

Module-8 Case Study

Module-8 Case Study

Problem Statement:

You work for XYZ Corporation and they are using AWS for their infrastructure. For administrative purposes, they need to provide access of certain tasks to certain employees.

You have been asked:

1. a) Create a user account that can login to the console
b) Create a group and make sure that the group can only launch and stop EC2 instances using that previously created account
2. a) Provide permission to let the user of previously created account to create VPCs, Subnets, NACL and security Groups.
b) Further add the permission so that the user can create RDS instance
c) Explore security options to protect the AWS resources and secure the permissions provided to the group

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type* ☐ Access key - Programmatic access
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ Password - AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ☒ Autogenerated password
☐ Custom password

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

* Required

[Cancel](#) [Next: Permissions](#)

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

18:52 10-03-2022

Inbox (1,754) - sakharevishal99@xIAM Management ConsolexStart Course - Intellipaatx+

us-east-1.console.aws.amazon.com/iam/home#/users\$new?step=permissions&login&userNames=IAM-user-1&passwordReset&passwordType=autogen

awsServices

Search for services, features, blogs, docs, and more

[Alt+S]

GlobalVishal Sakhare

Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Get started with groups
You haven't created any groups yet. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. Get started by creating a group. [Learn more](#)

Create group

Set permissions boundary

Set a permissions boundary to control the maximum permissions this user can have. This is an advanced feature used to delegate permission management to others. [Learn more](#)

☒

 Create user without a permissions boundary

☐

 Use a permissions boundary to control the maximum user permissions

Cancel

Previous

Next: Tags

FeedbackEnglish (US)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. PrivacyTermsCookie preferences

Type here to search

ENG18:5210-03-2022

Inbox (1,754) - sakharevishal99@xIAM Management ConsolexStart Course - Intellipaatx+

us-east-1.console.aws.amazon.com/iam/home#/users\$new?step=permissions&login&userNames=IAM-user-1&passwordReset&passwordType=autogen

awsServices

Search for services, features, blogs, docs, and more

[Alt+S]

GlobalVishal Sakhare

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions. [Learn more](#)

Group name

group-for-ec2

Create policy

Refresh

Filter policies

ec2

Showing 25 results

	Policy name	Type	Used as	Description
<input type="checkbox"/>	AmazonEC2ContainerS...	AWS managed	None	Policy to enable Task Autoscaling for Amazon EC2 Contain...
<input type="checkbox"/>	AmazonEC2ContainerS...	AWS managed	None	Policy to enable CloudWatch Events for EC2 Container Ser...
<input type="checkbox"/>	AmazonEC2ContainerS...	AWS managed	None	Default policy for the Amazon EC2 Role for Amazon EC2 C...
<input type="checkbox"/>	AmazonEC2ContainerS...	AWS managed	None	Default policy for Amazon ECS service role.
<input checked="" type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Permissions policy (2)	Provides full access to Amazon EC2 via the AWS Manage...
<input type="checkbox"/>	AmazonEC2ReadOnlyA...	AWS managed	None	Provides read-only access to Amazon EC2 via the AWS Ma...

Cancel

Create group

FeedbackEnglish (US)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. PrivacyTermsCookie preferences

Type here to search

ENG18:5310-03-2022

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Other permission policies (Selected 1/736) Info

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter policies by property or policy name and press enter 7 matches < 1 > ⚙

"VPC" X Clear filters

	Policy name	Type	Description
<input type="checkbox"/>	AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to VPC resources
<input type="checkbox"/>	AmazonVPCCrossAccountNetworkInterfaceOperations	AWS managed	Provides access to cross-account network interface operations
<input checked="" type="checkbox"/>	AmazonVPCFullAccess	AWS managed	Provides full access to VPC resources
<input type="checkbox"/>	AmazonDMSVPCManagementRole	AWS managed	Provides access to Amazon DMS VPC resources
<input type="checkbox"/>	AmazonDRSVPCManagement	AWS managed	Provides access to Amazon DR VPC resources
<input type="checkbox"/>	AWSLambdaVPCAccessExecutionRole	AWS managed	Provides minimum permissions for Lambda to access VPC resources
<input type="checkbox"/>	AmazonEKSVPCResourceController	AWS managed	Policy used by VPC resources to manage Amazon EKS resources

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

Add user

1 2 3 4 5

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://821782153972.signin.aws.amazon.com/console>

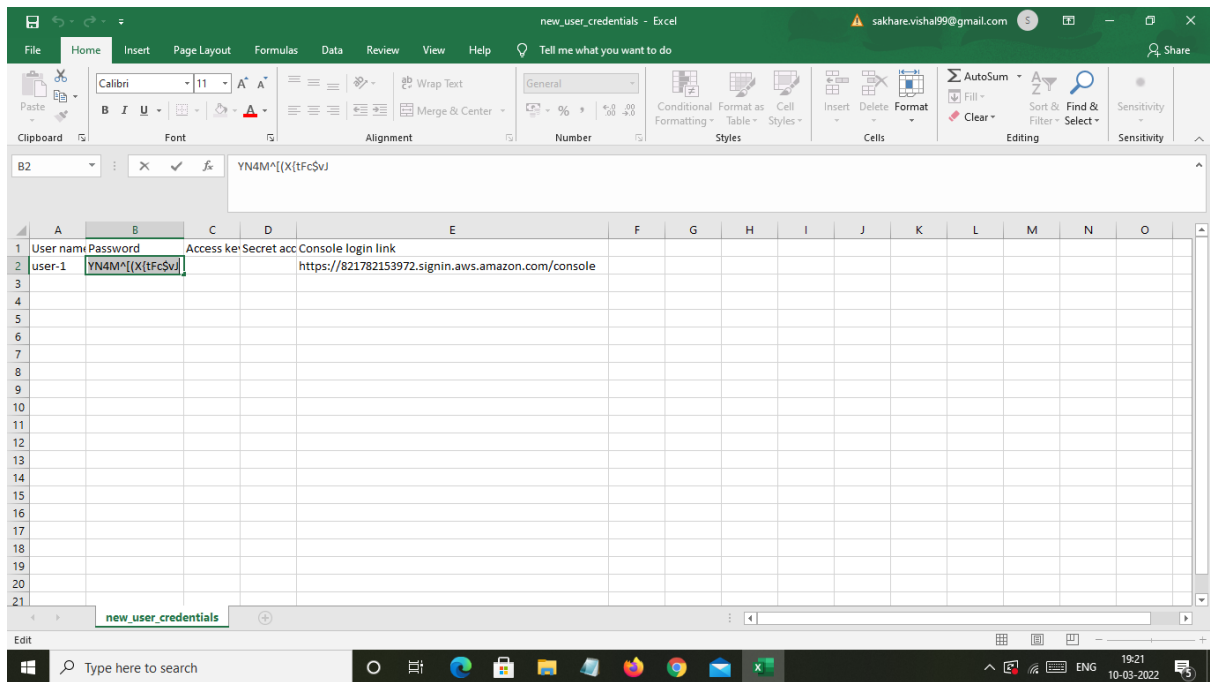
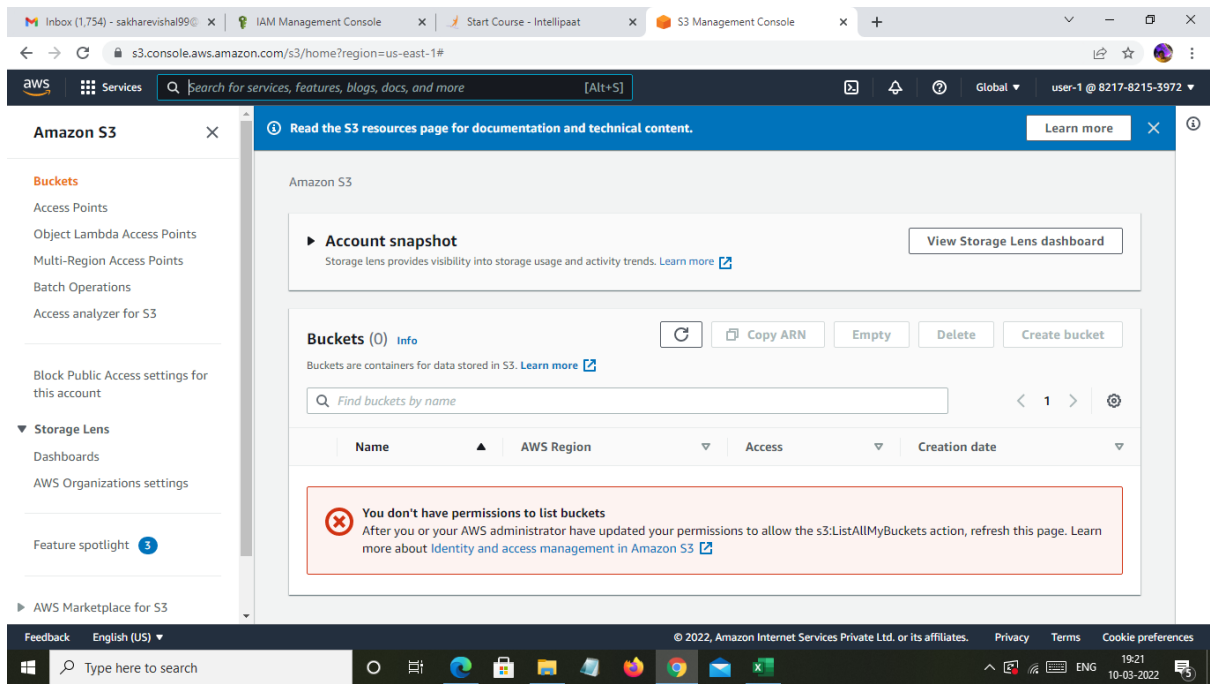
Download .csv

User	Password	Email login instructions
user-1	***** Show	Send email

Close

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search



Inbox (1,754) - sakharevishal99@ IAM Management Console Start Course - Intellipaat RDS Management Console

us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:gdb=false;s3-import=false

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia user-1 @ 8217-8215-3972

We listened to your feedback! Now, create a database with a single click using our pre-built configurations! Or choose your own configurations. [Switch to your original interface.](#) [Share your feedback](#)

RDS > Create database

Create database

Error loading resource

User: arn:aws:iam::821782153972:user/user-1 is not authorized to perform: rds:DescribeDBEngineVersions because no identity-based policy allows the rds:DescribeDBEngineVersions action (Service: AmazonRDS; Status Code: 403; Error Code: AccessDenied; Request ID: d8b34db3-6346-40c3-b907-67c71cd5e40c; Proxy: null)

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

Inbox (1,754) - sakharevishal99@ IAM Management Console Start Course - Intellipaat Amazon Web Services Sign-In

us-east-1.console.aws.amazon.com/iam/home#/users/user-1\$addPermissions?step=review&permissionType=policies&policies=arn:aws:iam::aws:policy%2FAmazonRDSDataFullAccess

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global Vishal Sakhare

Add permissions to user-1

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonRDSDataFullAccess
Managed policy	AmazonVPCFullAccess

Cancel Previous **Add permissions**

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

Type here to search

Browser tabs: Inbox (1,754) - sakharevishal99@, IAM Management Console, Start Course - Intellipaat, Amazon Web Services Sign-In, +

Address bar: us-east-1.console.aws.amazon.com/iam/home#/users/user-1

Header: AWS Services, Search for services, features, blogs, docs, and more, [Alt+S], Global, Vishal Sakhare

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users**
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analizers
 - Settings
 - Credential report
 - Organization activity

Summary

User ARN am:aws:iam::821782153972:user/user-1

Path /

Creation time 2022-03-10 19:13 UTC+0530

Permissions | Groups (1) | Tags | Security credentials | Access Advisor

Permissions policies (5 policies applied)

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

Policy name	Policy type
Attached directly	
IAMUserChangePassword	AWS managed policy
AmazonRDSDataFullAccess	AWS managed policy
Show 4 more	

Footer: Feedback, English (US), © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy, Terms, Cookie preferences

Browser tabs: Inbox (1,754) - sakharevishal99@, IAM Management Console, Start Course - Intellipaat, RDS Management Console, +

Address bar: us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:gdb=false;s3-import=false

Header: AWS Services, Search for services, features, blogs, docs, and more, [Alt+S], N. Virginia, Vishal Sakhare

Create database

Choose a database creation method

- ☒ **Standard create**
You set all of the configuration options, including ones for availability, security, backups, and maintenance.
- ☐ **Easy create**
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type

- ☒ **Amazon Aurora**
- ☐ MySQL
- ☐ MariaDB

Footer: Feedback, English (US), © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy, Terms, Cookie preferences

us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#SecurityGroup:groupId=sg-08e3629c33cd9c566

Services Search for services, features, blogs, docs, and more [Alt+S]

New EC2 Experience Tell us what you think

- EC2 Dashboard
- EC2 Global View
- Events
- Tags
- Limits

▼ Instances

- Instances **New**
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances **New**
- Dedicated Hosts
- Scheduled Instances
- Capacity Reservations

▼ Images

Security group (sg-08e3629c33cd9c566 | my-securityfor-ec2) was created successfully

Details

EC2 > Security Groups > sg-08e3629c33cd9c566 - my-securityfor-ec2

sg-08e3629c33cd9c566 - my-securityfor-ec2

Actions

Details

Security group name	Security group ID	Description	VPC ID
my-securityfor-ec2	sg-08e3629c33cd9c566	for secure permissions	vpc-069694fa8bb5bfdee
Owner	Inbound rules count	Outbound rules count	
821782153972	1 Permission entry	1 Permission entry	

Inbound rules Outbound rules Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Feedback English (US)

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

Type here to search

us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/group-for-ec2?section=permissions

Services Search for services, features, blogs, docs, and more [Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

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

▼ Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity

User group name: group-for-ec2

Creation time: March 10, 2022, 18:53 (UTC+05:30)

ARN: arn:aws:iam::821782153972:group/group-for-ec2

Users Permissions Access Advisor

Permissions policies (3) Info

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter

	Policy name	Type	Description
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2
<input type="checkbox"/>	AWSSecurityHubFullAccess	AWS managed	Provides full access to use AWS Security Hub
<input type="checkbox"/>	AmazonVPCFullAccess	AWS managed	Provides full access to Amazon VPC

Feedback English (US)

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

Type here to search

us-east-1.console.aws.amazon.com/iam/home#/policies/arn:aws:iam::aws:policy/AmazonVPCFullAccess\$serviceLevelSummary

Identity and Access Management (IAM)

- Dashboard
- Access management
 - User groups
 - Users
 - Roles
- Policies**
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analysers
 - Settings
 - Credential report
 - Organization activity

Policies > AmazonVPCFullAccess

Summary

Policy ARN arn:aws:iam::aws:policy/AmazonVPCFullAccess

Description Provides full access to Amazon VPC via the AWS Management Console.

Permissions | Policy usage | Policy versions | Access Advisor

Policy summary | {} JSON

Filter

Service	Access level	Resource	Request condition
Allow (1 of 317 services) Show remaining 316			
EC2	Full: Tagging Limited: List, Read, Write, Permissions management	All resources	None

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

us-east-1.console.aws.amazon.com/access-analyzer/home?region=us-east-1/

Identity and Access Management (IAM)


- Dashboard
- Access management
 - User Groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer**
 - Archive rules
 - Analysers
 - Settings
 - Credential report
 - Organization activity
 - Service control policies (SCP)

Access Analyzer


Monitor access to resources

[Create analyzer](#)

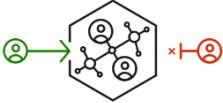
How it works



1 Create an analyzer
You can set the scope for the analyzer to an organization or an AWS account. This is your zone of trust. The analyzer scans all of the supported resources within your zone of trust.



2 Review active findings
When Access Analyzer finds a policy that allows access to a resource from outside of your zone of trust, it generates an active finding. Findings include details about the



3 Take action
If the access is intended, you can archive the finding so that you can focus on reviewing active findings. If the access is not intended, you can resolve the finding by modifying the

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

us-east-1.console.aws.amazon.com/access-analyzer/home?region=us-east-1#/findings

Identity and Access Management (IAM)

Dashboard

Access management

- User Groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCP)

Analyzer creation is complete

IAM > Access Analyzer

Last scan: a few seconds ago

Access Analyzer

Analyzer

ConsoleAnalyzer-f7e97bb9-fbef-4fc7-afe7-b32022a227bf

Zone of trust: Current account (821782153972)

Active Archived Resolved All

Active findings

Account ID 821782153972

Filter active findings

Finding ID	Resource	External principal	Condition	Shared through	Access level	Upd...
No findings						

No findings to display

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

20:20 10-03-2022

s3.console.aws.amazon.com/s3/home?region=us-east-1#

Amazon S3

Buckets

- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Learn how to effectively use the S3 Storage Classes. Learn more

Amazon S3

Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

View Storage Lens dashboard

Buckets (0) Info

Buckets are containers for data stored in S3. Learn more

Find buckets by name

Name	AWS Region	Access	Creation date
You don't have permissions to list buckets			

After you or your AWS administrator have updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3

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

20:29 10-03-2022

