Date
Page No.

1

Name - Gautam Bhatt
Univ Roll No - 1918345
Adm No - 1901144
father's Name - Mr Anil Bhatt
Sem - 5th sec-K
Subject - Cloud computing (Practical)
Date - 4/oct/2021 (Monday)

Ans-1 SSO stands for Single Sign On is an authentication method that enables users to securely aunthenticate with multiple application and website by using just one set of credentials

2

Obj → Practical on SSO (Single Sign On)

Steps to perform objective :-

1) Navigate to the AWS SSO console, and choose AWS accounts from the navigation pane. Choose which account you want users to access from the list of accounts. for this example, choosing three accounts from Marketing BU organizational unit. Then choose assign user.

2) Choose users, start typing to search for users, and then choose search connected directory This search will return a list of users from connected directory. You can also search for groups.

3) To select permission sets, you first have to create one. Choose create new permission set.

4) We can use an existing job function policy to create a permission set This type of policy allows us to apply predefined AWS managed policies to a permission set that are based on common job functions in the IT industry

Date.
Page No.

Alternatively, you can create a custom permission set based on custom policies.

5) for this example, choose the security Audit Job function policy and then choose Create, As a result, this permission set will be available to pick on the next screen

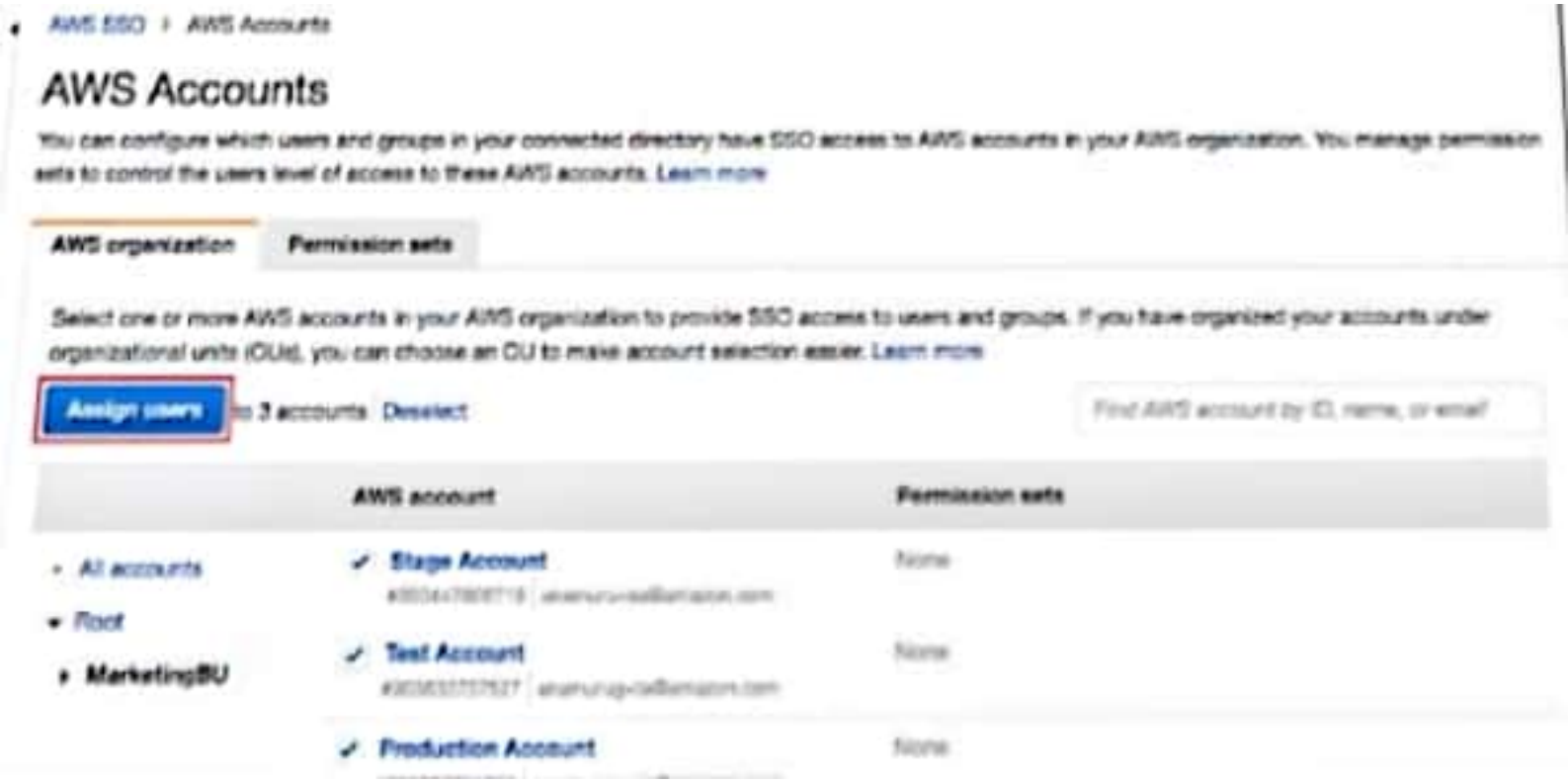
6) Choose a permission set to indicate what level of access you want to grant your users, for this example, assign the securityAdult permission set it's created in the previous step to the user choose. Then choose finish.

7) Your users can sign in to the user portal and access the accounts to which you gave them access. AWS SSO automatically sets up the necessary trust between accounts to enable SSO, AWS SSO also set up the necessary permission in each account. This helps us to scale our administrative tasks across multiple aws accounts.

Date
Page No.

4

8) The user can choose an account and a permission set to sign in to that account without needing to provide a password again. for eg:- if you grant a user two permission sets one that is more restrictive and one that is less restrictive - the user can choose which permission set to use for a specific session. Now we can sign into the production account with Security Audit permission.



Assign Users

1 Users and groups — 2 Permission sets

Select users or groups

You can search for the users and groups in your connected directory to assign SSO access. Type a user or group name to search in your connected directory. You can also specify an Active Directory domain (optional). You can add more than one user or group to your selection. Learn more

Groups | **Users**

anandcorp.com

Search connected directory

Found 4 matching users

- ✓ jadams
- jmadison
- jlewis
- jtyler

Selection

anandcorp.com\jadams Remove

Cancel | Next: Permission sets

Assign Users

1 Users and groups — 2 Permission sets

Select permission sets

Permission sets define the level of access that users and groups have to an AWS account. Permission sets are stored in AWS SSO and appear in the AWS account as IAM roles. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users with multiple permission sets on an AWS account must pick a specific permission set when accessing the account and then return to the user portal to pick a different set when necessary. Learn more

Create new permission set

Permission set	Description	Provisioned status	Created on

Create new permission set

How do you want to create your permission set?

- **Use an existing job function policy**
  Use job function policies to apply predefined AWS managed policies to a permission set. The policies are based on common job functions in the IT industry. Learn more
- **Create a custom permission set**
  Use custom policies to select up to 10 AWS managed policies. You can also define a new policy document that best meets your needs. Learn more

Select job function policy

AdministratorAccess
Provides full access to AWS services and resources.

Billing
Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

DataScientist
Grants permissions to AWS data analytics services.

Billing

Grants permissions for billing and cost management. This includes viewing account usage and viewing and modifying budgets and payment methods.

DataScientist

Grants permissions to AWS data analytics services.

DatabaseAdministrator

Grants full access permissions to AWS services and actions required to set up and configure AWS database services.

NetworkAdministrator

Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.

PowerUserAccess

Provides full access to AWS services and resources, but does not allow management of Users and groups.

SecurityAudit

The security audit template grants access to read security configuration metadata. It is useful for software that audits the configuration of an AWS account.

SupportUser

This policy grants permissions to troubleshoot and resolve issues in an AWS account. This policy also enables the user to contact AWS support to create and manage cases.

SystemAdministrator

Cancel Create

Assign Users

1 Users and groups — 2 Permission sets

Select permission sets

Permission sets define the level of access that users and groups have to an AWS account. Permission sets are stored in AWS SSO and appear in the AWS account as IAM roles. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users with multiple permission sets on an AWS account must pick a specific permission set when accessing the account and then return to the user portal to pick a different set when necessary. Learn more

Create new permission set

✔	Permission set	Description	Provisioned status	Created on
✔	SecurityAudit		Not provisioned	12/5/2017

Complete

e have successfully configured your AWS accounts. Your users can access these AWS accounts with the permissions you assigned.

Proceed to AWS accounts

Account	Status	
Stage Account	Complete	Show details
Test Account	Complete	Show details
Production Account	Complete	Show details

Practical - 2nd

Obj :- Upload files on Github from Desktop using Git command

Steps → 1) Create new repository on Github

2) Now open cmd use cd commands to the local file directory that you want to publish on Github

3) Initialize local directory
Command - git init

5

Date.
Page No.

4) Add local repository

command - git add, This command stages all the files in the directory

5) commit Repository

Command - git commit -m "first commit Message"

6) Now, copy the remote repository url provided by github to you when you published your repository on Github.

Command - git remote add origin https://github.com/yourname/your-repo-name.git

7) push local repository to github

command - git push origin master

8) Pull repository from Github

Commands - git pull origin master

All the commands to cd/your directory

Date.
Page No.

git init

git add . or git add ['filename']

git commit -m "my first file" .

git remote origin https://github.com/your name/your-repo-name.git.

git push origin master

git pull origin master.