Secure Packages with CodeArtifact

Seth Sekyere

	Package name	Namespace	Format	Latest version	Latest publish date	Publish	Upstream
○	backport-util-concurrent	backport-util-concurrent	maven	3.1	31 minutes ago	Block	Allow
○	classworlds	classworlds	maven	1.1	31 minutes ago	Block	Allow
○	google	com.google	maven	1	31 minutes ago	Block	Allow
○	jsr305	com.google.code.findbugs	maven	2.0.1	31 minutes ago	Block	Allow
○	google-collections	com.google.collections	maven	1.0	31 minutes ago	Block	Allow
○	commons-cli	commons-cli	maven	1.0	31 minutes ago	Block	Allow
○	commons-logging-api	commons-logging	maven	1.1	31 minutes ago	Block	Allow
○	junit	junit	maven	3.8.2	31 minutes ago	Block	Allow
○	log4j	log4j	maven	1.2.12	31 minutes ago	Block	Allow
○	apache	org.apache	maven	13	26 minutes ago	Block	Allow
○	maven	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
○	maven-artifact	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
○	maven-artifact-manager	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
○	maven-core	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
○	maven-error-diagnostics	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
○	maven-model	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
○	maven-monitor	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
○	maven-parent	org.apache.maven	maven	23	26 minutes ago	Block	Allow
○	maven-plugin-api	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow

Seth Sekyere

Introducing Today's Project!

In this project, I will demonstrate how to set up AWS CodeArtifact to manage and secure my app's dependencies. I'm doing this project to learn how to store, access, and publish packages as part of a secure CI/CD pipeline.

Key tools and concepts

Services I used were AWS CodeArtifact and Maven. Key concepts I learnt include configuring Maven with settings.xml, managing dependencies securely, using upstream repositories, and caching packages for faster, controlled builds.

Project reflection

This project took me approximately 30 minutes. The most challenging part was configuring the settings.xml file correctly. It was most rewarding to see dependencies flow through CodeArtifact, confirming the integration worked.

This project is part three of a DevOps series building a CI/CD pipeline! I'll be working on the next project soon to continue automating and improving the deployment process.

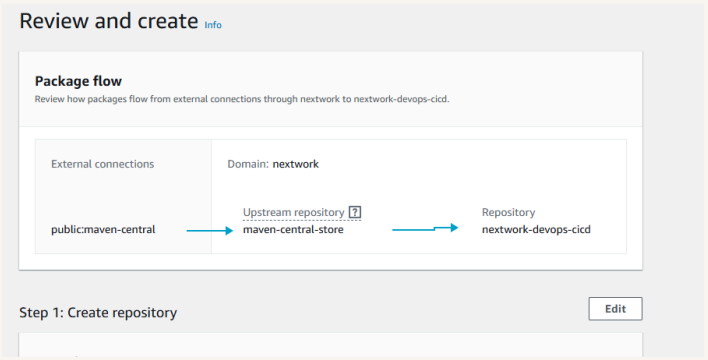
Seth Sekyere

CodeArtifact Repository

CodeArtifact is a secure, managed service that stores and manages software packages your app depends on. Engineering teams use artifact repositories like CodeArtifact to ensure consistent, reliable, and safe access to shared packages across projects.

A domain is a central place to manage access and settings for multiple repositories. My domain is nextwork, which helps enforce consistent security and share packages across all related CodeArtifact repositories.

A CodeArtifact repository can have an upstream repository, which means it fetches missing packages from another source. My repository's upstream is Maven Central, giving access to public Java libraries while improving speed, reliability, and control.



Seth Sekyere

CodeArtifact Security

Issue

To access CodeArtifact, we need an authorization token that verifies our identity and permissions. I ran into an error retrieving a token because my EC2 instance lacked the necessary AWS credentials to authenticate securely.

Resolution

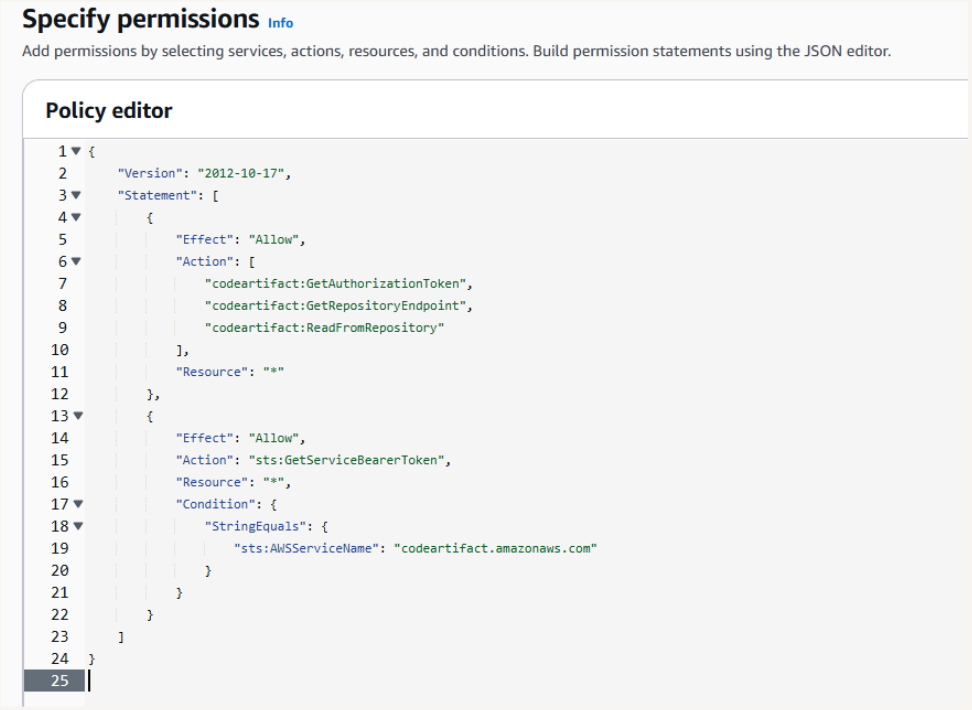
To resolve the permissions error, I created an IAM policy granting CodeArtifact access, attached it to an IAM role, and assigned that role to my EC2 instance. This gave my instance the needed permissions to get the authorization token.

It's security best practice to use IAM roles because they grant temporary, limited access without hardcoding credentials, reducing the risk of credential exposure.

Seth Sekyere

The JSON policy attached to my role

The JSON policy I set up grants permissions to get auth tokens, repo endpoints, and read packages from CodeArtifact. It also allows temporary access for CodeArtifact via STS. These are needed for secure and limited access to the repo.



Seth Sekyere

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 authenticate with CodeArtifact and access its repositories, enabling it to securely download dependencies for your projects.

Compiling means converting your source code into bytecode or machine code so the computer can understand and run it. It's how your written code becomes an executable program.

Seth Sekyere

Verify Connection

After compiling, I checked the CodeArtifact repository. I noticed that several dependencies were cached there, showing that Maven successfully pulled them from the upstream repository and stored them for future use.

Package name	Namespace	Format	Latest version	Latest publish date	Publish	Upstream
backport-util-concurrent	backport-util-concurrent	maven	3.1	31 minutes ago	Block	Allow
classworlds	classworlds	maven	1.1	31 minutes ago	Block	Allow
google	com.google	maven	1	31 minutes ago	Block	Allow
jsr305	com.google.code.findbugs	maven	2.0.1	31 minutes ago	Block	Allow
google-collections	com.google.collections	maven	1.0	31 minutes ago	Block	Allow
commons-cli	commons-cli	maven	1.0	31 minutes ago	Block	Allow
commons-logging-api	commons-logging	maven	1.1	31 minutes ago	Block	Allow
junit	junit	maven	3.8.2	31 minutes ago	Block	Allow
log4j	log4j	maven	1.2.12	31 minutes ago	Block	Allow
apache	org.apache	maven	13	26 minutes ago	Block	Allow
maven	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
maven-artifact	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
maven-artifact-manager	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
maven-core	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
maven-error-diagnostics	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
maven-model	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
maven-monitor	org.apache.maven	maven	2.2.1	31 minutes ago	Block	Allow
maven-parent	org.apache.maven	maven	23	26 minutes ago	Block	Allow