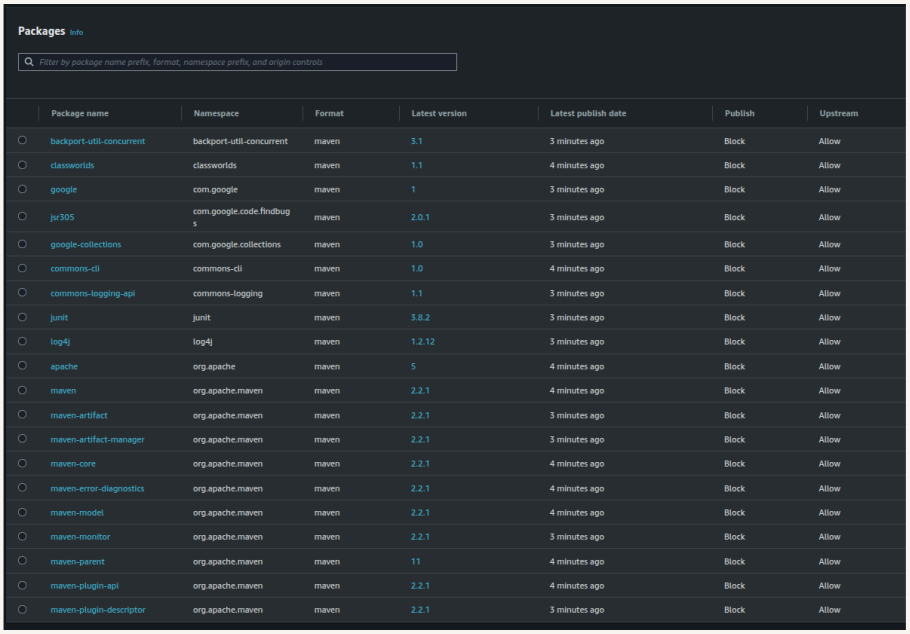
nextwork.org

Secure Packages with CodeArtifact

Shravan Kumar Satapathy



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	3 minutes ago	Block	Allow
classworlds	classworlds	maven	1.1	4 minutes ago	Block	Allow
google	com.google	maven	1	3 minutes ago	Block	Allow
jsr305	com.google.code.findbugs	maven	2.0.1	3 minutes ago	Block	Allow
google-collections	com.google.collections	maven	1.0	3 minutes ago	Block	Allow
commons-cli	commons-cli	maven	1.0	4 minutes ago	Block	Allow
commons-logging-api	commons-logging	maven	1.1	3 minutes ago	Block	Allow
junit	junit	maven	3.8.2	3 minutes ago	Block	Allow
log4j	log4j	maven	1.2.12	3 minutes ago	Block	Allow
apache	org.apache	maven	5	4 minutes ago	Block	Allow
maven	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-artifact	org.apache.maven	maven	2.2.1	3 minutes ago	Block	Allow
maven-artifact-manager	org.apache.maven	maven	2.2.1	3 minutes ago	Block	Allow
maven-core	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-error-diagnostics	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-model	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-monitor	org.apache.maven	maven	2.2.1	3 minutes ago	Block	Allow
maven-parent	org.apache.maven	maven	11	4 minutes ago	Block	Allow
maven-plugin-api	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-plugin-descriptor	org.apache.maven	maven	2.2.1	3 minutes ago	Block	Allow

Shravan Kumar Satapathy
NextWork Student

Introducing Today's Project!

In this project, I will demonstrate setting up AWS CodeArtifact to manage and secure Java dependencies. I'm doing this to learn how CodeArtifact provides a verified package repository, reducing errors and enhancing security within a CI/CD pipeline.

Key tools and concepts

Services I used were AWS EC2, IAM, CodeArtifact, GitHub, and Maven. Key concepts learned include IAM policies/roles, CodeArtifact domains/repos, upstream repos, authorization tokens, least privilege, compiling, and CI/CD package management.

Project reflection

This project took me approximately 2 hours. The most challenging part was resolving remote SSH connection issues. It was most rewarding to successfully establish secure CodeArtifact integration and see dependencies automatically cached.

This project is part three of a DevOps CI/CD pipeline series. I'll work on the next project soon: automating web app builds using AWS CodeBuild, integrating GitHub, and defining build specifications.

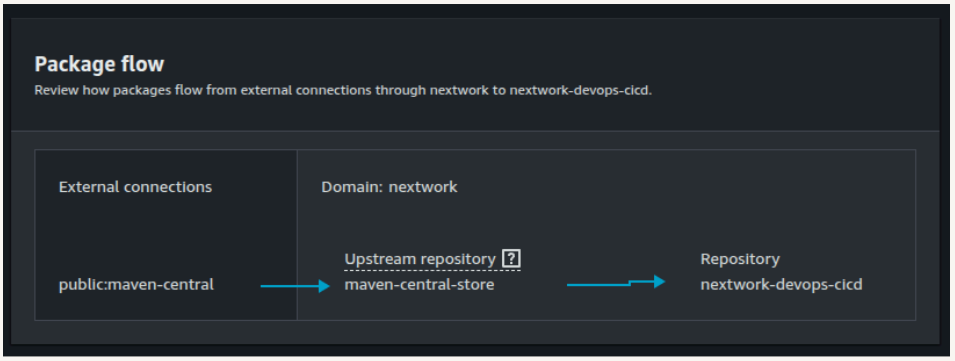
Shravan Kumar Satapathy
NextWork Student

CodeArtifact Repository

CodeArtifact is a secure central place to store software packages. Engineering teams use artifact repositories because they offer secure, reliable storage and retrieval of components, ensuring security, reliability, and control over package versions.

A domain is a folder holding multiple repositories. It offers a single point to manage permissions and security across all contained repositories, ensuring consistent, efficient control. My domain is nextwork.

A CodeArtifact repository can have an upstream, meaning it retrieves packages not locally available. My repository's upstream is Maven Central, for reliable, controlled access to public Java libraries.



Shravan Kumar Satapathy
NextWork Student

CodeArtifact Security

Issue

To access CodeArtifact, an authorization token (temporary password) is needed for Maven. The error occurred because my EC2 instance lacks default permissions for AWS services like CodeArtifact, due to least privilege.

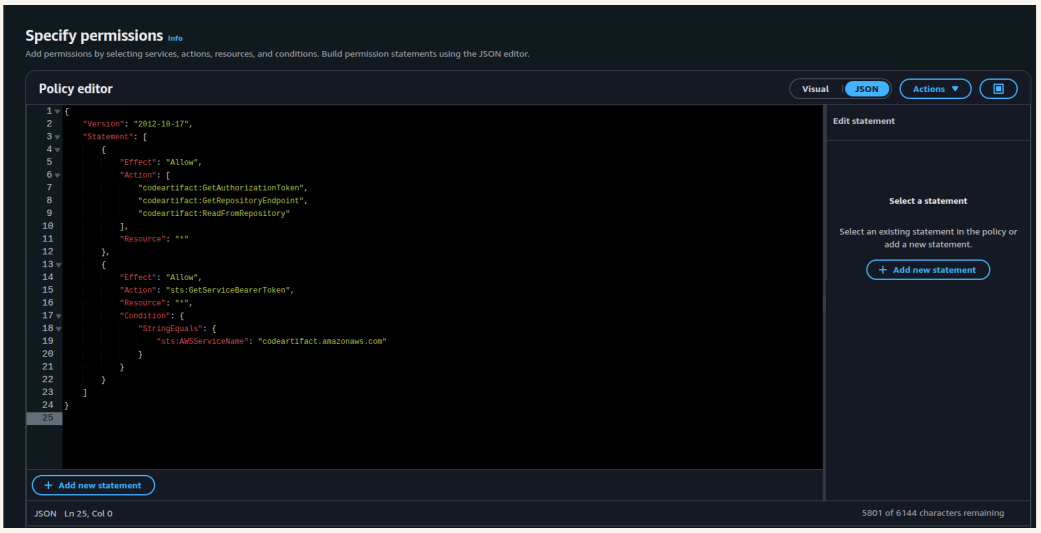
Resolution

To resolve the error with my security token, I created an IAM policy, attached it to an IAM role, and then associated that role with my EC2 instance. This granted the instance the necessary permissions to retrieve the CodeArtifact token.

It's security best practice to use IAM roles because they allow assigning permission sets to AWS resources without embedding credentials. This provides centralized, consistent security control via reusable policies, upholding least privilege.

The JSON policy attached to my role

The JSON policy grants permissions for CodeArtifact actions like token retrieval, endpoint access, and package reading. It also includes sts:GetServiceBearerToken for CodeArtifact, crucial for secure Maven integration while adhering to the principle.



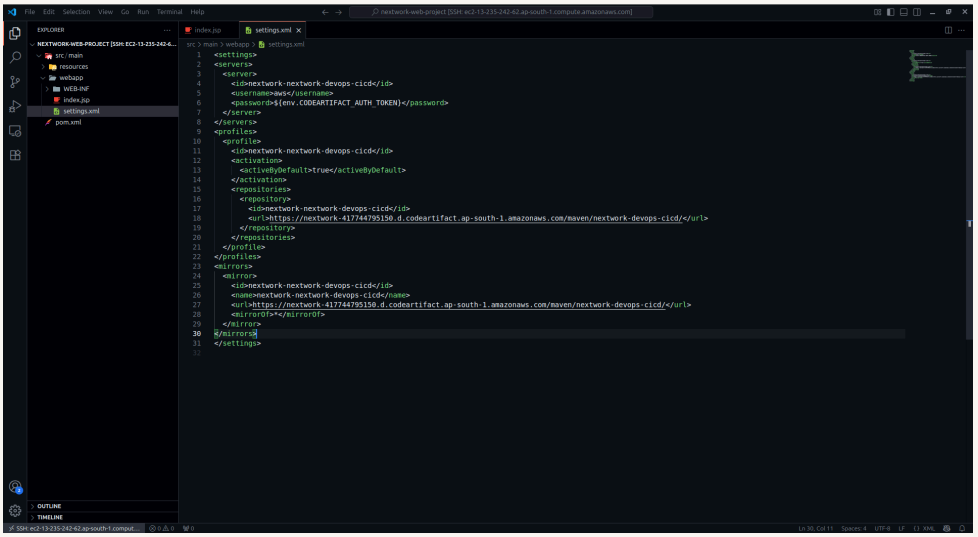
Shravan Kumar Satapathy
NextWork Student

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 locate and authenticate with repositories like CodeArtifact. It tells Maven where to find dependencies and how to access them, enabling seamless, secure retrieval for builds.

Compiling means translating a project's code into a language computers can understand and run. It ensures everything is correctly set up and ready to form a working application.



Verify Connection

After compiling, I checked my CodeArtifact repository. I noticed Maven packages, automatically pulled from Maven Central via CodeArtifact and cached. This provides faster, reliable, and controlled dependency management.

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	3 minutes ago	Block	Allow
classworlds	classworlds	maven	1.1	4 minutes ago	Block	Allow
google	com.google	maven	1	3 minutes ago	Block	Allow
jsr305	com.google.code.findbugs	maven	2.0.1	3 minutes ago	Block	Allow
google-collections	com.google.collections	maven	1.0	3 minutes ago	Block	Allow
commons-cli	commons-cli	maven	1.0	4 minutes ago	Block	Allow
commons-logging-api	commons-logging	maven	1.1	3 minutes ago	Block	Allow
junit	junit	maven	3.8.2	3 minutes ago	Block	Allow
log4j	log4j	maven	1.2.12	3 minutes ago	Block	Allow
apache	org.apache	maven	5	4 minutes ago	Block	Allow
maven	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-artifact	org.apache.maven	maven	2.2.1	3 minutes ago	Block	Allow
maven-artifact-manager	org.apache.maven	maven	2.2.1	3 minutes ago	Block	Allow
maven-core	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-error-diagnostics	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-model	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-monitor	org.apache.maven	maven	2.2.1	3 minutes ago	Block	Allow
maven-parent	org.apache.maven	maven	11	4 minutes ago	Block	Allow
maven-plugin-api	org.apache.maven	maven	2.2.1	4 minutes ago	Block	Allow
maven-plugin-descriptor	org.apache.maven	maven	2.2.1	3 minutes ago	Block	Allow

The place to learn & showcase your skills

Check out nextwork.org for more projects