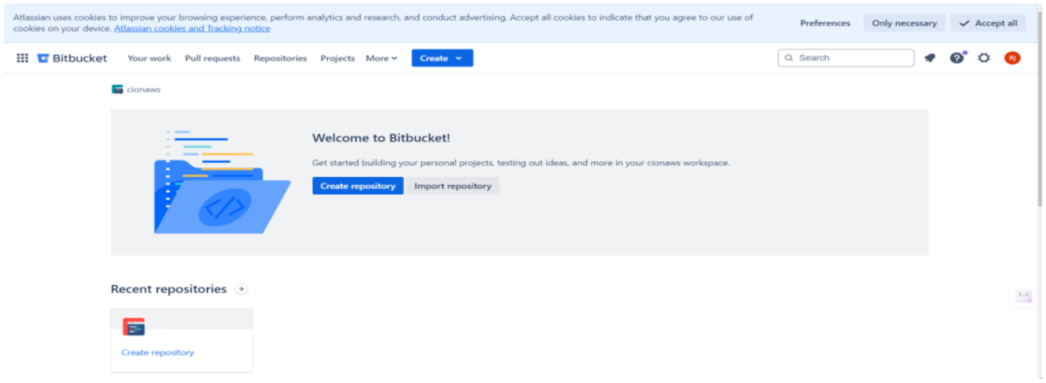
Aws code commit setup: -

1.create the account on bitbucket.org: - create the workspace: -

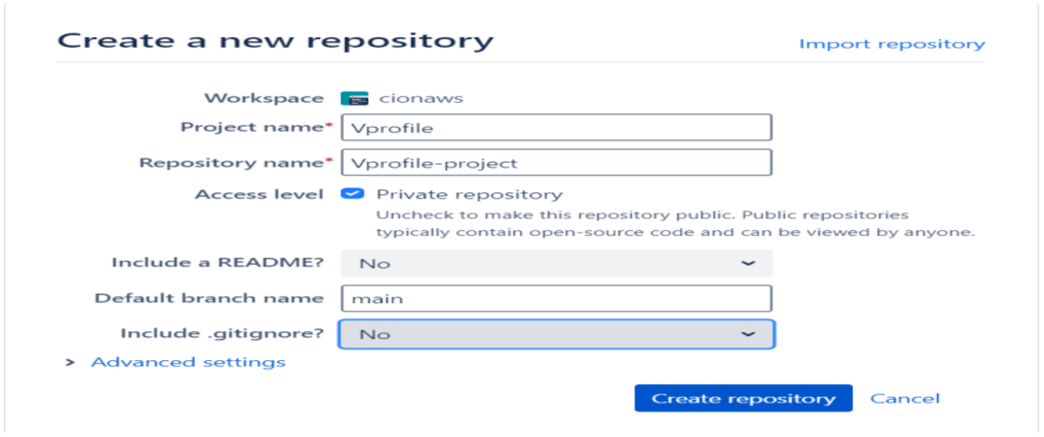


Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising. Accept all cookies to indicate that you agree to our use of cookies on your device. Atlassian cookies and Tracking notice

Welcome to Bitbucket!

Get started building your personal projects, testing out ideas, and more in your cionaws workspace.

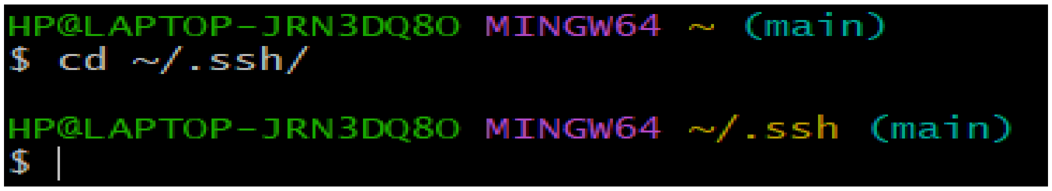
2.creating the bitbucket repository: -



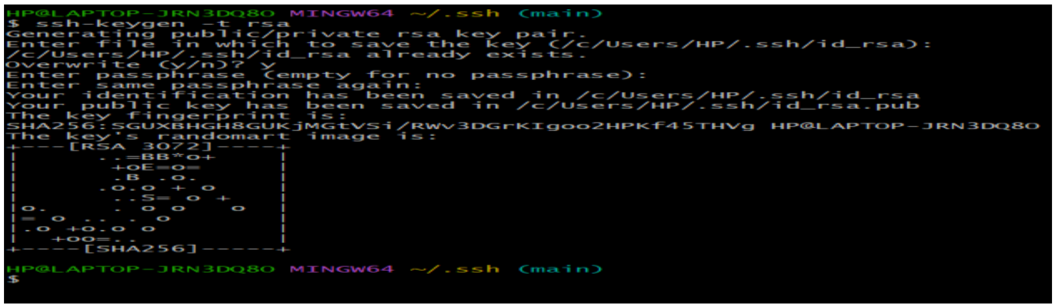
Create a new repository

Workspace	cionaws
Project name*	Vprofile
Repository name*	Vprofile-project
Access level	✓ Private repository Uncheck to make this repository public. Public repositories typically contain open-source code and can be viewed by anyone.
Include a README?	No
Default branch name	main
Include .gitignore?	No

3.adding the ssh for authenticating to the remote bitbucket repo from local: - navigate to .ssh/ directory.

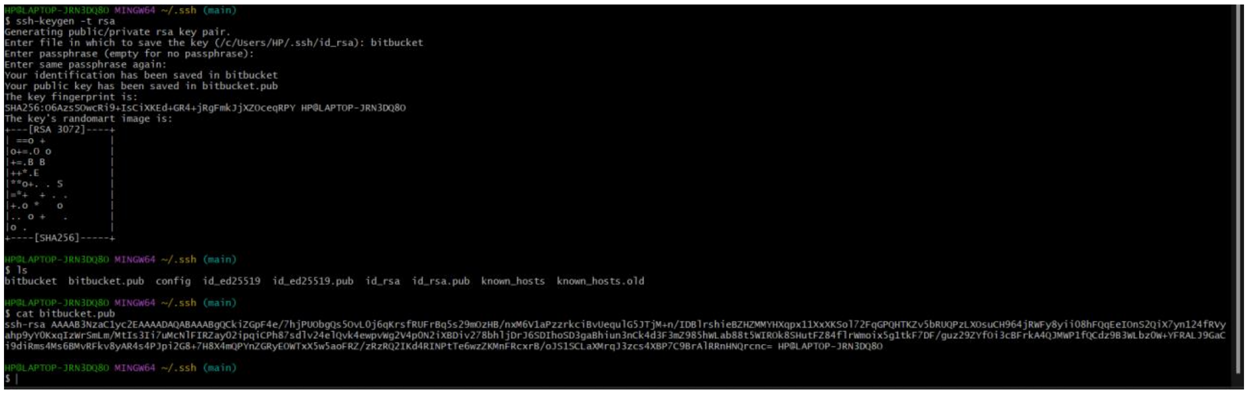


```
HP@LAPTOP-JRN3DQ8O MINGW64 ~ (main)
$ cd ~/.ssh/

HP@LAPTOP-JRN3DQ8O MINGW64 ~/.ssh (main)
$ |
```



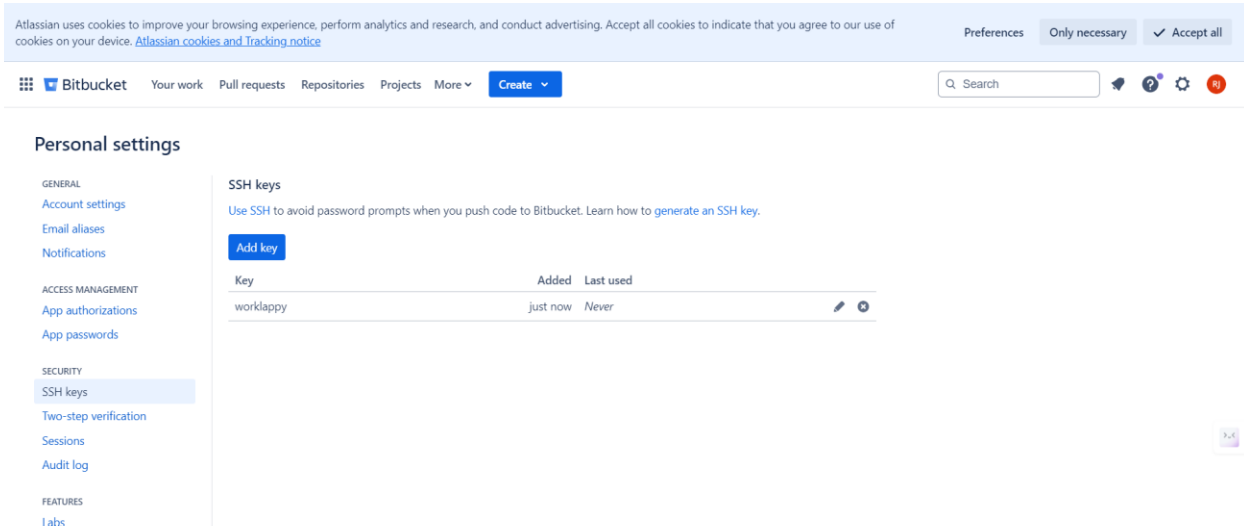
```
HP@LAPTOP-JRN3DQ8O MINGW64 ~/.ssh (main)
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/c/Users/HP/.ssh/id_rsa):
/c/Users/HP/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /c/Users/HP/.ssh/id_rsa
Your public key has been saved in /c/Users/HP/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:SGUXBHGH8GUKjMGtVSi/RWv3DGrKIgoo2HPKf45THVg HP@LAPTOP-JRN3DQ8O
The key's randomart image is:
+---[RSA 3072]----+
|       ..=BB*o+  |
|        +oE=o=   |
|        .B .o.   |
|       .o.o + o  |
|        ..S= o + |
|o.      . o o   o|
|= o ... . o      |
|.o +o.o o        |
|  +oo=..         |
+----[SHA256]-----+

HP@LAPTOP-JRN3DQ8O MINGW64 ~/.ssh (main)
$
```

Now you need to go into the file where you created your ssh pub keys then you need to cat those by hitting below commands in the ss:-



```
HP@LAPTOP-JRN3DQ80 MINGW64 ~/.ssh (main)
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/c/Users/HP/.ssh/id_rsa): bitbucket
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in bitbucket
Your public key has been saved in bitbucket.pub
The key fingerprint is:
SHA256:06AzsSOwcRi9+IsCiXKEd+GR4+jRgFmkJjXZOceqRPY HP@LAPTOP-JRN3DQ80
The key's randomart image is:
+---[RSA 3072]----+
| ==o +           |
|o+=.O o          |
|+=.B B           |
|++*.E            |
|**o+. . S        |
|=*+  + . .       |
|+.o *   o        |
|.. o +   .       |
|o .              |
+----[SHA256]-----+

HP@LAPTOP-JRN3DQ80 MINGW64 ~/.ssh (main)
$ ls
bitbucket  bitbucket.pub  config  id_ed25519  id_ed25519.pub  id_rsa  id_rsa.pub  known_hosts  known_hosts.old

HP@LAPTOP-JRN3DQ80 MINGW64 ~/.ssh (main)
$ cat bitbucket.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCkiZGpF4e/7hjPUObgQs5OvL0j6qKrsfRUFrBq5s29mOzHB/nxM6V1aPzzrkciBvUequlG5JTjM+n/IDBlrshieBZHZMMYHXqpx11XxXKSo172FqGPQHTKZv5bRUQPzLXOsuCH964jRWFy8yii08hFQqEeIOnS2QiX7yn124fRVy
ahp9yYOKxqIzWrSmLm/MtIs3Ii7uMcNlFIRZay02ipqiCPh87sdlv24elQvk4ewpvWg2V4pON2iXBDiv278bhljDrJ6SDIhoSD3gaBhiun3nCk4d3F3mZ985hWLab88t5WIROk8SHutFZ84flrWmoix5g1tkF7DF/guz29ZYfOi3cBFrkA4QJMWP1fQCdz9B3WLbzOW+YFRALJ9GaC
i9diRms4Ms6BMvRFkv8yAR4s4PJpi2G8+7H8X4mQPYnZGRyEOWTxX5w5aoFRZ/zRzRQ2IKd4RINPtTe6wzZKMnFRcxrB/oJS1SCLaXMrqJ3zcs4XBP7C9BrAlRRnHNQrcnc= HP@LAPTOP-JRN3DQ80

HP@LAPTOP-JRN3DQ80 MINGW64 ~/.ssh (main)
$ |
```

Note:-we are gonna paste this pub keys in our bitbucket account:-



Atlassian uses cookies to improve your browsing experience, perform analytics and research, and conduct advertising. Accept all cookies to indicate that you agree to our use of cookies on your device. Atlassian cookies and Tracking notice

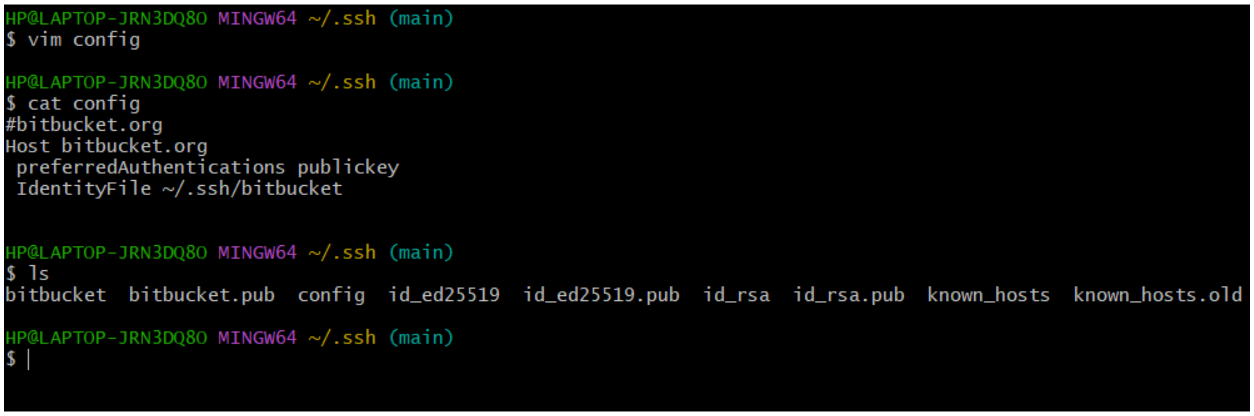
SSH keys

Use SSH to avoid password prompts when you push code to Bitbucket. Learn how to generate an SSH key.

Add key

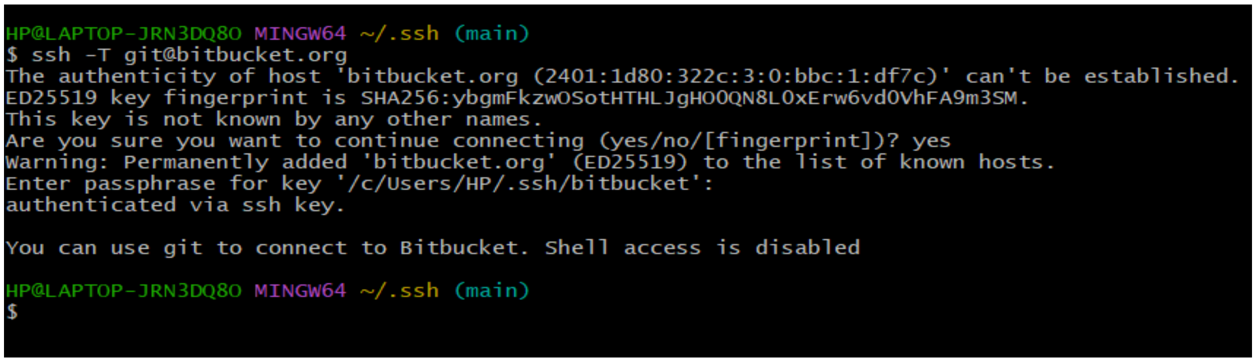
Key	Added	Last used
worklappy	just now	*Never*

and also add the private keys in ours config file on local to authenticate



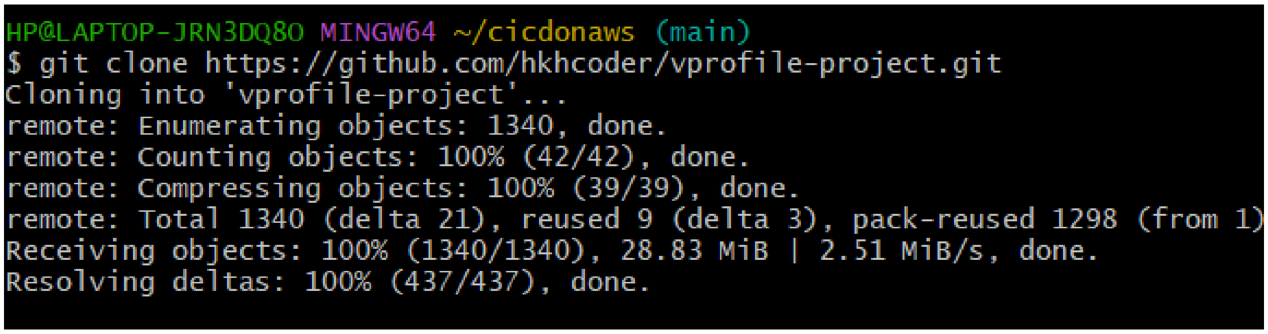
```
HP@LAPTOP-JRN3DQ80 MINGW64 ~/.ssh (main)
$ vim config

HP@LAPTOP-JRN3DQ80 MINGW64 ~/.ssh (main)
$ cat config
#bitbucket.org
Host bitbucket.org
 preferredAuthentications publickey
 IdentityFile ~/.ssh/bitbucket


HP@LAPTOP-JRN3DQ80 MINGW64 ~/.ssh (main)
$ ls
bitbucket  bitbucket.pub  config  id_ed25519  id_ed25519.pub  id_rsa  id_rsa.pub  known_hosts  known_hosts.old

HP@LAPTOP-JRN3DQ80 MINGW64 ~/.ssh (main)
$ |
```

now we can test if the authentication is properly configured or not between our remote and local: -



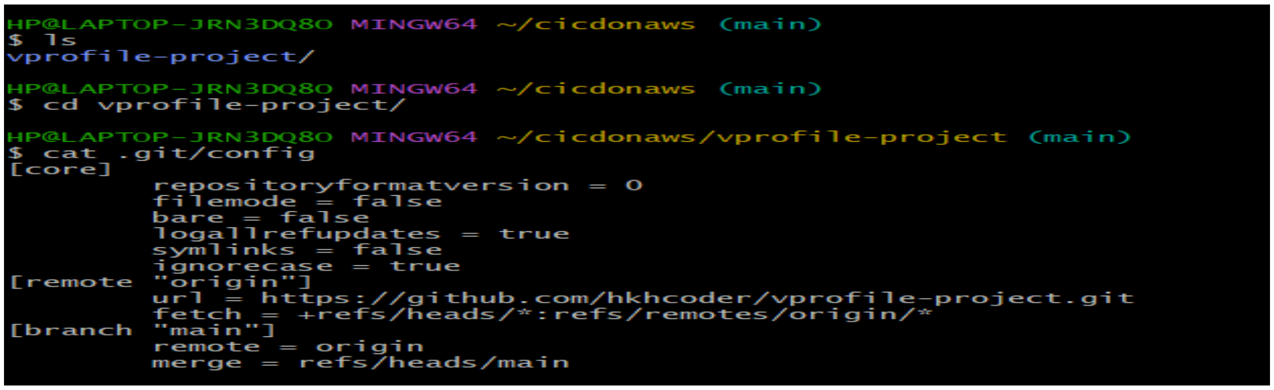
```
HP@LAPTOP-JRN3DQ8O MINGW64 ~/.ssh (main)
$ ssh -T git@bitbucket.org
The authenticity of host 'bitbucket.org (2401:1d80:322c:3:0:bbc:1:df7c)' can't be established.
ED25519 key fingerprint is SHA256:ybgmFkzwOSotHTHLJgHO0QN8L0xErw6vd0VhFA9m3SM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'bitbucket.org' (ED25519) to the list of known hosts.
Enter passphrase for key '/c/Users/HP/.ssh/bitbucket':
authenticated via ssh key.

You can use git to connect to Bitbucket. Shell access is disabled

HP@LAPTOP-JRN3DQ8O MINGW64 ~/.ssh (main)
$
```

Now we need to migrate our github source code from github to bitbucket: -
we need to migrate our source code from github to bitbucket for that we will be creating the directory named cicdaws then we need to navigate into it and clone our github repo there and from there we will be pushing that repo into our bitbucket created repo:-

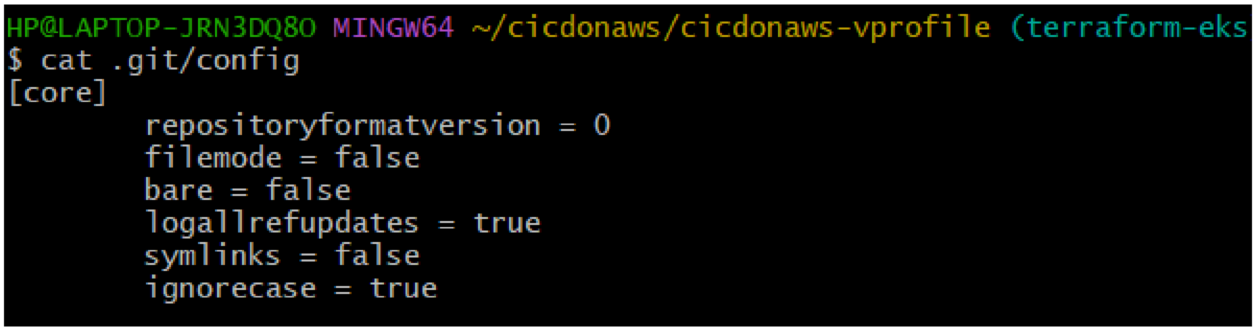


```
HP@LAPTOP-JRN3DQ8O MINGW64 ~/cicdonaws (main)
$ git clone https://github.com/hkhcoder/vprofile-project.git
Cloning into 'vprofile-project'...
remote: Enumerating objects: 1340, done.
remote: Counting objects: 100% (42/42), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 1340 (delta 21), reused 9 (delta 3), pack-reused 1298 (from 1)
Receiving objects: 100% (1340/1340), 28.83 MiB | 2.51 MiB/s, done.
Resolving deltas: 100% (437/437), done.
```

Now we need to remove our source github repo from below path and put there our bitbucket repo url:-

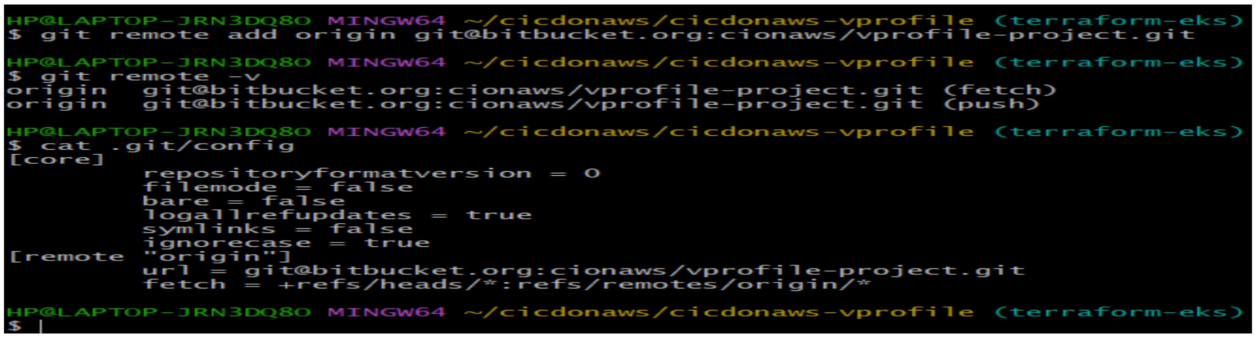


```
HP@LAPTOP-JRN3DQ8O MINGW64 ~/cicdonaws (main)
$ ls
vprofile-project/

HP@LAPTOP-JRN3DQ8O MINGW64 ~/cicdonaws (main)
$ cd vprofile-project/

HP@LAPTOP-JRN3DQ8O MINGW64 ~/cicdonaws/vprofile-project (main)
$ cat .git/config
[core]
        repositoryformatversion = 0
        filemode = false
        bare = false
        logallrefupdates = true
        symlinks = false
        ignorecase = true
[remote "origin"]
        url = https://github.com/hkhcoder/vprofile-project.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
        remote = origin
        merge = refs/heads/main
```



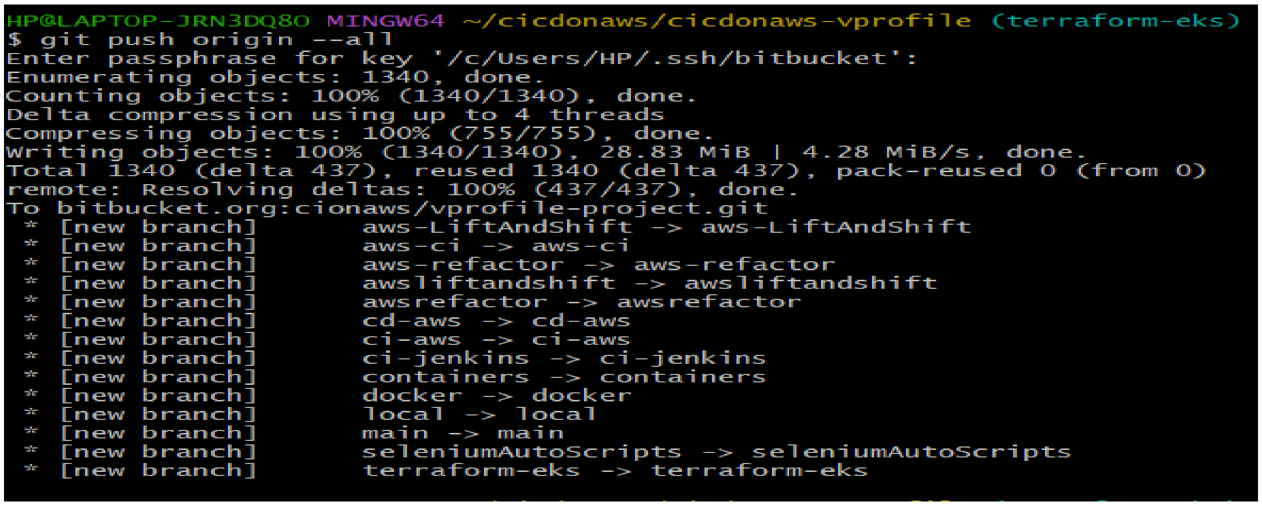
```
HP@LAPTOP-JRN3DQ80 MINGW64 ~/cicdonaws/cicdonaws-vprofile (terraform-eks
$ cat .git/config
[core]
        repositoryformatversion = 0
        filemode = false
        bare = false
        logallrefupdates = true
        symlinks = false
        ignorecase = true
```

As you can see the github remote repo has been removed from the config file and now we need to add our bitbucket repo url in the same: -

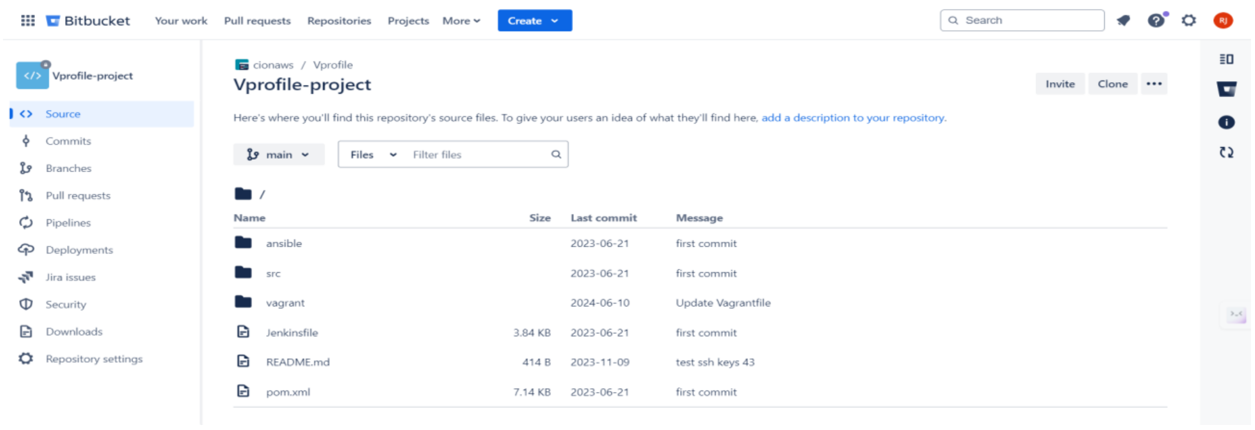


```
HP@LAPTOP-JRN3DQ80 MINGW64 ~/cicdonaws/cicdonaws-vprofile (terraform-eks)
$ git remote add origin git@bitbucket.org:cionaws/vprofile-project.git

HP@LAPTOP-JRN3DQ80 MINGW64 ~/cicdonaws/cicdonaws-vprofile (terraform-eks)
$ git remote -v
origin  git@bitbucket.org:cionaws/vprofile-project.git (fetch)
origin  git@bitbucket.org:cionaws/vprofile-project.git (push)

HP@LAPTOP-JRN3DQ80 MINGW64 ~/cicdonaws/cicdonaws-vprofile (terraform-eks)
$ cat .git/config
[core]
        repositoryformatversion = 0
        filemode = false
        bare = false
        logallrefupdates = true
        symlinks = false
        ignorecase = true
[remote "origin"]
        url = git@bitbucket.org:cionaws/vprofile-project.git
        fetch = +refs/heads/*:refs/remotes/origin/*

HP@LAPTOP-JRN3DQ80 MINGW64 ~/cicdonaws/cicdonaws-vprofile (terraform-eks)
$ |
```

now we will be pushing all our local git branches which were migrated from GitHub to bitbucket repository: -



```
HP@LAPTOP-JRN3DQ80 MINGW64 ~/cicdonaws/cicdonaws-vprofile (terraform-eks)
$ git push origin --all
Enter passphrase for key '/c/Users/HP/.ssh/bitbucket':
Enumerating objects: 1340, done.
Counting objects: 100% (1340/1340), done.
Delta compression using up to 4 threads
Compressing objects: 100% (755/755), done.
Writing objects: 100% (1340/1340), 28.83 MiB | 4.28 MiB/s, done.
Total 1340 (delta 437), reused 1340 (delta 437), pack-reused 0 (from 0)
remote: Resolving deltas: 100% (437/437), done.
To bitbucket.org:cionaws/vprofile-project.git
 * [new branch]      aws-LiftAndShift -> aws-LiftAndShift
 * [new branch]      aws-ci -> aws-ci
 * [new branch]      aws-refactor -> aws-refactor
 * [new branch]      awsliftandshift -> awsliftandshift
 * [new branch]      awsrefactor -> awsrefactor
 * [new branch]      cd-aws -> cd-aws
 * [new branch]      ci-aws -> ci-aws
 * [new branch]      ci-jenkins -> ci-jenkins
 * [new branch]      containers -> containers
 * [new branch]      docker -> docker
 * [new branch]      local -> local
 * [new branch]      main -> main
 * [new branch]      seleniumAutoScripts -> seleniumAutoScripts
 * [new branch]      terraform-eks -> terraform-eks
```



cionaws / Vprofile

Vprofile-project

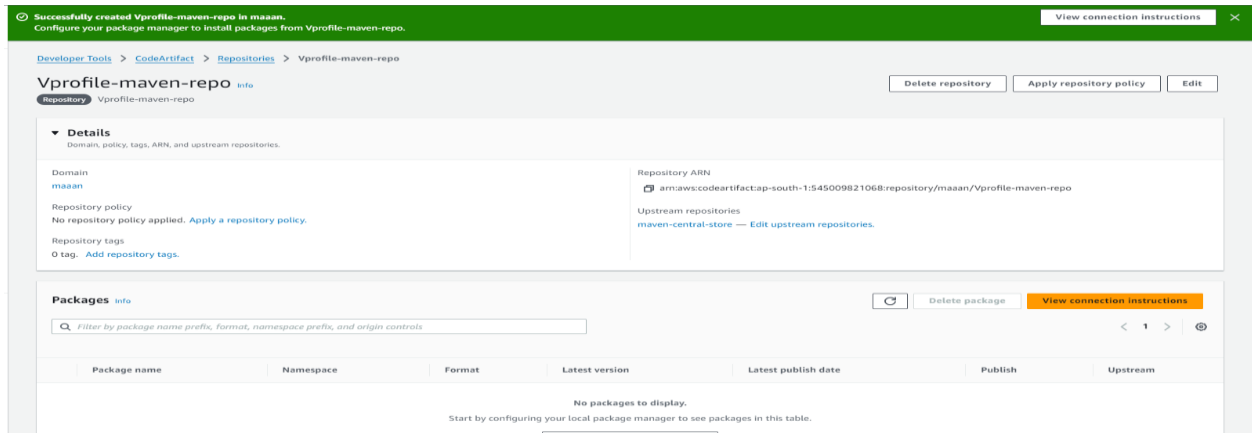
Here's where you'll find this repository's source files. To give your users an idea of what they'll find here, add a description to your repository.

main · Files · Filter files

/

Name	Size	Last commit	Message
ansible		2023-06-21	first commit
src		2023-06-21	first commit
vagrant		2024-06-10	Update Vagrantfile
Jenkinsfile	3.84 KB	2023-06-21	first commit
README.md	414 B	2023-11-09	test ssh keys 43
pom.xml	7.14 KB	2023-06-21	first commit

create code artifact repo to download the dependencies from it and save the build artifacts in the code artifact repo:-



Successfully created Vprofile-maven-repo in maaan.
Configure your package manager to install packages from Vprofile-maven-repo.

Developer Tools > CodeArtifact > Repositories > Vprofile-maven-repo

Vprofile-maven-repo Info
Repository Vprofile-maven-repo

Details
Domain, policy, tags, ARN, and upstream repositories.

Domain
maaan

Repository policy
No repository policy applied. Apply a repository policy.

Repository tags
0 tag. Add repository tags.

Repository ARN
arn:aws:codeartifact:ap-south-1:545009821068:repository/maaan/Vprofile-maven-repo

Upstream repositories
maven-central-store — Edit upstream repositories.

Packages Info

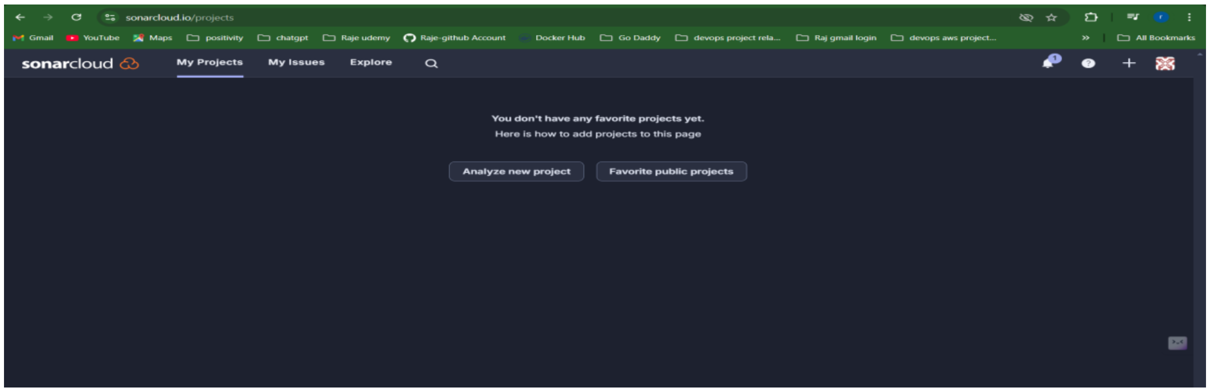
Filter by package name prefix, format, namespace prefix, and origin controls

Package name	Namespace	Format	Latest version	Latest publish date	Publish	Upstream

No packages to display.
Start by configuring your local package manager to see packages in this table.

Now you need to clone the project repositroy from your github remite repo in the vs code or any other code editor of your choice im using vs code in my case then you can see the setting.xml ,pom.xml,sonar-buildspec.yml build-buildspec.yml etc then you simply need to go through them and understand them step by step then.

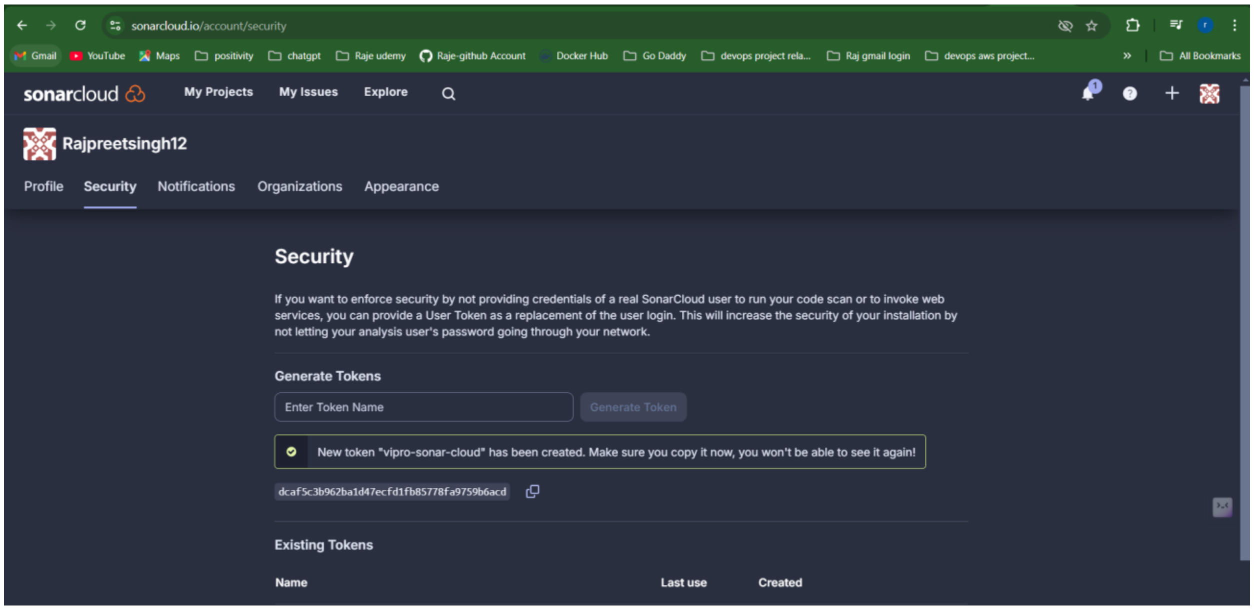
Now we will be setting up the sonar cloud to out check for the build result which is been shared there.



You don't have any favorite projects yet.
Here is how to add projects to this page

You need to hit sonarcloud.io to and get logged into it.

Now you need to navigate to account>security then you need to generate the token for your sonar cloud to authenticate it from aws code build:-



sonarcloud.io/account/security

Rajpreetsingh12

Profile | Security | Notifications | Organizations | Appearance

Security

If you want to enforce security by not providing credentials of a real SonarCloud user to run your code scan or to invoke web services, you can provide a User Token as a replacement of the user login. This will increase the security of your installation by not letting your analysis user's password going through your network.

Generate Tokens

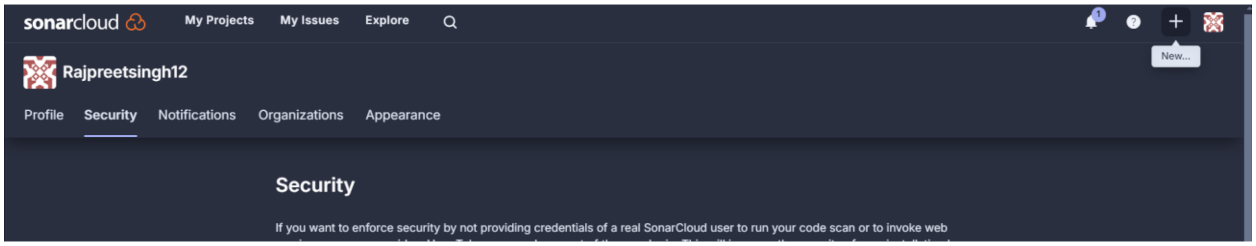
Enter Token Name | Generate Token

New token "vipro-sonar-cloud" has been created. Make sure you copy it now, you won't be able to see it again!

```
dcaf5c3b962ba1d47ecfd1fb85778fa9759b6acd
```

Existing Tokens

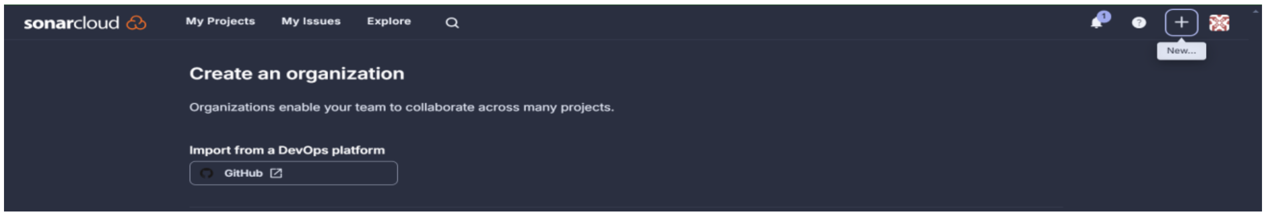
Name	Last use	Created



Security

If you want to enforce security by not providing credentials of a real SonarCloud user to run your code scan or to invoke web

now you need to click on the above + symbol and create your own organization:-

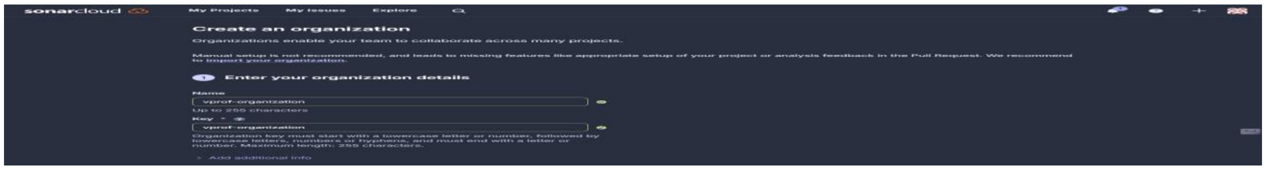


Create an organization

Organizations enable your team to collaborate across many projects.

Import from a DevOps platform

GitHub



Create an organization

Organizations enable your team to collaborate across many projects.

Manual setup is not recommended, and leads to missing features like appropriate setup of your project or analysis feedback in the Pull Request. We recommend to import your organization.

1 Enter your organization details

Name: vprof-organization

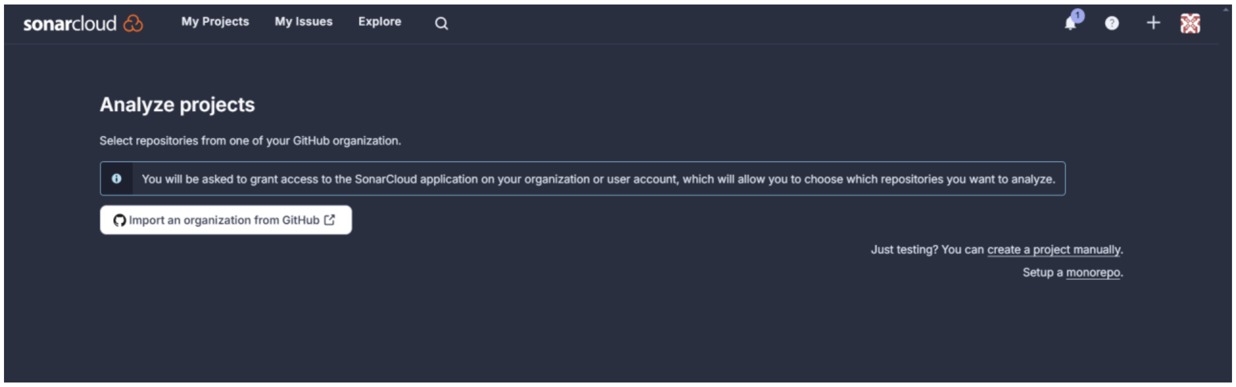
Up to 255 characters

Key *: vprof-organization

Organization key must start with a lowercase letter or number, followed by lowercase letters, numbers or hyphens, and must end with a letter or number. Maximum length: 255 characters.

> Add additional info

Now click on sonar cloud symbol in the left top corner and then click analyze new project



Analyze projects

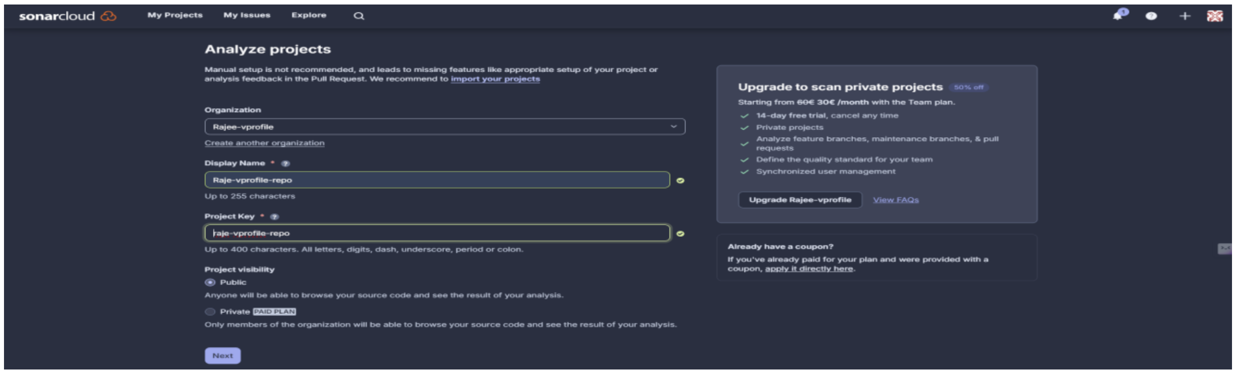
Select repositories from one of your GitHub organization.

You will be asked to grant access to the SonarCloud application on your organization or user account, which will allow you to choose which repositories you want to analyze.

Import an organization from GitHub

Just testing? You can create a project manually.

Setup a monorepo.



Analyze projects

Manual setup is not recommended, and leads to missing features like appropriate setup of your project or analysis feedback in the Pull Request. We recommend to import your projects

Organization: Rajee-vprofile

Create another organization

Display Name *: Raje-vprofile-repo

Up to 255 characters

Project Key *: raje-vprofile-repo

Up to 400 characters. All letters, digits, dash, underscore, period or colon.

Project visibility

[✓ Public] Anyone will be able to browse your source code and see the result of your analysis.

Private PAID PLAN Only members of the organization will be able to browse your source code and see the result of your analysis.

Next

Upgrade to scan private projects 50% off

Starting from ~~60€~~ 30€ /month with the Team plan.

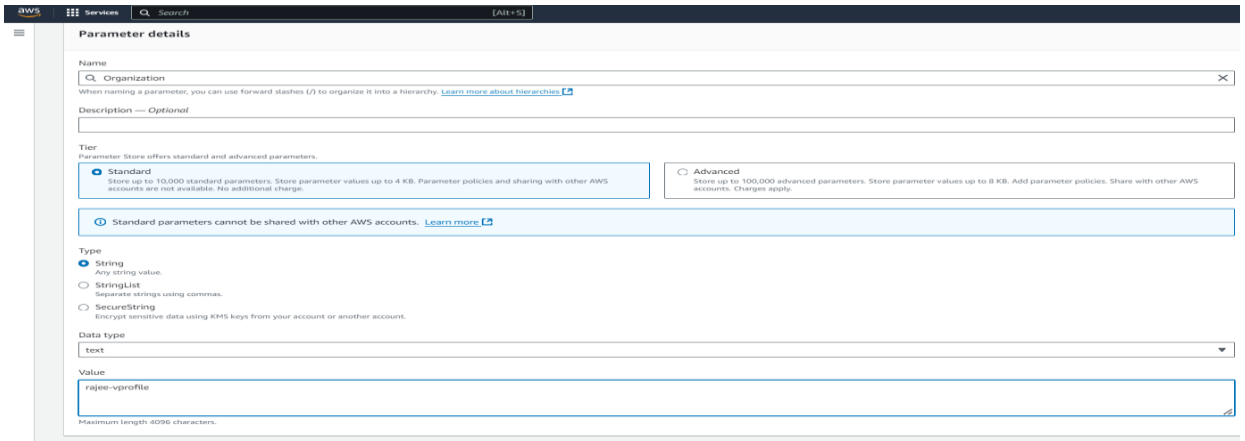
- ✓ 14-day free trial, cancel any time
- ✓ Private projects
- ✓ Analyze feature branches, maintenance branches, & pull requests
- ✓ Define the quality standard for your team
- ✓ Synchronized user management

Upgrade Rajee-vprofile View FAQs

Already have a coupon?

If you've already paid for your plan and were provided with a coupon, apply it directly here.

Now we will be creating the paramete from paramete store in the system manager and there all the variables will be saved securely so that we can use them in the sonarbuild-spec.xml file to login into sonar cloud and different integrative services:-



Parameter details

Name: Organization

When naming a parameter, you can use forward slashes (/) to organize it into a hierarchy. Learn more about hierarchies

Description — *Optional*

Tier

Parameter Store offers standard and advanced parameters.

[✓ Standard] Store up to 10,000 standard parameters. Store parameter values up to 4 KB. Parameter policies and sharing with other AWS accounts are not available. No additional charge.

Advanced: Store up to 100,000 advanced parameters. Store parameter values up to 8 KB. Add parameter policies. Share with other AWS accounts. Charges apply.

Standard parameters cannot be shared with other AWS accounts. Learn more

Type

[✓ String] Any string value.

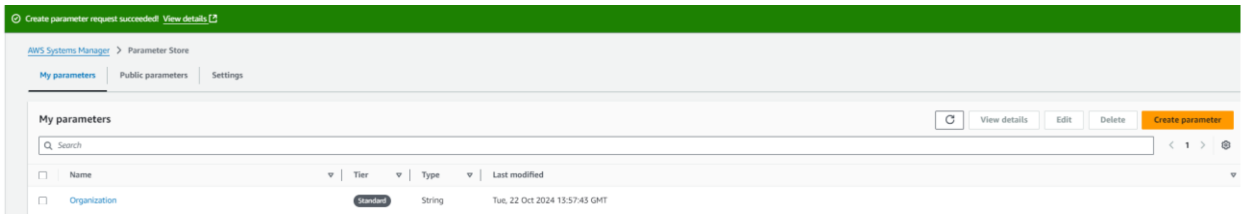
StringList: Separate strings using commas.

SecureString: Encrypt sensitive data using KMS keys from your account or another account.

Data type: text

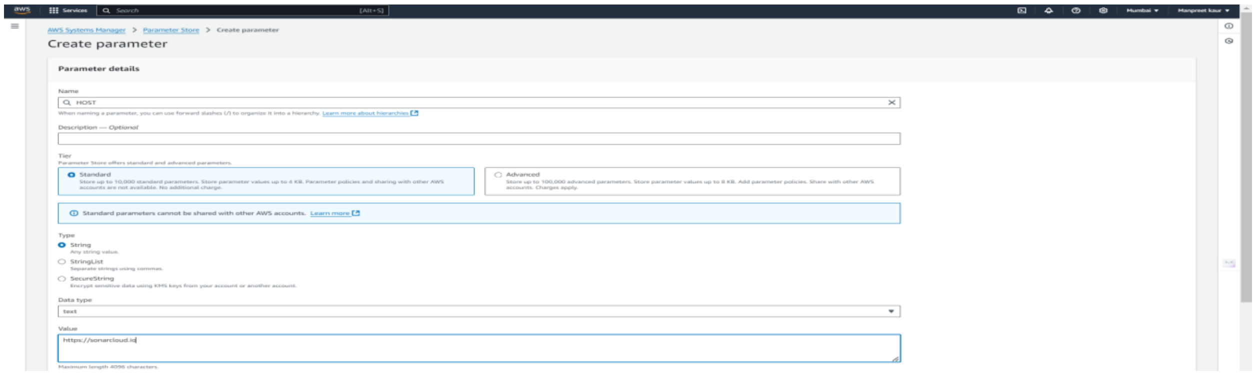
Value: rajee-vprofile

Maximum length 4096 characters.


Create parameter request succeeded! View details

My parameters

Name	Tier	Type	Last modified
Organization	Standard	String	Tue, 22 Oct 2024 13:57:43 GMT


AWS Systems Manager > Parameter Store > Create parameter

Create parameter

Parameter details

Name: HOST

When naming a parameter, you can use forward slashes (/) to organize it into a hierarchy. Learn more about hierarchies

Description — Optional

Tier: Parameter Store offers standard and advanced parameters.

- [✓ Standard] Store up to 10,000 standard parameters. Store parameter values up to 4 KB. Parameter policies and sharing with other AWS accounts are not available. No additional charge.
- Advanced: Store up to 100,000 advanced parameters. Store parameter values up to 8 KB. Add parameter policies. Share with other AWS accounts. Charges apply.

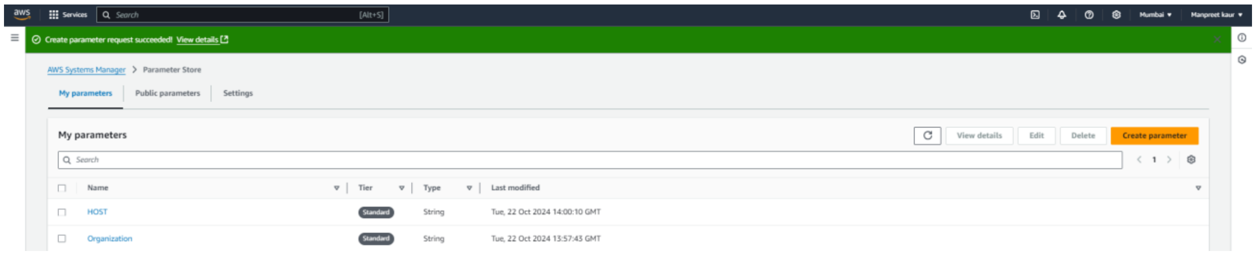
Standard parameters cannot be shared with other AWS accounts. Learn more

Type:
- [✓ String] Any string value.
- StringList: Separate strings using commas.
- SecureString: Encrypt sensitive data using KMS keys from your account or another account.

Data type: text

Value: https://sonarcloud.io

Maximum length 4096 characters.

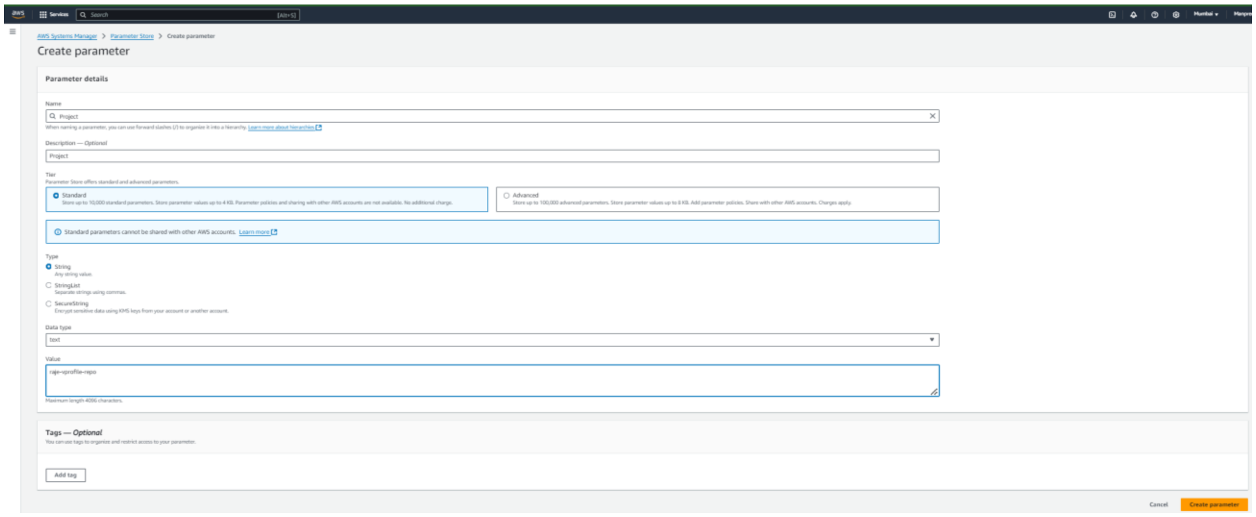

Create parameter request succeeded! View details

AWS Systems Manager > Parameter Store

My parameters | Public parameters | Settings

My parameters

Name	Tier	Type	Last modified
HOST	Standard	String	Tue, 22 Oct 2024 14:00:10 GMT
Organization	Standard	String	Tue, 22 Oct 2024 13:57:43 GMT


AWS Systems Manager > Parameter Store > Create parameter

Create parameter

Parameter details

Name: Project

When naming a parameter, you can use forward slashes (/) to organize it into a hierarchy. Learn more about hierarchies

Description — Optional: Project

Tier: Parameter Store offers standard and advanced parameters.

- [✓ Standard] Store up to 10,000 standard parameters. Store parameter values up to 4 KB. Parameter policies and sharing with other AWS accounts are not available. No additional charge.
- Advanced: Store up to 100,000 advanced parameters. Store parameter values up to 8 KB. Add parameter policies. Share with other AWS accounts. Charges apply.

Standard parameters cannot be shared with other AWS accounts. Learn more

Type:
- [✓ String] Any string value.
- StringList: Separate strings using commas.
- SecureString: Encrypt sensitive data using KMS keys from your account or another account.

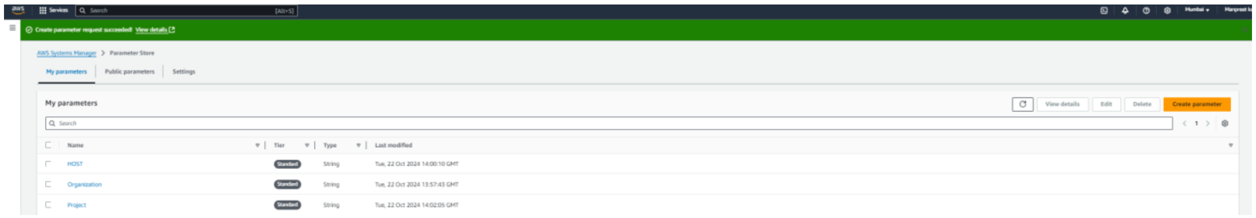
Data type: text

Value: raje-vprofile-repo

Maximum length 4096 characters.

Tags — *Optional*

You can use tags to organize and restrict access to your parameter.

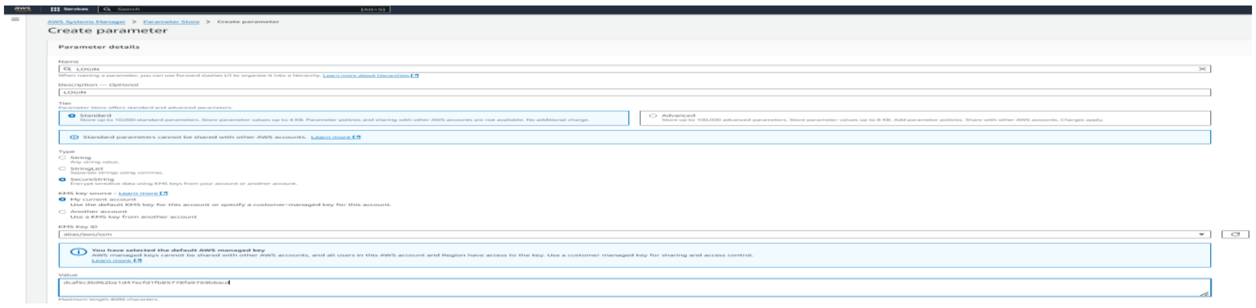

Create parameter request succeeded! View details

AWS Systems Manager > Parameter Store

My parameters | Public parameters | Settings

My parameters

Name	Tier	Type	Last modified
HOST	Standard	String	Tue, 22 Oct 2024 14:00:10 GMT
Organization	Standard	String	Tue, 22 Oct 2024 13:57:43 GMT
Project	Standard	String	Tue, 22 Oct 2024 14:02:05 GMT


AWS Systems Manager > Parameter Store > Create parameter

Create parameter

Parameter details

Name: LOGIN

When naming a parameter, you can use forward slashes (/) to organize it into a hierarchy. Learn more about hierarchies

Description — Optional: LOGIN

Tier: Parameter Store offers standard and advanced parameters.

- [✓ Standard] Store up to 10,000 standard parameters. Store parameter values up to 4 KB. Parameter policies and sharing with other AWS accounts are not available. No additional charge.
- Advanced: Store up to 100,000 advanced parameters. Store parameter values up to 8 KB. Add parameter policies. Share with other AWS accounts. Charges apply.

Standard parameters cannot be shared with other AWS accounts. Learn more

Type:
- String: Any string value.
- StringList: Separate strings using commas.
- [✓ SecureString] Encrypt sensitive data using KMS keys from your account or another account.

KMS key source - Learn more
- [✓ My current account] Use the default KMS key for this account or specify a customer-managed key for this account.
- Another account: Use a KMS key from another account

KMS Key ID: alias/aws/ssm

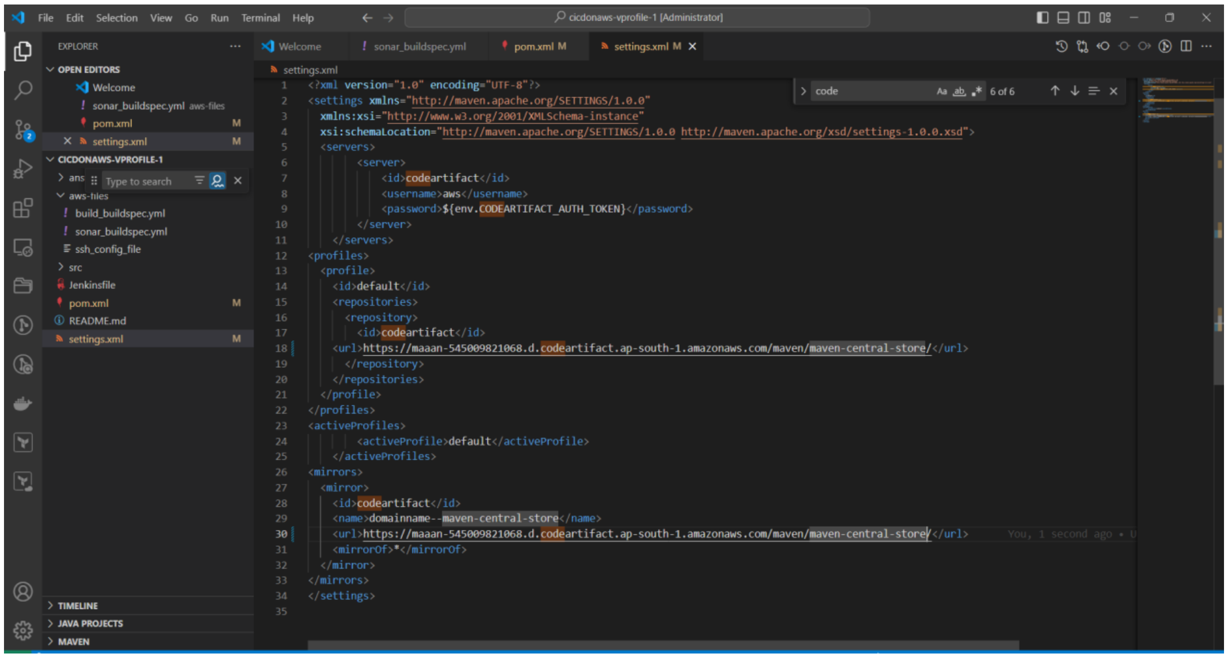
You have selected the default AWS managed key
AWS managed keys cannot be shared with other AWS accounts, and all users in this AWS account and Region have access to the key. Use a customer managed key for sharing and access control.
Learn more

Value: dcaf5c3b962ba1d47ecfd1fb85778fa9759b6acd

Maximum length 4096 characters.

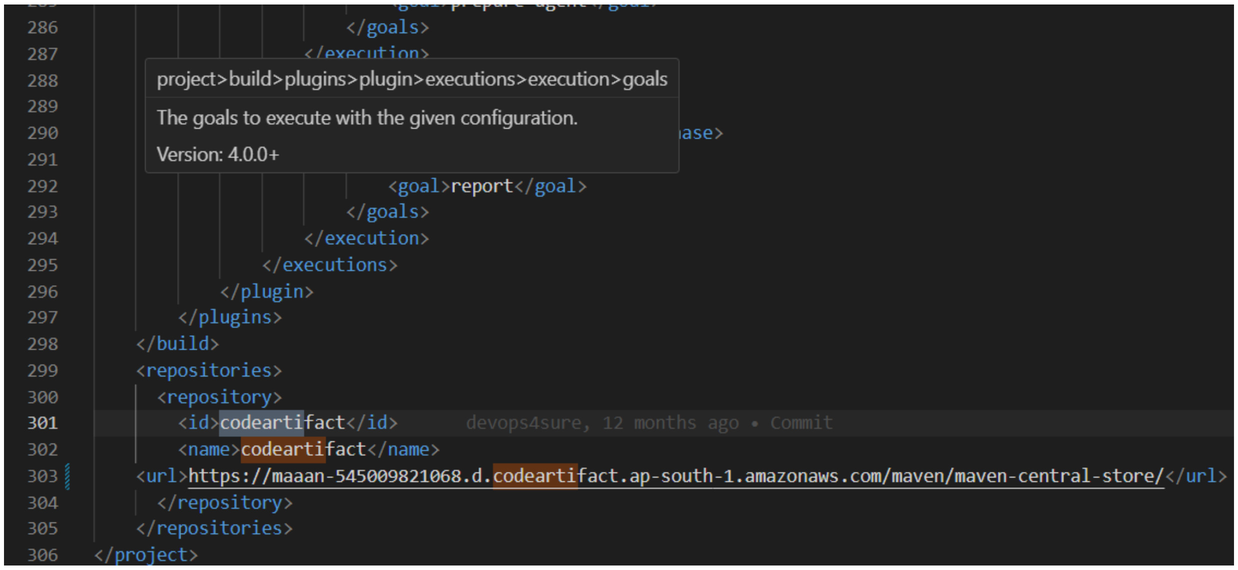
Now we will be creating a code build project which is same as crerating the jenkins job for automating the continous integration process and build the jobs: -

Now you need to create the changes in the repository url as mentioned in the below ss in the settings.xml file on your local: -



```xml
<?xml version="1.0" encoding="UTF-8"?>
<settings xmlns="http://maven.apache.org/SETTINGS/1.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/SETTINGS/1.0.0 http://maven.apache.org/xsd/settings-1.0.0.xsd">
  <servers>
        <server>
            <id>codeartifact</id>
            <username>aws</username>
            <password>${env.CODEARTIFACT_AUTH_TOKEN}</password>
        </server>
    </servers>
<profiles>
  <profile>
    <id>default</id>
    <repositories>
      <repository>
        <id>codeartifact</id>
    <url>https://maaan-545009821068.d.codeartifact.ap-south-1.amazonaws.com/maven/maven-central-store/</url>
      </repository>
    </repositories>
  </profile>
</profiles>
<activeProfiles>
        <activeProfile>default</activeProfile>
    </activeProfiles>
<mirrors>
  <mirror>
    <id>codeartifact</id>
    <name>domainname--maven-central-store</name>
    <url>https://maaan-545009821068.d.codeartifact.ap-south-1.amazonaws.com/maven/maven-central-store/</url>
    <mirrorOf>*</mirrorOf>
  </mirror>
</mirrors>
</settings>
```

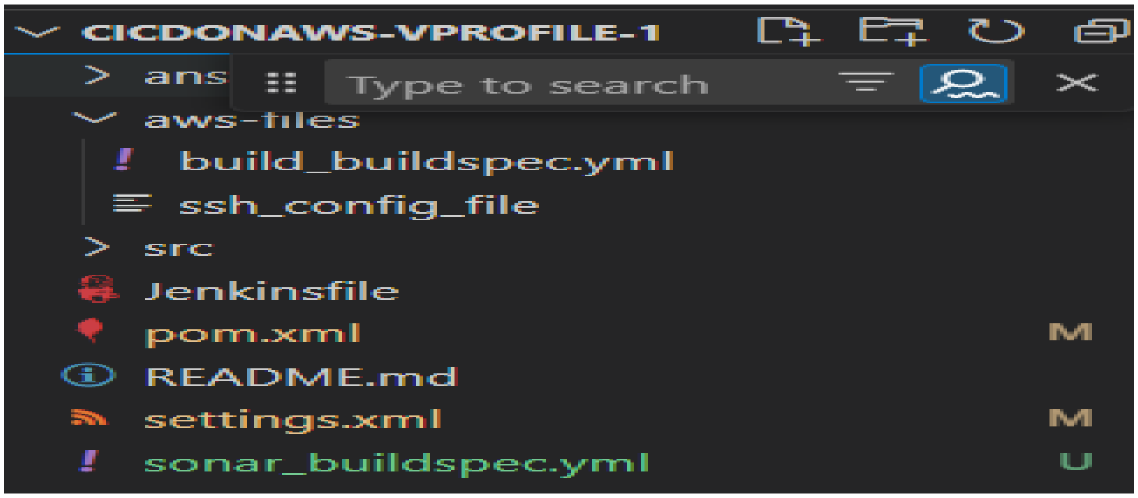
changes made in the pox.xml file: -



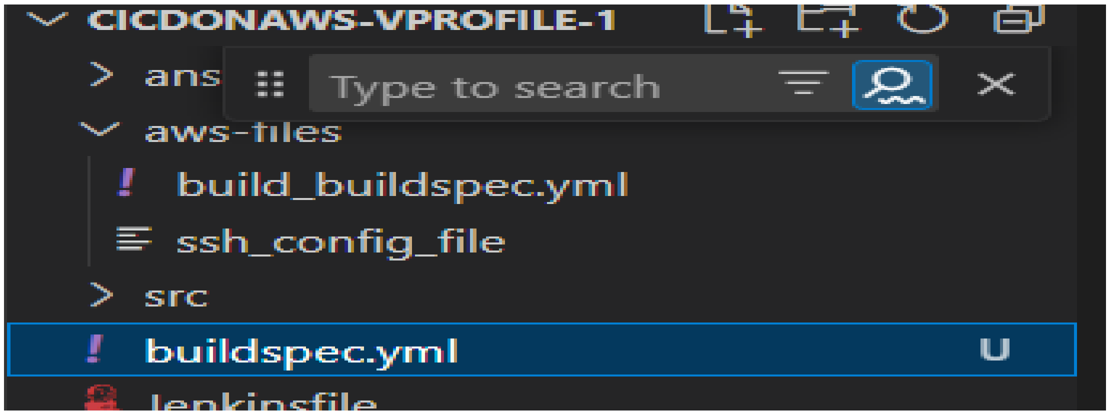
```xml
                </goals>
              </execution>
project>build>plugins>plugin>executions>execution>goals
The goals to execute with the given configuration.
Version: 4.0.0+
                                                 ase>
                  <goal>report</goal>
                </goals>
              </execution>
            </executions>
          </plugin>
        </plugins>
    </build>
    <repositories>
      <repository>
        <id>codeartifact</id>      devops4sure, 12 months ago • Commit
        <name>codeartifact</name>
    <url>https://maaan-545009821068.d.codeartifact.ap-south-1.amazonaws.com/maven/maven-central-store/</url>
      </repository>
    </repositories>
</project>
```

fix pom.xml,settings.xml then you need to fix the sonar-buildspec.xml

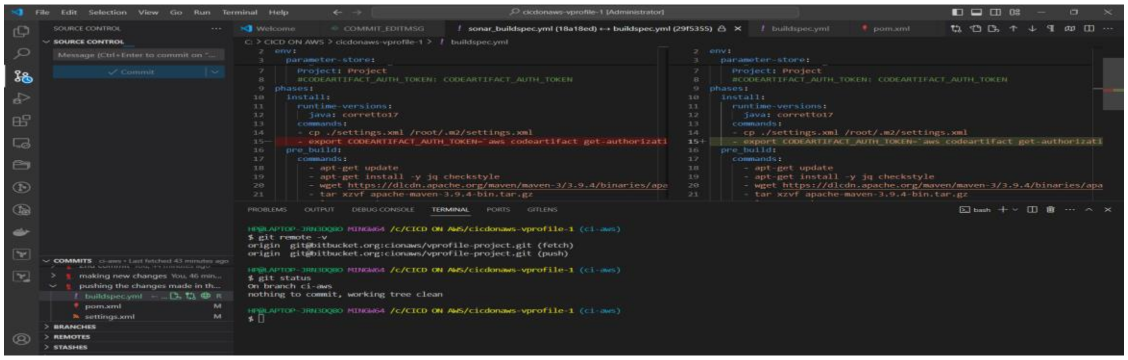
Drag the sonar build.xml file in the root directory where the other files are placed: -



and now we need to rename the above file to buildspec.yml as below:-



now you need to push the changes made and directly commit and push into the bitbuclet repository you configured:-

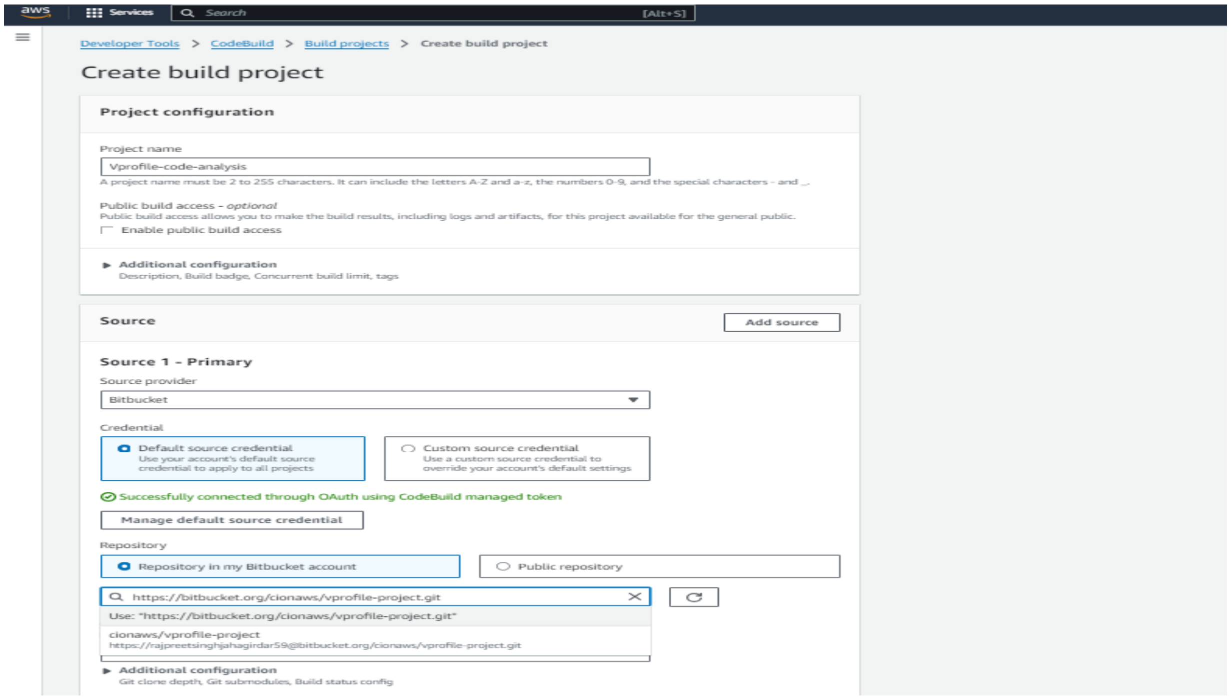

cicdonaws-vprofile-1 [Administrator]
Welcome
COMMIT_EDITMSG
sonar_buildspec.yml (18a18ed) ↔ buildspec.yml (29f5355)
buildspec.yml
pom.xml
C: > CICD ON AWS > cicdonaws-vprofile-1 > buildspec.yml
SOURCE CONTROL
Commit
COMMITS
BRANCHES
REMOTES
STASHES
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
GITLENS

```
env:
  parameter-store:
    Project: Project
    #CODEARTIFACT_AUTH_TOKEN: CODEARTIFACT_AUTH_TOKEN
phases:
  install:
    runtime-versions:
      java: corretto17
    commands:
    - cp ./settings.xml /root/.m2/settings.xml
    - export CODEARTIFACT_AUTH_TOKEN=`aws codeartifact get-authorizati
  pre_build:
    commands:
      - apt-get update
      - apt-get install -y jq checkstyle
      - wget https://dlcdn.apache.org/maven/maven-3/3.9.4/binaries/apa
      - tar xzvf apache-maven-3.9.4-bin.tar.gz
```

```
HP@LAPTOP-JRN3DQ8O MINGW64 /c/CICD ON AWS/cicdonaws-vprofile-1 (ci-aws)
$ git remote -v
origin  git@bitbucket.org:cionaws/vprofile-project.git (fetch)
origin  git@bitbucket.org:cionaws/vprofile-project.git (push)

HP@LAPTOP-JRN3DQ8O MINGW64 /c/CICD ON AWS/cicdonaws-vprofile-1 (ci-aws)
$ git status
On branch ci-aws
nothing to commit, working tree clean

HP@LAPTOP-JRN3DQ8O MINGW64 /c/CICD ON AWS/cicdonaws-vprofile-1 (ci-aws)
$ 
```

by clicking on the src ctrl button on the left pannel which will commit and push the changes to our bitbucket repo:-

Now we will be build our job in the aws code build in the same manner we used to do it in the jenkins to create the job:-



Developer Tools > CodeBuild > Build projects > Create build project

Create build project

Project configuration

Project name: Vprofile-code-analysis
A project name must be 2 to 255 characters. It can include the letters A-Z and a-z, the numbers 0-9, and the special characters - and _.

Public build access - *optional*
Public build access allows you to make the build results, including logs and artifacts, for this project available for the general public.
Enable public build access

Additional configuration
Description, Build badge, Concurrent build limit, tags

Source

Source 1 - Primary
Source provider: Bitbucket

Credential: Default source credential (Use your account's default source credential to apply to all projects) / Custom source credential (Use a custom source credential to override your account's default settings)

Successfully connected through OAuth using CodeBuild managed token

Manage default source credential

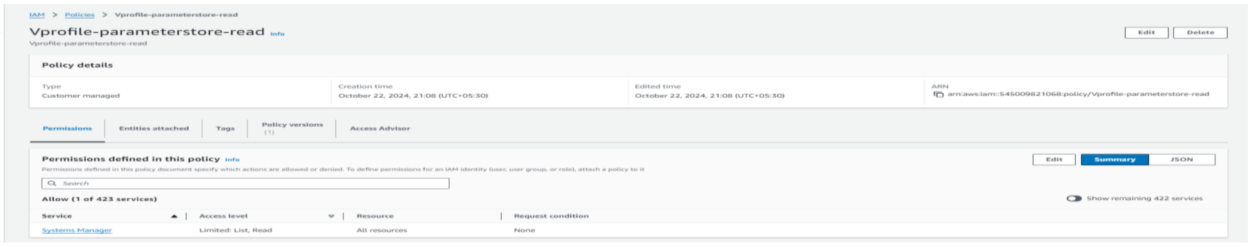
Repository: Repository in my Bitbucket account / Public repository

https://bitbucket.org/cionaws/vprofile-project.git
Use: "https://bitbucket.org/cionaws/vprofile-project.git"
cionaws/vprofile-project
https://rajpreetsinghjahagirdar59@bitbucket.org/cionaws/vprofile-project.git

Additional configuration
Git clone depth, Git submodules, Build status config

we will connect the code build with our bitbucket repo by o auth authorization process.

Now we will be modifying our service role which is attached to code build to access the aws system manger parameter store plz refer below ss for the same:-
we need to create the policy with the required permissions and attach the same to the service role which is been used by our aws codebuild:-



IAM > Policies > Vprofile-parameterstore-read

Vprofile-parameterstore-read
Vprofile-parameterstore-read

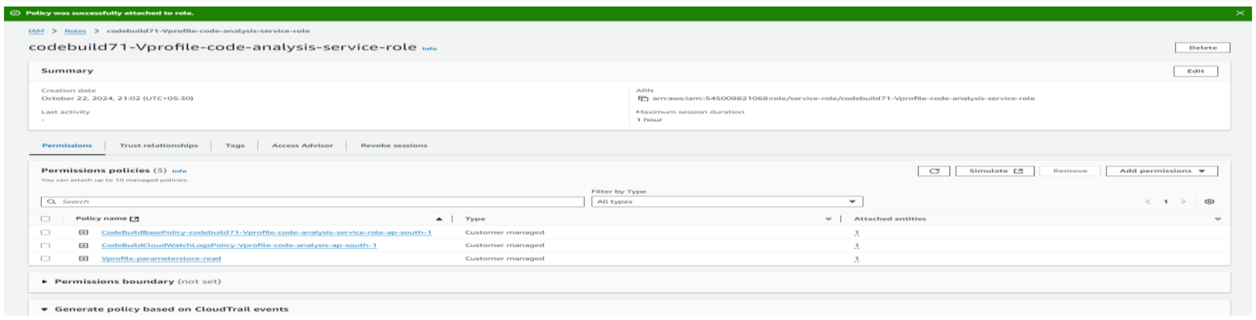
Policy details

Type	Creation time	Edited time	ARN
Customer managed	October 22, 2024, 21:08 (UTC+05:30)	October 22, 2024, 21:08 (UTC+05:30)	arn:aws:iam::545009821068:policy/Vprofile-parameterstore-read

Permissions defined in this policy
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 423 services)
Show remaining 422 services

Service	Access level	Resource	Request condition
Systems Manager	Limited: List, Read	All resources	None



Policy was successfully attached to role.

IAM > Roles > codebuild71-Vprofile-code-analysis-service-role

codebuild71-Vprofile-code-analysis-service-role

Summary

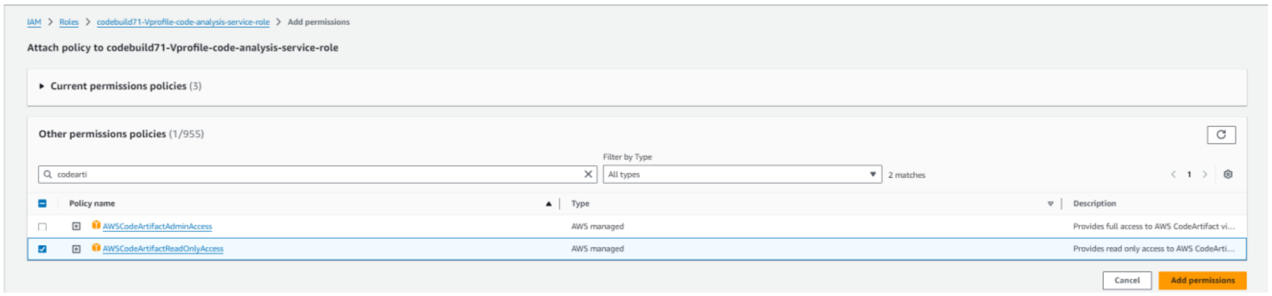
Creation date: October 22, 2024, 21:02 (UTC+05:30)
Last activity: -
ARN: arn:aws:iam::545009821068:role/service-role/codebuild71-Vprofile-code-analysis-service-role
Maximum session duration: 1 hour

Permissions policies (3)
You can attach up to 10 managed policies.
Filter by Type: All types

Policy name	Type	Attached entities
CodeBuildBasePolicy-codebuild71-Vprofile-code-analysis-service-role-ap-south-1	Customer managed	1
CodeBuildCloudWatchLogsPolicy-Vprofile-code-analysis-ap-south-1	Customer managed	1
Vprofile-parameterstore-read	Customer managed	1

Permissions boundary (not set)

Generate policy based on CloudTrail events



IAM > Roles > codebuild71-Vprofile-code-analysis-service-role > Add permissions

Attach policy to codebuild71-Vprofile-code-analysis-service-role

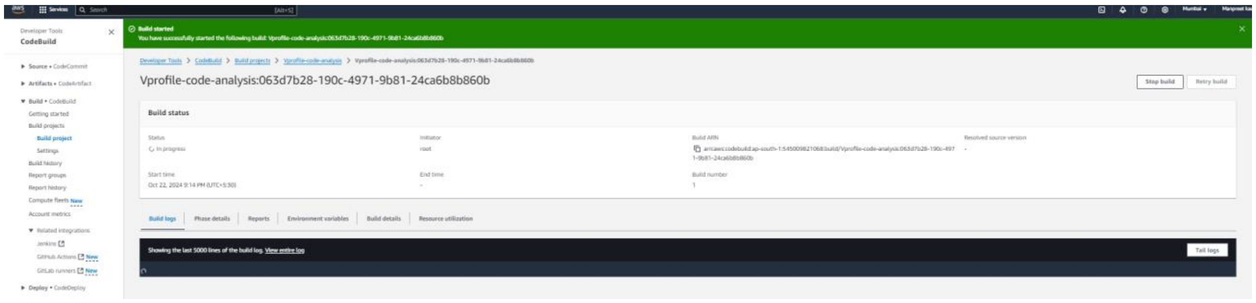
Current permissions policies (3)

Other permissions policies (1/955)

Filter by Type: All types — codearti — 2 matches

	Policy name	Type	Description
☐	AWSCodeArtifactAdminAccess	AWS managed	Provides full access to AWS CodeArtifact vi...
☑	AWSCodeArtifactReadOnlyAccess	AWS managed	Provides read only access to AWS CodeArti...

we also need to add the code artifact read only access to our role so that it may access our code artifact to use the dependencies to build the project using maven dep.



Build started
You have successfully started the following build: Vprofile-code-analysis:063d7b28-190c-4971-9b81-24ca6b8b860b

Developer Tools > CodeBuild > Build projects > Vprofile-code-analysis > Vprofile-code-analysis:063d7b28-190c-4971-9b81-24ca6b8b860b

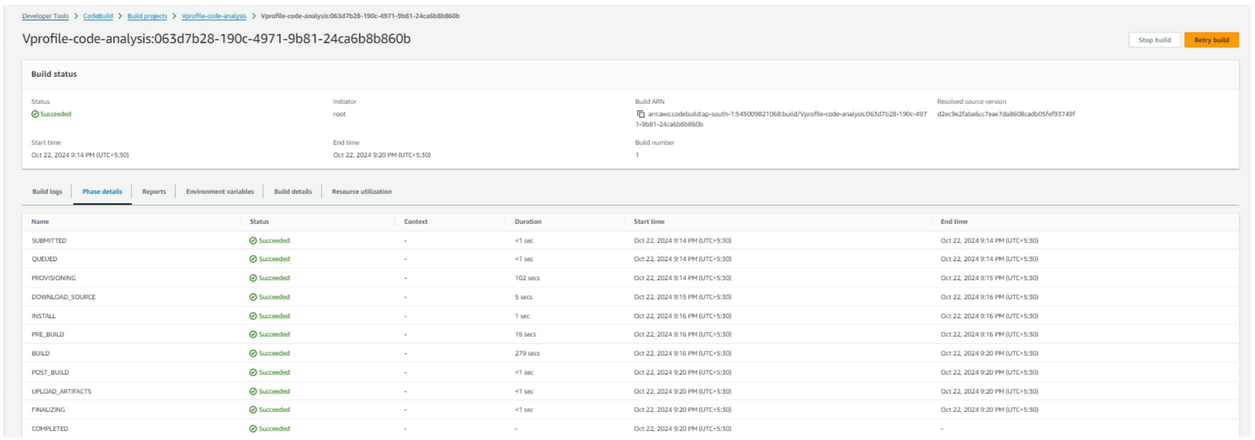
Vprofile-code-analysis:063d7b28-190c-4971-9b81-24ca6b8b860b

Build status

Status	Initiator	Build ARN	Resolved source version
In progress	root	arn:aws:codebuild:ap-south-1:545009821068:build/Vprofile-code-analysis:063d7b28-190c-4971-9b81-24ca6b8b860b	-

Start time	End time	Build number
Oct 22, 2024 9:14 PM (UTC+5:30)	-	1

Showing the last 5000 lines of the build log. View entire log



Developer Tools > CodeBuild > Build projects > Vprofile-code-analysis > Vprofile-code-analysis:063d7b28-190c-4971-9b81-24ca6b8b860b

Vprofile-code-analysis:063d7b28-190c-4971-9b81-24ca6b8b860b

Build status

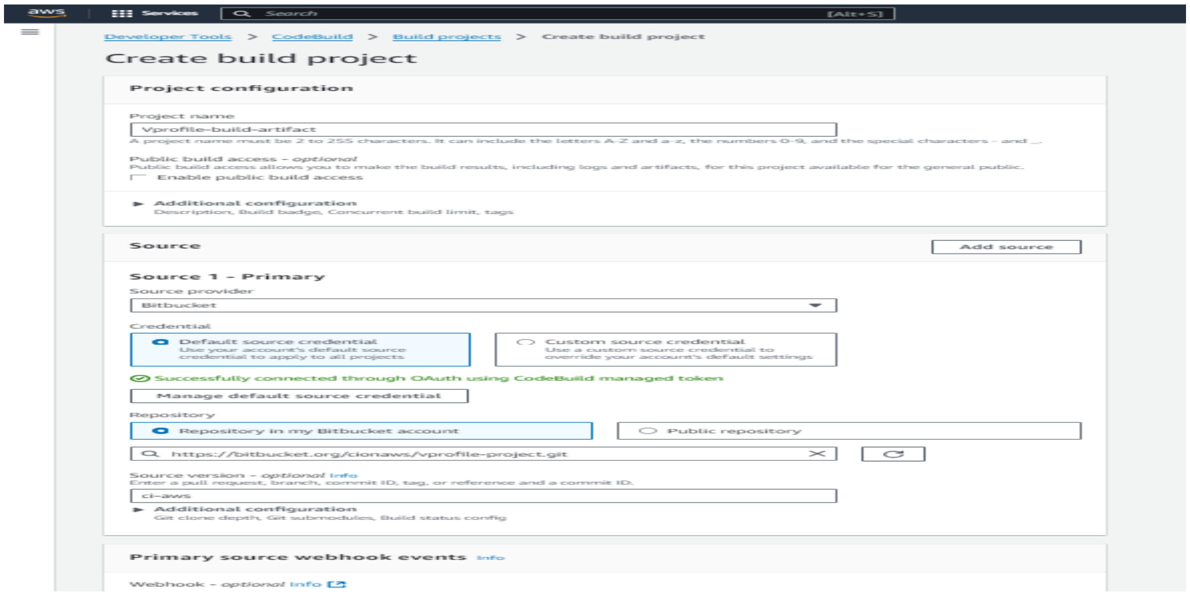
Status	Initiator	Build ARN	Resolved source version
Succeeded	root	arn:aws:codebuild:ap-south-1:545009821068:build/Vprofile-code-analysis:063d7b28-190c-4971-9b81-24ca6b8b860b	d2ec9e2faba6cc7eae7da8608cadb05fef93749f

Start time	End time	Build number
Oct 22, 2024 9:14 PM (UTC+5:30)	Oct 22, 2024 9:20 PM (UTC+5:30)	1

Name	Status	Context	Duration	Start time	End time
SUBMITTED	Succeeded	-	<1 sec	Oct 22, 2024 9:14 PM (UTC+5:30)	Oct 22, 2024 9:14 PM (UTC+5:30)
QUEUED	Succeeded	-	<1 sec	Oct 22, 2024 9:14 PM (UTC+5:30)	Oct 22, 2024 9:14 PM (UTC+5:30)
PROVISIONING	Succeeded	-	102 secs	Oct 22, 2024 9:14 PM (UTC+5:30)	Oct 22, 2024 9:15 PM (UTC+5:30)
DOWNLOAD_SOURCE	Succeeded	-	5 secs	Oct 22, 2024 9:15 PM (UTC+5:30)	Oct 22, 2024 9:16 PM (UTC+5:30)
INSTALL	Succeeded	-	1 sec	Oct 22, 2024 9:16 PM (UTC+5:30)	Oct 22, 2024 9:16 PM (UTC+5:30)
PRE_BUILD	Succeeded	-	16 secs	Oct 22, 2024 9:16 PM (UTC+5:30)	Oct 22, 2024 9:16 PM (UTC+5:30)
BUILD	Succeeded	-	279 secs	Oct 22, 2024 9:16 PM (UTC+5:30)	Oct 22, 2024 9:20 PM (UTC+5:30)
POST_BUILD	Succeeded	-	<1 sec	Oct 22, 2024 9:20 PM (UTC+5:30)	Oct 22, 2024 9:20 PM (UTC+5:30)
UPLOAD_ARTIFACTS	Succeeded	-	<1 sec	Oct 22, 2024 9:20 PM (UTC+5:30)	Oct 22, 2024 9:20 PM (UTC+5:30)
FINALIZING	Succeeded	-	<1 sec	Oct 22, 2024 9:20 PM (UTC+5:30)	Oct 22, 2024 9:20 PM (UTC+5:30)
COMPLETED	Succeeded	-	-	Oct 22, 2024 9:20 PM (UTC+5:30)	-

Now we will be building the other job for code artifact token auotharization and taking the dependencies from code artifact and building the artifact and pushing it to the code artifact repository we have created.

Now we will be creating the new code build project for this stage: -



Developer Tools > CodeBuild > Build projects > Create build project

Create build project

Project configuration

Project name: Vprofile-build-artifact

A project name must be 2 to 255 characters. It can include the letters A-Z and a-z, the numbers 0-9, and the special characters - and _.

Public build access - *optional*

Public build access allows you to make the build results, including logs and artifacts, for this project available for the general public.

Enable public build access

Additional configuration: Description, Build badge, Concurrent build limit, tags

Source

Source 1 - Primary

Source provider: Bitbucket

Credential: [✓ Default source credential — Use your account's default source credential to apply to all projects] Custom source credential — Use a custom source credential to override your account's default settings

Successfully connected through OAuth using CodeBuild managed token

Manage default source credential

Repository: [✓ Repository in my Bitbucket account] Public repository

https://bitbucket.org/cionaws/vprofile-project.git

Source version - *optional*: Enter a pull request, branch, commit ID, tag, or reference and a commit ID.

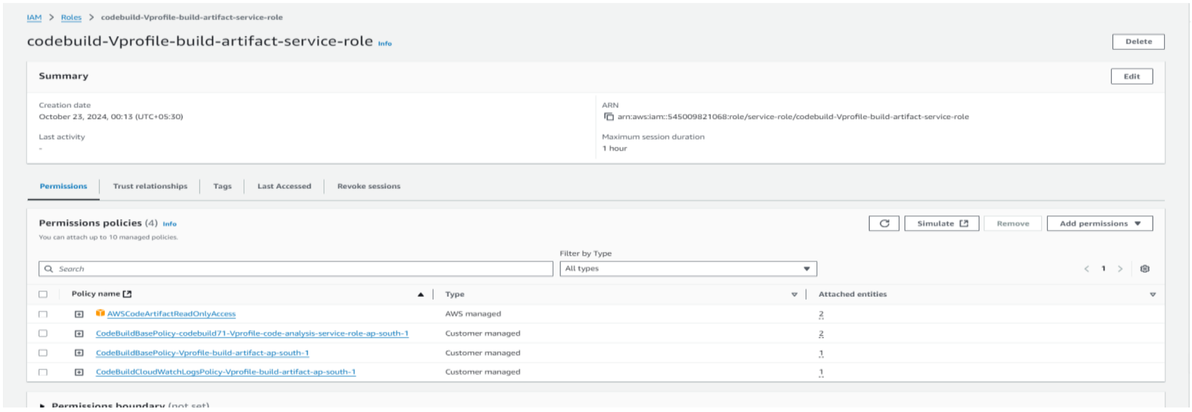
ci-aws

Additional configuration: Git clone depth, Git submodules, Build status config

Primary source webhook events

Webhook - *optional*

for the service role we will attach the same policies which we have attached to the previos build for code ananlysis that its plz find below ss for the same:-



IAM > Roles > codebuild-Vprofile-build-artifact-service-role

codebuild-Vprofile-build-artifact-service-role

Summary

Creation date: October 23, 2024, 00:13 (UTC+05:30)

Last activity: -

ARN: arn:aws:iam::545009821068:role/service-role/codebuild-Vprofile-build-artifact-service-role

Maximum session duration: 1 hour

Permissions | Trust relationships | Tags | Last Accessed | Revoke sessions

Permissions policies (4)

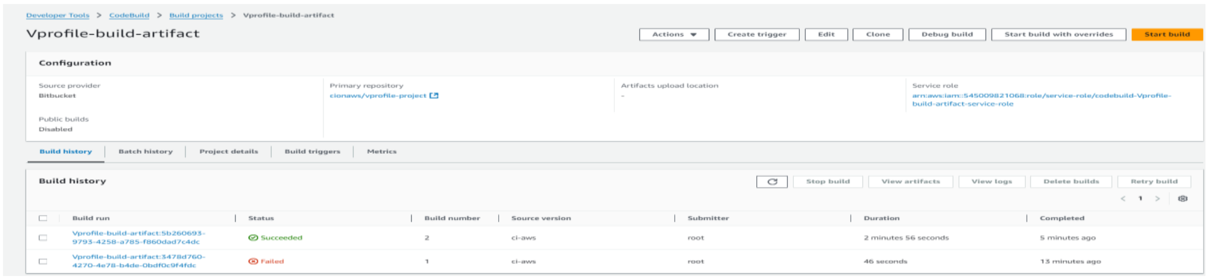
You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
AWSCodeArtifactReadOnlyAccess	AWS managed	2
CodeBuildBasePolicy-codebuild71-Vprofile-code-analysis-service-role-ap-south-1	Customer managed	2
CodeBuildBasePolicy-Vprofile-build-artifact-ap-south-1	Customer managed	1
CodeBuildCloudWatchLogsPolicy-Vprofile-build-artifact-ap-south-1	Customer managed	1

Permissions boundary (not set)

now after doing all the changes and configurations we will be finally click o start building our project and wait for the logs and click on the build phase to check the stages while it is exicuting steps by steps and in my case it is successfull after one failure because previously the service role was not having the enough permissions attached to it then i modified the role permissions and rebuild the build project then it got succeeded plz find the below ss for the your reference:-



Developer Tools > CodeBuild > Build projects > Vprofile-build-artifact

Vprofile-build-artifact

Configuration

Source provider: Bitbucket

Public builds: Disabled

Primary repository: cionaws/vprofile-project

Artifacts upload location: -

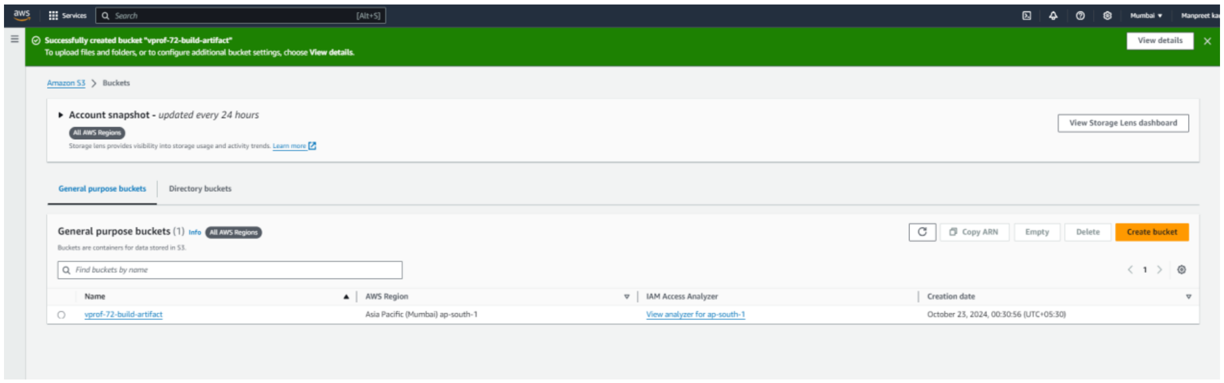
Service role: arn:aws:iam::545009821068:role/service-role/codebuild-Vprofile-build-artifact-service-role

Build history | Batch history | Project details | Build triggers | Metrics

Build history

Build run	Status	Build number	Source version	Submitter	Duration	Completed
Vprofile-build-artifact:5b260693-9793-4258-a785-f860dad7c4dc	Succeeded	2	ci-aws	root	2 minutes 56 seconds	5 minutes ago
Vprofile-build-artifact:3478d760-4270-4e78-b4de-0bdf0c9f4fdc	Failed	1	ci-aws	root	46 seconds	13 minutes ago

Now we will be creating the s3 bucket for storing the build artifacts in the same:-



Successfully created bucket "vprof-72-build-artifact"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

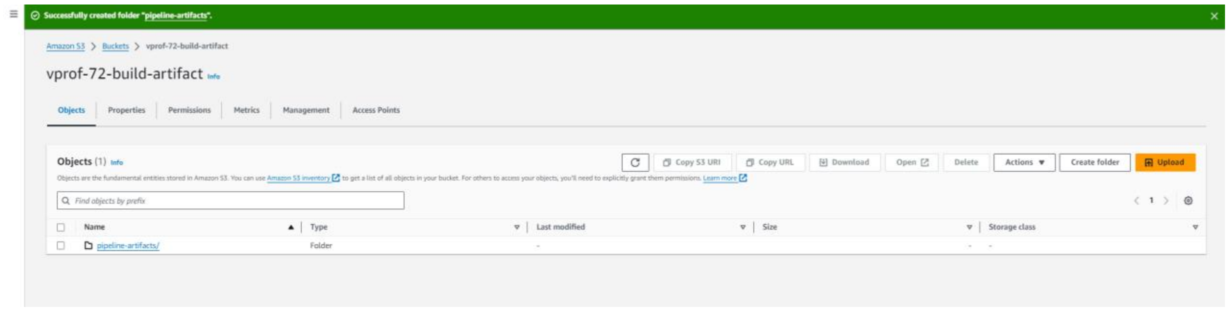
Amazon S3 > Buckets

Account snapshot - *updated every 24 hours*
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info All AWS Regions
Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
vprof-72-build-artifact	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	October 23, 2024, 00:30:56 (UTC+05:30)

now we will be creating the folder inside the same bucket which will be storing our build artifacts in the same: -


Successfully created folder "pipeline-artifacts".

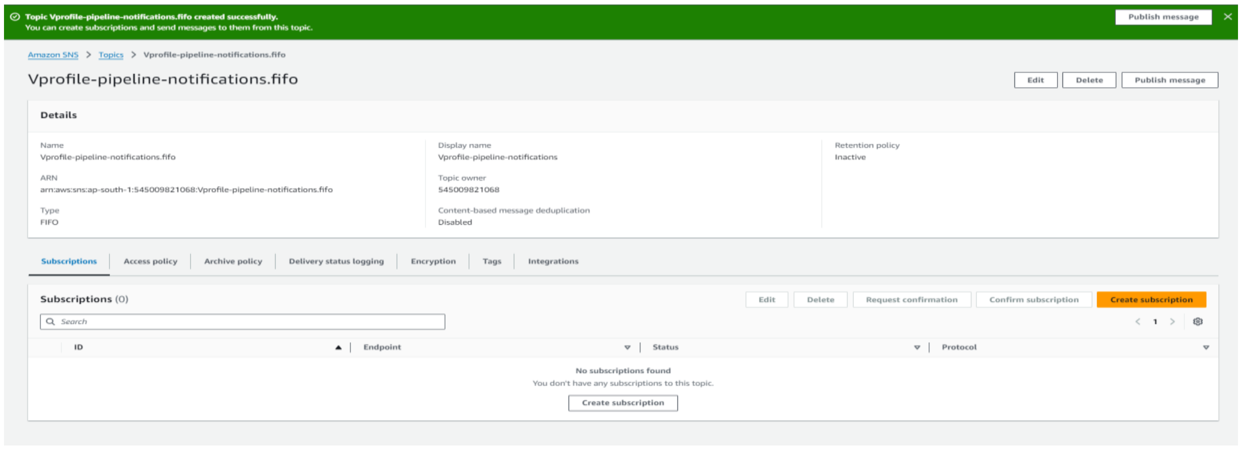
Amazon S3 > Buckets > vprof-72-build-artifact

vprof-72-build-artifact Info

Objects (1) Info
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
pipeline-artifacts/	Folder	-	-	-

Next service we will be setting up id sns (simple notification service which we will be using to send the build results notifications to the dev if its pass or fail so that the dev may made the changes and commit those to get it resolved asap: -


Topic Vprofile-pipeline-notifications.fifo created successfully.
You can create subscriptions and send messages to them from this topic.

Amazon SNS > Topics > Vprofile-pipeline-notifications.fifo

Vprofile-pipeline-notifications.fifo

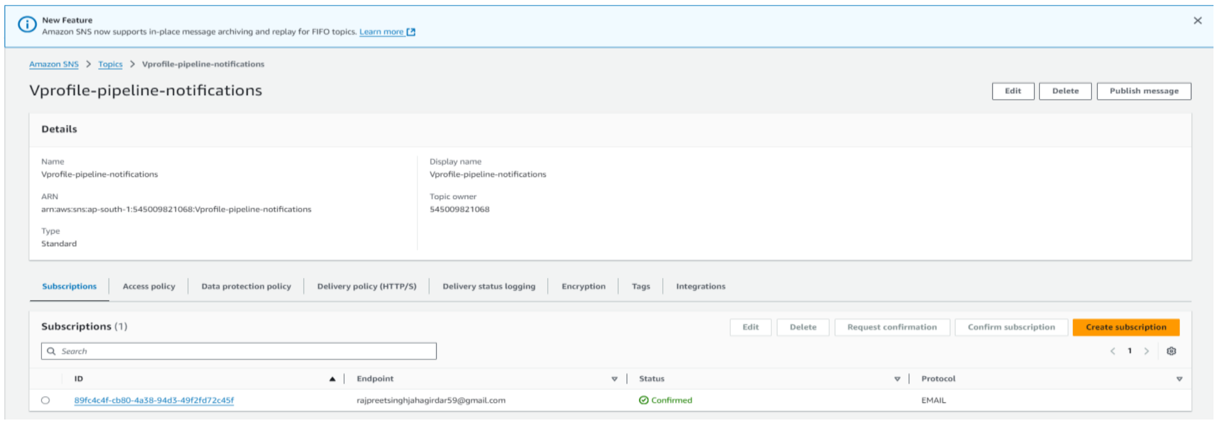
Details

Name Vprofile-pipeline-notifications.fifo	Display name Vprofile-pipeline-notifications	Retention policy Inactive
ARN arn:aws:sns:ap-south-1:545009821068:Vprofile-pipeline-notifications.fifo	Topic owner 545009821068	
Type FIFO	Content-based message deduplication Disabled	

Subscriptions (0)

ID	Endpoint	Status	Protocol

No subscriptions found
You don't have any subscriptions to this topic.


New Feature
Amazon SNS now supports in-place message archiving and replay for FIFO topics. Learn more

Amazon SNS > Topics > Vprofile-pipeline-notifications

Vprofile-pipeline-notifications

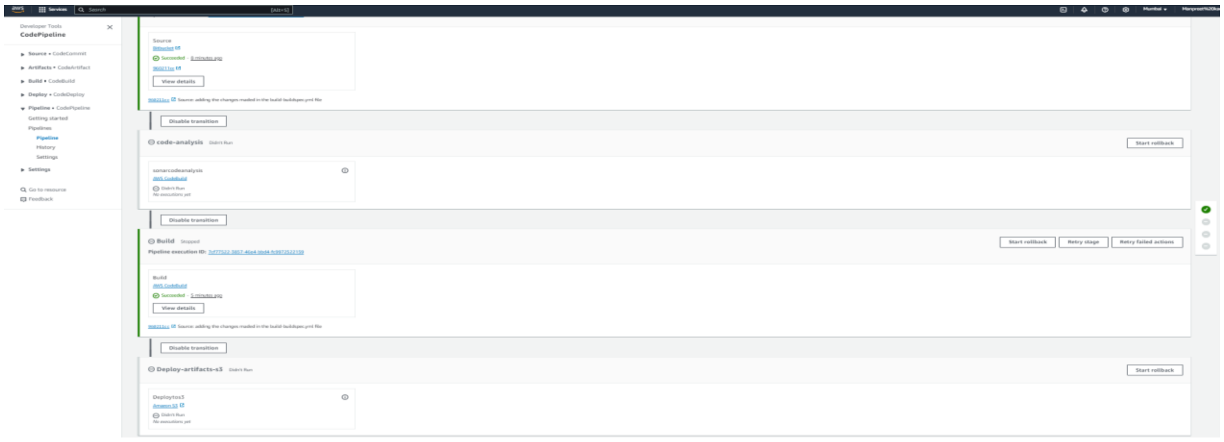
Details

Name: Vprofile-pipeline-notifications	Display name: Vprofile-pipeline-notifications
ARN: arn:aws:sns:ap-south-1:545009821068:Vprofile-pipeline-notifications	Topic owner: 545009821068
Type: Standard	

Subscriptions (1)

ID	Endpoint	Status	Protocol
89fc4c4f-cb80-4a38-94d3-49f2fd72c45f	rajpreetsinghjahagirdar59@gmail.com	Confirmed	EMAIL

now we will be creating the code pipeline which will be binding our all integrations to deploy our application: -

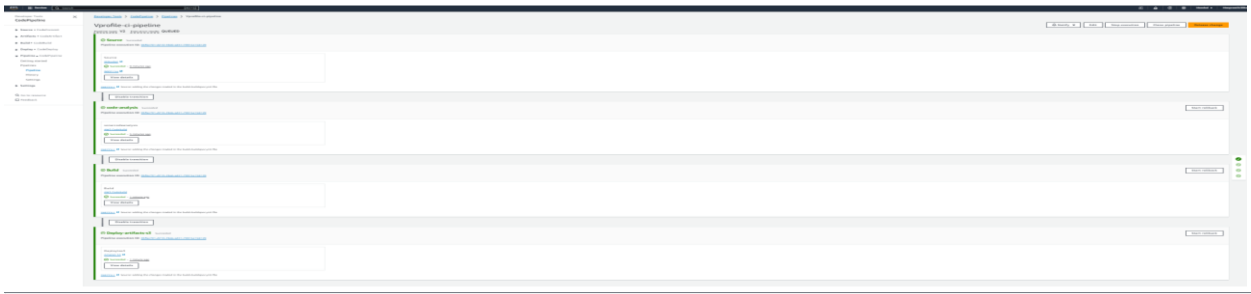

Source
Bitbucket
Succeeded - 8 minutes ago
960211cc
998211cc Source: adding the changes maded in the build-buildspec.yml file

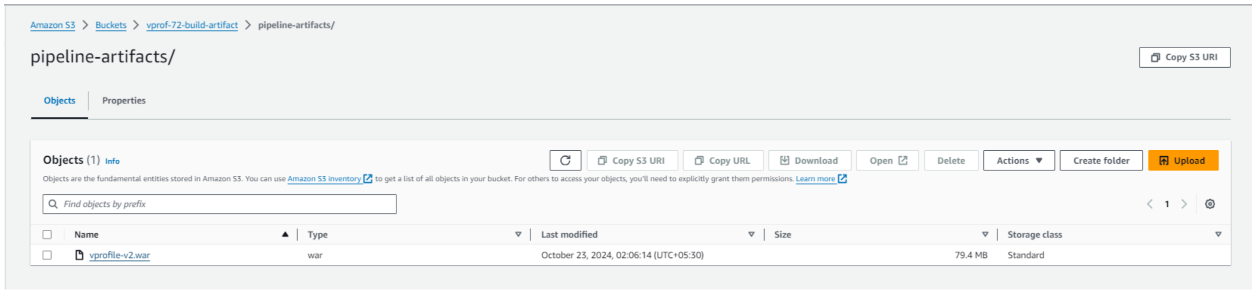
code-analysis Didn't Run
sonarcodeanalysis
AWS CodeBuild
Didn't Run
No executions yet

Build Stopped
Pipeline execution ID: 7cf77522-3857-46e4-bbd4-fc9972522159
Build
AWS CodeBuild
Succeeded - 5 minutes ago
998211cc Source: adding the changes maded in the build-buildspec.yml file

Deploy-artifacts-s3 Didn't Run
Deploytos3
Amazon S3
Didn't Run
No executions yet

now as our pipeline has successfully completed all the stages and now our artifacts are been stored into the s3 bucket as we designed our architecture: -



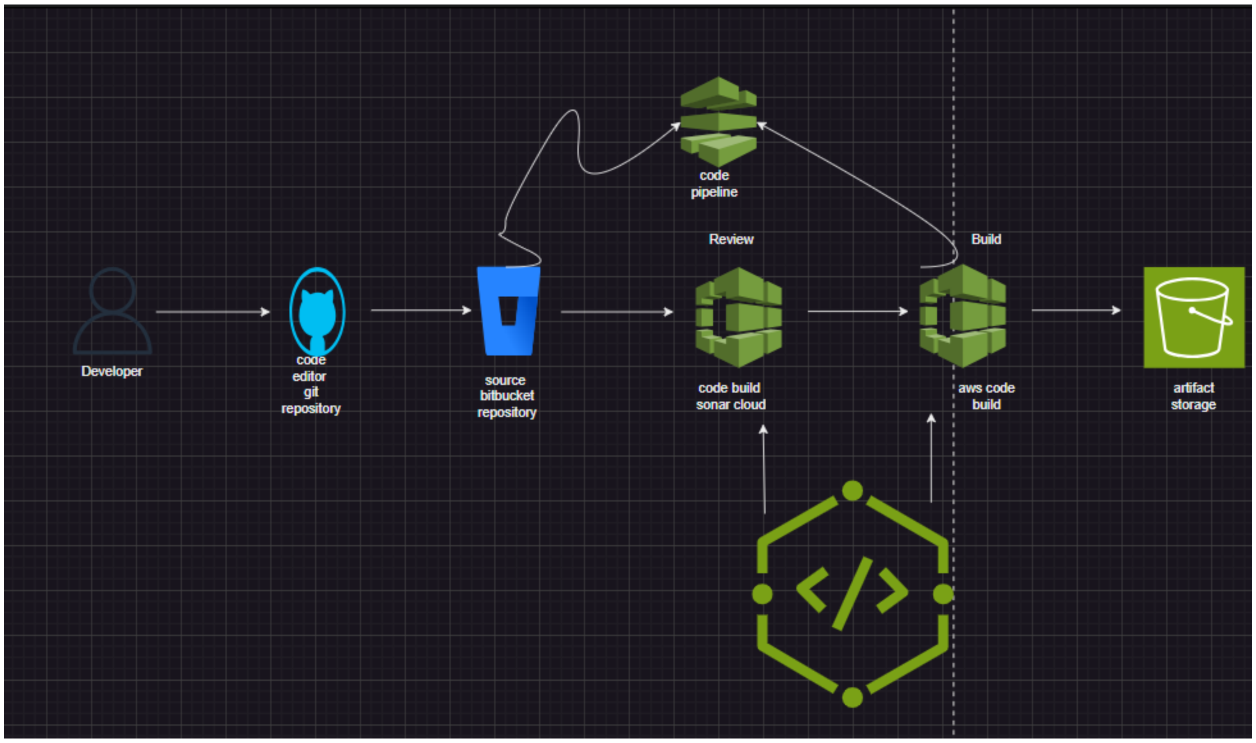

Amazon S3 > Buckets > vprof-72-build-artifact > pipeline-artifacts/

pipeline-artifacts/

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Name	Type	Last modified	Size	Storage class
vprofile-v2.war	war	October 23, 2024, 02:06:14 (UTC+05:30)	79.4 MB	Standard



Above is the architecture of our above flow we have folled till now:-