

Name - Tushar Bisheti

Subject - Cloud Based Application Development and Management
Subject Code - PCS - 552

Date - 4/10/21

Roll No - 19011267/1918771/52

Q-1 - What is the use of SSO? Show the implementation of SSO.

Ans-1 - Single Sign-on (SSO) is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.

- 1 - It improves security capabilities.
- 2 - It reduces password fatigue.
- 3 - It increases employee and IT productivity.
- 4 - It combines with Risk-Based Authentication (RBA).
- 5 - It increases software adoption rates.
- 6 - It prevents shadow IT.
- 7 - It streamlines the user experience.

Implementation of SSO :

- 1 - Navigate to the AWS SSO console, and choose AWS accounts from the navigation pane. Choose which account from Marketing Bu organizational unit. Then choose Assign users.
- 2 - choose user, 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 - You can use an existing job function policy to create a permission set. This type of policy allows you to apply predefined AWS managed policies to a permission set that are based on common job functions in the IT industry. 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 Security Audit Permission set (it's created in the previous step) to the user choose. Then choose Finish.
- 7 - Your user can sign in to the user portal and access the accounts to which you gave them access. AWS SSO automatically set up the necessary trust b/w accounts to enable SSO. This helps you scale your administrative tasks across multiple AWS accounts.
- 8 - The users can choose an account and a permission set to sign in to that account without needing to provide a password again.

Dashboard

AWS accounts

Applications

Connected directory

AWS SSO > **AWS Accounts**

AWS Accounts

You can configure which users and groups in your connected directory have SSO access to AWS accounts in your AWS organization. You manage permission sets to control the users level of access to these AWS accounts. [Learn more](#)

[AWS organization](#) [Permission sets](#)

Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. [Learn more](#)

[Assign users](#) [to 3 accounts](#) [De-select](#) [Find AWS account by ID, name, or alias](#)

AWS account	permission sets
All accounts	None
Root	None
MarketingEU	None
Stage Account	None
Test Account	None
Production Account	None

Assign Users

1

2

Users and groups

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
- jmadsen
- jpm
- ryan

Selection

anandcorp.com/jadams Remove

Cancel

Next Step >

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
----------------	-------------	--------------------	------------

You have not yet assigned any permission sets.

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

Administrator Access

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.

Data Migration

Provides permissions to AWS data migration 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

This policy grants permissions to read security configuration information. It is used for auditing and monitoring 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 through the AWS Support Center.

SystemAdministrator

...more

Create

Assign Users

1

2

Users and groups

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

12/6/2017

[Cancel](#)

[Previous](#)

[Finish](#)

Complete

We 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 View details	Complete	Show details
Test Account View details	Complete	Show details
Production Account View details	Complete	Show details

Search



AWS Management
Console (3)

650 (Account) >

903 (Account) >

6BC (Production Account)
SecurityAudit

Terms of Use

Powered by CamScanner

Name - Tushar Bish

Section - K

Subject - Cloud Based Application Development and Management

Subject Code - PCS-552

Date - 04/10/21

Roll no - 19011267 / 1918771 / 52

Q-3 - Show the working in GitHub for fork and Pull Request.

- Ans-3 - 1- Navigate to the original repository where you created your fork.
- 2- In the 'Branch' menu, choose the branch that contains your commits.
- 3- Above the list of files, click pull request.
- 4- Use the base branch dropdown menu to select the branch you'd like to merge your changes into, then use the compare branch drop-down menu to choose the to pic branch you made changes in.
- 5- Type a title and description for your pull request.
- 6- To create pull request ready for review, click create pull Request to create a draft pull request, use the drop down and select create Draft pull request then click Draft Pull Request.
- Draft Pull Request has been reviewed.
- 7- After your Pull Request has been reviewed, It can be merged into repository.

Tushar-04-03 / Mid-Term-Cloud-Based-Application-Development-and-Management-PCS-552 · Public

Forked from Lisaverma1520/Mid-Term-Cloud-Based-Application-Development-and-Management-PCS-552 ·

Code Pull requests Issues Marketplace Explore

main · 1 branch · 0 tags

This branch is even with Lisaverma1520:main.

Lisaverma1520 Delete index.html · c5b683d · 14 hours ago · 5 commits

Question Paper PCS 552 · Delete index.html · 14 hours ago

README.md · Update README.md · 3 days ago

README.md

-Mid-Term-Cloud-Based-Application-Development-and-Management-PCS-552

About

No description, website, or topics provided.

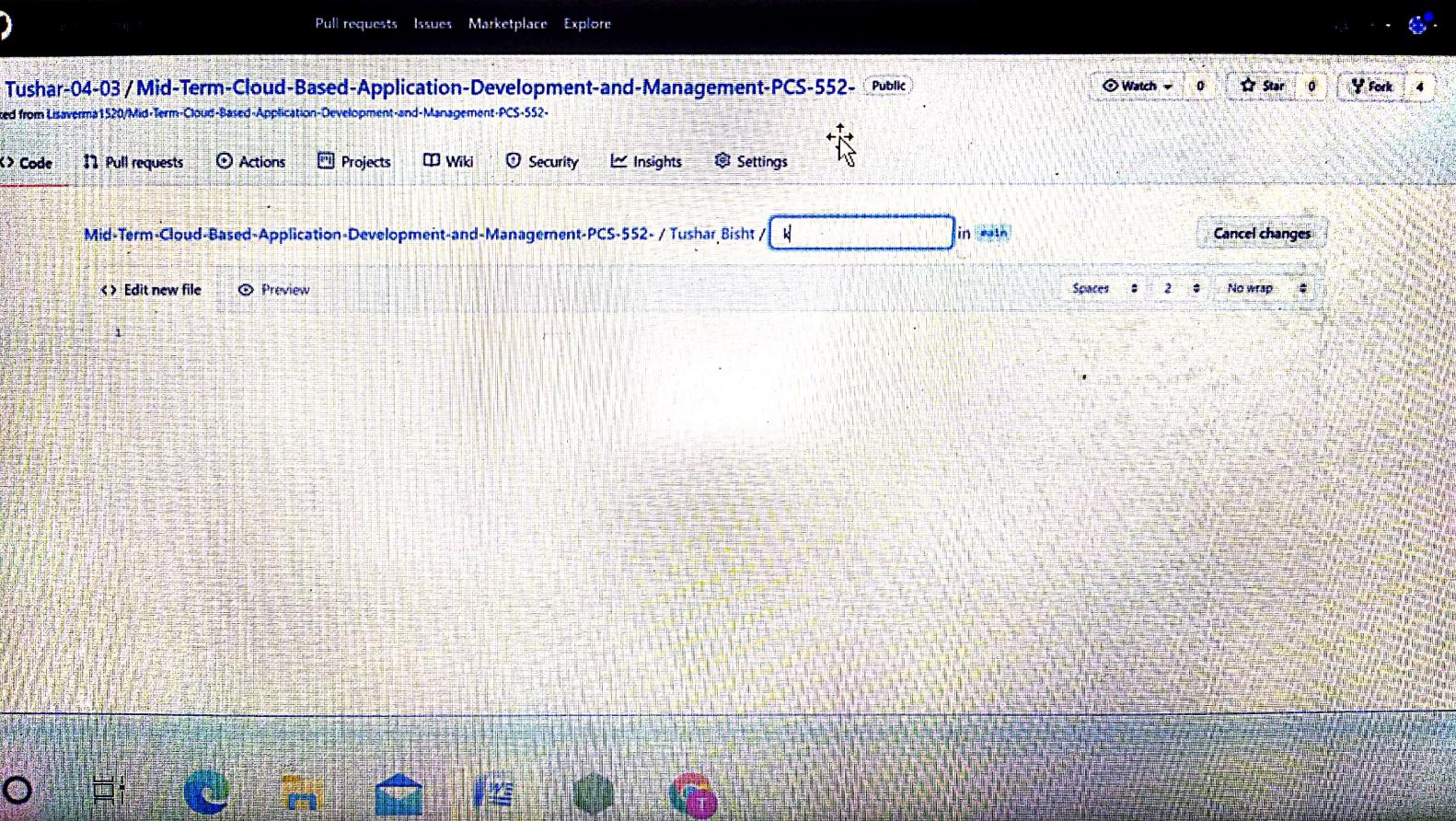
Readme

Releases

No releases published. Create a new release

Packages

No packages published. Publish your first package





Commit new file

Create a new file

Add an optional extended description...

Commit directly to the ~~main~~ branch

Create a new branch for this commit and start a pull request. Learn more about pull requests.

P Tushar-64-03-patch

Propose new file

Cancel



Open a pull request

The change you just made was written to a new branch named [Tushar-04-03-patch-1](#). Create a pull request below to propose these changes.

base: main ✓ compare: Tushar-04-03-patch-1 ✓ Able to merge. These branches can be automatically merged.

Tushar Bisht

Write Preview

Leave a comment

Attach files by dragging & dropping, selecting or pasting them.

Reviewers No reviews

Assignees No one—assign yourself

Labels None yet

Projects None yet

Milestone No milestones

Create pull request

Remember: contributions to this repository should follow our GitHub Contribution Guidelines

Tushar-04-03 / Mid-Term-Cloud-Based-Application-Development-and-Management-PCS-552 - Public

Forked from lisaverma1520/Mid-Term-Cloud-Based-Application-Development-and-Management-PCS-552

[Code](#) [Pull requests 1](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#) [Settings](#)

Tushar Bisht #1

[Open](#) Tushar-04-03 wants to merge 1 commit into [main](#) from [Tushar-04-03-patch-1](#)

[Conversation 0](#) [Commits 1](#) [Checks 0](#) [Files changed 1](#) [+1 -0](#)

Tushar-04-03 commented now

No description provided

[Create PR](#)

Owner ...

Verified Oct 6 4b

Reviewers
No reviews
Still in progress? Convert to draft

Assignees
No one—assign yourself

Labels
None yet

Projects
None yet

Add more commits by pushing to the [Tushar-04-03-patch-1](#) branch on Tushar-04-03/Mid-Term-Cloud-Based-Application-Development-and-Management-PCS-552.

Continuous integration has not been set up
GitHub Actions and several other apps can be used to automatically catch bugs and enforce style.

This branch has no conflicts with the base branch