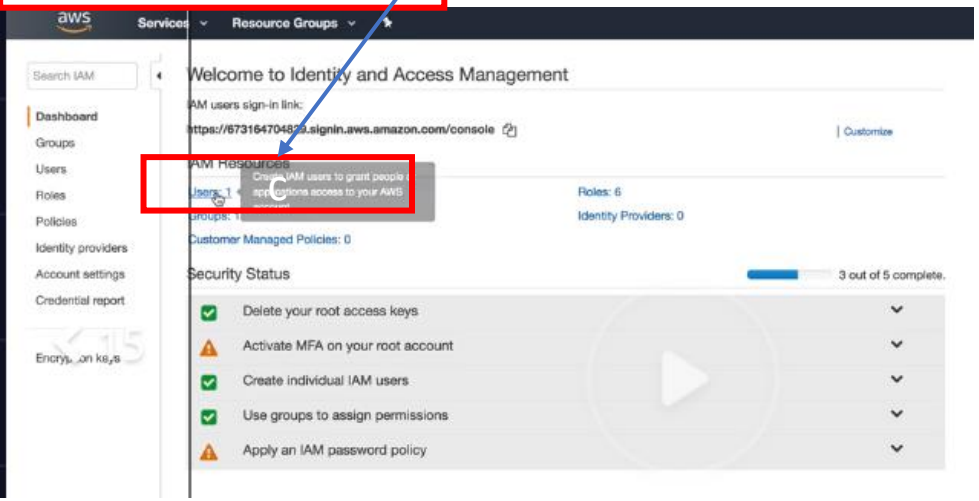
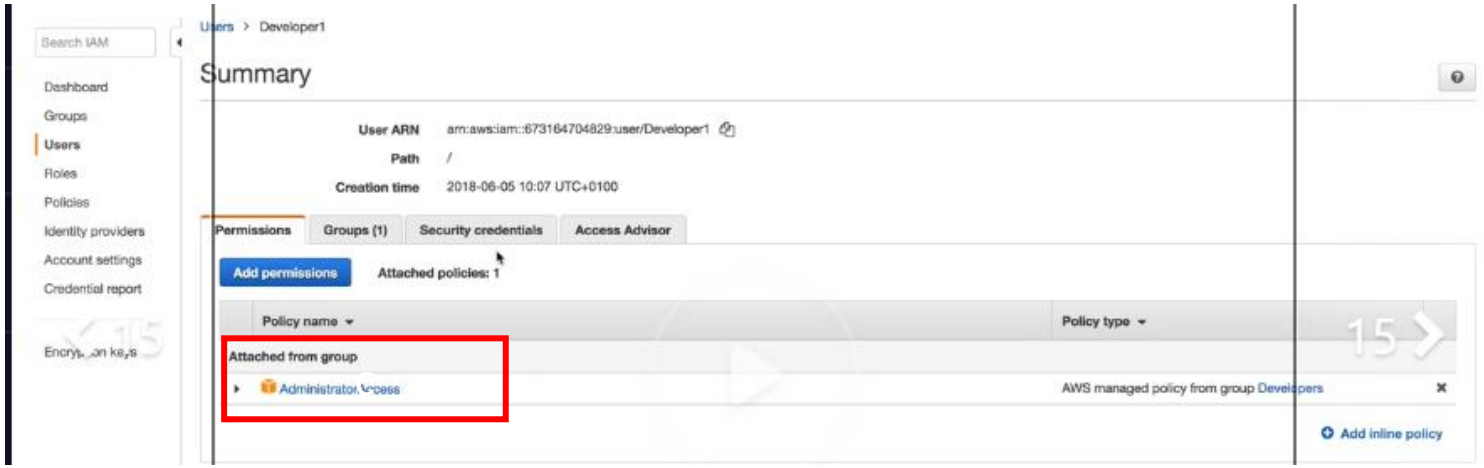
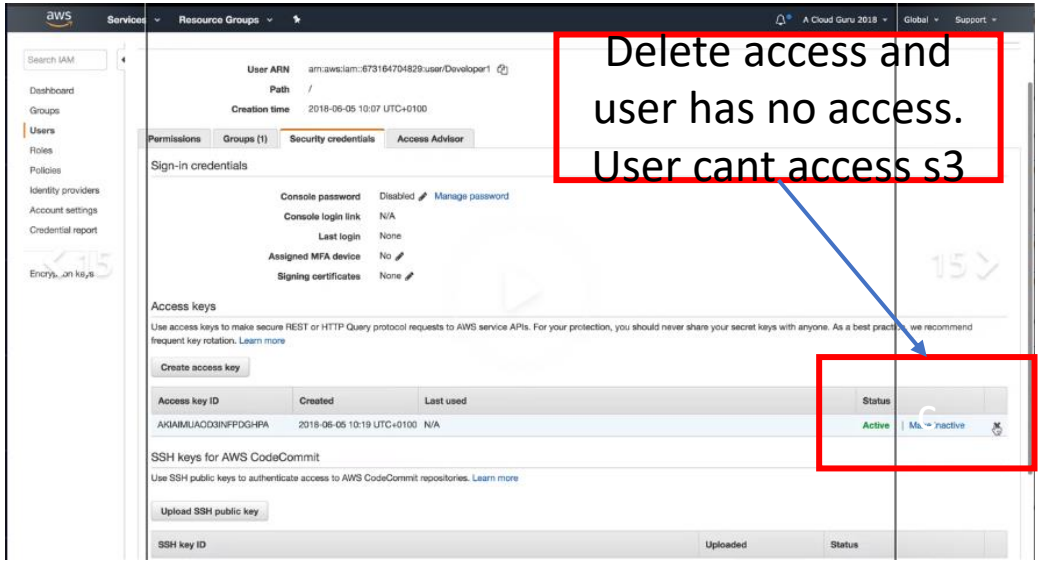
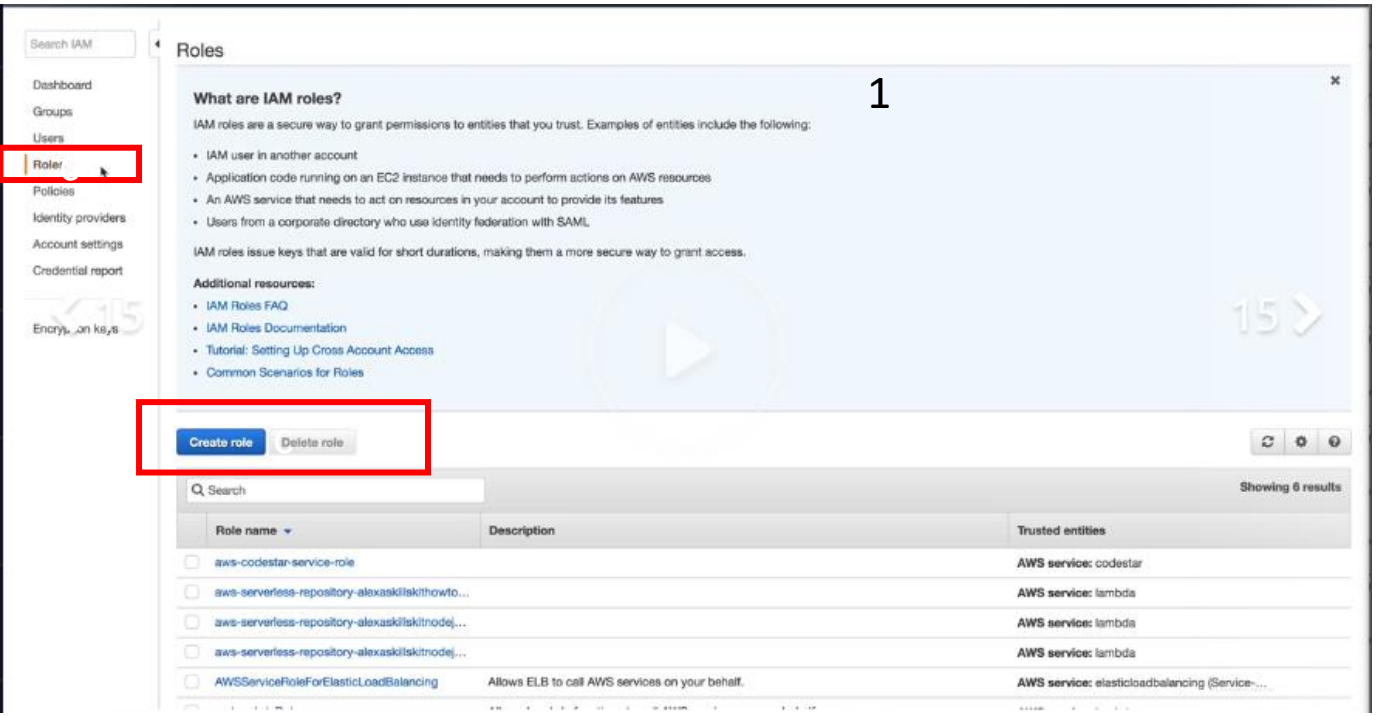
Services → IAM →

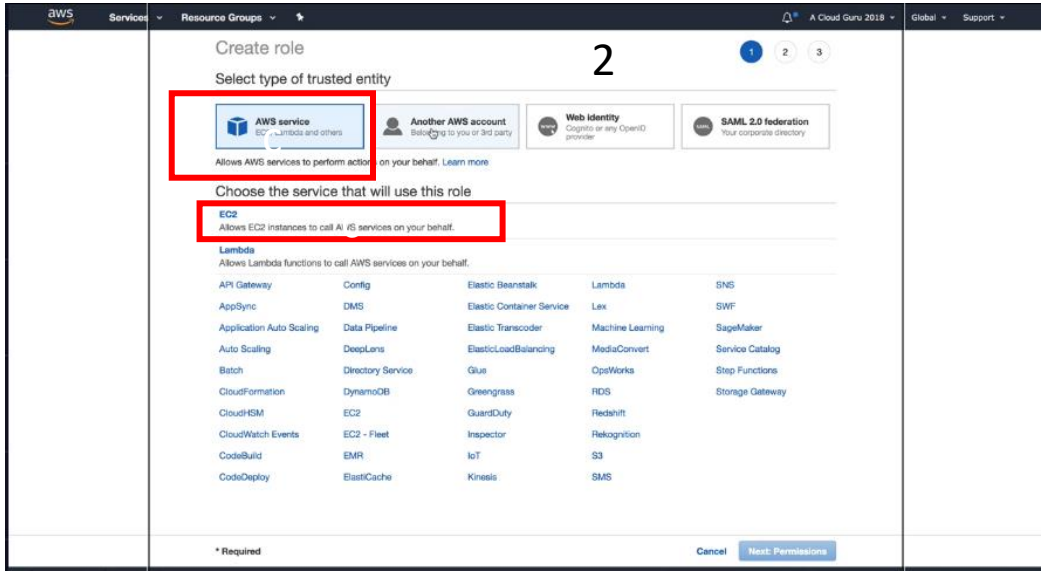


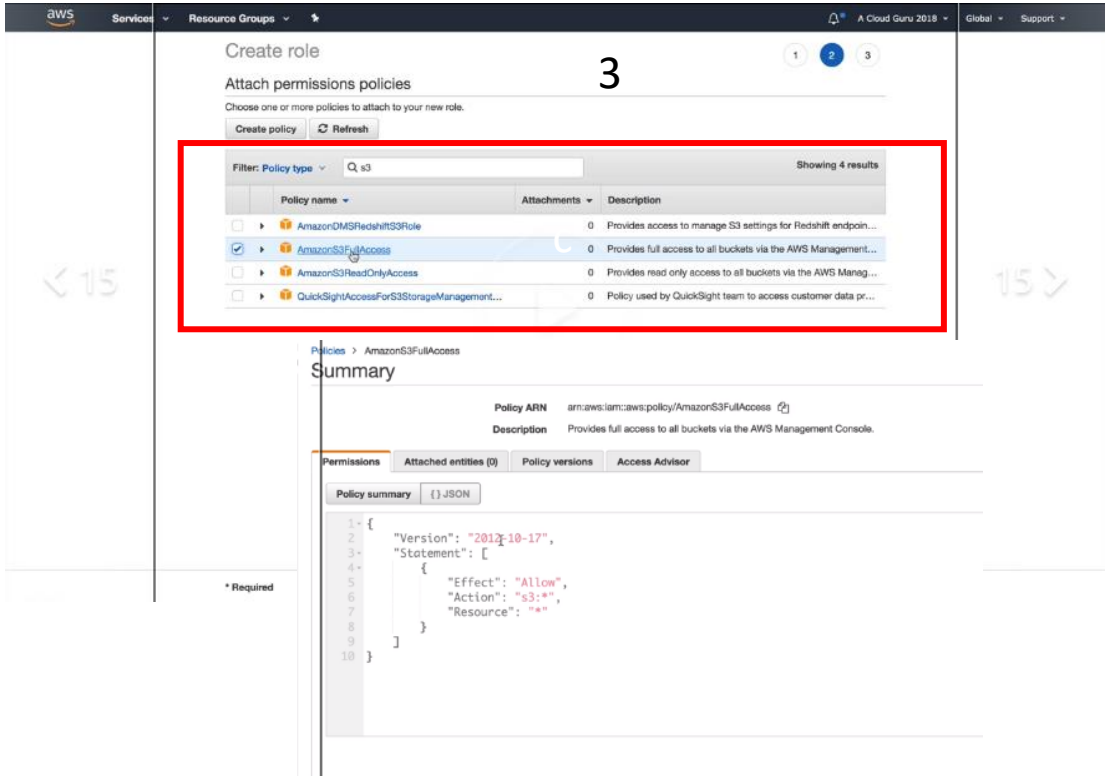


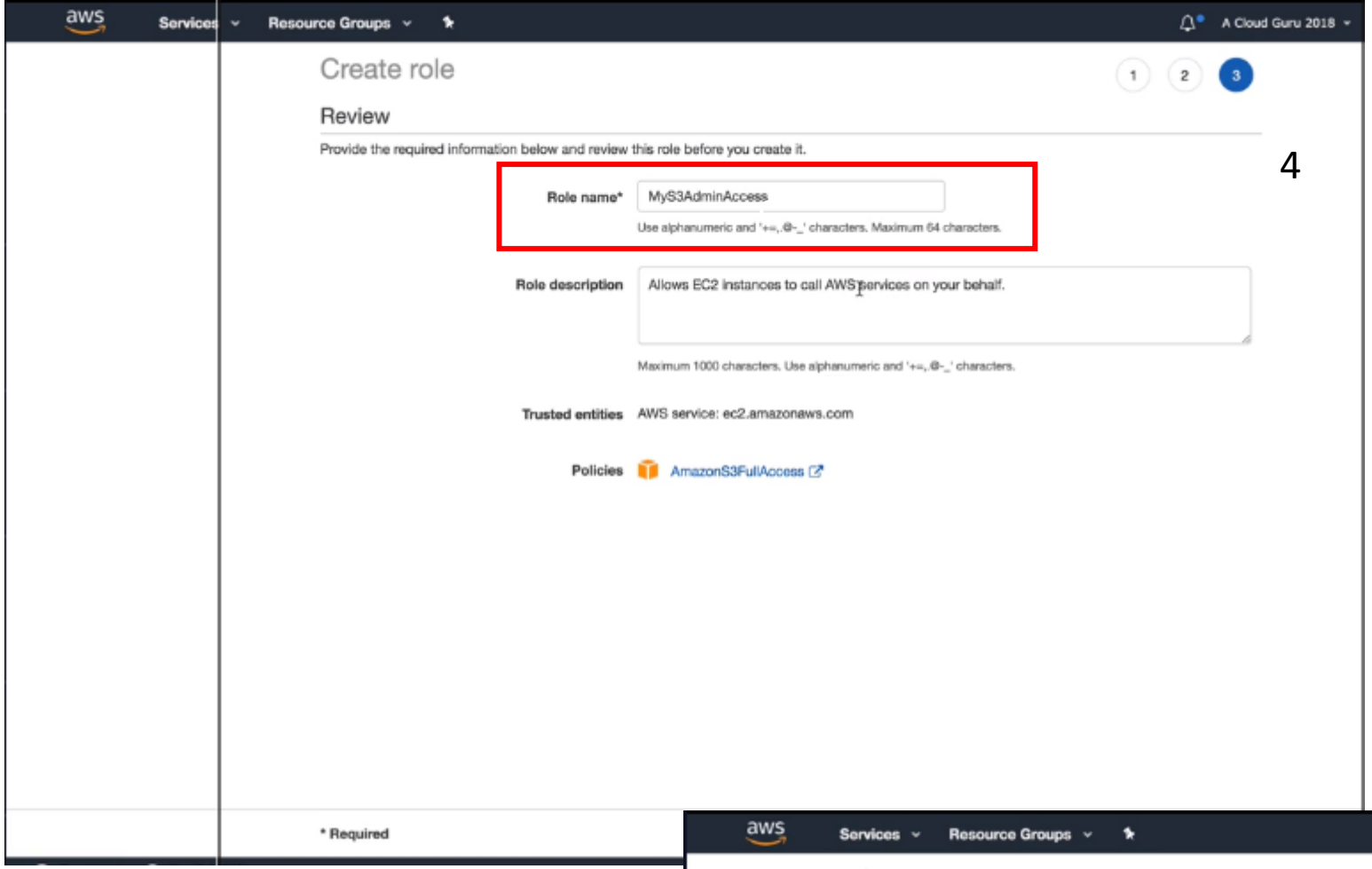


Creating Roles

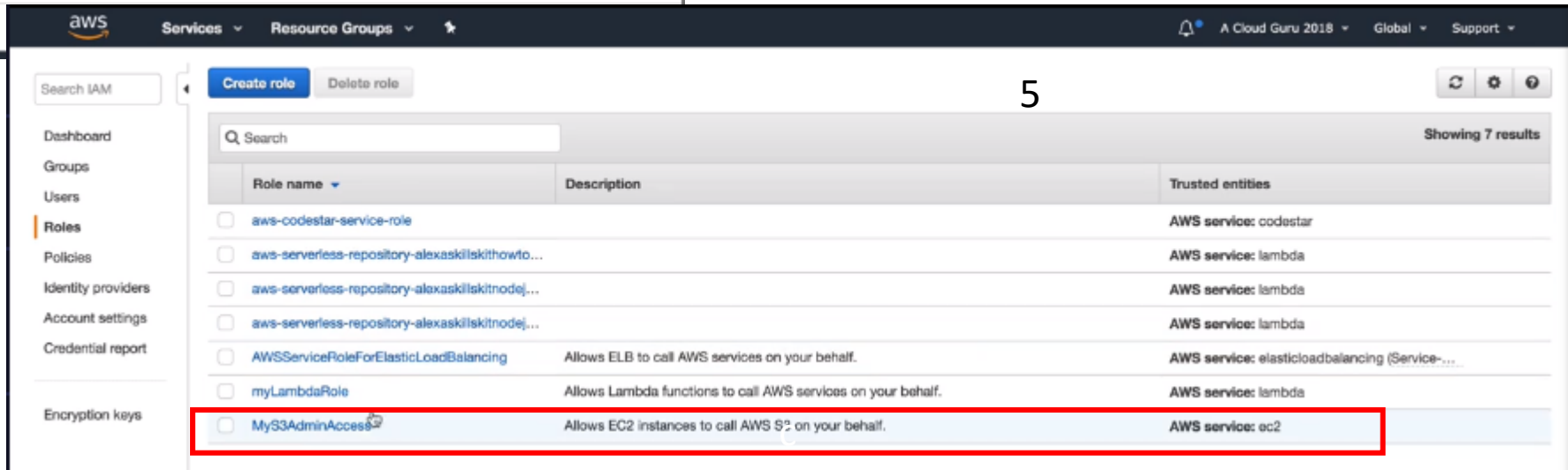






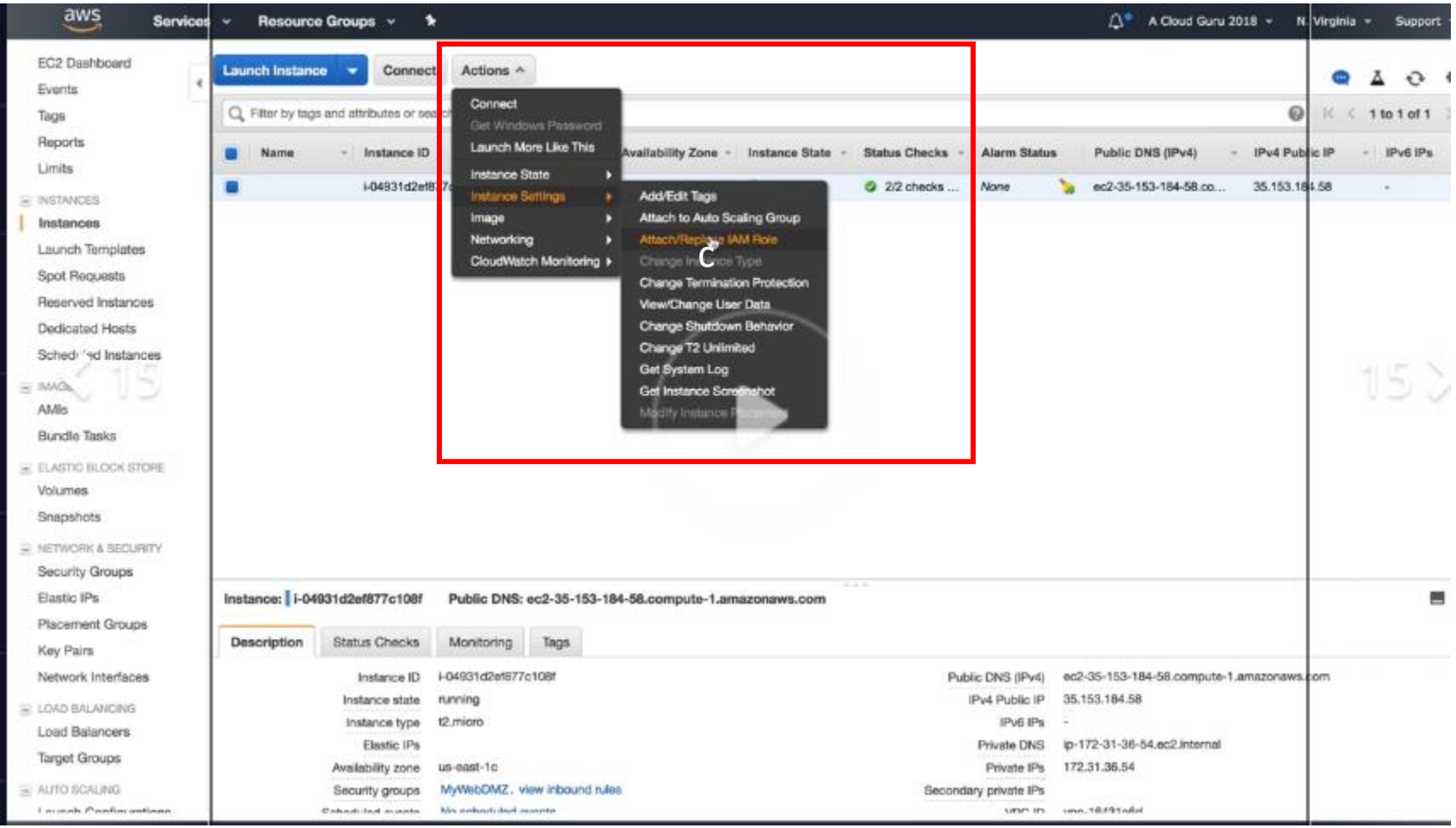

Services
Resource Groups
A Cloud Guru 2018
Create role
1
2
3
Review
Provide the required information below and review this role before you create it.
Role name*
MyS3AdminAccess
Use alphanumeric and '+=,.@-_' characters. Maximum 64 characters.
Role description
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Trusted entities
AWS service: ec2.amazonaws.com
Policies
AmazonS3FullAccess
* Required

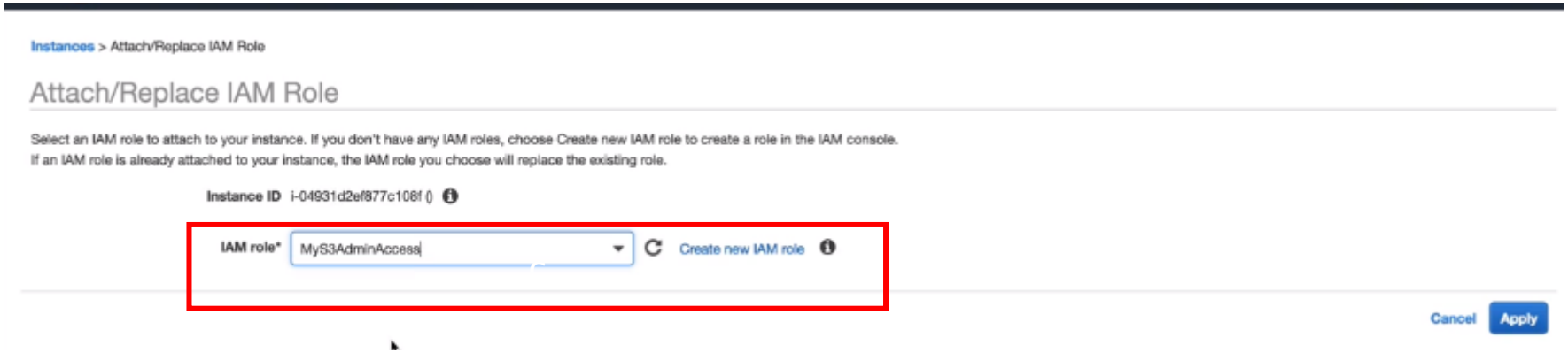
4


Services
Resource Groups
A Cloud Guru 2018
Global
Support
Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Create role
Delete role
Search
Showing 7 results
Role name
Description
Trusted entities
aws-codestar-service-role
AWS service: codestar
aws-serverless-repository-alexaskillskithowto...
AWS service: lambda
aws-serverless-repository-alexaskillskitnodej...
AWS service: lambda
aws-serverless-repository-alexaskillskitnodej...
AWS service: lambda
AWSServiceRoleForElasticLoadBalancing
Allows ELB to call AWS services on your behalf.
AWS service: elasticloadbalancing (Service-...
myLambdaRole
Allows Lambda functions to call AWS services on your behalf.
AWS service: lambda
MyS3AdminAccess
Allows EC2 instances to call AWS S3 on your behalf.
AWS service: ec2

5

Attaching IAM role to EC2 instance





1

```
[root@ip-172-31-36-54 ec2-user]# aws s3 ls

An error occurred (InvalidAccessKeyId) when calling the ListBuckets oper
ation: The AWS Access Key Id you provided does not exist in our records.
[root@ip-172-31-36-54 ec2-user]# aws s3 ls

An error occurred (InvalidAccessKeyId) when calling the ListBuckets oper
ation: The AWS Access Key Id you provided does not exist in our records.
[root@ip-172-31-36-54 ec2-user]# cd ~/.aws
[root@ip-172-31-36-54 .aws]# ls
config  credentials
[root@ip-172-31-36-54 .aws]# rm credentials
rm: remove regular file 'credentials'? y
[root@ip-172-31-36-54 .aws]# rm config
rm: remove regular file 'config'? y
[root@ip-172-31-36-54 .aws]# ls
[root@ip-172-31-36-54 .aws]# cd /
[root@ip-172-31-36-54 /]#
```

Throws error because it has invalid keys
Deleting config and credentials from the root directory will help in accessing the s3 again
Accessing S3 using roles instead of access and secret key

2

```
[root@ip-172-31-36-54 /]# aws s3 ls
2018-06-05 09:09:28 acloudguru1234-rk
[root@ip-172-31-36-54 /]# aws s3 ls s3://acloudguru1234-rk
2018-06-05 09:10:35         18 hello.txt
[root@ip-172-31-36-54 /]# echo "Hello Cloud Gurus 2" > hello2.txt
[root@ip-172-31-36-54 /]# aws s3 cp hello2.txt s3://acloudguru1234-rk
upload: ./hello2.txt to s3://acloudguru1234-rk/hello2.txt
[root@ip-172-31-36-54 /]# aws s3 ls s3://acloudguru1234-rk
2018-06-05 09:10:35         18 hello.txt
2018-06-05 10:50:08         20 hello2.txt
[root@ip-172-31-36-54 /]#
```

AWS Documentation » AWS Command Line Interface » User Guide » Configuring the AWS CLI » Configuration and Credential Files

Configuration and Credential Files

The CLI stores credentials specified with `aws configure` in a local file named `credentials` in a folder named `.aws` in your home directory. Home directory location varies but can be referred to using the environment variables `%UserProfile%` in Windows and `$HOME` or ~ (tilde) in Unix-like systems.

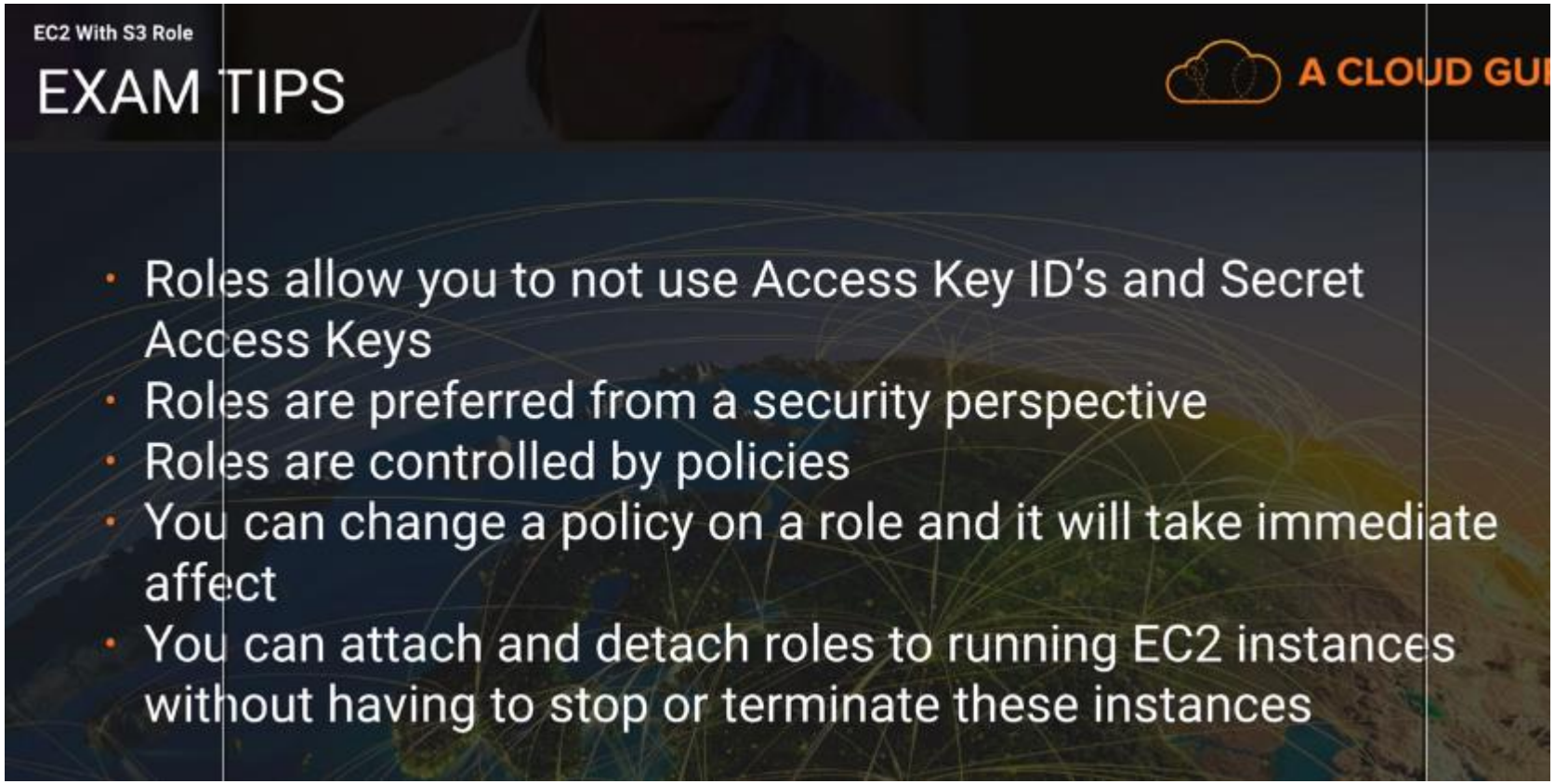
For example, the following commands list the contents of the `.aws` folder:

Linux, macOS, or Unix

```
$ ls ~/.aws
```

Windows

```
> dir "%UserProfile%\.aws"
```


EC2 With S3 Role
EXAM TIPS
A CLOUD GU
Roles allow you to not use Access Key ID's and Secret Access Keys
Roles are preferred from a security perspective
Roles are controlled by policies
You can change a policy on a role and it will take immediate affect
You can attach and detach roles to running EC2 instances without having to stop or terminate these instances