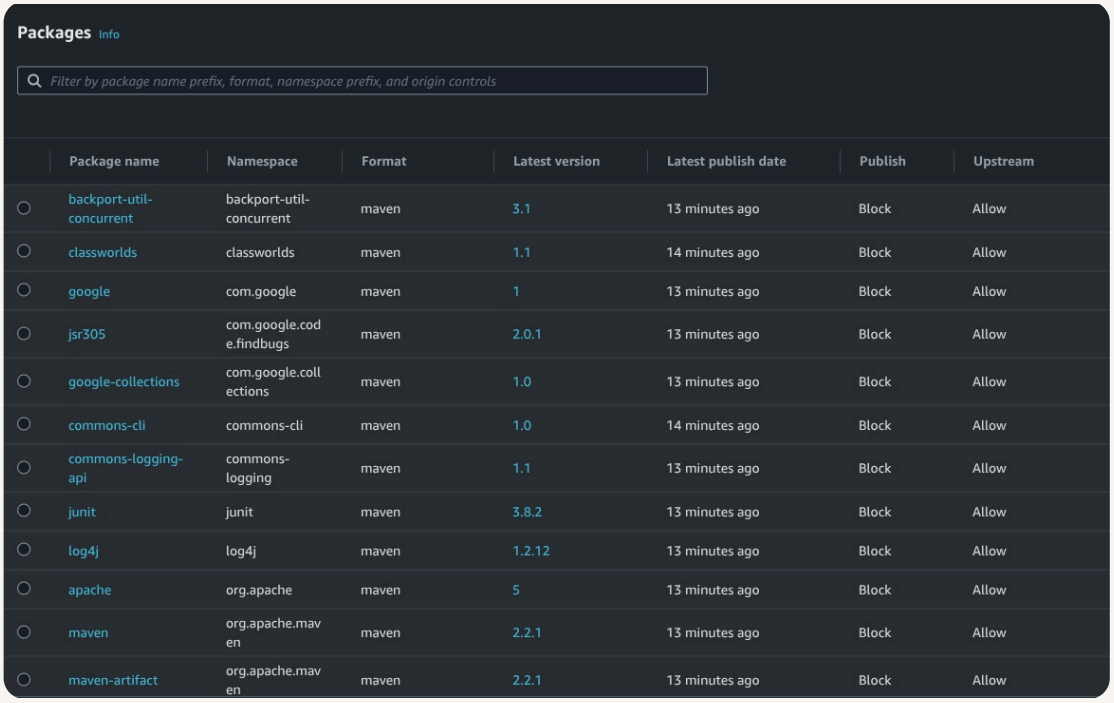
Secure Packages with CodeArtifact

Shadrack Kalukwo



Packages Info

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

Package name	Namespace	Format	Latest version	Latest publish date	Publish	Upstream
backport-util-concurrent	backport-util-concurrent	maven	3.1	13 minutes ago	Block	Allow
classworlds	classworlds	maven	1.1	14 minutes ago	Block	Allow
google	com.google	maven	1	13 minutes ago	Block	Allow
jsr305	com.google.code.findbugs	maven	2.0.1	13 minutes ago	Block	Allow
google-collections	com.google.collections	maven	1.0	13 minutes ago	Block	Allow
commons-cli	commons-cli	maven	1.0	14 minutes ago	Block	Allow
commons-logging-api	commons-logging	maven	1.1	13 minutes ago	Block	Allow
junit	junit	maven	3.8.2	13 minutes ago	Block	Allow
log4j	log4j	maven	1.2.12	13 minutes ago	Block	Allow
apache	org.apache	maven	5	13 minutes ago	Block	Allow
maven	org.apache.maven	maven	2.2.1	13 minutes ago	Block	Allow
maven-artifact	org.apache.maven	maven	2.2.1	13 minutes ago	Block	Allow

S
Shadrack Kalukwo
NextWork Student

Introducing Today's Project!

In this project, I will demonstrate how to securely get packages from CodeArtifact Upstream to my CodeArtifact local repo. I'll be doing this to learn how securely run command in my ec2 to compile make call to my CodeArtifact.

Key tools and concepts

Services I used were; 1. CodeArticat 2. CodeArtifact Upstream 3. IAM roles and policy 4. ec2 key concepts; 1. Compilling 2. Package managers 3. Security and least privilege

Project reflection

This project took me approximately 2 hours. It was most rewarding to compile and download all the packages succesfully.

IThis 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 from April 14th, 2025

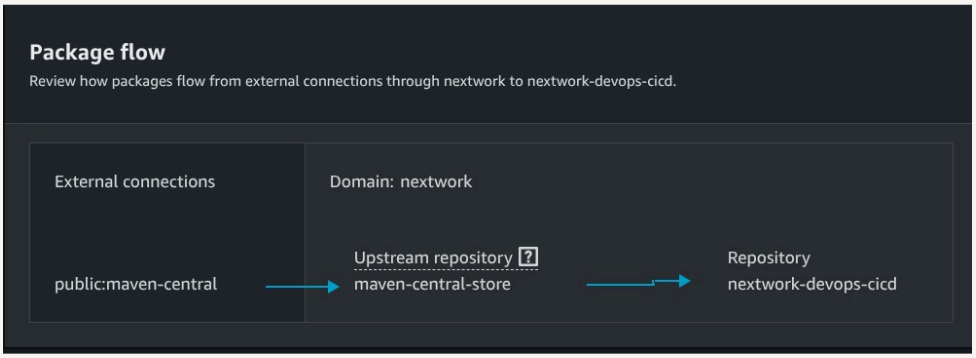
Shadrack Kalukwo
NextWork Student

CodeArtifact Repository

CodeArtifcat is a secure, central place to store all your software packages. Engineering teams use artifact repositories because it gives you a consistent, reliable place to store and retrieve these components.

A domain is a folder holding multiple repositories belonging to the same organization and provide a single place to manage security settings applying to all repositories. My domain is nextwork-533266965260.d.codeartifact.us-east-1.amazonaws.com

A CodeArtifact repository can have an upstream repository, which means it is like the backup libraries that your primary repository can access when it doesn't have what you need. My repository's upstream repository is 'maven-central-store'



S
Shadrack Kalukwo
NextWork Student

CodeArtifact Security

Issue

To access CodeArtifact,I need to Export a CodeArtifact authorization token for authorization to my repo from my shell. I ran into an error when retrieving the token because by default EC2 instance doesn't have permission to access other resources.

Resolution

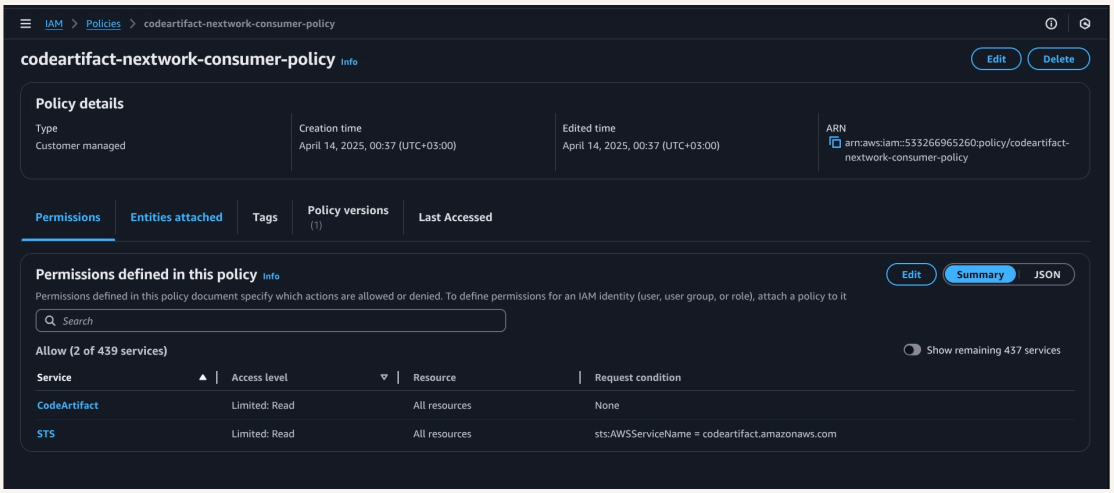
To resolve the error with my security token, I setup an IAM policy and created a role for it which I attached to my instance. This solved the error because the policy will retrieve a temporary authorization token for CodeArtifact and store it.

It's security best practice to use IAM roles because AWS automatically provides and rotates security temp credentials for that instance thus applications can automatically use these temporary credentials to make API calls without handling credentials

S
Shadrack Kalukwo
NextWork Student

The JSON policy attached to my role

The JSON policy I set up grants permissions to allow: 1. Getting an authorization token for CodeArtifact 2. Retrieving the endpoint for a CodeArtifact repository 3. Reading packages from a CodeArtifact repository Actions are allowed on all resources



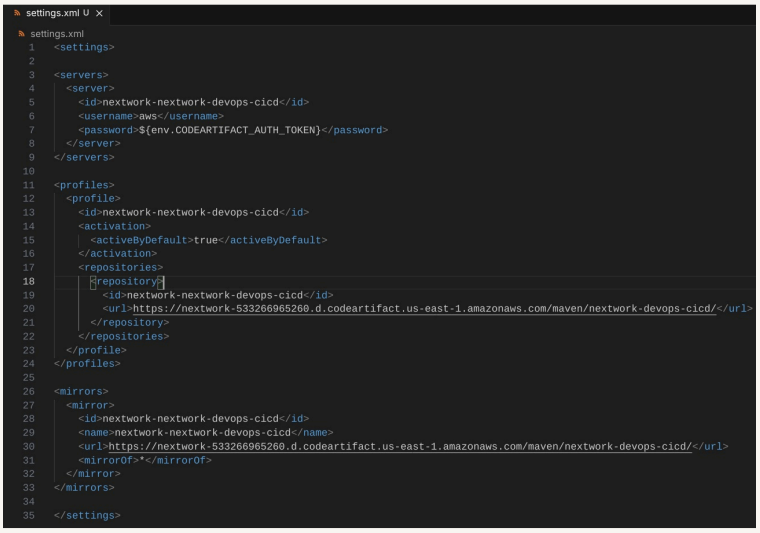
Shadrack Kalukwo
NextWork Student

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 use our CodeArtifcat repository. It supplie maven with the name and authentication token to get access to the CodeArtifact repository and also set's up a profile section incase we have multiple repositories.

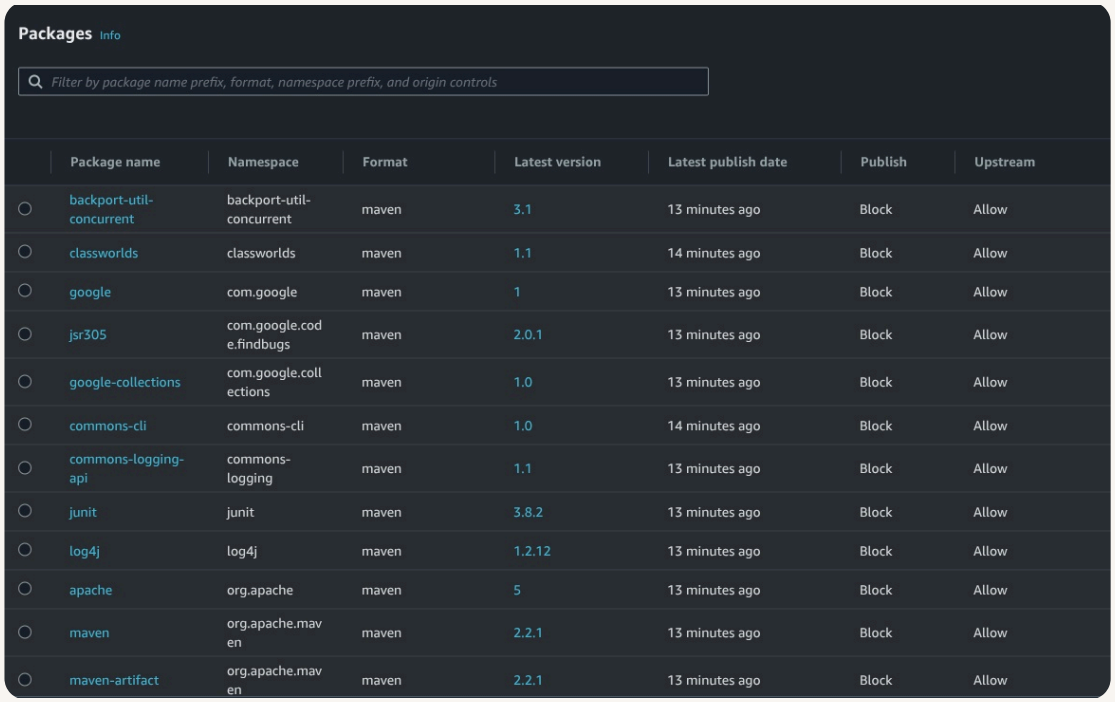
Compiling means the process of translating source code into a something machines can run. Maven compiler will need to put together all the packeges needed for the web app to run. It will visit our repo which will lead it to the upstream repository.



S
Shadrack Kalukwo
NextWork Student

Verify Connection

fter compiling, I checked our CodeArtifact repo and I noticed 4 pages of packages inside. That means we stored our web app dependencies in a Artifact repository.



Packages Info

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

Package name	Namespace	Format	Latest version	Latest publish date	Publish	Upstream
backport-util-concurrent	backport-util-concurrent	maven	3.1	13 minutes ago	Block	Allow
classworlds	classworlds	maven	1.1	14 minutes ago	Block	Allow
google	com.google	maven	1	13 minutes ago	Block	Allow
jsr305	com.google.code.findbugs	maven	2.0.1	13 minutes ago	Block	Allow
google-collections	com.google.collections	maven	1.0	13 minutes ago	Block	Allow
commons-cli	commons-cli	maven	1.0	14 minutes ago	Block	Allow
commons-logging-api	commons-logging	maven	1.1	13 minutes ago	Block	Allow
junit	junit	maven	3.8.2	13 minutes ago	Block	Allow
log4j	log4j	maven	1.2.12	13 minutes ago	Block	Allow
apache	org.apache	maven	5	13 minutes ago	Block	Allow
maven	org.apache.maven	maven	2.2.1	13 minutes ago	Block	Allow
maven-artifact	org.apache.maven	maven	2.2.1	13 minutes ago	Block	Allow

NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for more projects