Operations Playbook

Name**: HIMA SREE CHALASANI**

Class: **IFT 422-562: Cloud Security & Operations for IT**

Contents

How to connect to the Mom & Pop Cafe Test EC2 instance

1. Ensure you have a copy of the necessary ppk/pem file for instance verification.
2. Open Putty and configure your connection with the specified settings.
3. In the Connection section, set the "Seconds between keepalives" to 30.
4. Input the public IPv4 address of your EC2 instance into the hostname area.
5. Add the ppk/pem file to your connection configuration.
6. Start the session by selecting "open" and log in using the "ec2-user" as the username to gain entry to the instance.

How to use the AWS CLI to connect to your AWS account

1. Initiate an SSH connection to your EC2 instance.
2. Adjust settings in Putty as follows:

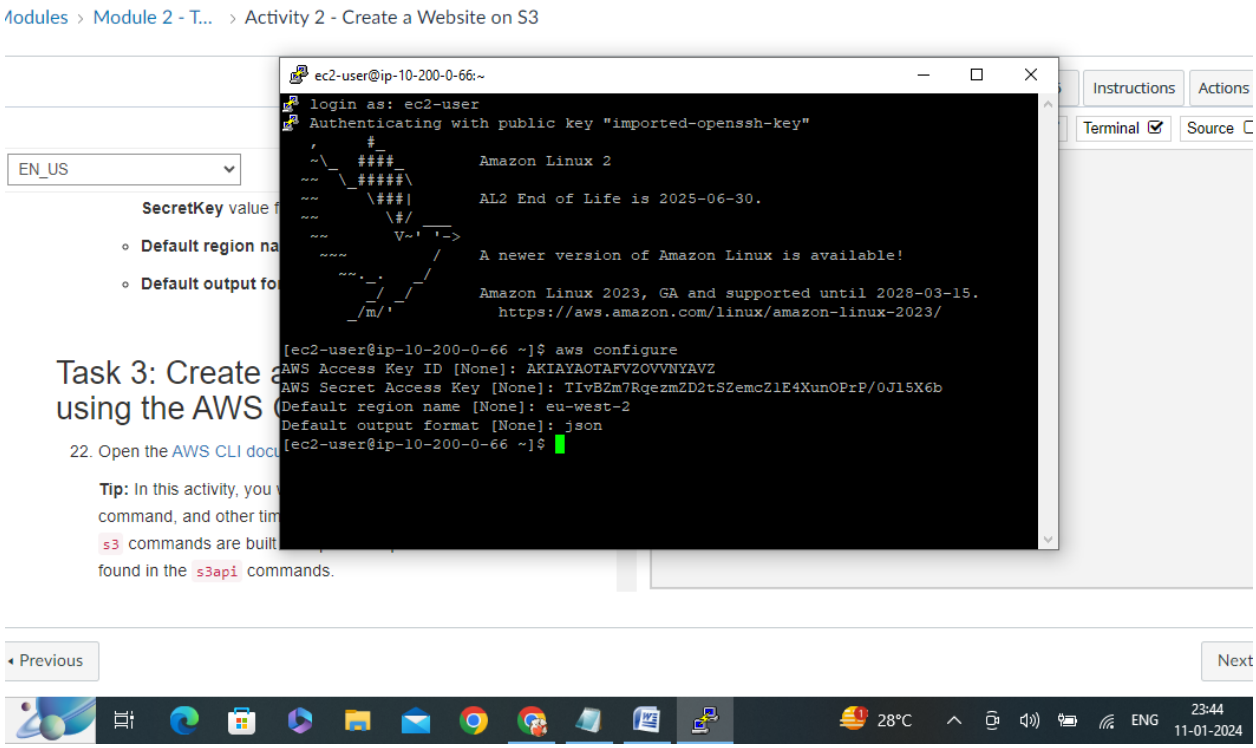
   - To prolong the Putty session time, go to the Connections section and adjust the "Seconds between keepalives" setting to 30.

   - Enter the IPv4 address of the Bastion Host in the Hostname/IPv4 input field.

   - Within the Connection tab, access the SSH section, and in the Authentication (Auth) area, you need to load the private key file.

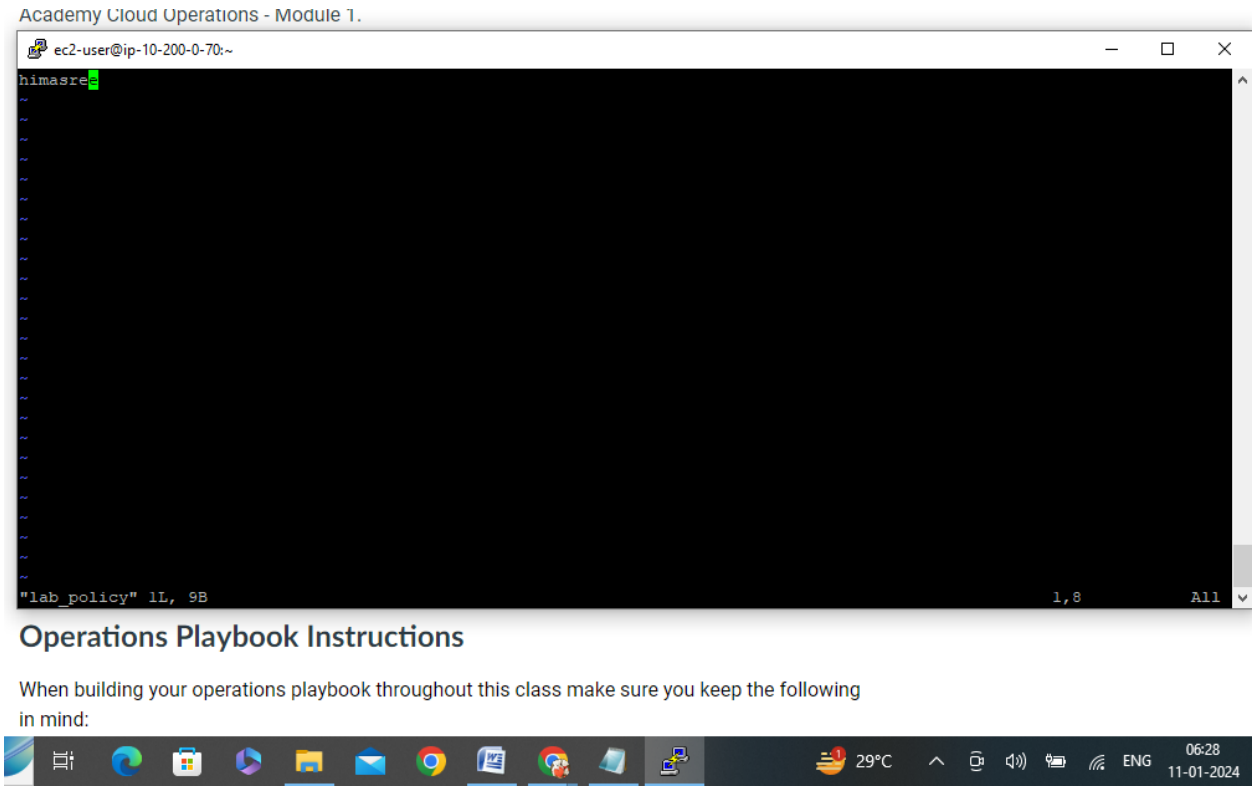
   - Use the "browse" option to upload the ppk file you have previously acquired.

   - After ensuring the checkbox has been marked, click "Open," then proceed with "Approve." Input "ec2-user" for the username to initiate a connection to the instance.



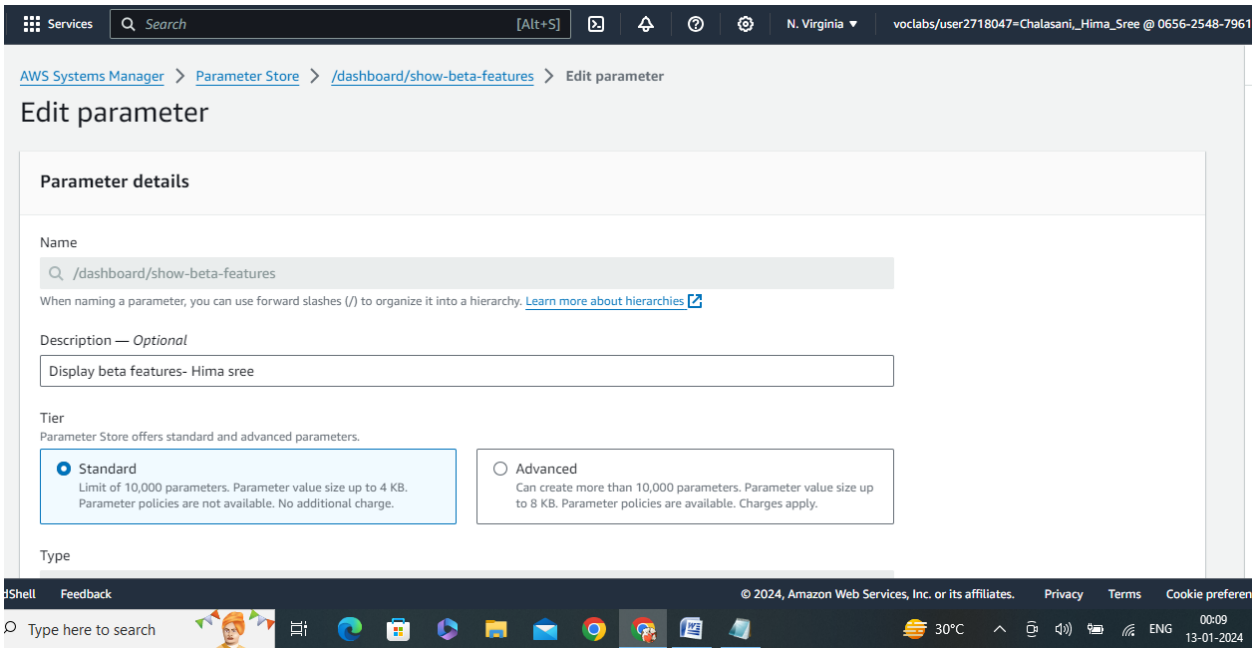
How to make a modification to the lab policy using the AWS CLI

1. After setting up the AWS CLI within our AWS account, we are required to modify the JSON policy document provided during the lab.
2. Executing the "AWS IAM list-users" command will generate a JSON output listing all users managed by IAM for this account, allowing us to review IAM configurations.
3. Upon receiving the list, we'll replicate the previous output and save it into a file named "lab_policy.json."
4. To inspect the contents of this file, the "cat" command is useful, and for editing purposes, the "vi" editor is recommended. After making all necessary edits, save your changes by executing the "wq" command within the vi editor.



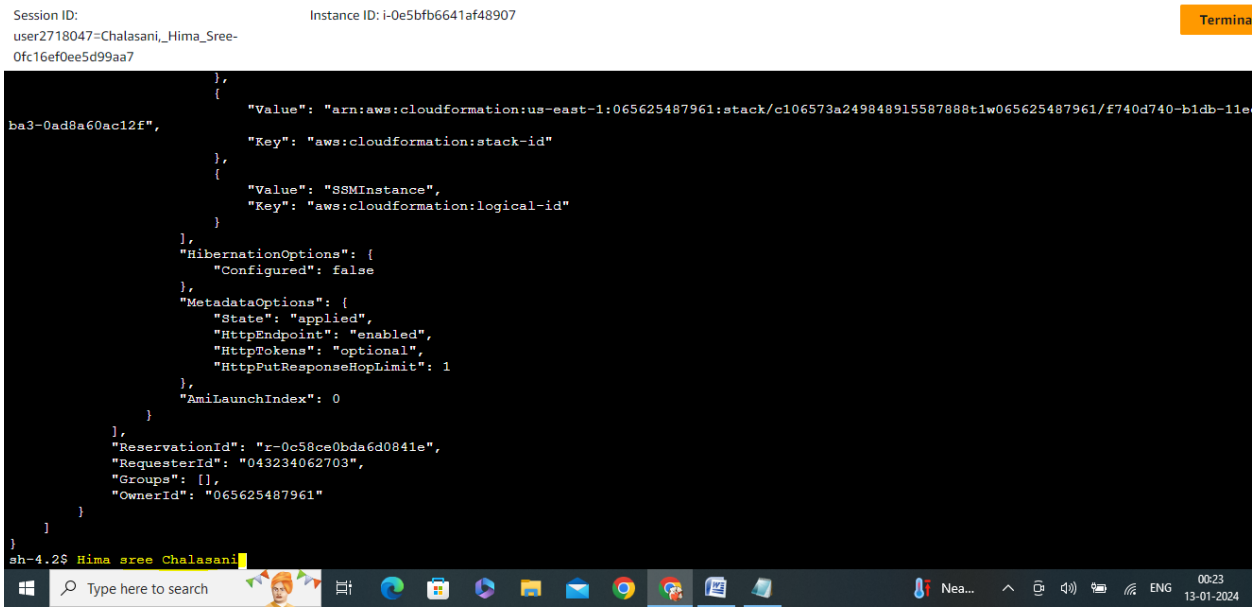
How to add a parameter to the parameter store for allowing cookies on the website

1. Navigate to the AWS Management Console and click on "Parameter Store" from the sidebar menu.
2. Upon selecting this feature, you will be asked to enter both a name and a description for the parameter.
3. The software operating on the linked EC2 instance will verify the parameter's presence before it processes any input in designated areas.
4. Should the application detect an additional argument, it will integrate that functionality and reflect the changes on the related web page.
5. The system will seamlessly integrate any new parameters found throughout this procedure into its operations.



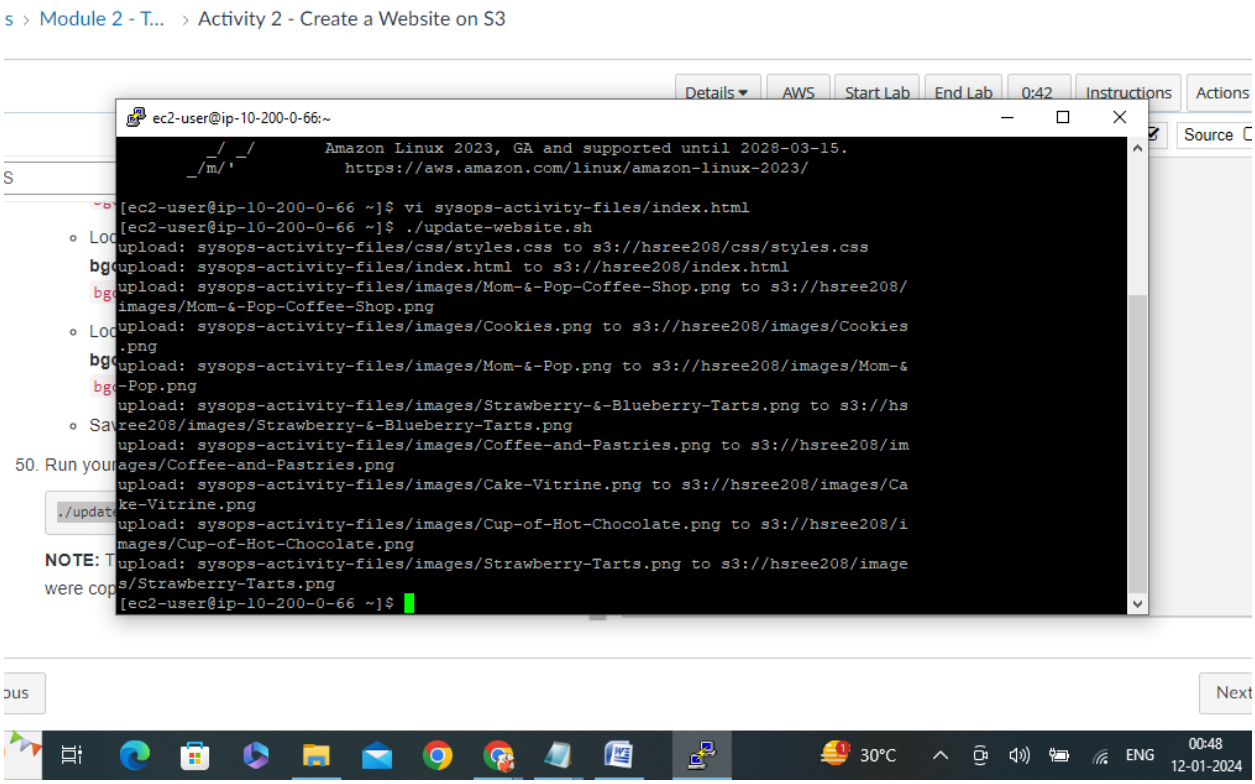
How to connect to an EC2 instance to describe instances

1. Log into the AWS Management Console and navigate to the Systems Manager section.
2. Choose "Session Manager" from the navigation pane on the left.
3. Initiate a session by clicking on "Start session."
4. Execute the command "ls /var/www/html" during the session to inspect the files located on the EC2 instance.
5. Utilize the command "aws ec2 describe-instances" to establish a connection with an EC2 instance.



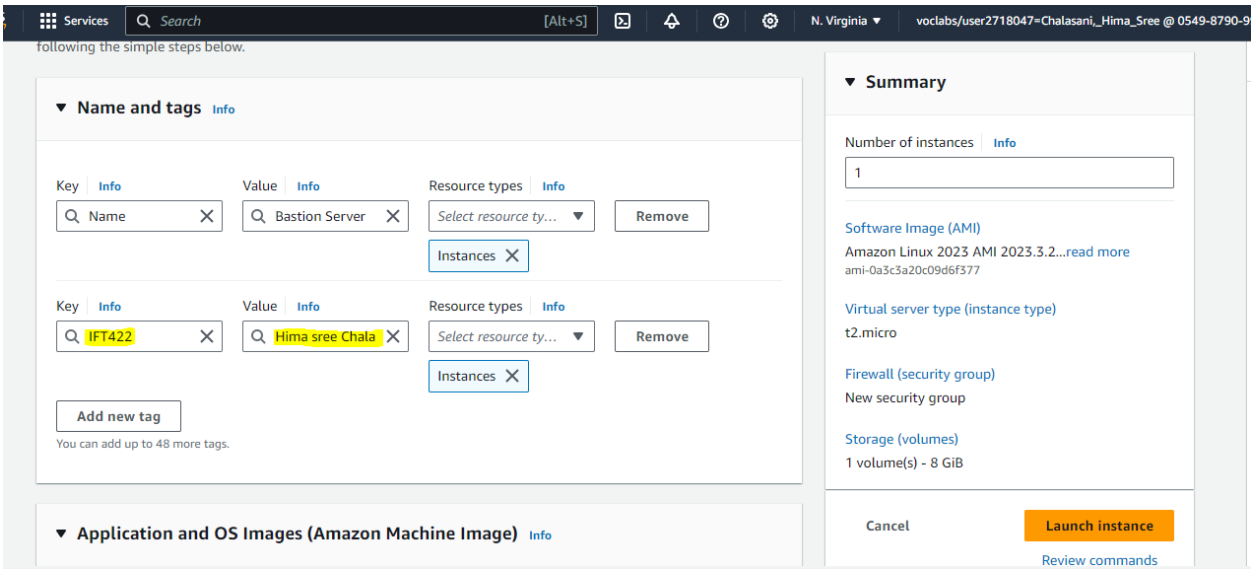
How to create a batch file to upload update the café website to change its colors

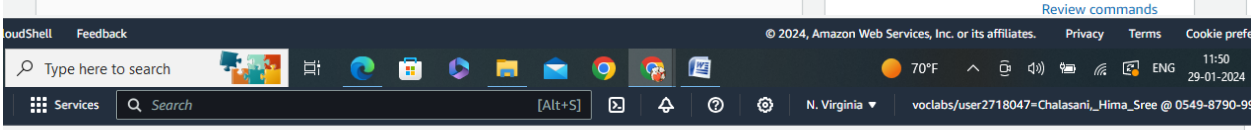
1. Generate a file called "update-website.sh" by employing the "touch" command and moving to the desired directory with "cd."
2. Open the "update-website.sh" file for editing by using the "vi" text editor.
3. Commit any changes you've made to the file by saving them.
4. Use a text editor to access the "vi sysops-activity-files/index.html" file.
5. Once the background color has been altered, save the modifications and proceed to upload the revised file.

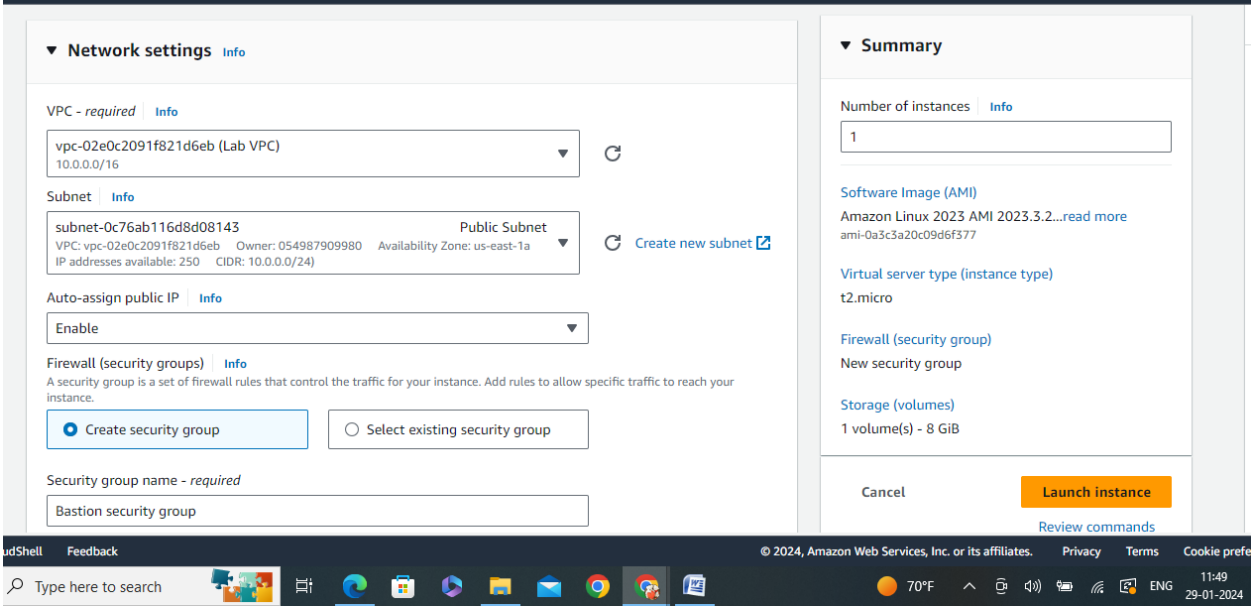


How to launch an EC2 instance

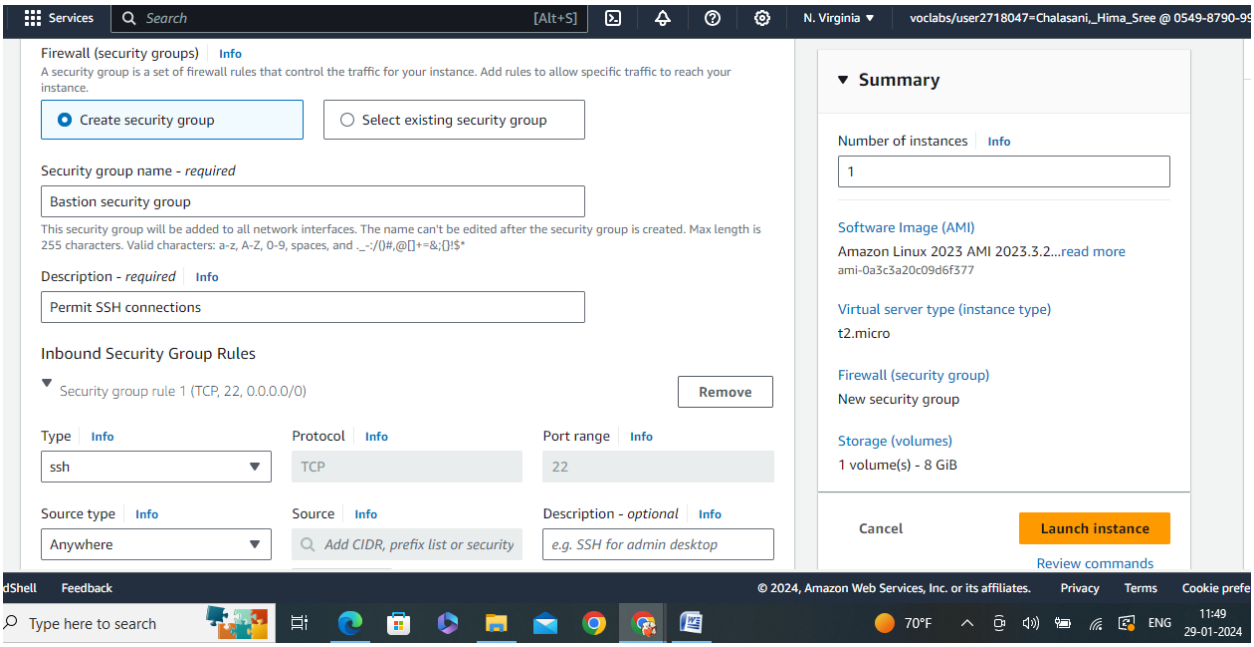
1. Begin by accessing the EC2 dashboard.
2. Identify and select the specific EC2 instance you intend to launch before starting the creation process.
3. Once an instance is chosen, click on "Launch Instance" to proceed.
4. In the subsequent window, assign a name or identifier to your new instance.
5. Following the naming, select the desired operating system (OS) and application image to serve as the foundation for your instance.
6. Next, choose a key pair for the instance, ensuring to pick the "vockey" key pair in this step.
7. After hitting the "Launch Instance" option, take a moment to review your network configurations carefully.


Services
Search
[Alt+S]
N. Virginia
voclabs/user2718047=Chalasani,_Hima_Sree @ 0549-8790-9
following the simple steps below.
Name and tags Info
Key Info
Value Info
Resource types Info
Name
Bastion Server
Select resource ty...
Remove
Instances
Key Info
Value Info
Resource types Info
IFT422
Hima sree Chala
Select resource ty...
Remove
Instances
Add new tag
You can add up to 48 more tags.
Application and OS Images (Amazon Machine Image) Info
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0a3c3a20c09d6f377
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands


CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie prefe
Type here to search
70°F
ENG
11:50
29-01-2024
Services
Search
[Alt+S]
N. Virginia
voclabs/user2718047=Chalasani,_Hima_Sree @ 0549-8790-99

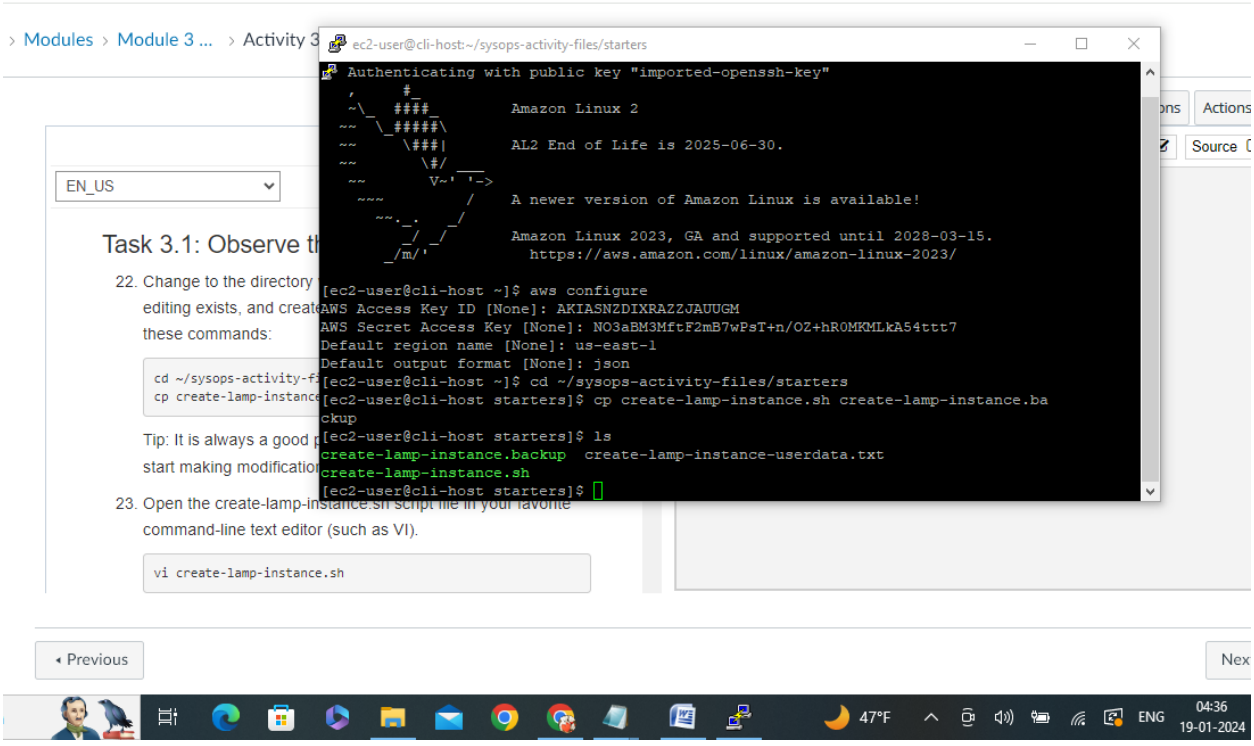

Network settings Info
VPC - required Info
vpc-02e0c2091f821d6eb (Lab VPC)
10.0.0.0/16
Subnet Info
subnet-0c76ab116d8d08143
Public Subnet
VPC: vpc-02e0c2091f821d6eb Owner: 054987909980 Availability Zone: us-east-1a
IP addresses available: 250 CIDR: 10.0.0.0/24)
Create new subnet
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
Bastion security group
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0a3c3a20c09d6f377
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands

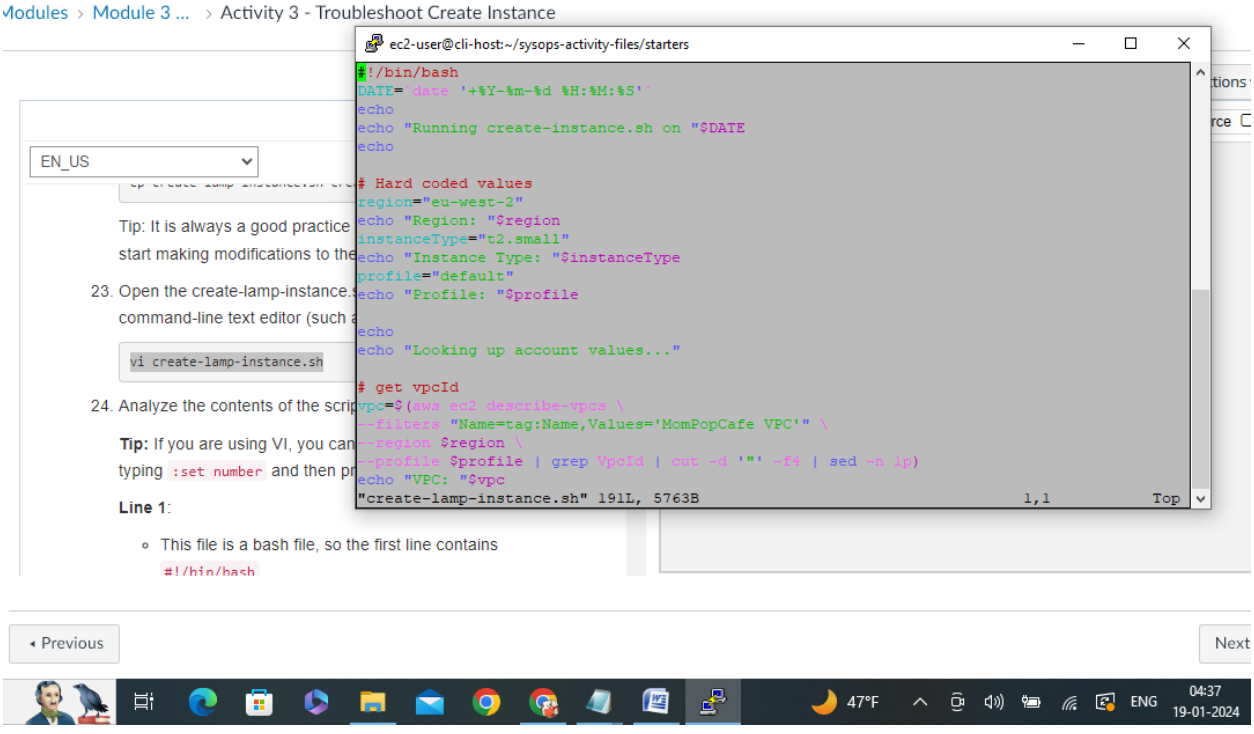
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie prefe
Type here to search
70°F
ENG
11:49
29-01-2024



How to change the AMI instance on the create-lamp-instance.sh script

1. The process begins by initiating an SSH connection to an EC2 instance, which is the first step towards modifying the AMI instance.
2. Next, adjust the AWS setup to meet the particular demands of the operation.
3. Then, it's essential to create a backup and work with the "create-lamp-instance.sh" script, which contains important information such as VPC, SubnetID, Security Group, and InstanceID.
4. In case you encounter the "InvalidAMIID.noround" error, it's recommended to execute the script again. Use the error notification to pinpoint the exact location of the error's origin.
5. Note that the script includes a default AMI ID, which must be replaced with the specific AMI ID you plan to use, to ensure the deployment of the correct AMI instance.
6. Once you have completed the required changes and validated the exact AMI ID, rerun the command to ensure that the AMI ID has been correctly modified as planned.





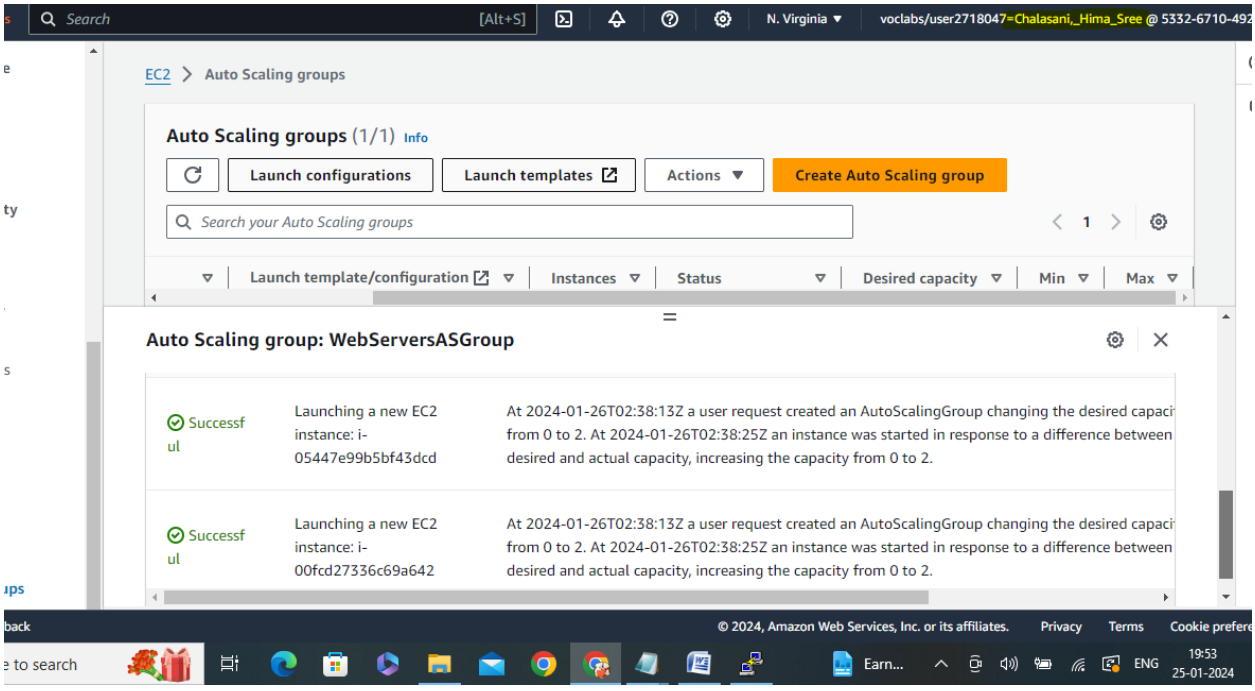
How to tail a log in Linux

1. Examine the contents of the log file.

2. Use the command "tail -f" to display the most recent 10 entries while also receiving updates in real-time.
3. To adjust the number of lines displayed, employ the '-n' option.
4. To stop monitoring and save any modifications, press CTRL+C; to exit, enter ":q."

How to create an Auto Scaling Group in the AWS UI

1. Sign into your AWS account and navigate to the Services menu to select EC2 on the sidebar.
2. Opt for "Create an Auto Scaling Group" among the listed services.
3. Select a launch template and adjust settings like VPC and Subnet configurations.
4. Link to the load balancer and determine the group's size parameters:
   - Desired capacity: 6
   - Minimum capacity: 4
   - Maximum capacity: 10
5. Implement a scaling policy and append relevant tags.
6. Following these instructions will effectively establish your Auto Scaling Group.



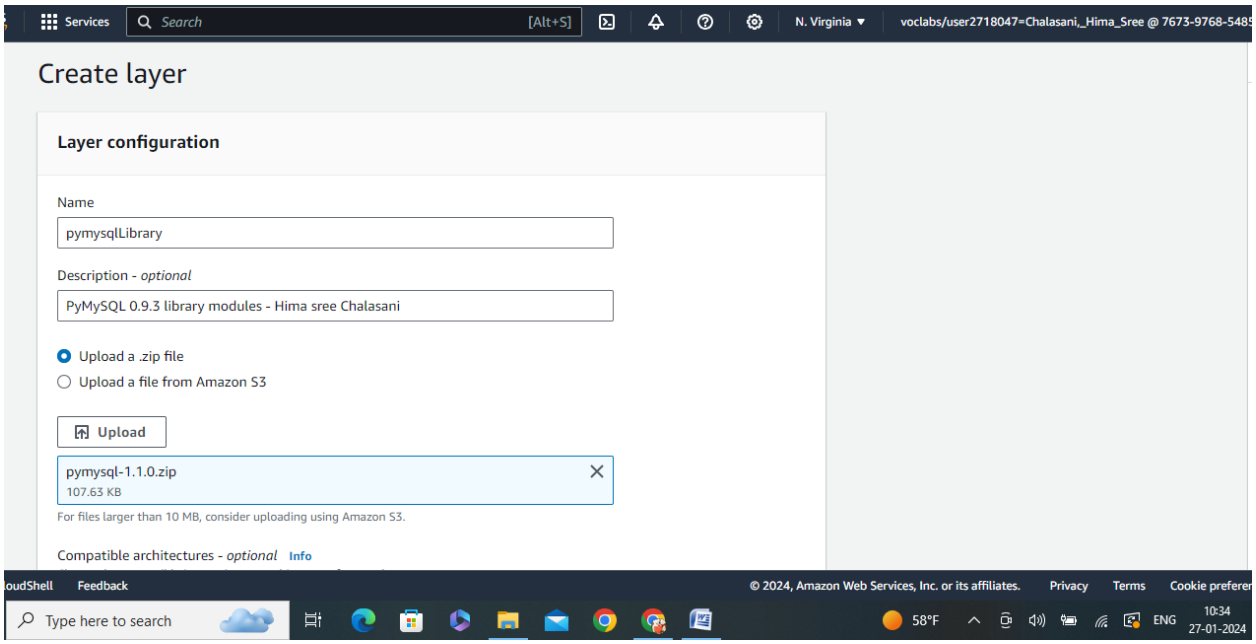
How to create a Route 53 health check

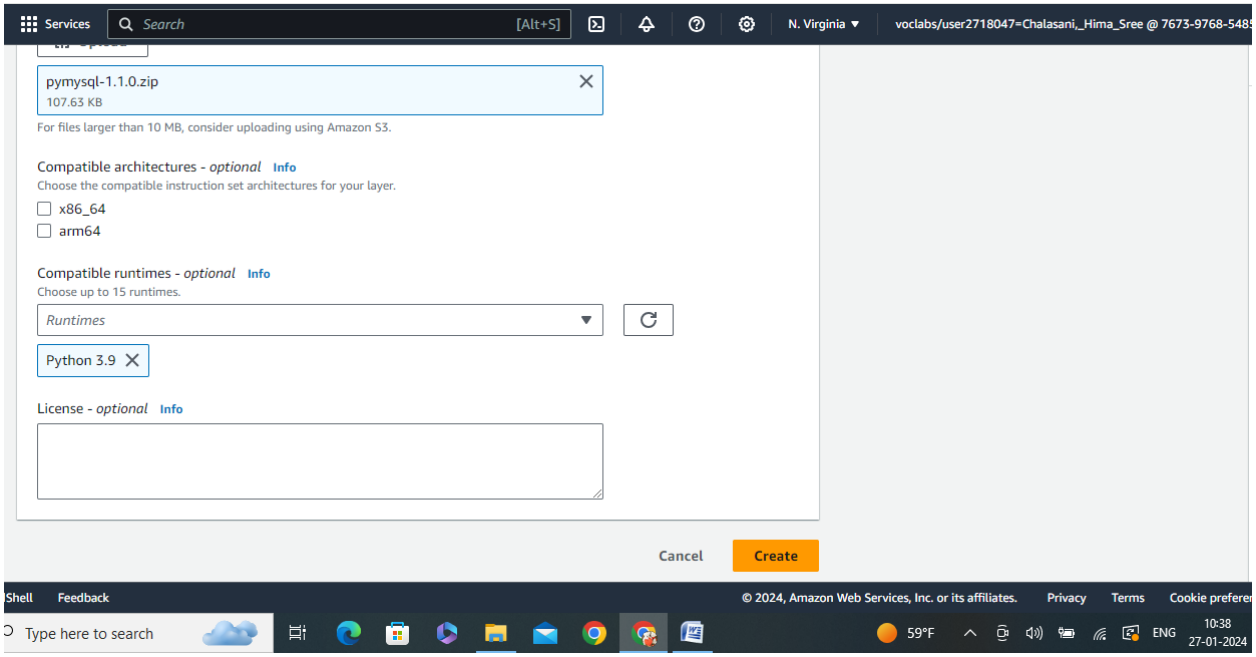
1. Start by logging into the AWS Management Console and proceed to Route 53. Within the dashboard of Route 53, on the navigation pane to the left, choose "Health Check" before selecting the "Create Health Check" option.
2. Begin the creation process by selecting "Create Health Check" found within the options for Health Checks.
3. Assign a distinctive and informative name to the Health Check.
4. In the "What to Monitor" section, select "Endpoint."

5. Identify and enter the IP address you wish to monitor, which is available in the instance details section, specifically copying the IPv4 Public IP Address from "MomPopCafeInstance1."
6. Adjust the "Requested Interval" to "Fast" and set the "Failure Threshold" to 2 within the advanced settings area.
7. Decide to generate an alarm by choosing "Create Alarm: Yes."
8. Upon request, designate a name for your newly created Simple Notification Service (SNS) topic as desired.
9. Fill in the email address to which notifications will be dispatched once this health check is accomplished.

How to create a Lambda Layer and add it to a Lambda function

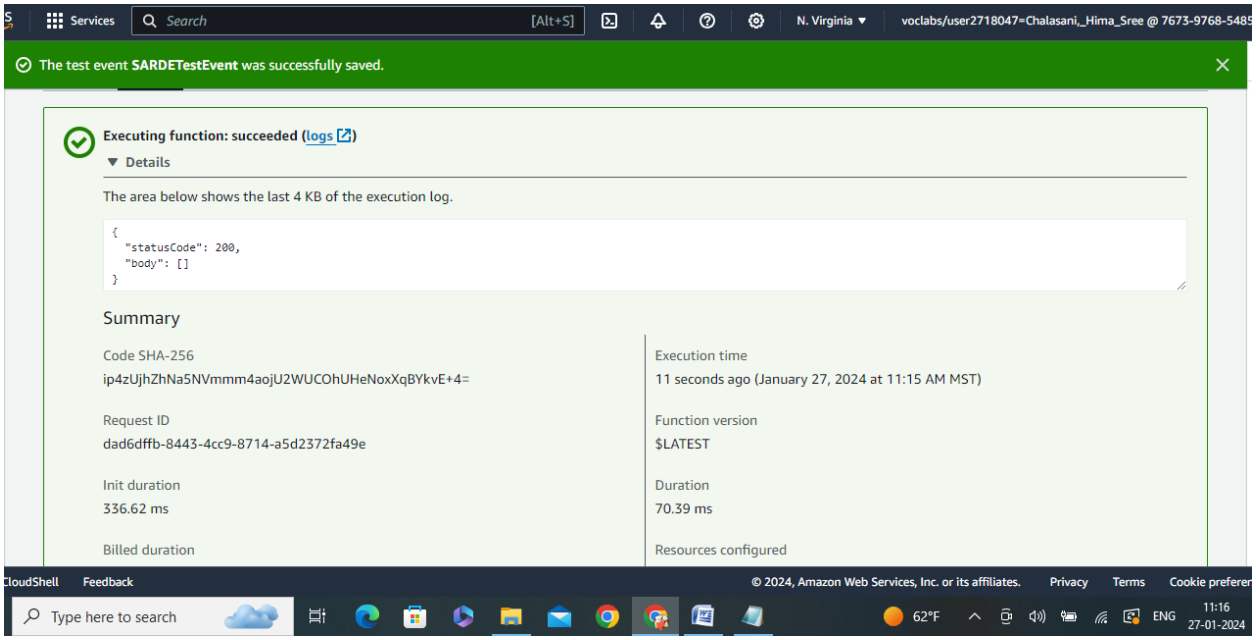
1. Navigate to the AWS Management Console and select Lambda from the options.
2. For introducing a new layer, access "Layers" and press "Create Layer." During this step, provide a name, detailed description, and select the method for code input.
3. From the creation options, hit "Run" to verify the command executes properly.
4. Initiate the creation of a new function by opting for "Author from Scratch."
5. Proceed to create the function by clicking "Create Function." During this process, fill in details such as the function's name, its runtime environment, and the roles it will execute under.
6. Go to "Add Layers" and choose "Custom Layers" for inclusion.
7. Observe as the interface updates. Following the function's setup, confirm the layer's addition was successful.





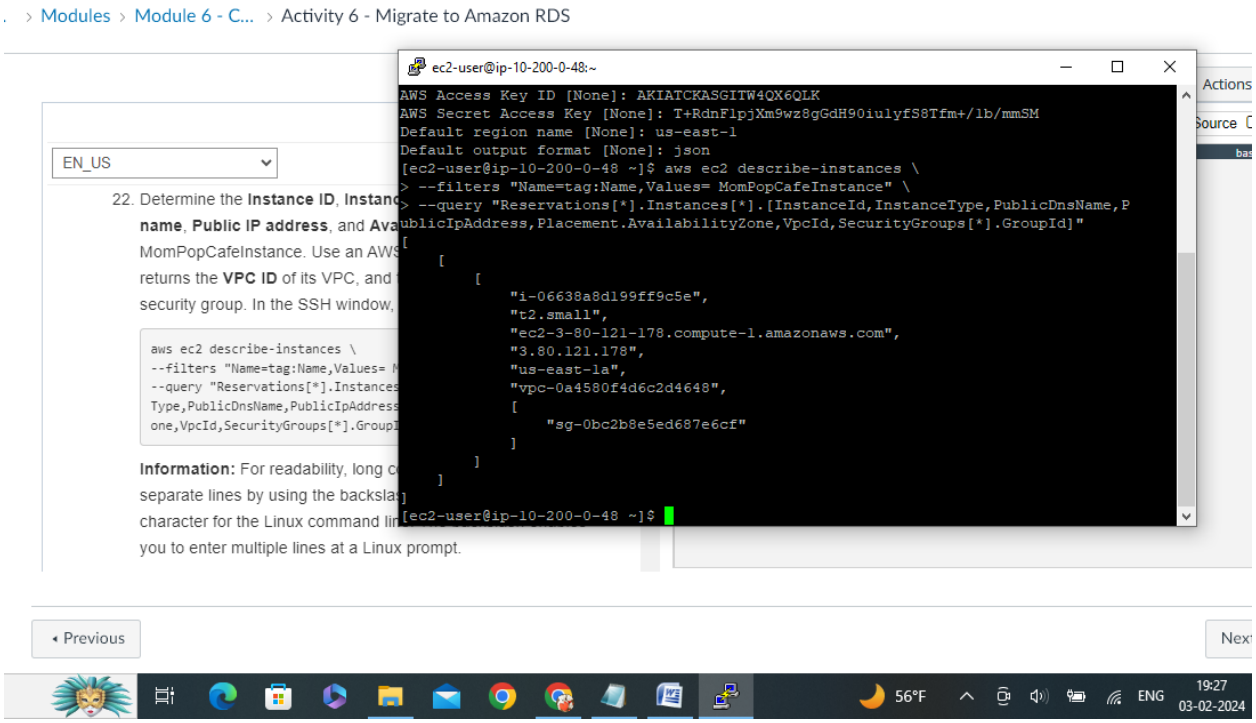
How to create a Lambda function from a prebuilt package

1. Launch the AWS Management Console and proceed to the Lambda section.
2. Initiate a fresh function, selecting "Author from Scratch" as the method. Name this function "SalesAnalysisReportDataExtractor," choose Python 3.7 as the runtime, and designate the correct execution role.
3. Incorporate the necessary library along with a custom layer.
4. Proceed to upload a zip file, conduct a validation of the data, and modify the handler entry to "salesAnalysisDataExtractor.lambda_handler."



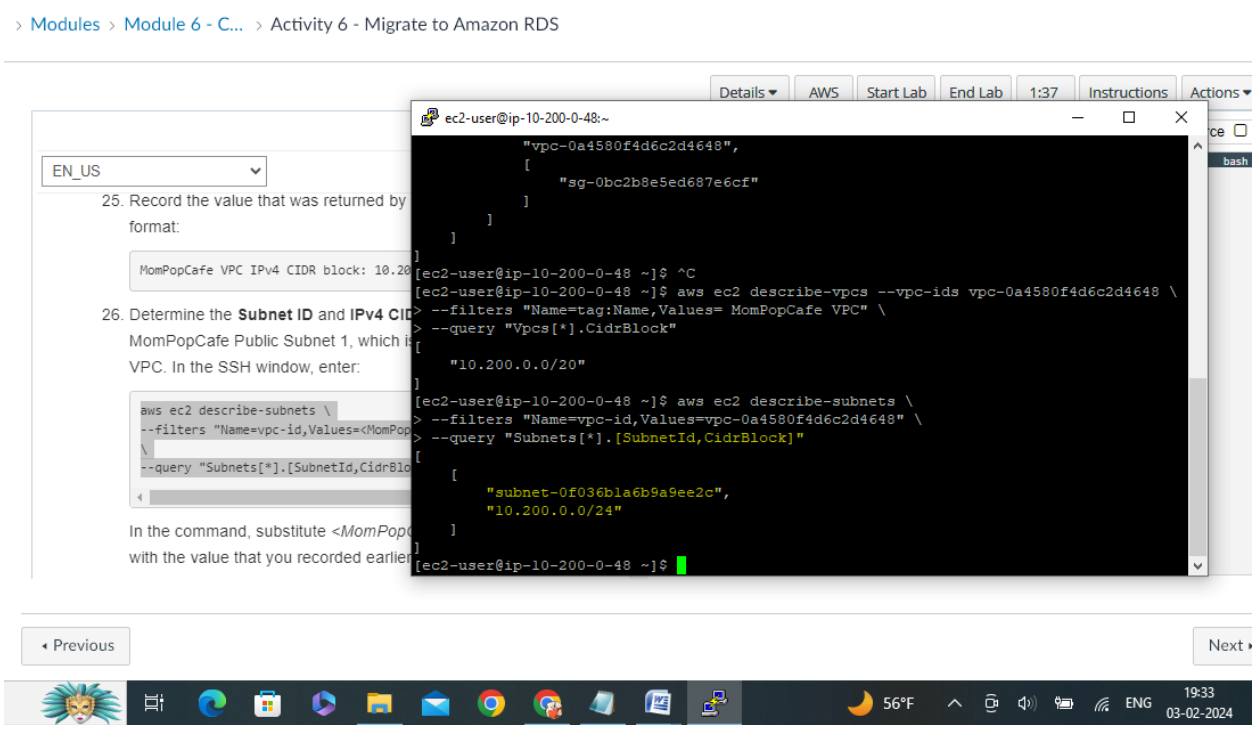
How to create a Lambda function from a prebuilt package

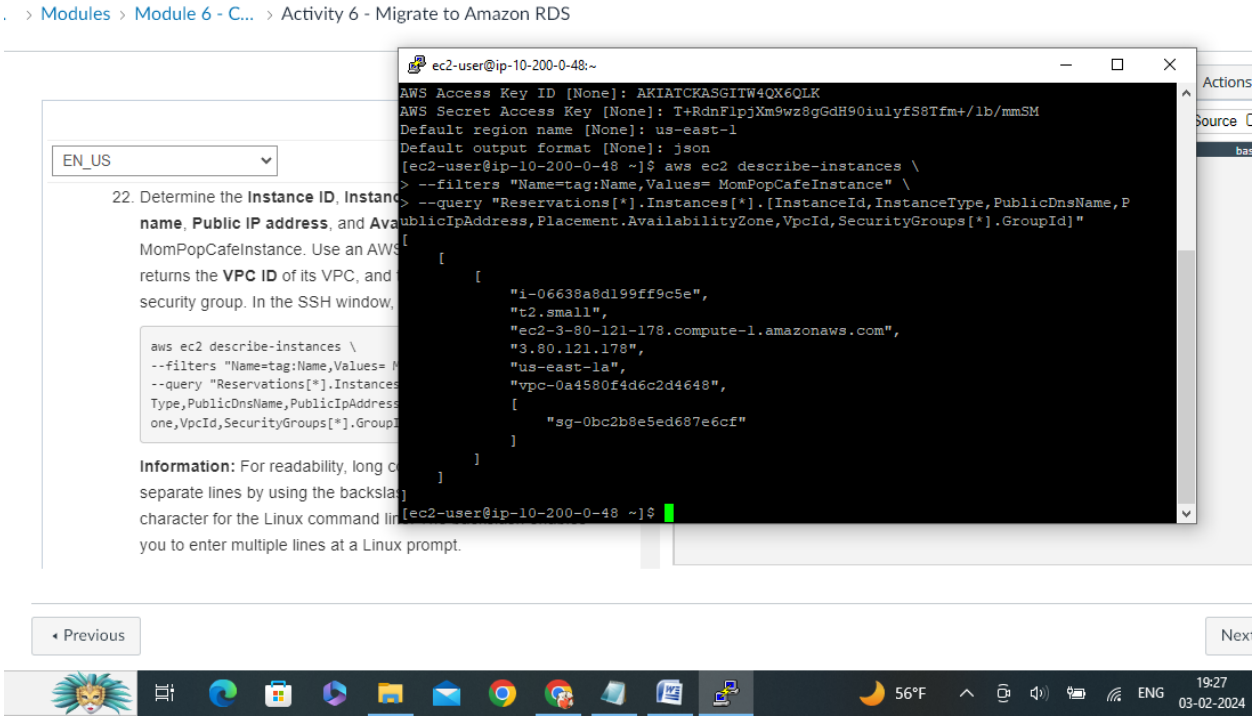
1. Install and configure the AWS CLI on your machine.
2. Use the following command to create a Database (DB) subnet group: `aws rds create-db-subnet-group`.
3. Create a DB parameter group by executing: `aws rds create-db-parameter-group`.
4. Start the RDS instance setup process with the command: `aws rds create-db-instance`.
5. Check the progress of the RDS instance with: `aws rds describe-db-instances`.



How to collect information about an instance

1. Step 1: Acquire the Instance ID
   Execute the command "aws ec2 describe-instances" and isolate the InstanceId by applying a specific query.
2. Step 2: Fetch Details of the Instance
   Utilize "aws ec2 describe-instances" alongside the instance-ids option to gather data. Isolate important details such as InstanceType, PublicDnsName, among others, via a query.
3. Step 3: Gather Data on Regional Availability Zones
   Invoke "aws ec2 describe-availability-zones" to get details.
   From AvailabilityZones[*], deduce the ZoneName.

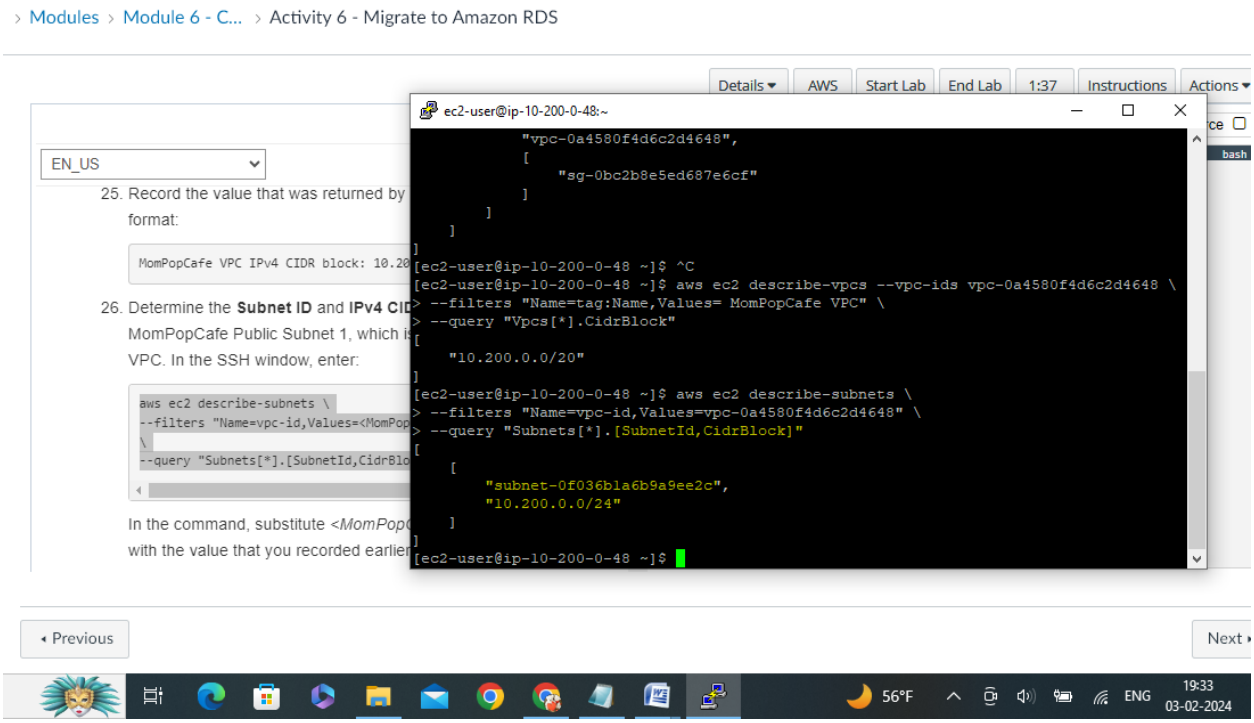


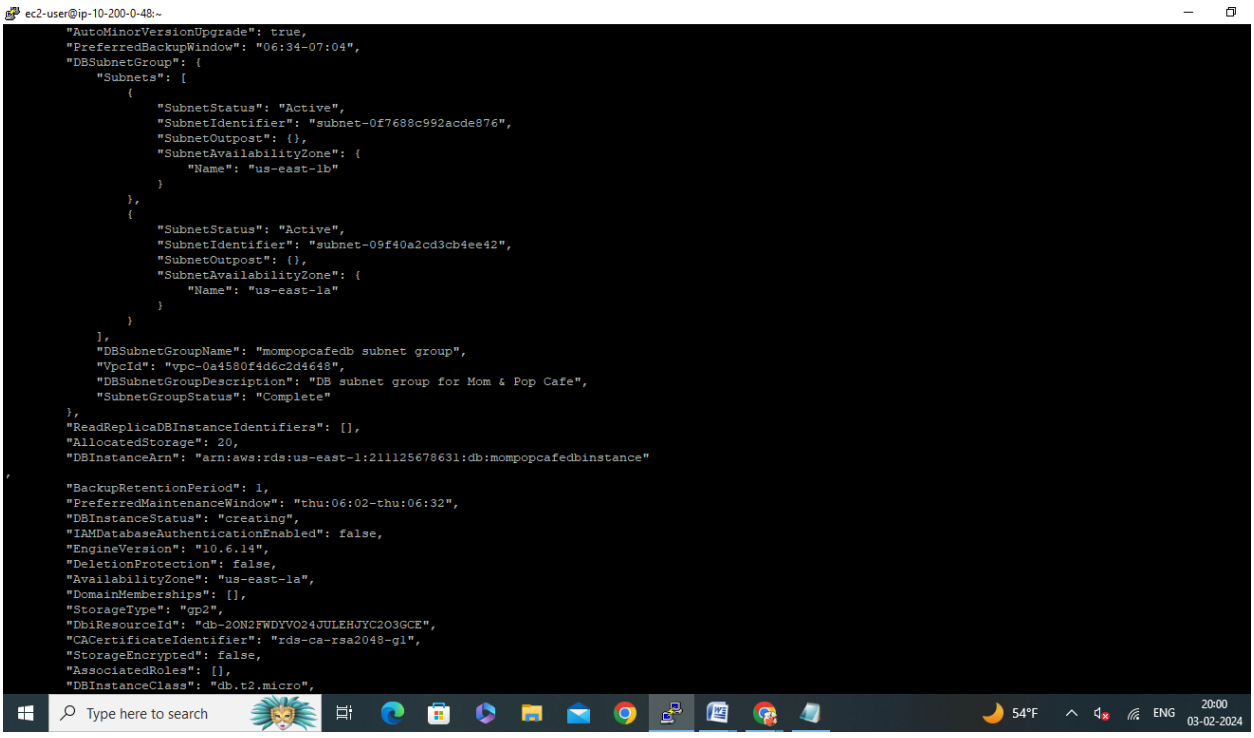


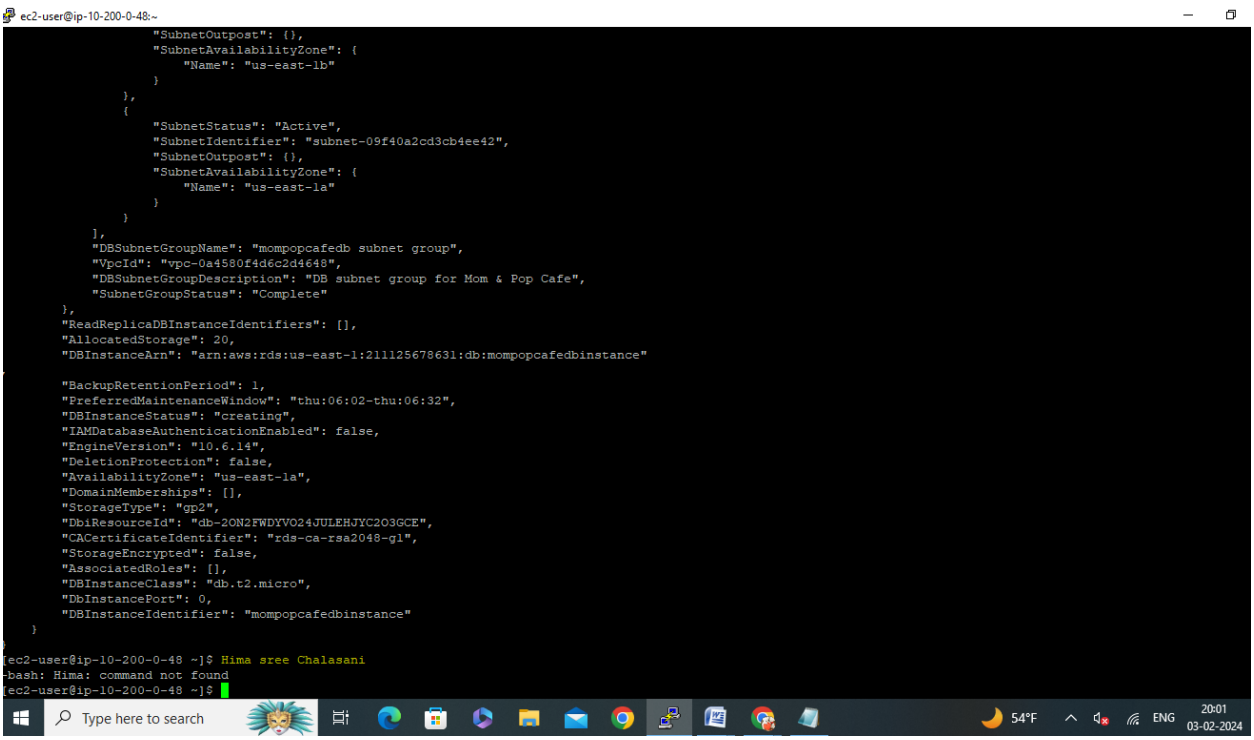
How to create two subnets in a subnet group via the AWS CLI

1. Begin with the creation of the first subnet by executing the `create-subnet` command in AWS EC2. Specify the VPC ID, CIDR block, and the availability zone designated for this subnet.

2. Create another subnet by utilizing the `create-subnet` command within AWS EC2. This time, ensure you input the VPC ID, a different CIDR block, and choose an alternative availability zone from the first subnet.
3. Form a subnet group using the `create-db-subnet-group` command in AWS RDS, incorporating the subnet IDs from the first and second steps into this setup.







How to use the mysqldump tool to take a backup of a SQL database and restore it on another SQL instance

1. Install mysqldump on the primary database server.
2. Use mysqldump to generate a backup of the database with the command: `mysqldump -u <user> -p<password> <database> > backup.sql`.
3. Transfer the backup file to the target server.
4. Create a fresh database on the destination server using the command: `mysql> create database <database name>`.
5. Restore the backup onto the new database using mysql with the command: `mysql -u <user> -p<password> <database name> < backup.sql`.

```
[ec2-user@ip-10-200-0-143 ~]$ mysql --user=root --password='Re:Start!9' \
> --host=mompopcafedbinstance.cpmcmgyw0eqz.us-east-1.rds.amazonaws.com \
> mom_pop_db
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 49
Server version: 10.6.14-MariaDB-log managed by https://aws.amazon.com/rds/

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [mom_pop_db]> select * from product;
+----+--------------------------+-----------------------------------------------------------------+-------+---------------+-----------------------------------------+
| id | product_name             | description                                                     | price | product_group | image_url                               |
+----+--------------------------+-----------------------------------------------------------------+-------+---------------+-----------------------------------------+
|  1 | Croissant                | Fresh, buttery and fluffy... Simply delicious!                  |  1.50 |             1 | images/Croissants.jpg                   |
|  2 | Donut                    | We have more than half-a-dozen flavors!                         |  1.00 |             1 | images/Donuts.jpg                       |
|  3 | Chocolate Chip Cookie    | Made with Swiss chocolate with a touch of Madagascar vanilla    |  2.50 |             1 | images/Chocolate-Chip-Cookies.jpg       |
|  4 | Muffin                   | Banana bread, blueberry, cranberry or apple                     |  3.00 |             1 | images/Muffins.jpg                      |
|  5 | Strawberry Blueberry Tart | Bursting with the taste and aroma of fresh fruit                |  3.50 |             1 | images/Strawberry-&-Blueberry-Tarts.jpg |
|  6 | Strawberry Tart          | Made with fresh ripe strawberries and a delicious whipped cream |  3.50 |             1 | images/Strawberry-Tarts.jpg             |
|  7 | Coffee                   | Freshly-ground black or blended Columbian coffee                |  3.00 |             2 | images/Coffee.jpg                       |
|  8 | Hot Chocolate            | Rich and creamy, and made with real chocolate                   |  3.00 |             2 | images/Cup-of-Hot-Chocolate.jpg         |
|  9 | Latte                    | Offered hot or cold and in various delicious flavors            |  3.50 |             2 | images/Latte.jpg                        |
+----+--------------------------+-----------------------------------------------------------------+-------+---------------+-----------------------------------------+
9 rows in set (0.00 sec)

MariaDB [mom_pop_db]> Hima sree Chalasani
```

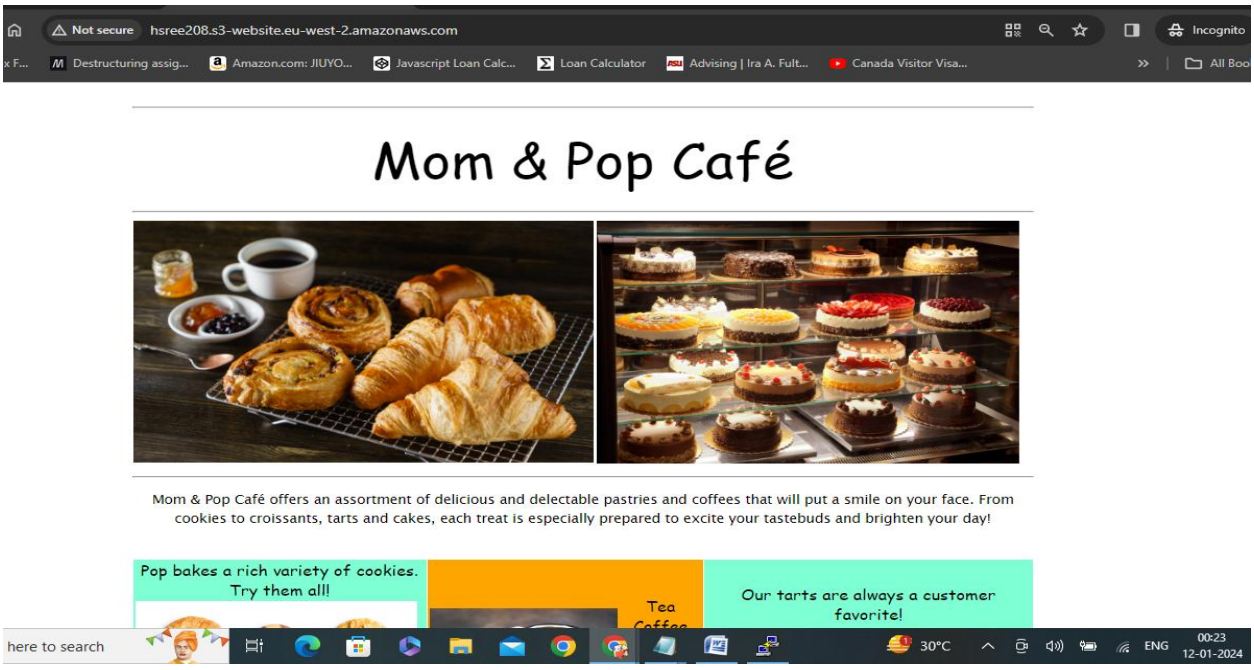

How to enable VPC Flow Logs via the command line interface

1. Generate an IAM role for VPC Flow Logs: 'aws iam create-role --role-name VPCFlowLogsRole'.
2. Establish a CloudWatch log group: 'aws logs create-log-group --log-group-name VPCFlowLogs'.
3. Activate flow logs on the VPC using 'aws ec2 create-flow-logs', indicating the log destination.

```
ec2-user@cli-host:~
[ec2-user@cli-host ~]$ aws s3api create-bucket --bucket flowlog5555 --region us-east-1
{
    "Location": "/flowlog5555"
}
[ec2-user@cli-host ~]$ aws ec2 describe-vpcs --query 'Vpcs[*].[VpcId,Tags[?Key==`Name`].Value,CidrBlock
]' --filters "Name=tag:Name,Values='VPC1'"
[
    [
        "vpc-0fd9d12917af77872",
        [
            "VPC1"
        ],
        "10.0.0.0/16"
    ]
]
[ec2-user@cli-host ~]$ aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-0fd9d12917af7787
2 --traffic-type ALL --log-destination-type s3 --log-destination arn:aws:s3:::flowlog5555
{
    "Unsuccessful": [],
    "FlowLogIds": [
        "fl-00af88eb8f0a99990"
    ],
    "ClientToken": "SouhAv29sbTz9y7mc4dqr8klXCG/6E7EdJuKJ6Ql5Eg="
}
[ec2-user@cli-host ~]$ aws ec2 describe-flow-logs
{
    "FlowLogs": [
        {
            "LogDestinationType": "s3",
            "Tags": [],
            "ResourceId": "vpc-0fd9d12917af77872",
            "CreationTime": "2024-02-09T20:07:31.917Z",
            "TrafficType": "ALL",
            "FlowLogStatus": "ACTIVE",
            "LogFormat": "${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${d
stport} ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status}",
            "FlowLogId": "fl-00af88eb8f0a99990",
            "MaxAggregationInterval": 600,
            "LogDestination": "arn:aws:s3:::flowlog5555",
            "DeliverLogsStatus": "SUCCESS"
        }
    ]
}
[ec2-user@cli-host ~]$ Hima sree Chalasani
```

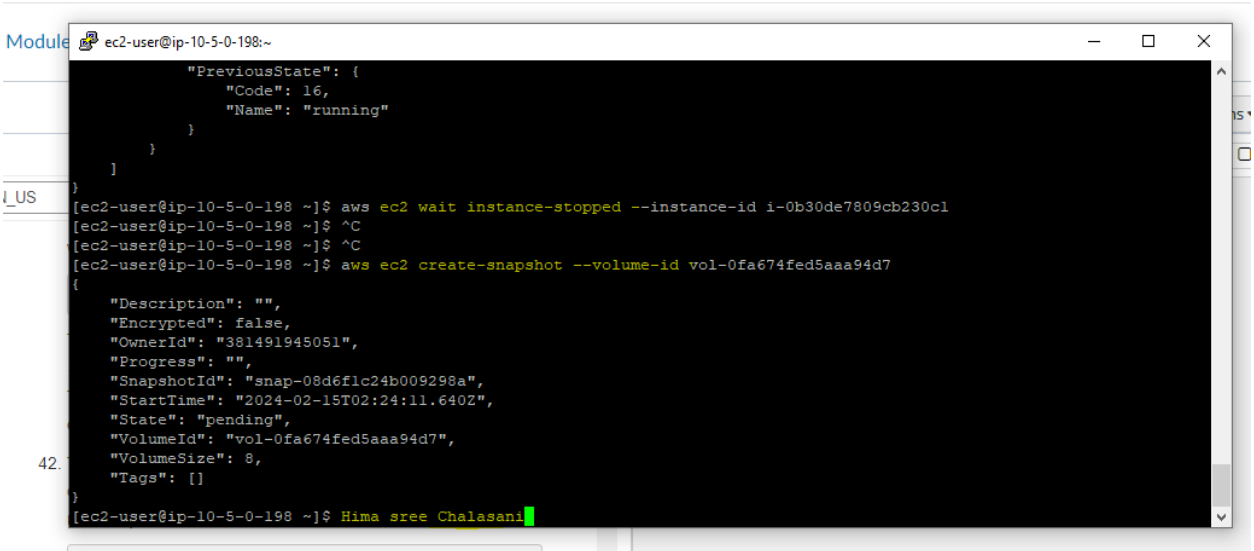
How to troubleshoot network connectivity on an instance

1. Ensure that the instance's associated security groups permit both incoming and outgoing traffic on the necessary ports.
2. Validate that Network ACLs linked with the subnet allow essential traffic.
3. Verify the accuracy of the route table configurations, directing traffic to the appropriate destination.
4. Check the instance's operational status and ensure it is running correctly.
5. Confirm that the instance possesses a valid public IP address or Elastic IP if external communication is required.
6. Review system and application logs on the instance for any network connectivity-related error messages.
7. Conduct ping tests from both the instance and external systems to assess reachability.
8. Execute a traceroute to identify the network path and potential bottlenecks.
9. Check for the presence of security software (such as firewalls or antivirus) on the instance that may obstruct traffic.
10. If the instance communicates with resources in another VPC, validate VPC peering configurations.
11. Inspect instance metadata to ensure the accuracy of network settings.
12. Confirm that DNS resolution is functioning correctly.
13. Temporarily adjust security group rules to permit all traffic for testing purposes.
14. Ensure that subnet routing is appropriately configured and functional.



How to take a snapshot of an EBS volume

1. Tailor the settings in Putty to suit your preferences.
2. Set a 30-second interval for keepalives to bolster connection reliability.
3. Enter the public IPv4 address of the EC2 instance into the hostname field.
4. Connect securely by configuring Putty to use the designated PPK/PEM file for authentication.
5. Open the connection by clicking "Open" and inputting "ec2-user" as the username when prompted to gain access.
6. Retrieve the volume ID linked with the specified snapshot using the provided AWS CLI command: aws ec2 describe-instances --filter 'Name=tag:Name,Values=Processor' –query 'Reservations[0].Instances[0].BlockDeviceMappings[0].Ebs.{VolumeId:VolumeId}'
7. Obtain the instance ID necessary for terminating the instance with the following AWS CLI command: aws ec2 describe-instances --filters 'Name=tag:Name,Values=Processor' -query 'Reservations[0].Instances[0].InstanceId'
8. Halt the ongoing process by executing the provided AWS CLI command: aws ec2 stop-instances --instance-ids INSTANCE-ID
9. Create a snapshot of the specified EBS volume using the provided AWS CLI command: aws ec2 create-snapshot --volume-id VOLUME-ID

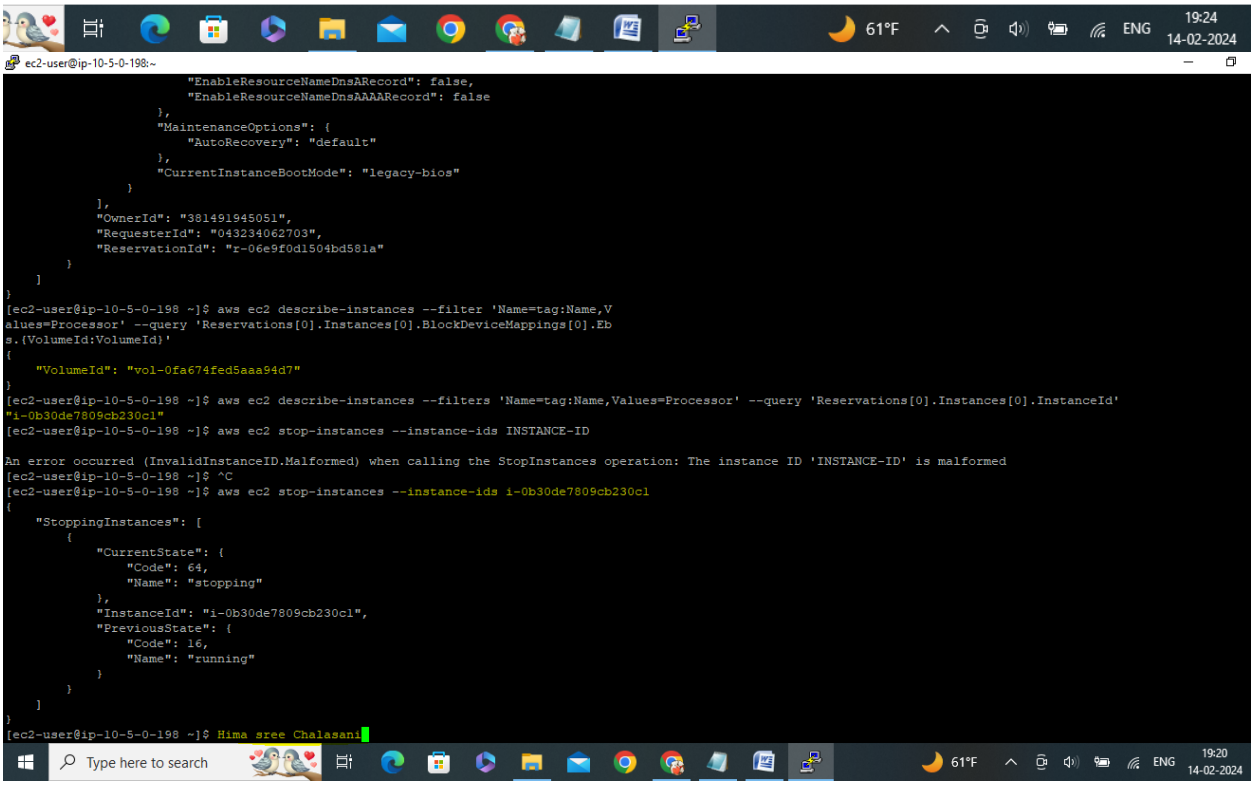


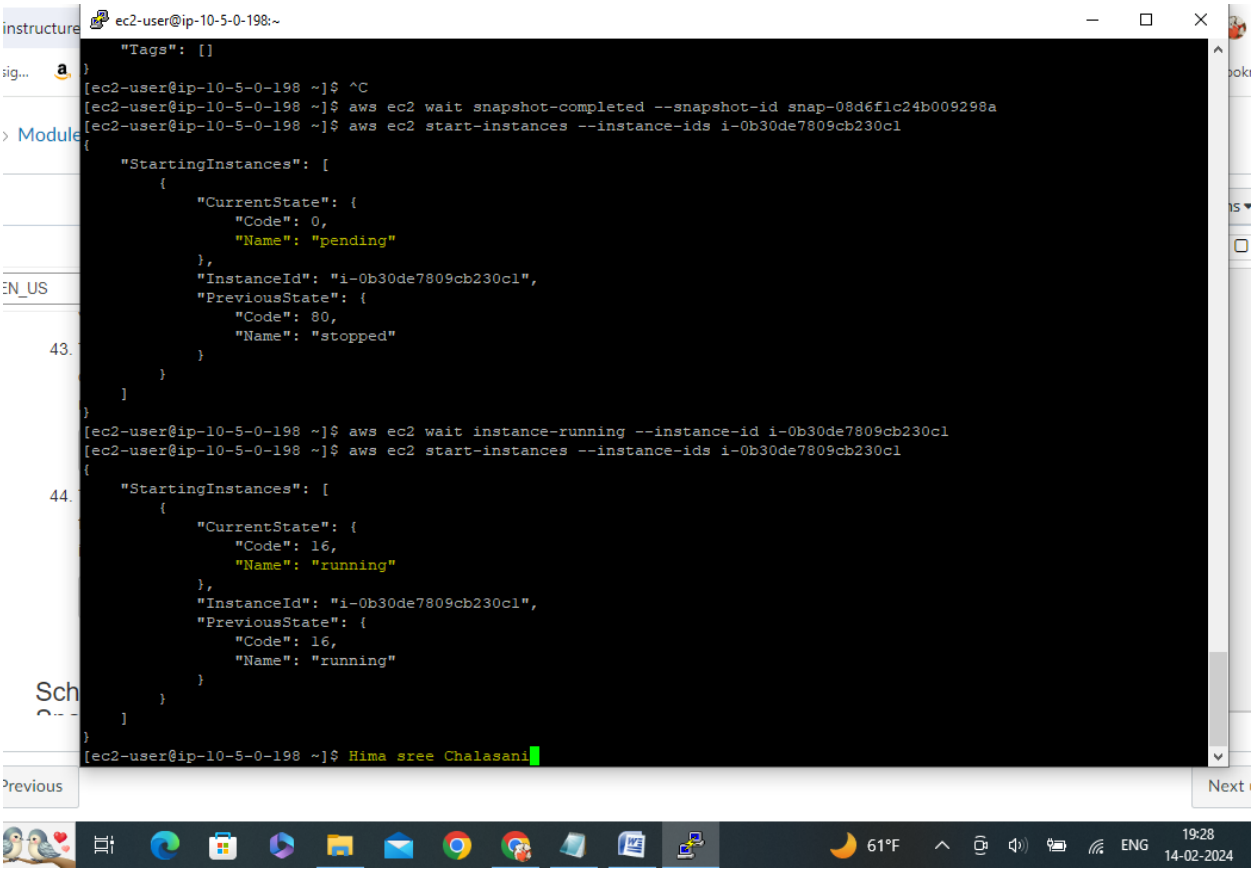
aws ec2 wait snapshot-completed --snapshot-id SNAPSHOT-ID

Continue with the below procedure when the command

evious

Next

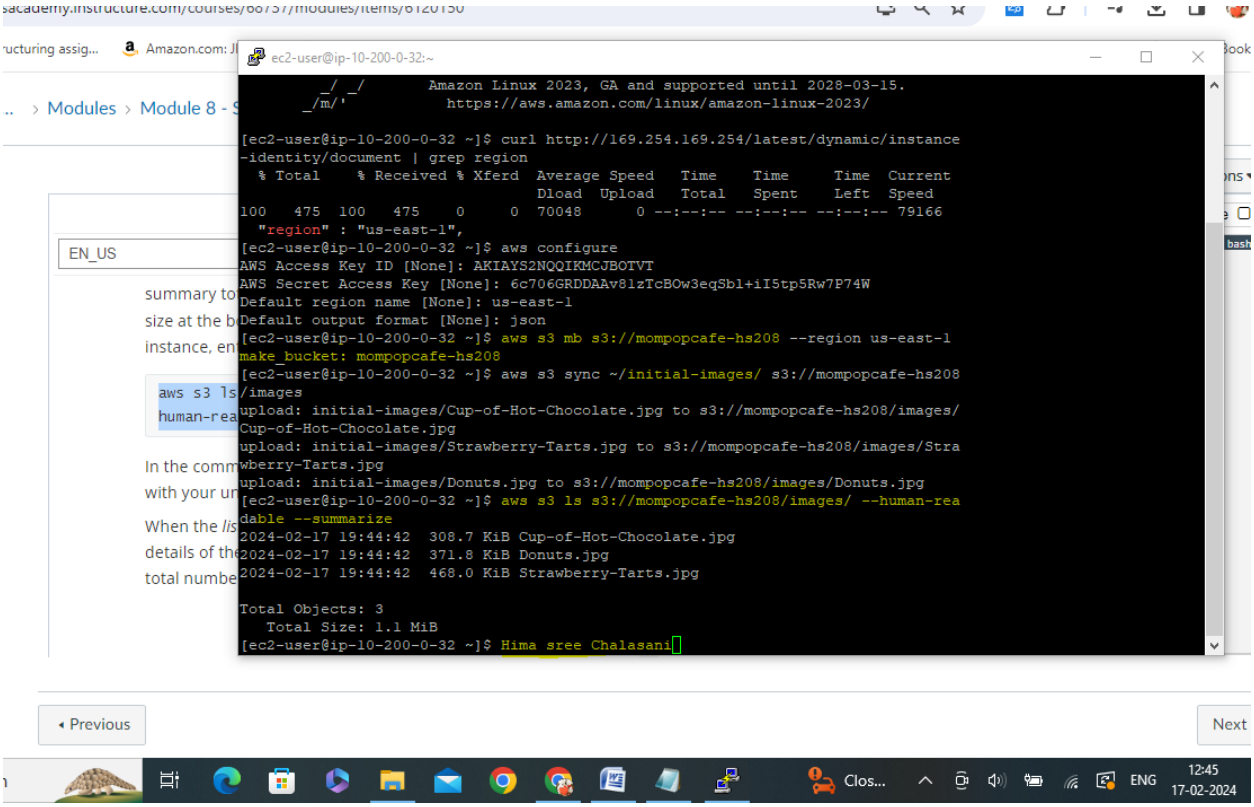


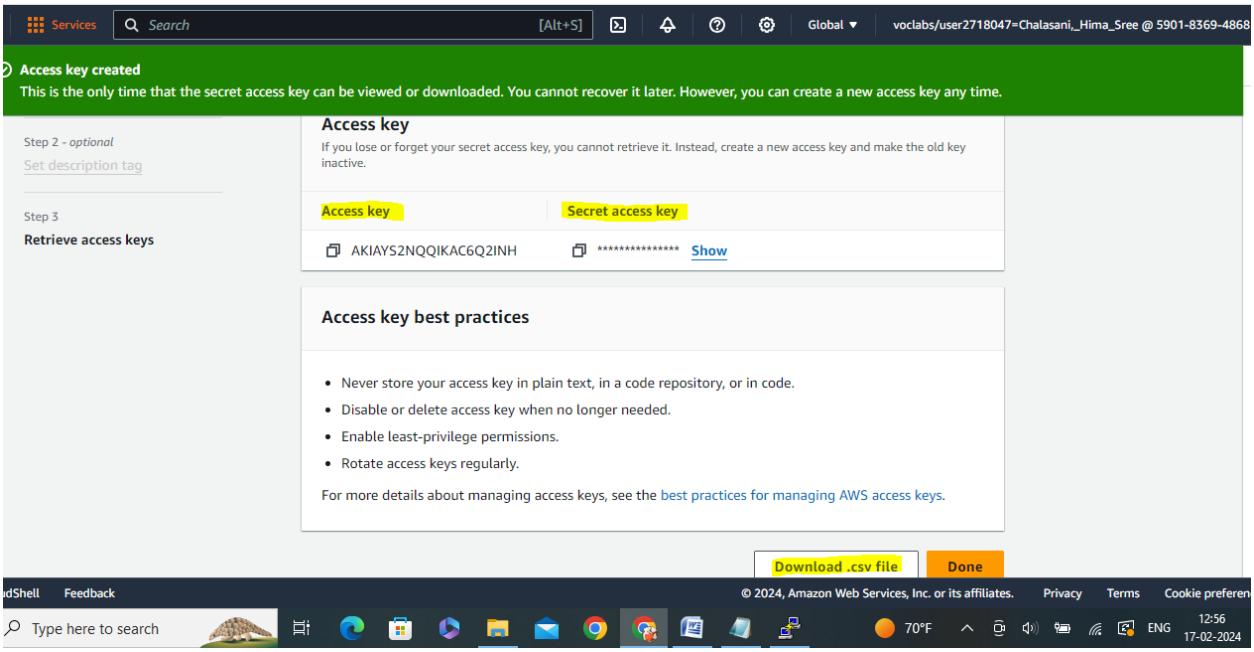


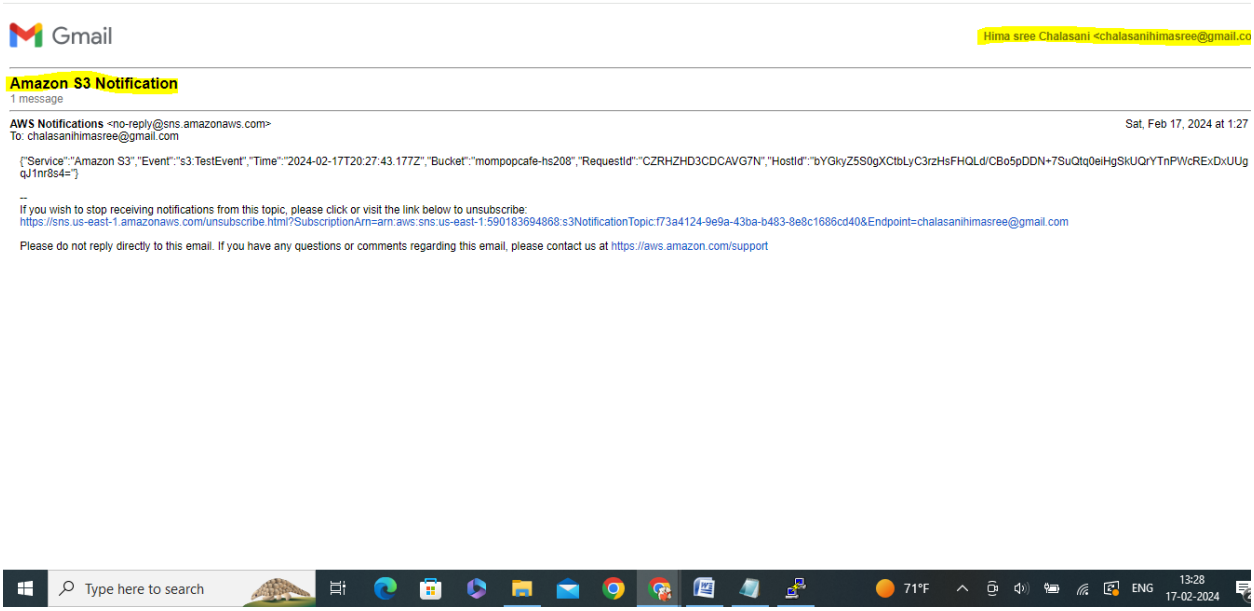
How to synchronize files using the command line (aws s3api and aws s3)

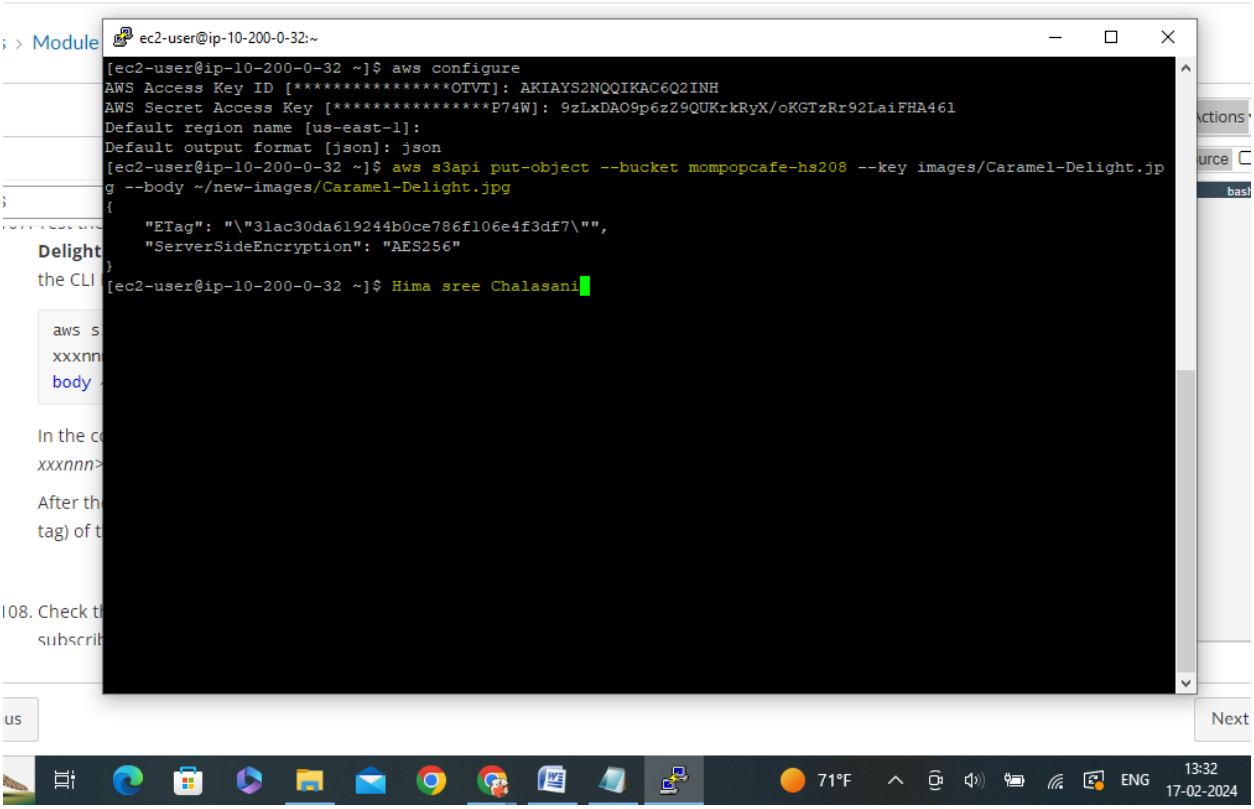
1. Activate Versioning for the Bucket: Ensure that versioning is turned on for the bucket to effectively utilize Amazon's s3api commands.
2. Synchronize Local Files with Amazon S3: Use the `aws s3 sync` command to match your local files with those on Amazon S3.
3. Remove Local File: Delete the file from your local storage device.
4. Restore Deleted File from Amazon S3: Utilize `aws s3api list-object-versions` and `aws s3api get-object` commands to retrieve a previous version of a deleted file from Amazon S3. Use AWS S3 Sync to restore the file. Sample files are available for download. Access the processor instance and download the sample file by following the link provided in the lab instructions.
5. Extract Downloaded File: Execute the `unzip files.zip` command in the terminal to decompress the downloaded file.
6. Activate Versioning: Enable versioning using the command `aws s3api put-bucket-versioning --smmr --versioning-configuration Status=Enabled`.
7. Synchronize Folder Content with S3 Bucket: Match the content of the folder with the S3 bucket using `aws s3 sync files s3://smmr/files/`.
8. Delete Local File: Remove the file from local storage using the command `rm files/file1.txt`.

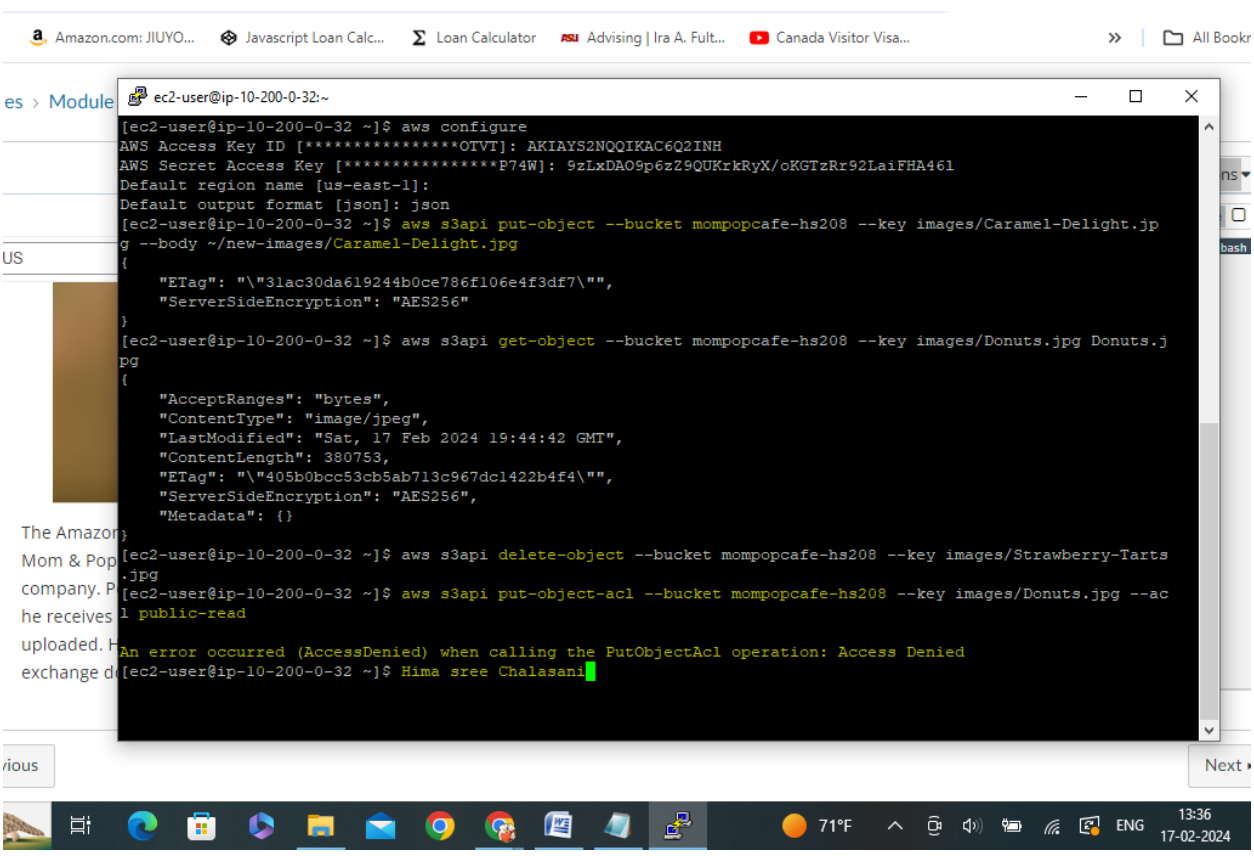
9. Delete File from S3 Using --delete Option: Use `aws s3 sync` with the `--delete` option to erase the same file from the server: `aws s3 sync files s3://S3-BUCKET-NAME/files/ --delete`.
10. Confirm Remote Deletion: Verify the deletion of the file from the server by running the command `ls s3 aws s3://smmr/files/`.
11. Synchronize Old File Version with Amazon S3: Match the previous version of the file with Amazon S3 using the command `aws s3api get-object --bucket smmr --key files/file1.txt --version-id VERSION-ID files/file1.txt`.
12. Re-Synchronize File or Folder to Amazon S3: Execute `aws s3 sync files s3://S3-BUCKET-NAME/files/` to re-synchronize the content of a file or folder with Amazon S3.




Services
Search
[Alt+S]
Global
voclabs/user2718047=Chalasani,_Hima_Sree @ 5901-8369-4868
Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.
Access key
Secret access key
AKIAYS2NQQIKAC6Q2INH
****
Show
Access key best practices
Never store your access key in plain text, in a code repository, or in code.
Disable or delete access key when no longer needed.
Enable least-privilege permissions.
Rotate access keys regularly.
For more details about managing access keys, see the best practices for managing AWS access keys.
Download .csv file
Done
dShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferen
Type here to search
70°F
ENG
12:56
17-02-2024

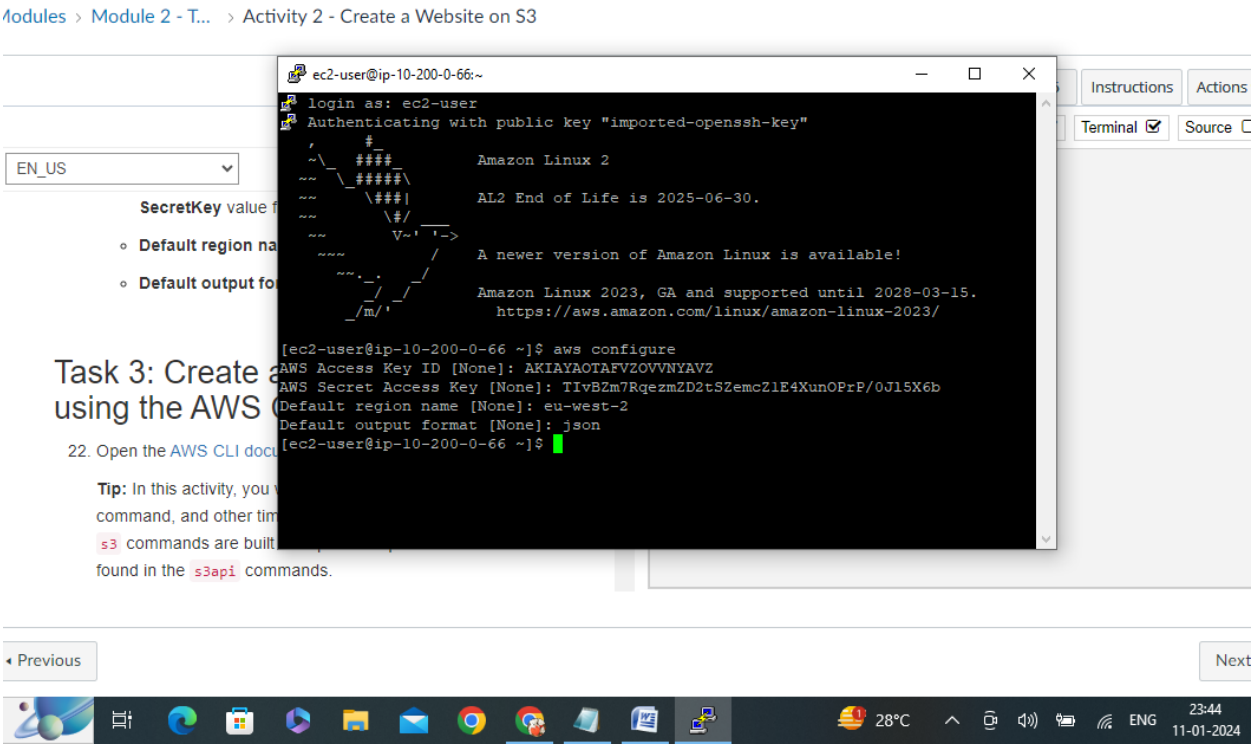

Gmail
Hima sree Chalasani <chalasanihimasree@gmail.co
Amazon S3 Notification
1 message
AWS Notifications <no-reply@sns.amazonaws.com>
To: chalasanihimasree@gmail.com
Sat, Feb 17, 2024 at 1:27
{"Service":"Amazon S3","Event":"s3:TestEvent","Time":"2024-02-17T20:27:43.177Z","Bucket":"mompopcafe-hs208","RequestId":"CZRHZHD3CDCAVG7N","HostId":"bYGkyZ5S0gXCtbLyC3rzHsFHQLd/CBo5pDDN+7SuQtq0eiHgSkUQrYTnPWcRExDxUUgqJ1nr8s4="}
--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:590183694868:s3NotificationTopic:f73a4124-9e9a-43ba-b483-8e8c1686cd40&Endpoint=chalasanihimasree@gmail.com
Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support
Type here to search
71°F
ENG
13:28
17-02-2024

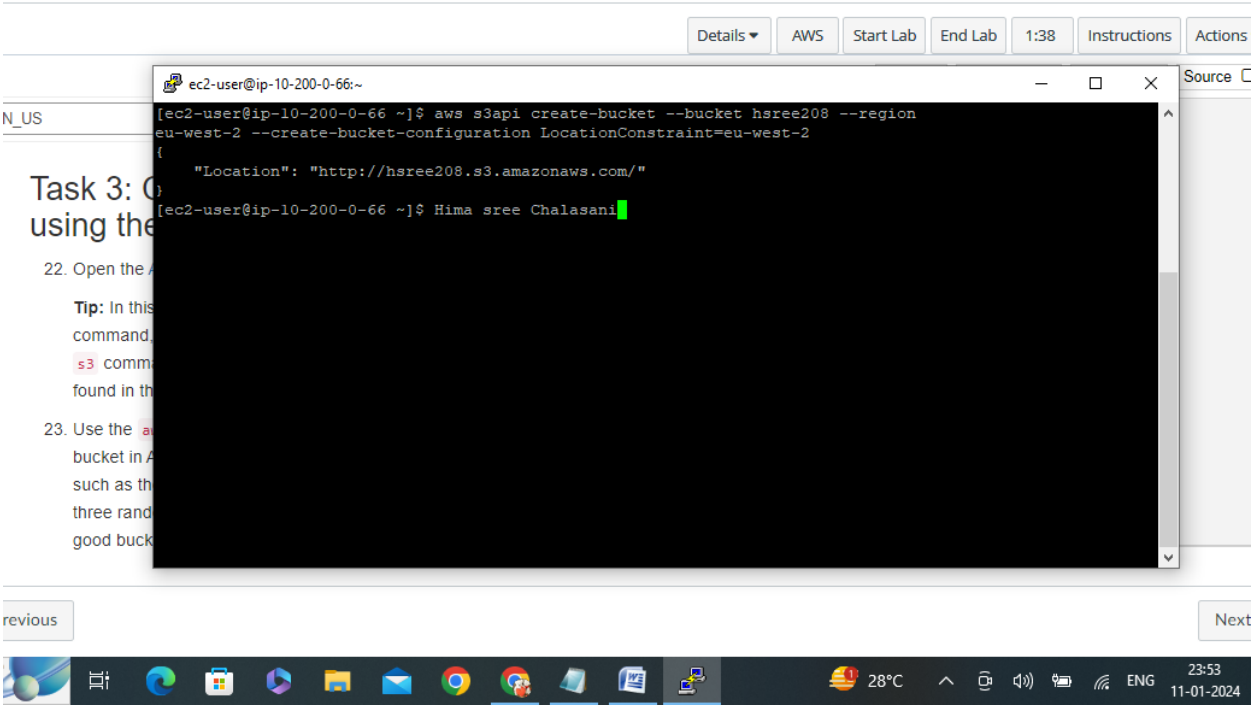

ec2-user@ip-10-200-0-32:~
[ec2-user@ip-10-200-0-32 ~]$ aws configure
AWS Access Key ID [****************OTVT]: AKIAYS2NQQIKAC6Q2INH
AWS Secret Access Key [****************P74W]: 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
Default region name [us-east-1]:
Default output format [json]: json
[ec2-user@ip-10-200-0-32 ~]$ aws s3api put-object --bucket mompopcafe-hs208 --key images/Caramel-Delight.jpg --body ~/new-images/Caramel-Delight.jpg
{
"ETag": "\"31ac30da619244b0ce786f106e4f3df7\"",
"ServerSideEncryption": "AES256"
}
[ec2-user@ip-10-200-0-32 ~]$ Hima sree Chalasani
Next
71°F
ENG
13:32
17-02-2024

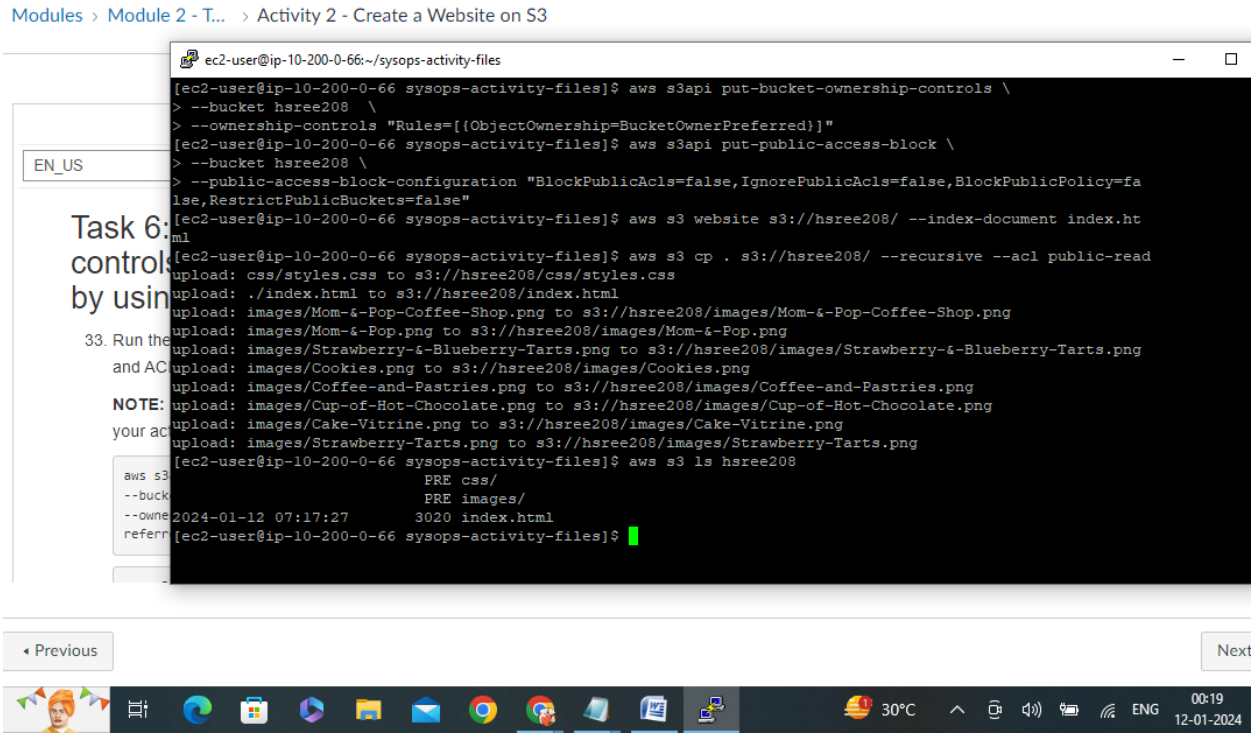

Amazon.com: JIUYO...
Javascript Loan Calc...
Loan Calculator
Advising | Ira A. Fult...
Canada Visitor Visa...
All Bookr
ec2-user@ip-10-200-0-32:~
[ec2-user@ip-10-200-0-32 ~]$ aws configure
AWS Access Key ID [****************OTVT]: AKIAYS2NQQIKAC6Q2INH
AWS Secret Access Key [****************P74W]: 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
Default region name [us-east-1]:
Default output format [json]: json
[ec2-user@ip-10-200-0-32 ~]$ aws s3api put-object --bucket mompopcafe-hs208 --key images/Caramel-Delight.jpg --body ~/new-images/Caramel-Delight.jpg
{
"ETag": "\"31ac30da619244b0ce786f106e4f3df7\"",
"ServerSideEncryption": "AES256"
}
[ec2-user@ip-10-200-0-32 ~]$ aws s3api get-object --bucket mompopcafe-hs208 --key images/Donuts.jpg Donuts.jpg
{
"AcceptRanges": "bytes",
"ContentType": "image/jpeg",
"LastModified": "Sat, 17 Feb 2024 19:44:42 GMT",
"ContentLength": 380753,
"ETag": "\"405b0bcc53cb5ab713c967dc1422b4f4\"",
"ServerSideEncryption": "AES256",
"Metadata": {}
}
[ec2-user@ip-10-200-0-32 ~]$ aws s3api delete-object --bucket mompopcafe-hs208 --key images/Strawberry-Tarts.jpg
[ec2-user@ip-10-200-0-32 ~]$ aws s3api put-object-acl --bucket mompopcafe-hs208 --key images/Donuts.jpg --acl public-read
An error occurred (AccessDenied) when calling the PutObjectAcl operation: Access Denied
[ec2-user@ip-10-200-0-32 ~]$ Hima sree Chalasani
Next
71°F
ENG
13:36
17-02-2024

How to create a S3 bucket via the CLI

1. Set up and customize the AWS CLI on your personal computer.
2. Select a name for the bucket that is unique worldwide.
3. Decide on the AWS region where the bucket will reside.
4. Establish the S3 bucket employing the aws s3api create-bucket command: 'aws s3 create-bucket --bucket $bucket_name --region $aws_region'.
5. Confirm the creation of the bucket by running: 'aws s3 ls'

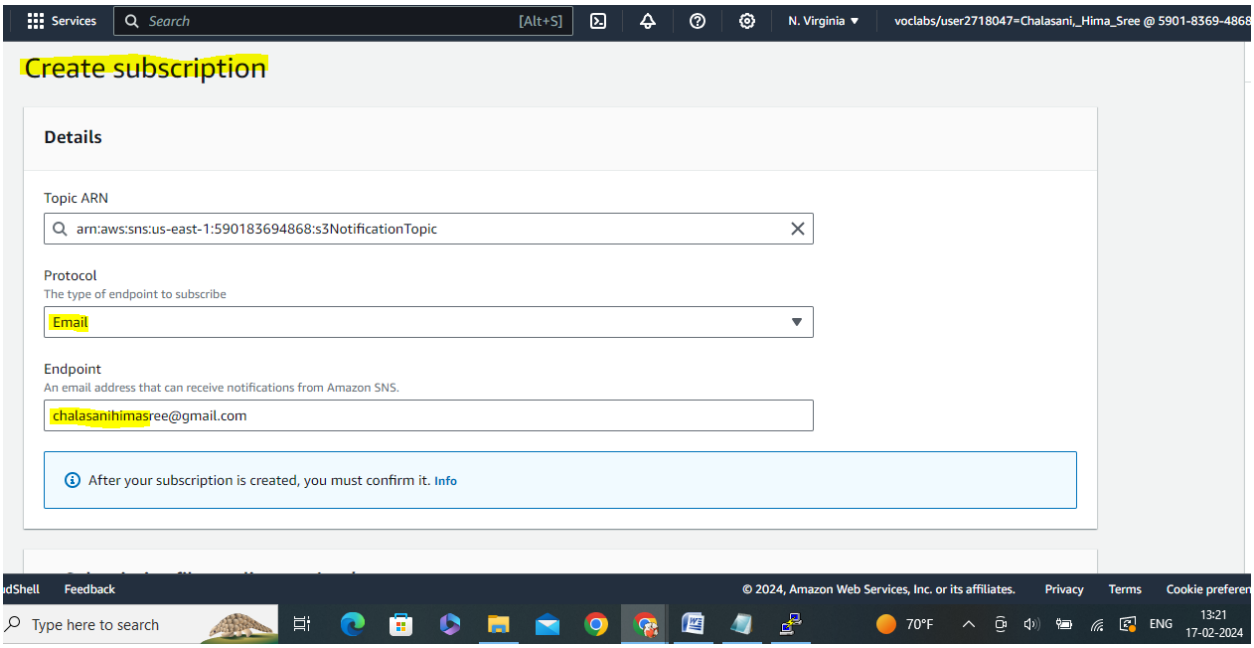


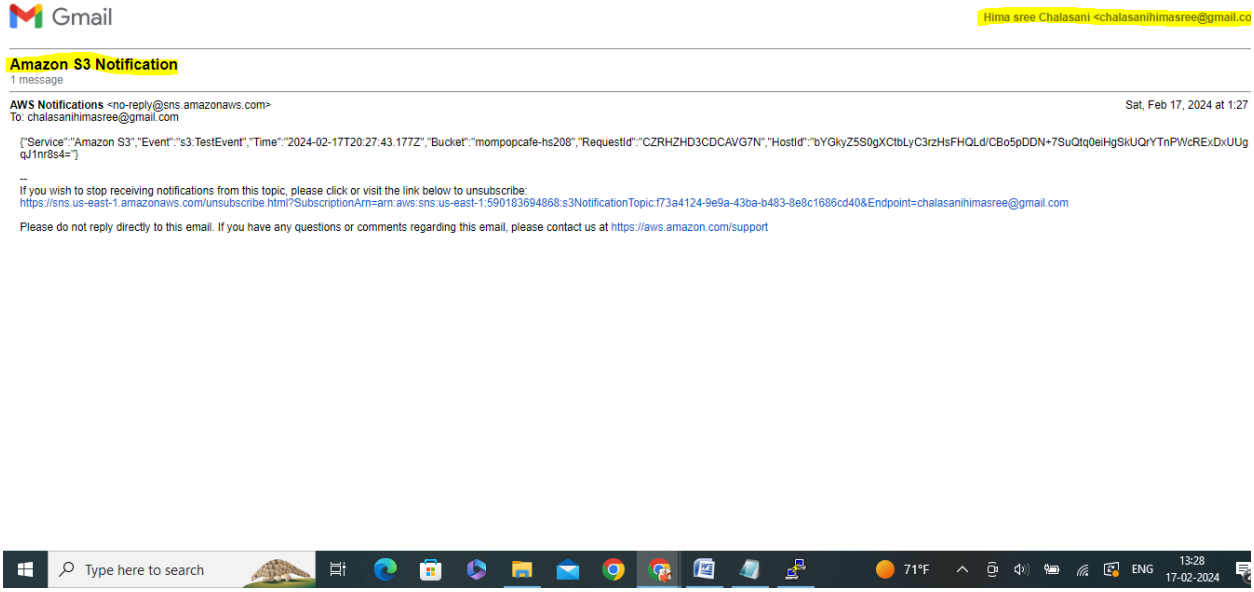

Details
AWS
Start Lab
End Lab
1:38
Instructions
Actions
Source
ec2-user@ip-10-200-0-66:~
[ec2-user@ip-10-200-0-66 ~]$ aws s3api create-bucket --bucket hsree208 --region
eu-west-2 --create-bucket-configuration LocationConstraint=eu-west-2
{
"Location": "http://hsree208.s3.amazonaws.com/"
}
[ec2-user@ip-10-200-0-66 ~]$ Hima sree Chalasani
N_US
Task 3:
using the
22. Open the
Tip: In this
command
s3 comma
found in th
23. Use the a
bucket in A
such as th
three rand
good buck
revious
Next
28°C
ENG
23:53
11-01-2024


Modules
Module 2 - T...
Activity 2 - Create a Website on S3
ec2-user@ip-10-200-0-66:~/sysops-activity-files
[ec2-user@ip-10-200-0-66 sysops-activity-files]$ aws s3api put-bucket-ownership-controls \
> --bucket hsree208 \
> --ownership-controls "Rules=[{ObjectOwnership=BucketOwnerPreferred}]"
[ec2-user@ip-10-200-0-66 sysops-activity-files]$ aws s3api put-public-access-block \
> --bucket hsree208 \
> --public-access-block-configuration "BlockPublicAcls=false,IgnorePublicAcls=false,BlockPublicPolicy=fa
lse,RestrictPublicBuckets=false"
[ec2-user@ip-10-200-0-66 sysops-activity-files]$ aws s3 website s3://hsree208/ --index-document index.ht
ml
[ec2-user@ip-10-200-0-66 sysops-activity-files]$ aws s3 cp . s3://hsree208/ --recursive --acl public-read
upload: css/styles.css to s3://hsree208/css/styles.css
upload: ./index.html to s3://hsree208/index.html
upload: images/Mom-&-Pop-Coffee-Shop.png to s3://hsree208/images/Mom-&-Pop-Coffee-Shop.png
upload: images/Mom-&-Pop.png to s3://hsree208/images/Mom-&-Pop.png
upload: images/Strawberry-&-Blueberry-Tarts.png to s3://hsree208/images/Strawberry-&-Blueberry-Tarts.png
upload: images/Cookies.png to s3://hsree208/images/Cookies.png
upload: images/Coffee-and-Pastries.png to s3://hsree208/images/Coffee-and-Pastries.png
upload: images/Cup-of-Hot-Chocolate.png to s3://hsree208/images/Cup-of-Hot-Chocolate.png
upload: images/Cake-Vitrine.png to s3://hsree208/images/Cake-Vitrine.png
upload: images/Strawberry-Tarts.png to s3://hsree208/images/Strawberry-Tarts.png
[ec2-user@ip-10-200-0-66 sysops-activity-files]$ aws s3 ls hsree208
PRE css/
PRE images/
2024-01-12 07:17:27 3020 index.html
[ec2-user@ip-10-200-0-66 sysops-activity-files]$
EN_US
Task 6:
control
by usin
33. Run the
and AC
NOTE:
your ac
Previous
Next
30°C
ENG
00:19
12-01-2024

How to add an event notification to a S3 bucket

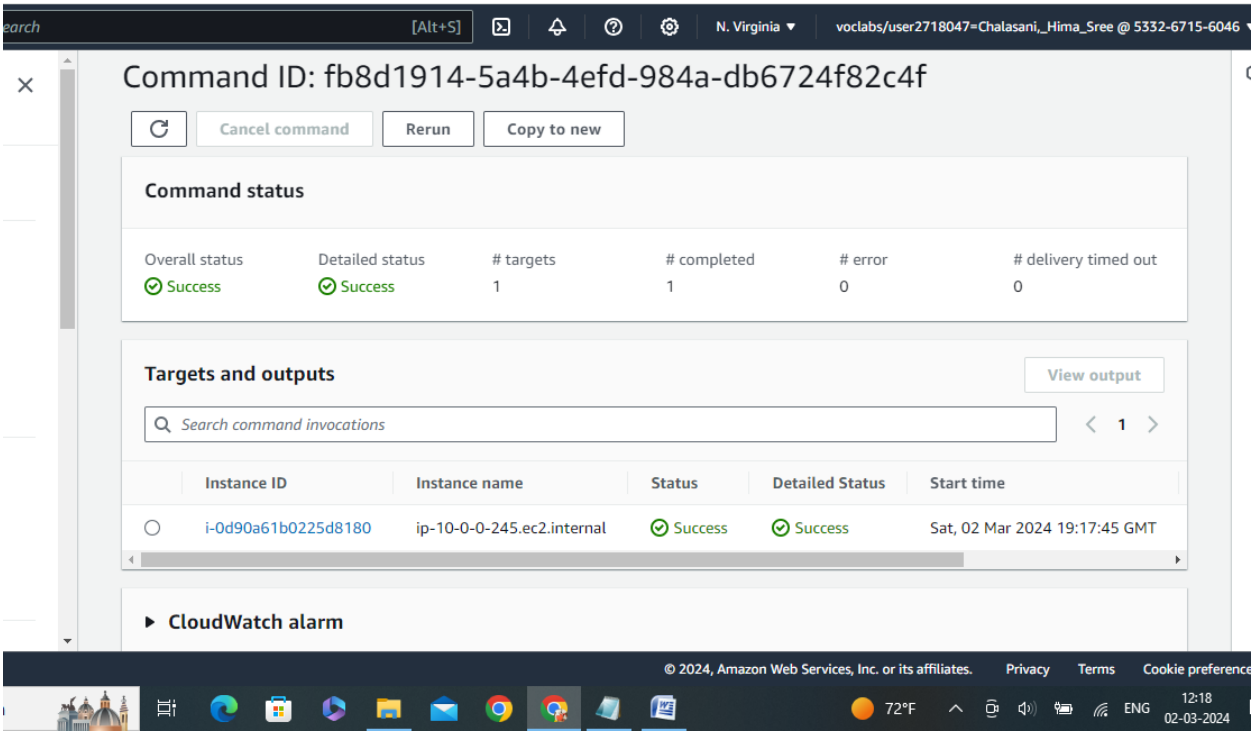
1. Generate an SNS topic.
2. Retrieve the Amazon Resource Name (ARN) of the topic.
3. Grant permission to enable S3 to publish messages to the SNS topic.
4. Configure the event notification settings for the S3 bucket.

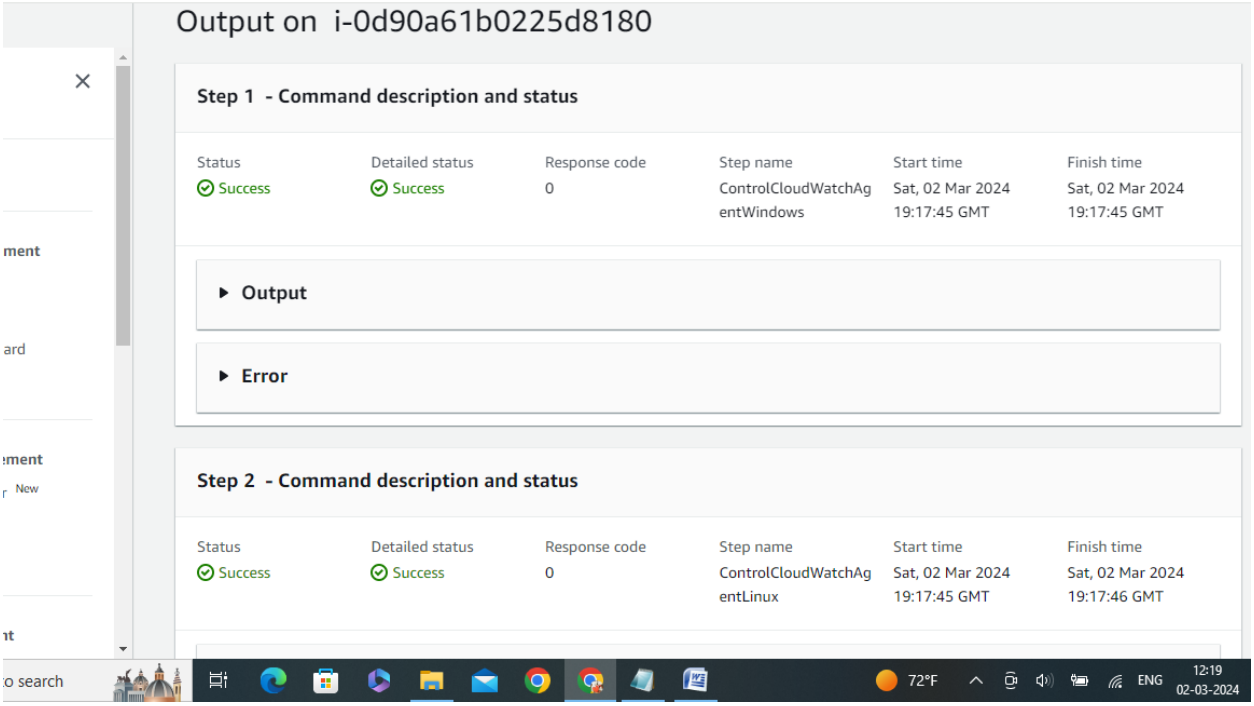




How to install the CloudWatch Agent

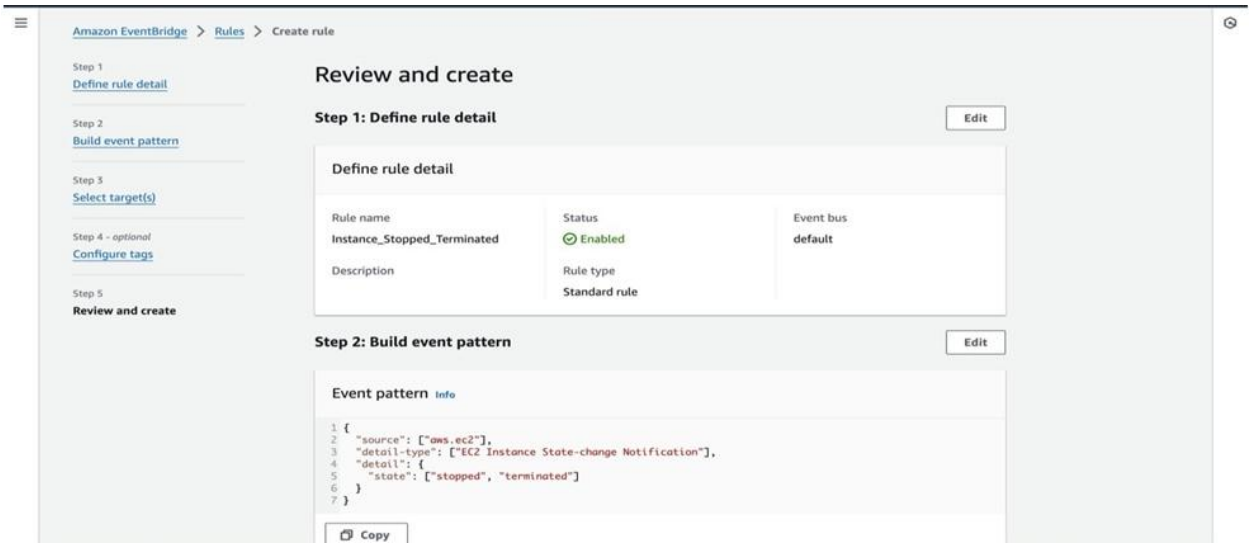
1. Access the Systems Manager console.
2. Navigate to the Run Command section and opt for AWS-ConfigureAWSPackage.
3. Customize the installation parameters for the CloudWatch Agent (Action, Name, Version).
4. Designate the specific EC2 instance as the target.
5. Commence the installation process for the CloudWatch Agent.
6. Monitor the installation progress and await confirmation of success.
7. Validate the successful installation through command output.
8. Review instance details and expand the status of the command.
9. Ensure the appearance of the "Successfully installed CloudWatchAgent" message.
10. Establish the configuration of the CloudWatch Agent by generating a config file within Parameter Store.
11. Define the desired logs and metrics for collection within the config file.

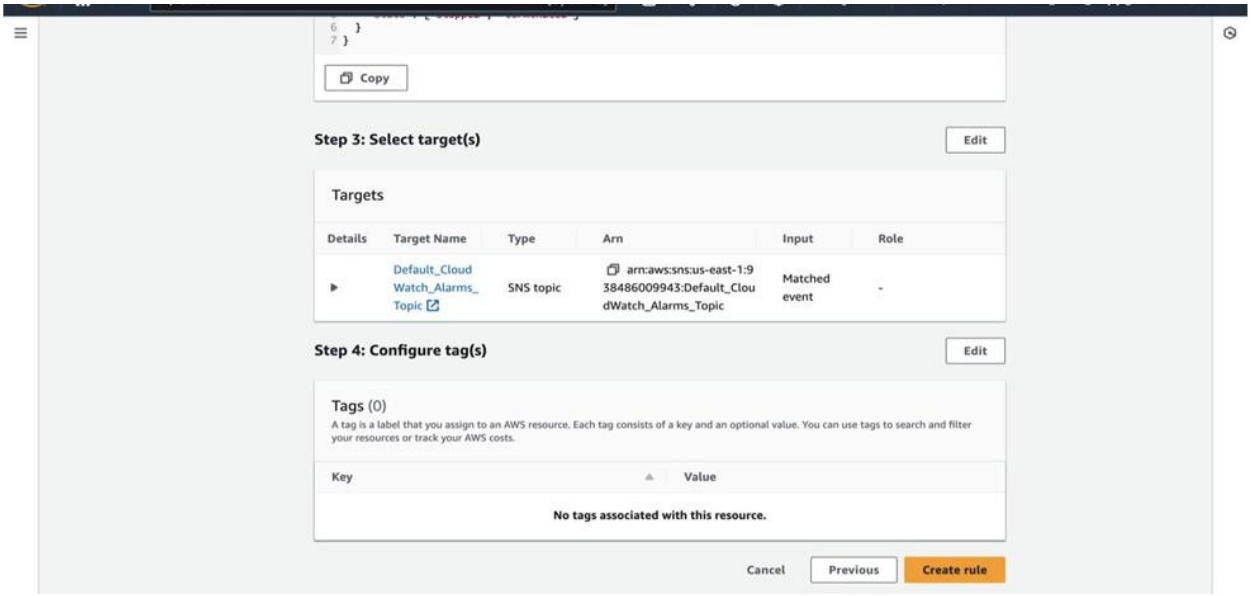




How to create a CloudWatch Events/CloudWatch EventBridge notification rule

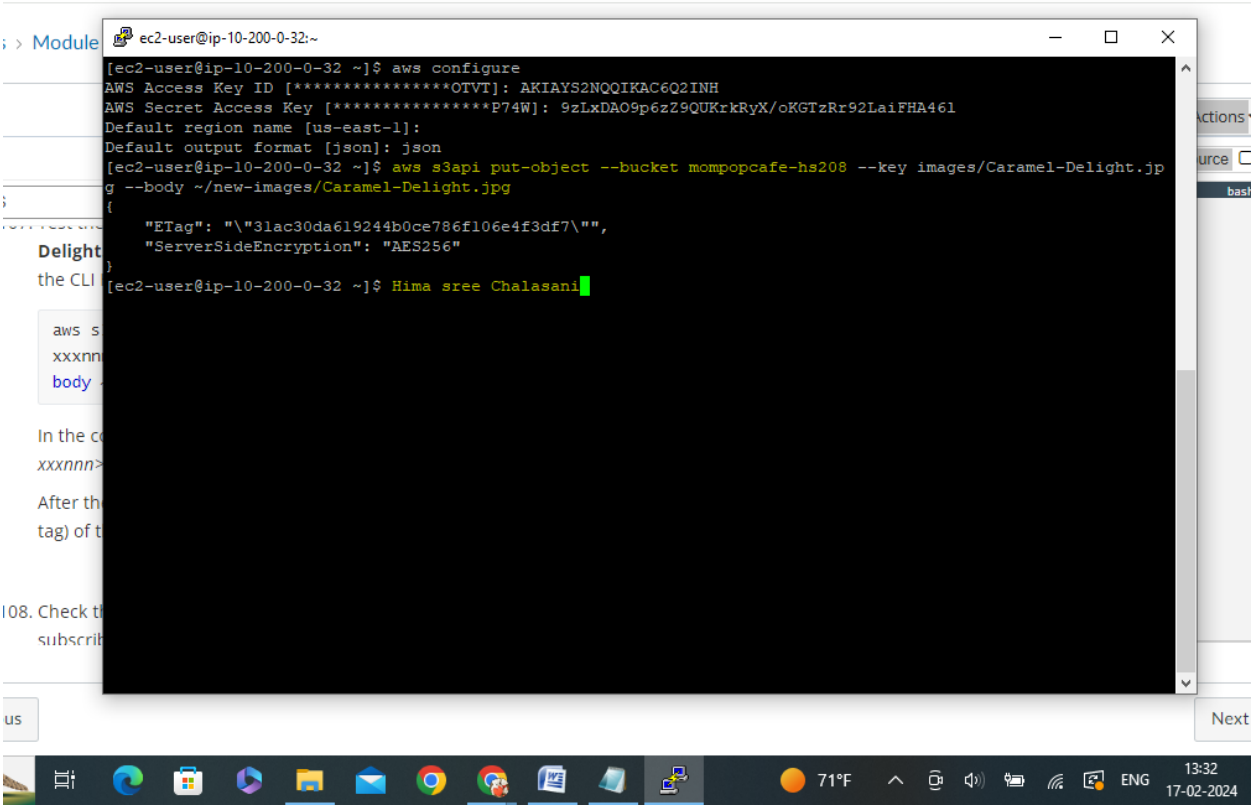
1. Execute aws configure to configure AWS CLI credentials.
2. Utilize the AWS CloudWatch Events put-rule command:aws events put-rule --name RuleName --event-pattern '{"source": ["aws.ec2"],"detail-type": ["EC2 Instance State-change Notification"],"resources": ["arn:aws:ec2:Region:AccountID:instance/InstanceID"],"detail": {"state": ["stopped"]}}'
3. Execute the AWS CloudWatch Events put-targets command:aws events put-targets --rule RuleName --targets Id=1,Arn=arn:aws:lambda:Region:AccountID:function:LambdaFunctionName
4. Validate the rule and associated target by checking the CloudWatch Events Console or executing aws events list-targets-by-rule --rule RuleName.





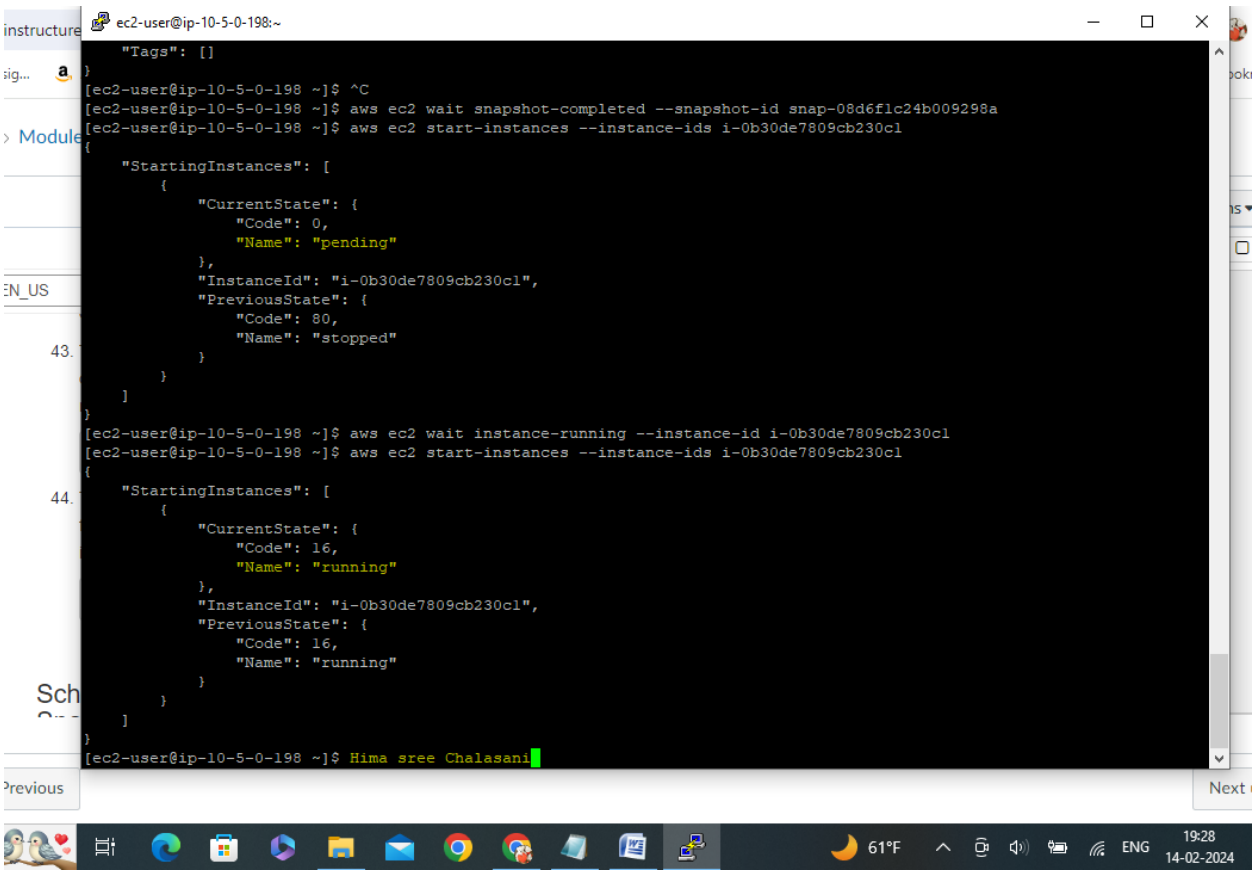
How to use the prebuilt stopinator script to turn off instances with the tag value of your full name

1. Retrieve the pre-assembled Stopinator script from the AWS GitHub repository:
2. curl -O https://raw.githubusercontent.com/awsdocs/aws-doc-sdk-examples/main/python/example_code/cloudwatch/stopinator.py
3. Grant executable permissions to the script: chmod +x stopinator.py
4. Execute the script: ./stopinator.py HimasreeChalasani



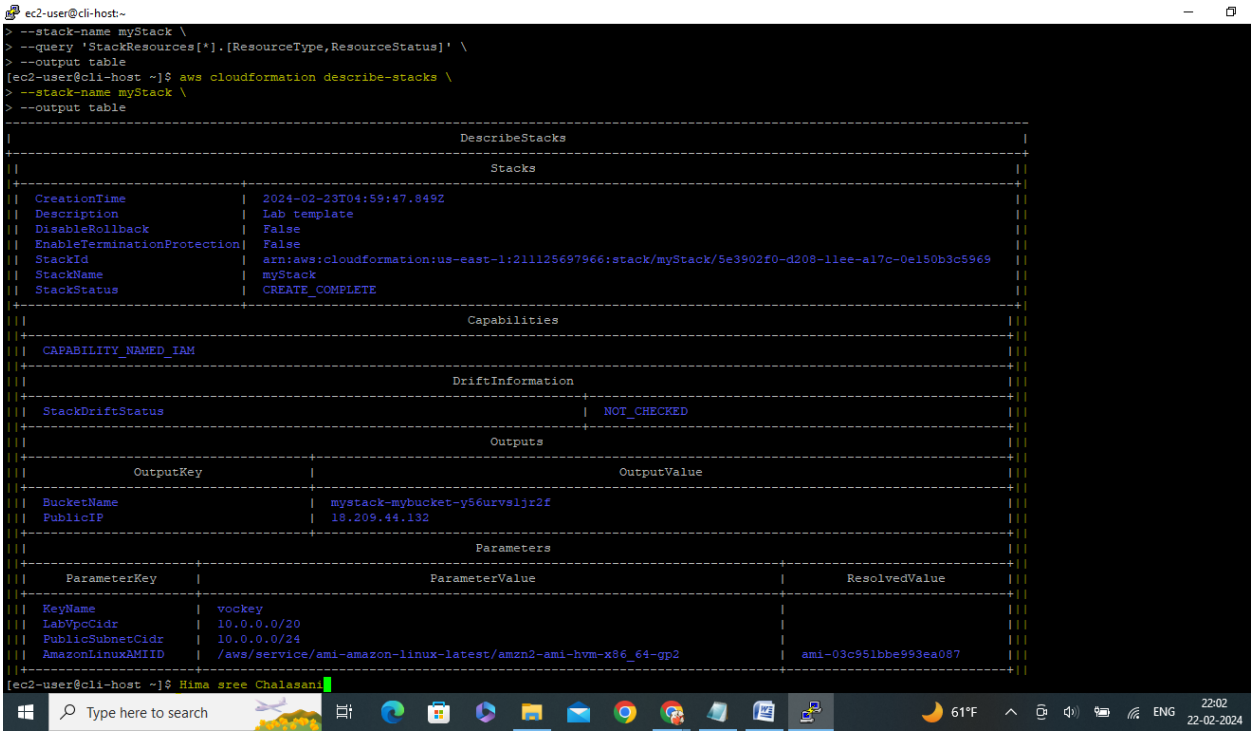
How to resize an EC2 instance using the AWS CLI

1. Utilize aws configure to configure AWS CLI credentials.
2. Execute the AWS EC2 modify-instance-attribute command:
   aws ec2 modify-instance-attribute --instance-id InstanceID --instance-type NewInstanceType
3. Substitute InstanceID with the EC2 instance ID that requires resizing.
4. Replace NewInstanceType with the desired instance type.
5. Validate the modifications in the AWS EC2 Console or execute aws ec2 describe-instances --instance-ids InstanceID to verify the instance type.
6. Optionally, it may be necessary to halt and restart the instance for the changes to take effect:
7. aws ec2 stop-instances --instance-ids InstanceID
   aws ec2 start-instances --instance-ids InstanceID



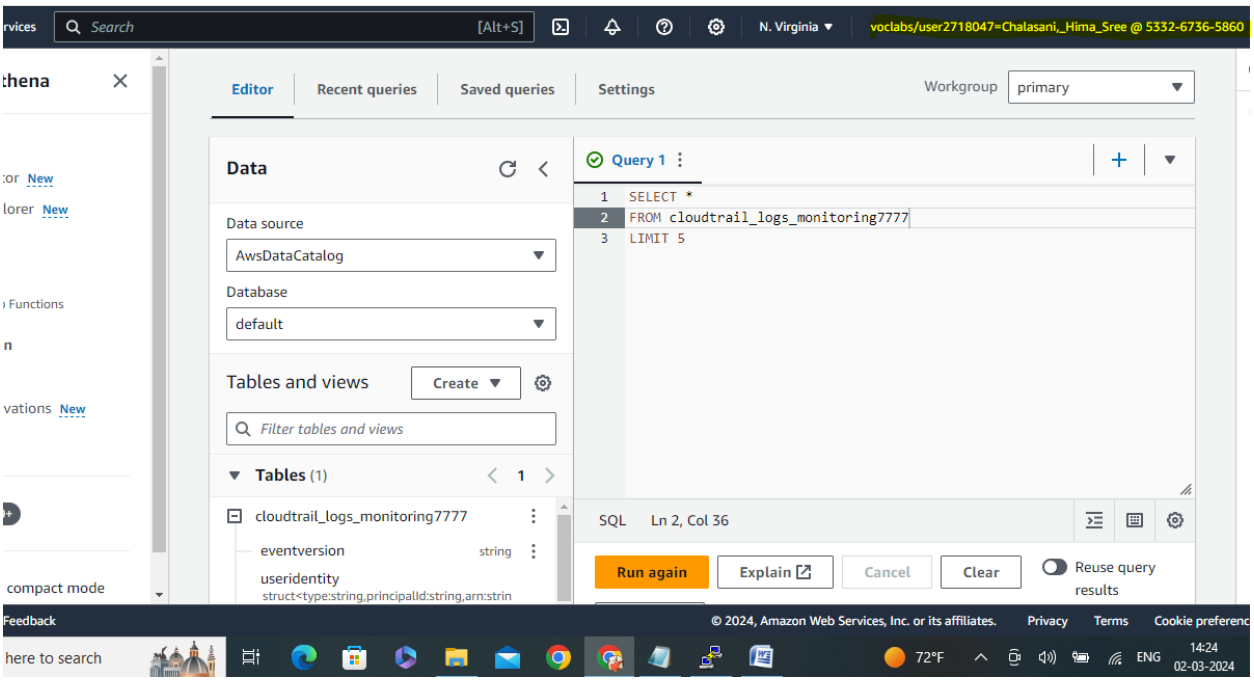
How to detect drift in a CloudFormation template

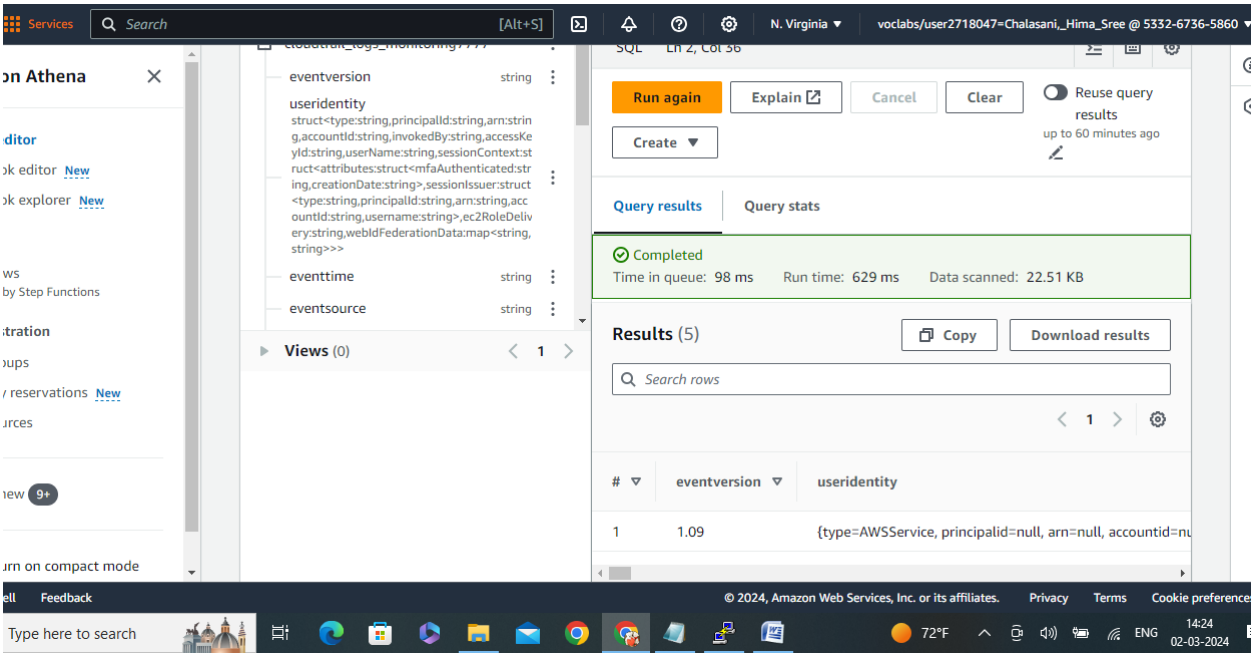
1. Utilize aws configure to establish AWS CLI credentials.
2. Execute the AWS CloudFormation detect-stack-drift command: aws cloudformation detect-stack-drift --stack-name StackName
3. Keep track of the drift detection status: aws cloudformation describe-stack-drift-detection-status --stack-drift-detection-id DriftDetectionId
4. Review the drift results: aws cloudformation describe-stack-resource-drifts --stack-name StackName
5. Alternatively, the drift detection process can be automated through CloudWatch Events or AWS Config, if desired.

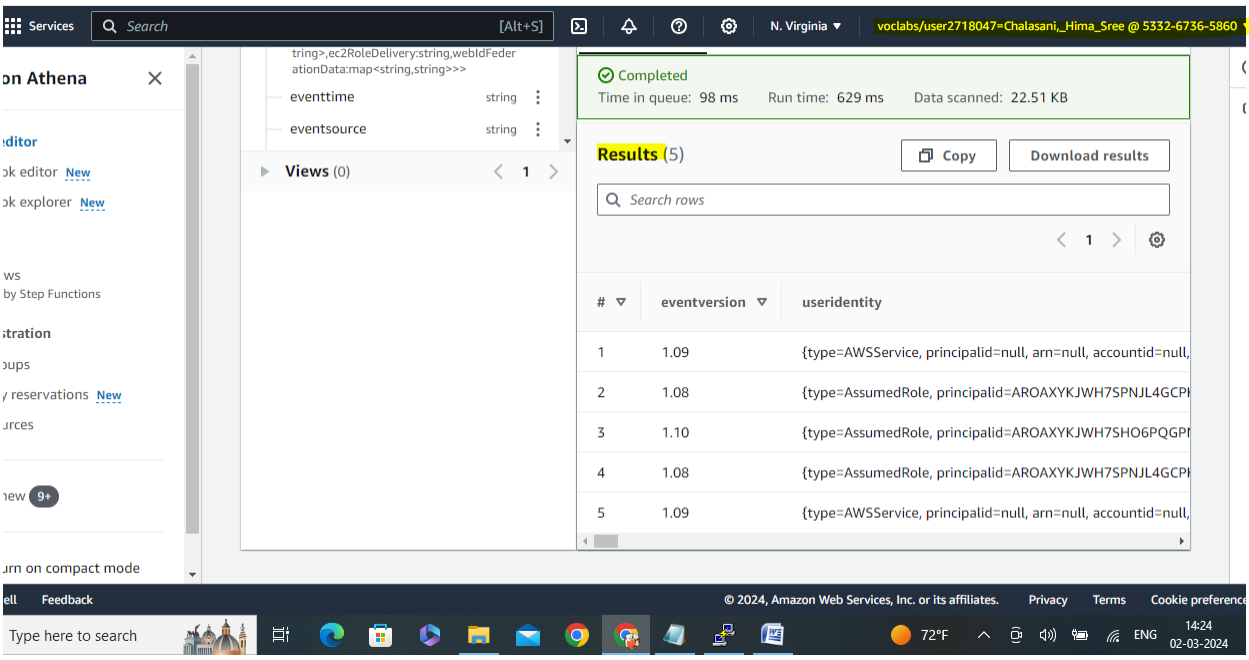


How to create an Amazon Athena table

1. Access the Amazon Athena Console.
2. Choose the Database: From the left panel, select the database in which we intend to establish the table.
3. Execute a CREATE TABLE Query:
   Example:
   CREATE TABLE IF NOT EXISTS table_name (column1_name datatype1, column2_name datatype2, ...);
4. Initiate the execution of the CREATE TABLE statement by clicking the "Run Query" button.
5. Upon completion of the query execution, confirm the creation of the table by inspecting the "Tables" tab within the Athena console.

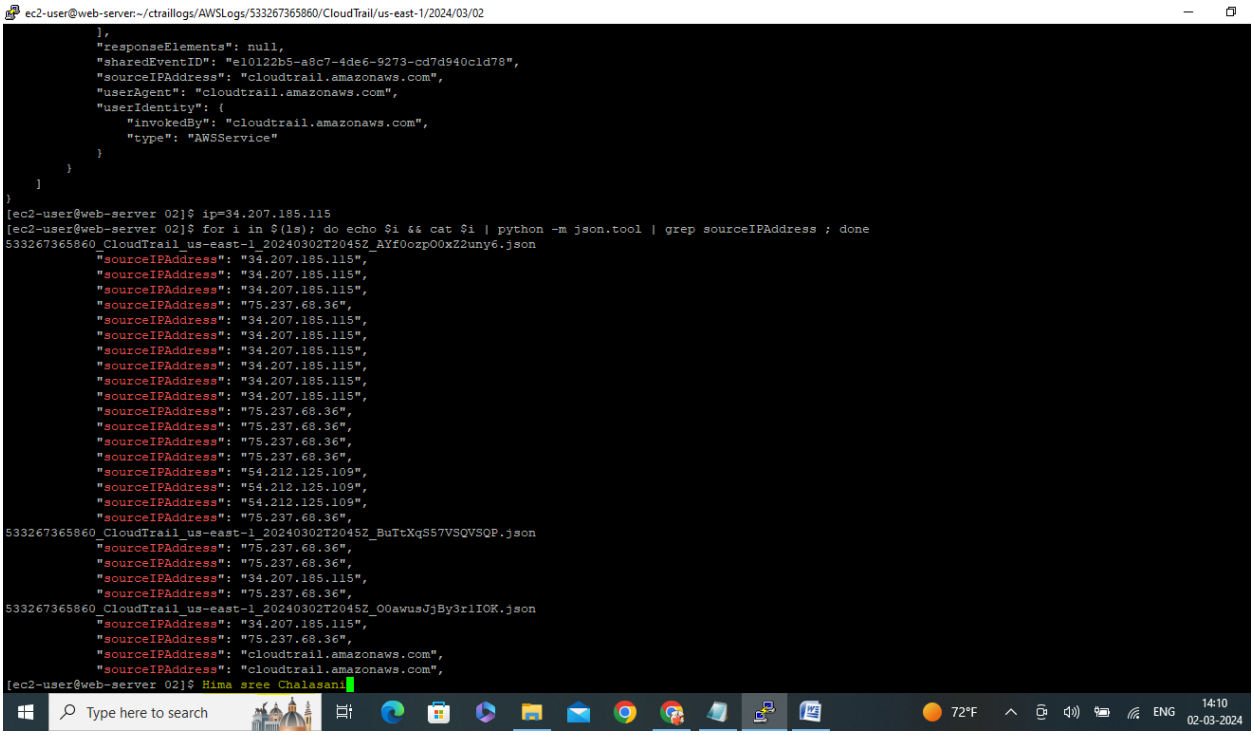

Search [Alt+S]
N. Virginia
voclabs/user2718047=Chalasani,_Hima_Sree @ 5332-6736-5860
Editor
Recent queries
Saved queries
Settings
Workgroup
primary
Data
Data source
AwsDataCatalog
Database
default
Tables and views
Create
Filter tables and views
Tables (1)
cloudtrail_logs_monitoring7777
eventversion
string
useridentity
struct<type:string,principalId:string,arn:strin
Query 1
SELECT *
FROM cloudtrail_logs_monitoring7777
LIMIT 5
SQL Ln 2, Col 36
Run again
Explain
Cancel
Clear
Reuse query results
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferenc
here to search
72°F
ENG
14:24
02-03-2024

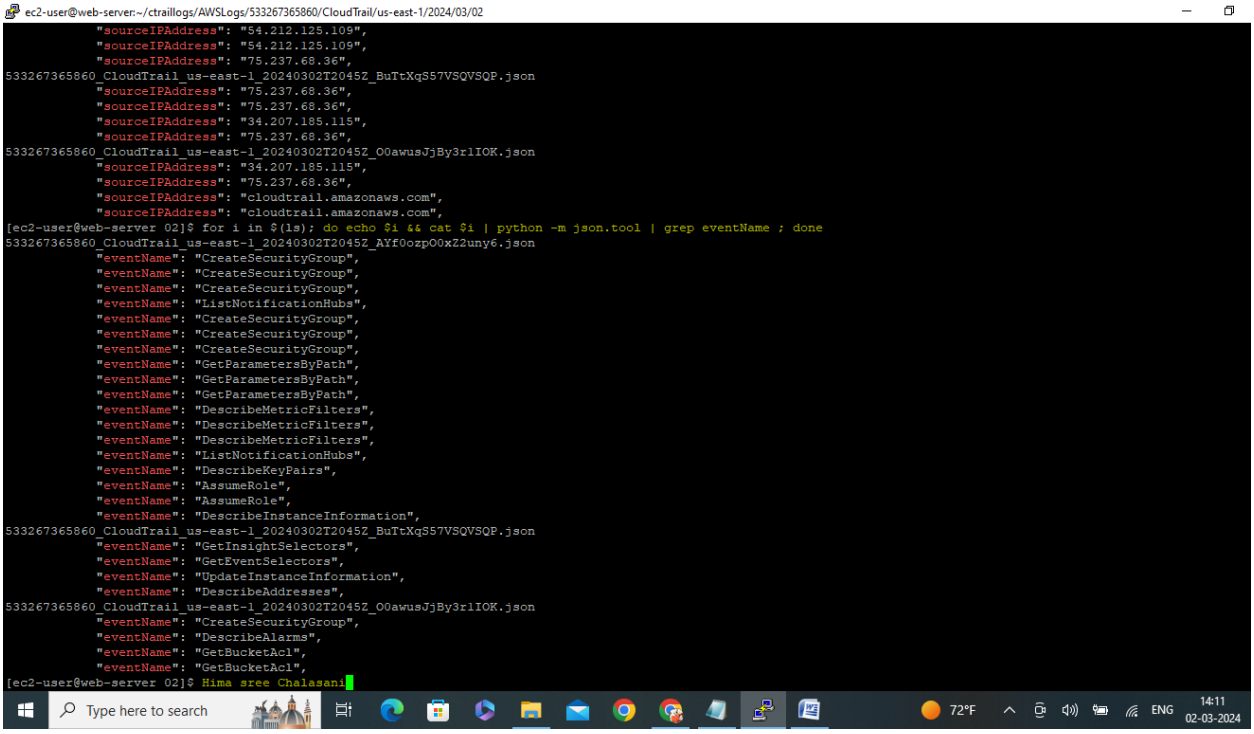

Services
Search [Alt+S]
N. Virginia
voclabs/user2718047=Chalasani,_Hima_Sree @ 5332-6736-5860
eventversion
string
useridentity
struct<type:string,principalId:string,arn:string,accountId:string,invokedBy:string,accessKeyId:string,userName:string,sessionContext:struct<attributes:struct<mfaAuthenticated:string,creationDate:string>,sessionIssuer:struct<type:string,principalId:string,arn:string,accountId:string,username:string>,ec2RoleDelivery:string,webIdFederationData:map<string,string>>>
eventtime
string
eventsource
string
Views (0)
Run again
Explain
Cancel
Clear
Reuse query results
up to 60 minutes ago
Create
Query results
Query stats
Completed
Time in queue: 98 ms
Run time: 629 ms
Data scanned: 22.51 KB
Results (5)
Copy
Download results
Search rows
eventversion useridentity
1 1.09 {type=AWSService, principalid=null, arn=null, accountid=nu
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
72°F
ENG
14:24
02-03-2024



How to manually review access logs to find anomalous user activity

1. Determine the location of access logs.
2. Understand the format of access logs.
3. Ensure that logs are collected and stored in a centralized repository for streamlined analysis. Solutions such as AWS CloudWatch Logs, Elasticsearch, or Splunk can facilitate this process.
4. Establish a baseline representing typical user behavior. Familiarize yourself with common access patterns, IP addresses, user agents, and standard actions.
5. Regularly monitor access logs and configure alerts for detecting specific events or irregular patterns suggestive of anomalous behavior.
6. Be vigilant for any unusual patterns within the access logs.
7. Scrutinize user agents for anomalies, as malicious entities might utilize uncommon or altered user agents.
8. Investigate instances of abnormal access patterns by delving into the corresponding logs. Identify the impacted user accounts and associated resources.
9. Correlate access logs with other log types, such as authentication or system logs, to gain a comprehensive understanding of user activities.
10. Incorporate threat intelligence feeds to recognize IP addresses or user agents linked with documented malicious behavior.
11. Deploy User Behavior Analytics (UBA) tools to automate the detection of aberrant user actions using machine learning algorithms.
12. Document and report any identified findings. Maintain an incident response plan to effectively manage confirmed security incidents.

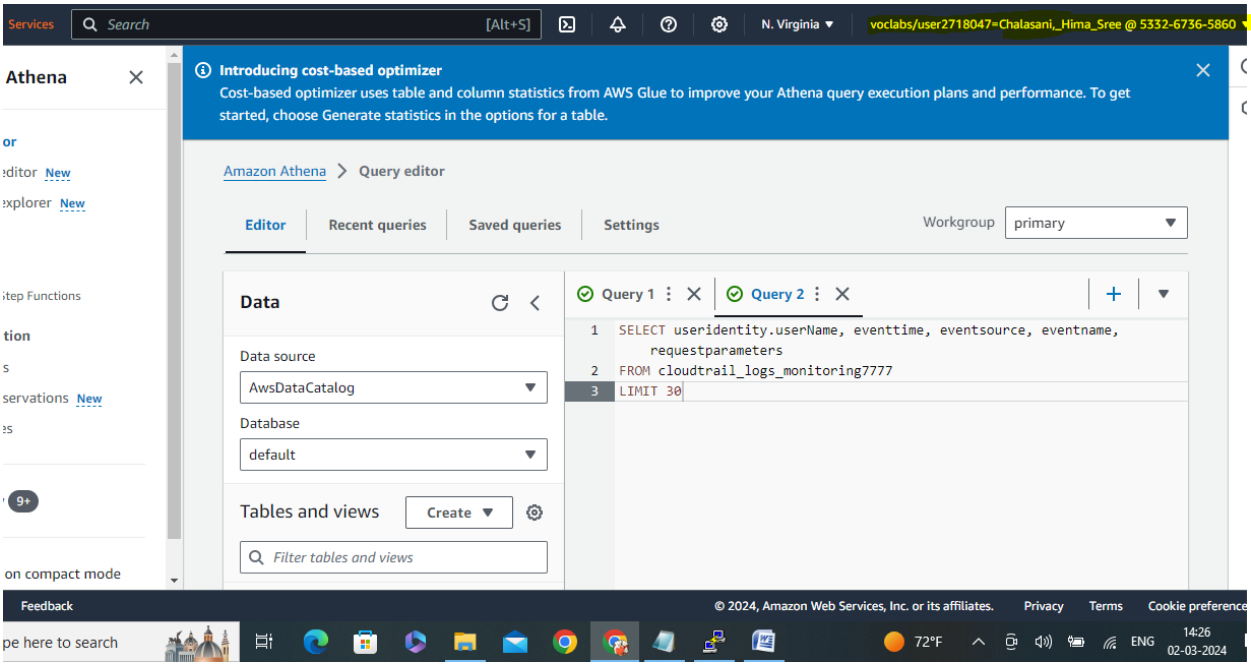


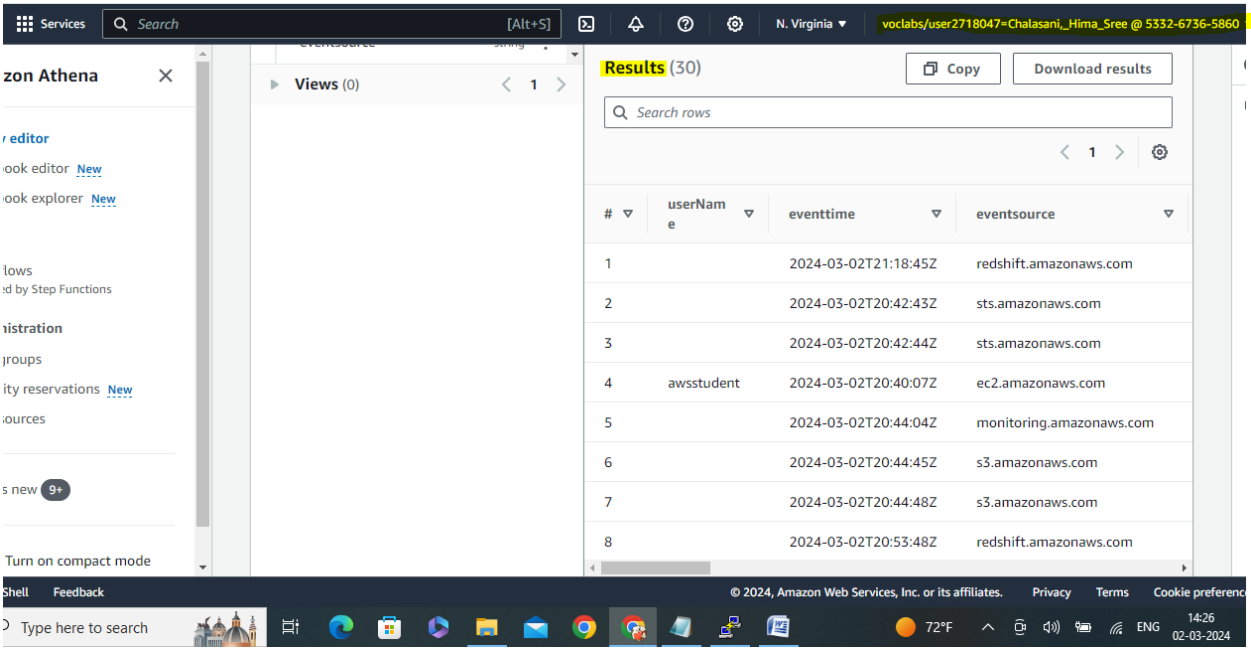


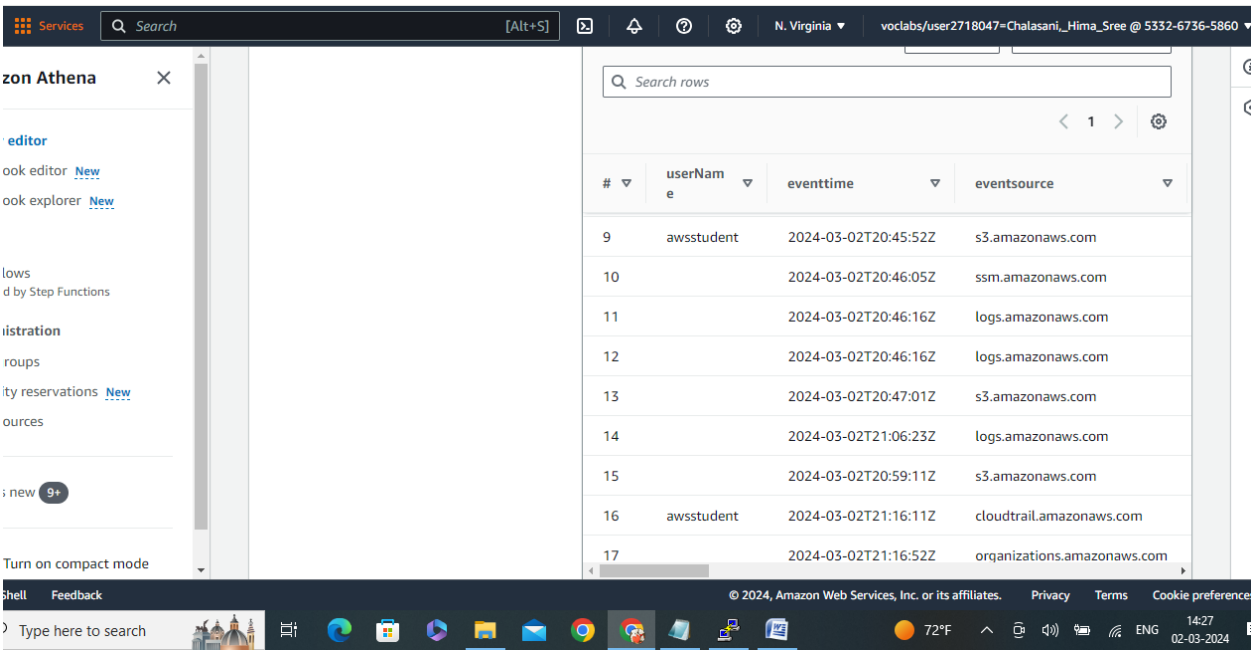
To find using Athena:

1. Utilize the + icon to initiate a new tab for inserting a fresh query.
2. Implement filters on the results by employing a WHERE clause, such as WHERE eventsource = 'ec2.amazonaws.com'.

3. Examine the acquired data and enhance the query to detect occurrences of the term "security."
4. After analyzing the outcomes, construct the following query to retrieve all users active within the account throughout the day:
5. SELECT useridentity.userName, eventtime, eventsource, eventname, requestparameters
   FROM cloudtrail_logs_monitoring7777
   LIMIT 30







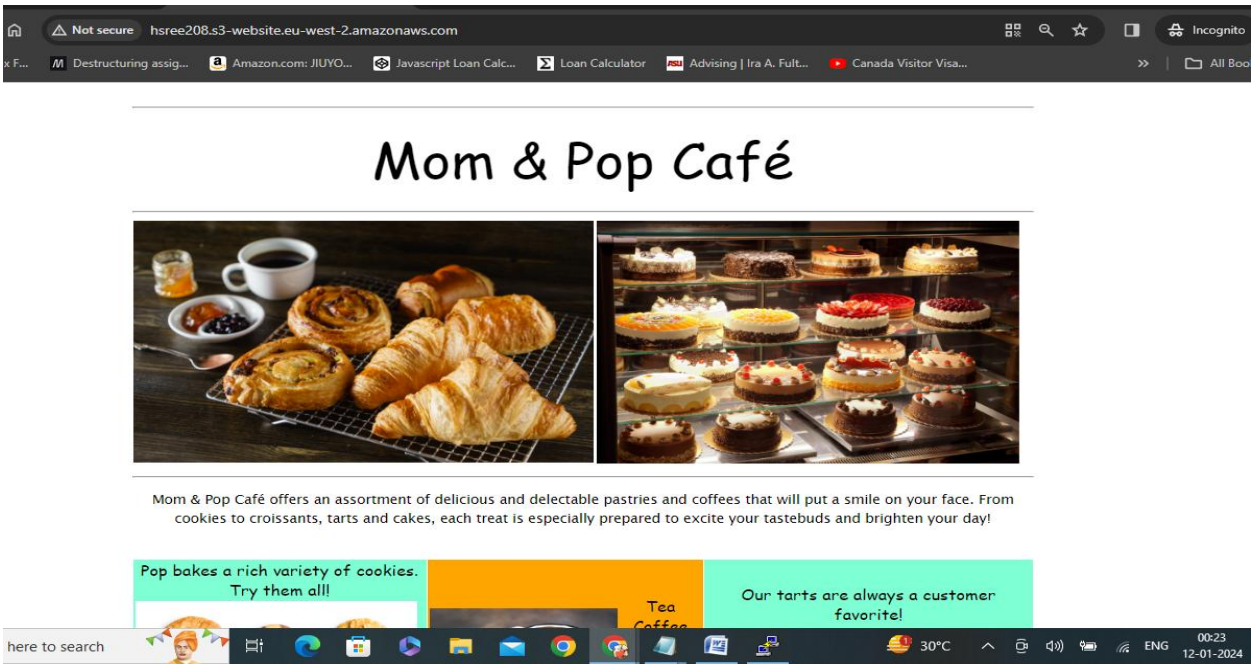
How to create a batch file to update the café website to change its colors

13. Launch a text editor, such as Notepad, and initiate a new file.
14. Navigate to the directory containing the website files.
15. Create the Batch File: In the text editor, generate a batch file with a .bat extension. For instance, name it update_colors.bat.
16. Modify the Batch File: Customize the batch file to incorporate commands for updating the CSS file. Below is an example of the batch file content:

    batch

    ```
    @echo off
    echo Updating website colors...
    set old_color=#ff0000
    set new_color=#00ff00
    set css_file=styles.css
    powershell -Command "(Get-Content %css_file%) -replace '%old_color%',
    '%new_color%' | Set-Content %css_file%"
    echo Colors updated successfully.
    ```

17. Save the batch file.
18. Execute the color update by either double-clicking the batch file or running it from the command prompt.



How to create a Lambda Layer and add it to a Lambda function

Create a Lambda Layer:

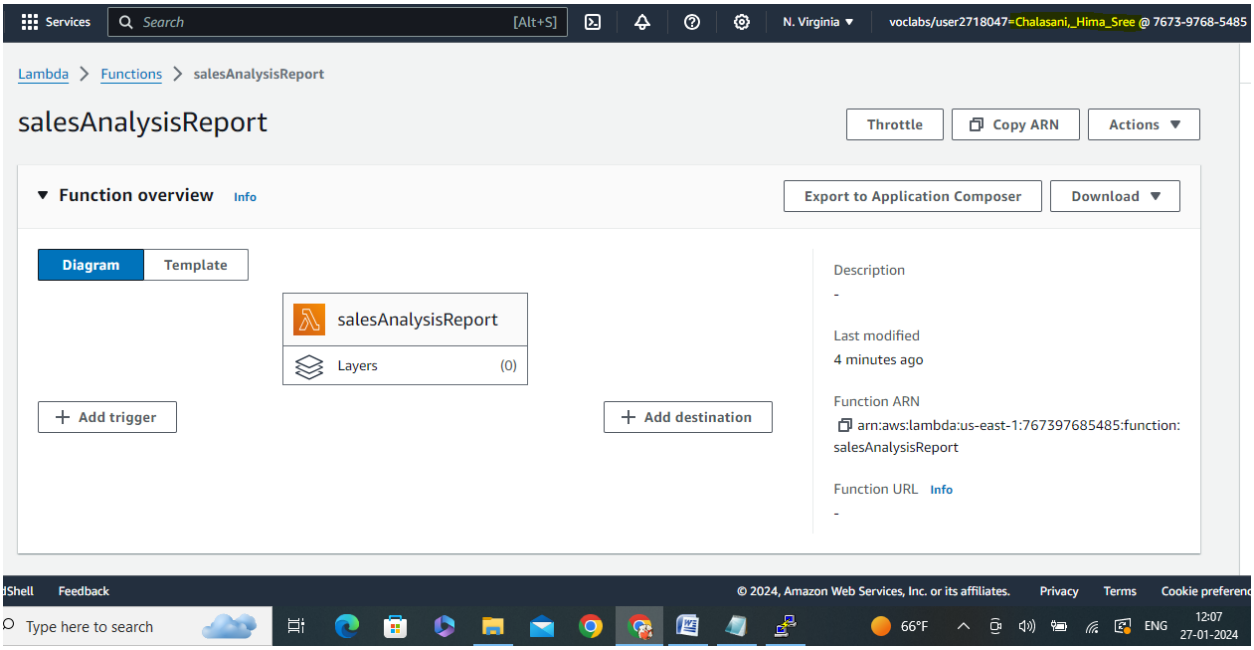
1. Prepare Layer Content: Arrange the content of the layer in a directory structure, such as: my_layer/ ├── python │ └── lib │ └── python3.8 │ └── site-packages └── my_custom_code.py
2. Package the Layer Content: Navigate to the directory containing the layer content and execute the following command to zip it:
   cd my_layer
   cd my_layer zip -r my_layer.zip
3. Document the Layer: Update the operations playbook with comprehensive information about the layer, including its purpose, dependencies, and any considerations regarding runtime compatibility.

Add the Layer to a Lambda Function:

6. Identify Target Function: Identify the Lambda function in the operations playbook where the layer will be incorporated.
7. Specify Layer Configuration: Document the specific details of adding the layer, including runtime compatibility and any versioning considerations.
8. Verify Lambda Configuration: Ensure that the Lambda function configuration in the playbook reflects the addition of the layer.
9. Document Changes: Update the operations playbook to incorporate details about the layer addition, such as the layer name, version, and a concise description.

Using the Layer in Lambda Function Code:

10. Code Integration: Document in the playbook how the Lambda function code should integrate with the layer, specifying any dependencies or modules to import from the layer.
11. Deployment Instructions: Offer clear instructions on deploying the updated Lambda function, emphasizing the importance of rigorous testing.
12. Testing Procedure: Document a step-by-step procedure for testing the Lambda function to ensure seamless access to the content of the layer.

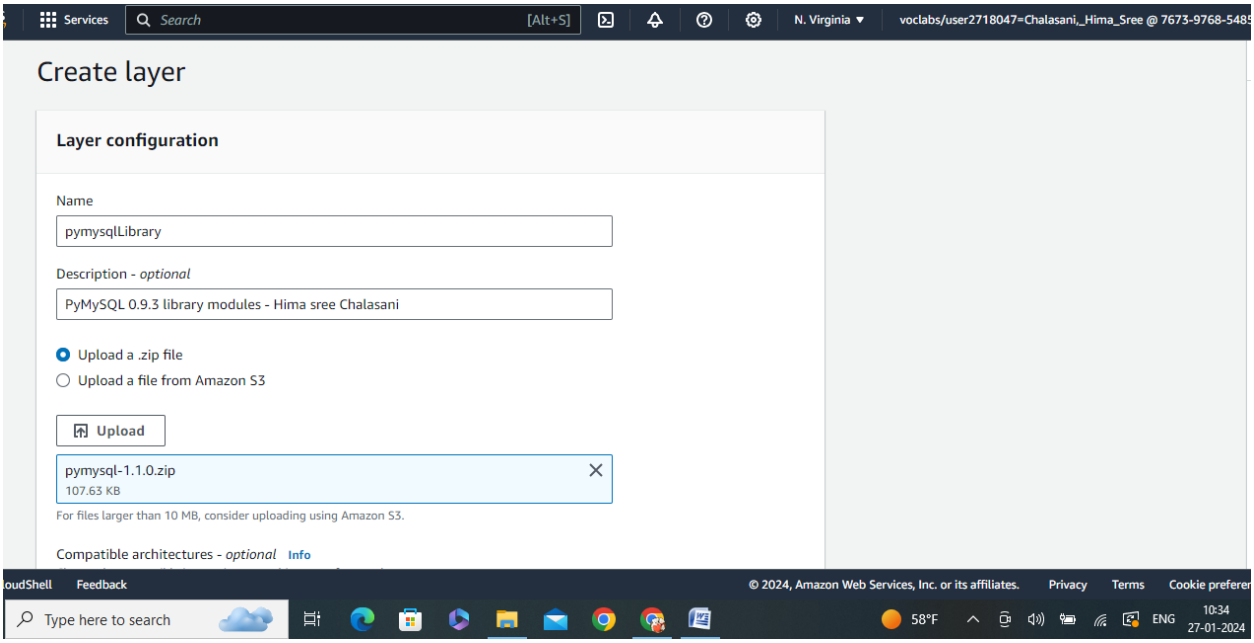


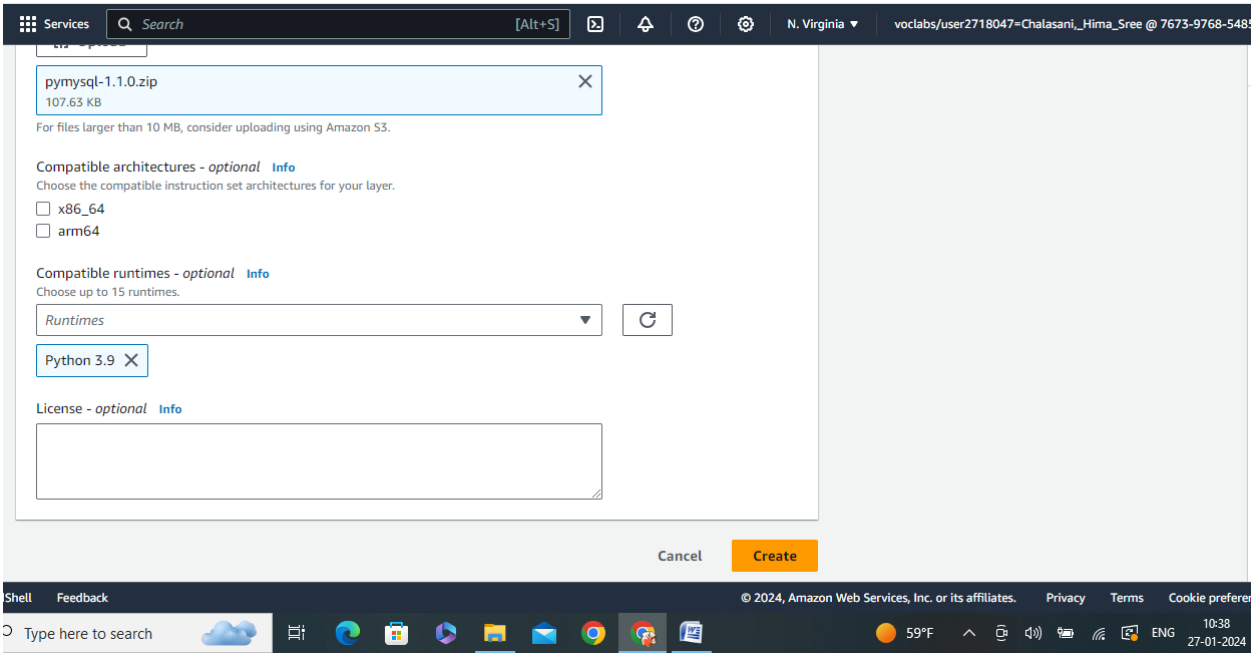
How to create a Lambda function from a prebuilt package

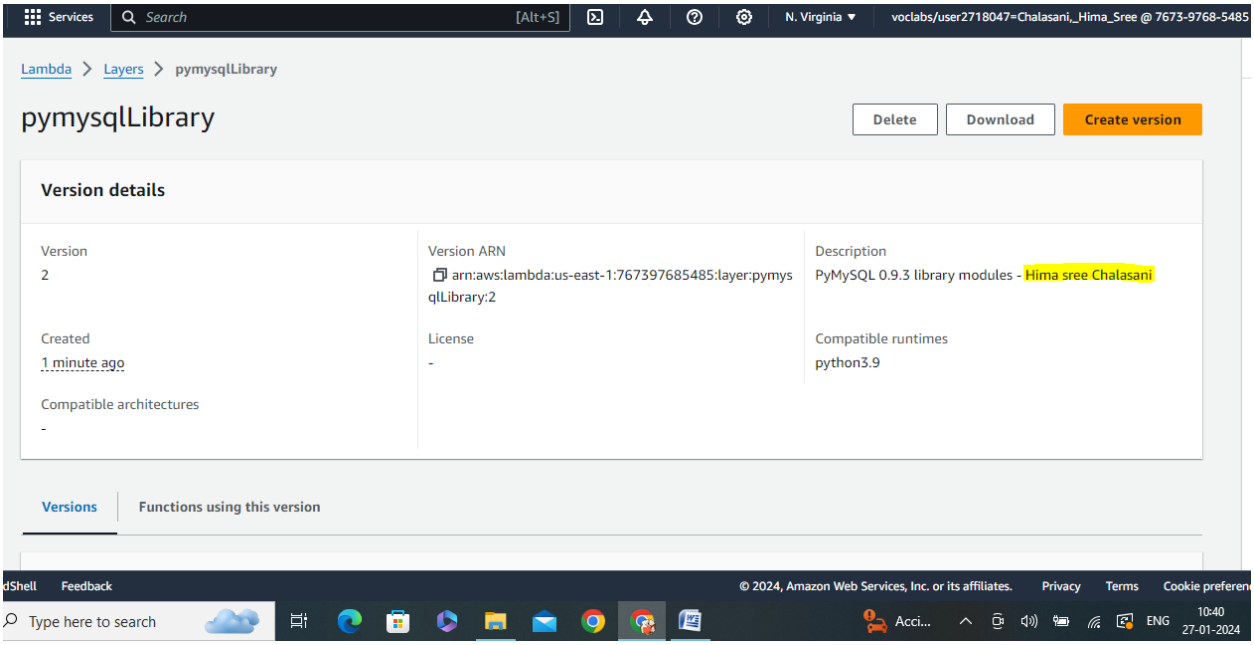
19. Open the Lambda Console.
20. Select "Create function."
21. Opt for "Author from scratch."
22. Provide a name for the function and choose the appropriate runtime compatible with the prebuilt package, such as Python, Node.js, or Java.
23. Choose an existing role containing the necessary permissions or create a new role.
24. Proceed by clicking "Create function."
25. Within the "Function code" section, select "Upload a .zip file" under "Code entry type."
26. Upload the prebuilt package ZIP file from the local machine by clicking "Upload."
27. If the handler information differs from the default, specify it accordingly.
28. Include environment variables as required by the function.
29. Modify other settings like timeout, memory allocation, and VPC configuration if necessary.

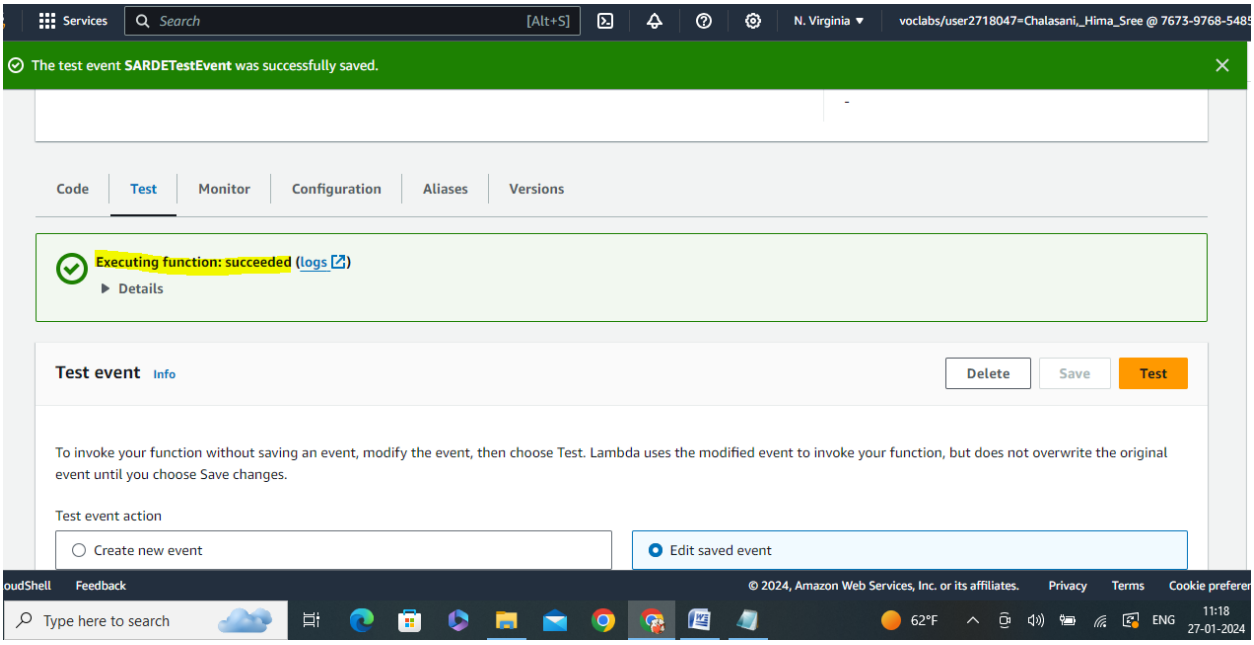
30. Save the function configuration by clicking "Save."
31. Deploy the function by clicking "Deploy"

After uploading the code and conducting testing.





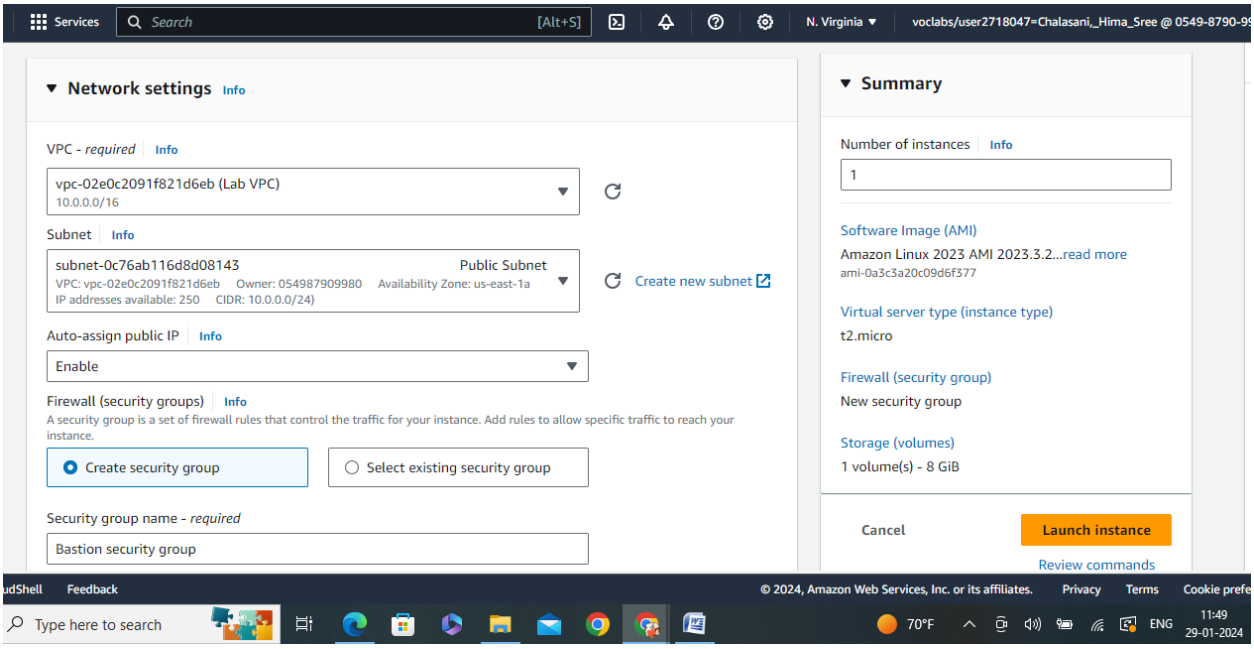


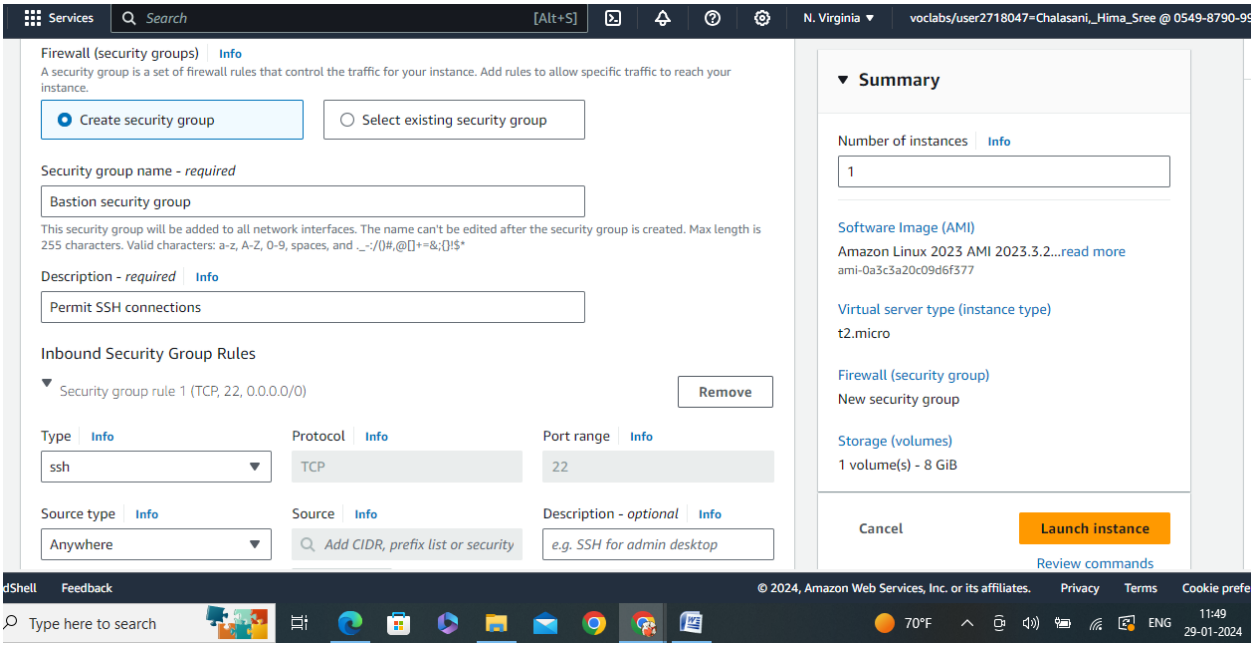


How to setup a VPC

1. Access the VPC service from the AWS Management Console.
2. Navigate to "VPCs" in the left sidebar and proceed to click on the "Create VPC" button.
3. Specify a name for the VPC and define its IPv4 CIDR block, for example, 10.0.0.0/16.
4. If necessary, enable DNS hostnames by selecting the corresponding option.
5. Go to "Subnets" in the left sidebar and click on "Create subnet."

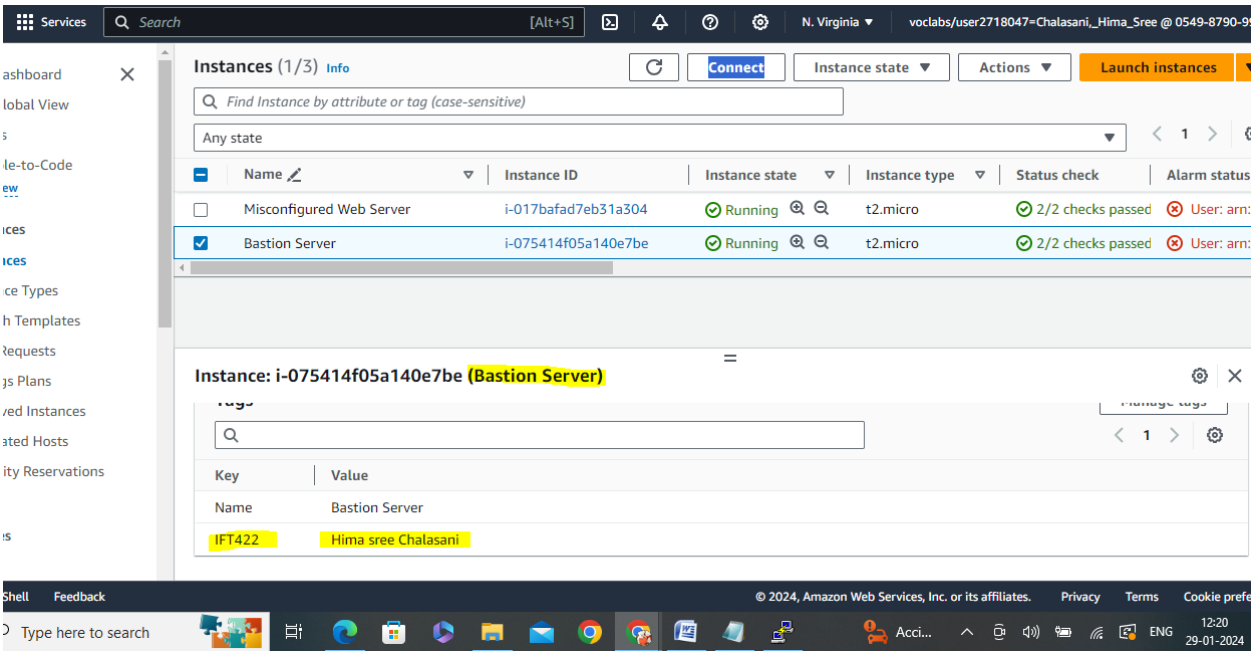
6. Associate the subnet with the VPC, assign a name, and specify its IPv4 CIDR block, such as 10.0.1.0/24.
7. Access "Internet Gateways" from the left sidebar.
8. Click on "Create internet gateway" and link it to the VPC.
9. Proceed to "Route Tables" in the left sidebar.
10. Choose the default route table and append a route for 0.0.0.0/0 directed to the internet gateway.
11. Access "Security Groups" from the left sidebar and establish security groups for instances.
12. Navigate to "Instances" in the left sidebar.
13. Launch instances into the public subnet and assign the designated security group.





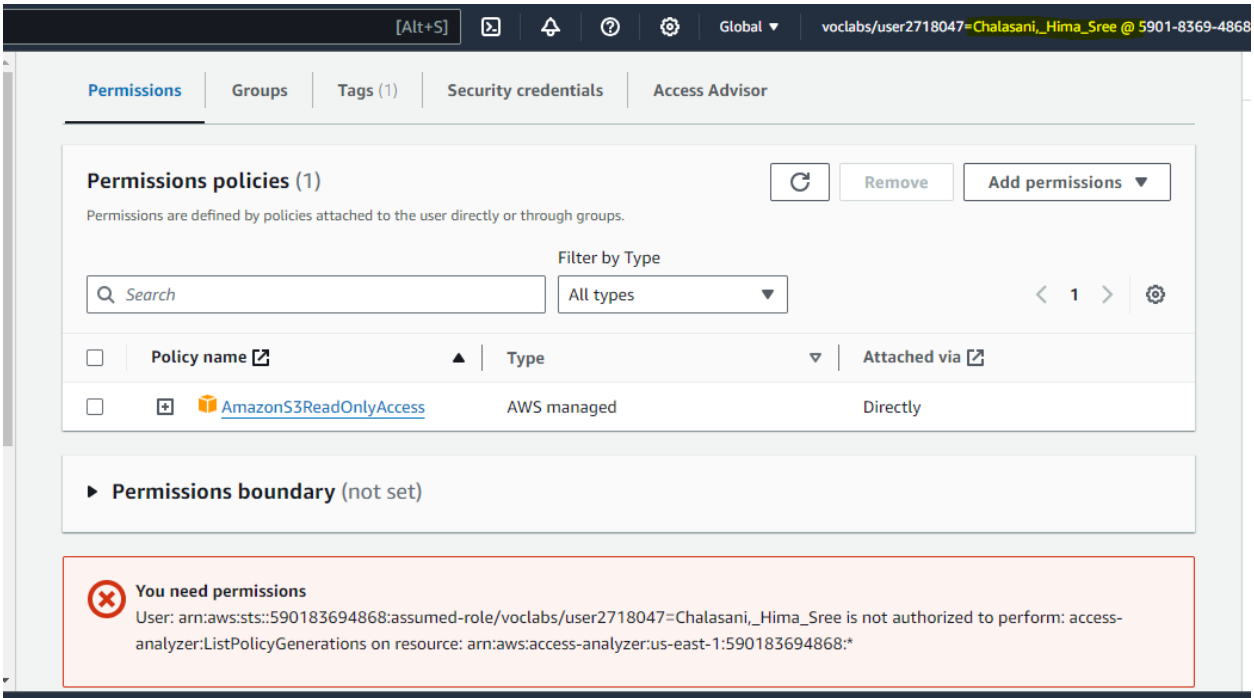
How to add a bastion host (Linux) to the public subnet of a VPC to connect to instances in the private subnet

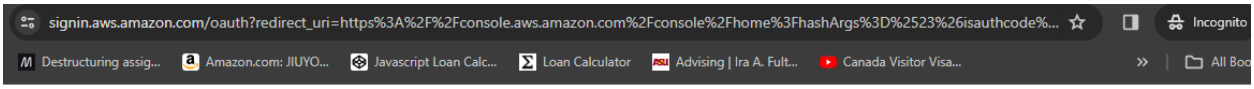
1. Initiate the launch of an EC2 instance within the public subnet.
2. Select an appropriate Amazon Machine Image (AMI) according to preference, such as Amazon Linux.
3. Configure the instance with a security group allowing inbound SSH (port 22) traffic from a specific IP address.
4. Enhance stability by considering the allocation of an Elastic IP to the bastion host, ensuring a consistent IP address.
5. Access the VPC dashboard and navigate to "Security Groups."
6. Establish a new security group dedicated to instances within the private subnet, permitting inbound SSH traffic solely from the bastion host.
7. Proceed to the VPC dashboard and locate "Route Tables."
8. Create a fresh route table tailored for the private subnet.
9. Associate the private subnet with the recently generated route table.
10. Integrate a route to the public subnet CIDR block via the bastion host.
11. Initiate the launch of instances within the private subnet.
12. Associate these instances with the security group established in step 6.



How to setup IAM so a user can assume an IAM role to access a resource

1. Access the IAM console, then select "Roles" from the left sidebar and proceed to click on "Create Role."
2. Opt for "Another AWS account" as the trusted entity type. Input the Account ID of the AWS account to which the user is associated.
3. Associate a policy with the role, providing the necessary permissions.
4. Within the "Trust relationships" tab, formulate a trust relationship policy permitting the IAM principal of the user to assume the role. For instance:
   Json {
   "Effect": "Allow",
   "Principal": {
   "AWS": "arn:aws:iam::user-account-id:root" },
   "Action": "sts:AssumeRole"
   }
5. Generate an IAM user account for the individual designated to assume the role.
6. Assign policies to the user, granting permissions to assume the role.
7. The IAM user can utilize either the AssumeRole API or the AWS Management Console to undertake the role.
8. If opting for the console, the user should navigate to the "Roles" section, select the designated role, and then click on "Switch Role."





aws

Sign in as IAM user

Account ID (12 digits) or account alias

590183694868

IAM user name

mediacouser

Password

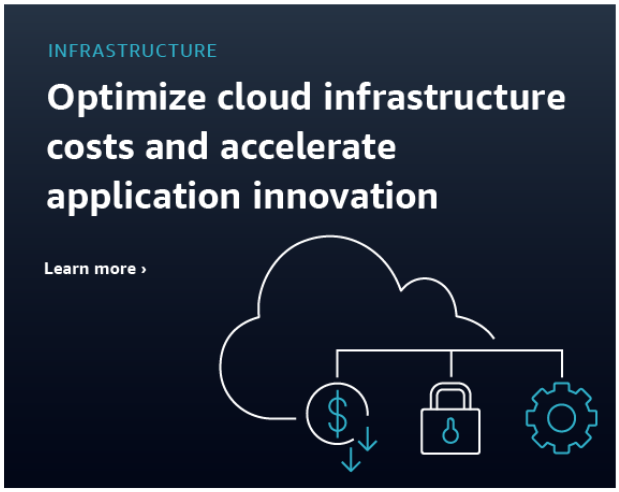
••••••••••

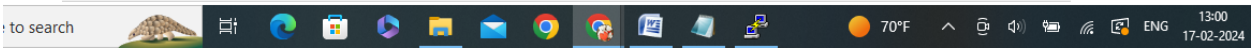
Remember this account

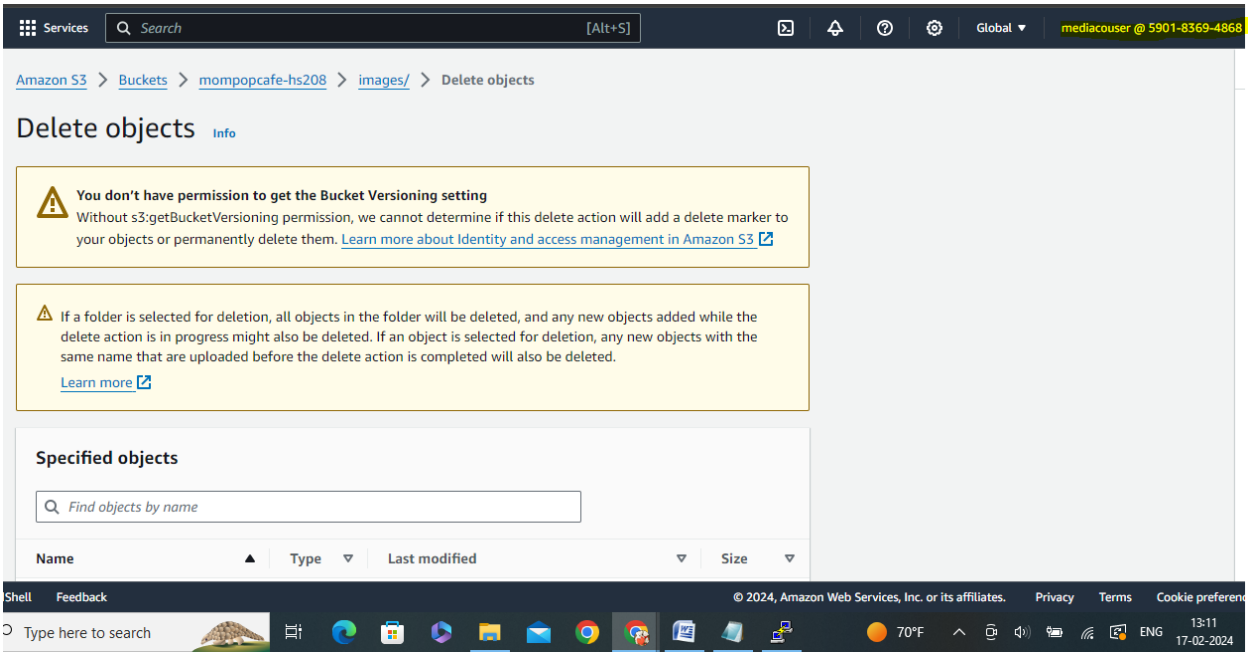
Sign in

Sign in using root user email

Forgot password?

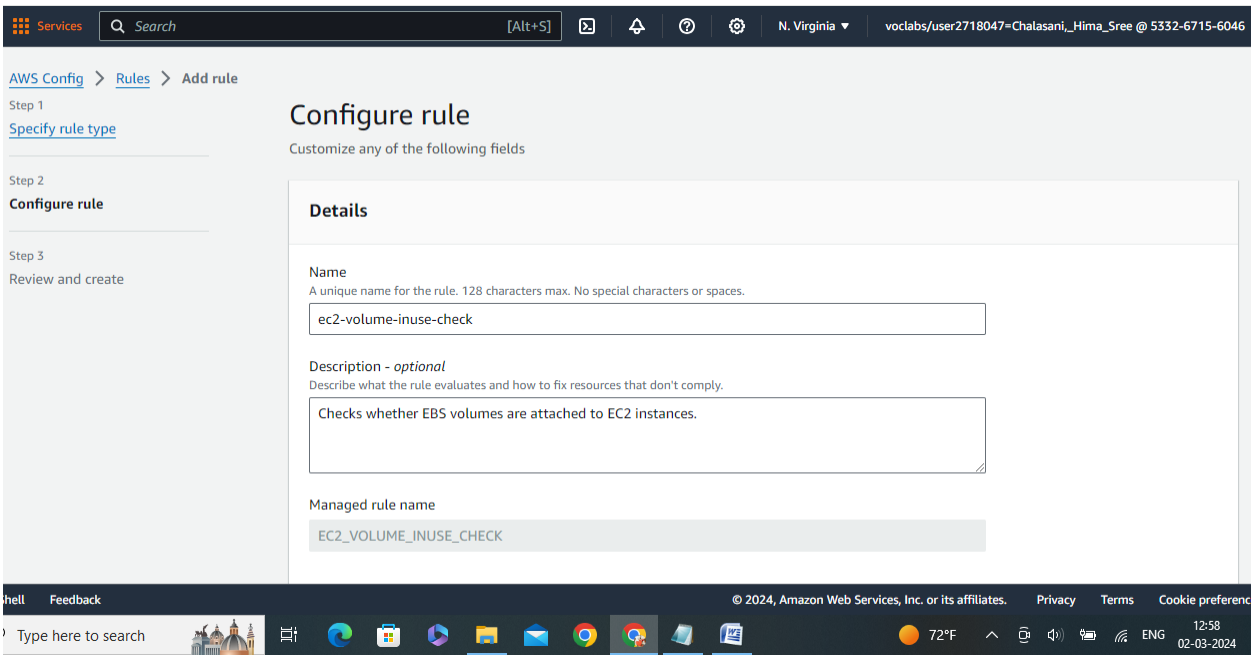


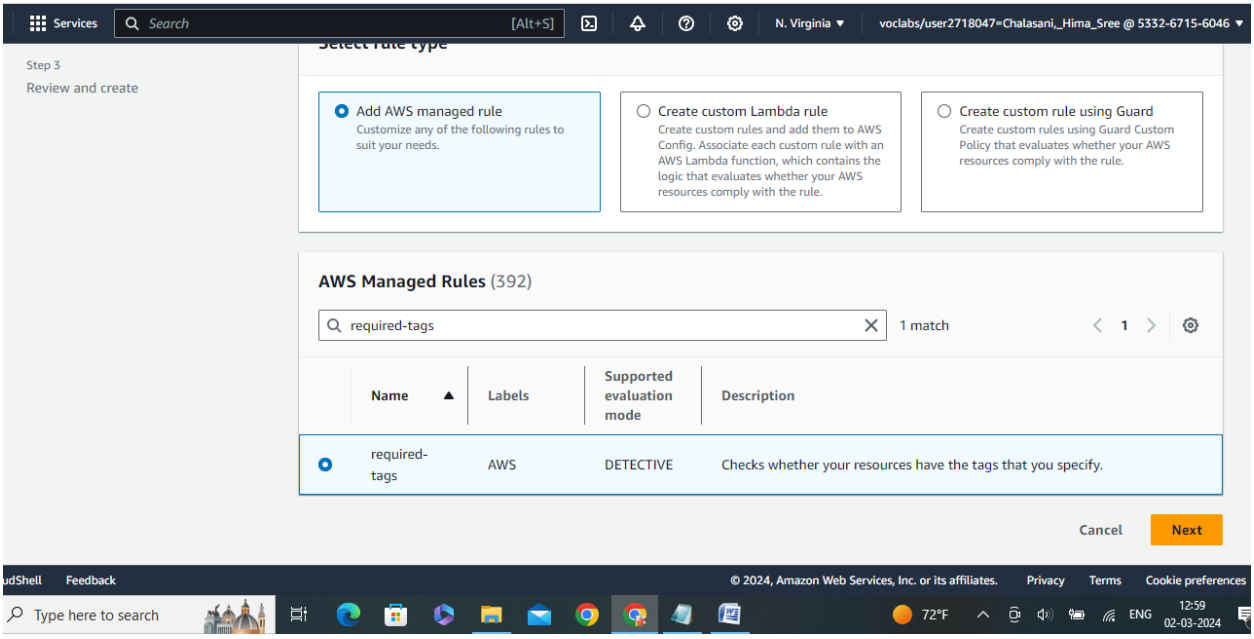


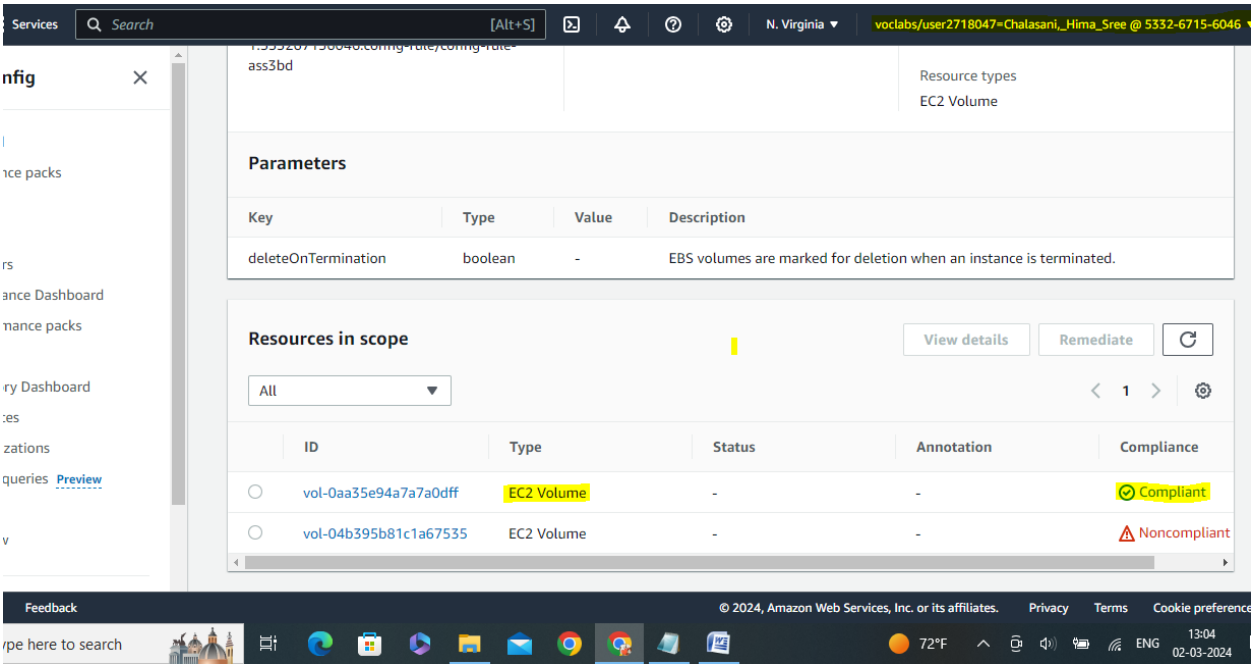


How to setup AWS Config to monitor resources

1. Sign in to the AWS Management Console and access the AWS Config service.
2. Select either "Get started" or "Set up AWS Config."
3. Specify the AWS resources to be monitored, such as All resources, and proceed by clicking "Next."
4. Choose the AWS Config rules to activate, whether AWS managed rules or custom rules, and adjust rule configurations as necessary.
5. Select an existing Amazon S3 bucket or create a new one to store AWS Config's configuration history. Configure bucket settings accordingly and proceed by clicking "Next."
6. Review the configured settings.
7. If all settings appear accurate, click "Confirm."
8. Proceed by clicking "Continue" to finalize the setup.
9. AWS Config will commence recording configuration alterations and evaluating rules.


Services
Search
[Alt+S]
N. Virginia
voclabs/user2718047=Chalasani,_Hima_Sree @ 5332-6715-6046
AWS Config
Rules
Add rule
Step 1
Specify rule type
Step 2
Configure rule
Step 3
Review and create
Configure rule
Customize any of the following fields
Details
Name
A unique name for the rule. 128 characters max. No special characters or spaces.
ec2-volume-inuse-check
Description - optional
Describe what the rule evaluates and how to fix resources that don't comply.
Checks whether EBS volumes are attached to EC2 instances.
Managed rule name
EC2_VOLUME_INUSE_CHECK
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferenc
Type here to search
72°F
ENG
12:58
02-03-2024

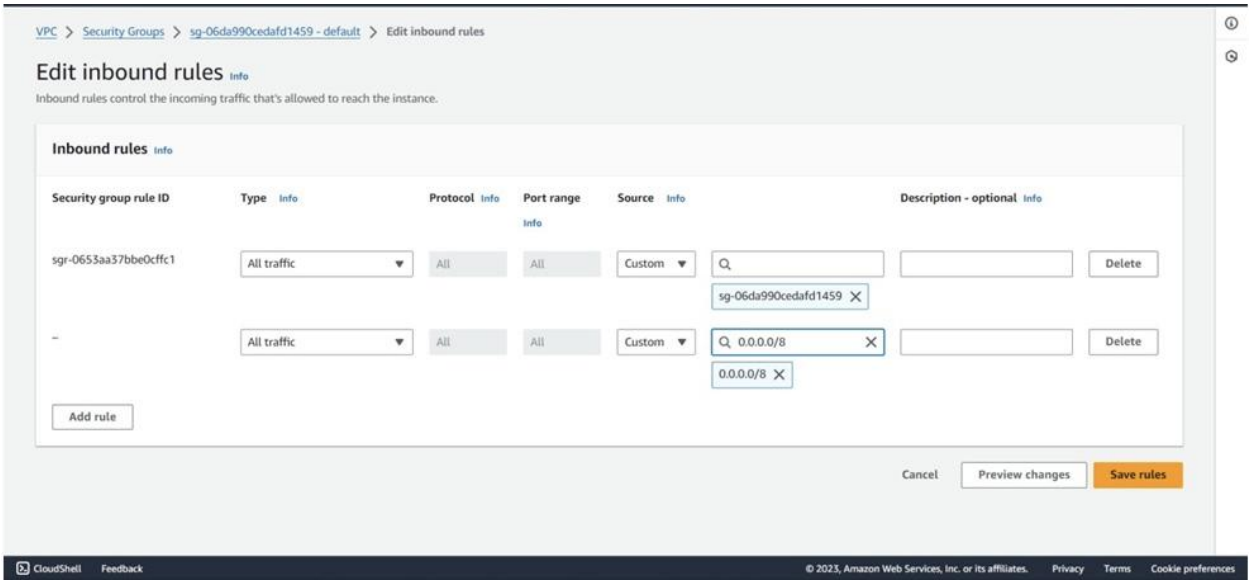

Services
Search
[Alt+S]
N. Virginia
voclabs/user2718047=Chalasani,_Hima_Sree @ 5332-6715-6046
Step 3
Review and create
Add AWS managed rule
Customize any of the following rules to suit your needs.
Create custom Lambda rule
Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.
Create custom rule using Guard
Create custom rules using Guard Custom Policy that evaluates whether your AWS resources comply with the rule.
AWS Managed Rules (392)
required-tags
1 match
Name
Labels
Supported evaluation mode
Description
required-tags
AWS
DETECTIVE
Checks whether your resources have the tags that you specify.
Cancel
Next
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
72°F
ENG
12:59
02-03-2024



How to add inbound rules to both security groups and network ACLs

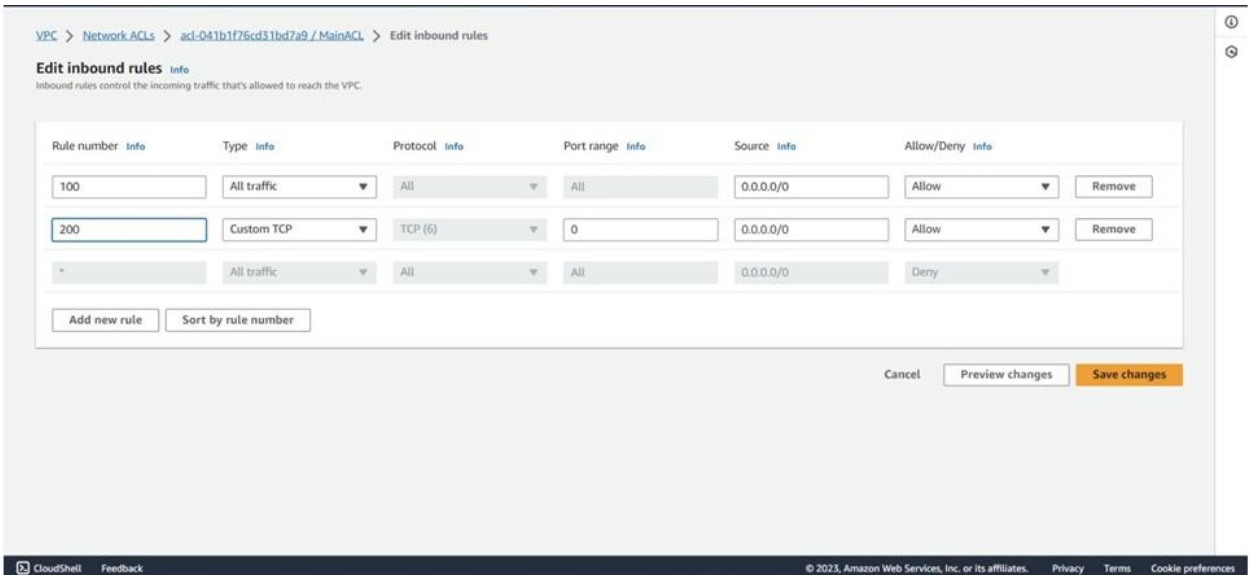
Adding Inbound Rules to Security Groups:

1. Access the EC2 Dashboard.
2. Navigate to "Security Groups" under "Network & Security" in the left sidebar.
3. Select the security group linked with the EC2 instances requiring adjustments.
4. Within the "Inbound rules" tab, click on "Edit inbound rules."
5. Specify rules for the desired protocol, port range, and source IP or security group.
6. Confirm the changes by clicking "Save rules."



Adding Inbound Rules to Network ACLs:

1. Go to the VPC Dashboard.
2. Click on "Network ACLs" under "Security" in the left sidebar.
3. Choose the network ACL associated with the subnet containing the targeted EC2 instances.
4. Click "Edit inbound rules" in the "Inbound Rules" tab.
5. Define rules for the desired protocol, port range, and source IP or CIDR range.
6. As Network ACLs use rule numbers for sequencing, ensure correct ordering of rules.
7. Apply the modifications by clicking "Save rules."

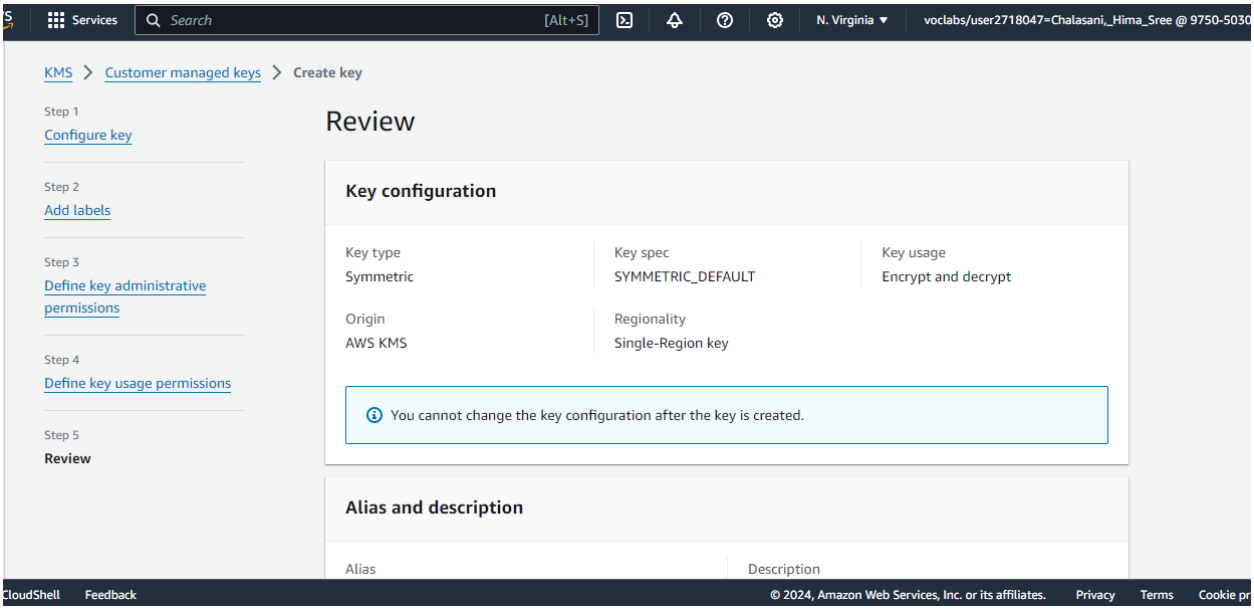


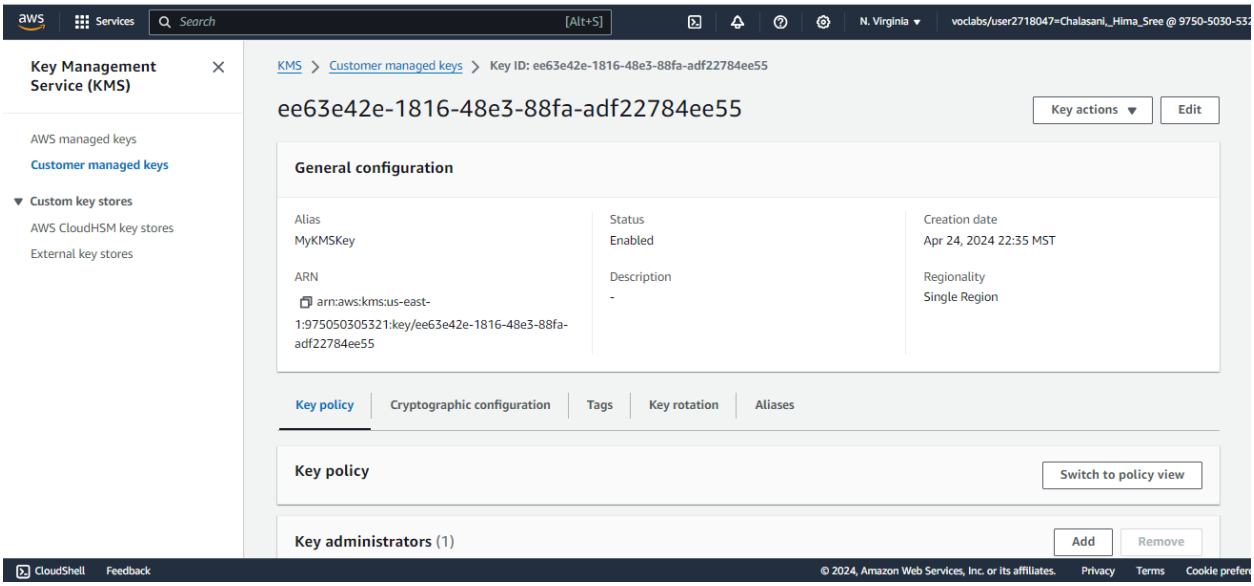
How to encrypt the root volume of an existing EC2 instance

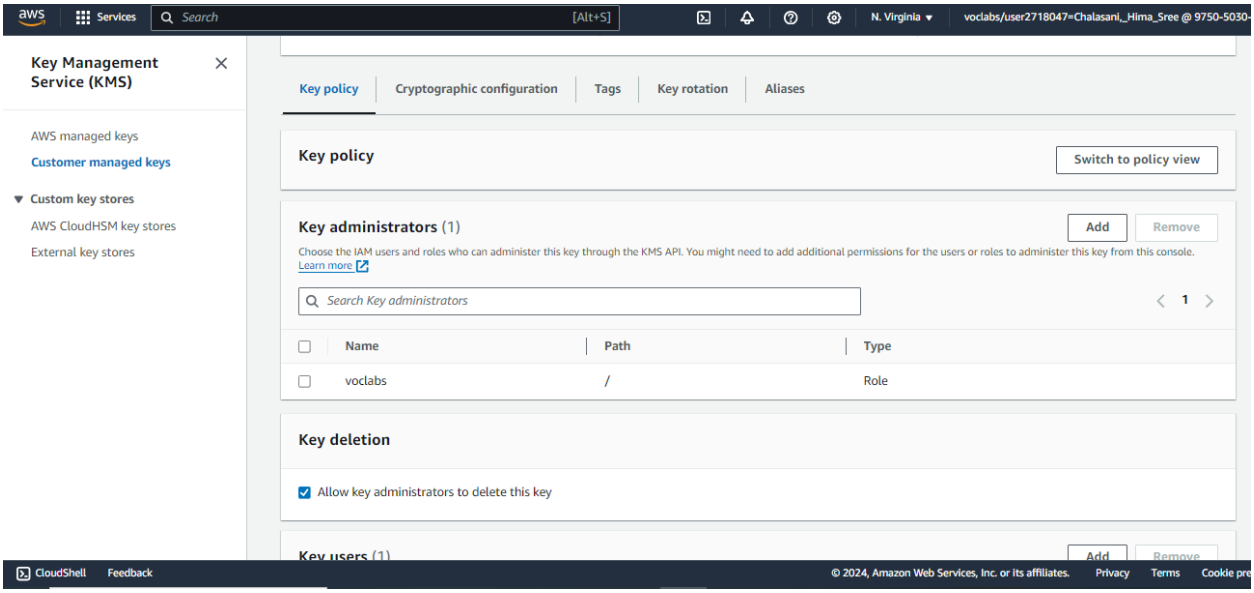
10. Navigate to the EC2 section within the AWS Management Console and access the instances.
11. Choose the desired instance, such as "LabInstance," and verify whether the storage tab indicates encryption status.
12. Halt the instance to enable snapshot creation by accessing the instance details and changing its status to "stopped."
13. Take note of the volume ID and availability zone of the unencrypted EBS volume by inspecting the storage tab and capturing a screenshot.
14. Click on the action button and select "Create Snapshot." Provide the necessary key and value pairs, such as a name for the snapshot and indication of it being from an unencrypted volume, then proceed with the snapshot creation.
15. Within the Elastic Block Store, navigate to the snapshot section. Locate the previously generated unencrypted volume snapshot, choose to create a volume from it, and configure the settings as follows:

- Set the Availability Zone to us-east-1.
- Select the MyKMSKey key for encryption.
- Click on "Create Volume."

16. Establish a customer-managed key by selecting "Customer Managed Key," initiate the creation of a new key, choose "Standard" for key usage, enable encryption and decryption capabilities, and assign a name to the key (e.g., MyKMSKey). Proceed through the default settings, review all configurations, and finalize the key creation process by clicking "Create."

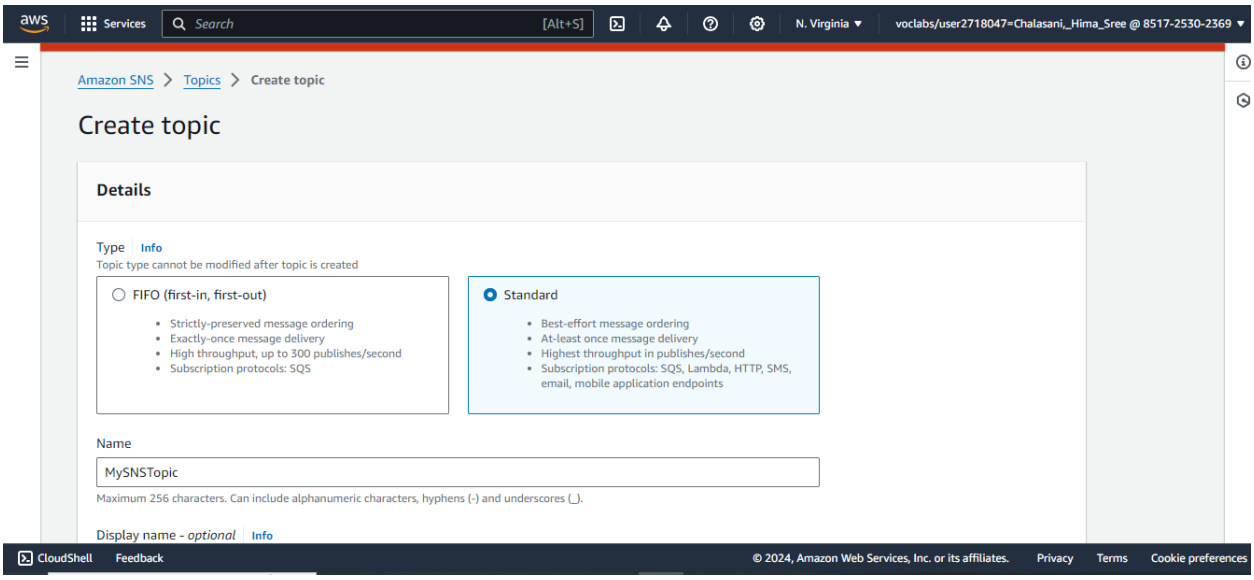


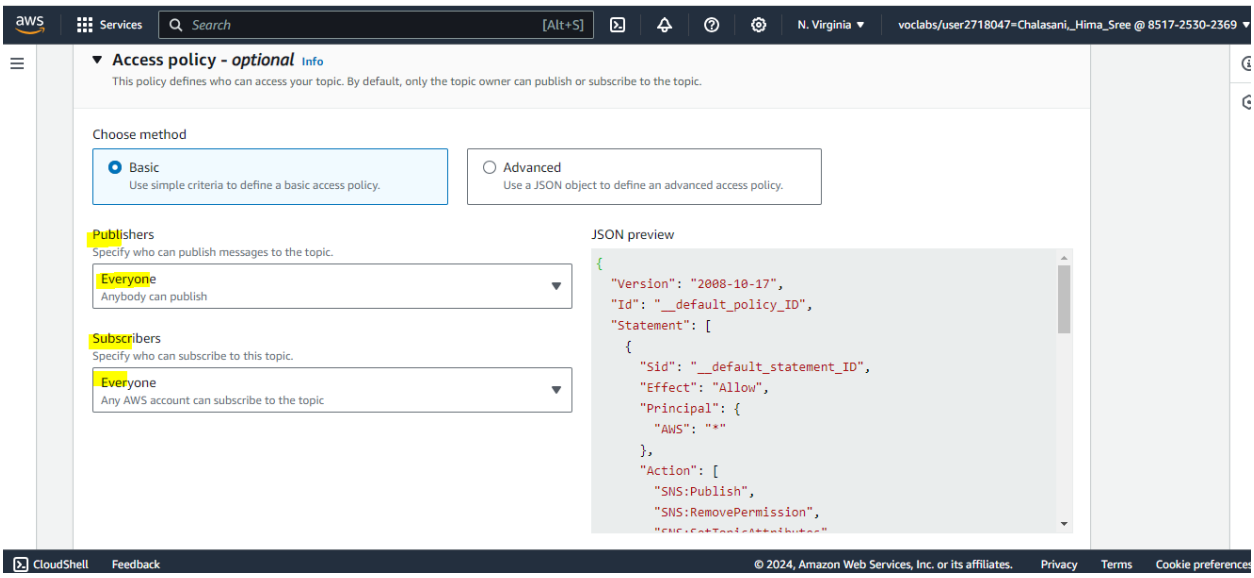


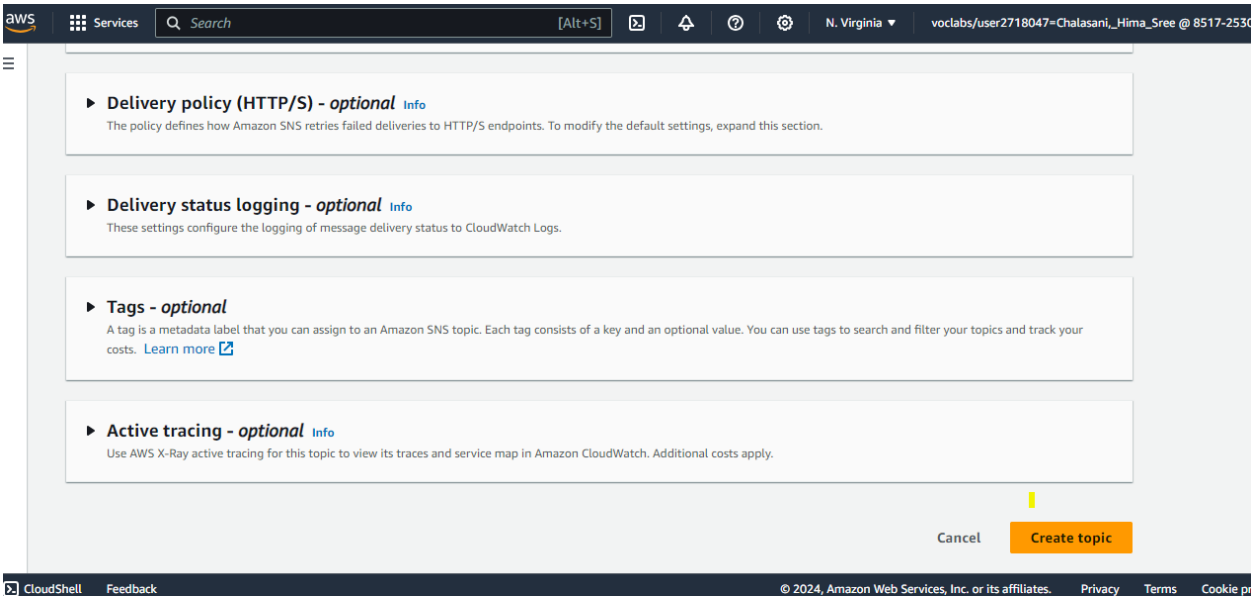


How to create a SNS topic

1. Utilize the AWS services search bar to locate and select "Simple Notification Service" (SNS).
2. Navigate to the SNS dashboard and access the "Topics" section from the left sidebar. Proceed to click on the "Create topic" button.
3. Input a name for the topic and optionally include a display name if desired.
4. Complete the topic creation process by clicking on "Create topic."
5. Upon successful creation, the newly formed topic will be displayed in the list. Click on the recently generated topic.
6. On the Topic Details page, the Amazon Resource Name (ARN) can be copied for future reference.



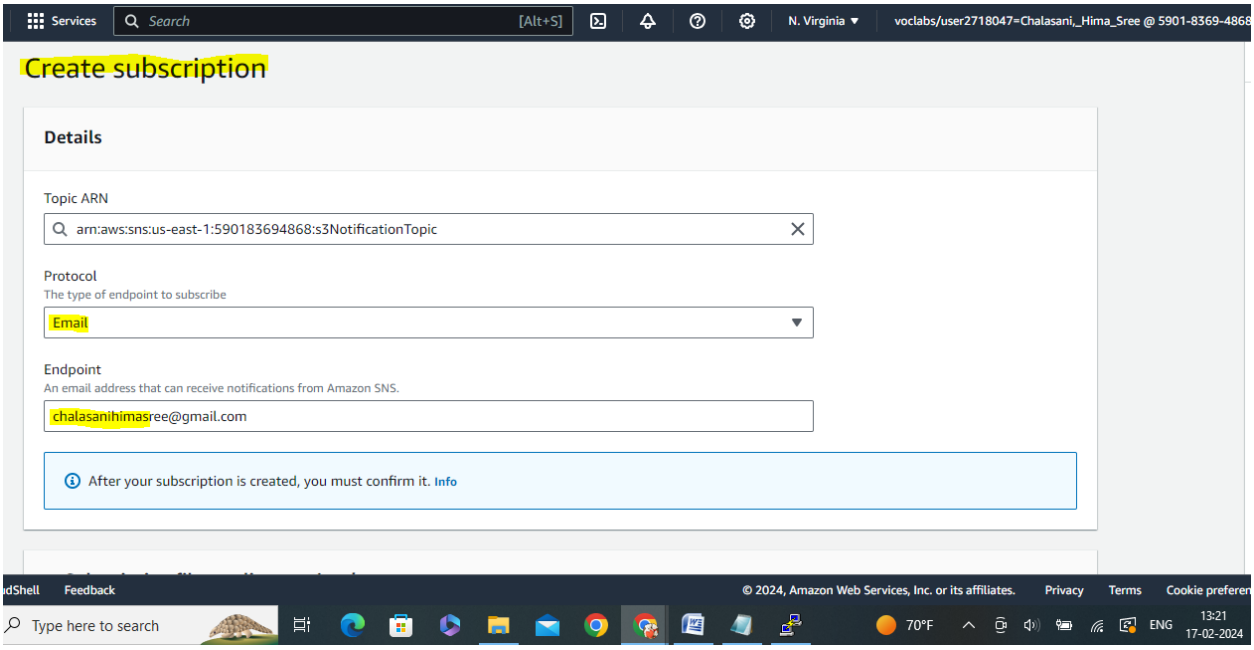


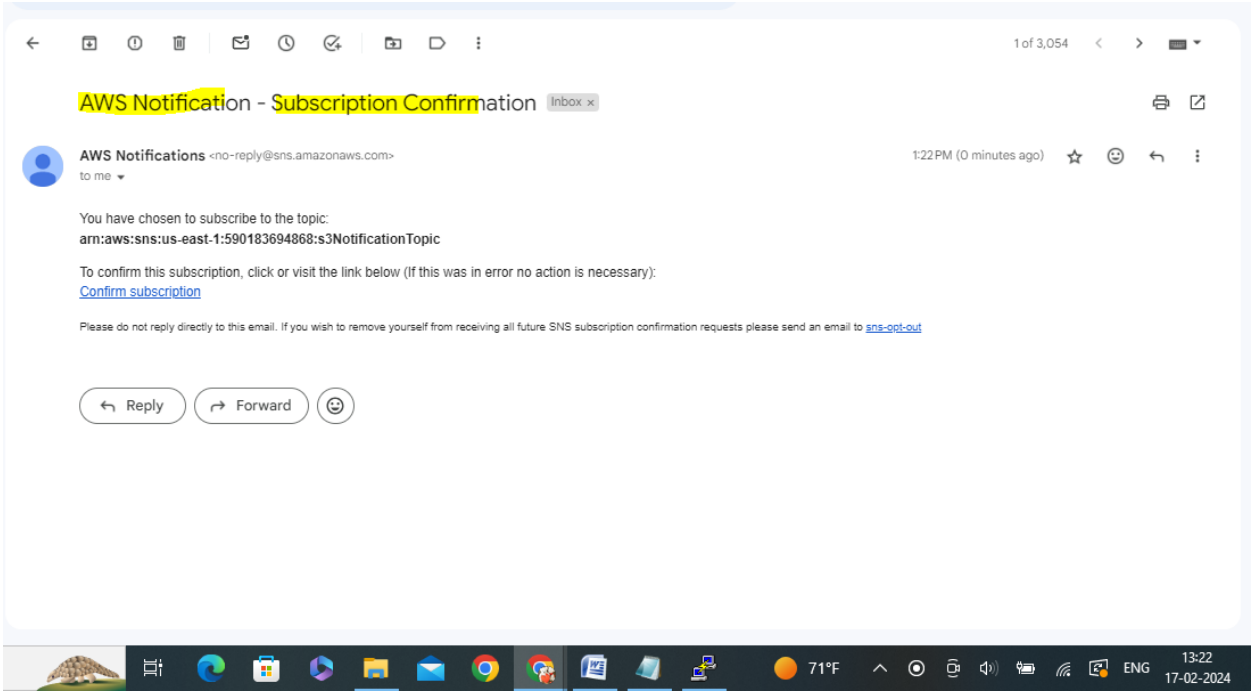


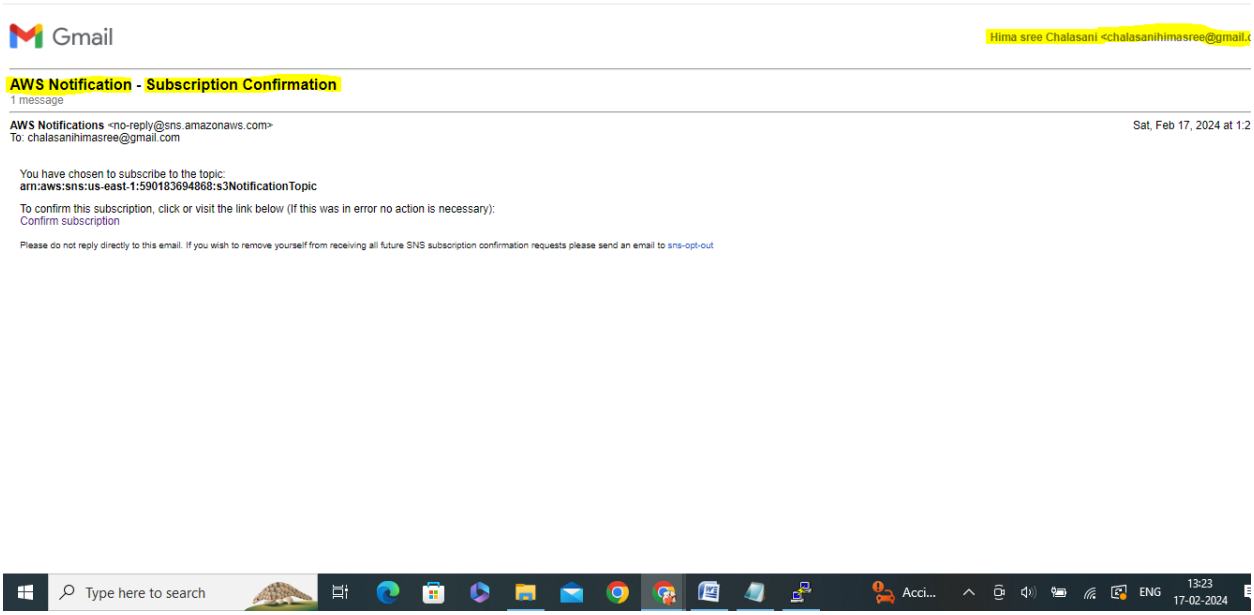
How to subscribe to a SNS topic

17. Navigate to the AWS services search bar and input "SNS" to locate and select "Simple Notification Service."
18. Access the SNS dashboard and proceed to click on "Topics" situated in the left sidebar.
19. Select the specific topic to which subscription is desired.
20. Within the Topic Details page, initiate the subscription process by clicking on the "Create subscription" button.
21. Choose the preferred protocol for message delivery, such as email, HTTP, or HTTPS.
22. Provide the requisite information corresponding to the selected protocol, such as an email address or endpoint URL.
23. Finalize the subscription creation by clicking on "Create subscription."

24. Depending on the chosen protocol, it might be necessary to confirm the subscription, which may involve actions like clicking a confirmation link sent via email.

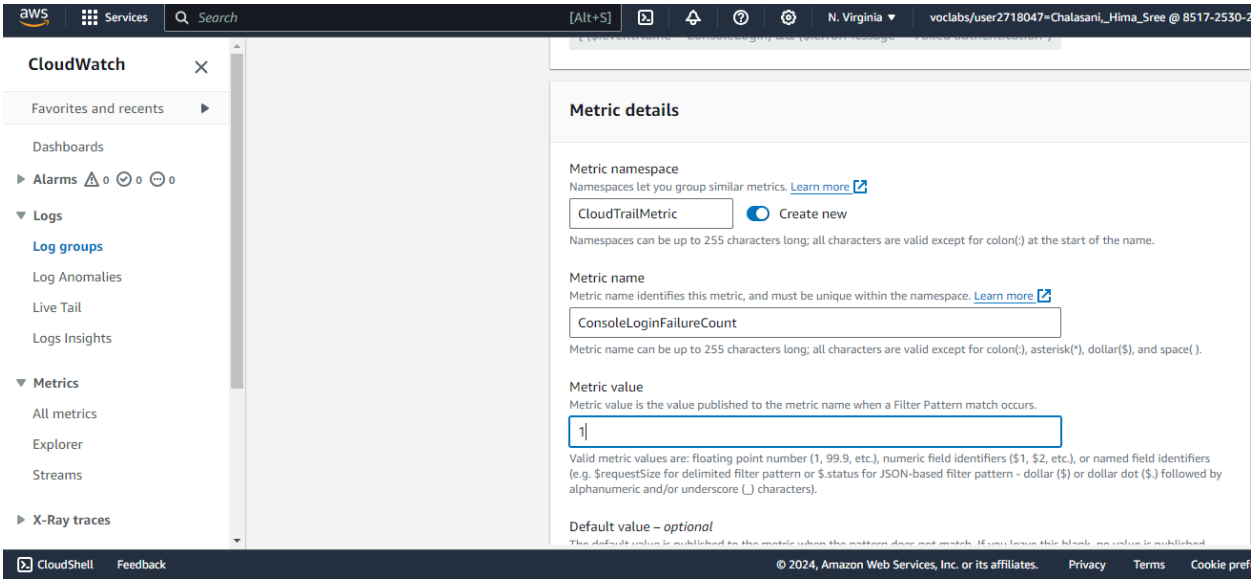


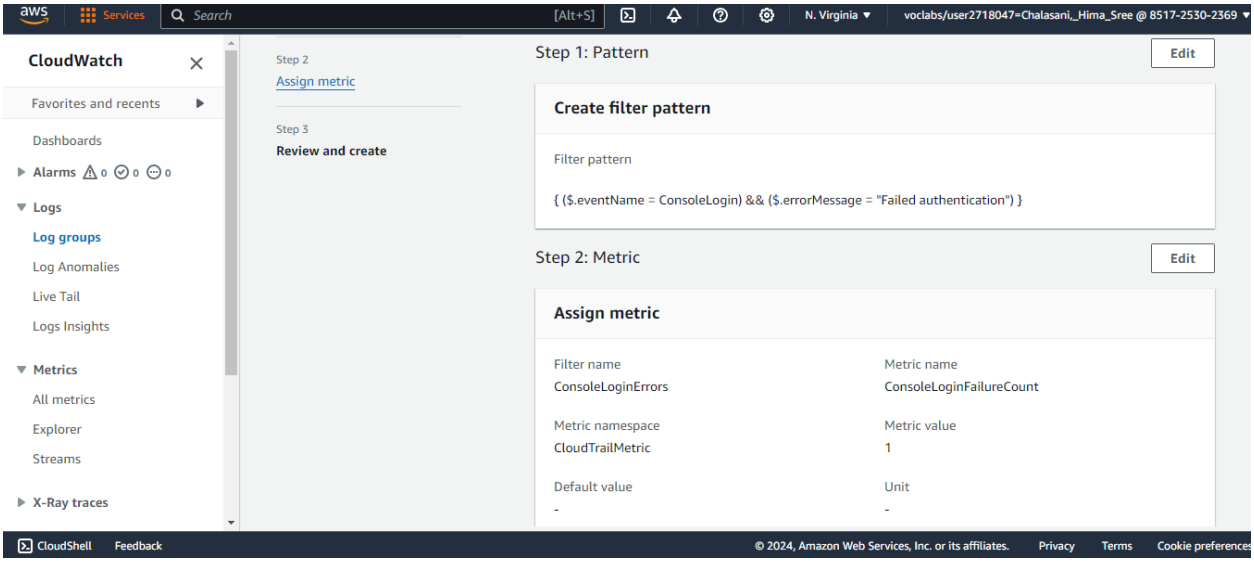


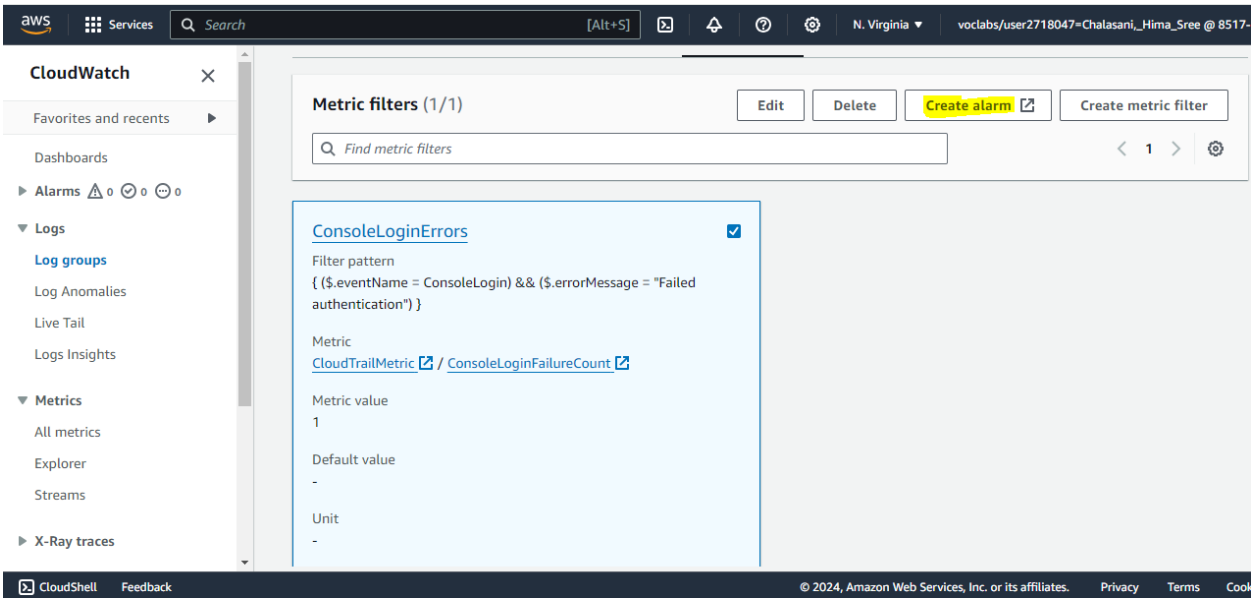


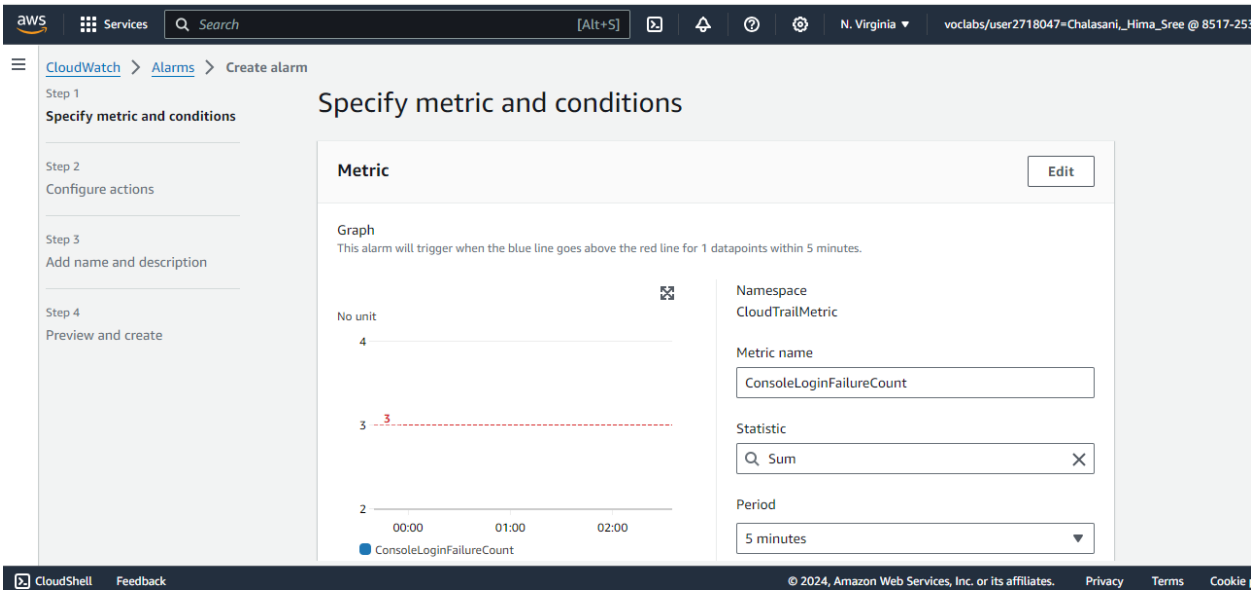
How to create a CloudWatch alarm using a metrics-based filter

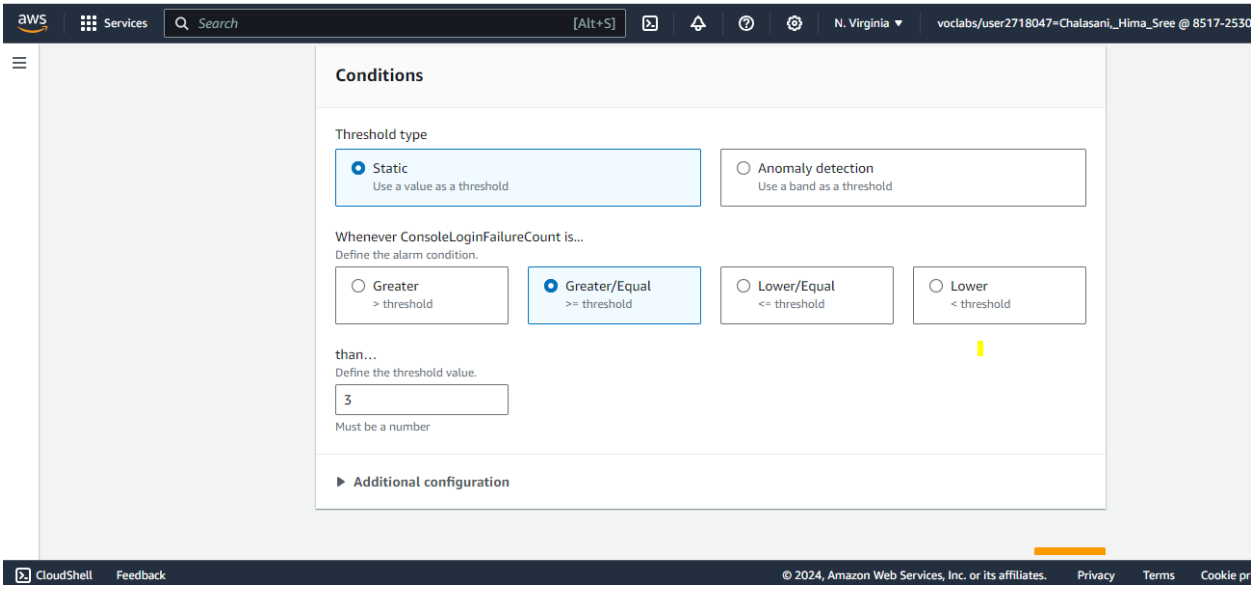
1. Utilize the AWS services search bar to input "CloudWatch" and then proceed to select "CloudWatch" from the results.
2. Navigate to the CloudWatch dashboard and access the "Logs" section located in the left sidebar.
3. Choose the specific log group for which a metric filter needs to be established.
4. Initiate the creation of a Metric Filter by clicking on the corresponding button.
5. Craft a filter pattern tailored to match the desired log events.
6. Name the filter and finalize its creation by selecting "Create Filter."
7. Return to the CloudWatch dashboard and access the "Alarms" section from the left sidebar.
8. Begin the alarm creation process by clicking on "Create Alarm."
9. Select the metric linked with the previously established filter.
10. Define the conditions for triggering the alarm, such as setting threshold values.
11. Configure the actions to be executed upon the alarm state activation.
12. Provide a distinctive name and description for the alarm.
13. Complete the alarm creation process by clicking on "Create Alarm."


Services
Search
[Alt+S]
N. Virginia
CloudWatch
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Metrics
All metrics
Explorer
Streams
X-Ray traces
Metric details
Metric namespace
Namespaces let you group similar metrics. Learn more
CloudTrailMetric
Create new
Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.
Metric name
Metric name identifies this metric, and must be unique within the namespace. Learn more
ConsoleLoginFailureCount
Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(*), dollar($), and space( ).
Metric value
Metric value is the value published to the metric name when a Filter Pattern match occurs.
1
Valid metric values are: floating point number (1, 99.9, etc.), numeric field identifiers ($1, $2, etc.), or named field identifiers (e.g. $requestSize for delimited filter pattern or $.status for JSON-based filter pattern - dollar ($) or dollar dot ($.) followed by alphanumeric and/or underscore (_) characters).
Default value – optional
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms


Services
Search
[Alt+S]
N. Virginia
CloudWatch
Step 2
Assign metric
Step 3
Review and create
Step 1: Pattern
Edit
Create filter pattern
Filter pattern
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
Step 2: Metric
Edit
Assign metric
Filter name
ConsoleLoginErrors
Metric name
ConsoleLoginFailureCount
Metric namespace
CloudTrailMetric
Metric value
1
Default value
-
Unit
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2718047=Chalasani,_Hima_Sree @ 8517-
CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 0
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Metrics
All metrics
Explorer
Streams
X-Ray traces
Metric filters (1/1)
Edit
Delete
Create alarm
Create metric filter
Find metric filters
1
ConsoleLoginErrors
Filter pattern
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
Metric
CloudTrailMetric / ConsoleLoginFailureCount
Metric value
1
Default value
-
Unit
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2718047=Chalasani,_Hima_Sree @ 8517-253
CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Specify metric and conditions
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.
No unit
4
3
2
00:00
01:00
02:00
ConsoleLoginFailureCount
Namespace
CloudTrailMetric
Metric name
ConsoleLoginFailureCount
Statistic
Sum
Period
5 minutes
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user2718047=Chalasani,_Hima_Sree @ 8517-2530
Conditions
Threshold type
Static
Use a value as a threshold
Anomaly detection
Use a band as a threshold
Whenever ConsoleLoginFailureCount is...
Define the alarm condition.
Greater
> threshold
Greater/Equal
>= threshold
Lower/Equal
<= threshold
Lower
< threshold
than...
Define the threshold value.
3
Must be a number
Additional configuration
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie pr