



nextwork.org

Secure Packages with CodeArtifact



naveen msd

Packages <small>(10)</small>						
Package name	Namespace	Format	Latest version	Latest publish date	Publish	Upstream
badger-fit-concurrent	badger-fit-concurrent	maven	5.1	4 minutes ago	Block	Allow
classewds	classewds	maven	1.1	4 minutes ago	Block	Allow
google	com.google	maven	1	4 minutes ago	Block	Allow
jar395	com.googlecode.findbugs	maven	2.0.1	4 minutes ago	Block	Allow
google-collections	com.google.collections	maven	1.0	4 minutes ago	Block	Allow
commons-cli	commons-cli	maven	1.0	4 minutes ago	Block	Allow
common-logging-api	common-logging	maven	1.1	4 minutes ago	Block	Allow
junit	junit	maven	5.8.2	4 minutes ago	Block	Allow
log4j	log4j	maven	2.12.12	4 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	4 minutes ago	Block	Allow
maven-artifact-manager	org.apache.maven	maven	2.2.1	4 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	4 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	4 minutes ago	Block	Allow



Introducing Today's Project!

In this project, I will demonstrate how to create a CodeArtifact repository. Setting up your EC2 instance's permissions to access the CodeArtifact repository, and I will see the CodeArtifact repository store your web app's packages!

Key tools and concepts

Services I used were AWS Code Artifact, IAM Policies and roles. Key concepts I learnt include creating a repo in code artifact and connecting maven to upstream the dependencies required for the web app.

Project reflection

This project took me approximately 2 hrs. The most challenging part was understanding how AWS CodeArtifact works and it was most rewarding to see how the packages are downloaded from maven.

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 you're building an application, you typically use dozens of external packages or libraries things other developers have created that you don't want to build from scratch.

CodeArtifact domain is like a folder that holds multiple repositories belonging to the same project or organization. We like using domains because they give you a single place to manage permissions and security settings that apply to all repositories

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

The screenshot shows a web-based interface for managing CodeArtifact repositories. At the top, there's a navigation bar with 'Developer Tools', 'CodeArtifact', and 'Repositories'. Below the navigation is a search bar and a 'Create repository' button. The main area displays a table of repositories:

Repository name	Domain	Domain owner	Repository description
maven-central-store	network	919586591094	Provides Maven artifacts from Maven Central Repository.
nextwork-devops-ci-cd	nextwork	919586591094	This repository stores packages related to a Java web app created as a part of NextWork's CI/CD Pipeline series.



CodeArtifact Security

Issue

To access CodeArtifact, we need to export a CodeArtifact authorization token for authorization to the repository from preferred shell. I ran into an error when retrieving a token because AWS follows the principle of least privilege.

Resolution

To resolve the error with my security token, I created a policy to the EC2 instance and assigned role with this policy to my EC2 instance. This resolved the error because the policy granted permission to manage CodeArtifact.

It's a security best practice to use IAM roles because creating an IAM role specifically for an EC2 instance to get CodeArtifact access, but roles can grant permissions to any AWS service.



The JSON policy attached to my role

The JSON policy I set up grants only the minimum permissions needed to perform the required tasks, enhancing your security posture.

The screenshot shows the AWS IAM Policy Editor interface. On the left, there is a large code editor window displaying a JSON policy document. On the right, there is a sidebar titled "Select a statement" with a button "+ Add new statement". At the bottom, there are tabs for "Visual", "JSON" (which is selected), and "Actions". Below the tabs, there are buttons for "Cancel" and "Next".

```
1+ {
2+   "Version": "2012-10-17",
3+   "Statement": [
4+     {
5+       "Effect": "Allow",
6+       "Action": [
7+         "cloudformation:GetStackResource",
8+         "cloudformation:GetStackResources",
9+         "cloudformation:DescribeStacks"
10+      ],
11+      "Resource": "*"
12+    },
13+    {
14+      "Effect": "Allow",
15+      "Action": "AmazonSQS:SendMessage",
16+      "Resource": "*",
17+      "Condition": {
18+        "StringEquals": {
19+          "SQS:NgServiceQueue": "codepipeline.amazonaws.com"
20+        }
21+      }
22+    }
23+  ]
24+}
```

Below the code editor, there are status indicators: "JSON: Ln 25, Col 0", "Security: 0", "Errors: 0", "Warnings: 0", "Suggestions: 0", and "5801 of 6144 characters remaining".



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 when we add CodeArtifact information to this file. By configuring settings.xml properly, we're creating a seamless connection between Maven and CodeArtifact.

Compiling is like translating the project's code into a language that computers can understand and run. When I compile my project, I'm making sure everything is correctly set up and ready to turn into a working app.

```
<setting>
<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-919586551094.d.codeartifact.us-east-2.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-919586551094.d.codeartifact.us-east-2.amazonaws.com/maven/nextwork-devops-cicd/<url>
    <mirrorOf>*</mirrorOf>
  </mirror>
</mirrors>
</settings>
```



Verify Connection

After compiling, I checked the repository that I created in the ASW Code artifact, and I noticed the packages for my webapp had appeared by contacting Maven to provide the required dependencies.

Packages: info						
Filter by package name, profile, 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	4 minutes ago	Block	Allow
○ classworlds	classworlds	maven	1.1	4 minutes ago	Block	Allow
○ google	com.google	maven	1	4 minutes ago	Block	Allow
○ jstl05	com.google.code.findbugs	maven	2.0.1	4 minutes ago	Block	Allow
○ google-collections	com.google.collections	maven	1.0	4 minutes ago	Block	Allow
○ commons-dl	commons-dl	maven	1.0	4 minutes ago	Block	Allow
○ commons-logging-api	commons-logging	maven	1.1	4 minutes ago	Block	Allow
○ junit	junit	maven	3.8.2	4 minutes ago	Block	Allow
○ log4j	log4j	maven	1.2.17	4 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	4 minutes ago	Block	Allow
○ maven-artifact-manager	org.apache.maven	maven	2.2.1	4 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	4 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	4 minutes ago	Block	Allow



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

