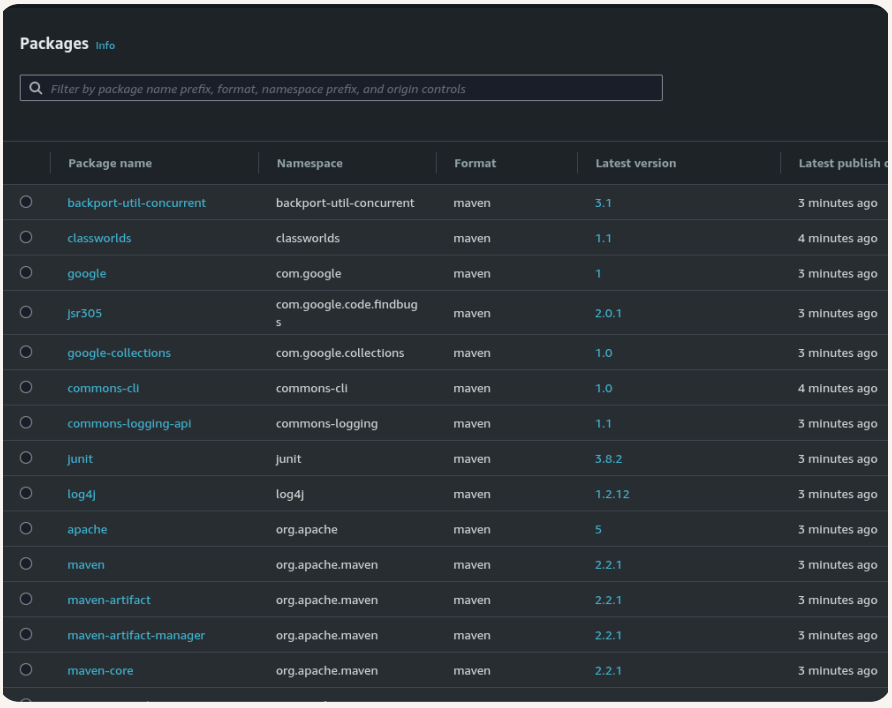
nextwork.org

Secure Packages with CodeArtifact

MA Harish madhavan J U



Introducing Today's Project!

In this project, I will demonstrate how to set up a codeartifact repo and connect it with the web app, I'm doing this project because setting up codeartifact repo will be a valuable step towards building a secure and efficient CI/CD pipleine.

Key tools and concepts

Services I used were Amazon EC2, IAM, CodeArtiFact. Key concepts I learnt include creating codeartifact repo and domain, creating roles using policies and attatching them to EC2 instance.

Project reflection

This project tooke me approximately 120 min to complete. The most challenging part was connecting EC2 instance with VS code and it was most rewarding to keep the CPU utilisation of instance under 100 :)

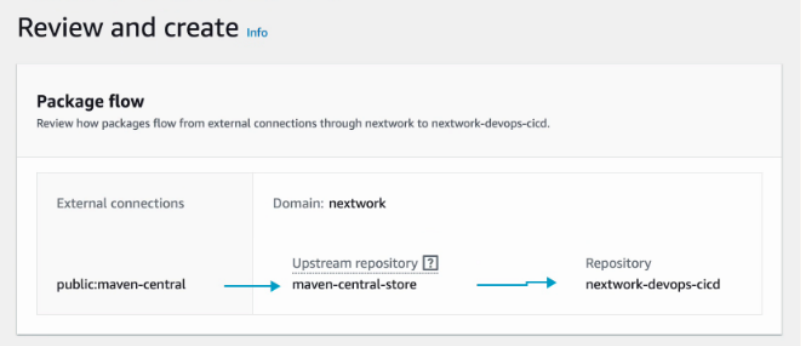
This project is part three of a series of DevOps projects where I'm building a CI/CD pipeline! I'll be working on the next project tomorrow

CodeArtifact Repository

Codeartifact is a repository containing packages required while building a web app, this elimnates time invested in building the same package from scratch. Engineering teams use artifact repo because it provides a secure, reliable and consistent access to packages required while devoleping.

A domain is like a folder that contains multiple repos required by a project or organisation. This provides a consistent way to manage security controls and permission across all multiple repo.My domain is devops-hm which contains repos required for our project.

A codeartifact repo can have a upstream repo which means if the package required is not availble locally, it will automatically search and fetch packages from upstream repo, this set up will reduce time taken to build the app after importing necessary packages and ensures reliablity and control. My repository's upstream repository is Maven central because its the central hub of all the java libraries that devolepers publish.


Review and create Info
Package flow
Review how packages flow from external connections through nextwork to nextwork-devops-cicd.
External connections
Domain: nextwork
Upstream repository
Repository
public:maven-central
maven-central-store
nextwork-devops-cicd

MA
Harish madhavan J U
NextWork Student

CodeArtifact Security

Issue

To access codeartifact, we need an authorization token because this will act as a temproary password for the instance to access the resources in codeartifact.I ran into an error when retrieving a token because an EC2 instance does not have permission to access other AWS services. This is a practical example of the principle of least privilege in action.

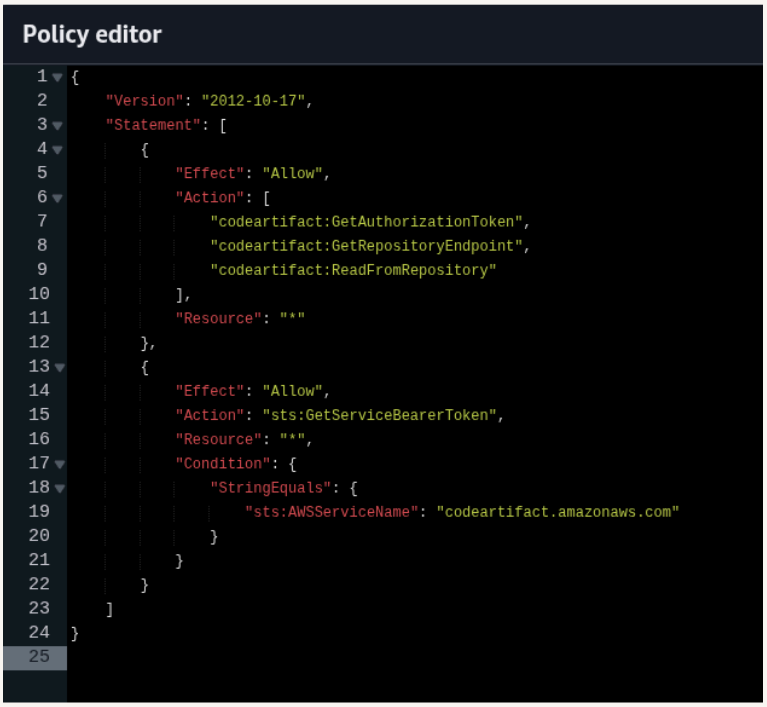
Resolution

To resolve the error with my security token, I had to assign a role to EC2 instance with necessary permissions. This resolved the error because EC2 instances generally dont have permission to access other AWS services, by assuming a role the instance can get access to AWS services.

Using IAM roles is a security best practice because a role can have multiple policies attached to it—each defining a set of permissions. Users or services can assume the role to gain the necessary access. When permissions need to be modified, updating the attached policy automatically affects all users or services that assume the role.

The JSON policy attached to my role

The JSON policy I set up grants permissions to get an authorisation token, retrieve repository endpoints and read from the repository on all possible resources and allows the user to call getservicebearertoken function from AWS Secure Token Service only when the aws service name is codeartifact.amazonaws.com.



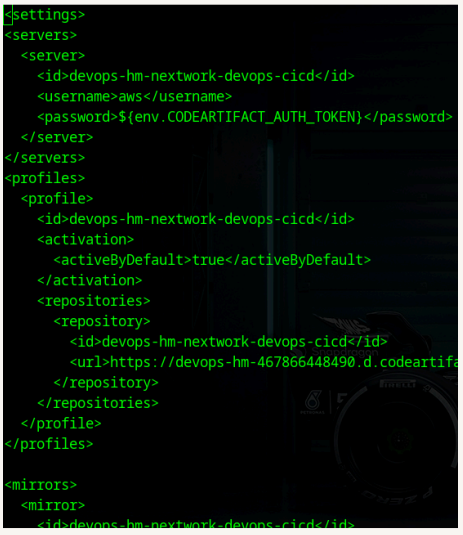
MA
Harish madhavan J U
NextWork Student

Maven and CodeArtifact

To test the connection between Maven and CodeArtifact, I compiled my web app using settings.xml

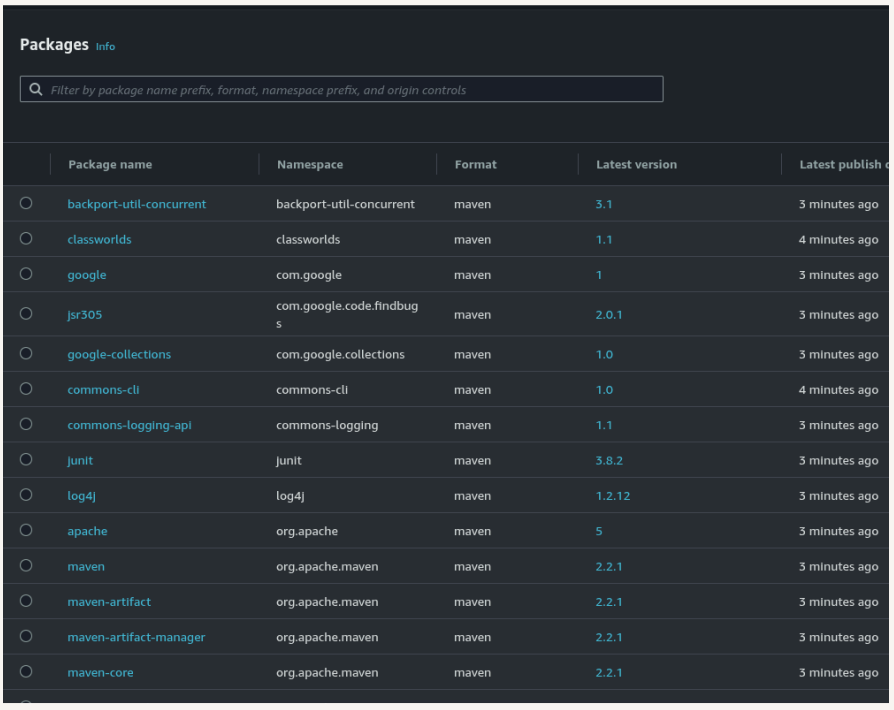
The settings.xml file configures Maven to connect with our CodeArtifact repo for dependencies required to build the web app, settings.xml file consists of instructions for maven on how to behave across projects including settings for authentication, repos etc.

Compiling means the process of converting human understandable langueage to computer understandable one.



Verify Connection

After compiling, I checked my codeartifact repo and I noticed a lot of packages were downloaded, this happend because when we ran the maven compile command, maven collects the required dependencies form the pom.xml file and checks for it in the codeartifact repo, if not found it retrieves from the upstream repo maven-central in our case for the dependency this ensures that packages are downloaded from a secure and reliable source. CodeArtiFact would cache those packages in the repo for faster access.



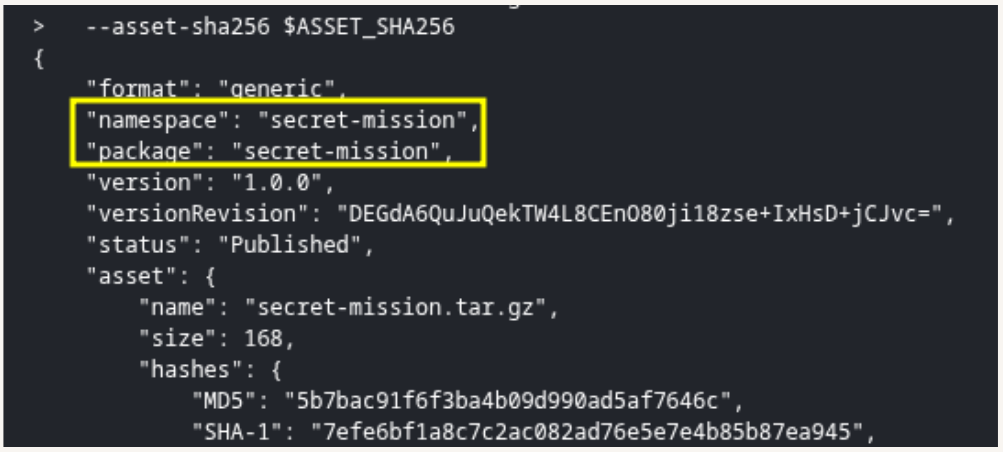
Uploading My Own Packages

As an extension to the project, I also created a custom package and published it to CodeArtifact, making it available exclusively to my organization. This approach is valuable in scenarios where companies develop proprietary libraries—such as for UI components, data processing, or other internal functionalities—and want to securely manage and distribute them without exposing their intellectual property to the public.

To create my own package, I bundled my file into tar.gz file because tar.gz bundles multiple files and saves space. I also generated a security hash because on comparing we can check whether the file is consistent.

To publsh the package I had to activate the cloud shell and run a bunch of commands to publish the package. When I look at the package details in CodeArtifact, I can see metadata of the pacakage including when it was created, origin, sha256 hash.

To validate my package, I then downloaded and unzipped it after doing so I saw the text file containing the sentence I had written in it.


> --asset-sha256 $ASSET_SHA256
{
"format": "generic",
"namespace": "secret-mission",
"package": "secret-mission",
"version": "1.0.0",
"versionRevision": "DEGdA6QuJuQekTW4L8CEnO80ji18zse+IxHsD+jCJvc=",
"status": "Published",
"asset": {
"name": "secret-mission.tar.gz",
"size": 168,
"hashes": {
"MD5": "5b7bac91f6f3ba4b09d990ad5af7646c",
"SHA-1": "7efe6bf1a8c7c2ac082ad76e5e7e4b85b87ea945",

The place to learn & showcase your skills

Check out nextwork.org for more projects