



[nextwork.org](https://nextwork.org)

# Secure Packages with CodeArtifact

VE

vedikagangil@gmail.com

Packages <small>Info</small>						
<input type="button" value="Filter by package name prefix, format, namespace prefix, and origin controls"/> <input type="button" value="Delete package"/> <input type="button" value="View connection instructions"/>						
	Package name	Namespace	Format	Latest version	Latest publish date	Publish
<input type="radio"/>	backport-util-concurrent	backport-util-concurrent	maven	3.1	5 minutes ago	Block
<input type="radio"/>	classworlds	classworlds	maven	1.1	5 minutes ago	Block
<input type="radio"/>	google	com.google	maven	1	4 minutes ago	Block
<input type="radio"/>	jsr305	com.google.code.findbugs	maven	2.0.1	4 minutes ago	Block
<input type="radio"/>	google-collections	com.google.collections	maven	1.0	4 minutes ago	Block
<input type="radio"/>	commons-cli	commons-cli	maven	1.0	5 minutes ago	Block
<input type="radio"/>	commons-logging-api	commons-logging	maven	1.1	5 minutes ago	Block

# Introducing Today's Project!

In this project I will set up CodeArtifact as a repository for my project's dependencies. Then use IAM roles and policies to give my web app access to CodeArtifact. Next verify my web app's connection to CodeArtifact.

## Key tools and concepts

The major service I learned about today was CodeArtifact where I created my very own repository.

## Project reflection

This project took me 1 hour from start to finish.

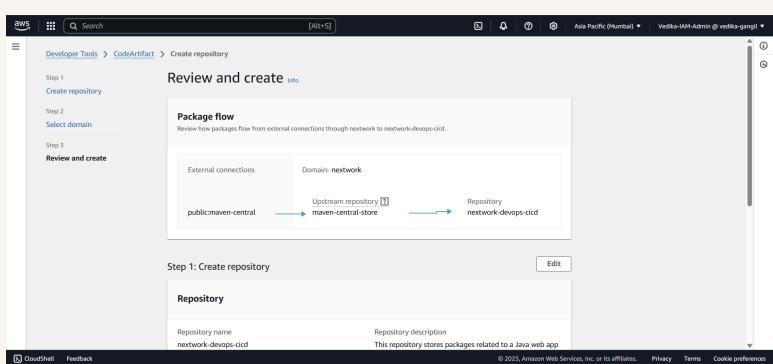
This project is part three of a series of DevOps projects where I'm building a CI/CD pipeline! I'll be working on the next project tomorrow!

# CodeArtifact Repository

CodeArtifact is a secure, central place to store all software packages. When building an application, one typically uses dozens of external packages or libraries - things other developers have created that you don't want to build from scratch.

A domain in AWS CodeArtifact acts like a shared container for multiple repositories. It simplifies management by grouping related repos together under one namespace. With a domain, you control permissions centrally. My domain name is nextwork.

Upstream repositories are like backup libraries that my primary repository can access when it doesn't have what it need. If I didn't set up CodeArtifact or have an upstream repository, my build would fail because a package is missing!



# CodeArtifact Security

## Issue

To access CodeArtifact, we need an authorization token because AWS uses it to authenticate and authorize package manager requests to private repositories. I ran into an error when retrieving a token because certain IAM permissions were missing.

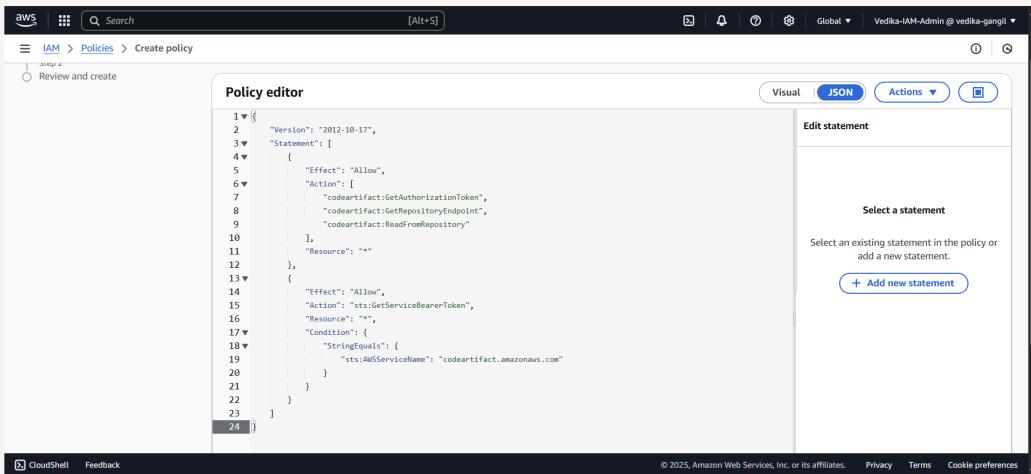
## Resolution

To resolve the error with my security token, I created a new IAM policy and then created a new IAM role which had the newly created policy. I then attached that role to my EC2 instance.

It's security best practice to use IAM roles because they provide temporary, limited-privilege credentials instead of long-term access keys, reducing the risk of compromised credentials. Roles enable fine-grained permissions without sharing secrets.

# The JSON policy attached to my role

This IAM policy grants four key permissions for accessing AWS CodeArtifact: GetAuthorizationToken, GetRepositoryEndpoint, ReadFromRepository, and sts:GetServiceBearerToken. These permissions are essential for configuring tools.



The screenshot shows the AWS IAM Policy editor interface. The left pane displays the JSON code of the policy, and the right pane shows a modal for adding a new statement. The JSON code is as follows:

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Action": [  
7                 "codeartifact:GetAuthorizationToken",  
8                 "codeartifact:GetRepositoryEndpoint",  
9                 "codeartifact:ReadFromRepository"  
10            ],  
11            "Resource": "*"  
12        },  
13        {  
14            "Effect": "Allow",  
15            "Action": "sts:GetServiceBearerToken",  
16            "Resource": "*",  
17            "Condition": {  
18                "StringEquals": {  
19                    "sts:AWSServiceName": "codeartifact.amazonaws.com"  
20                }  
21            }  
22        }  
23    ]  
24}
```

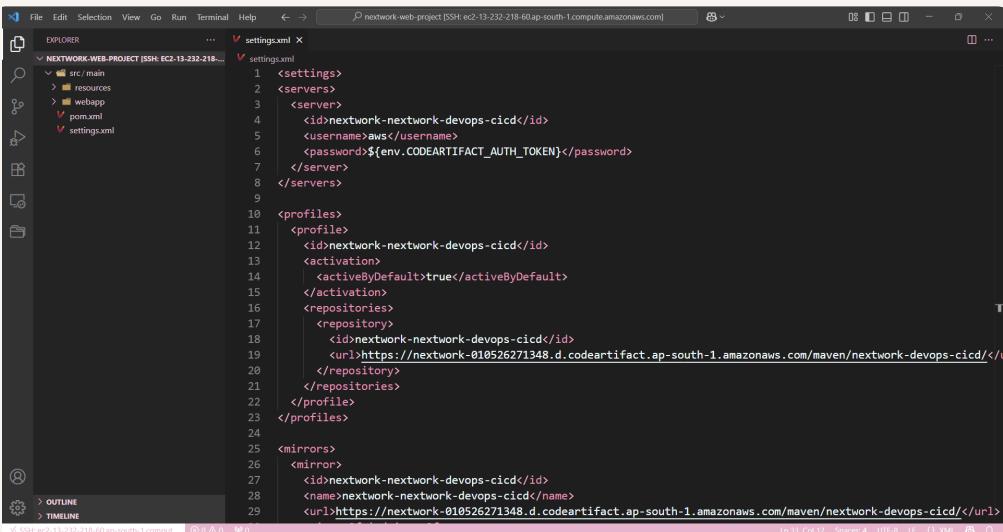
The right pane has a modal titled "Edit statement" with the sub-section "Select a statement". It contains the instruction "Select an existing statement in the policy or add a new statement." and a button "+ Add new statement".

# Maven and CodeArtifact

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

The settings.xml file enables Maven to work with CodeArtifact by configuring the repository URL and authentication. It defines the CodeArtifact endpoint as a <server> and uses a temporary AWS auth token (generated via CLI) as the password.

Compiling converts human-written code (e.g., Java) into machine-readable instructions, catching errors and optimizing performance. It's essential for languages like C++/Java but not for interpreted ones like Python.



```
<settings>
  <servers>
    <server>
      <id>nextwork-nextwork-devops-cicd</id>
      <username>aws</username>
      <password>${env.CODEARTIFACT_AUTH_TOKEN}</password>
    </server>
  </servers>
  <profiles>
    <profile>
      <id>nextwork-nextwork-devops-cicd</id>
      <activation>
        <activeByDefault>true</activeByDefault>
      </activation>
      <repositories>
        <repository>
          <id>nextwork-nextwork-devops-cicd</id>
          <url>https://nextwork-010526271348.d.codeartifact.ap-south-1.amazonaws.com/maven/nextwork-devops-cicd/</url>
        </repository>
      </repositories>
    </profile>
  </profiles>
  <mirrors>
    <mirror>
      <id>nextwork-nextwork-devops-cicd</id>
      <name>nextwork-nextwork-devops-cicd</name>
      <url>https://nextwork-010526271348.d.codeartifact.ap-south-1.amazonaws.com/maven/nextwork-devops-cicd/</url>
    </mirror>
  </mirrors>
</settings>
```

# Verify Connection

After compiling, I checked my CodeArtifact repository. I noticed that several packages were now visible in the repository.

Packages <small>Info</small>		<input type="button" value="C"/>	<input type="button" value="Delete package"/>	<input type="button" value="View connection instructions"/>			
<input type="text"/> Filter by package name prefix, format, namespace prefix, and origin controls							
	Package name	Namespace	Format	Latest version	Latest publish date	Publish	Upstream
<input type="radio"/>	backport-util-concurrent	backport-util-concurrent	maven	3.1	5 minutes ago	Block	Allow
<input type="radio"/>	classworlds	classworlds	maven	1.1	5 minutes ago	Block	Allow
<input type="radio"/>	google	com.google	maven	1	4 minutes ago	Block	Allow
<input type="radio"/>	jsr305	com.google.code.findbugs	maven	2.0.1	4 minutes ago	Block	Allow
<input type="radio"/>	google-collections	com.google.collections	maven	1.0	4 minutes ago	Block	Allow
<input type="radio"/>	commons-cli	commons-cli	maven	1.0	5 minutes ago	Block	Allow
<input type="radio"/>	commons-logging-api	commons-logging	maven	1.1	5 minutes ago	Block	Allow



[nextwork.org](https://nextwork.org)

# The place to learn & showcase your skills

Check out [nextwork.org](https://nextwork.org) for more projects

