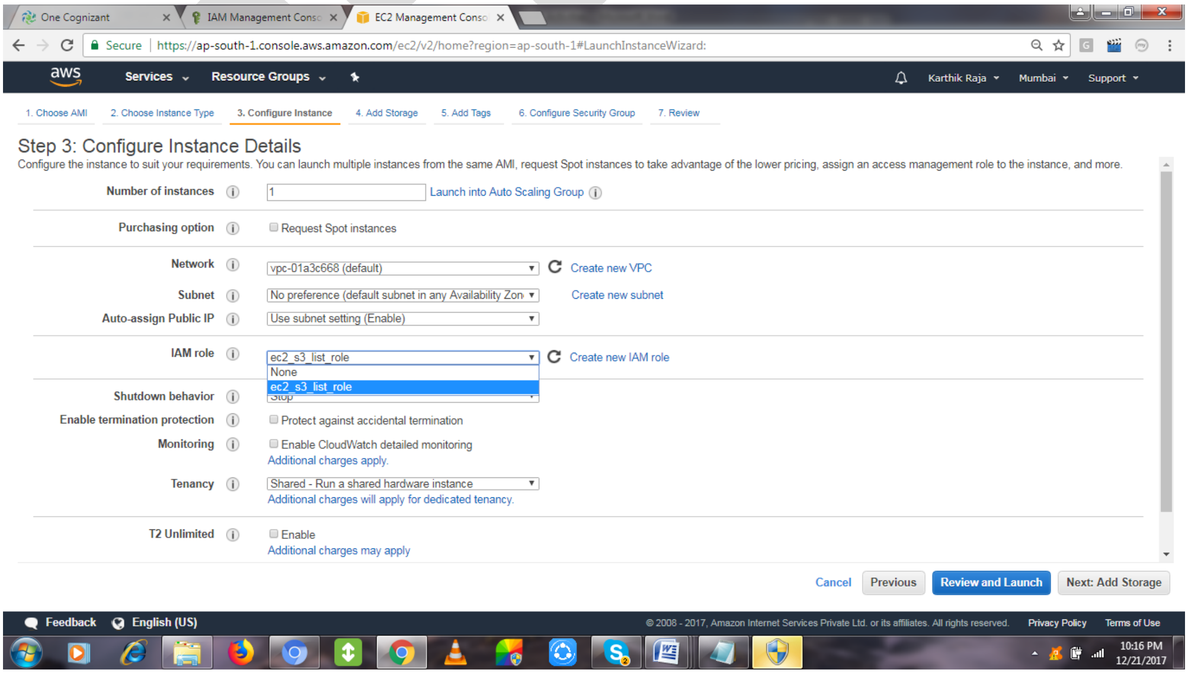
	Role name	Description	Trusted entities
□	ec2_s3_list_role	ec2_s3_list_role	AWS service: ec2

IAM Role Test scenario:

Create an EC2 with IAM Role and attached to it, so that after login in into the EC2 server it will not expect.

- "AWS configuration" to list the S3 listing activity [for which the role has been created].
- Also No access/secret key is required for setting the configuration.

Mapping the created the Role for the Creating EC2:



https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 | Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-01a3c668 (default) | Create new VPC

Subnet: No preference (default subnet in any Availability Zon | Create new subnet

Auto-assign Public IP: Use subnet setting (Enable)

IAM role: ec2_s3_list_role (options: None, ec2_s3_list_role) | Create new IAM role

Shutdown behavior: Stop

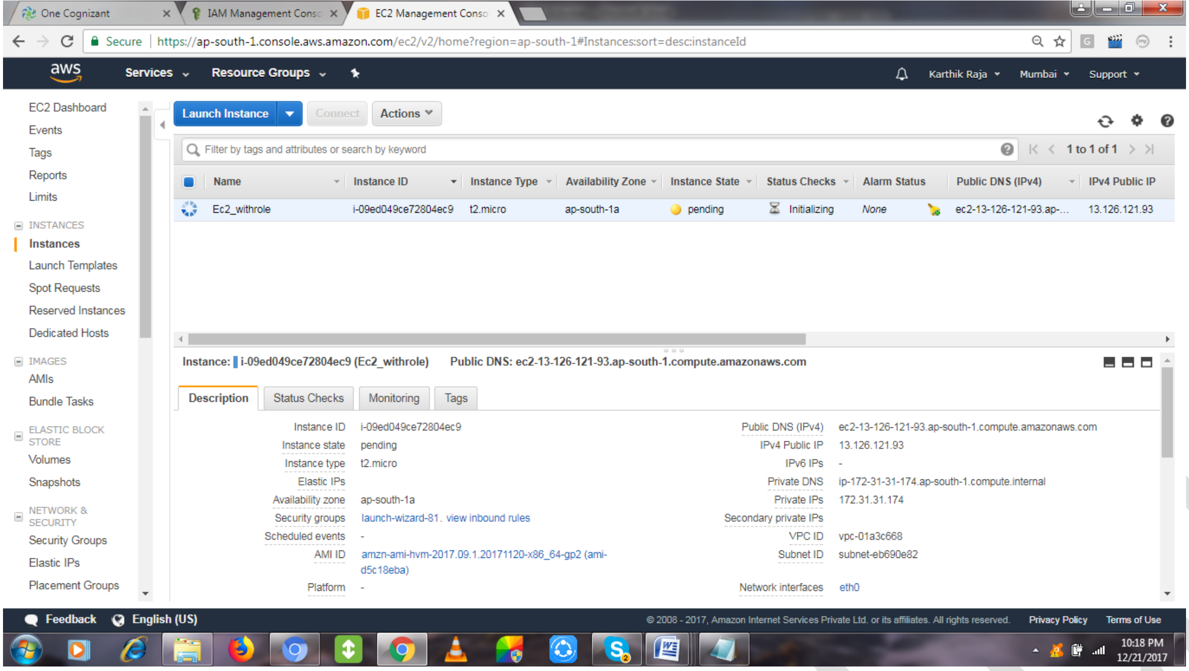
Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

T2 Unlimited: □ Enable
Additional charges may apply

Cancel | Previous | Review and Launch | Next: Add Storage

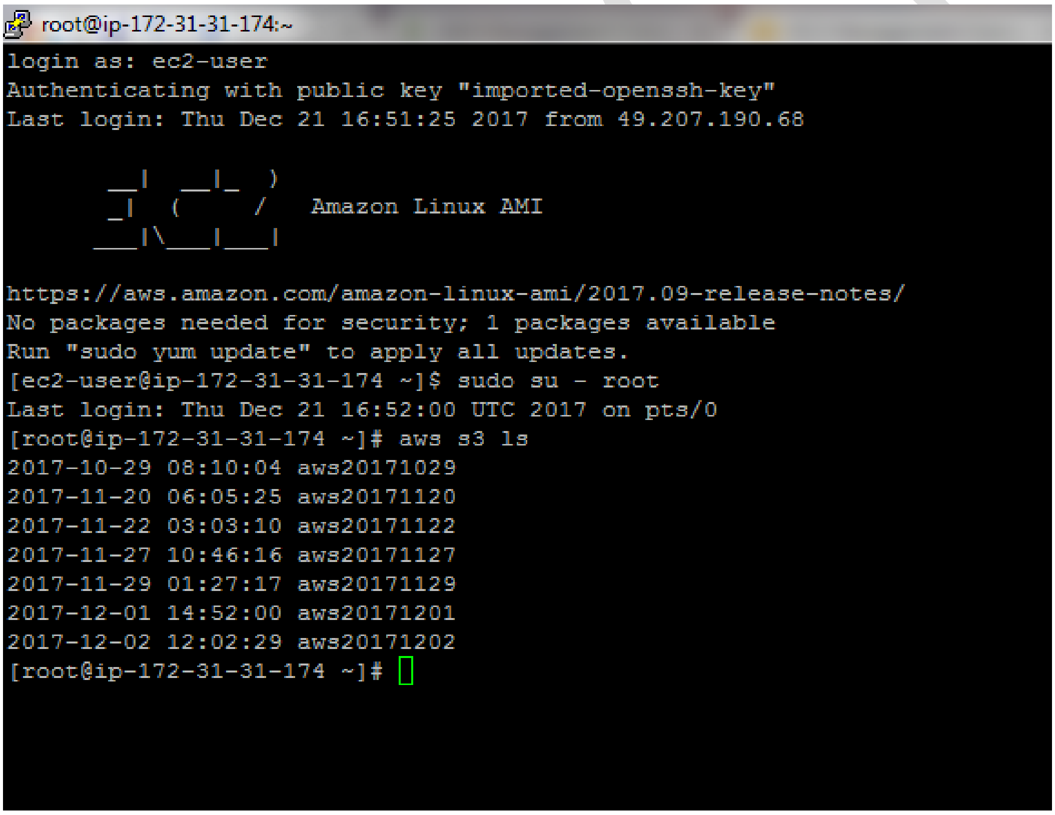


Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
Ec2_withrole	i-09ed049ce72804ec9	t2.micro	ap-south-1a	pending	Initializing	None	ec2-13-126-121-93.ap-...	13.126.121.93

Instance: i-09ed049ce72804ec9 (Ec2_withrole) Public DNS: ec2-13-126-121-93.ap-south-1.compute.amazonaws.com

Instance ID	i-09ed049ce72804ec9	Public DNS (IPv4)	ec2-13-126-121-93.ap-south-1.compute.amazonaws.com
Instance state	pending	IPv4 Public IP	13.126.121.93
Instance type	t2.micro	IPv6 IPs	-
Elastic IPs		Private DNS	ip-172-31-31-174.ap-south-1.compute.internal
Availability zone	ap-south-1a	Private IPs	172.31.31.174
Security groups	launch-wizard-81. view inbound rules	Secondary private IPs	
Scheduled events	-	VPC ID	vpc-01a3c668
AMI ID	amzn-ami-hvm-2017.09.1.20171120-x86_64-gp2 (ami-d5c18eba)	Subnet ID	subnet-eb690e82
Platform	-	Network interfaces	eth0

Once login into the EC2 and check with the S3 Bucket Listing command – **AWS S3 ls**



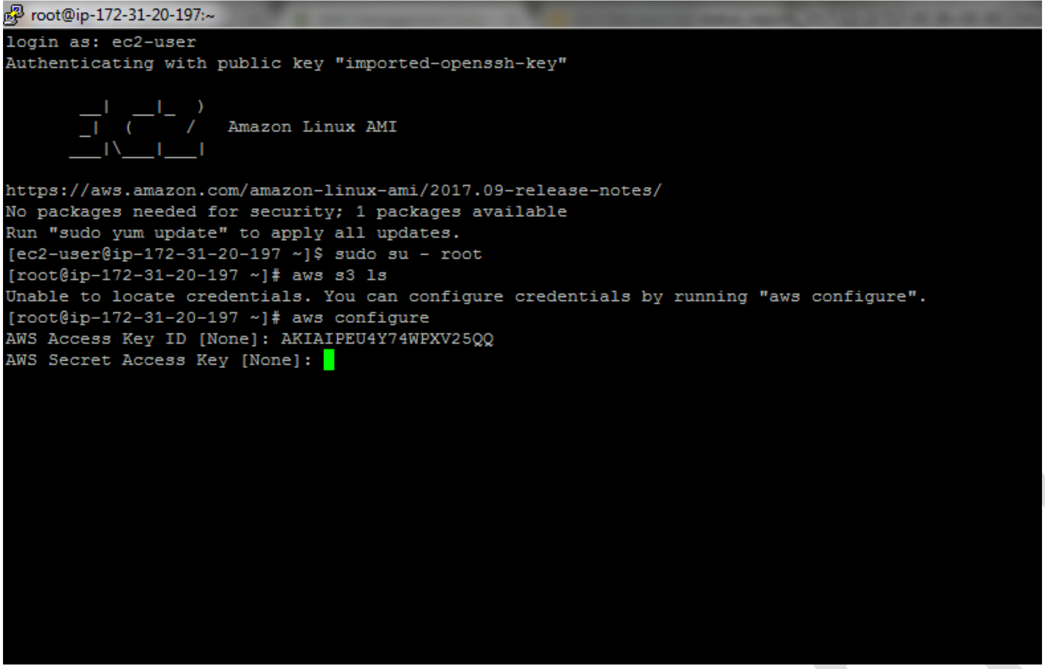
```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Thu Dec 21 16:51:25 2017 from 49.207.190.68

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

https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
No packages needed for security; 1 packages available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-31-174 ~]$ sudo su - root
Last login: Thu Dec 21 16:52:00 UTC 2017 on pts/0
[root@ip-172-31-31-174 ~]# aws s3 ls
2017-10-29 08:10:04 aws20171029
2017-11-20 06:05:25 aws20171120
2017-11-22 03:03:10 aws20171122
2017-11-27 10:46:16 aws20171127
2017-11-29 01:27:17 aws20171129
2017-12-01 14:52:00 aws20171201
2017-12-02 12:02:29 aws20171202
[root@ip-172-31-31-174 ~]#
```

Compare the same by creating an EC2 without attaching the role, you can see the difference.

It will ask Access/Secret Key, etc.



```
login as: ec2-user
Authenticating with public key "imported-openssh-key"

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

https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/
No packages needed for security; 1 packages available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-20-197 ~]$ sudo su - root
[root@ip-172-31-20-197 ~]# aws s3 ls
Unable to locate credentials. You can configure credentials by running "aws configure".
[root@ip-172-31-20-197 ~]# aws configure
AWS Access Key ID [None]: AKIAIPEU4Y74WPXV25QQ
AWS Secret Access Key [None]:
```