



참조 안내서

# AWS SDKs 및 도구



# AWS SDKs 및 도구: 참조 안내서

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

# Table of Contents

AWS SDKs 및 도구 참조 가이드 .....	1
개발자 리소스 .....	2
툴킷 텔레메트리 알림 .....	3
구성 .....	4
공유 config 및 credentials 파일 .....	4
프로파일 .....	5
구성 파일 형식 .....	6
보안 인증 파일의 형식 .....	9
공유 파일의 위치 .....	10
홈 디렉터리 해석 .....	10
이러한 파일의 기본 위치 변경 .....	11
환경 변수 .....	12
환경 변수를 설정하는 방법 .....	12
서버리스 환경 변수 설정 .....	13
JVM 시스템 속성 .....	14
JVM 시스템 속성 설정 방법 .....	14
인증 및 액세스 .....	16
애플리케이션 코드를 인증할 메서드 선택 .....	16
인증 방법 .....	19
AWS Builder ID .....	21
콘솔 자격 증명을 사용하여 로그인 .....	21
작동 방식 .....	22
IAM Identity Center 인증 .....	22
사전 조건 .....	23
IAM Identity Center를 사용하여 프로그래밍 방식 액세스 구성 .....	23
포털 액세스 세션 새로 고침 .....	26
IAM Identity Center 인증 이해하기 .....	26
IAM Roles Anywhere .....	29
1단계: IAM Roles Anywhere 구성 .....	30
2단계: IAM Roles Anywhere 사용 .....	30
역할 수임 .....	31
IAM 역할 수임 .....	32
역할 수임(웹) .....	33
웹 자격 증명 또는 OpenID Connect와 페더레이션 .....	34

AWS 액세스 키 .....	35
단기 보안 인증 정보를 사용합니다 .....	35
장기 보안 인증 정보 사용 .....	36
단기 보안 인증 .....	37
장기 보안 인증 .....	38
EC2 인스턴스용 IAM 역할 .....	41
IAM 역할 생성 .....	42
Amazon EC2 인스턴스 시작과 IAM 역할 지정 .....	42
EC2 인스턴스에 연결 .....	42
EC2 인스턴스에서 애플리케이션 실행 .....	43
신뢰할 수 있는 ID 전파 .....	43
TIP 플러그인을 사용하기 위한 사전 조건 .....	44
코드에서 TIP 플러그인 사용 .....	45
TIP를 사용한 코드 예제 .....	47
설정 참조 .....	54
서비스 클라이언트 생성 .....	54
설정의 우선 순위 .....	54
이 안내서의 설정 페이지의 이해 .....	55
Config 파일 설정 목록 .....	57
Credentials 파일 설정 목록 .....	61
환경 변수 목록 .....	61
JVM 시스템 속성 목록 .....	66
표준화된 보안 인증 공급자 .....	70
자격 증명 공급자 체인의 이해 .....	70
SDK별 및 도구별 자격 증명 공급자 체인 .....	72
AWS 액세스 키 .....	72
로그인 공급자 .....	75
역할 공급자 수입 .....	78
컨테이너 제공업체 .....	85
IAM Identity Center 공급자 .....	88
IMDS 공급사 .....	95
프로세스 공급자 .....	100
표준화된 기능 .....	104
계정 기반 엔드포인트 .....	105
애플리케이션 ID .....	108
Amazon EC2 인스턴스 메타데이터 .....	111

Amazon S3 액세스 포인트 .....	114
Amazon S3 다중 리전 액세스 포인트 .....	117
S3 Express One Zone 세션 인증 .....	119
인증 체계 .....	122
AWS 리전 .....	125
AWS STS 리전 엔드포인트 .....	128
데이터 무결성 보호 .....	133
이중 스택 엔드포인트 및 FIPS 엔드포인트 .....	138
엔드포인트 검색 .....	141
일반 구성 .....	143
호스트 접두사 삽입 .....	147
IMDS 클라이언트 .....	152
재시도 동작 .....	155
요청 압축 .....	161
서비스별 엔드포인트 .....	164
스마트 구성 기본값 .....	219
공통 런타임 .....	224
CRT 종속성 .....	225
유지 관리 정책 .....	226
개요 .....	226
버전 관리 .....	226
SDK 주요 버전 수명 주기 .....	226
종속성 수명 주기 .....	227
통신 메서드 .....	228
버전 수명 주기 .....	229
설명서 기록 .....	232
.....	CCXXXV

# AWS SDKs 및 도구 참조 가이드에서 다루는 내용

많은 SDK와 도구는 설계 사양 공유나 공유 라이브러리를 통해 몇 가지 일반 기능을 공유합니다.

이 안내서에는 다음과 관련된 정보가 포함되어 있습니다.

- [글로벌 구성 AWS SDKs 및 도구](#) - 공유 config 및 credentials 파일 또는 환경 변수를 사용하여 AWS SDKs 및 도구를 구성하는 방법.
- [AWS SDKs 및 도구를 사용한 인증 및 액세스](#) -를 개발할 AWS 때 코드 또는 도구를 인증하는 방법을 설정합니다 AWS 서비스.
- [AWS SDKs 및 도구 설정 참조](#) - 인증 및 구성에 사용할 수 있는 모든 표준 설정에 대한 참조
- [AWS 공통 런타임\(CRT\) 라이브러리](#) - 거의 모든 SDK에서 사용할 수 있는 공유 AWS 공통 런타임 (CRT) 라이브러리의 개요입니다. SDKs
- [AWS SDKs 및 도구 유지 관리 정책](#)에서는 모바일 및 사물 인터넷(IoT) SDKs를 비롯한 AWS 소프트웨어 개발 키트(SDKs) 및 도구에 대한 유지 관리 정책 및 버전 관리와 기본 종속성을 다룹니다.

이 AWS SDKs 및 도구 참조 가이드는 여러 SDKs 및 도구에 적용할 수 있는 정보의 기반이 되기 위한 것입니다. 여기에 제공된 모든 정보 외에도 사용자가 사용하고 있는 SDK 또는 도구에 대한 특정 가이드도 사용해야 합니다. 다음은 이 가이드의 관련 자료 섹션이 포함된 SDK 및 도구입니다.

<p>사용 중인 제품:</p> <ul style="list-style-type: none"> <li>• 모든 SDK 또는 도구</li> </ul>	<p>본 안내서에서 사용자를 위한 관련 섹션은 다음과 같습니다.</p> <p><a href="#">AWS SDKs 및 도구 유지 관리 정책</a></p>
<ul style="list-style-type: none"> <li>• <a href="#">AWS Cloud9</a></li> <li>• <a href="#">AWS CDK</a></li> <li>• <a href="#">AWS Toolkit for Azure DevOps</a></li> <li>• <a href="#">AWS Toolkit for JetBrains</a></li> <li>• <a href="#">AWS Toolkit for Visual Studio</a></li> <li>• <a href="#">AWS Toolkit for Visual Studio Code</a></li> <li>• <a href="#">AWS Serverless Application Model</a></li> <li>• <a href="#">AWS CodeArtifact</a></li> <li>• <a href="#">AWS CodeBuild</a></li> </ul>	<p><a href="#">글로벌 구성 AWS SDKs 및 도구</a></p> <p><a href="#">AWS SDKs 및 도구를 사용한 인증 및 액세스</a></p> <p><a href="#">AWS SDKs 및 도구 유지 관리 정책</a></p>

<p>사용 중인 제품:</p>	<p>본 안내서에서 사용자를 위한 관련 섹션은 다음과 같습니다.</p>
<ul style="list-style-type: none"> <li>• <a href="#">Amazon CodeCatalyst</a></li> <li>• <a href="#">AWS CodeCommit</a></li> <li>• <a href="#">AWS CodeDeploy</a></li> <li>• <a href="#">AWS CodePipeline</a></li> </ul>	
<ul style="list-style-type: none"> <li>• <a href="#">AWS CLI</a></li> <li>• <a href="#">AWS SDK for C++</a></li> <li>• <a href="#">AWS SDK for Go</a></li> <li>• <a href="#">AWS SDK for Java</a></li> <li>• <a href="#">AWS SDK for JavaScript</a></li> <li>• <a href="#">AWS SDK for Kotlin</a></li> <li>• <a href="#">AWS SDK for .NET</a></li> <li>• <a href="#">AWS SDK for PHP</a></li> <li>• <a href="#">AWS SDK for Python (Boto3)</a></li> <li>• <a href="#">AWS SDK for Ruby</a></li> <li>• <a href="#">AWS SDK for Rust</a></li> <li>• <a href="#">AWS SDK for Swift</a></li> <li>• <a href="#">AWS Tools for Windows PowerShell</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">글로벌 구성 AWS SDKs 및 도구</a></li> <li>• <a href="#">AWS SDKs 및 도구를 사용한 인증 및 액세스</a></li> <li>• <a href="#">AWS SDKs 및 도구 설정 참조</a></li> <li>• <a href="#">AWS 공통 런타임(CRT) 라이브러리</a></li> <li>• <a href="#">AWS SDKs 및 도구 유지 관리 정책</a></li> <li>• <a href="#">AWS SDKs 및 도구 버전 수명 주기</a></li> </ul>
<ul style="list-style-type: none"> <li>• 애플리케이션을 개발하는 데 도움이 되는 도구에 대한 개요는 <a href="#">빌드 기반 도구를 AWS</a> 참조하세요.</li> <li>• 지원에 대한 자세한 내용은 <a href="#">AWS 지식 센터</a>를 참조하십시오.</li> <li>• AWS 용어에 대해서는 AWS 용어집 참조의 <a href="#">AWS 용어집</a>을 참조하세요.</li> </ul>	

## 개발자 리소스

Amazon Q Developer는 AWS 애플리케이션을 이해, 구축, 확장 및 운영하는 데 도움이 되는 생성형 AI 기반 대화형 어시스턴트입니다. 빌드 속도를 높이기 위해 Amazon Q AWS를 지원하는 모델을 고품질 AWS 콘텐츠로 보강하여 더 완전하고 실행 가능하며 참조된 답변을 생성합니다. 자세한 내용은 Amazon Q Developer 사용 설명서의 [Amazon Q Developer란 무엇인가요?](#)를 참조하세요.

## 툴킷 텔레메트리 알림

AWS 통합 개발 환경(IDE) 도구 키트는 IDE의 AWS 서비스에 액세스할 수 있는 플러그인 및 확장 프로그램입니다. Amazon Q IDE 플러그인 및 확장을 사용하면 IDE에서 생성형 AI 지원을 사용할 수 있습니다. 각 IDE 툴킷에 대한 자세한 정보는 앞의 표에 있는 툴킷 사용 설명서를 참고하세요. IDE에서 Amazon Q를 사용하는 방법에 대한 자세한 내용은 Amazon Q Developer 안내서의 [IDE에서의 Amazon Q 사용](#)을 참조하세요.

AWS IDE Toolkits 및 Amazon Q는 클라이언트 측 원격 측정 데이터를 수집하고 저장하여 향후 AWS Toolkit 및 Amazon Q 릴리스에 대한 결정을 알릴 수 있습니다. 수집된 데이터는 AWS 도구 키트 및 Amazon Q의 사용량을 정량화합니다.

모든 AWS IDE 도구 키트 및 Amazon Q에서 수집된 원격 측정 데이터에 대한 자세한 내용은 `aws-toolkit-common` Github 리포지토리의 [commonDefinitions.json](#) 문서를 참조하세요.

각 AWS IDE 도구 키트 및 Amazon Q 확장에서 수집한 원격 측정 데이터에 대한 자세한 내용은 다음 AWS 도구 키트 Github 리포지토리의 리소스 문서를 참조하세요.

- [AWS Amazon Q를 사용한 Visual Studio Toolkit](#)
- [AWS Toolkit for Visual Studio Code 및 VS Code용 Amazon Q 확장](#)
- [AWS Toolkit for JetBrains 및 JetBrains용 Amazon Q 플러그인](#)
- [Eclipse용 Amazon Q](#)

AWS 도구 키트에서 액세스할 수 있는 특정 AWS 서비스는 추가 클라이언트 측 원격 측정 데이터를 수집할 수 있습니다. 각 개별 AWS 서비스에서 수집하는 데이터 유형에 대한 자세한 내용은 관심 있는 특정 서비스의 [AWS 설명서](#) 주제를 참조하세요.

## 글로벌 구성 AWS SDKs 및 도구

AWS SDKs 및 AWS Command Line Interface (AWS CLI)와 같은 기타 AWS 개발자 도구를 사용하면 AWS 서비스 APIs. 하지만 이를 시도하기 전에 요청 작업을 수행하는 데 필요한 정를 사용하여 SDK 또는 도구를 구성해야 합니다.

이 정보에는 다음과 같은 항목이 포함됩니다.

- API의 직접 호출자를 식별하는 보안 인증 정보. 자격 증명은 AWS 서버에 대한 요청을 암호화하는 데 사용됩니다. 이 정보를 사용하여 자격 증명을 AWS 확인하고 이와 연결된 권한 정책을 검색할 수 있습니다. 그러면 사용자에게 허용된 작업을 결정할 수 있습니다.
- AWS CLI 또는 SDK에 요청을 처리하는 방법, 요청을 보낼 위치(서비스 AWS 엔드포인트), 응답을 해석하거나 표시하는 방법을 알리는 데 사용하는 기타 구성 세부 정보입니다.

각 SDK 또는 도구는 필요한 보안 인증 및 구성 정보를 제공하는 데 사용할 수 있는 여러 소스를 지원합니다. 일부 소스는 SDK 또는 도구에만 적용되며, 해당 방법을 사용하는 방법에 대한 자세한 사항은 해당 도구 또는 SDK 설명서를 참조해야 합니다.

그러나 AWS SDKs 및 도구는 코드 자체 이외의 기본 소스에서 공통 설정을 지원합니다. 이 섹션은 다음 주제를 포함합니다.

### 주제

- [공유 config 및 credentials 파일을 사용하여 AWS SDKs 및 도구 전역 구성](#)
- [AWS SDKs 및 도구의 공유 config 및 credentials 파일 위치 찾기 및 변경](#)
- [환경 변수를 사용하여 AWS SDKs 및 도구 전역 구성](#)
- [JVM 시스템 속성을 사용하여 및 전역 구성 AWS SDK for Java AWS SDK for Kotlin](#)

## 공유 config 및 credentials 파일을 사용하여 AWS SDKs 및 도구 전역 구성

공유 AWS config 및 credentials 파일은 AWS SDK 또는 도구에 대한 인증 및 구성을 지정할 수 있는 가장 일반적인 방법입니다.

공유 config 및 credentials 파일에는 프로파일 집합이 포함되어 있습니다. 프로파일은 키-값 페어로 구성된 구성 설정 세트로, AWS SDKs, AWS Command Line Interface (AWS CLI) 및 기타 도구에서 사용됩니다. 구성 값은 프로파일이 사용될 때 SDK/도구의 일부 측면을 구성하기 위해 프로파일에 첨부됨

니다. 이러한 파일은 값이 사용자의 로컬 환경에 있는 모든 애플리케이션, 프로세스 또는 SDK에 적용된다는 점에서 “공유”됩니다.

공유 config 및 credentials 파일 모두 ASCII 문자만 포함된 일반 텍스트 파일입니다(UTF-8 인코딩). 이들은 일반적으로 [INI](#) 파일이라고 하는 형식을 취합니다.

## 프로파일

공유 config 및 credentials 파일 내의 설정은 특정 프로파일과 연결됩니다. 파일 안에 여러 프로파일을 정의해, 서로 다른 개발 환경에 적용할 다양한 설정 구성을 만들 수 있습니다.

[default] 프로파일에는 이름이 지정된 특정 프로파일이 지정되지 않은 경우 SDK 또는 도구 작업에 사용되는 값이 포함됩니다. 이름으로 명시적으로 참조할 수 있는 별도의 프로파일을 만들 수도 있습니다. 각 프로파일은 애플리케이션과 시나리오에 따라 서로 다른 설정과 값을 사용할 수 있습니다.

### Note

[default]는 단순히 이름이 지정되지 않은 프로파일입니다. 이 프로파일은 사용자가 프로파일을 지정하지 않을 경우 SDK에서 사용하는 기본 프로파일이기 때문에 default(이)라는 이름이 지정되었습니다. 상속된 기본값을 다른 프로파일에 제공하지 않습니다. [default] 프로파일에서 무언가를 설정하고 명명된 프로파일에서는 설정하지 않으면 명명된 프로파일을 사용할 때 값이 설정되지 않습니다.

## 명명된 프로파일 설정

동일한 파일 안에 [default] 프로파일과 여러 명명된 프로파일이 함께 존재할 수 있습니다. 코드를 실행할 때 SDK나 도구에서 사용할 프로파일의 설정을 선택하려면 다음 설정을 사용하세요. 프로파일은 코드 내부에서 선택할 수도 있고, AWS CLI를 사용할 때 명령별로 지정할 수도 있습니다.

다음을 설정하여 이 기능을 구성하세요.

### AWS\_PROFILE - 환경 변수

이 환경 변수가 명명된 프로파일 또는 “기본값”으로 설정된 경우 모든 SDK 코드와 AWS CLI 명령은 해당 프로파일의 설정을 사용합니다.

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_PROFILE="my_default_profile_name";
```

명령줄을 통해 환경 변수를 설정하는 Windows 예제:

```
setx AWS_PROFILE "my_default_profile_name"
```

## aws.profile - JVM 시스템 속성

JVM에서 실행되는 Kotlin SDK와 Java SDK 2.x의 경우, [aws.profile 시스템 속성을 설정할 수](#) 있습니다. SDK가 서비스 클라이언트를 생성할 때, 코드에서 별도로 재정의하지 않는 한 명명된 프로파일의 설정을 사용합니다. Java SDK 1.x는 이 시스템 속성을 지원하지 않습니다.

### Note

여러 애플리케이션이 실행되는 서버에서 애플리케이션을 운영하는 경우, 기본 프로파일 대신 항상 명명된 프로파일을 사용할 것을 권장합니다. 기본 프로파일은 환경의 모든 AWS 애플리케이션에서 자동으로 선택되며 이들 간에 공유됩니다. 따라서 누군가 자신의 애플리케이션을 위해 기본 프로파일을 수정하면, 다른 애플리케이션에도 의도치 않은 영향을 줄 수 있습니다. 이를 방지하기 위해 공유 config 파일에 명명된 프로파일을 정의하고, 코드에서 해당 프로파일을 지정하여 애플리케이션에서 사용하도록 설정하세요. 적용 범위가 오직 사용자의 애플리케이션에만 영향을 준다는 것이 확실한 경우, 환경 변수나 JVM 시스템 속성을 사용해 명명된 프로파일을 설정할 수도 있습니다.

## 구성 파일 형식

config 파일은 섹션으로 구성됩니다. 섹션은 이름이 지정된 설정 모음이며 다른 섹션 정의 라인을 찾을 때까지 계속됩니다.

config 파일은 다음 형식을 사용하는 일반 텍스트 파일입니다.

- 섹션의 모든 항목은 setting-name=value와 같은 일반적인 형식을 취합니다.
- 줄은 해시태그 문자(#)로 시작하여 주석 처리할 수 있습니다.

## 섹션 유형

섹션 정의는 설정 모음에 이름을 적용하는 줄입니다. 섹션 정의 줄은 대괄호([])로 시작하고 끝납니다. 대괄호 안에는 섹션 유형 식별자와 섹션의 사용자 지정 이름이 있습니다. 문자, 숫자, 하이픈(-) 및 밑줄(\_)은 사용할 수 있지만 공백은 사용할 수 없습니다.

**섹션 유형: default**

섹션 정의 줄의 예: [default]

[default]는 profile 섹션 식별자가 필요하지 않은 유일한 프로파일입니다.

다음은 [default] 프로파일이 있는 기본 config 파일을 보여주는 예입니다. [region](#) 설정값을 설정합니다. 이 줄 이후에 나오는 모든 설정은 다른 섹션 정의가 나타나기 전까지 해당 프로파일에 속하는 것으로 간주됩니다.

```
[default]
#Full line comment, this text is ignored.
region = us-east-2
```

**섹션 유형: profile**

섹션 정의 줄의 예: [profile *dev*]

profile 섹션 정의 줄은 서로 다른 개발 시나리오에 적용할 수 있는 명명된 구성 그룹입니다. 명명된 프로파일의 이해를 높이려면 프로파일의 이전 섹션을 참조하십시오.

다음 예제는 profile 섹션 정의 줄과 foo라고 부르는 명명된 프로파일이 포함된 config 파일을 보여줍니다. 이 줄 이후에 나오는 모든 설정은 다른 섹션 정의가 나타나기 전까지 이 명명된 프로파일에 속하는 것으로 간주됩니다.

```
[profile foo]
...settings...
```

일부 설정에는 다음 예제의 s3 설정 및 하위 설정과 같은 중첩된 자체 하위 설정 그룹이 있습니다. 하나 이상의 공백으로 들여쓰기하여 하위 설정을 그룹과 연결합니다.

```
[profile test]
region = us-west-2
s3 =
    max_concurrent_requests=10
    max_queue_size=1000
```

**섹션 유형: sso-session**

섹션 정의 줄의 예: [sso-session *my-ss0*]

sso-session 섹션 정의 줄은를 사용하여 AWS 자격 증명을 확인하도록 프로필을 구성하는 데 사용하는 설정 그룹의 이름을 지정합니다 AWS IAM Identity Center. Single Sign-On 인증 구성에 대한 자세한 내용은 [IAM Identity Center를 사용하여 AWS SDK 및 도구 인증](#) 섹션을 참조하십시오. 프로파일은 키-값 쌍으로 sso-session 섹션에 연결됩니다. 여기서 sso-session 값은 키이고 sso-session 섹션 이름은 sso-session = <name-of-sso-session-section> 같은 값입니다.

1다음 예에서는 'my-sso'의 토큰을 사용하여 '111122223333' 계정의 'SampleRole' IAM 역할에 대한 단기 AWS 보안 인증을 가져올 프로파일을 구성합니다. "my-sso" sso-session 섹션은 sso-session 키를 사용하여 profile 섹션에서 이름으로 참조됩니다.

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
```

섹션 유형: **services**

섹션 정의 줄의 예: [services dev]

#### Note

이 services 섹션은 서비스별 엔드포인트 사용자 정의를 지원하며 이 기능이 포함된 SDK 및 도구에서만 사용할 수 있습니다. SDK에서 이 기능을 사용할 수 있는지 확인하려면 서비스별 엔드포인트에 대한 [AWS SDKs 도구 지원](#)(를)참조하십시오.

services 섹션 정의 줄은 AWS 서비스 요청에 대한 사용자 지정 엔드포인트를 구성하는 설정 그룹의 이름을 지정합니다. 프로파일은 키-값 쌍으로 services 섹션에 연결됩니다. 여기서 services 값은 키이고 services 섹션 이름은 services = <name-of-services-section> 같은 값입니다.

services 섹션은 <SERVICE> = 줄별로 하위 섹션으로 더 구분됩니다. 여기서는 AWS 서비스 식별자 키<SERVICE>입니다. AWS 서비스 식별자는 모든 공백을 밑줄로 바꾸고 모든 문자를 소문자로 대체serviceId하여 API 모델의를 기반으로 합니다. services 섹션에서 사용할 모든 서비스 식별자 키 목록은 [서비스별 엔드포인트 식별자](#)을 참조하세요. 서비스 식별자 키 뒤에는 각각 고유한 줄에 공백 두 개로 들여쓰기하여 중첩된 설정이 이어집니다.



credentials 파일에서 'default' 프로파일을 사용하든 명명된 프로파일을 사용하든, 여기의 모든 설정은 같은 프로파일 이름을 사용하는 config 파일의 설정과 결합됩니다. 동일한 이름을 공유하는 프로파일에 대한 보안 인증이 두 파일 모두에 있는 경우 보안 인증 파일의 키가 우선합니다.

## AWS SDKs 및 도구의 공유 config 및 credentials 파일 위치 찾기 및 변경

공유 AWS config 및 credentials 파일은 AWS SDKs. 파일은 환경에 로컬로 상주하며 SDK 코드 또는 해당 환경에서 실행하는 AWS CLI 명령에 의해 자동으로 사용됩니다. 개인용 컴퓨터에서나 Amazon Elastic Compute Cloud 인스턴스에서 개발할 때 등을 예로 들 수 있습니다.

SDK나 도구가 실행되면, 이 파일들을 확인한 뒤 사용 가능한 구성 설정을 불러옵니다. 파일이 아직 존재하지 않는 경우, SDK나 도구가 기본 파일을 자동으로 생성합니다.

기본적으로 이러한 파일은 사용자 폴더 또는 home 안에 위치한 .aws 폴더에 저장됩니다.

운영 체제	기본 위치 및 파일 이름
Linux 및 macOS	~/.aws/config ~/.aws/credentials
Windows	%USERPROFILE%\aws\config %USERPROFILE%\aws\credentials

### 홈 디렉터리 해석

~는 다음과 같은 경우에만 홈 디렉터리 해석을 위해 사용됩니다.

- 경로를 시작하는 경우
- 바로 뒤에 / 또는 플랫폼별 구분자가 오는 경우. Windows에서는 ~/와 ~\ 모두 홈 디렉터리로 해석됩니다.

홈 디렉터리를 결정할 때는 다음 변수가 확인됩니다.

- (모든 플랫폼)HOME 환경 변수

- (Windows 플랫폼)USERPROFILE 환경 변수
- (Windows 플랫폼) HOMEDRIVE와 HOMEPATH 환경 변수의 연결(\$HOMEDRIVE\$HOMEPATH)
- (SDK 또는 도구별 선택 사항)SDK 또는 도구별 홈 경로 확인 기능 또는 변수

가능한 경우, 경로의 시작 부분에 사용자의 홈 디렉터리(예:~username/)가 지정되어 있으면 그것은 요청된 사용자 이름의 홈 디렉터리(예: /home/username/.aws/config)로 확정됩니다.

## 이러한 파일의 기본 위치 변경

SDK나 도구가 이 파일들을 불러오는 위치를 재정의하려면, 다음 중 어떤 방법이든 사용할 수 있습니다.

### 환경 변수 사용

다음 환경 변수는 이러한 파일의 위치 또는 이름을 기본값에서 사용자 지정 값으로 변경할 수 있습니다.

- config 파일 환경 변수:**AWS\_CONFIG\_FILE**
- credentials 파일 환경 변수:**AWS\_SHARED\_CREDENTIALS\_FILE**

### Linux/macOS

Linux 또는 macOS에서 다음의 [내보내기](#) 명령을 실행하여 대체 위치를 지정할 수 있습니다.

```
$ export AWS_CONFIG_FILE=/some/file/path/on/the/system/config-file-name
$ export AWS_SHARED_CREDENTIALS_FILE=/some/other/file/path/on/the/system/credentials-file-name
```

### Windows

Windows에서 다음의 [setx](#) 명령을 실행하여 대체 위치를 지정할 수 있습니다.

```
C:\> setx AWS_CONFIG_FILE c:\some\file\path\on\the\system\config-file-name
C:\> setx AWS_SHARED_CREDENTIALS_FILE c:\some\other\file\path\on\the\system\credentials-file-name
```

환경 변수를 사용해 시스템을 구성하는 방법에 대한 자세한 내용은 [환경 변수를 사용하여 AWS SDKs 및 도구 전역 구성](#)에서 확인하세요.

## JVM 시스템 속성 사용

JVM에서 실행되는 Kotlin SDK와 Java SDK 2.x의 경우, 다음 JVM 시스템 속성을 설정하여 이 파일들의 기본 위치나 이름을 사용자 지정 값으로 변경할 수 있습니다.

- config 파일 JVM 시스템 속성: **aws.configFile**
- credentials 파일 환경 변수: **aws.sharedCredentialsFile**

JVM 시스템 속성을 설정하는 방법에 대한 지침은 [the section called “JVM 시스템 속성 설정 방법”](#)에서 확인하세요. Java SDK 1.x는 이러한 시스템 속성을 지원하지 않습니다.

## 환경 변수를 사용하여 AWS SDKs 및 도구 전역 구성

환경 변수는 AWS SDKs 및 도구를 사용할 때 구성 옵션과 자격 증명을 지정하는 또 다른 방법을 제공합니다. 환경 변수는 스크립팅을 수행하거나 명명된 프로파일을 임시로 기본값으로 설정할 때 유용할 수 있습니다. 대부분의 SDK에서 지원하는 환경 변수 목록은 [환경 변수 목록](#) 섹션을 참조하십시오.

### 옵션의 우선 순위

- 환경 변수를 사용하여 설정을 지정하면 공유 AWS config 및 credentials 파일의 프로파일에서 로드된 모든 값이 재정의됩니다.
- AWS CLI 명령줄에서 파라미터를 사용하여 설정을 지정하면 해당 환경 변수 또는 구성 파일의 프로파일에서 모든 값을 재정의합니다.

## 환경 변수를 설정하는 방법

다음은 기본 사용자에게 환경 변수를 구성할 수 있는 방법을 보여주는 예입니다.

Linux, macOS, or Unix

```
$ export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
$ export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
$ export
  AWS_SESSION_TOKEN=AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40lgk
$ export AWS_REGION=us-west-2
```

환경 변수를 설정하면 사용되는 값이 변경되어 쉘 세션이 종료될 때까지 또는 변수를 다른 값으로 설정할 때까지 유지됩니다. 쉘의 스타트업 스크립트에서 변수를 설정하면 해당 변수가 향후 세션에서도 영구적으로 적용되도록 할 수 있습니다.

## Windows Command Prompt

```
C:\> setx AWS_ACCESS_KEY_ID AKIAIOSFODNN7EXAMPLE
C:\> setx AWS_SECRET_ACCESS_KEY wJa1rXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
C:\> setx
AWS_SESSION_TOKEN AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40lglk
C:\> setx AWS_REGION us-west-2
```

환경 변수를 설정하는 데 [set](#)를 사용하면 사용되는 값이 변경되어 현재 명령 프롬프트 세션이 종료될 때까지 또는 변수를 다른 값으로 설정할 때까지 유지됩니다. 환경 변수를 설정하는 데 [setx](#)를 사용하면 현재 명령 프롬프트 세션과 명령 실행 후 생성한 모든 명령 프롬프트 세션에서 사용되는 값이 변경됩니다. 명령을 실행하는 시점에 이미 실행 중인 다른 명령 쉘에는 영향을 주지 않습니다.

## PowerShell

```
PS C:\> $Env:AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
PS C:\> $Env:AWS_SECRET_ACCESS_KEY="wJa1rXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"
PS C:\>
PS C:\> $Env:AWS_SESSION_TOKEN="AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40lglk"
PS C:\> $Env:AWS_REGION="us-west-2"
```

이전 예에 표시된 대로 PowerShell 프롬프트에서 환경 변수를 설정하면 현재 세션 기간에만 해당 값이 저장됩니다. 모든 PowerShell 및 명령 프롬프트 세션에서 환경 변수 설정이 영구적으로 적용되도록 하려면 제어판에서 시스템 애플리케이션을 사용하여 해당 설정을 저장합니다. 또는 PowerShell 프로파일에 변수를 추가하여 향후 모든 PowerShell 세션에 적용되도록 변수를 설정할 수 있습니다. 환경 변수 저장 또는 세션에 영구적 적용에 대한 자세한 내용은 [PowerShell 설명서](#)를 참조하십시오.

## 서버리스 환경 변수 설정

개발에 서버리스 아키텍처를 사용하는 경우 환경 변수를 설정할 수 있는 다른 옵션이 있습니다. 컨테이너에 따라 클라우드가 아닌 환경과 마찬가지로 해당 컨테이너에서 실행되는 코드에 대해 다양한 전략을 사용하여 환경 변수를 보고 액세스할 수 있습니다.

예를 들어를 AWS Lambda 사용하면 환경 변수를 직접 설정할 수 있습니다. 자세한 내용은 AWS Lambda 개발자 안내서의 [AWS Lambda 환경 변수 사용](#)을 참조하세요.

서버리스 프레임워크에서는 환경 설정 아래의 공급자 키 아래에 있는 `serverless.yml` 파일에 SDK 환경 변수를 설정할 수 있는 경우가 많습니다. `serverless.yml` 파일에 대한 자세한 내용은 서버리스 프레임워크 설명서의 [일반 함수 설정](#)을 참조하십시오.

컨테이너 환경 변수를 설정하는 데 사용하는 메커니즘에 관계없이 [정의된 런타임 환경 변수](#)에 Lambda에 대해 문서화된 것과 같이 컨테이너에서 예약한 것도 있습니다. 환경 변수가 처리되는 방식과 제한 사항이 있는지 확인하려면 항상 사용 중인 컨테이너의 공식 설명서를 참조하세요.

## JVM 시스템 속성을 사용하여 및 전역 구성 AWS SDK for Java AWS SDK for Kotlin

[JVM 시스템 속성](#)은 AWS SDK for Java 및와 같이 JVM에서 실행되는 SDKs에 대한 구성 옵션 및 자격 증명을 지정하는 또 다른 방법을 제공합니다 AWS SDK for Kotlin. SDK에서 지원하는 JVM 시스템 속성 목록은 [설정 참조](#)를 확인하세요.

### 옵션의 우선 순위

- JVM 시스템 속성을 사용해 설정 값을 지정하면, 환경 변수나 공유 AWS config 및 credentials 파일의 프로파일에서 불러온 어떤 값보다도 우선하여 적용됩니다.
- 환경 변수를 사용하여 설정을 지정할 경우, 공유 AWS config 및 credentials 파일의 프로파일에서 로드된 값을 재정의합니다.

## JVM 시스템 속성 설정 방법

여러 가지 방법으로 JVM 시스템 속성을 설정할 수 있습니다.

### 명령줄에서

-D 스위치를 사용해 명령을 간접 호출할 때, java 명령줄에서 JVM 시스템 속성을 설정합니다. 다음 명령은 코드에서 값을 명시적으로 재정의하지 않는 한, 모든 서비스 클라이언트에 대해 AWS 리전을 글로벌로 구성합니다.

```
java -Daws.region=us-east-1 -jar <your_application.jar> <other_arguments>
```

여러 JVM 시스템 속성을 설정해야 하는 경우, -D 스위치를 여러 번 지정하면 됩니다.

## 환경 변수 사용

애플리케이션을 실행하기 위해 JVM을 간접 호출하는 명령줄에 접근할 수 없다면, JAVA\_TOOL\_OPTIONS 환경 변수를 사용해 명령줄 옵션을 구성할 수 있습니다. 이 방식은 Java 런타임에서 AWS Lambda 함수를 실행하거나, 임베디드 JVM에서 코드를 실행하는 경우 등에 유용합니다.

다음 예제에서는 코드의 값을 명시적으로 재정의하지 않는 한 모든 서비스 클라이언트에 대해 AWS 리전 전역적으로를 구성합니다.

Linux, macOS, or Unix

```
$ export JAVA_TOOL_OPTIONS="-Daws.region=us-east-1"
```

환경 변수를 설정하면 사용되는 값이 변경되어 셸 세션이 종료될 때까지 또는 변수를 다른 값으로 설정할 때까지 유지됩니다. 셸의 스타트업 스크립트에서 변수를 설정하면 해당 변수가 향후 세션에서도 영구적으로 적용되도록 할 수 있습니다.

Windows Command Prompt

```
C:\> setx JAVA_TOOL_OPTIONS -Daws.region=us-east-1
```

환경 변수를 설정하는 데 [set](#)를 사용하면 사용되는 값이 변경되어 현재 명령 프롬프트 세션이 종료될 때까지 또는 변수를 다른 값으로 설정할 때까지 유지됩니다. 환경 변수를 설정하는 데 [setx](#)를 사용하면 현재 명령 프롬프트 세션과 명령 실행 후 생성한 모든 명령 프롬프트 세션에서 사용되는 값이 변경됩니다. 명령을 실행하는 시점에 이미 실행 중인 다른 명령 셸에는 영향을 주지 않습니다.

## 런타임 시

다음 예제와 같이 System.setProperty 방법을 사용하면, 코드 내에서 런타임 시 JVM 시스템 속성을 설정할 수도 있습니다.

```
System.setProperty("aws.region", "us-east-1");
```

### Important

SDK 서비스 클라이언트를 초기화하기 전에 JVM 시스템 속성을 모두 설정해야 합니다. 그렇지 않으면 서비스 클라이언트가 다른 값을 사용할 수 있습니다.

# AWS SDKs 및 도구를 사용한 인증 및 액세스

AWS SDK 애플리케이션을 개발하거나 사용할 AWS 도구를 사용하는 AWS 서비스 경우 코드 또는 도구가 인증되는 방법을 설정해야 합니다. AWS 코드가 실행되는 환경과 사용 가능한 액세스에 따라 다양한 방식으로 AWS 리소스에 대한 프로그래밍 방식 AWS 액세스를 구성할 수 있습니다.

아래 옵션은 [자격 증명 공급자 체인](#)의 일부입니다. 즉, 그에 따라 공유 AWS config 및 credentials 파일을 구성하면 AWS SDK 또는 도구가 해당 인증 방법을 자동으로 검색하고 사용합니다.

## 애플리케이션 코드를 인증할 메서드 선택

애플리케이션에서 수행한 호출을 인증할 메서드 AWS 드를 선택합니다.

코드 INSIDE a AWS 서비스 (예: Amazon EC2, Lambda, Amazon ECS, Amazon EKS, CodeBuild)를 실행하고 있습니까?

코드가 실행되면 애플리케이션에서 AWS 자격 증명을 자동으로 사용할 수 있습니다. 예를 들어, 애플리케이션이 Amazon Elastic Compute Cloud에서 호스팅되고 해당 리소스에 IAM 역할이 연결되어 있다면, 애플리케이션에 자격 증명이 자동으로 제공됩니다. 마찬가지로, Amazon ECS나 Amazon EKS 컨테이너를 사용하는 경우, 컨테이너 내부에서 실행되는 코드는 SDK의 [자격 증명 공급자 체인](#)을 통해 IAM 역할에 설정된 자격 증명을 자동으로 가져올 수 있습니다.

코드가 Amazon Elastic Compute Cloud 인스턴스에 있나요?

[IAM 역할을 사용하여 Amazon EC2에 배포된 애플리케이션 인증](#) - Amazon EC2 인스턴스에서 IAM 역할을 사용하여 사용자 애플리케이션을 안전하게 실행합니다.

코드가 AWS Lambda 함수에 있습니까?

Lambda는 [Lambda 함수를 생성](#)할 때 최소한의 권한으로 실행 역할을 생성합니다. 그런 다음 AWS SDK 또는 도구는 Lambda 실행 환경을 통해 런타임 시 Lambda에 연결된 IAM 역할을 자동으로 사용합니다.

코드가 Amazon Elastic Container Service(Amazon EC2 또는 Amazon ECS) AWS Fargate 에 있습니까?

작업에 대한 IAM 역할을 사용하세요. [Amazon ECS 작업 정의](#)에서 사용할 [작업 역할을 생성](#)하고, 해당 역할을 명시해야 합니다. 그 후, AWS SDK나 도구는 Amazon ECS 메타데이터를 통해 런타임 시 작업에 할당된 IAM 역할을 자동으로 사용합니다.

코드가 Amazon Elastic Kubernetes Service에 있나요?

[Amazon EKS Pod Identity](#)를 사용하는 것이 좋습니다.

참고: [서비스 계정에 대한 IAM 역할\(IRSA\)](#)이 고유한 요구 사항에 더 적합하다고 판단되면, Amazon EKS 사용 설명서의 [EKS Pod Identity와 IRSA 비교](#)를 참조하세요.

코드가에서 실행되고 있습니까? AWS CodeBuild

[CodeBuild에 대한 ID 기반 정책 사용](#)을 참조하세요.

코드가 다른 AWS 서비스에 있나요?

AWS 서비스에 대한 전용 안내서를 참조하세요. 에서 코드를 실행하면 SDK [자격 증명 공급자 체인](#) AWS이 자동으로 자격 증명을 가져오고 새로 고칠 수 있습니다.

모바일 애플리케이션 또는 클라이언트 기반 웹 애플리케이션을 생성 중입니까?

액세스가 필요한 모바일 애플리케이션 또는 클라이언트 기반 웹 애플리케이션을 생성하는 경우 AWS 웹 자격 증명 연동을 사용하여 임시 AWS 보안 자격 증명을 동적으로 요청하도록 앱을 빌드합니다.

웹 ID 페더레이션을 사용하면 사용자 정의 로그인 코드를 생성하거나 자신의 사용자 보안 인증을 관리할 필요가 없습니다. 대신에, 앱 사용자는 Login with Amazon, Facebook, Google 또는 다른 OpenID Connect(OIDC)호환 IdP와 같은 널리 알려진 외부 ID 제공업체(idP)를 사용해 로그인할 수 있습니다. 인증 토큰을 받은 다음 해당 토큰을 리소스를 사용할 권한이 있는 IAM 역할에 매핑 AWS 되는의 임시 보안 자격 증명으로 교환할 수 있습니다 AWS 계정.

SDK 또는 도구에 맞게 이를 구성하는 방법을 알아보려면 [웹 자격 증명 또는 OpenID Connect를 사용하여 역할을 수입하여 인증 AWS SDKs 및 도구](#)을 참조하십시오.

모바일 애플리케이션의 경우 Amazon Cognito를 사용하는 것이 좋습니다. Amazon Cognito는 ID 브로커로 활동하며 사용자를 대신하여 상당한 페더레이션을 합니다. 자세한 정보는 IAM 사용 설명서의 [모바일 앱용 Amazon Cognito](#)를 참조하십시오.

코드를 로컬로 개발하고 실행하고 있나요?

[콘솔 자격 증명을 사용하여 AWS SDKs 및 도구 인증](#)을 권장합니다.

빠른 브라우저 기반 인증 흐름 후는 AWS CLI, AWS Tools for PowerShell AWS SDKs와 같은 로컬 개발 도구에서 작동하는 임시 자격 증명을 AWS 자동으로 생성합니다.

## AWS 계정 액세스에 Identity Center를 사용하는 경우

이미 AWS 계정에 대한 액세스 권한이 있거나 작업 인력에 대한 액세스를 관리해야 하는 경우 IAM Identity Center를 사용하여 AWS SDK 및 도구를 인증합니다. 보안 모범 사례로 IAM Identity Center AWS Organizations 와 함께 사용하여 모든 AWS 계정에서 액세스를 관리하는 것이 좋습니다. IAM Identity Center에서 사용자를 생성하거나, Microsoft Active Directory를 사용하거나, SAML 2.0 ID 제공업체(IdP)를 사용하거나, IdP를 AWS 계정에 개별적으로 페더레이션할 수 있습니다. 리전에서 IAM Identity Center를 지원하는지 확인하려면 Amazon Web Services 일반 참조의 [IAM Identity Center를 사용하여 AWS SDK 및 도구 인증](#) IAM Identity Center 엔드포인트 및 할당량을 참조하세요.

### 다른 인증 방법을 찾고 있는 경우

에 대한 권한이 있는 최소 권한의 IAM 사용자를 `sts:AssumeRole` 대상 역할에 생성합니다. 그런 다음 해당 사용자에 대한 `source_profile` 설정을 사용하여 역할을 수임하도록 프로필을 구성합니다.

환경 변수 또는 공유 자격 증명 파일을 통해 임시 IAM AWS 자격 증명을 사용할 수도 있습니다. 단기 자격 증명을 사용하여 AWS SDKs.

참고: 샌드박스 또는 학습 환경에서만 장기 자격 증명을 사용하여 AWS SDKs 및 도구를 인증하는 것을 고려할 수 있습니다.

이 코드는 온프레미스 환경에서 실행되고 있나요? 아니면 하이브리드나 온디맨드 VM(예: Amazon S3에 대해 읽거나 쓰는 서버, 혹은 클라우드에 배포하는 Jenkins 등)에서 실행되고 있나요?

X.509 클라이언트 인증서를 사용하고 있나요?

예: [IAM Roles Anywhere를 사용하여 AWS SDKs 및 도구 인증](#)을 참조하세요. IAM Roles Anywhere를 사용하여 외부에서 실행되는 서버, 컨테이너 및 애플리케이션과 같은 워크로드에 대해 IAM에서 임시 보안 자격 증명을 얻을 수 있습니다 AWS. IAM Roles Anywhere를 사용하려면 워크로드에 X.509 인증서를 사용해야 합니다.

환경에서 페더레이션 ID 제공업체(예: Microsoft Entra 또는 Okta)에 안전하게 연결하여 임시 AWS 자격 증명을 요청할 수 있습니까?

예: [프로세스 보안 인증 제공자](#)를 사용하세요.

[프로세스 보안 인증 제공자](#)를 사용하여 런타임 시 자동으로 자격 증명을 가져올 수 있습니다. 이러한 시스템은 도우미 도구 나 플러그인을 사용해 자격 증명을 얻을 수 있으며, 내부적으로는 `sts:AssumeRole`을 통해 IAM 역할을 수임할 수도 있습니다.

아니요:를 통해 주입된 임시 자격 증명 사용 AWS Secrets Manager

를 통해 주입된 임시 자격 증명을 사용합니다 AWS Secrets Manager. 단기 액세스 키를 얻는 방법에 대한 자세한 내용은 IAM 사용 설명서의 [임시 보안 자격 증명 요청](#)을 참조하세요. 이러한 임시 자격 증명을 저장하는 옵션은 [AWS 액세스 키](#)에서 확인하세요.

이러한 자격 증명을 사용하면 프로덕션 비밀이나 장기 역할 기반 자격 증명을 저장할 수 있는 [Secrets Manager](#)에서 더 광범위한 애플리케이션 권한을 안전하게 가져올 수 있습니다.

에 없는 타사 도구를 사용하고 있습니까 AWS?

자격 증명을 얻는 방법에 대해서는 타사 공급자의 문서를 참고하는 것이 가장 좋습니다.

타사에서 문서를 제공하지 않은 경우 임시 자격 증명을 안전하게 입력할 수 있나요?

예: 환경 변수와 임시 AWS STS 자격 증명을 사용합니다.

아니요: 암호화된 암호 관리자(마지막 수단)에 저장된 정적 액세스 키를 사용합니다.

## 인증 방법

AWS 환경 내에서 실행되는 코드에 대한 인증 방법

코드가 실행되면 애플리케이션에서 AWS자격 증명을 자동으로 사용할 수 있습니다. 예를 들어, 애플리케이션이 Amazon Elastic Compute Cloud에서 호스팅되고 해당 리소스에 IAM 역할이 연결되어 있다면, 애플리케이션에 자격 증명이 자동으로 제공됩니다. 마찬가지로, Amazon ECS나 Amazon EKS 컨테이너를 사용하는 경우, 컨테이너 내부에서 실행되는 코드는 SDK의 자격 증명 공급자 체인을 통해 IAM 역할에 설정된 자격 증명을 자동으로 가져올 수 있습니다.

- [IAM 역할을 사용하여 Amazon EC2에 배포된 애플리케이션 인증](#) - Amazon EC2 인스턴스에서 IAM 역할을 사용하여 사용자 애플리케이션을 안전하게 실행합니다.
- 다음과 같은 방법으로 IAM Identity Center를 AWS 사용하여 프로그래밍 방식으로와 상호 작용할 수 있습니다.
  - [AWS CloudShell](#)를 사용하여 콘솔에서 AWS CLI 명령을 실행합니다.
  - 소프트웨어 개발 팀을 위한 클라우드 기반 협업 공간은 [Amazon CodeCatalyst](#)를 고려하십시오.

웹 기반 ID 제공자를 통한 인증 - 모바일 혹은 클라이언트 기반 웹 애플리케이션

액세스가 필요한 모바일 애플리케이션 또는 클라이언트 기반 웹 애플리케이션을 생성하는 경우 AWS 웹 자격 증명 연동을 사용하여 임시 AWS 보안 자격 증명을 동적으로 요청하도록 앱을 빌드합니다.

웹 ID 페더레이션을 사용하면 사용자 정의 로그인 코드를 생성하거나 자신의 사용자 보안 인증을 관리할 필요가 없습니다. 대신에, 앱 사용자는 Login with Amazon, Facebook, Google 또는 다른 OpenID Connect(OIDC)호환 IdP와 같은 널리 알려진 외부 ID 제공업체(idP)를 사용해 로그인할 수 있습니다. 인증 토큰을 받은 다음 해당 토큰을의 리소스를 사용할 권한이 있는 IAM 역할에 매핑 AWS 되는의 임시 보안 자격 증명으로 교환할 수 있습니다 AWS 계정.

SDK 또는 도구에 맞게 이를 구성하는 방법을 알아보려면 [웹 자격 증명 또는 OpenID Connect를 사용하여 역할을 수입하여 인증 AWS SDKs 및 도구](#)을 참조하십시오.

모바일 애플리케이션의 경우 Amazon Cognito를 사용하는 것이 좋습니다. Amazon Cognito는 ID 브로커로 활동하며 사용자를 대신하여 상당한 페더레이션을 합니다. 자세한 정보는 IAM 사용 설명서의 [모바일 애플용 Amazon Cognito](#)를 참조하십시오.

로컬(AWS외부)에서 실행되는 코드의 인증 메서드

- [콘솔 자격 증명을 사용하여 AWS SDKs 및 도구 인증](#) -이 기능은 AWS Command Line Interface와 Tools for PowerShell 모두에서 작동하며 AWS CLI, Tools for PowerShell 및 같은 로컬 개발 도구에서 작동하는 새로 고침 가능한 자격 증명을 제공합니다 AWS.
- [IAM Identity Center를 사용하여 AWS SDK 및 도구 인증](#) - 보안 모범 사례로 IAM Identity Center AWS Organizations 와 함께를 사용하여 모든에서 액세스를 관리하는 것이 좋습니다 AWS 계정. 에서 사용자를 생성하거나 AWS IAM Identity Center, Microsoft Active Directory를 사용하거나, SAML 2.0 ID 제공업체(IdP)를 사용하거나, IdP를 개별적으로 페더레이션할 수 있습니다 AWS 계정. 사용자 리전에서 Identity Center를 지원하는지 확인하려면 Amazon Web Services 일반 참조.의 [AWS IAM Identity Center 엔드포인트 및 할당량](#)을 참조하십시오.
- [IAM Roles Anywhere를 사용하여 AWS SDKs 및 도구 인증](#) - IAM Roles Anywhere를 사용하여 외부에서 실행되는 서버, 컨테이너 및 애플리케이션과 같은 워크로드에 대해 IAM에서 임시 보안 자격 증명을 얻을 수 있습니다 AWS. IAM Roles Anywhere를 사용하려면 워크로드에 X.509 인증서를 사용해야 합니다.
- [자격 AWS 증명이 있는 역할을 수입하여 AWS SDKs 및 도구 인증](#) - IAM 역할을 수입하여 액세스 권한이 없는 AWS 리소스에 일시적으로 액세스할 수 있습니다.
- [AWS 액세스 키를 사용하여 AWS SDKs 및 도구 인증](#) - 편리하지 않거나 AWS 리소스에 대한 보안 위험을 증가시킬 수 있는 다른 옵션.

액세스 관리에 대한 추가 정보

IAM 사용 설명서에는 AWS 리소스에 대한 액세스를 안전하게 제어하는 방법에 대한 다음 정보가 나와 있습니다.

- [IAM 자격 증명\(사용자, 사용자 그룹 및 역할\)](#) -의 자격 증명 기본 사항을 이해합니다 AWS.
- [IAM의 보안 모범 사례 — 공유 책임 모델](#)에 따라 AWS 애플리케이션을 개발할 때 따라야 할 보안 권장 사항.

Amazon Web Services 일반 참조에는 다음에 대한 기본 사항이 있습니다.

- [AWS 보안 인증 이해 및 취득](#) — 콘솔 및 프로그래밍 방식 액세스 모두에 대한 액세스 키 옵션 및 관리 관행.

IAM Identity Center 신뢰할 수 있는 ID 전파(TIP) 플러그인을 사용하여 AWS 서비스에 접근

- [TIP 플러그인을 사용하여 액세스 AWS 서비스](#) - 신뢰할 수 있는 자격 증명 전파를 지원하는 Amazon Q Business 또는 기타 서비스용 애플리케이션을 생성하고 AWS SDK for Java 또는를 사용하는 경우 AWS SDK for JavaScript간소화된 권한 부여 환경을 위해 TIP 플러그인을 사용할 수 있습니다.

## AWS Builder ID

는 이미 소유하거나 생성하려는 모든 AWS 계정 를 AWS Builder ID 보완합니다. 는 사용자가 생성하는 AWS 리소스의 컨테이너 AWS 계정 역할을 하고 해당 리소스에 대한 보안 경계를 제공하지만는 사용자를 개인으로 AWS Builder ID 나타냅니다. 로 로그인하여 Amazon Q 및 Amazon CodeCatalyst와 같은 개발자 도구 및 서비스에 AWS Builder ID 액세스할 수 있습니다.

- AWS 로그인 사용 설명서의 [로 로그인 AWS Builder ID](#) -를 생성 및 사용하는 방법과 Builder ID가 제공하는 내용을 AWS Builder ID 알아봅니다.
- [CodeCatalyst 개념 - Amazon CodeCatalyst 사용 설명서에서 AWS Builder ID](#) - CodeCatalyst에서 AWS Builder ID를 사용하는 방법을 알아보십시오.

## 콘솔 자격 증명을 사용하여 AWS SDKs 및 도구 인증

콘솔 자격 증명을 사용하는 것은 로컬 환경 또는 기타 컴퓨팅이 아닌AWS 서비스 환경에서 AWS 애플리케이션을 개발할 때 자격 AWS 증명을 제공하는 데 권장되는 방법입니다. Amazon Elastic Compute Cloud(Amazon EC2) 또는 AWS CloudShell과 같은 AWS 리소스에서 개발하는 경우 대신 해당 서비스에서 자격 증명을 가져오는 것이 좋습니다.

IAM Identity Center를 통해 인증할 수도 있습니다. [IAM Identity Center를 사용하여 AWS SDK 및 도구 인증](#). 이 옵션은 조직이 작업 인력에 대한 액세스를 관리하는 일반적인 방법이며 Identity Center를 활성화해야 합니다.

## 어떻게 작동하나요?

[콘솔 자격 증명을 사용하여 AWS 로컬 개발을 위한 로그인](#)을 사용하면 기존 AWS Management Console 로그인 자격 증명을 사용하여 AWS 서비스에 프로그래밍 방식으로 액세스할 수 있습니다. 브라우저 기반 인증 흐름 후는 AWS CLI, Tools for PowerShell 및 AWS SDKs와 같은 로컬 개발 도구에서 작동하는 임시 자격 증명을 AWS 생성합니다. 이 기능은 특히 장기 액세스 키를 관리하는 것보다 대화형 인증을 선호하는 경우 AWS CLI 자격 증명을 구성하고 관리하는 프로세스를 간소화합니다.

이 프로세스를 사용하면 초기 계정 설정 중에 생성된 루트 자격 증명, IAM 사용자 또는 자격 증명 공급자의 페더레이션 자격 증명을 사용하여 인증할 수 있습니다.

개발을 위해 SDKs 사용하는 경우 SDK 클라이언트를 통해 임시 자격 증명을 사용합니다. [AWS SDKs 및 도구 표준화 자격 증명 공급자](#). 를 구성할 수도 있습니다. [로그인 자격 증명 공급자](#).

로그인 명령을 통한 인증은 AWS CLI와 Tools for PowerShell에서 모두 지원됩니다.

- [콘솔 자격 증명을 사용하여 AWS 로컬 개발을 위해 로그인](#)
- AWS Tools for PowerShell 사용 설명서의 [콘솔 자격 증명을 사용하여 로그인](#)

## IAM Identity Center를 사용하여 AWS SDK 및 도구 인증

AWS IAM Identity Center 는 AWS 컴퓨팅이 아닌 서비스 환경에서 애플리케이션을 개발할 AWS 때 AWS 자격 증명을 제공하는 데 사용할 수 있습니다. Amazon Elastic Compute Cloud(Amazon EC2) 또는 같은 AWS 리소스에서 개발하는 경우 대신 해당 서비스에서 자격 증명을 가져오는 AWS Cloud9가 좋습니다.

AWS 계정 액세스에 이미 Identity Center를 사용하거나 조직의 액세스를 관리해야 하는 경우 IAM Identity Center 인증을 사용합니다.

이 자습서에서는 IAM Identity Center 액세스를 설정하고 AWS 액세스 포털 및를 사용하여 SDK 또는 도구에 맞게 구성합니다 AWS CLI.

- AWS 액세스 포털은 IAM Identity Center에 수동으로 로그인하는 웹 위치입니다. URL 형식은 `d-xxxxxxxxx.awsapps.com/start` 또는 `your_subdomain.awsapps.com/start`입니다.

AWS 액세스 포털에 로그인하면 해당 사용자에게 대해 구성된 AWS 계정 및 역할을 볼 수 있습니다. 이 절차에서는 AWS 액세스 포털을 사용하여 SDK/도구 인증 프로세스에 필요한 구성 값을 가져옵니다.

- AWS CLI 는 코드에서 수행한 API 호출에 IAM Identity Center 인증을 사용하도록 SDK 또는 도구를 구성하는 데 사용됩니다. 이 일회성 프로세스는 공유 AWS config 파일을 업데이트한 다음 코드를 실행할 때 SDK 또는 도구에서 사용합니다.

## 사전 조건

이 절차를 시작하기 전에, 다음 사항을 완료해야 합니다.

- 이 없는 경우 AWS 계정에 [가입합니다 AWS 계정](#).
- 아직 IAM Identity Center를 활성화하지 않았다면, AWS IAM Identity Center 사용 설명서의 지침에 따라 [IAM Identity Center를 활성화](#)합니다.

## IAM Identity Center를 사용하여 프로그래밍 방식 액세스 구성

### 1 단계: 액세스 설정 및 적절한 권한 세트 선택

자격 AWS 증명에 액세스하려면 다음 방법 중 하나를 선택합니다.

IAM ID 센터를 통한 액세스 권한을 설정하지 않았습니다.

1. AWS IAM Identity Center 사용 설명서의 [기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스 구성](#) 절차를 따라 사용자를 추가하고 관리자 권한을 부여합니다.
2. AdministratorAccess 권한 세트는 일반적인 개발 작업에는 사용해서는 안 됩니다. 대신, 고용주가 이 목적을 위해 별도의 사용자 지정 권한 세트를 만들어 두지 않았다면, 미리 정의된 PowerUserAccess 권한 세트를 사용하는 것을 권장합니다.

동일한 [기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스 구성](#) 절차를 다시 따라 진행 하되, 이번에는 다음을 수행하세요.

- *Admin team* 그룹을 생성하는 대신, *Dev team* 그룹을 생성한 다음 지침에서 이를 대체하여 사용합니다.
- 기존 사용자를 그대로 사용할 수 있지만, 해당 사용자를 새로 만든 *Dev team* 그룹에 추가해야 합니다.
- *AdministratorAccess* 권한 세트를 생성하는 대신, *PowerUserAccess* 권한 세트를 생성한 다음 지침에서 이를 대체하여 사용합니다.

완료되면 다음 항목들이 준비되어 있어야 합니다.

- Dev team 그룹.
  - Dev team 그룹에 연결된 PowerUserAccess 권한 세트.
  - Dev team 그룹에 추가된 사용자.
3. 포털을 종료하고 다시 로그인하여 Administrator 또는에 대한 AWS 계정 및 옵션을 확인합니다. PowerUserAccess. 도구나 SDK를 사용하여 작업할 때는 PowerUserAccess를 선택하세요.

이미 고용주가 관리하는 페더레이션 ID 제공업체(예: Microsoft Entra 또는 Okta)를 AWS 통해 액세스할 수 있습니다.

ID 제공업체의 포털을 AWS 통해 로그인합니다. 클라우드 관리자가 사용자 PowerUserAccess(개발자)에게 권한을 부여한 경우 액세스 권한이 AWS 계정 있는 및 권한 세트가 표시됩니다. 권한 집합 이름 옆에는 해당 권한 집합을 사용하여 수동으로 또는 프로그래밍 방식으로 계정에 액세스할 수 있는 옵션이 표시됩니다.

사용자 지정 구현으로 인해 사용 권한 집합 이름이 달라지는 등 다양한 경험이 발생할 수 있습니다. 어떤 권한 세트를 사용할지 확실하지 않은 경우 IT 팀에 문의하세요.

고용주가 관리하는 AWS 액세스 포털을 AWS 통해 이미 액세스할 수 있음

AWS 액세스 포털을 AWS 통해 로그인합니다. 클라우드 관리자가 사용자 PowerUserAccess(개발자)에게 권한을 부여한 경우 액세스 권한이 있는 AWS 계정 과 권한 집합이 표시됩니다. 권한 집합 이름 옆에는 해당 권한 집합을 사용하여 수동으로 또는 프로그래밍 방식으로 계정에 액세스할 수 있는 옵션이 표시됩니다.

이미 고용주가 관리하는 페더레이션 사용자 지정 ID 제공업체를 AWS 통해 액세스할 수 있습니다.

IT 팀에 문의하십시오.

## 2 단계: IAM Identity Center를 사용할 SDK 및 도구 구성

1. 사용자 개발 시스템에 최신 AWS CLI을 설치합니다.
  - a. 자세한 내용은 AWS Command Line Interface 사용 설명서의 [AWS CLI 최신 버전의 설치 또는 업데이트](#)를 참조하십시오.
  - b. (선택 사항) AWS CLI 이 작동하는지 확인하려면 명령 프롬프트를 열고 `aws --version` 명령을 실행합니다.

2. AWS 액세스 포털에 로그인합니다. 사용자의 고용주가 이 URL을 제공할 수도 있으며 1단계: 액세스 설정 후 이메일로 받을 수도 있습니다. 그렇지 않은 경우, <https://console.aws.amazon.com/singlesignon/>의 대시보드에서 AWS 액세스 포털 URL을 확인합니다.
  - a. AWS 액세스 포털의 계정 탭에서 관리할 개별 계정을 선택합니다. 사용자의 역할이 표시됩니다. 액세스 키를 선택하여 적절한 권한 세트를 위한 명령줄 또는 프로그래밍 방식의 액세스에 대한 자격 증명을 가져옵니다. 사전 정의된 PowerUserAccess 권한 세트를 사용하거나, 사용자 또는 고용주가 개발을 위한 최소 권한을 적용하기 위해 생성한 권한 세트를 사용할 수 있습니다.
  - b. 보안 인증 가져오기 대화 상자에서 운영 체제에 따라 MacOS 및 Linux 또는 Windows를 선택합니다.
  - c. IAM Identity Center 보안 인증 방법을 선택하여 다음 단계에 필요한 Issuer URL 및 SSO Region 값을 가져옵니다. 참고: SSO Start URL은 Issuer URL과 서로 바꿔 사용될 수 있습니다.
3. AWS CLI 명령 프롬프트에서 `aws configure sso` 명령을 실행합니다. 메시지가 표시되면 이전 단계에서 수집한 구성 값을 입력합니다. 이 AWS CLI 명령에 대한 자세한 내용은 [aws configure sso 마법사를 사용하여 프로필 구성을 참조하세요](#).
  - a. 프롬프트 SSO Start URL에 대해 Issuer URL에서 얻은 값을 입력합니다.
  - b. CLI 프로파일 이름의 경우 시작할 때 `###`을 입력하는 것이 좋습니다. 기본이 아닌 (명명된) 프로파일 및 관련 환경 변수를 설정하는 방법에 대한 자세한 내용은 [프로파일을 참조하십시오](#).
4. (선택 사항) AWS CLI 명령 프롬프트에서 `aws sts get-caller-identity` 명령을 실행하여 활성 세션 자격 증명을 확인합니다. 응답에는 구성된 IAM Identity Center 권한 세트가 표시되어야 합니다.
5. AWS SDK를 사용하는 경우 개발 환경에서 SDK용 애플리케이션을 생성합니다.
  - a. 일부 SDK의 경우 IAM Identity Center 인증을 사용하려면 먼저 SSO과 SSO0IDC와 같은 추가 패키지를 애플리케이션에 추가해야 합니다. 자세한 내용은 특정 SDK를 참조하십시오.
  - b. 이전에에 대한 액세스를 구성한 경우 공유 AWS credentials 파일에서를 AWS검토합니다 [AWS 액세스 키, 자격 증명 공급자 체인의 이해](#) 우선 순위로 인해 SDK 또는 도구에서 IAM Identity Center 보안 인증을 사용하려면 먼저 정적 보안 인증을 반드시 제거해야 합니다.

SDK 및 도구가 이 구성을 사용하여 보안 인증을 사용하고 새로 고치는 방법에 대한 자세한 내용은 [AWS SDKs 및 도구에 대한 IAM Identity Center 인증 확인 방법](#)을 참조하십시오.

공유 config 파일에서 IAM Identity Center 공급자 설정을 직접 구성하려면, 이 안내서의 [IAM 아이덴티티 센터 보안 인증 공급자](#)를 참고하세요.

## 포털 액세스 세션 새로 고침

액세스는 결국 만료되며, 그러면 SDK나 도구에서 인증 오류가 발생하게 됩니다. 이 만료가 발생하는 시기는 구성된 세션 길이에 따라 달라집니다. 필요한 경우 액세스 포털 세션을 다시 새로 고치려면 AWS CLI 를 사용하여 `aws sso login` 명령을 실행합니다.

IAM Identity Center 액세스 포털 세션 기간과 권한 설정 세션 기간을 모두 연장할 수 있습니다. 이렇게 하면 코드를 실행하여 수동으로 다시 로그인해야 하는 시간이 길어집니다. AWS CLI 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다음 주제를 참조하세요.

- IAM Identity Center 세션 기간 - [사용자의 AWS 액세스 포털 세션 기간을 구성합니다](#)
- 권한 설정 세션 기간 - 세션 기간을 [설정합니다](#)

## AWS SDKs 및 도구에 대한 IAM Identity Center 인증 확인 방법

### IAM Identity Center 관련 용어

다음 용어는 기본 AWS IAM Identity Center 프로세스와 구성을 이해하는 데 도움이 됩니다. AWS SDK APIs 설명서는 이러한 인증 개념 중 일부에 대해 IAM Identity Center와 다른 이름을 사용합니다. 두 이름을 모두 알고 있으면 도움이 됩니다.

다음 표에서는 이름이 서로 연결되는 방식을 보여줍니다.

IAM Identity Center 이름	SDK API 이름	설명
Identity Center	sso	AWS Single Sign-On의 이름은 변경되지만 sso API 네임스페이스는 이전 버전과의 호환성을 위해 원래 이름을 유지합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 <a href="#">IAM Identity Center 이름 변경</a> 을 참조하십시오.

IAM Identity Center 이름	SDK API 이름	설명
IAM Identity Center 콘솔 관리자 콘솔		싱글 사인온을 구성하는 데 사용하는 콘솔입니다.
AWS 액세스 포털 URL		사용자 IAM ID 센터 계정의 고유한 URL(예 <code>https://xxx.awsapps.com/start</code> ). 사용자 IAM ID 센터 로그인 보안 인증을 사용하여 이 포털에 로그인합니다.
IAM Identity Center 액세스 포털 세션	인증 세션	발신자에게 베어러 액세스 토큰을 제공합니다.
권한 집합 세션		SDK가 내부적으로 AWS 서비스 호출하는 데 사용하는 IAM 세션입니다. 비공식 토론에서는 이를 '역할 세션'이라고 잘못 지칭하는 것을 볼 수 있습니다.
권한 세트 보안 인증	AWS 자격 증명 sigv4 보안 인증	SDK가 실제로 대부분의 AWS 서비스 호출(특히 모든 sigv4 AWS 서비스 호출)에 사용하는 자격 증명입니다. 비공식 토론에서는 이를 '역할 보안 인증'이라고 잘못 지칭하는 것을 볼 수 있습니다.
IAM 아이덴티티 센터 보안 인증 공급자	SSO 보안 인증 공급자	기능을 제공하는 클래스 또는 모듈 같은 보안 인증을 얻는 방법.

## 에 대한 SDK 자격 증명 확인 이해 AWS 서비스

IAM ID 센터 API는 베어러 토큰 보안 인증을 sigv4 보안 인증으로 교환합니다. 대부분은 AWS 서비스 및와 같은 몇 가지 예외를 제외하고 Amazon CodeWhisperer sigv4 APIs Amazon CodeCatalyst. 다음은 애플리케이션 코드에 대한 대부분의 AWS 서비스 호출을 지원하기 위한 자격 증명 확인 프로세스를 설명합니다 AWS IAM Identity Center.

### AWS 액세스 포털 세션 시작

- 사용자 보안 인증으로 세션에 로그인하여 프로세스를 시작하십시오.
  - AWS Command Line Interface ()에서 `aws sso login` 명령을 사용합니다AWS CLI. 아직 활성 세션이 없는 경우 새 IAM Identity Center 세션이 시작됩니다.
- 새 세션을 시작하면 IAM ID 센터로부터 새로 고침 토큰과 액세스 토큰을 받습니다. AWS CLI 또한는 SSO 캐시 JSON 파일을 새 액세스 토큰 및 새로 고침 토큰으로 업데이트하고 SDKs.
- 이미 활성 세션이 있는 경우 AWS CLI 명령은 기존 세션을 재사용하고 기존 세션이 만료될 때마다 만료됩니다. IAM Identity Center 세션의 길이를 설정하는 방법을 알아보려면 AWS IAM Identity Center 사용 설명서 [의 사용자의 AWS 액세스 포털 세션 기간 구성을 참조하세요](#).
- 자주 로그인해야 하는 필요성을 줄이기 위해 최대 세션 길이가 90일로 연장되었습니다.

### SDK가 AWS 서비스 호출에 대한 자격 증명을 가져오는 방법

SDKs 서비스당 클라이언트 객체를 인스턴스화할 AWS 서비스 때에 대한 액세스를 제공합니다. 공유 AWS config 파일의 선택한 프로필이 IAM Identity Center 자격 증명 확인을 위해 구성된 경우 IAM Identity Center는 애플리케이션의 자격 증명을 확인하는 데 사용됩니다.

- [보안 인증 확인 프로세스](#)는 클라이언트가 생성되면 런타임 중에 완료됩니다.

IAM ID 센터 싱글 사인온을 사용하여 sigv4 API의 보안 인증을 가져오기 위해 SDK는 IAM ID 센터 액세스 토큰을 사용하여 IAM 세션을 가져옵니다. 이 IAM 세션을 권한 세트 세션이라고 하며, IAM 역할을 수입하여 SDK에 대한 AWS 액세스를 제공합니다.

- 권한 세트 세션 기간은 IAM ID 센터 세션 기간과 별개로 설정됩니다.
  - 권한 설정 세션 기간을 설정하는 방법을 알아보려면 사용 AWS IAM Identity Center 설명서의 [세션 기간 설정](#)을 참조하십시오.
- 권한 세트 자격 증명은 대부분의 AWS SDK API 설명서에서 AWS 자격 증명 및 sigv4 자격 증명이라고도 합니다.

IAM ID 센터 API의 [GetRoleCredentials](#)를 직접 호출하면 권한 세트 보안 인증이 SDK로 반환됩니다. SDK의 클라이언트 객체는 수입한 IAM 역할을 사용하여 Amazon S3에 계정의 버킷을 나열하도록 요청하는 AWS 서비스등을 호출합니다. 클라이언트 객체는 권한 설정 세션이 만료될 때까지 해당 권한 집합 보안 인증을 사용하여 계속 작동할 수 있습니다.

## 세션 만료 및 새로 고침

[SSO 토큰 공급자 구성](#)를 사용하는 경우 IAM Identity Center에서 가져온 시간별 액세스 토큰은 새로 고침 토큰을 사용하여 자동으로 새로 고쳐집니다.

- SDK가 액세스 토큰을 사용하려고 할 때 액세스 토큰이 만료되면 SDK는 새로 고침 토큰을 사용하여 새 액세스 토큰을 가져오려고 합니다. IAM ID 센터는 새로 고침 토큰을 IAM ID 센터 액세스 포털 세션 기간과 비교합니다. 새로 고침 토큰이 만료되지 않은 경우 IAM ID 센터는 다른 액세스 토큰으로 응답합니다.
- 이 액세스 토큰은 기존 클라이언트의 권한 설정 세션을 새로 고치거나 새 클라이언트의 보안 인증을 확인하는 데 사용할 수 있습니다.

하지만 IAM Identity Center 액세스 포털 세션이 만료되면 새 액세스 토큰이 부여되지 않습니다. 따라서 권한 세트 기간은 갱신할 수 없습니다. 캐시된 권한 세트 세션 기간이 초과되면 기존 클라이언트가 만료되고 액세스를 하지 못합니다.

새 클라이언트를 생성하는 모든 코드는 IAM Identity Center 세션이 만료되는 즉시 인증에 실패합니다. 권한 세트 보안 인증이 캐시되지 않기 때문입니다. 유효한 액세스 토큰을 확보하기 전까지는 코드를 사용하여 새 클라이언트를 만들고 보안 인증 확인 프로세스를 완료할 수 없습니다.

요약하자면, SDK에 새 권한 집합 보안 인증이 필요한 경우 SDK는 먼저 유효한 기존 보안 인증을 확인하고 이를 사용합니다. 이는 보안 인증이 새 클라이언트용이든 보안 인증이 만료된 기존 클라이언트용이든 상관없이 적용됩니다. 보안 인증을 찾을 수 없거나 유효하지 않은 경우 SDK는 IAM Identity Center API를 직접 호출하여 새 보안 인증을 가져옵니다. API를 직접 호출하려면 액세스 토큰이 필요합니다. 액세스 토큰이 만료되면 SDK는 새로 고침 토큰을 사용하여 IAM Identity Center 서비스로부터 새 액세스 토큰을 가져오려고 시도합니다. 이 토큰은 IAM Identity Center 액세스 포털 세션이 만료되지 않은 경우 부여됩니다.

## IAM Roles Anywhere를 사용하여 AWS SDKs 및 도구 인증

IAM Roles Anywhere를 사용하여 외부에서 실행되는 서버, 컨테이너 및 애플리케이션과 같은 워크로드에 대해 IAM에서 임시 보안 자격 증명을 가져올 수 있습니다 AWS. IAM Roles Anywhere를 사용하여

면 워크로드에 X.509 인증서를 사용해야 합니다. 클라우드 관리자는 IAM Roles Anywhere를 보안 인증 공급자로 구성하는 데 필요한 인증서와 프라이빗 키를 제공해야 합니다.

## 1단계: IAM Roles Anywhere 구성

IAM Roles Anywhere는 외부에서 실행되는 워크로드 또는 프로세스에 대한 임시 자격 증명을 가져오는 방법을 제공합니다. 인증 권한에 트러스트 앵커를 설정하여 관련 IAM 역할에 대한 임시 보안 인증을 가져옵니다. 역할에서 코드가 IAM Roles Anywhere로 인증될 때 워크로드가 갖게 될 권한을 설정합니다.

트러스트 앵커, IAM 역할 및 IAM Roles Anywhere 프로파일을 설정하는 단계는 IAM [Roles Anywhere 사용 설명서의 AWS Identity and Access Management Roles Anywhere에서 트러스트 앵커 및 프로파일 생성을 참조](#)하세요.

### Note

IAM Roles Anywhere 사용 설명서의 프로파일은 IAM Roles Anywhere 서비스 내의 고유한 개념을 말합니다. 공유 AWS config 파일 내의 프로필과는 관련이 없습니다.

## 2단계: IAM Roles Anywhere 사용

IAM Roles Anywhere에서 임시 보안 인증을 가져오려면 IAM Roles Anywhere에서 제공하는 보안 인증 도우미 도구를 사용합니다. 보안 인증 도구는 IAM Roles Anywhere의 서명 프로세스를 구현합니다.

자격 증명 헬퍼 도구를 다운로드하는 지침은 IAM [AWS Identity and Access Management Roles Anywhere 사용 설명서의 Roles Anywhere에서 임시 보안 자격 증명 얻기](#)를 참조하세요.

IAM Roles Anywhere의 임시 보안 자격 증명을 AWS SDKs 및와 함께 사용하려면 공유 AWS config 파일에서 `credential_process` 설정을 구성할 AWS CLI 수 있습니다. SDKs 및는가 인증에 사용하는 프로세스 자격 증명 공급자 `credential_process`를 AWS CLI 지원합니다. 다음은 `credential_process` 설정의 일반 구조를 보여줍니다.

```
credential_process = [path to helper tool] [command] [--parameter1 value] [--parameter2 value] [...]
```

도우미 도구의 `credential-process` 명령은 `credential_process` 설정과 호환되는 표준 JSON 형식의 임시 보안 인증을 반환합니다. 명령 이름에는 하이픈이 포함되지만 설정 이름에는 밑줄이 포함된다는 점에 유의하십시오. 명령에는 다음과 같은 파라미터를 요구합니다.

- `private-key` - 요청에 서명한 개인 키의 경로.
- `certificate` - 보안 인증의 경로.
- `role-arn` - 임시 보안 인증을 가져올 역할의 ARN.
- `profile-arn` - 지정된 역할에 대한 매핑을 제공하는 프로파일의 ARN.
- `trust-anchor-arn` - 트러스트 앵커의 ARN.

클라우드 관리자가 인증서와 프라이빗 키를 제공해야 합니다. AWS Management Console에서 세 개의 ARN 값을 모두 복사할 수 있습니다. 다음 예는 도우미 도구에서 임시 보안 인증을 검색하도록 구성하는 공유 config 파일을 보여줍니다.

```
[profile dev]
credential_process = ./aws_signing_helper credential-process --certificate /
path/to/certificate --private-key /path/to/private-key --trust-anchor-
arn arn:aws:rolesanywhere:region:account:trust-anchor/TA_ID --profile-
arn arn:aws:rolesanywhere:region:account:profile/PROFILE_ID --role-
arn arn:aws:iam::account:role/ROLE_ID
```

선택적 파라미터 및 추가 도우미 도구 세부 정보는 GitHub의 [IAM Roles Anywhere 보안 인증 도우미를](#) 참조하십시오.

SDK 구성 설정 자체 및 프로세스 보안 인증 공급자에 대한 자세한 내용은 이 설명서의 [프로세스 보안 인증 제공자](#)를 참조하십시오.

## 자격 AWS 증명이 있는 역할을 수임하여 AWS SDKs 및 도구 인증

역할 수임에는 액세스 권한이 없을 수 있는 AWS 리소스에 액세스하기 위해 일련의 임시 보안 인증을 사용하는 것이 포함됩니다. 이러한 임시 보안 인증은 액세스 키 ID, 보안 액세스 키 및 보안 토큰으로 구성됩니다. AWS Security Token Service (AWS STS) API 요청에 대해 자세히 알아보려면 AWS Security Token Service API 참조의 [작업](#)을 참조하세요.

역할을 수임하도록 SDK 또는 도구를 설정하려면 먼저 수임할 특정 역할을 만들거나 식별해야 합니다. IAM 역할은 Amazon 리소스 이름(ARN) 역할로 고유하게 식별됩니다. 역할은 다른 엔티티와 신뢰 관계를 구축합니다. 역할을 사용하는 신뢰할 수 있는 엔티티는 AWS 서비스 또는 다른 엔티티일 수 있습니다. AWS 계정. IAM 역할에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 역할](#) 섹션을 참조하십시오.

IAM 역할을 식별한 후 해당 역할을 신뢰할 수 있는 경우 해당 역할에서 부여한 권한을 사용하도록 SDK 또는 도구를 구성할 수 있습니다.

**Note**

가능하면 리전 엔드포인트를 사용하고를 구성하는 것이 AWS 가장 좋습니다 [AWS 리전](#).

## IAM 역할 수입

역할을 수입할 때는 임시 보안 자격 증명 세트를 AWS STS 반환합니다. 이러한 보안 인증은 다른 프로파일이나 코드가 실행되는 인스턴스 또는 컨테이너에서 제공됩니다. 일반적으로 이런 형태의 역할 수입은 한 계정의 AWS 자격 증명은 가지고 있지만, 애플리케이션이 다른 계정의 리소스에 접근해야 할 때 가장 많이 사용됩니다.

### 1단계: IAM 역할 설정

역할을 수입하도록 SDK 또는 도구를 설정하려면 먼저 수입할 특정 역할을 만들거나 식별해야 합니다. IAM 역할은 역할 [ARN](#)을 사용하여 고유하게 식별됩니다. 역할은 일반적으로 계정 내에서 또는 크로스 계정 액세스를 위해 다른 엔티티와 신뢰 관계를 구축합니다. 자세한 내용은 IAM 사용 설명서의 [IAM 역할 생성](#)을 참조하십시오.

### 2단계: SDK 또는 도구 구성

`credential_source` 또는 `source_profile`에서 보안 인증을 소싱하도록 SDK 또는 도구를 구성합니다.

Amazon ECS 컨테이너, Amazon EC2 인스턴스 또는 환경 변수에서 보안 인증을 소싱하는 데 `credential_source`를 사용합니다.

다른 프로파일에서 보안 인증을 소싱하는 데 `source_profile`을 사용합니다. `source_profile`은 또한 수입된 역할을 사용하여 다른 역할을 수입하는 프로파일 계층 구조인 역할 체인을 지원합니다.

프로필에서 이를 지정하면 SDK 또는 도구가 자동으로 해당 AWS STS [AssumeRole](#) API 호출을 수행합니다. 역할을 수입하여 임시 자격 증명을 검색하고 사용하려면 공유 AWS config 파일에 다음 구성 값을 지정합니다. 이러한 설정에 대한 자세한 내용은 [역할 보안 인증 제공자 수입 설정](#) 섹션을 참조하십시오.

- `role_arn` - 1단계에서 생성한 IAM 역할에서
- `credential_source` 또는 `source_profile` 중 하나를 구성
- (선택 사항) `duration_seconds`



SDK에서 IAM 역할을 구성한 후 해당 역할이 자격 증명 공급자를 신뢰하도록 구성된 경우 임시 AWS 자격 증명을 가져오기 위해 해당 역할을 수입하도록 SDK를 추가로 구성할 수 있습니다.

### Note

가능하면 리전 엔드포인트를 사용하고를 구성하는 것이 AWS 가장 좋습니다 [AWS 리전](#).

## 웹 자격 증명 또는 OpenID Connect와 페더레이션

Login With Amazon, Facebook, Google과 같은 퍼블릭 자격 증명 공급자의 JSON 웹 토큰(JWTs)을 사용하여 사용하여 임시 AWS 자격 증명을 가져올 수 있습니다 `AssumeRoleWithWebIdentity`. 사용 방식에 따라 이러한 JWT는 ID 토큰 또는 액세스 토큰이라고 불릴 수 있습니다. 또한 EntraID나 PingFederate처럼 OIDC 디스커버리 프로토콜을 지원하는 ID 제공업체(idP)가 발급한 JWT도 사용할 수 있습니다.

Amazon Elastic Kubernetes Service를 사용하는 경우, 이 기능을 통해 Amazon EKS 클러스터 내 각 서비스 계정마다 서로 다른 IAM 역할을 지정할 수 있습니다. 이 Kubernetes 기능은 JWTs 포드에 배포한 다음이 자격 증명 공급자가 임시 AWS 자격 증명을 얻는 데 사용합니다. 이 Amazon EKS 구성에 대한 자세한 내용은 Amazon EKS 사용 설명서의 [서비스 계정에 대한 IAM 역할](#)을 참조하세요. 그러나 더 간단한 옵션을 원하면 [SDK에서 지원하는 경우 Amazon EKS Pod Identity](#)를 대신 사용하는 것이 좋습니다.

### 1단계: 보안 인증 공급자 및 IAM 역할 설정

외부 IdP와의 페더레이션을 구성하려면 IAM 자격 증명 공급자를 사용하여 외부 IdP 및 해당 구성에 AWS 대해 알립니다. 이렇게 하면 AWS 계정 와 외부 IdP 간에 신뢰가 설정됩니다. SDK에서 인증을 위해 JSON 웹 토큰(JWT)을 사용하도록 구성하기 전에, 먼저 ID 제공업체(idP)와 해당 idP에 접근하는 데 사용될 IAM 역할을 설정해야 합니다. 이러한 설정을 하려면 IAM 사용 설명서의 [웹 보안 인증 또는 OpenID Connect 페더레이션을 위한 역할 생성\(콘솔\)](#)을 참조하십시오.

### 2단계: SDK 또는 도구 구성

AWS STS 인증을 위한 JSON 웹 토큰(JWT)을 사용하도록 SDK 또는 도구를 구성합니다.

프로필에서 이를 지정하면 SDK 또는 도구가 자동으로 해당 AWS STS `AssumeRoleWithWebIdentity` API 호출을 수행합니다. 웹 자격 증명 연동을 사용하여 임시 자격 증명을 검색하고 사용하려면 공유 AWS config 파일에 다음 구성 값을 지정합니다. 이러한 설정에 대한 자세한 내용은 [역할 보안 인증 제공자 수입 설정](#) 섹션을 참조하십시오.

- `role_arn` - 1단계에서 생성한 IAM 역할에서
- `web_identity_token_file`- 외부 IdP에서
- (선택 사항) `duration_seconds`
- (선택 사항) `role_session_name`

다음은 웹 ID를 사용하여 역할을 수입하는 공유 config 파일 구성의 예입니다.

```
[profile web-identity]
role_arn=arn:aws:iam::123456789012:role/my-role-name
web_identity_token_file=/path/to/a/token
```

### Note

모바일 애플리케이션의 경우 Amazon Cognito를 사용하는 것이 좋습니다. Amazon Cognito는 ID 브로커로 활동하며 사용자를 대신하여 상당한 페더레이션을 합니다. 하지만 Amazon Cognito 보안 인증 공급자는 다른 보안 인증 공급자처럼 SDK 및 도구 코어 라이브러리에 포함되지 않습니다. Amazon Cognito API에 액세스하려면 SDK 또는 도구용 빌드 또는 라이브러리에 Amazon Cognito 서비스 클라이언트를 포함시키십시오. AWS SDKs. [https://docs.aws.amazon.com/cognito/latest/developerguide/service\\_code\\_examples.html](https://docs.aws.amazon.com/cognito/latest/developerguide/service_code_examples.html) Amazon Cognito

모든 역할 수입 보안 인증 공급자 설정에 대한 자세한 내용은 이 안내서의 [역할 보안 인증 제공자 수입](#)을 참조하세요.

## AWS 액세스 키를 사용하여 AWS SDKs 및 도구 인증

AWS 액세스 키 사용은 AWS SDKs.

### 단기 보안 인증 정보를 사용합니다

연장된 세션 기간 옵션 사용에 [IAM Identity Center를 사용하여 AWS SDK 및 도구 인증](#)을 사용하도록 SDK 또는 도구를 구성하는 것이 좋습니다.

하지만 SDK 또는 도구의 임시 보안 인증을 직접 설정하려면 [단기 자격 증명을 사용하여 AWS SDKs 및 도구 인증](#)을 참조하십시오.

## 장기 보안 인증 정보 사용

### ⚠ Warning

보안 위험을 방지하려면 목적별 소프트웨어를 개발하거나 실제 데이터로 작업할 때 IAM 사용자를 인증에 사용하지 마십시오. 대신 [AWS IAM Identity Center](#)과 같은 보안 인증 공급자를 통한 페더레이션을 사용하십시오.

## 에서 액세스 관리 AWS 계정

보안 모범 사례로 IAM Identity Center AWS Organizations 와 함께 사용하여 모든에서 액세스를 관리하는 것이 좋습니다 AWS 계정. 자세한 내용은 IAM 사용 설명서의 [IAM의 보안 모범 사례](#)를 참조하세요.

IAM Identity Center에서 사용자를 생성하거나, Microsoft Active Directory를 사용하거나, SAML 2.0 ID 제공업체(IdP)를 사용하거나, IdP에 개별적으로 페더레이션할 수 있습니다 AWS 계정. 이러한 접근 방식 중 하나를 사용하면 사용자에게 Single Sign-On 경험을 제공할 수 있습니다. 다중 인증(MFA)을 적용하고 AWS 계정 액세스에 임시 자격 증명을 사용할 수도 있습니다. 이는 공유할 수 있는 장기 보안 인증 정보이며 AWS 리소스에 대한 보안 위험을 증가시킬 수 있는 IAM 사용자와는 다릅니다.

## 샌드박스 환경에서만 사용할 IAM 사용자 생성

를 처음 사용하는 경우 테스트 IAM 사용자를 AWS생성한 다음 이를 사용하여 자습서를 실행하고 제공해야 할 사항을 살펴볼 수 AWS 있습니다. 학습 중에는 이러한 유형의 보안 인증 정보를 사용해도 괜찮지만 샌드박스 환경 밖에서는 사용하지 않는 것이 좋습니다.

다음 사용 사례의 경우에서 IAM 사용자를 시작하는 것이 합리적일 수 있습니다. AWS

- AWS SDK 또는 도구를 시작하고 AWS 서비스 샌드박스 환경에서 탐색합니다.
- 사람이 직접 진행하는 로그인 프로세스를 지원하지 않는 예약된 스크립트, 작업 및 기타 자동화된 프로세스를 학습의 일부로 실행하세요.

이러한 사용 사례 외부에서 IAM 사용자를 사용하는 경우 가능한 한 AWS 계정 빨리 IAM Identity Center로 전환하거나 ID 제공업체를 로 페더레이션합니다. 자세한 내용은 [AWS에서 자격 증명 공급자 및 페더레이션](#)을 참조하세요.

## 보안 IAM 사용자 액세스 키

IAM 사용자 액세스 키는 정기적으로 교체해야 합니다. IAM 사용자 설명서의 [액세스 키 교체](#)에 있는 지침을 따르세요. 실수로 IAM 사용자 액세스 키를 공유했다고 생각되면 액세스 키를 교체하세요.

IAM 사용자 액세스 키는 로컬 시스템의 공유 AWS credentials 파일에 저장해야 합니다. 코드에 IAM 사용자 액세스 키를 저장하지 마세요. IAM 사용자 액세스 키가 포함된 구성 파일을 소스 코드 관리 소프트웨어에 포함시키지 마세요. 오픈 소스 프로젝트 [git-secrets](#)와 같은 외부 도구를 사용하면 중요한 정보를 실수로 Git 리포지토리에 커밋하는 것을 방지할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 [IAM ID\(사용자, 그룹 및 역할\)](#)을 참조하십시오.

IAM 사용자 시작을 설정하려면 [장기 자격 증명을 사용하여 AWS SDKs 및 도구 인증](#)을 참조하십시오.

## 단기 자격 증명을 사용하여 AWS SDKs 및 도구 인증

확장 세션 기간 옵션과 [IAM Identity Center를 사용하여 AWS SDK 및 도구 인증](#) 함께 사용하도록 AWS SDK 또는 도구를 구성하는 것이 좋습니다. 그러나 AWS 액세스 포털에서 사용할 수 있는 임시 자격 증명을 복사하고 사용할 수 있습니다. 보안 인증이 만료되면 새 보안 인증을 복사해야 합니다. 프로파일에서 임시 보안 인증을 사용하거나 이를 시스템 속성 및 환경 변수의 값으로 사용할 수 있습니다.

모범 사례: 자격 증명 파일에서 액세스 키와 토큰을 수동으로 관리하는 대신, 애플리케이션이 다음 경우를 통해 제공되는 임시 자격 증명을 사용하도록 하는 것을 권장합니다.

- Amazon Elastic Compute Cloud 또는에서 애플리케이션을 실행하는 것과 같은 AWS 컴퓨팅 서비스입니다 AWS Lambda.
- 자격 증명 공급자 체인에 있는 다른 옵션(예: [IAM Identity Center를 사용하여 AWS SDK 및 도구 인증](#))을 사용하는 경우.
- 또는 [프로세스 보안 인증 제공자](#)를 사용해 임시 자격 증명을 가져오는 경우.

AWS 액세스 포털에서 검색한 단기 자격 증명을 사용하여 자격 증명 파일 설정

1. [공유 보안 인증 파일 생성](#).
2. 보안 인증 파일에 임시 동작 보안 인증을 붙여 넣을 때까지 다음 자리 표시자 텍스트를 붙여 넣습니다.

```
[default]
aws_access_key_id=<value from AWS access portal>
aws_secret_access_key=<value from AWS access portal>
```



IAM 사용자를 사용하여 코드를 실행하는 경우 개발 환경의 SDK 또는 도구는 공유 AWS credentials 파일의 장기 IAM 사용자 자격 증명을 사용하여 인증합니다. [IAM의 보안 모범 사례](#) 주제를 검토하고 가능한 한 빨리 IAM Identity Center 또는 기타 임시 보안 인증으로 전환하십시오.

## 보안 인증에 대한 중요 경고 및 지침

### 보안 인증에 대한 경고

- 금지 사항. AWS 리소스에 액세스할 때는 계정의 루트 보안 인증을 사용해서는 안 됩니다. 이 보안 인증은 계정 액세스에 제한이 없고 취소하기 어렵습니다.
- 금지 사항. 애플리케이션 파일에 리터럴 액세스 키나 보안 인증 정보를 넣으면 안 됩니다. 이를 어기는 경우, 예를 들어 프로젝트를 퍼블릭 리포지토리에 업로드하면 뜻하지 않게 보안 인증이 노출될 위험이 있습니다.
- 금지 사항. 프로젝트 영역에 보안 인증이 포함된 파일을 포함하지 마십시오.
- 공유 AWS credentials 파일에 저장된 모든 자격 증명은 일반 텍스트로 저장됩니다.

### 보안 인증 정보를 안전하게 관리하기 위한 추가 지침

자격 AWS 증명을 안전하게 관리하는 방법에 대한 일반적인 설명은 [AWS 액세스 키 관리 모범 사례](#)를 참조하세요. [AWS 일반 참조](#). 해당 설명과 더불어 다음 사항을 고려하십시오.

- Amazon Elastic Container Service(Amazon ECS) 작업에 [작업용 IAM 역할](#)을 사용하십시오.
- Amazon EC2 인스턴스에서 실행 중인 애플리케이션에 [IAM 역할](#)을 사용하십시오.

## 사전 조건: AWS 계정 생성

IAM 사용자를 사용하여 AWS 서비스에 액세스하려면 AWS 계정과 AWS 자격 증명에 필요합니다.

### 1. 계정을 생성합니다.

AWS 계정을 생성하려면 AWS Account Management 참조 안내서의 [시작하기: 처음 AWS 사용하시나요?](#)를 참조하세요.

### 2. 관리 사용자를 생성합니다.

관리 콘솔 및 서비스에 액세스하기 위해 루트 사용자 계정(사용자가 생성하는 초기 계정)을 사용하지 않습니다. 대신 IAM 사용 설명서의 [관리 사용자 생성](#)에 설명된 대로 관리 사용자 계정을 생성합니다.

관리 사용자 계정을 만들고 로그인 세부 정보를 기록한 후 반드시 루트 사용자 계정에서 로그아웃하고 관리 계정을 사용하여 다시 로그인합니다.

이러한 계정 중 어느 것도에서 개발을 수행 AWS 하거나에서 애플리케이션을 실행하는 데 적합하지 않습니다 AWS. 모범 사례로서 이러한 작업에 적합한 사용자, 권한 집합 및 서비스 역할을 만들어야 합니다. 자세한 정보는 IAM 사용 설명서의 [최소 권한 적용](#)을 참조하십시오.

## 1단계: IAM 사용자 생성

- IAM 사용 설명서의 [IAM 사용자 생성\(콘솔\)](#) 절차에 따라 IAM 사용자를 생성합니다. IAM 사용자를 생성하는 경우:
  - AWS Management Console에 대한 사용자 액세스 권한 제공을 선택하는 것이 좋습니다. 이를 통해 실행 중인 코드와 관련된 AWS 서비스 를 시각적 환경에서 확인할 수 있습니다. 예를 들어 AWS CloudTrail 진단 로그를 확인하거나 Amazon Simple Storage Service에 파일을 업로드하는 등의 작업을 수행할 수 있습니다. 이는 코드 디버깅에 도움이 됩니다.
  - 권한 설정 - 권한 옵션에서 이 사용자에게 권한을 부여하는 방식으로 정책 직접 연결을 선택합니다.
    - 대부분의 “시작하기” SDK 자습서에서는 Amazon S3 서비스를 예로 사용합니다. 애플리케이션에 Amazon S3에 대한 전체 액세스 권한을 제공하려면 이 사용자에게 연결할 AmazonS3FullAccess 정책을 선택하십시오.
  - 해당 절차에서 권한 경계나 태그를 설정하는 선택적 단계는 무시해도 됩니다.

## 2단계: 액세스 키 가져오기

1. IAM 콘솔의 탐색 창에서 사용자를 선택한 다음 이전에 생성한 사용자의 **User name**을 선택합니다.
2. 사용자 페이지에서 보안 보안 인증 페이지를 선택합니다. 그런 다음 액세스 키에서 액세스 키 생성을 선택합니다.
3. 액세스 키 생성 1단계에서 명령줄 인터페이스(CLI)또는 로컬 코드를 선택합니다. 두 옵션 모두 AWS CLI 및 SDKs 모두에 사용할 동일한 유형의 키를 생성합니다.
4. 액세스 키 만들기 2단계에서 선택적 태그를 입력하고 다음을 선택합니다.
5. 액세스 키 생성 3단계에서 .csv 파일 다운로드를 선택하여 IAM 사용자의 액세스 키 및 보안 액세스 키와 함께 .csv 파일을 저장합니다. 나중에 이 정보가 필요합니다.

**⚠ Warning**

적절한 보안 조치를 사용하여 이러한 보안 인증을 안전하게 유지합니다.

- 완료(Done)를 선택합니다.

### 3단계: **credentials** 파일 업데이트

- 공유 AWS credentials 파일을 생성하거나 엽니다. 이 파일은 Linux 및 macOS 시스템의 경우 `~/.aws/credentials`이며, Windows의 경우 `%USERPROFILE%\aws\credentials`입니다. 자세한 내용은 [보안 인증 파일 위치](#)를 참조하십시오.
- 다음 텍스트를 공유 credentials 파일에 추가합니다. 예제 ID 값 및 예제 키 값을 이전에 다운로드한 .csv 파일의 값으로 바꾸십시오.

```
[default]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
```

- 파일을 저장합니다.

공유 credentials 파일은 보안 인증을 저장하는 가장 일반적인 방법입니다. 환경 변수로 설정할 수도 있습니다. 환경 변수 이름은 [AWS 액세스 키](#) 섹션을 참조하십시오. 이 방법으로 시작할 수 있지만 가능한 한 빨리 IAM Identity Center 또는 기타 임시 보안 인증으로 전환하는 것이 좋습니다. 장기 보안 인증을 사용하지 않도록 전환한 후에는 공유 credentials 파일에서 해당 보안 인증을 삭제해야 합니다.

## IAM 역할을 사용하여 Amazon EC2에 배포된 애플리케이션 인증

이 예제에서는 Amazon Elastic Compute Cloud 인스턴스에 배포된 애플리케이션에서 사용할 Amazon S3 액세스 권한이 있는 AWS Identity and Access Management 역할을 설정하는 방법을 다룹니다.

Amazon Elastic Compute Cloud 인스턴스에서 AWS SDK 애플리케이션을 실행하려면 IAM 역할을 생성한 다음 Amazon EC2 인스턴스에 해당 역할에 대한 액세스 권한을 부여합니다. 자세한 내용은 Amazon EC2 사용 설명서의 [Amazon EC2의 IAM 역할](#)을 참조하세요.

## IAM 역할 생성

개발하는 AWS SDK 애플리케이션은 작업을 수행하기 AWS 서비스 위해 하나 이상의에 액세스할 수 있습니다. 애플리케이션을 실행하는 데 필요한 권한을 부여하는 IAM 역할을 생성합니다.

이 절차에서는 예시로 Amazon S3에 대한 읽기 전용 액세스 권한을 부여하는 역할을 생성합니다. 많은 AWS SDK 가이드에는 Amazon S3에서 읽는 "시작" 자습서가 있습니다.

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/iam/> IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택한 다음 역할 생성을 선택합니다.
3. 신뢰할 수 있는 엔터티 선택을 위해 신뢰할 수 있는 엔터티 유형 아래에서 AWS 서비스 서비스를 선택합니다.
4. 사용 사례에서 Amazon EC2를 선택한 후 다음을 선택합니다.
5. 권한 추가의 경우 정책 목록에서 Amazon S3 읽기 전용 액세스 확인란을 선택한 후 다음을 선택합니다.
6. 역할 이름을 입력한 다음 역할 생성을 선택합니다. Amazon EC2 인스턴스를 생성할 때 필요하므로 이 이름을 기억해 두세요.

## Amazon EC2 인스턴스 시작과 IAM 역할 지정

다음을 수행하여 IAM 역할을 사용하여 Amazon EC2 인스턴스를 생성하고 시작할 수 있습니다.

- Amazon EC2 사용 설명서의 [빠르게 인스턴스 시작](#)을 따라 진행하세요. 하지만 최종 제출 단계로 넘어가기 전에, 다음 작업들도 함께 수행하세요.
  - 고급 세부 정보의 IAM 인스턴스 프로파일에서 이전 단계에서 생성한 역할을 선택합니다.

이 IAM 및 Amazon EC2 설정에서 애플리케이션을 Amazon EC2 인스턴스로 배포하여, 애플리케이션에서 Amazon S3 서비스에 읽기 액세스를 할 수 있습니다.

## EC2 인스턴스에 연결

Amazon EC2 인스턴스에 연결하여 애플리케이션을 전송한 뒤 실행할 수 있도록 하세요. 인스턴스를 생성할 때 키 페어(로그인)에서 사용한 키 페어의 비공개 키가 들어 있는 파일, 즉 PEM 파일이 필요합니다.

이 작업은 인스턴스 유형에 맞는 안내를 따라 수행할 수 있습니다. 즉, [Linux 인스턴스 연결](#) 또는 [Windows 인스턴스 연결](#) 지침을 참고하세요. 연결할 때는 개발 머신에서 인스턴스로 파일을 전송할 수 있는 방식으로 연결합니다.

#### Note

Linux 또는 macOS 터미널에서는 보안 복사 명령을 사용해 애플리케이션을 복사할 수 있습니다. 키 페어를 사용해 scp를 이용하려면, `scp -i path/to/key file/to/copy ec2-user@ec2-xx-xx-xxx-xxx.compute.amazonaws.com:~` 명령어를 사용할 수 있습니다. Windows에 대한 자세한 내용은 [Windows 인스턴스로 파일 전송](#)을 참조하세요.

AWS 도구 키트를 사용하는 경우 도구 키트를 사용하여 인스턴스에 연결할 수도 있습니다. 자세한 내용은 사용하는 툴킷의 특정한 사용 설명서를 참조하십시오.

## EC2 인스턴스에서 애플리케이션 실행

1. 애플리케이션 파일을 로컬 드라이브에서 Amazon EC2 인스턴스로 복사합니다.
2. 애플리케이션을 시작하고 개발 시스템에서 동일한 결과로 실행되는지 확인합니다.
3. (선택 사항) 애플리케이션이 IAM 역할에서 제공하는 보안 인증을 사용하는지 확인합니다.
  - a. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/ec2/> Amazon EC2 콘솔을 엽니다.
  - b. 인스턴스를 선택합니다.
  - c. 작업에서 보안을 선택한 다음 IAM 역할 수정을 선택합니다.
  - d. IAM 역할의 경우 IAM 역할 없음을 선택하여 IAM 역할을 분리합니다.
  - e. IAM 역할 업데이트를 선택합니다.
  - f. 애플리케이션을 다시 실행하고 인증 오류가 반환되는지 확인합니다.

## TIP 플러그인을 사용하여 액세스 AWS 서비스

신뢰할 수 있는 자격 증명 전파(TIP)는 관리자가 그룹 연결과 같은 사용자 속성을 기반으로 권한을 부여 AWS 서비스 할 수 AWS IAM Identity Center 있는의 기능입니다. 신뢰할 수 있는 자격 증명 전파를 통해 자격 증명 컨텍스트가 IAM 역할에 추가되어 AWS 리소스에 대한 액세스를 요청하는 사용자를 식별합니다. 이 컨텍스트는 다른 AWS 서비스에 전파됩니다.

자격 증명 컨텍스트가 액세스 요청을 수신할 때 권한 부여 결정을 내리는 데 AWS 서비스 사용하는 정보로 구성됩니다. 이 정보에는 요청자(예: IAM Identity Center 사용자), 액세스가 요청 AWS 서비스 되는 (예: Amazon Redshift) 및 액세스 범위(예: 읽기 전용 액세스)를 식별하는 메타데이터가 포함됩니다. 수신은 이 컨텍스트와 사용자에게 할당된 모든 권한을 AWS 서비스 사용하여 리소스에 대한 액세스를 승인합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [신뢰할 수 있는 자격 증명 전파 개요](#)의 섹션을 참조하세요.

TIP 플러그인은 신뢰할 수 있는 AWS 서비스 있는 자격 증명 전파를 지원하는와 함께 사용할 수 있습니다. 참조 사용 사례로는 Amazon Q Business 사용 설명서의 [Configuring an Amazon Q Business application using AWS IAM Identity Center](#)를 참고하세요.

### Note

Amazon Q Business를 사용하는 경우, 서비스별 지침은 [Configuring an Amazon Q Business application using AWS IAM Identity Center](#)를 참고하세요.

## TIP 플러그인을 사용하기 위한 사전 조건

플러그인이 작동하려면 다음 리소스가 필요합니다.

1. AWS SDK for Java 또는를 사용해야 합니다 AWS SDK for JavaScript.
2. 사용 중인 서비스가 신뢰할 수 있는 ID 전파를 지원하는지 확인합니다.

자세한 내용은 AWS IAM Identity Center 사용 설명서에 있는 'IAM Identity Center와 통합되는 [AWS 관리형 애플리케이션 포의 IAM Identity Center](#)를 통해 신뢰할 수 있는 ID 전파 활성화 열을 참고하세요.

3. IAM Identity Center와 신뢰할 수 있는 ID 전파(TIP)를 활성화하세요.

AWS IAM Identity Center 사용 설명서의 [TIP 필수 조건 및 고려 사항](#)을 참조하세요.

4. Identity Center와 통합된 애플리케이션이 있어야 합니다.

AWS IAM Identity Center 사용 설명서의 [AWS 관리형 애플리케이션](#) 또는 [고객 관리형 애플리케이션](#)을 참조하세요.

5. 신뢰할 수 있는 토큰 발급자(TTI)를 설정하고 서비스를 IAM Identity Center에 연결해야 합니다.

AWS IAM Identity Center 사용 설명서의 [신뢰할 수 있는 토큰 발급자의 사전 조건](#) 및 [신뢰할 수 있는 토큰 발급자 설정 작업](#)을 참조하세요.

## 코드에서 TIP 플러그인 사용

1. 신뢰할 수 있는 ID 전파 플러그인의 인스턴스를 생성합니다.
2. 와 상호 작용하기 위한 서비스 클라이언트 인스턴스를 생성하고 신뢰할 수 있는 자격 증명 전파 플러그인을 추가하여 서비스 클라이언트를 AWS 서비스 사용자 지정합니다.

TIP 플러그인은 다음 입력 매개변수를 사용합니다.

- **webTokenProvider**: 고객이 외부 ID 제공업체로부터 OpenID 토큰을 얻기 위해 구현하는 함수입니다.
- **accessRoleArn**: ID 강화 자격 증명을 가져오기 위해 사용자의 ID 컨텍스트와 함께 플러그인에서 수입할 IAM 역할 ARN입니다.
- **applicationArn**: 클라이언트 또는 애플리케이션의 고유 식별자 문자열입니다. 이 값은 OAuth 권한이 구성된 애플리케이션 ARN입니다.
- **ssoOidcClient**: (선택 사항) Java용 [SsoOidcClient](#) 또는 JavaScript용 [client-sso-oidc](#)와 같은 SSO OIDC 클라이언트로, 사용자가 정의한 구성을 포함할 수 있습니다. 제공되지 않으면 `applicationRoleArn`을 사용하는 OIDC 클라이언트가 인스턴스화되고 사용됩니다.
- **stsClient**: (선택사항) 고객이 정의한 구성을 사용하는 AWS STS 클라이언트로, 사용자의 ID 컨텍스트로 `accessRoleArn`을 수입하는 데 사용됩니다. 제공되지 않으면 사용하는 AWS STS 클라이언트 `applicationRoleArn`가 인스턴스화되고 사용됩니다.
- **applicationRoleArn**: (선택 사항) OIDC와 AWS STS 클라이언트를 부트스트래핑할 수 `AssumeRoleWithWebIdentity` 있도록 수입할 IAM 역할 ARN입니다.
  - 제공하지 않는 경우, `ssoOidcClient` 및 `stsClient` 매개변수 둘 다 제공해야 합니다.
  - 제공하는 경우, `applicationRoleArn`은 `accessRoleArn` 매개변수와 동일한 값을 사용할 수 없습니다. `applicationRoleArn`은 `accessRole`을 수입하기 위해 사용되는 `stsClient`를 구성하는 데 사용됩니다. `applicationRole` 및 모두에 동일한 역할을 사용하는 경우 역할을 사용하여 자신을 수입(자체 역할 가정)하는 `accessRole`것을 의미하므로 권장되지 않습니다 AWS. 자세한 내용은 [공지 사항](#)을 참조하세요.

### **ssoOidcClient**, **stsClient**, **applicationRoleArn** 매개변수에 대한 고려 사항

TIP 플러그인을 구성할 때, 제공하는 매개변수에 따라 다음과 같은 권한 요구 사항을 고려해야 합니다.

- `ssoOidcClient` 및 `stsClient`를 제공하는 경우:

- ssoOidcClient에 설정된 자격 증명은 Identity Center를 직접 호출해 해당 Identity Center 전용 사용자 컨텍스트를 가져올 수 있는 `oauth:CreateTokenWithIAM` 권한을 보유해야 합니다.
- stsClient에 설정된 자격 증명은 `accessRole`에서 `sts:AssumeRole` 및 `sts:SetContext` 권한을 가져야 합니다. 또한 `accessRole`은 stsClient에 있는 자격 증명과의 신뢰 관계도 구성해야 합니다.
- `applicationRoleArn`을 제공하는 경우:
  - `applicationRole`은 OIDC와 STS 클라이언트를 생성하는 데 사용되므로, 필요한 리소스 (IdC 인스턴스, `accessRole`)에 대해 `oauth:CreateTokenWithIAM`, `sts:AssumeRole`, `sts:SetContext` 권한을 보유해야 합니다.
  - `applicationRole`은 `webToken`을 생성하는 데 사용되는 ID 제공업체와 신뢰 관계를 가지고 있어야 합니다. 이는 플러그인이 [AssumeRoleWithWebIdentity](#) 직접 호출을 통해 `applicationRole`을 수입할 때 `webToken`이 사용되기 때문입니다.

ApplicationRole 구성의 예:

웹 토큰 공급자의 신뢰 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::ACCOUNT_ID:oidc-provider/IDENTITY_PROVIDER_URL"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "IDENTITY_PROVIDER_URL:aud": "CLIENT_ID_TO_BE_TRUSTED"
        }
      }
    }
  ]
}
```

권한 정책:

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "sts:AssumeRole",
      "sts:SetContext"
    ],
    "Resource": [
      "accessRoleArn"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "sso-oauth:CreateTokenWithIAM"
    ],
    "Resource": [
      "*"
    ]
  }
]
}

```

## TIP를 사용한 코드 예제

아래 예제에서는 AWS SDK for Java 또는를 사용하여 코드에 TIP 플러그인을 구현하는 방법을 보여줍니다 AWS SDK for JavaScript.

### Java

AWS SDK for Java 프로젝트에서 TIP 플러그인을 사용하려면 프로젝트 pom.xml 파일의 종속성으로 선언해야 합니다.

```

<dependency>
<groupId>software.amazon.awssdk.trustedIdentityPropagation</groupId>
<artifactId>aws-sdk-java-trustedIdentityPropagation-java-plugin</artifactId>
  <version>2.0.0</version>
</dependency>

```

소스 코드에 software.amazon.awssdk.trustedidentitypropagation에 대한 필수 패키지 선언을 포함합니다.

아래 예제는 신뢰할 수 있는 ID 전파 플러그인 인스턴스를 생성하고 이를 서비스 클라이언트에 추가하는 두 가지 방법을 보여줍니다. 두 예제 모두 Amazon S3를 서비스로 사용하고 S3AccessGrantsPlugin를 사용하여 사용자별 권한을 관리하지만 신뢰할 수 있는 AWS 서비스 있는 자격 증명 전파(TIP)를 지원하는 모든에 적용할 수 있습니다.

### Note

이 예제에서는 S3 Access Grants에서 사용자별 권한을 설정해야 합니다. 자세한 내용은 [S3 Access Grants 문서](#)를 참고하세요.

## 옵션 1: OIDC 및 STS 클라이언트 빌드 및 전달

```
SsoOidcClient oidcClient = SsoOidcClient.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(credentialsProvider).build();

StsClient stsClient = StsClient.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(credentialsProvider).build();

TrustedIdentityPropagationPlugin trustedIdentityPropagationPlugin =
    TrustedIdentityPropagationPlugin.builder()
        .webTokenProvider(() -> webToken)
        .applicationArn(idcApplicationArn)
        .accessRoleArn(accessRoleArn)
        .ssoOidcClient(oidcClient)
        .stsClient(stsClient)
        .build();

S3AccessGrantsPlugin accessGrantsPlugin = S3AccessGrantsPlugin.builder()
    .build();

S3Client s3Client =
    S3Client.builder().region(Region.US_EAST_1)
        .crossRegionAccessEnabled(true)
        .addPlugin(trustedIdentityPropagationPlugin)
        .addPlugin(accessGrantsPlugin)
        .build();

final var resp = s3Client.getObject(GetObjectRequest.builder()
    .key("path/to/object/fileName")
```

```
.bucket("bucketName")
.build());
```

## 옵션 2: applicationRoleArn 전달 및 플러그인으로의 클라이언트 생성 연기

```
TrustedIdentityPropagationPlugin trustedIdentityPropagationPlugin =
    TrustedIdentityPropagationPlugin.builder()
        .webTokenProvider(() -> webToken)
        .applicationArn(idcApplicationArn)
        .accessRoleArn(accessRoleArn)
        .applicationRoleArn(applicationRoleArn)
        .build();

S3AccessGrantsPlugin accessGrantsPlugin = S3AccessGrantsPlugin.builder()
    .build();

S3Client s3Client =
    S3Client.builder().region(Region.US_EAST_1)
        .crossRegionAccessEnabled(true)
        .addPlugin(trustedIdentityPropagationPlugin)
        .addPlugin(accessGrantsPlugin)
        .build();

final var resp = s3Client.getObject(GetObjectRequest.builder()
    .key("path/to/object/fileName")
    .bucket("bucketName")
    .build());
```

추가 세부 정보 및 소스는 GitHub의 [trusted-identity-propagation-java](#)를 참조하세요.

## JavaScript

다음 명령을 실행하여 AWS SDK for JavaScript 프로젝트에 TIP 인증 플러그인 패키지를 설치합니다.

```
$ npm i @aws-sdk-extension/trusted-identity-propagation
```

최종 package.json에는 다음과 유사한 종속성이 포함되어야 합니다.

```
"dependencies": {
"@aws-sdk-extension/trusted-identity-propagation": "^2.0.0"
},
```

소스 코드에서 필요한 `TrustedIdentityPropagationExtension` 종속성을 가져옵니다.

아래 예제는 신뢰할 수 있는 ID 전파 플러그인 인스턴스를 생성하고 이를 서비스 클라이언트에 추가하는 두 가지 방법을 보여줍니다. 두 예제 모두 Amazon S3를 서비스로 사용하고 Amazon S3 Access Grants를 사용하여 사용자별 권한을 관리하지만 신뢰할 수 있는 AWS 서비스 있는 자격 증명 전파(TIP)를 지원하는 모든에 적용할 수 있습니다.

### Note

이 예제에서는 Amazon S3 Access Grants에서 사용자별 권한을 설정해야 합니다. 자세한 내용은 [Amazon S3 Access Grants 문서](#)를 참조하세요.

## 옵션 1: OIDC 및 STS 클라이언트 빌드 및 전달

```
import { S3Client, GetObjectCommand } from "@aws-sdk/client-s3";
import { S3ControlClient, GetDataAccessCommand } from "@aws-sdk/client-s3-control";
import { TrustedIdentityPropagationExtension } from "@aws-sdk-extension/trusted-identity-propagation";

const s3ControlClient = new S3ControlClient({
  region: "us-east-1",
  extensions: [
    TrustedIdentityPropagationExtension.create({
      webTokenProvider: async () => {
        return 'ID_TOKEN_FROM_YOUR_IDENTITY_PROVIDER';
      },
      ssoOidcClient: customOidcClient,
      stsClient: customStsClient,
      accessRoleArn: accessRoleArn,
      applicationArn: applicationArn,
    }),
  ],
});

const getDataAccessParams = {
  Target: "S3_URI_PATH",
  Permission: "READ",
  AccountId: ACCOUNT_ID,
  InstanceArn: S3_ACCESS_GRANTS_ARN,
  TargetType: "Object",
};
```

```

try {
  const command = new GetDataAccessCommand(getDataAccessParams);
  const response = await s3ControlClient.send(command);

  const credentials = response.Credentials;

  // Create a new S3 client with the temporary credentials
  const temporaryS3Client = new S3Client({
    region: "us-east-1",
    credentials: {
      accessKeyId: credentials.AccessKeyId,
      secretAccessKey: credentials.SecretAccessKey,
      sessionToken: credentials.SessionToken,
    },
  });

  // Use the temporary S3 client to perform the operation
  const s3Params = {
    Bucket: "BUCKET_NAME",
    Key: "S3_OBJECT_KEY",
  };
  const getObjectCommand = new GetObjectCommand(s3Params);
  const s3Object = await temporaryS3Client.send(getObjectCommand);

  const fileContent = await s3Object.Body.transformToString();

  // Process the S3 object data
  console.log("Successfully retrieved S3 object:", fileContent);
} catch (error) {
  console.error("Error accessing S3 data:", error);
}

```

## 옵션 2: applicationRoleArn 전달 및 플러그인으로의 클라이언트 생성 연기

```

import { S3Client, GetObjectCommand } from "@aws-sdk/client-s3";
import { S3ControlClient, GetDataAccessCommand } from "@aws-sdk/client-s3-control";
import { TrustedIdentityPropagationExtension } from "@aws-sdk-extension/trusted-identity-propagation";

const s3ControlClient = new S3ControlClient({
  region: "us-east-1",
  extensions: [

```

```
    TrustedIdentityPropagationExtension.create({
      webTokenProvider: async () => {
        return 'ID_TOKEN_FROM_YOUR_IDENTITY_PROVIDER';
      },
      accessRoleArn: accessRoleArn,
      applicationRoleArn: applicationRoleArn,
      applicationArn: applicationArn,
    }),
  ],
});

// Same S3 AccessGrants workflow as Option 1
const getDataAccessParams = {
  Target: "S3_URI_PATH",
  Permission: "READ",
  AccountId: ACCOUNT_ID,
  InstanceArn: S3_ACCESS_GRANTS_ARN,
  TargetType: "Object",
};

try {
  const command = new GetDataAccessCommand(getDataAccessParams);
  const response = await s3ControlClient.send(command);

  const credentials = response.Credentials;

  const temporaryS3Client = new S3Client({
    region: "us-east-1",
    credentials: {
      accessKeyId: credentials.AccessKeyId,
      secretAccessKey: credentials.SecretAccessKey,
      sessionToken: credentials.SessionToken,
    },
  });

  const s3Params = {
    Bucket: "BUCKET_NAME",
    Key: "S3_OBJECT_KEY",
  };

  const getObjectCommand = new GetObjectCommand(s3Params);
  const s3object = await temporaryS3Client.send(getObjectCommand);

  const fileContent = await s3object.Body.transformToString();
}
```

```
console.log("Successfully retrieved S3 object:", fileContent);  
} catch (error) {  
  console.error("Error accessing S3 data:", error);  
}
```

추가 세부 정보 및 소스는 GitHub의 [trusted-identity-propagation-js](#)를 참조하세요.

# AWS SDKs 및 도구 설정 참조

SDKs 언어별 APIs 제공합니다 AWS 서비스. 이 SDK는 인증, 재시도 동작 등을 포함하여 API 직접 호출을 성공적으로 수행하는 데 필요한 일부 번거로운 작업을 처리합니다. 이를 위해 SDK에는 요청에 사용할 보안 인증을 얻고, 각 서비스에 사용할 설정을 유지 관리하고, 글로벌 설정에 사용할 값을 가져오는 유연한 전략이 있습니다.

다음 섹션에서 구성 설정에 대한 자세한 정보를 확인할 수 있습니다.

- [AWS SDKs 및 도구 표준화 자격 증명 공급자](#) - 여러 SDK에 표준화된 공통 보안 인증 공급자.
- [AWS SDKs 및 도구 표준화된 기능](#) - 여러 SDK에 표준화된 공통 기능.

## 서비스 클라이언트 생성

프로그래밍 방식으로 액세스하기 위해 AWS 서비스 SDKs 각각에 대해 클라이언트 클래스/객체를 사용합니다 AWS 서비스. 예를 들어, 애플리케이션이 Amazon EC2에 액세스해야 하는 경우, 애플리케이션은 Amazon EC2 클라이언트 객체를 생성하여 해당 서비스와 인터페이스 합니다. 그런 다음 서비스 클라이언트를 사용하여 요청을 AWS 서비스에 보내면 됩니다. 대부분의 SDK에서 서비스 클라이언트 객체는 변경할 수 없으므로 요청을 보내는 각 서비스마다 새 클라이언트를 생성해야 하며, 동일한 서비스에 대해 다른 구성을 사용하여 요청을 보내려는 경우에도 새 클라이언트를 만들어야 합니다.

## 설정의 우선 순위

글로벌 설정은 대부분의 SDK가 지원하는 기능, 보안 인증 공급자 및 기타 기능을 구성하며 AWS 서비스 전반에 광범위하게 영향을 미칩니다. 모든 SDK에는 글로벌 설정 값을 찾기 위해 확인하는 일련의 위치 (또는 소스)가 있습니다. 조회 우선 순위 설정은 다음과 같습니다.

1. 코드나 서비스 클라이언트 자체에 설정된 모든 명시적 설정은 다른 모든 설정보다 우선합니다.
  - 일부 설정은 작업별로 설정할 수 있으며 간접 호출하는 각 작업에 대해 필요에 따라 변경할 수 있습니다. AWS CLI 또는의 경우 명령줄에 입력하는 작업당 파라미터의 형태를 AWS Tools for PowerShell 취합니다. SDK의 경우 명시적 할당은 AWS 서비스 클라이언트 또는 구성 객체를 인스턴스화할 때 또는 경우에 따라 개별 API를 호출할 때 설정한 파라미터의 형태를 취할 수 있습니다.
2. Java/Kotlin 전용: 이 설정에 대한 JVM 시스템 속성이 확인됩니다. 설정이 되면 클라이언트 구성에 해당 값이 사용됩니다.
3. 환경 변수를 확인합니다. 설정이 되면 클라이언트 구성에 해당 값이 사용됩니다.

4. SDK가 공유 credentials 파일에서 설정을 확인합니다. 설정된 경우 클라이언트가 이를 사용합니다.
5. 이 설정에 대한 공유 config 파일입니다. 설정이 있으면 SDK는 해당 설정을 사용합니다.
  - AWS\_PROFILE 환경 변수 또는 aws.profile JVM 시스템 속성을 사용하여 SDK가 로드할 프로파일을 지정할 수 있습니다.
6. SDK 소스 코드 자체에서 제공하는 모든 기본값이 마지막에 사용됩니다.

### Note

일부 SDK 및 도구는 순서가 다를 수 있습니다. 또한 일부 SDK 및 도구는 다른 파라미터 저장과 검색 방법을 지원합니다. 예를 들어는 [SDK 스토어](#)라는 추가 소스를 AWS SDK for .NET 지원합니다. 특정 SDK 또는 도구 제공자에 대한 자세한 내용은 사용 중인 특정 SDK 또는 도구의 설명서를 참조합니다.

순서에 따라 어떤 방법이 다른 메서드보다 우선 적용되는지 결정됩니다. 예를 들어 공유 config 파일에 프로파일을 설정하면 SDK 또는 도구가 먼저 다른 위치를 확인한 후에 해당 프로파일을 찾아 사용합니다. 즉, credentials 파일에 설정을 입력하면 config 파일에 있는 설정이 아닌 해당 설정이 사용됩니다. 설정과 값으로 환경 변수를 구성하면 credentials 및 config 파일 모두의 해당 설정을 재정의 합니다. 마지막으로 개별 작업(AWS CLI 명령줄 매개 변수 또는 API 매개 변수)또는 코드의 설정이 해당 명령에 대한 다른 모든 값을 재정의합니다.

## 이 안내서의 설정 페이지의 이해

이 안내서의 설정 참조 섹션에 포함된 페이지에서는 다양한 메커니즘으로 설정할 수 있는 사용 가능한 설정을 자세히 설명합니다. 다음 표에서는 코드 외부에서 기능을 구성할 수 있도록 사용 가능한 구성 및 자격 증명 파일 설정, 환경 변수, 그리고 (Java 및 Kotlin SDK의 경우) JVM 설정을 나열합니다. 각 목록의 링크된 주제를 클릭하면 해당 설정 페이지로 이동합니다.

- [Config 파일 설정 목록](#)
- [Credentials 파일 설정 목록](#)
- [환경 변수 목록](#)
- [JVM 시스템 속성 목록](#)

각 자격 증명 공급자나 기능에는 해당 기능을 구성하는 데 사용되는 설정이 나열된 전용 페이지가 있습니다. 각 설정에 대한 값은 일반적으로 구성 파일에 추가하거나, 환경 변수를 설정하거나, (Java 및 Kotlin의 경우에만) JVM 시스템 속성을 설정하는 방식으로 설정할 수 있습니다. 각 설정 항목에는 설명 세부 정보 위쪽 블록에 값을 설정할 수 있는 모든 지원 방법이 함께 표시됩니다. [우선순위](#)는 다를 수 있지만, 어떤 방식으로 설정하든 결과 기능은 동일합니다.

설명에는 별도로 설정하지 않았을 때 적용되는 기본값(있는 경우)도 포함됩니다. 이는 또한 해당 설정에 대해 유효한 값이 무엇인지를 정의합니다.

예를 들어 [요청 압축](#) 기능 페이지에서 설정을 살펴보겠습니다.

`disable_request_compression` 예제 설정의 정보는 다음을 문서화합니다.

- 코드베이스 외부에서 요청 압축을 제어하는 방법에는 세 가지 동등한 방식이 있습니다. 다음 작업 중 하나를 수행할 수 있습니다.
  - `disable_request_compression`을 사용하여 구성 파일에서 설정
  - `AWS_DISABLE_REQUEST_COMPRESSION`을 사용하여 환경 변수로 설정
  - 또는 Java나 Kotlin SDK를 사용하는 경우, `aws.disableRequestCompression`을 사용하여 JVM 시스템 속성으로 설정

#### Note

코드 안에서 직접 동일한 기능을 구성하는 방법도 있을 수 있지만, 이 참조에서는 다루지 않습니다. SDK마다 구현 방식이 다르기 때문입니다. 코드 내에서 직접 구성을 설정하려면, 특정 SDK 안내서 또는 API 참조를 참조하세요.

- 아무 작업도 수행하지 않으면 값이 기본적으로 `false`로 설정됩니다.
- 이 부울 설정에 사용할 수 있는 유효한 값은 `true`와 `false`뿐입니다.

각 기능 페이지 하단에는 Support AWS SDKs.

이 표는 SDK가 해당 페이지에 나열된 설정들을 지원하는지 여부를 보여줍니다. Supported 열은 다음 값을 통해 지원 수준을 나타냅니다.

- Yes - 해당 설정은 SDK에서 작성된 그대로 완전히 지원됩니다.
- Partial - 일부 설정만 지원되거나, 동작이 설명과 다르게 작동하는 경우가 있습니다. Partial의 경우 추가 참고 사항에 이러한 차이가 명시되어 있습니다.

- No - 어떠한 설정도 지원되지 않습니다. 이는 코드에서 동일한 기능을 구현할 수 있는지 여부에 대한 주장을 하지 않으며, 단지 나열된 외부 구성 설정이 지원되지 않음을 나타냅니다.

## Config 파일 설정 목록

다음 표에 나열된 설정은 공유 AWS config 파일에 할당할 수 있습니다. 이는 전 세계에 적용되며 모든 AWS 서비스에 영향을 미칩니다. SDK와 도구는 또한 고유한 설정 및 환경 변수를 지원할 수도 있습니다. 개별 SDK나 도구에서만 지원되는 설정 및 환경 변수를 확인하려면, 해당 SDK 또는 도구의 안내서를 참조하세요.

설정 이름	세부 정보
account_id_endpoint_mode	<a href="#">계정 기반 엔드포인트</a>
api_versions	<a href="#">일반 구성 설정</a>
auth_scheme_preference	<a href="#">인증 체계</a>
aws_access_key_id	<a href="#">AWS 액세스 키</a>
aws_account_id	<a href="#">계정 기반 엔드포인트</a>
aws_secret_access_key	<a href="#">AWS 액세스 키</a>
aws_session_token	<a href="#">AWS 액세스 키</a>
ca_bundle	<a href="#">일반 구성 설정</a>
credential_process	<a href="#">프로세스 보안 인증 제공자</a>

설정 이름	세부 정보
credential_source	<a href="#">역할 보안 인증 제공자 수입</a>
defaults_mode	<a href="#">스마트 구성 기본값</a>
disable_host_prefix_injection	<a href="#">호스트 접두사 삽입</a>
disable_request_compression	<a href="#">요청 압축</a>
duration_seconds	<a href="#">역할 보안 인증 제공자 수입</a>
ec2_metadata_service_endpoint	<a href="#">IMDS 보안 인증 제공자</a>
ec2_metadata_service_endpoint_mode	<a href="#">IMDS 보안 인증 제공자</a>
ec2_metadata_v1_disabled	<a href="#">IMDS 보안 인증 제공자</a>
endpoint_discovery_enabled	<a href="#">엔드포인트 검색</a>
endpoint_url	<a href="#">서비스별 엔드포인트</a>
external_id	<a href="#">역할 보안 인증 제공자 수입</a>

설정 이름	세부 정보
ignore_configured_endpoint_urls	<a href="#">서비스별 엔드포인트</a>
max_attempts	<a href="#">재시도 동작</a>
metadata_service_num_attempts	<a href="#">Amazon EC2 인스턴스 메타데이터</a>
metadata_service_timeout	<a href="#">Amazon EC2 인스턴스 메타데이터</a>
mfa_serial	<a href="#">역할 보안 인증 제공자 수입</a>
output	<a href="#">일반 구성 설정</a>
parameter_validation	<a href="#">일반 구성 설정</a>
region	<a href="#">AWS 리전</a>
request_checksum_calculation	<a href="#">Amazon S3에 대한 데이터 무결성 보호</a>
request_min_compression_size_bytes	<a href="#">요청 압축</a>
response_checksum_validation	<a href="#">Amazon S3에 대한 데이터 무결성 보호</a>
retry_mode	<a href="#">재시도 동작</a>

설정 이름	세부 정보
role_arn	<a href="#">역할 보안 인증 제공자 수입</a>
role_session_name	<a href="#">역할 보안 인증 제공자 수입</a>
s3_disable_express_session_auth	<a href="#">S3 Express One Zone 세션 인증</a>
s3_disable_multiregion_access_points	<a href="#">Amazon S3 다중 리전 액세스 포인트</a>
s3_use_arn_region	<a href="#">Amazon S3 액세스 포인트</a>
sdk_ua_app_id	<a href="#">애플리케이션 ID</a>
sigv4_signing_region_set	<a href="#">인증 체계</a>
source_profile	<a href="#">역할 보안 인증 제공자 수입</a>
sso_account_id	<a href="#">IAM 아이덴티티 센터 보안 인증 공급자</a>
sso_region	<a href="#">IAM 아이덴티티 센터 보안 인증 공급자</a>
sso_registration_scopes	<a href="#">IAM 아이덴티티 센터 보안 인증 공급자</a>
sso_role_name	<a href="#">IAM 아이덴티티 센터 보안 인증 공급자</a>
sso_start_url	<a href="#">IAM 아이덴티티 센터 보안 인증 공급자</a>
sts_regional_endpoints	<a href="#">AWS STS 리전 엔드포인트</a>

설정 이름	세부 정보
use_duals_tack_endpoint	<a href="#">이중 스택 엔드포인트 및 FIPS 엔드포인트</a>
use_fips_endpoint	<a href="#">이중 스택 엔드포인트 및 FIPS 엔드포인트</a>
web_identity_token_file	<a href="#">역할 보안 인증 제공자 수입</a>

## Credentials 파일 설정 목록

다음 표에 나열된 설정은 공유 AWS credentials 파일에 할당할 수 있습니다. 이는 전 세계에 적용되며 모든 AWS 서비스에 영향을 미칩니다. SDK와 도구는 또한 고유한 설정 및 환경 변수를 지원할 수도 있습니다. 개별 SDK나 도구에서만 지원되는 설정 및 환경 변수를 확인하려면, 해당 SDK 또는 도구의 안내서를 참조하세요.

설정 이름	세부 정보
aws_access_key_id	<a href="#">AWS 액세스 키</a>
aws_secret_access_key	<a href="#">AWS 액세스 키</a>
aws_session_token	<a href="#">AWS 액세스 키</a>

## 환경 변수 목록

대부분의 SDK에서 지원되는 환경 변수가 아래에 나열되어 있습니다. 이는 전 세계에 적용되며 모든 AWS 서비스에 영향을 미칩니다. SDK와 도구는 또한 고유한 설정 및 환경 변수를 지원할 수도 있습니다. 개별 SDK나 도구에서만 지원되는 설정 및 환경 변수를 확인하려면, 해당 SDK 또는 도구의 안내서를 참조하세요.

설정 이름	세부 정보
AWS_ACCESS_KEY_ID	<a href="#">AWS 액세스 키</a>
AWS_ACCOUNT_ID	<a href="#">계정 기반 엔드포인트</a>
AWS_ACCOUNT_ID_ENDPOINT_MODE	<a href="#">계정 기반 엔드포인트</a>
AWS_AUTH_SCHEME_PREFERENCE	<a href="#">인증 체계</a>
AWS_CA_BUNDLE	<a href="#">일반 구성 설정</a>
AWS_CONFIG_FILE	<a href="#">AWS SDKs 및 도구의 공유 config 및 credentials 파일 위치 찾기 및 변경</a>
AWS_CONTAINER_AUTHORIZATION_TOKEN	<a href="#">컨테이너 보안 인증 제공업체</a>
AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE	<a href="#">컨테이너 보안 인증 제공업체</a>
AWS_CONTAINER_CREDENTIALS_FULL_URI	<a href="#">컨테이너 보안 인증 제공업체</a>
AWS_CONTAINER_CREDENTIALS	<a href="#">컨테이너 보안 인증 제공업체</a>

설정 이름	세부 정보
ENTIALS_RELATIVE_URI	
AWS_DEFAULTS_MODE	<a href="#">스마트 구성 기본값</a>
AWS_DISABLE_HOST_PREFIX_INJECTION	<a href="#">호스트 접두사 삽입</a>
AWS_DISABLE_REQUEST_COMPRESSION	<a href="#">요청 압축</a>
AWS_EC2_METADATA_DISABLED	<a href="#">IMDS 보안 인증 제공자</a>
AWS_EC2_METADATA_SERVICE_ENDPOINT	<a href="#">IMDS 보안 인증 제공자</a>
AWS_EC2_METADATA_SERVICE_ENDPOINT_MODE	<a href="#">IMDS 보안 인증 제공자</a>
AWS_EC2_METADATA_V1_DISABLED	<a href="#">IMDS 보안 인증 제공자</a>
AWS_ENABLE_ENDPOINT_DISCOVERY	<a href="#">엔드포인트 검색</a>

설정 이름	세부 정보
AWS_ENDPOINT_URL	<a href="#">서비스별 엔드포인트</a>
AWS_ENDPOINT_URL_<SERVICE>	<a href="#">서비스별 엔드포인트</a>
AWS_IGNORE_CONFIGURED_ENDPOINT_URLS	<a href="#">서비스별 엔드포인트</a>
AWS_MAX_ATTEMPTS	<a href="#">재시도 동작</a>
AWS_METADATA_SERVICE_NUM_ATTEMPTS	<a href="#">Amazon EC2 인스턴스 메타데이터</a>
AWS_METADATA_SERVICE_TIMEOUT	<a href="#">Amazon EC2 인스턴스 메타데이터</a>
AWS_PROFILE	<a href="#">공유 config 및 credentials 파일을 사용하여 AWS SDKs 및 도구 전역 구성</a>
AWS_REGION	<a href="#">AWS 리전</a>
AWS_REQUEST_CHECKSUM_CALCULATION	<a href="#">Amazon S3에 대한 데이터 무결성 보호</a>
AWS_REQUEST_MIN_COMPRESSION_SIZE_BYTES	<a href="#">요청 압축</a>

설정 이름	세부 정보
AWS_RESPONSE_CHECKSUM_VALIDATION	<a href="#">Amazon S3에 대한 데이터 무결성 보호</a>
AWS_RETRY_MODE	<a href="#">재시도 동작</a>
AWS_ROLE_ARN	<a href="#">역할 보안 인증 제공자 수입</a>
AWS_ROLE_SESSION_NAME	<a href="#">역할 보안 인증 제공자 수입</a>
AWS_S3_DISABLE_EXPRESS_SESSION_AUTH	<a href="#">S3 Express One Zone 세션 인증</a>
AWS_S3_DISABLE_MULTIREGION_ACCESS_POINTS	<a href="#">Amazon S3 다중 리전 액세스 포인트</a>
AWS_S3_US_E_ARN_REGION	<a href="#">Amazon S3 액세스 포인트</a>
AWS_SDK_UA_APP_ID	<a href="#">애플리케이션 ID</a>
AWS_SECRET_ACCESS_KEY	<a href="#">AWS 액세스 키</a>
AWS_SESSION_TOKEN	<a href="#">AWS 액세스 키</a>
AWS_SHARED_CREDENTIALS_FILE	<a href="#">AWS SDKs 및 도구의 공유 config 및 credentials 파일 위치 찾기 및 변경</a>

설정 이름	세부 정보
AWS_SIGV4 A_SIGNING _REGION_SET	<a href="#">인증 체계</a>
AWS_STS_R EGIONAL_E NDPOINTS	<a href="#">AWS STS 리전 엔드포인트</a>
AWS_USE_D UALSTACK_ ENDPOINT	<a href="#">이중 스택 엔드포인트 및 FIPS 엔드포인트</a>
AWS_USE_F IPS_ENDPOINT	<a href="#">이중 스택 엔드포인트 및 FIPS 엔드포인트</a>
AWS_WEB_I DENTITY_T OKEN_FILE	<a href="#">역할 보안 인증 제공자 수입</a>

## JVM 시스템 속성 목록

AWS SDK for Java 및 AWS SDK for Kotlin (JVM 대상 지정)에 대해 다음 JVM 시스템 속성을 사용할 수 있습니다. JVM 시스템 속성을 설정하는 방법에 대한 지침은 [the section called “JVM 시스템 속성 설정 방법”](#)에서 확인하세요.

설정 이름	세부 정보
<code>aws.accessKeyId</code>	<a href="#">AWS 액세스 키</a>
<code>aws.accountId</code>	<a href="#">계정 기반 엔드포인트</a>
<code>aws.accountIdEndpointMode</code>	<a href="#">계정 기반 엔드포인트</a>

설정 이름	세부 정보
<code>aws.authSchemePreference</code>	<a href="#">인증 체계</a>
<code>aws.configFile</code>	<a href="#">AWS SDKs 및 도구의 공유 config 및 credentials 파일 위치 찾기 및 변경</a>
<code>aws.defaultsMode</code>	<a href="#">스마트 구성 기본값</a>
<code>aws.disableEc2MetadataV1</code>	<a href="#">IMDS 보안 인증 제공자</a>
<code>aws.disableHostPrefixInjection</code>	<a href="#">호스트 접두사 삽입</a>
<code>aws.disableRequestCompression</code>	<a href="#">요청 압축</a>
<code>aws.disableS3ExpressAuth</code>	<a href="#">S3 Express One Zone 세션 인증</a>
<code>aws.ec2MetadataServiceEndpoint</code>	<a href="#">IMDS 보안 인증 제공자</a>
<code>aws.ec2MetadataServiceEndpointMode</code>	<a href="#">IMDS 보안 인증 제공자</a>

설정 이름	세부 정보
<code>aws.endpointDiscoveryEnabled</code>	<a href="#">엔드포인트 검색</a>
<code>aws.endpointUrl</code>	<a href="#">서비스별 엔드포인트</a>
<code>aws.endpointUrl&lt;ServiceName&gt;</code>	<a href="#">서비스별 엔드포인트</a>
<code>aws.ignoreConfiguredEndpointUrls</code>	<a href="#">서비스별 엔드포인트</a>
<code>aws.maxAttempts</code>	<a href="#">재시도 동작</a>
<code>aws.profile</code>	<a href="#">공유 config 및 credentials 파일을 사용하여 AWS SDKs 및 도구 전역 구성</a>
<code>aws.region</code>	<a href="#">AWS 리전</a>
<code>aws.requestChecksumCalculation</code>	<a href="#">Amazon S3에 대한 데이터 무결성 보호</a>
<code>aws.requestMinCompressionSizeBytes</code>	<a href="#">요청 압축</a>
<code>aws.responseChecksumValidation</code>	<a href="#">Amazon S3에 대한 데이터 무결성 보호</a>
<code>aws.retryMode</code>	<a href="#">재시도 동작</a>
<code>aws.roleArn</code>	<a href="#">역할 보안 인증 제공자 수임</a>

설정 이름	세부 정보
<code>aws.roleSessionName</code>	<a href="#">역할 보안 인증 제공자 수입</a>
<code>aws.s3DisableMultiRegionAccessPoints</code>	<a href="#">Amazon S3 다중 리전 액세스 포인트</a>
<code>aws.s3UseArnRegion</code>	<a href="#">Amazon S3 액세스 포인트</a>
<code>aws.secretAccessKey</code>	<a href="#">AWS 액세스 키</a>
<code>aws.sessionToken</code>	<a href="#">AWS 액세스 키</a>
<code>aws.sharedCredentialsFile</code>	<a href="#">AWS SDKs 및 도구의 공유 config 및 credentials 파일 위치 찾기 및 변경</a>
<code>aws.useDualstackEndpoint</code>	<a href="#">이중 스택 엔드포인트 및 FIPS 엔드포인트</a>
<code>aws.useFipsEndpoint</code>	<a href="#">이중 스택 엔드포인트 및 FIPS 엔드포인트</a>
<code>aws.webIdentityTokenFile</code>	<a href="#">역할 보안 인증 제공자 수입</a>
<code>sdk.ua.appId</code>	<a href="#">애플리케이션 ID</a>

# AWS SDKs 및 도구 표준화 자격 증명 공급자

많은 보안 인증 공급자가 일관된 기본값을 유지하고 여러 SDK에서 동일한 방식으로 작동하도록 표준화되었습니다. 이러한 일관성은 여러 SDK에서 코딩할 때 생산성과 명확성을 높입니다. 코딩으로 모든 설정을 재정의할 수 있습니다. 자세한 내용은 특정 SDK API를 참조하십시오.

## Important

모든 SDK가 모든 제공자를 지원하는 것은 아니며 공급자 내의 모든 측면을 지원하는 것은 아닙니다.

## 주제

- [자격 증명 공급자 체인의 이해](#)
- [SDK별 및 도구별 자격 증명 공급자 체인](#)
- [AWS 액세스 키](#)
- [로그인 자격 증명 공급자](#)
- [역할 보안 인증 제공자 수입](#)
- [컨테이너 보안 인증 제공업체](#)
- [IAM 아이덴티티 센터 보안 인증 공급자](#)
- [IMDS 보안 인증 제공자](#)
- [프로세스 보안 인증 제공자](#)

## 자격 증명 공급자 체인의 이해

모든 SDK에는 AWS 서비스에 요청을 하는 데 사용할 유효한 보안 인증을 찾기 위해 확인하는 일련의 위치 (또는 소스)가 있습니다. 유효한 보안 인증 정보를 찾은 후에는 검색이 중지됩니다. 이러한 체계적인 검색을 자격 증명 공급자 체인이라고 합니다.

표준화된 자격 증명 공급자 중 하나를 사용하는 경우 AWS SDKs 만료 시 항상 자격 증명을 자동으로 갱신하려고 시도합니다. 내장된 자격 증명 공급자 체인은 체인 내에서 어떤 공급자를 사용하든 관계없이 애플리케이션이 자격 증명을 갱신할 수 있도록 지원합니다. SDK가 이를 수행하는 데 추가 코드가 필요하지 않습니다.

각 SDK에서 사용하는 고유한 체인은 다르지만 대부분 다음과 같은 소스를 포함합니다.

보안 인증 제공업체	설명
<a href="#">AWS 액세스 키</a>	AWS IAM 사용자의 액세스 키(예: AWS_ACCESS_KEY_ID , 및 AWS_SECRET_ACCESS_KEY ).
<a href="#">웹 자격 증명 또는 OpenID Connect 와 페더레이션- 역할 보안 인증 제공자 수임</a>	Login with Amazon, Facebook, Google 또는 다른 OpenID Connect(OIDC)호환 IdP와 같은 널리 알려진 외부 보안 인증 공급자(IdP)를 사용해 로그인합니다. AWS Security Token Service ()의 JSON 웹 토큰(JWT)을 사용하여 IAM 역할의 권한을 수임합니다AWS STS.
<a href="#">로그인 자격 증명 공급자</a>	로그인한 새 콘솔 세션 또는 기존 콘솔 세션의 자격 증명을 가져옵니다.
<a href="#">IAM 아이덴티티 센터 보안 인증 공급자</a>	에서 자격 증명을 가져옵니다 AWS IAM Identity Center.
<a href="#">역할 보안 인증 제공자 수임</a>	IAM 역할의 권한을 수임하여 다른 리소스에 액세스할 수 있습니다. (역할에 대한 임시 보안 인증을 검색하여 사용).
<a href="#">컨테이너 보안 인증 제공업체</a>	Amazon Elastic Container Service(Amazon ECS) 및 Amazon Elastic Kubernetes Service(Amazon EKS) 보안 인증. 컨테이너 자격 증명 공급자는 고객의 컨테이너 애플리케이션에 대한 자격 증명을 가져옵니다.
<a href="#">프로세스 보안 인증 제공자</a>	사용자 정의 보안 인증 공급자. IAM Roles Anywhere를 비롯한 외부 소스 또는 프로세스에서 보안 인증을 가져옵니다.
<a href="#">IMDS 보안 인증 제공자</a>	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 프로파일 보안 인증. IAM 역할을 사용자의 각 EC2 인스턴스에 연결합니다. 그러면 인스턴스에서 실행되는 코드에 대해 해당 역할의 임시 보안 인증을 사용할 수 있게 됩니다. 보안 인증은 Amazon EC2 메타데이터 서비스를 통해 전달됩니다.

체인의 각 단계마다 설정 값을 할당하는 여러 방법이 있습니다. 코드에 지정된 설정값이 항상 우선합니다. 그러나 [환경 변수](#)와 [공유 config 및 credentials 파일을 사용하여 AWS SDKs 및 도구 전역 구성](#)같은 경우도 있습니다. 자세한 내용은 [설정의 우선 순위](#) 단원을 참조하십시오.

## SDK별 및 도구별 자격 증명 공급자 체인

자신이 사용하는 SDK 또는 도구의 특정 자격 증명 공급자 체인 세부 정보를 바로 확인하려면, 아래에서 해당 SDK나 도구를 선택하세요.

- [AWS CLI](#)
- [SDK for C++](#)
- [SDK for Go](#)
- [SDK for Java](#)
- [SDK for JavaScript](#)
- [SDK for Kotlin](#)
- [SDK for .NET](#)
- [SDK for PHP](#)
- [SDK for Python \(Boto3\)](#)
- [SDK for Ruby](#)
- [SDK for Rust](#)
- [SDK for Swift](#)
- [PowerShell용 도구](#)

## AWS 액세스 키

### Warning

보안 위험을 방지하려면 목적별 소프트웨어를 개발하거나 실제 데이터로 작업할 때 IAM 사용자를 인증에 사용하지 마세요. 대신 [AWS IAM Identity Center](#)과 같은 보안 인증 공급자를 통한 페더레이션을 사용하십시오.

AWS IAM 사용자의 액세스 키를 자격 AWS 증명으로 사용할 수 있습니다. AWS SDK는 이러한 AWS 자격 증명을 자동으로 사용하여 API 요청에 서명 AWS하므로 워크로드가 AWS 리소스와 데이터에 안

전하고 편리하게 액세스할 수 있습니다. 보안 인증이 일시적 유효하지 않거나 만료 후에는 더 이상 유효하지 않도록 항상 `aws_session_token`을 사용하는 것이 좋습니다. 장기 자격 증명 사용은 권장되지 않습니다.

### Note

AWS 에서 이러한 임시 자격 증명을 새로 고칠 AWS 수 없는 경우 워크로드가 영향을 받지 않도록 자격 증명의 유효성을 확장할 수 있습니다.

공유 AWS `credentials` 파일은 애플리케이션 소스 디렉터리 외부에 안전하게 있고 공유 `config` 파일의 SDK별 설정과 분리되어 있으므로 자격 증명 정보를 저장하는 데 권장되는 위치입니다.

자격 AWS 증명 및 액세스 키 사용에 대한 자세한 내용은 IAM 사용 설명서의 [AWS 보안 자격 증명 및 IAM 사용자의 액세스 키 관리를 참조하세요.](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html) [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_access-keys.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html)

다음을 사용하여 이 기능을 구성하십시오.

**aws\_access\_key\_id** - 공유 AWS `config` 파일 설정, **aws\_access\_key\_id** - 공유 AWS `credentials` 파일 설정(권장 방법), **AWS\_ACCESS\_KEY\_ID** - 환경 변수, **aws.accessKeyId** - JVM 시스템 속성: Java/Kotlin만 해당

사용자를 인증하기 위한 자격 증명의 일부로 사용되는 AWS 액세스 키를 지정합니다.

**aws\_secret\_access\_key** - 공유 AWS `config` 파일 설정, **aws\_secret\_access\_key** - 공유 AWS `credentials` 파일 설정(권장 방법), **AWS\_SECRET\_ACCESS\_KEY** - 환경 변수, **aws.secretAccessKey** - JVM 시스템 속성: Java/Kotlin만 해당

사용자를 인증하기 위한 자격 증명의 일부로 사용되는 AWS 보안 키를 지정합니다.

**aws\_session\_token** - 공유 AWS `config` 파일 설정, **aws\_session\_token** - 공유 AWS `credentials` 파일 설정(권장 방법), **AWS\_SESSION\_TOKEN** - 환경 변수, **aws.sessionToken** - JVM 시스템 속성: Java/Kotlin만 해당

사용자를 인증하기 위한 자격 증명의 일부로 사용되는 AWS 세션 토큰을 지정합니다. 역할 수입 요청이 성공하면 반환되는 임시 보안 인증 정보의 일부로 이 값을 받습니다. 세션 토큰은 수동으로 임시 보안 인증을 지정하는 경우에만 필요합니다. 하지만 장기 보안 인증 정보를 사용하는 대신 항상 임시 보안 인증을 사용하는 것이 좋습니다. 보안 권장 사항은 [IAM의 보안 모범 사례](#)를 참조하십시오.

이러한 값을 구하는 방법에 대한 자세한 내용은 [단기 자격 증명을 사용하여 AWS SDKs 및 도구 인증 단원을 참조하십시오.](#)

config 또는 credentials 파일에 이러한 필수 값을 설정하는 예:

```
[default]
aws_access_key_id = AKIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
aws_session_token = AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40lgk
```

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
export
  AWS_SESSION_TOKEN=AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40lgk
```

명령줄을 통해 환경 변수를 설정하는 Windows 예제:

```
setx AWS_ACCESS_KEY_ID AKIAIOSFODNN7EXAMPLE
setx AWS_SECRET_ACCESS_KEY wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
setx
  AWS_SESSION_TOKEN AQoEXAMPLEH4aoAH0gNCAPy...truncated...zrkuWJ0gQs8IZZaIv2BXIa2R40lgk
```

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 통	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	공유 config 파일은 지원되지 않습니다.
<a href="#">SDK for Go V2 (1.x)</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for Go 1.x (V1)</a>	예	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	예	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	예	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	환경 변수는 지원되지 않습니다.

## 로그인 자격 증명 공급자

[기존 AWS Management Console 로그인 자격 증명을 사용하여](#) 프로그래밍 방식 액세스에 사용할 수 있는 단기 자격 증명을 획득할 수 있습니다. 브라우저 기반 인증 흐름을 완료하면 AWS CLI, AWS

Tools for PowerShell 및 AWS SDKs와 같은 로컬 개발 도구에서 작동하는 임시 자격 증명을 AWS 생성합니다.

이러한 자격 증명을 생성하려면 AWS CLI에서 `aws login` 명령을 실행하거나 AWS Tools for PowerShell에서 `Invoke-AWSLogin cmdlet`을 실행합니다. 결과 단기 자격 증명은 로컬에 캐시되어 AWS SDKs에서 재사용할 수 있습니다. 단기 자격 증명은 15분 후에 만료되지만 CLI 및 SDKs는 필요에 따라 최대 12시간까지 자동으로 자격 증명을 새로 고칩니다. 새로 고침 토큰이 만료되면 CLI 또는 PowerShell을 통해 다시 로그인하라는 메시지가 표시됩니다.

로그인 명령은 지정한 프로파일을 `login_session` 설정으로 업데이트합니다. 이 설정은 로그인 워크플로 중에 선택한 관리 콘솔 세션의 자격 증명을 저장합니다.

```
[profile console]
login_session = arn:aws:iam::0123456789012:user/username
region = us-west-2
```

기본적으로 단기 자격 증명 및 새로 고침 토큰은 Linux 및 macOS 또는 Windows의 `~/.aws/login/cache` 디렉터리 `%USERPROFILE%\aws\login\cache`에 있는 JSON 파일에 저장됩니다. 파일 이름은 로그인 세션 이름을 기반으로 합니다. `AWS_LOGIN_CACHE_DIRECTORY` 환경 변수를 설정하여 디렉터리를 재정의할 수 있습니다.

## 로그인 공급자 설정

다음을 사용하여 이 기능을 구성하십시오.

### **AWS\_LOGIN\_CACHE\_DIRECTORY** - 환경 변수

CLI 및 SDKs가 로그인 세션 프로파일에 매핑되는 캐시된 자격 증명을 저장하는 대체 디렉터리입니다.

기본값: `~/.aws/login/cache` Linux 및 macOS 또는 `%USERPROFILE%\aws\login\cache` Windows.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 통	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	아 니 요	
<a href="#">SDK for Go 1.x (V1)</a>	예	
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	아 니 요	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	아 니 요	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	CRT 필요
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	아 니 요	

## 역할 보안 인증 제공자 수임

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#) [이 안내서의 설정 페이지의 이해](#).

역할 수임에는 액세스 권한이 없을 수 있는 AWS 리소스에 액세스하기 위해 일련의 임시 보안 보안 인증을 사용하는 것이 포함됩니다. 이러한 임시 보안 인증은 액세스 키 ID, 보안 액세스 키 및 보안 토큰으로 구성됩니다.

역할을 수임하도록 SDK 또는 도구를 설정하려면 먼저 수임할 특정 역할을 만들거나 식별해야 합니다. IAM 역할은 Amazon 리소스 이름(ARN) 역할로 고유하게 식별됩니다. 역할은 다른 엔티티와 신뢰 관계를 구축합니다. 역할을 사용하는 신뢰할 수 있는 엔티티는 AWS 서비스, 다른 AWS 계정, 웹 자격 증명 공급자 또는 OIDC 또는 SAML 페더레이션일 수 있습니다.

IAM 역할을 식별한 후 해당 역할을 신뢰할 수 있는 경우 해당 역할에서 부여한 권한을 사용하도록 SDK 또는 도구를 구성할 수 있습니다. 이렇게 하려면 다음 설정을 사용하십시오.

이러한 설정 사용을 시작하는 방법에 대한 지침은 이 안내서의 [자격 AWS 증명이 있는 역할을 수임하여 AWS SDKs 및 도구 인증](#)를 참조하세요.

## 역할 보안 인증 제공자 수임 설정

다음을 사용하여 이 기능을 구성하십시오.

## credential\_source - 공유 AWS config 파일 설정

SDK나 도구가 `role_arn` 파라미터로 지정된 역할을 수입하기 위한 권한을 가진 보안 인증을 인증을 찾을 수 있는 위치를 지정하기 위해 Amazon EC2 인스턴스 또는 Amazon Elastic Container Service 컨테이너 내에서 사용됩니다.

기본값: 없음

유효값:

- 환경 – SDK나 도구가 [AWS\\_ACCESS\\_KEY\\_ID](#) 및 [AWS\\_SECRET\\_ACCESS\\_KEY](#) 환경 변수에서 소스 보안 인증을 검색하도록 지정합니다.
- `Ec2InstanceMetadata` – SDK 또는 도구가 [EC2 인스턴스 프로파일에 연결된 IAM 역할](#)을 사용하여 소스 보안 인증을 가져오도록 지정합니다.
- `EcsContainer` - SDK 또는 도구가 소스 자격 증명을 얻기 위해 [Amazon ECS 컨테이너에 연결된 IAM 역할](#) 또는 [Amazon EKS 컨테이너에 연결된 IAM 역할](#)을 사용하도록 지정합니다.

`credential_source`과 `source_profile` 모두를 동일한 프로파일에서 지정할 수 없습니다.

보안 인증을 Amazon EC2에서 소싱해야 함을 나타내도록 config 파일에 설정하는 예:

```
credential_source = Ec2InstanceMetadata
role_arn = arn:aws:iam::123456789012:role/my-role-name
```

## duration\_seconds - 공유 AWS config 파일 설정

역할 세션의 최대 기간(초)을 지정합니다.

이 설정은 프로파일에서 역할 수입을 지정한 경우에만 적용됩니다.

기본값: 3600초(1시간)

유효한 값: 이 값의 범위는 900초(15분)부터 해당 역할에 대한 구성된 최대 세션 기간 설정(최대값: 43200초 또는 12시간)까지 가능합니다. 자세한 내용은 IAM 사용 설명서의 [역할의 최대 세션 기간 설정 보기](#)를 참조하십시오.

config 파일에서 이를 설정하는 예:

```
duration_seconds = 43200
```

## external\_id - 공유 AWS config 파일 설정

타사에서 고객 계정의 역할을 수입하는 데 사용하는 고유한 식별자를 지정합니다.

이 설정은 프로파일에서 역할을 수입하도록 지정하고 역할에 대한 신뢰 정책에서 ExternalId에 대한 값을 필요로 하는 경우에만 적용됩니다. 값은 프로파일이 역할을 지정할 때 AssumeRole 작업에 전달되는 ExternalId 파라미터에 매핑됩니다.

기본값: 없음.

유효한 값: IAM 사용 설명서의 [AWS 리소스에 대한 액세스 권한을 타사에 부여할 때 외부 ID를 사용하는 방법을 참조하세요](#).

config 파일에서 이를 설정하는 예:

```
external_id = unique_value_assigned_by_3rd_party
```

### **mfa\_serial** - 공유 AWS config 파일 설정

사용자가 역할 수입 시 사용해야 하는 다중 인증(MFA)장치의 ID 또는 일련 번호를 지정합니다.

해당 역할에 대한 신뢰 정책에 MFA 인증을 필요로 하는 조건이 포함된 역할을 수입하는 경우 필요합니다. MFA에 대한 자세한 내용은 IAM 사용 설명서의 [IAM에서의AWS 다단계 인증](#)을 참고하세요.

기본값: 없음.

유효한 값: 이 값은 하드웨어 디바이스용 일련 번호(예: GAHT12345678)또는 가상 MFA 디바이스용 Amazon 리소스 이름(ARN)(예: )일 수 있습니다. ARN 형식은 `arn:aws:iam::account-id:mfa/mfa-device-name`입니다.

config 파일에서 이를 설정하는 예:

이 예제는 계정에 대해 생성되고 특정 사용자에게 대해 활성화된 MyMFADevice라는 이름의 가상 MFA 장치를 사용한다고 가정합니다.

```
mfa_serial = arn:aws:iam::123456789012:mfa/MyMFADevice
```

### **role\_arn** - 공유 AWS config 파일 설정, **AWS\_ROLE\_ARN** - 환경 변수, **aws.roleArn** - JVM 시스템 속성: Java/Kotlin만 해당

이 프로파일을 사용하여 요청된 작업을 수행하는 데 사용할 IAM 역할의 Amazon 리소스 이름 (ARN)을 지정합니다.

기본값: 없음.

유효한 값: 이 값은 다음과 같은 형식의 IAM 역할의 ARN이어야 합니다.

```
arn:aws:iam::account-id:role/role-name
```

또한 다음 설정 중 하나를 지정해야 합니다.

- `source_profile` — 이 프로파일에서 역할을 수임할 권한이 있는 보안 인증을 찾는 데 사용할 다른 프로파일을 식별합니다.
- `credential_source` — 현재 환경 변수로 식별되는 보안 인증 또는 Amazon EC2 인스턴스 프로파일 또는 Amazon ECS 컨테이너 인스턴스에 첨부된 보안 인증을 사용합니다.
- `web_identity_token_file` — 모바일 또는 웹 애플리케이션에서 인증된 사용자에 대해 퍼블릭 ID 공급자 또는 OpenID Connect(OIDC)호환 보안 인증 공급자를 사용합니다.

**role\_session\_name** - 공유 AWS config 파일 설정, **AWS\_ROLE\_SESSION\_NAME** - 환경 변수, **aws.roleSessionName** - JVM 시스템 속성: Java/Kotlin만 해당

역할 세션에 연결할 이름을 지정합니다. 이 이름은 이 세션과 연결된 항목에 대한 AWS CloudTrail 로그에 나타나며, 감사할 때 유용할 수 있습니다. 세부 정보는 AWS CloudTrail 사용 설명서의 [CloudTrail userIdentity 요소](#)를 참조하세요.

기본값: 선택적 파라미터입니다. 이 값을 제공하지 않은 경우 프로파일이 역할을 수임할 때 세션 이름이 자동으로 생성됩니다.

유효한 값: AWS CLI 또는 AWS API가 사용자를 대신하여 AssumeRole 작업(또는 작업과 같은 AssumeRoleWithWebIdentity 작업)을 호출할 때 RoleSessionName 파라미터에 제공됩니다. 값은 쿼리할 수 있는 수임된 역할 사용자 Amazon 리소스 이름(ARN)의 일부가 되며, 이 프로파일에서 간접 호출한 작업에 대한 CloudTrail 로그 항목의 일부로 표시됩니다.

```
arn:aws:sts::123456789012:assumed-role/my-role-name/my-role_session_name.
```

config 파일에서 이를 설정하는 예:

```
role_session_name = my-role-session-name
```

**source\_profile** - 공유 AWS config 파일 설정

보안 인증이 원래 프로파일의 `role_arn` 설정에 지정된 역할을 수임하는 데 사용되는 다른 프로파일을 지정합니다. 공유 AWS config 및 credentials 파일에서 프로필이 사용되는 방법을 이해하려면 섹션을 참조하세요 [공유 config 및 credentials 파일](#).

역할 수임 프로파일이기도 한 프로파일을 지정하는 경우 보안 인증을 완전히 확인하기 위해 각 역할이 순차적으로 수임됩니다. SDK가 보안 인증이 있는 프로파일을 발견하면 이 체인이 중지됩니다.

다. 역할 체인은 AWS CLI 또는 AWS API 역할 세션을 최대 1시간으로 제한하며 늘릴 수 없습니다. 자세한 내용은 IAM 사용 설명서의 [역할 용어 및 개념](#)을 참조하십시오.

기본값: 없음.

유효한 값: config 및 credentials 파일에 정의된 프로파일 이름으로 구성된 텍스트 문자열입니다. 또한 현재 프로파일에서 role\_arn의 값도 지정해야 합니다.

credential\_source과 source\_profile 모두를 동일한 프로파일에서 지정할 수 없습니다.

구성 파일에서 이를 설정하는 예:

```
[profile A]
source_profile = B
role_arn = arn:aws:iam::123456789012:role/RoleA
role_session_name = ProfileARoleSession

[profile B]
credential_process = ./aws_signing_helper credential-process --certificate /
path/to/certificate --private-key /path/to/private-key --trust-anchor-
arn arn:aws:rolesanywhere:region:account:trust-anchor/TA_ID --profile-
arn arn:aws:rolesanywhere:region:account:profile/PROFILE_ID --role-arn
arn:aws:iam::account:role/ROLE_ID
```

앞선 예제에서 A 프로파일은 SDK나 도구가 연결된 B 프로파일의 자격 증명을 자동으로 조회하도록 지시합니다. 이 경우 B 프로파일은 [IAM Roles Anywhere를 사용하여 AWS SDKs 및 도구 인증](#)에서 제공하는 자격 증명 도우미 도구를 사용하여 AWS SDK에 필요한 자격 증명을 가져옵니다. 이러한 임시 보안 인증은 코드에서 AWS 리소스에 액세스하기 위해 사용됩니다. 지정된 역할에는 명령 AWS 서비스또는 API 메서드와 같이 요청된 코드를 실행할 수 있도록 허용하는 IAM 권한 정책이 연결되어 있어야 합니다. 프로파일 A가 수행하는 모든 작업에는 역할 세션 이름이 CloudTrail 로그에 기록됩니다.

역할 체이닝의 두 번째 예로, Amazon Elastic Compute Cloud 인스턴스에서 애플리케이션을 실행하고 있고 그 애플리케이션이 다른 역할을 수입하도록 하려는 경우, 다음 구성을 사용할 수 있습니다.

```
[profile A]
source_profile = B
role_arn = arn:aws:iam::123456789012:role/RoleA
role_session_name = ProfileARoleSession
```

```
[profile B]
credential_source=Ec2InstanceMetadata
```

프로파일 A는 Amazon EC2 인스턴스의 자격 증명을 사용해 지정된 역할을 수입하며, 자격 증명을 자동으로 갱신합니다.

**web\_identity\_token\_file** - 공유 AWS config 파일 설정, **AWS\_WEB\_IDENTITY\_TOKEN\_FILE** - 환경 변수, **aws.webIdentityTokenFile** - JVM 시스템 속성: Java/Kotlin만 해당

[지원되는 OAuth 2.0 공급자](#) 또는 [OpenID Connect ID 공급자](#)의 액세스 토큰을 포함하는 파일의 경로를 지정합니다.

이 설정을 사용하면 [Google](#), [Facebook](#) 및 [Amazon](#) 등과 같은 웹 ID 페더레이션 공급자를 사용하여 인증할 수 있습니다. SDK 또는 개발자 도구는 이 파일의 내용을 로드하고 사용자를 대신하여 AssumeRoleWithWebIdentity 작업을 직접 호출할 때 WebIdentityToken 인수로서 전달합니다.

기본값: 없음.

유효한 값: 이 값은 경로 및 파일 이름이어야 합니다. 파일에는 ID 공급자가 제공한 OAuth 2.0 액세스 토큰 또는 OpenID Connect ID 토큰을 포함해야 합니다. 상대 경로는 프로세스의 작업 디렉터리를 기준으로 처리됩니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 원 톤	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	부 분 적	credential_source 이 지원되지 않음. duration_seconds 이 지원되지 않음. mfa_serial 이 지원되지 않음.
<a href="#">SDK for Go V2 (1.x)</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for Go 1.x (V1)</a>	예	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	부 분 적	mfa_serial 은 지원되지 않습니다. duration_ seconds 는 지원되지 않습니다.
<a href="#">SDK for Java 1.x</a>	부 분 적	credential_source 는 지원되지 않습니다. mfa_seria l 은 지원되지 않습니다. JVM 시스템 속성은 지원되지 않습니다.
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	부 분 적	credential_source 이 지원되지 않음.
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## 컨테이너 보안 인증 제공업체

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs 이 안내서의 설정 페이지의 이해](#).

컨테이너 자격 증명 공급자는 고객의 컨테이너화 애플리케이션에 대한 자격 증명을 가져옵니다. 이 보안 인증 공급자는 Amazon Elastic Container Service(Amazon ECS) 및 Amazon Elastic Kubernetes Service(Amazon EKS) 고객에게 유용합니다. SDK는 GET 요청을 통해 지정된 HTTP 엔드포인트에서 보안 인증을 로드하려고 시도합니다.

Amazon ECS를 사용하는 경우 보안 인증 격리, 권한 부여 및 감사 가능성을 개선하기 위해 작업 IAM 역할을 사용하는 것이 좋습니다. 구성된 경우 Amazon ECS는 SDK 및 도구가 보안 인증을 얻기 위해 사용하는 `AWS_CONTAINER_CREDENTIALS_RELATIVE_URI` 환경 변수를 설정합니다. 이 기능을 사용하도록 Amazon ECS를 구성하려면 Amazon Elastic Container Service 개발자 안내서의 [태스크 IAM 역할](#)을 참조하세요.

Amazon EKS를 사용하는 경우 보안 인증 격리, 최소 권한, 감사 가능성, 독립적인 운영, 재사용성 및 확장성을 개선하기 위해 Amazon EKS Pod Identity를 사용하는 것이 좋습니다. 포드와 IAM 역할은 모두 Kubernetes 서비스 계정과 연결되어 애플리케이션에 대한 보안 인증을 관리합니다. Amazon EKS 포드 ID에 대해 자세히 알아보려면 Amazon EKS 사용 설명서의 [Amazon EKS Pod Identities](#)를 참조하세요. 구성된 경우 Amazon EKS는 SDK 및 도구가 보안 인증을 얻기 위해 사용하는 `AWS_CONTAINER_CREDENTIALS_FULL_URI` 및 `AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE` 환경 변수를 설정합니다. 설정 정보는 Amazon [EKS 사용 설명서의 Amazon EKS Pod Identity Agent 설정](#)을 참조하거나 AWS 블로그 웹 사이트의 [Amazon EKS Pod Identity simplifies IAM permissions for applications on Amazon EKS clusters](#)를 참조하세요.

다음을 사용하여 이 기능을 구성하십시오.

### `AWS_CONTAINER_CREDENTIALS_FULL_URI` - 환경 변수

보안 인증을 요청할 때 SDK가 사용할 전체 HTTP URL 엔드포인트를 지정합니다. 여기에는 스키마와 호스트가 모두 포함됩니다.

기본값: 없음.

유효한 값: 유효한 URI.

참고: 이 설정은 `AWS_CONTAINER_CREDENTIALS_RELATIVE_URI` 설정의 대안이며 `AWS_CONTAINER_CREDENTIALS_RELATIVE_URI` 이 설정되지 않은 경우에만 사용됩니다.

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_CONTAINER_CREDENTIALS_FULL_URI=http://localhost/get-credentials
```

또는

```
export AWS_CONTAINER_CREDENTIALS_FULL_URI=http://localhost:8080/get-credentials
```

### `AWS_CONTAINER_CREDENTIALS_RELATIVE_URI` - 환경 변수

보안 인증을 요청할 때 SDK가 사용할 상대 HTTP URL 엔드포인트를 지정합니다. 값은 기본 Amazon ECS 호스트 이름인 `169.254.170.2`에 추가됩니다.

기본값: 없음.

유효한 값: 유효한 상대 URI.

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_CONTAINER_CREDENTIALS_RELATIVE_URI=/get-credentials?a=1
```

### `AWS_CONTAINER_AUTHORIZATION_TOKEN` - 환경 변수

인증 토큰을 일반 텍스트로 지정합니다. 이 변수를 설정하면 SDK는 환경 변수 값을 사용하여 HTTP 요청의 권한 헤더를 설정합니다.

기본값: 없음.

유효한 값: 문자열.

참고: 이 설정은 `AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE` 설정의 대안이며 `AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE` 이 설정되지 않은 경우에만 사용됩니다.

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_CONTAINER_CREDENTIALS_FULL_URI=http://localhost/get-credential
export AWS_CONTAINER_AUTHORIZATION_TOKEN=Basic abcd
```

## AWS\_CONTAINER\_AUTHORIZATION\_TOKEN\_FILE - 환경 변수

일반 텍스트로 된 인증 토큰을 포함하는 파일의 절대 파일 경로를 지정합니다.

기본값: 없음.

유효한 값: 문자열.

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_CONTAINER_CREDENTIALS_FULL_URI=http://localhost/get-credential
export AWS_CONTAINER_AUTHORIZATION_TOKEN_FILE=/path/to/token
```

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	예	
<a href="#">SDK for Java 2.x</a>	예	<a href="#">Lambda SnapStart</a> 가 활성화되면, 인증을 위해 AWS_CONTAINER_CREDENTIALS_FULL_URI 와 AWS_CONTAINER_AUTHORIZATION_TOKEN 이 자동으로 사용됩니다.
<a href="#">SDK for Java 1.x</a>	예	<a href="#">Lambda SnapStart</a> 가 활성화되면, 인증을 위해 AWS_CONTAINER_CREDENTIALS_FULL_URI 와 AWS_CONTAINER_AUTHORIZATION_TOKEN 이 자동으로 사용됩니다.
<a href="#">SDK for JavaScript 3.x</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for JavaScript 2.x</a>	예	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	<a href="#">Lambda SnapStart</a> 가 활성화되면, 인증을 위해 AWS_CONTAINER_CREDENTIALS_FULL_URI 와 AWS_CONTAINER_AUTHORIZATION_TOKEN 이 자동으로 사용됩니다.
<a href="#">SDK for .NET 3.x</a>	예	<a href="#">Lambda SnapStart</a> 가 활성화되면, 인증을 위해 AWS_CONTAINER_CREDENTIALS_FULL_URI 와 AWS_CONTAINER_AUTHORIZATION_TOKEN 이 자동으로 사용됩니다.
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	<a href="#">Lambda SnapStart</a> 가 활성화되면, 인증을 위해 AWS_CONTAINER_CREDENTIALS_FULL_URI 와 AWS_CONTAINER_AUTHORIZATION_TOKEN 이 자동으로 사용됩니다.
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## IAM 아이덴티티 센터 보안 인증 공급자

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 Support AWS SDKs [이 안내서의 설정 페이지의 이해](#).

이 인증 메커니즘은 AWS IAM Identity Center 를 사용하여 코드 AWS 서비스에 대한 Single Sign-On(SSO) 액세스 권한을 얻습니다.

### Note

AWS SDK API 설명서에서 IAM Identity Center 자격 증명 공급자를 SSO 자격 증명 공급자라고 합니다.

IAM Identity Center를 활성화한 후 공유 AWS config 파일에서 설정에 대한 프로파일을 정의합니다. 이 프로파일은 IAM ID 센터 액세스 포털에 연결하는 데 사용됩니다. 사용자가 IAM Identity Center에서 성공적으로 인증하면 포털은 해당 사용자와 관련된 IAM 역할에 대한 단기 보안 인증을 반환합니다. SDK가 구성에서 임시 자격 증명을 가져와 AWS 서비스 요청에 사용하는 방법을 알아보려면 섹션을 참조하세요 [AWS SDKs 및 도구에 대한 IAM Identity Center 인증 확인 방법](#).

config 파일을 통해 IAM ID 센터를 구성하는 두 가지 방법이 있습니다.

- (권장) SSO 토큰 공급자 구성 - 연장된 세션 지속 시간. 사용자 지정 세션 지속 시간을 지원합니다.
- 새로 고칠 수 없는 레거시 구성 - 고정된 8시간 세션 사용.

두 구성 모두 세션이 만료되면 다시 로그인해야 합니다.

다음 두 안내서에는 IAM Identity Center에 대한 추가 정보가 포함되어 있습니다.

- [AWS IAM Identity Center 사용 설명서](#)
- [AWS IAM Identity Center 포털 API 참조](#)

SDK 및 도구가 이 구성을 사용하여 보안 인증을 사용하고 새로 고치는 방법에 대한 자세한 내용은 [AWS SDKs 및 도구에 대한 IAM Identity Center 인증 확인 방법](#) 섹션을 참조하십시오.

## 사전 조건

먼저 IAM Identity Center를 활성화해야 합니다. IAM Identity Center 활성화에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [AWS IAM Identity Center 활성화](#)를 참조하세요.

**Note**

또한, 이 페이지에 자세히 설명된 전체 사전 조건 및 필요한 공유 config 파일 구성을 확인하려면, [IAM Identity Center를 사용하여 AWS SDK 및 도구 인증 설정을 위한 안내형 지침](#)을 참고하세요.

## SSO 토큰 공급자 구성

SSO 토큰 공급자 구성을 사용하면 AWS SDK 또는 도구가 연장된 세션 기간까지 세션을 자동으로 새로 고칩니다. 세션 기간 및 최대 기간에 대한 자세한 내용은 [AWS IAM Identity Center 사용 설명서의 AWS 액세스 포털 및 IAM Identity Center 통합 애플리케이션의 세션 기간 구성](#)을 참조하세요.

config 파일의 sso-session 섹션은 SSO 액세스 토큰을 획득하기 위한 구성 변수를 그룹화하는 데 사용되며, 그런 다음 자격 AWS 증명을 획득하는 데 사용할 수 있습니다. config 파일 내에서 이 섹션에 대한 더 자세한 내용은 [구성 파일 형식](#)를 참고하세요.

다음의 공유 config 파일 예시는, dev 프로파일을 사용하여 IAM Identity Center 자격 증명을 요청하도록 SDK 또는 도구를 구성합니다.

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

앞의 예제에서는 sso-session 섹션을 정의하고 이를 프로파일에 연결한다는 것을 보여줍니다. 일반적으로 SDK가 AWS 자격 증명을 요청할 수 있도록 profile 섹션에서 sso\_account\_id 및 sso\_role\_name 설정해야 합니다. sso-session 섹션 내에서 sso\_start\_url, 및 sso\_region를 설정해야 sso\_registration\_scopes 합니다.

sso\_account\_id 및 sso\_role\_name은 SSO 토큰 구성의 모든 시나리오에 필수적이지는 않습니다. 애플리케이션에서 보유자 인증을 지원하는 AWS 서비스 만 사용하는 경우 기존 AWS 자격 증명도 필요하지 않습니다. 보유자 인증은 보유자 토큰이라는 보안 토큰을 사용하는 HTTP 인증 체계입니다. 이 시나리오에서는 sso\_account\_id 및 sso\_role\_name은 필수가 아닙니다. 서비스가 보유자 토큰 권한 부여를 지원하는지 확인하려면 개별 AWS 서비스 가이드를 참조하세요.

등록 범위는 `sso-session`의 일부로 구성됩니다. 범위는 애플리케이션의 사용자 계정 액세스를 제한하는 OAuth 2.0의 메커니즘입니다. 앞의 예제에서는 계정과 역할을 나열하는 데 필요한 액세스를 제공하기 위해 `sso_registration_scopes`를 설정합니다.

다음 예제는 동일한 `sso-session` 구성을 여러 프로파일에 재사용하는 방법을 보여줍니다.

```
[profile dev]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole

[profile prod]
sso_session = my-sso
sso_account_id = 111122223333
sso_role_name = SampleRole2

[sso-session my-sso]
sso_region = us-east-1
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_registration_scopes = sso:account:access
```

인증 토큰은 세션 이름을 기반으로 하는 파일 이름을 사용하여 `~/.aws/sso/cache` 디렉터리 아래의 디스크에 캐시됩니다.

## 새로 고칠 수 없는 레거시 구성

새로 고칠 수 없는 기존 구성을 사용하는 자동 토큰 새로 고침은 지원되지 않습니다. 대신 [SSO 토큰 공급자 구성](#)을(를)사용하는 것이 좋습니다.

새로 고칠 수 없는 기존 구성을 사용하려면 프로파일에 다음 설정을 지정해야 합니다.

- `sso_start_url`
- `sso_region`
- `sso_account_id`
- `sso_role_name`

`sso_start_url` 및 `sso_region` 설정을 사용하여 프로파일의 사용자 포털을 지정합니다. `sso_account_id` 및 `sso_role_name` 설정으로 권한을 지정합니다.

다음 예제에서는 `config` 파일에 필요한 네 가지 값을 설정합니다.

```
[profile my-sso-profile]
sso_start_url = https://my-sso-portal.awsapps.com/start
sso_region = us-west-2
sso_account_id = 111122223333
sso_role_name = SSOReadOnlyRole
```

인증 토큰은 `sso_start_url`에 기반한 파일 이름을 가진 `~/.aws/sso/cache` 디렉터리 아래의 디스크에 캐시됩니다.

## IAM Identity Center 보안 인증 공급자 설정

다음을 사용하여 이 기능을 구성하십시오.

### `sso_start_url` - 공유 AWS `config` 파일 설정

조직의 IAM Identity Center 발급자 URL 또는 액세스 포털 URL을 가리키는 URL입니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [AWS 액세스 포털 사용](#)을 참조하세요.

이 값을 찾으려면 [IAM Identity Center 콘솔](#)을 열고 대시보드를 확인한 다음 AWS 액세스 포털 URL을 찾으세요.

- 또는 버전 2.22.0부터 AWS 발급자 URL 값을 대신 사용할 AWS CLI 수 있습니다.

### `sso_region` - 공유 AWS `config` 파일 설정

IAM Identity Center 포털 호스트, 즉 IAM Identity Center를 활성화하기 전에 선택한 리전이 AWS 리전 포함됨. 이는 기본 AWS 리전과 독립적이며 다를 수 있습니다.

AWS 리전 및 해당 코드의 전체 목록은 [리전 엔드포인트](#)를 참조하세요 Amazon Web Services 일반 참조. 이 값을 찾으려면 [IAM Identity Center 콘솔](#)을 열고 대시보드를 확인한 다음 리전을 찾으십시오.

### `sso_account_id` - 공유 AWS `config` 파일 설정

인증을 위해 AWS Organizations 서비스를 통해 추가된 숫자 ID AWS 계정입니다.

사용 가능한 계정 목록을 보려면 [IAM Identity Center 콘솔](#)로 이동하여 AWS 계정 페이지를 여십시오. AWS IAM Identity Center 포털 API 참조의 [ListAccounts API](#) 메서드를 사용하여 사용 가능한 계정 목록을 볼 수도 있습니다. 예를 들어 AWS CLI, 메서드 [list-accounts](#)를 호출할 수 있습니다.

## sso\_role\_name - 공유 AWS config 파일 설정

사용자의 최종 권한을 정의하는 IAM 역할로 프로비저닝된 권한 집합의 이름입니다. 역할은에서 AWS 계정 지정함에 있어야 합니다 sso\_account\_id. Amazon 리소스 이름(ARN) 역할을 사용하지 말고 역할 이름을 사용하십시오.

권한 세트에는 IAM 정책 및 사용자 지정 권한 정책이 첨부되어 있으며 할당된 AWS 계정에 대한 사용자의 액세스 수준을 정의합니다.

당 사용 가능한 권한 세트 목록을 보려면 [IAM Identity Center 콘솔](#)로 AWS 계정이동하여 AWS 계정 페이지를 엽니다. AWS 계정 테이블에 나열된 올바른 권한 세트 이름을 선택합니다. AWS IAM Identity Center 포털 API 참조의 [ListAccountsRoles](#) API 메서드를 사용하여 사용 가능한 권한 집합 목록을 볼 수도 있습니다. 예를 들어 AWS CLI, 메서드 [list-account-roles](#)를 호출할 수 있습니다.

## sso\_registration\_scopes - 공유 AWS config 파일 설정

sso-session에 대해 인증될 심포로 구분된 유효한 범위 문자열 목록입니다. 애플리케이션은 하나 이상의 범위를 요청할 수 있으며 애플리케이션에 발급되는 액세스 토큰은 부여된 범위로 제한됩니다. IAM Identity Center 서비스에서 새로 고침 토큰을 다시 받으려면 sso:account:access의 최소 범위를 부여해야 합니다. 사용 가능한 액세스 범위 옵션 목록은 AWS IAM Identity Center 사용 설명서의 [액세스 범위](#)를 참조하세요.

이러한 범위는 등록된 OIDC 클라이언트에 대해 인증받기 위해 요청된 권한과 클라이언트가 검색한 액세스 토큰을 정의합니다. 범위는 IAM Identity Center 보유자 토큰 인증 엔드포인트에 대한 액세스를 승인합니다.

이 설정은 새로 고칠 수 없는 레거시 구성에는 적용되지 않습니다. 레거시 구성을 사용하여 발급된 토큰은 암시적으로 범위 sso:account:access(으)로 제한됩니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지참고 또는 추가 정보 온 통
<a href="#">AWS CLI v2</a>	예

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	예	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	예	구성 값은 credentials 파일에서도 지원됩니다.
<a href="#">SDK for Java 1.x</a>	아 니 요	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	예	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	부 분 적	새로 고칠 수 없는 레거시 구성에만 해당.
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">PowerShell V4용 도구</a>	예	

## IMDS 보안 인증 제공자

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 Support AWS SDKs [이 안내서의 설정 페이지의 이해](#).

인스턴스 메타데이터 서비스(IMDS)는 실행 중인 인스턴스를 구성 또는 관리하는 데 사용할 수 있는 인스턴스 관련 데이터를 제공합니다. 사용 가능한 데이터에 대한 자세한 내용은 Amazon EC2 사용 설명서의 [인스턴스 메타데이터를 사용한 작업](#)을 참고하세요. Amazon EC2는 인스턴스에 대한 다양한 정보를 제공할 수 있는 로컬 엔드포인트를 제공합니다. 인스턴스에 역할이 연결된 경우 해당 역할에 유효한 보안 인증 세트를 제공할 수 있습니다. SDK는 해당 엔드포인트를 사용하여 [기본 보안 인증 공급자](#) 체인의 일부로 보안 인증을 확인할 수 있습니다. 세션 토큰을 사용하는 보다 안전한 IMDS 버전인 인스턴스 메타데이터 서비스 버전 2(IMDSv2)가 기본으로 사용됩니다. 재시도할 수 없는 조건(HTTP 오류 코드 403, 404, 405)으로 인해 이 기본이 실패할 경우 IMDSv1이 대체 수단으로 사용됩니다.

다음을 사용하여 이 기능을 구성하십시오.

### AWS\_EC2\_METADATA\_DISABLED - 환경 변수

보안 인증 획득에 Amazon EC2 인스턴스 메타데이터 서비스 (IMDS)사용 시도 여부

기본값: false.

유효값:

- **true** - 보안 인증을 얻는 데 IMDS를 사용하지 않습니다.
- **false** - 보안 인증을 얻는 데 IMDS를 사용합니다.

**ec2\_metadata\_v1\_disabled** - 공유 AWS config 파일 설정,  
**AWS\_EC2\_METADATA\_V1\_DISABLED** - 환경 변수, **aws.disableEc2MetadataV1** - JVM 시스템 속성: Java/Kotlin만 해당

IMDSv2가 실패할 경우 IMDSv1(Instance Metadata Service Version 1)을 폴백으로 사용할지 여부.

**Note**

새 SDK는 IMDSv1을 지원하지 않으므로 이 설정을 지원하지 않습니다. 자세한 내용은 테이블 [AWS SDKs 도구 지원](#)를 참조하세요.

기본값: false

유효값:

- **true** - IMDSv1을 폴백으로 사용하지 않습니다.
- **false** - IMDSv1을 폴백으로 사용합니다.

**ec2\_metadata\_service\_endpoint** - 공유 AWS config 파일 설정,  
**AWS\_EC2\_METADATA\_SERVICE\_ENDPOINT** - 환경 변수, **aws.ec2MetadataServiceEndpoint** - JVM 시스템 속성: Java/Kotlin만 해당

IMDS 엔드포인트. 이 값은 AWS SDKs. Amazon EC2

기본값: ec2\_metadata\_service\_endpoint\_mode와 IPv4이 같으면 기본 엔드포인트는 http://169.254.169.254입니다. ec2\_metadata\_service\_endpoint\_mode와 IPv6이 같으면 기본 엔드포인트는 http://[fd00:ec2::254]입니다.

유효한 값: 유효한 URI.

**ec2\_metadata\_service\_endpoint\_mode** - 공유 AWS config 파일 설정, **AWS\_EC2\_METADATA\_SERVICE\_ENDPOINT\_MODE** - 환경 변수, **aws.ec2MetadataServiceEndpointMode** - JVM 시스템 속성: Java/Kotlin만 해당

IMDS의 엔드포인트 모드.

기본값: IPv4.

유효한 값: IPv4, IPv6.

**Note**

IMDS 보안 인증 제공자는 [자격 증명 공급자 체인의 이해](#)의 일부입니다. 그러나 IMDS 자격 증명 제공자는 여기에 있는 일련의 제공자를 거친 후에만 확인됩니다. 따라서 프로그램에서 이 공급자의 보안 인증을 사용하려면 구성에서 다른 유효한 보안 인증 공급자를 제거하거나 다른 프로파일을 사용해야 합니다. 또는 보안 인증 제공자 체인에 의존하여 어떤 제공자가 유효한 보안 인증을 반환하는지 자동으로 검색하는 대신 IMDS 보안 인증 제공자의 사용을 코드로 지정하십시오. 서비스 클라이언트를 생성할 때 보안 인증 소스를 직접 지정할 수 있습니다.

## IMDS 보안 인증 보안

기본적으로 AWS SDK가 유효한 자격 증명으로 구성되지 않은 경우 SDK는 Amazon EC2 인스턴스 메타데이터 서비스(IMDS)를 사용하여 AWS 역할의 자격 증명을 검색하려고 시도합니다. `AWS_EC2_METADATA_DISABLED` 환경 변수를 `true`로 설정하여 이 동작을 비활성화할 수 있습니다. 이를 통해 Amazon EC2 인스턴스 메타데이터 서비스를 가장 신뢰할 수 없는 네트워크에서 불필요한 네트워크 활동을 방지하고 보안을 강화합니다.

**Note**

AWS 유효한 자격 증명으로 구성된 SDK 클라이언트는 이러한 설정에 관계없이 IMDS를 사용하여 자격 증명을 검색하지 않습니다.

### Amazon EC2 IMDS 보안 인증 비활성화

이 환경 변수를 설정하는 방법은 사용 중인 운영 체제와 변경 내용을 지속적으로 적용할지 여부에 따라 달라집니다.

#### Linux 및 macOS

Linux 또는 macOS를 사용하는 고객은 다음 명령을 사용해 이 환경 변수를 설정할 수 있습니다.

```
$ export AWS_EC2_METADATA_DISABLED=true
```

여러 셸 세션 및 시스템 재시작 시에도 이 설정을 유지하려면 위의 명령을 `.bash_profile`, `.zsh_profile`, 혹은 `.profile` 등의 셸 프로파일 파일에 추가할 수 있습니다.

## Windows

Windows를 사용하는 고객은 다음 명령을 사용해 이 환경 변수를 설정할 수 있습니다.

```
$ set AWS_EC2_METADATA_DISABLED=true
```

이 설정을 여러 셸 세션 및 시스템 재시작에 걸쳐 지속되게 하려면 다음 명령을 대신 사용할 수 있습니다.

```
$ setx AWS_EC2_METADATA_DISABLED=true
```

### Note

이 setx 명령은 현재 셸 세션에 값을 적용하지 않으므로 변경 내용을 적용하려면 셸을 다시 로드하거나 다시 열어야 합니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	예	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	부 분 적	JVM 시스템 속성: <code>aws.disableEc2MetadataV1</code> 대신 <code>com.amazonaws.sdk.disableEc2MetadataV1</code> 을 사용하며, <code>aws.ec2MetadataServiceEndpoint</code> 와

SDK	지 운 톤	참고 또는 추가 정보
		aws.ec2MetadataServiceEndpointMode 는 지원되지 않습니다.
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	예	
<a href="#">SDK for Kotlin</a>	예	IMDSv1 폴백을 사용하지 않습니다.
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	IMDSv1 폴백을 사용하지 않습니다.
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	[Amazon.Util.EC2InstanceMetadata]::EC2MetadataV1Disabled = \$true 를 사용하여 코드에서 IMDSv1 폴백을 명시적으로 비활성화할 수 있습니다.
<a href="#">PowerShell V4용 도구</a>	예	[Amazon.Util.EC2InstanceMetadata]::EC2MetadataV1Disabled = \$true 를 사용하여 코드에서 IMDSv1 폴백을 명시적으로 비활성화할 수 있습니다.

## 프로세스 보안 인증 제공자

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#) [이 안내서의 설정 페이지의 이해](#).

SDK는 사용자 지정 사용 사례에 맞게 보안 인증 공급자 체인을 확장할 수 있는 방법을 제공합니다. 이 공급자를 사용하면 온프레미스 자격 증명 저장소에서 자격 증명을 가져오거나, 온프레미스 ID 공급자와 통합하는 등 사용자 지정 구현을 제공할 수 있습니다.

예를 들어 IAM Roles Anywhere는 `credential_process`를 사용하여 애플리케이션을 대신하여 임시 자격 증명을 가져옵니다. 이 용도로 `credential_process`를 구성하려면 [IAM Roles Anywhere를 사용하여 AWS SDKs 및 도구 인증을\(를\)참조하십시오](#).

### Note

다음은 외부 프로세스에서 자격 증명을 가져오는 방법을 설명한 것으로, AWS외부에서 소프트웨어를 실행하는 경우 사용할 수 있습니다. AWS 컴퓨팅 리소스를 기반으로 빌드하는 경우 다른 자격 증명 공급자를 사용합니다. 이 옵션을 사용하는 경우 운영체제의 보안 모범 사례를 적용해 구성 파일을 가능한 한 엄격하게 보호해야 합니다. SDKs 및는 이러한 정보를 캡처하고 기록할 AWS CLI 수 `StdErr`있어 권한이 없는 사용자에게 노출될 수 있으므로 사용자 지정 자격 증명 도구가에 비밀 정보를 쓰지 않는지 확인합니다.

다음을 사용하여 이 기능을 구성하십시오.

### `credential_process` - 공유 AWS config 파일 설정

사용할 보안 인증을 생성하거나 검색하기 위해 SDK 또는 도구가 실행하는 외부 명령을 지정합니다. 설정은 SDK가 간접 호출할 프로그램/명령의 이름을 지정합니다. SDK는 프로세스를 간접 호출할 때 프로세스가 `stdout`에 JSON 데이터를 쓸 때까지 기다립니다. 사용자 지정 공급자는 특정 형식으로 정보를 반환해야 합니다. 이 정보에는 SDK 또는 도구가 사용자를 인증하는 데 사용할 수 있는 보안 인증이 포함됩니다.

**Note**

프로세스 보안 인증 공급자는 [자격 증명 공급자 체인의 이해](#)의 일부입니다. 그러나 프로세스 보안 인증 공급자는 이 시리즈에 속한 다른 여러 공급자를 거친 후에만 확인됩니다. 따라서 프로그램에서 이 공급자의 보안 인증을 사용하려면 구성에서 다른 유효한 보안 인증 공급자를 제거하거나 다른 프로파일을 사용해야 합니다. 또는 보안 인증 공급자 체인에 의존하여 유효한 보안 인증을 반환하는 공급자를 자동으로 검색하는 대신 코드에 프로세스 보안 인증 공급자의 사용을 지정하십시오. 서비스 클라이언트를 생성할 때 보안 인증 소스를 직접 지정할 수 있습니다.

## 보안 인증 프로그램 경로 지정

설정 값은 SDK 또는 개발 도구가 사용자를 대신하여 실행하는 프로그램의 경로를 포함하는 문자열입니다.

- 경로와 파일 이름은 A~Z, a~z, 0~9, 하이픈(-), 밑줄(\_), 마침표(.), 슬래시(/), 백슬래시(\) 및 공백 등의 문자는 다음과 같습니다.
- 경로 또는 파일 이름에 공백이 있으면 전체 경로와 파일 이름을 큰 따옴표(" ")로 묶습니다.
- 파라미터 이름이나 파라미터 값에 공백이 있으면 해당 요소를 큰 따옴표(" ")로 묶습니다. 전체 페어가 아니라 이름 또는 값만 묶으세요.
- 문자열 안에 환경 변수를 포함하지 마십시오. 예를 들어 \$HOME 또는 %USERPROFILE%을 포함할 수 없습니다.
- 홈 폴더를 ~로 지정하지 마십시오. \* 전체 경로 또는 기본 파일 이름을 지정해야 합니다. 기본 파일 이름이 있는 경우, 시스템은 PATH 환경 변수로 지정된 폴더 내에서 프로그램을 찾으려고 시도합니다. 경로는 운영 체제에 따라 다릅니다.

다음 예제는 Linux/macOS의 공유 config 파일에서 credential\_process를 설정하는 방법을 보여줍니다.

```
credential_process = "/path/to/credentials.sh" parameterWithoutSpaces "parameter with spaces"
```

다음 예제는 Windows의 공유 config 파일에서 credential\_process를 설정하는 방법을 보여줍니다.

```
credential_process = "C:\Path\To\credentials.cmd" parameterWithoutSpaces "parameter with spaces"
```

- 전용 프로파일 내에서 지정할 수 있습니다.

```
[profile cred_process]
credential_process = /Users/username/process.sh
region = us-east-1
```

## 보안 인증 프로그램에서 유효한 출력

SDK는 프로파일에 지정된 대로 명령을 실행한 다음, 표준 출력 스트림에서 데이터를 읽습니다. 지정한 명령은 스크립트나 바이너리 프로그램이 STDOUT에서 다음 구문과 일치하는 JSON 출력을 생성해야 하는지 여부를 지정합니다.

```
{
  "Version": 1,
  "AccessKeyId": "an AWS access key",
  "SecretAccessKey": "your AWS secret access key",
  "SessionToken": "the AWS session token for temporary credentials",
  "Expiration": "RFC3339 timestamp for when the credentials expire"
}
```

### Note

이 문서의 작성일 현재, Version 키는 1로 설정되어 있습니다. 구조가 발전하면서 시간에 따라 이 값이 증가할 수 있습니다.

Expiration 키는 RFC3339 형식의 타임스탬프입니다. Expiration 키가 도구의 출력에 존재하지 않으면 SDK는 보안 인증이 새로 고침이 되지 않은 장기 보안 인증이라고 가정합니다. 그렇지 않은 경우 보안 인증은 임시 보안 인증으로 간주되며, 기간이 만료되기 전에 credential\_process 명령을 다시 실행하면 자동으로 새로 고침됩니다.

### Note

SDK는 assume-role 보안 인증을 맡는 방법으로 외부 프로세스 보안 인증을 캐싱하지 않습니다. 캐싱이 필요한 경우에는 외부 프로세스에서 이를 실행해야 합니다.

외부 프로세스는 보안 인증을 검색하는 동안 오류가 발생했음을 나타내기 위해 0이 아닌 반환 코드를 반환할 수 있습니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	예	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	예	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	예	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	

SDK	지원 여부	참고 또는 추가 정보
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## AWS SDKs 및 도구 표준화된 기능

많은 기능이 일관된 기본값을 유지하고 여러 SDK에서 동일한 방식으로 작동하도록 표준화되었습니다. 이러한 일관성은 여러 SDK에서 코딩할 때 생산성과 명확성을 높입니다. 코드에서 모든 설정을 재정의할 수 있습니다. 자세한 내용은 사용자 특정 SDK API를 참조하십시오.

### Important

모든 SDK가 모든 기능을 지원하거나 기능 내의 모든 측면을 지원하는 것은 아닙니다.

### 주제

- [계정 기반 엔드포인트](#)
- [애플리케이션 ID](#)
- [Amazon EC2 인스턴스 메타데이터](#)
- [Amazon S3 액세스 포인트](#)
- [Amazon S3 다중 리전 액세스 포인트](#)
- [S3 Express One Zone 세션 인증](#)
- [인증 체계](#)
- [AWS 리전](#)
- [AWS STS 리전 엔드포인트](#)
- [Amazon S3에 대한 데이터 무결성 보호](#)

- [이중 스택 엔드포인트 및 FIPS 엔드포인트](#)
- [엔드포인트 검색](#)
- [일반 구성 설정](#)
- [호스트 접두사 삽입](#)
- [IMDS 클라이언트](#)
- [재시도 동작](#)
- [요청 압축](#)
- [서비스별 엔드포인트](#)
- [스마트 구성 기본값](#)

## 계정 기반 엔드포인트

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 Support AWS SDKs [이 안내서의 설정 페이지의 이해](#).

계정 기반 엔드포인트는 이 기능을 지원하는 서비스에 대한 요청을 사용자의 AWS 계정 ID를 사용해 라우팅함으로써, 높은 성능과 확장성을 보장하는 데 도움이 됩니다. 계정 기반 엔드포인트를 지원하는 AWS SDK와 서비스를 사용할 경우, SDK 클라이언트는 리전 기반 엔드포인트가 아닌 계정 기반 엔드포인트를 구성하고 사용합니다. SDK 클라이언트에 계정 ID가 표시되지 않는 경우 클라이언트는 리전 엔드포인트를 사용합니다. 계정 기반 엔드포인트는 형식입니다. `https://<account-id>.ddb.<region>.amazonaws.com` 여기서 `<account-id>` 및 `<region>`는 AWS 계정 ID 및 입니다 AWS 리전.

다음을 사용하여 이 기능을 구성하십시오.

**aws\_account\_id** - 공유 AWS config 파일 설정, **AWS\_ACCOUNT\_ID** - 환경 변수, **aws.accountId** - JVM 시스템 속성: Java/Kotlin만 해당

AWS 계정 ID입니다. 계정 기반 엔드포인트 라우팅에 사용됩니다. AWS 계정 ID의 형식은 111122223333입니다.

계정 기반 엔드포인트 라우팅은 일부 서비스에 더 나은 요청 성능을 제공합니다.

**account\_id\_endpoint\_mode** - 공유 AWS **config** 파일 설정,

**AWS\_ACCOUNT\_ID\_ENDPOINT\_MODE** - 환경 변수, **aws.accountIdEndpointMode** - JVM 시스템 속

성: Java/Kotlin만 해당

이 설정은 필요한 경우 계정 기반 엔드포인트 라우팅을 끄고 계정 기반 규칙을 우회하는 데 사용됩니다.

기본값: preferred

유효한 값:

- **preferred** - 엔드포인트에는 사용 가능한 경우 계정 ID가 포함되어야 합니다.
- **disabled** - 확인된 엔드포인트에는 계정 ID가 포함되지 않습니다.
- **required** - 엔드포인트에는 계정 ID가 포함되어야 합니다. 계정 ID를 사용할 수 없는 경우 SDK에서 오류가 발생합니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지원됨	SDK 버전에서 릴리스	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	2.25.0	
<a href="#">AWS CLI v1</a>	예	1.38.0	
<a href="#">SDK for C++</a>	아니요		
<a href="#">SDK for Go V2 (1.x)</a>	예	v1.35.0	
<a href="#">SDK for Go 1.x (V1)</a>	아니요		
<a href="#">SDK for Java 2.x</a>	예	v2.28.4	

SDK	지원됨	SDK 버전에서 릴리스	참고 또는 추가 정보
<a href="#">SDK for Java 1.x</a>	예	v1.12.771	
<a href="#">SDK for JavaScript 3.x</a>	예	v3.656.0	
<a href="#">SDK for JavaScript 2.x</a>	아니요		
<a href="#">SDK for Kotlin</a>	예	v1.3.37	
<a href="#">.NET 4.x용 SDK</a>	예	4.0.0	
<a href="#">SDK for .NET 3.x</a>	아니요		
<a href="#">SDK for PHP 3.x</a>	예	v3.318.0	
<a href="#">SDK for Python (Boto3)</a>	예	1.37.0	
<a href="#">SDK for Ruby 3.x</a>	예	v1.123.0	
<a href="#">SDK for Rust</a>	예	릴리스-2025-04-24	
<a href="#">SDK for Swift</a>	예	1.2.0	
<a href="#">PowerShell V5용 도구</a>	아니요		

SDK	지원됨	SDK 버전에서 릴리스	참고 또는 추가 정보
<a href="#">PowerShell V4용 도구</a>	아니요		

## 애플리케이션 ID

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs이 안내서의 설정 페이지의 이해](#).

여러 고객 애플리케이션에서 단일 사용자 에이전트를 호출할 AWS 계정 수 있습니다 AWS 서비스. 애플리케이션 ID는 고객을 사용하여 호출 세트를 수행한 소스 애플리케이션을 식별할 수 있는 방법을 제공합니다 AWS 계정. AWS SDKs 및 서비스는 이 값을 고객 커뮤니케이션에 다시 표시하는 것 외에는 이 값을 사용하거나 해석하지 않습니다. 예를 들어 이 값을 운영 이메일 또는에 포함하여 알림과 연결된 애플리케이션을 AWS Health Dashboard 고유하게 식별할 수 있습니다.

다음을 사용하여 이 기능을 구성하십시오.

**sdk\_ua\_app\_id** - 공유 AWS **config** 파일 설정, **AWS\_SDK\_UA\_APP\_ID** - 환경 변수,  
**sdk.ua.appId** - JVM 시스템 속성: Java/Kotlin만 해당

이 설정은 특정 내의 어떤 애플리케이션이 AWS 계정 호출하는지 식별하기 위해 애플리케이션에 할당하는 고유한 문자열입니다 AWS.

기본값: None

유효한 값: 최대 길이가 50인 문자열. 문자, 숫자 및 !, ,, #, ,, \$, ,, % &, ' \* + - . , ^ \_ , ` | , 등의 특수 문자가 허용됩니다~.

config 파일에서 이 값을 설정하는 예:

```
[default]
```

```
sdk_ua_app_id=ABCDEF
```

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_SDK_UA_APP_ID=ABCDEF
export AWS_SDK_UA_APP_ID="ABC DEF"
```

명령줄을 통해 환경 변수를 설정하는 Windows 예제:

```
setx AWS_SDK_UA_APP_ID ABCDEF
setx AWS_SDK_UA_APP_ID="ABC DEF"
```

사용 중인 셸에서 특별한 의미를 갖는 기호를 포함하는 경우, 해당 값에 적절한 이스케이프 처리를 해주세요.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 원 되 는 동	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	공유 config 파일은 지원되지 않습니다.
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	아 니 요	
<a href="#">SDK for Java 2.x</a>	부 분 적	공유 config 파일 설정은 지원되지 않으며, 환경 변수도 지원되지 않습니다.

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for Java 1.x</a>	아 니 요	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	아 니 요	
<a href="#">SDK for Kotlin</a>	예	JVM 시스템 속성은 <code>aws.userAgentAppId</code> 입니다.
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## Amazon EC2 인스턴스 메타데이터

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#) [이 안내서의 설정 페이지의 이해](#).

Amazon EC2는 인스턴스 메타데이터 서비스(IMDS)라는 인스턴스 서비스를 제공합니다. 이 서비스에 대한 자세한 내용은 Amazon EC2 사용 설명서의 [인스턴스 메타데이터를 사용한 작업](#)에서 확인하세요. IAM 역할을 사용하여 구성된 Amazon EC2 인스턴스에서 보안 인증을 가져오려면 인스턴스 메타데이터 서비스에 대한 연결을 조정할 수 있습니다.

다음을 사용하여 이 기능을 구성하십시오.

**metadata\_service\_num\_attempts** - 공유 AWS **config** 파일 설정,  
**AWS\_METADATA\_SERVICE\_NUM\_ATTEMPTS** - 환경 변수

이 설정은 인스턴스 메타데이터 서비스에서 데이터 검색을 시도할 때 검색 포기하기 전까지의 총 시도 횟수를 지정합니다.

기본값: 1

유효한 값: 1 보다 크거나 같음.

**metadata\_service\_timeout** - 공유 AWS **config** 파일 설정,  
**AWS\_METADATA\_SERVICE\_TIMEOUT** - 환경 변수

인스턴스 메타데이터 서비스에서 데이터 검색을 시도할 때 제한 시간 도달까지 걸리는 시간(초)을 지정합니다.

기본값: 1

유효한 값: 1 보다 크거나 같음.

config파일에서 이러한 값을 설정하는 예:

```
[default]
metadata_service_num_attempts=10
```

```
metadata_service_timeout=10
```

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_METADATA_SERVICE_NUM_ATTEMPTS=10
export AWS_METADATA_SERVICE_TIMEOUT=10
```

명령줄을 통해 환경 변수를 설정하는 Windows 예제:

```
setx AWS_METADATA_SERVICE_NUM_ATTEMPTS 10
setx AWS_METADATA_SERVICE_TIMEOUT 10
```

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 원 된	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	아 니 요	
<a href="#">SDK for Go V2 (1.x)</a>	아 니 요	
<a href="#">SDK for Go 1.x (V1)</a>	아 니 요	
<a href="#">SDK for Java 2.x</a>	부 편 적	AWS_METADATA_SERVICE_TIMEOUT 만 지원됩니다.

SDK	지 원 된	참고 또는 추가 정보
<a href="#">SDK for Java 1.x</a>	부 편 적	AWS_METADATA_SERVICE_TIMEOUT 만 지원됩니다.
<a href="#">SDK for JavaScript 3.x</a>	아 니 요	
<a href="#">SDK for JavaScript 2.x</a>	아 니 요	
<a href="#">SDK for Kotlin</a>	아 니 요	
<a href="#">.NET 4.x용 SDK</a>	아 니 요	
<a href="#">SDK for .NET 3.x</a>	아 니 요	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	아 니 요	
<a href="#">SDK for Rust</a>	아 니 요	

SDK	지원 통	참고 또는 추가 정보
<a href="#">SDK for Swift</a>	아 니 요	
<a href="#">PowerShell V5용 도구</a>	아 니 요	
<a href="#">PowerShell V4용 도구</a>	아 니 요	

## Amazon S3 액세스 포인트

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 Support AWS SDKs [이 안내서의 설정 페이지의 이해](#).

Amazon S3 서비스는 Amazon S3 버킷과의 상호 작용 대체 방법으로 액세스 포인트를 제공합니다. 액세스 포인트는 버킷에 직접 적용되지 않고 S3 버킷에 고유한 정책 및 구성을 적용할 수 있습니다. AWS SDKs 사용하면 버킷 이름을 명시적으로 지정하는 대신 API 작업에 버킷 필드의 액세스 포인트 Amazon 리소스 이름(ARNs)을 사용할 수 있습니다. 액세스 포인트 ARN과 [GetObject](#) 을 사용하여 버킷에서 객체를 가져오거나, 액세스 포인트 ARN과 [PutObject](#) 을 사용하여 버킷에 객체를 추가하는 등의 특정 작업에 이 방법을 사용합니다.

Amazon S3 액세스 포인트 및 ARN에 대한 자세한 내용은 Amazon S3 사용 설명서의 [액세스 포인트 사용](#)을 참조하십시오.

다음을 사용하여 이 기능을 구성하십시오.

**s3\_use\_arn\_region** - 공유 AWS **config** 파일 설정, **AWS\_S3\_USE\_ARN\_REGION** - 환경 변수, **aws.s3UseArnRegion** - JVM 시스템 속성: Java/Kotlin만 해당, 코드에서 값을 직접 구성하려면 특정 SDK를 직접 참조하십시오.

이 설정은 SDK가 액세스 포인트 ARN을 사용하여 요청에 대한 리전 엔드포인트를 AWS 리전 구성할지 여부를 제어합니다. SDK는 ARN AWS 리전 이 가장 실패할 가능성이 높은 교차 AWS 파티션 호출을 방지 AWS 리전 하도록 구성된 클라이언트의와 동일한 파티션에서 제공되는지 확인합니다. 다중 정의의 경우 코드로 구성된 설정이 우선 적용되고 환경 변수 설정이 그 뒤를 따릅니다.

기본값: `false`

유효한 값:

- **true** - SDK는 클라이언트가 구성한 대신 엔드포인트를 구성할 AWS 리전 때 ARN을 사용합니다 AWS 리전. 예외: 클라이언트의 구성 AWS 리전 이 FIPS인 AWS 리전 경우 ARN의와 일치해야 합니다 AWS 리전. 이렇게 하지 않으면 오류가 발생합니다.
- **false**— SDK는 엔드포인트를 구성할 클라이언트가 구성한 AWS 리전 을 사용합니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	예	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	예	JVM 시스템 속성은 지원되지 않습니다.

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	예	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	표준 우선순위를 따르지 않습니다. 공유 config 파일 값이 환경 변수보다 우선합니다.
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	아 니 요	
<a href="#">SDK for Swift</a>	아 니 요	
<a href="#">PowerShell V5용 도구</a>	예	표준 우선순위를 따르지 않습니다. 공유 config 파일 값이 환경 변수보다 우선합니다.
<a href="#">PowerShell V4용 도구</a>	예	표준 우선순위를 따르지 않습니다. 공유 config 파일 값이 환경 변수보다 우선합니다.

## Amazon S3 다중 리전 액세스 포인트

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs 이 안내서의 설정 페이지의 이해](#).

Amazon S3 다중 리전 액세스 포인트는 애플리케이션이 여러 AWS 리전리전에 있는 Amazon S3 버킷의 요청을 이행하는 데 사용할 수 있는 글로벌 엔드포인트를 제공합니다. 다중 리전 액세스 포인트를 사용하여 단일 리전에서 사용되는 것과 동일한 아키텍처로 다중 리전 애플리케이션을 구축하면 전 세계 어디에서나 해당 애플리케이션을 실행할 수 있습니다.

다중 리전 액세스 포인트에 대한 자세한 내용을 알아보려면 Amazon S3 사용 설명서의 [Amazon S3의 다중 리전 액세스 포인트](#)를 참조하십시오.

다중 리전 액세스 포인트 Amazon 리소스 이름(ARN)에 대한 자세한 내용을 알아보려면 Amazon S3 사용 설명서의 [다중 리전 액세스 포인트를 사용하여 요청 생성하기](#)를 참조하십시오.

다중 리전 액세스 포인트 생성에 대한 자세한 내용을 알아보려면 Amazon S3 사용 설명서의 [Amazon S3의 다중 리전 액세스 포인트 관리](#)를 참조하십시오.

SigV4A 알고리즘은 글로벌 리전 요청에 서명하는 데 사용되는 서명 구현입니다. 이 알고리즘은 [AWS 공통 런타임\(CRT\) 라이브러리](#)에 대한 종속성을 통해 SDK로 획득됩니다.

다음을 사용하여 이 기능을 구성하십시오.

**s3\_disable\_multiregion\_access\_points** - 공유 AWS config 파일 설정, **AWS\_S3\_DISABLE\_MULTIREGION\_ACCESS\_POINTS** - 환경 변수, **aws.s3DisableMultiRegionAccessPoints** - JVM 시스템 속성: Java/Kotlin만 해당, 코드에서 값을 직접 구성하려면 특정 SDK를 직접 참조하십시오.

이 설정은 SDK가 잠재적으로 리전 간 요청을 시도할지 여부를 제어합니다. 다중 정의의 경우 코드로 구성된 설정이 우선 적용되고 환경 변수 설정이 그 뒤를 따릅니다.

기본값: false

유효값:

- **true**— 리전 간 요청 사용을 중지합니다.

- **false**— 다중 리전 액세스 포인트를 사용하여 리전 간 요청을 활성화합니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 통	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	아 니 요	
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	아 니 요	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	아 니 요	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	아 니 요	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## S3 Express One Zone 세션 인증

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs이 안내서의 설정 페이지의 이해](#).

S3 Express One Zone은 자주 액세스되는 데이터에 대해 한 자릿수 밀리초 지연 시간을 제공하는 Amazon S3의 고성능 스토리지 클래스입니다. S3 Express One Zone 버킷을 사용하는 경우 AWS SDKs 및 도구는 데이터 요청의 지연 시간이 짧은 권한 부여에 최적화된 세션 기반 인증을 자동으로 사용합니다. 세션 내 여러 요청에 인증 지연을 분산시키기 위해 영역(오브젝트 단위) 작업에서는 세션 토큰을 사용합니다. 이를 통해 인증 오버헤드를 줄이고 전체 요청 성능을 향상시킬 수 있습니다.

S3 Express One Zone 버킷은 bucket-name--usw2-az1--x-s3와 같은 가용 영역 ID를 포함하는 특정한 이름 형식을 사용합니다. SDK가 이러한 이름 패턴을 감지하면, 해당 S3 Express One Zone 엔드포인트로 요청을 자동으로 라우팅하고 최적화된 인증 흐름을 적용합니다. 세션 인증은 버킷 전용의 임시 자격 증명을 생성하여 버킷에 저지연으로 액세스할 수 있도록 하며, 이러한 자격 증명은 SDK에 의해 자동으로 캐시되고 갱신됩니다. 자세한 내용은 Amazon S3 사용 설명서의 [S3 Express One Zone](#)을 참조하세요.

기본적으로 세션 인증은 S3 Express One Zone 버킷에 대해 활성화됩니다.

다음을 사용하여 이 기능을 구성하십시오.

**s3\_disable\_express\_session\_auth** - 공유 AWS **config** 파일 설정,  
**AWS\_S3\_DISABLE\_EXPRESS\_SESSION\_AUTH** - 환경 변수, **aws.disableS3ExpressAuth** - JVM  
 시스템 속성: Java/Kotlin만 해당

S3 Express One Zone 세션 인증을 비활성화할지 여부를 제어합니다. `true`로 설정하면, SDK는 세션 인증 대신 S3 Express One Zone 버킷에 대해 표준 SigV4 인증을 사용합니다.

기본값: `false`

유효한 값:

- **true** - S3 Express One Zone 세션 인증을 비활성화합니다.
- **false** - S3 Express One Zone 세션 인증을 활성화합니다.

config 파일에서 이 값을 설정하는 예:

```
[default]
s3_disable_express_session_auth=true
```

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_S3_DISABLE_EXPRESS_SESSION_AUTH=true
```

명령줄을 통해 환경 변수를 설정하는 Windows 예제:

```
setx AWS_S3_DISABLE_EXPRESS_SESSION_AUTH true
```

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지원됨	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">AWS CLI v1</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	아니요	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	아니요	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	아니요	
<a href="#">SDK for Kotlin</a>	예	JVM 시스템 속성은 <code>aws.s3DisableExpressSessionAuth</code> 입니다.
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	

SDK	지원됨	참고 또는 추가 정보
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## 인증 체계

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs이 안내서의 설정 페이지의 이해](#).

AWS 서비스는 AWS 서명 버전 4(SigV4) 및 AWS 서명 버전 4a(SigV4a)와 같은 여러 인증 체계를 지원합니다. 기본적으로 SDK는 서비스 모델 정의를 기반으로 인증 체계를 선택하며, 가장 뛰어난 호환성을 제공하는 체계를 우선합니다. 그러나 특정 요구 사항에 맞춰 최적화할 수 있도록 선호하는 인증 체계를 직접 구성할 수도 있습니다.

SigV4과 달리, SigV4a로 서명된 요청은 여러 AWS 리전에서 유효합니다. SigV4a는 크로스 리전 요청 서명을 지원하여 가용성을 강화합니다. 이를 통해 특정 리전에 장애가 발생하더라도 백업 리전으로 자동 장애 조치가 가능해집니다. 이는 AWS Identity and Access Management 또는 Amazon CloudFront와 같은 글로벌 서비스에 특히 유용합니다.

이 두 인증 체계에 대한 자세한 내용은 IAM 사용 설명서의 [API 요청용AWS Signature Version 4](#)에서 확인하세요.

다음을 사용하여 이 기능을 구성하십시오.

**auth\_scheme\_preference** - 공유 AWS **config** 파일 설정, **AWS\_AUTH\_SCHEME\_PREFERENCE** - 환경 변수, **aws.authSchemePreference** - JVM 시스템 속성: Java/Kotlin만 해당

우선순위에 따라 쉼표로 구분된 선호 인증 체계 목록을 지정합니다. 서비스가 여러 인증 체계를 지원하는 경우, SDK는 이 목록에 지정된 순서대로 인증 방식을 사용하려 시도하며, 선호 체계가 모두 사용 불가능한 경우 기본 동작으로 되돌아갑니다.

기본값: 없음.

유효한 값: 다음 항목 중 하나 이상을 쉼표로 구분한 목록입니다.

- **sigv4** - Signature Version 4(가장 빠른 성능, 단일 리전)
- **sigv4a** - Signature Version 4a(가용성 강화, 크로스 리전 지원, SigV4보다 서명 성능이 더 느림)
- **httpBearerAuth** - HTTP 베어러 토큰 인증

스킵 이름 사이의 공백 및 탭 문자는 무시됩니다.

config 파일에서 이 값을 설정하여 SigV4a를 우선하도록 구성하는 예:

```
[default]
auth_scheme_preference=sigv4a,sigv4
```

**sigv4a\_signing\_region\_set** - 공유 AWS **config** 파일 설정, **AWS\_SIGV4A\_SIGNING\_REGION\_SET** - 환경 변수

SigV4a 다중 리전 서명을 AWS 리전 위한 쉼표로 구분된 목록을 지정합니다. SigV4a가 선택된 인증 체계인 경우, 이는 요청에 설정되는 기본 리전 값으로 사용됩니다.

기본값: 요청에 의해 결정됩니다.

유효한 값: AWS 리전을 쉼표로 구분한 목록입니다. 리전 사이의 공백 및 탭 문자는 무시됩니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 통	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	아 니 요	
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	아 니 요	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	아 니 요	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	아 니 요	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	아 니 요	

## AWS 리전

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#)이 [안내서의 설정 페이지의 이해](#).

AWS 리전은 작업 시 이해해야 할 중요한 개념입니다 AWS 서비스.

를 사용하면 특정 지리적 영역에 물리적으로 상주 AWS 서비스 하는에 액세스할 AWS 리전수 있습니다. 이는 데이터와 애플리케이션이 귀사 및 귀사의 사용자가 액세스하기 가까운 곳에서 계속 실행되도록 하는 데 도움이 될 수 있습니다. 리전에서는 내결함성, 안정성 및 복원성을 지원하고 지연 시간을 줄일 수도 있습니다. 리전을 통해 사용자는 가용 상태를 유지하며 리전 중단에 영향을 받지 않는 중복 리소스를 생성할 수 있습니다.

대부분의 AWS 서비스 요청은 특정 지리적 리전과 연결됩니다. 한 리전에서 생성한 리소스는 AWS 서비스서비스에서 제공하는 복제 기능을 명시적으로 사용하지 않는 한 다른 리전에 존재하지 않습니다. 예를 들어, Amazon S3와 Amazon EC2 크로스 리전 복제를 지원합니다. IAM과 같은 일부 서비스의 경우 리전 리소스가 없습니다.

AWS 일반 참조에는 다음 정보가 포함됩니다.

- 리전과 엔드포인트 간의 관계를 이해하고 기존 리전 엔드포인트 목록을 보려면 [AWS 서비스 엔드포인트](#)를 참조하십시오.

- 각각의 AWS 서비스에 대해 지원되는 모든 리전 및 엔드포인트의 현재 목록을 보려면 [서비스 엔드포인트 및 할당량](#)을 참조하십시오.

## 서비스 클라이언트 생성

프로그래밍 방식으로 액세스하기 위해 AWS 서비스 SDKs 각에 대해 클라이언트 클래스/객체를 사용합니다 AWS 서비스. 예를 들어 애플리케이션에서 Amazon EC2에 액세스해야 하는 경우 애플리케이션은 Amazon EC2 클라이언트 객체를 생성하여 해당 서비스와 인터페이스합니다.

코드에서 클라이언트에 대해 리전이 명시적으로 지정되지 않은 경우, 클라이언트는 다음 region 설정을 통해 지정된 리전을 기본값으로 사용합니다. 하지만 개별 클라이언트 객체에 대해 클라이언트의 활성 리전을 명시적으로 설정할 수 있습니다. 이러한 방식으로 리전을 설정하면 특별한 서비스 클라이언트에 대한 전역 설정에 우선합니다. 대체 리전은 해당 클라이언트를 인스턴스화하는 동안 SDK에 따라 지정됩니다(특정 SDK 가이드 또는 SDK의 코드 베이스 확인).

다음을 사용하여 이 기능을 구성하십시오.

**region** - 공유 AWS config 파일 설정, **AWS\_REGION** - 환경 변수, **aws.region** - JVM 시스템 속성: Java/Kotlin만 해당

AWS 요청에 사용할 기본 AWS 리전 값을 지정합니다. 이 리전은 사용할 특정 지역과 함께 제공되지 않은 SDK 서비스 요청에 사용됩니다.

기본값: 없음. 이 값을 명시적으로 지정해야 합니다.

유효값:

- AWS 일반 참조의 [AWS 서비스 엔드포인트](#)에 나열된 대로 선택한 서비스에서 사용할 수 있는 모든 리전 코드. 예를 들어, us-east-1 값은 엔드포인트를 AWS 리전 미국 동부(버지니아 북부)로 설정합니다.
- aws-global은 AWS Security Token Service (AWS STS) 및 Amazon Simple Storage Service(Amazon S3)와 같은 리전 엔드포인트 외에도 별도의 글로벌 엔드포인트를 지원하는 서비스에 대한 글로벌 엔드포인트를 지정합니다.

config 파일에서 이 값을 설정하는 예:

```
[default]
region = us-west-2
```

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_REGION=us-west-2
```

명령줄을 통해 환경 변수를 설정하는 Windows 예제:

```
setx AWS_REGION us-west-2
```

대부분의 SDK에는 애플리케이션 코드 내에서 기본 리전을 설정하는 데 사용할 수 있는 “구성” 객체가 있습니다. 자세한 내용은 특정 AWS SDK 개발자 안내서를 참조하세요.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	AWS CLI v2는의 값의 값AWS_REGION 보다 먼저 사용합니 다AWS_DEFAULT_REGION (두 변수 모두 확인됨).
<a href="#">AWS CLI v1</a>	예	AWS CLI v1은이 용도로 AWS_DEFAULT_REGION 라는 환경 변수를 사용합니다.
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	예	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	예	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	이 SDK는 이러한 용도로 명명된 <code>AWS_DEFAULT_REGION</code> 환경 변수를 사용합니다. 환
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## AWS STS 리전 엔드포인트

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 Support AWS SDKs [이 안내서의 설정 페이지의 이해](#).

AWS Security Token Service (AWS STS)는 글로벌 및 리전 서비스로 사용할 수 있습니다. 일부 AWS SDKs 및 CLIs 기본적으로 글로벌 서비스 엔드포인트(`https://sts.amazonaws.com`)를 사용하는 반면, 일부는 리전 서비스 엔드포인트(`https://sts.{region_identifier}.{partition_domain}`)를 사용합니다. [기본적으로 활성화된](#) 리전에서 AWS STS 글로벌 엔드포인트에 대한 요청은 요청이 시작된 리전과 동일한 리전에서 자동으로 처리됩니다. 옵트인 리전에서 AWS STS 글로벌 엔드포인트에 대한 요청은 단일 AWS 리전(미국 동부(버지니아 북부)에

서 처리됩니다. AWS STS 엔드포인트에 대한 자세한 내용은 AWS Security Token Service API 참조의 [엔드포인트](#) 또는 AWS Identity and Access Management 사용 설명서의 [AWS STS의 관리를 AWS 리전](#) 참조하세요.

가능하면 리전 엔드포인트를 사용하고를 구성하는 것이 AWS 가장 좋습니다 [AWS 리전](#). 상용 이외의 [파티션](#)에 속하는 고객은 반드시 리전 엔드포인트를 사용해야 합니다. 모든 SDK와 도구가 이 설정을 지원하는 것은 아니지만, 글로벌 및 리전 엔드포인트에 대해서는 모두 정의된 동작을 가지고 있습니다. 자세한 내용은 다음 섹션을 참조하세요.

#### Note

AWS는 복원력과 성능을 향상시키기 위해 [기본적으로 활성화된](#) 리전의 AWS Security Token Service (AWS STS) 글로벌 엔드포인트(<https://sts.amazonaws.com>)를 변경했습니다. 글로벌 엔드포인트에 대한 AWS STS 요청은 워크로드 AWS 리전과 동일한에서 자동으로 제공됩니다. 이러한 변경 사항은 옵트인 리전에 배포되지 않습니다. 적절한 AWS STS 리전 엔드포인트를 사용하는 것이 좋습니다. 자세한 내용은 AWS Identity and Access Management 사용 설명서의 [AWS STS 글로벌 엔드포인트 변경 사항](#)을 참조하세요.

이 설정을 지원하는 SDK와 도구의 경우, 고객은 다음 방법을 통해 해당 기능을 구성할 수 있습니다.

**sts\_regional\_endpoints** - 공유 AWS config 파일 설정, **AWS\_STS\_REGIONAL\_ENDPOINTS** - 환경 변수

이 설정은 SDK 또는 도구가 AWS Security Token Service ()와 통신하는 데 사용하는 엔드포인트를 결정하는 AWS 서비스 방법을 지정합니다 AWS STS.

기본값: `regional`, 다음 표의 예외를 참조하세요.

#### Note

2022년 7월 이후에 출시되는 모든 새 SDK 메이저 버전은 `regional`으로 기본값이 설정됩니다. 새 SDK 메이저 버전에서는 `regional` 동작을 사용하여 이 설정을 없앨 수 있습니다. 이 변경으로 인한 향후 영향을 줄이려면 가능하면 사용자 애플리케이션에서 `regional`을 사용하여 시작하는 것이 좋습니다.

유효한 값: (권장 값: `regional`)

- **legacy** - 글로벌 AWS STS 엔드포인트를 사용합니다 `sts.amazonaws.com`.
- **regional** - SDK 또는 도구는 항상 현재 구성된 리전의 AWS STS 엔드포인트를 사용합니다. 예를 들어 클라이언트가 사용하도록 구성된 경우 `us-west-2`에 대한 모든 호출 AWS STS 은 글로벌 엔드포인트 `sts.us-west-2.amazonaws.com` 대신 리전 `sts.amazonaws.com` 엔드포인트에 이루어집니다. 이 설정이 활성화된 상태에서 글로벌 엔드포인트에 요청을 보내려면 리전을 `aws-global`로 설정하면 됩니다.

config 파일에서 이러한 값을 설정하는 예:

```
[default]
sts_regional_endpoints = regional
```

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_STS_REGIONAL_ENDPOINTS=regional
```

명령줄을 통해 환경 변수를 설정하는 Windows 예제:

```
setx AWS_STS_REGIONAL_ENDPOINTS regional
```

## AWS SDKs 도구 지원

### Note

가능하면 리전 엔드포인트를 사용하고를 구성하는 것이 AWS 가장 좋습니다 [AWS 리전](#).

다음 표는 SDK 또는 도구에 대한 요약을 제공합니다.

- 지원 설정: STS 리전 엔드포인트를 위한 공유 config 파일 변수와 환경 변수가 지원되는지 여부.
- 기본 설정 값: 해당 설정이 지원되는 경우의 기본값.
- 기본 서비스 클라이언트 대상 STS 엔드포인트: 해당 설정을 변경할 수 없는 경우에도 클라이언트가 기본적으로 사용하는 엔드포인트.
- 서비스 클라이언트 폴백 동작: SDK가 리전 엔드포인트를 사용해야 하지만 리전이 구성되어 있지 않을 때 수행하는 동작. 이는 기본값에 따라 리전 엔드포인트를 사용하는 경우든, 설정을 통해 `regional`이 선택된 경우든 동일하게 적용되는 동작입니다.

또한, 표에서는 다음과 같은 값을 사용합니다.

- 글로벌 엔드포인트: <https://sts.amazonaws.com>.
- 리전 엔드포인트: 애플리케이션에서 사용하는 구성된 [AWS 리전](#)을 기반으로 합니다.
- **us-east-1**(리전): us-east-1 리전 엔드포인트를 사용하지만, 일반적인 글로벌 요청보다 더 긴 세션 토큰과 함께 사용합니다.

SDK	기본 설정 값	기본 서비스 클라이언트 대상 STS 엔드포인트	서비스 클라이언트 폴백 동작	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	이 해당 사항 없음	리전 엔드포인트	글로벌 엔드포인트	
<a href="#">AWS CLI v1</a>	legacy	글로벌 엔드포인트	글로벌 엔드포인트	
<a href="#">SDK for C++</a>	이 해당 사항 없음	리전 엔드포인트	us-east-1 (리전)	
<a href="#">SDK for Go V2 (1.x)</a>	이 해당 사항 없음	리전 엔드포인트	요청 실패	
<a href="#">SDK for Go 1.x (V1)</a>	legacy	글로벌 엔드포인트	글로벌 엔드포인트	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	이 해당 사항 없음	리전 엔드포인트	요청 실패	리전이 구성되지 않은 경우 AssumeRole 및 AssumeRoleWithWebIdentity 는 글로벌 STS 엔드포인트를 사용합니다.

SDK	기본 설정 값	기본 서비스 클라이언트 대상 STS 엔드포인트	서비스 클라이언트 폴백 동작	참고 또는 추가 정보
<a href="#">SDK for Java 1.x</a>	0: legacy	글로벌 엔드포인트	글로벌 엔드포인트	
<a href="#">SDK for JavaScript 3.x</a>	이 해당 사항 없음	리전 엔드포인트	us-east-1 (리전)	
<a href="#">SDK for JavaScript 2.x</a>	0: legacy	글로벌 엔드포인트	글로벌 엔드포인트	
<a href="#">SDK for Kotlin</a>	이 해당 사항 없음	리전 엔드포인트	글로벌 엔드포인트	
<a href="#">.NET 4.x용 SDK</a>	이 해당 사항 없음	리전 엔드포인트	us-east-1 (리전)	
<a href="#">SDK for .NET 3.x</a>	0: regional	글로벌 엔드포인트	글로벌 엔드포인트	
<a href="#">SDK for PHP 3.x</a>	0: regional	글로벌 엔드포인트	요청 실패	
<a href="#">SDK for Python (Boto3)</a>	0: regional	글로벌 엔드포인트	글로벌 엔드포인트	
<a href="#">SDK for Ruby 3.x</a>	0: regional	리전 엔드포인트	요청 실패	

SDK	기본 설정 값	기본 서비스 클라이언트 대상 STS 엔드포인트	서비스 클라이언트 폴백 동작	참고 또는 추가 정보
<a href="#">SDK for Rust</a>	이 해당 사항 없음	리전 엔드포인트	요청 실패	
<a href="#">SDK for Swift</a>	이 해당 사항 없음	리전 엔드포인트	요청 실패	
<a href="#">PowerShell V5용 도구</a>	0: regional	글로벌 엔드포인트	글로벌 엔드포인트	
<a href="#">PowerShell V4용 도구</a>	0: regional	글로벌 엔드포인트	글로벌 엔드포인트	

## Amazon S3에 대한 데이터 무결성 보호

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs이 안내서의 설정 페이지의 이해](#).

일정 기간 동안 AWS SDKs는 Amazon Simple Storage Service에 데이터를 업로드하거나 Amazon Simple Storage Service에서 데이터를 다운로드할 때 데이터 무결성 검사를 지원했습니다. 이전에는 이러한 검사들이 선택적으로만 활성화되었습니다. 이제 CRC32나 CRC64NVME와 같은 CRC 기반 알고리즘을 사용해, 이러한 검사들이 기본적으로 활성화되도록 했습니다. 각 SDK나 도구에는 기본 알고리즘이 정해져 있지만, 다른 알고리즘을 선택해 사용할 수도 있습니다. 원한다면 업로드 시 미리 계산해둔 체크섬을 계속해서 직접 제공할 수도 있습니다. 업로드, 멀티파트 업로드, 다운로드, 암호화 모드 전반에 걸쳐 일관된 동작을 제공함으로써 클라이언트 측 무결성 검사가 더욱 단순해집니다.

최신 버전의 AWS SDKs 및는 각 업로드에 대한 [순환 중복 검사\(CRC\) 기반 체크섬](#)을 AWS CLI 자동으로 계산하여 Amazon S3로 전송합니다. Amazon S3는 서버 측에서 독립적으로 체크섬을 계산한 뒤, 제

공된 값과 비교해 검증한 후에야 객체와 해당 체크섬을 안정적으로 저장하고 객체 메타데이터에 기록합니다. 체크섬을 객체와 함께 메타데이터에 저장해 두면, 객체를 다운로드할 때 동일한 체크섬이 자동으로 반환되어 다운로드 검증에도 사용할 수 있습니다. 또한 객체 메타데이터에 저장된 체크섬은 언제든지 검증할 수 있습니다.

체크섬 작업, 멀티파트 업로드, 지원되는 체크섬 알고리즘 목록에 대해 더 알아보려면 Amazon Simple Storage Service 사용 설명서의 [Amazon S3에서 객체 무결성 확인](#)을 참고하세요.

멀티파트 업로드:

Amazon S3는 단일 파트 업로드와 멀티파트 업로드 모두에서 일관된 전체 객체 체크섬을 개발자에게 제공합니다.

파일을 여러 파트로 업로드할 때, SDK는 각 파트에 대한 체크섬을 계산합니다. Amazon S3는 이러한 체크섬을 사용하여 UploadPart API를 통해 각 파트의 무결성을 검증합니다. 또한 Amazon S3는 CompleteMultipartUpload API를 직접 호출할 때 전체 파일의 크기와 체크섬도 검증합니다.

SDK에 멀티파트 업로드를 지원하는 Amazon S3 Transfer Manager가 있는 경우, 파트별 체크섬은 [AWS SDKs 도구 지원](#) 표에 있는 SDK별 기본 알고리즘을 사용하여 검증됩니다. checksum\_type을 FULL\_OBJECT로 설정하거나 CRC64NVME 알고리즘 사용을 선택해 전체 객체 체크섬을 선택적으로 활성화할 수 있습니다.

이전 버전의 SDK나 AWS CLI를 사용 중인 경우:

애플리케이션이 2024년 12월 이전 버전의 SDK나 도구를 사용하고 있는 경우에도, Amazon S3는 신규 객체에 대해 여전히 CRC64NVME 체크섬을 컴퓨팅하고 이를 객체 메타데이터에 저장하여 이후에 참고할 수 있도록 합니다. 나중에 사용자 측에서 컴퓨팅한 CRC 값과 저장된 CRC 값을 비교해 네트워크 전송이 올바르게 이루어졌는지 검증할 수 있습니다. 또한 기존 방식대로, [PutObject](#) 또는 [UploadPart](#) 요청에 직접 미리 컴퓨팅한 체크섬을 제공해 무결성 보호를 수동으로 확장할 수도 있습니다. 이는 이전 버전에서 이를 처리하는 표준적인 방법입니다.

다음을 사용하여 이 기능을 구성하십시오.

**request\_checksum\_calculation** - 공유 AWS config 파일 설정,  
**AWS\_REQUEST\_CHECKSUM\_CALCULATION** - 환경 변수, **aws.requestChecksumCalculation** - JVM 시스템 속성: Java/Kotlin만 해당

기본적으로 요청을 보낼 때 요청 체크섬을 계산하는 기능이 자동으로 활성화되어 있습니다. 사용자는 요청을 구성할 때 [제공되는 체크섬 알고리즘](#) 중 원하는 것을 선택해 사용할 수 있습니다. 그러지

않으면 SDK별 기본 알고리즘이 사용됩니다. 각 SDK 또는 도구의 기본 알고리즘은 [AWS SDKs 도구 지원](#) 표를 참고하세요.

기본값: WHEN\_SUPPORTED

유효한 값:

- **WHEN\_SUPPORTED** - Amazon S3로의 데이터 전송처럼 API 작업에서 지원되는 경우, 모든 요청 페이로드에 대해 체크섬 검증이 수행됩니다.
- **WHEN\_REQUIRED** - 체크섬 검증은 API 작업에 필요한 경우에만 수행됩니다.

**response\_checksum\_validation** - 공유 AWS config 파일 설정,

**AWS\_RESPONSE\_CHECKSUM\_VALIDATION** - 환경 변수, **aws.responseChecksumValidation** - JVM 시스템 속성: Java/Kotlin만 해당

기본적으로, 요청을 보낼 때 응답 체크섬 검증도 자동으로 활성화됩니다. 응답 페이로드에 대해 체크섬이 계산되며, 이를 응답 헤더에 포함된 체크섬 값과 비교합니다. 체크섬 검증에 실패하면, 페이로드를 읽는 시점에 사용자에게 오류가 발생합니다.

체크섬 응답 헤더는 체크섬의 알고리즘도 나타냅니다. Amazon S3 클라이언트는 체크섬을 지원하는 모든 Amazon S3 API 작업에 대해 응답 체크섬을 검증하려고 시도합니다. 그러나 SDK가 지정된 체크섬 알고리즘을 구현하지 않은 경우, 해당 검증은 건너뛰게 됩니다.

기본값: WHEN\_SUPPORTED

유효한 값:

- **WHEN\_SUPPORTED** - Amazon S3로의 데이터 전송처럼 API 작업에서 지원되는 경우, 모든 응답 페이로드에 대해 체크섬 검증이 수행됩니다.
- **WHEN\_REQUIRED** - 체크섬 검증은 API 작업이 이를 지원하고, 직접 호출자가 해당 작업에 대해 체크섬을 명시적으로 활성화한 경우에만 수행됩니다. Amazon S3 GetObject API가 직접 호출되고 ChecksumMode 매개변수가 활성화된 상태로 설정된 경우를 예로 들 수 있습니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

**Note**

아래 표에서 'CRT'는 [AWS 공통 런타임\(CRT\) 라이브러리](#)를 의미하며, 프로젝트에 추가 종속성을 포함해야 할 수도 있습니다.

SDK	지원됨	기본 체크섬 알고리즘	지원되는 체크섬 알고리즘	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	CRC64NVME	CRC64NVME, CRC32, CRC32C, SHA1, SHA256	AWS CLI v1의 경우 기본 알고리즘과 지원되는 알고리즘은 Python(Boto3)과 동일합니다.
<a href="#">SDK for C++</a>	예	CRC64NVME	CRC64NVME, CRC32, CRC32C, SHA1, SHA256	
<a href="#">SDK for Go V2 (1.x)</a>	예	CRC32	CRC64NVME, CRC32, CRC32C, SHA1, SHA256	
<a href="#">SDK for Go 1.x (V1)</a>	아니요			
<a href="#">SDK for Java 2.x</a>	예	CRC32	CRC64NVME(CRT를 통해서만 지원), CRC32, CRC32C, SHA1, SHA256	
<a href="#">SDK for Java 1.x</a>	아니요			
<a href="#">SDK for JavaScript 3.x</a>	예	CRC32	CRC32, CRC32C, SHA1, SHA256	

SDK	지원 됨	기본 체크섬 알고리즘	지원되는 체크섬 알고리즘	참고 또는 추가 정보
<a href="#">SDK for JavaScript 2.x</a>	아 니 요			
<a href="#">SDK for Kotlin</a>	예	CRC32	CRC32, CRC32C, SHA1, SHA256	
<a href="#">.NET 4.x용 SDK</a>	예	CRC32	CRC32, CRC32C, SHA1, SHA256	
<a href="#">SDK for .NET 3.x</a>	예	CRC32	CRC32, CRC32C, SHA1, SHA256	
<a href="#">SDK for PHP 3.x</a>	예	CRC32	CRC32, CRC32C(CRT를 통해서만 지원), SHA1, SHA256	CRC32C를 사용하려면 awscrt 확장이 필요합니다.
<a href="#">SDK for Python (Boto3)</a>	예	CRC32	CRC64NVME(CRT를 통해서만 지원), CRC32, CRC32C(CRT를 통해서만 지원), SHA1, SHA256	
<a href="#">SDK for Ruby 3.x</a>	예	CRC32	CRC64NVME(CRT를 통해서만 지원), CRC32, CRC32C(CRT를 통해서만 지원), SHA1, SHA256	
<a href="#">SDK for Rust</a>	예	CRC32	CRC64NVME, CRC32, CRC32C, SHA1, SHA256	

SDK	지원됨	기본 체크섬 알고리즘	지원되는 체크섬 알고리즘	참고 또는 추가 정보
<a href="#">SDK for Swift</a>	예	CRC32	CRC64NVME, CRC32, CRC32C, SHA1, SHA256	모든 알고리즘에 필요한 CRT 종속성입니다.
<a href="#">PowerShell V5 용 도구</a>	예	CRC32	CRC32, CRC32C, SHA1, SHA256	
<a href="#">PowerShell V4 용 도구</a>	예	CRC32	CRC32, CRC32C, SHA1, SHA256	

## 이중 스택 엔드포인트 및 FIPS 엔드포인트

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#)이 안내서의 [설정 페이지의 이해](#).

다음을 사용하여 이 기능을 구성하십시오.

**use\_dualstack\_endpoint** - 공유 AWS config 파일 설정, **AWS\_USE\_DUALSTACK\_ENDPOINT** - 환경 변수, **aws.useDualstackEndpoint** - JVM 시스템 속성: Java/Kotlin만 해당

SDK에서 듀얼 스택 엔드포인트에 요청을 보낼지 여부를 설정합니다. IPv4 및 IPv6 트래픽을 모두 지원하는 이중 스택 엔드포인트에 대한 자세한 내용은 Amazon 심플 스토리지 서비스 사용 설명서의 [Amazon S3 이중 스택 엔드포인트](#) 사용을 참조하십시오. 이중 스택 엔드포인트는 일부 리전에 사용할 수 있는 서비스입니다.

기본값: `false`

유효한 값:

- **true**— SDK 또는 도구는 이중 스택 엔드포인트를 사용하여 네트워크 요청을 시도합니다. 서비스 및/또는 AWS 리전에 대한 이중 스택 엔드포인트가 없는 경우 요청 오류가 생깁니다.
- **false**— SDK 또는 도구는 듀얼 스택 엔드포인트를 사용하여 네트워크 요청을 하지 않습니다.

**use\_fips\_endpoint** - 공유 AWS **config** 파일 설정, **AWS\_USE\_FIPS\_ENDPOINT** - 환경 변수,  
**aws.useFipsEndpoint** - JVM 시스템 속성: Java/Kotlin만 해당

SDK 또는 도구로 FIPS 호환 엔드포인트로 요청을 보낼지 여부 활성화 혹은 비활성화 합니다. 연방 정보 처리 표준 (FIPS)은 데이터 및 암호화에 대한 미국 정부 보안 요구 사항의 집합입니다. 정부 기관, 파트너 및 연방 정부와 거래하려는 기관은 FIPS 지침을 준수해야 합니다. 표준 AWS 엔드포인트와 달리 FIPS 엔드포인트는 FIPS 140에 대해 검증된 TLS 소프트웨어 라이브러리를 사용합니다. 이 설정이 활성화되어 있고의 서비스에 대한 FIPS 엔드포인트가 없는 경우 AWS 호출 AWS 리전이 실패할 수 있습니다. [서비스별 엔드포인트](#) 및 `--endpoint-url` 옵션은 이 설정을 AWS Command Line Interface 재정의합니다.

FIPS 엔드포인트를 지정하는 다른 방법에 대한 자세한 내용은 서비스별 FIPS 엔드포인트를 AWS 리전참조하세요. <https://aws.amazon.com/compliance/fips/> Amazon Elastic Compute Cloud 서비스 엔드포인트에 대한 자세한 내용은 Amazon EC2 API 참조의 [이중 스택\(IPv4 및 IPv6\) 엔드포인트](#)를 참조하십시오.

기본값: `false`

유효값:

- **true**— SDK 또는 도구는 FIPS 준수 엔드포인트에 요청을 보냅니다.
- **false**— SDK 또는 도구는 FIPS 호환 엔드포인트에 요청을 보내지 않습니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 돈	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	예	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.

SDK	지 운 톤 참고 또는 추가 정보
<a href="#">SDK for Java 2.x</a>	예
<a href="#">SDK for Java 1.x</a>	아 니 요
<a href="#">SDK for JavaScript 3.x</a>	예
<a href="#">SDK for JavaScript 2.x</a>	예
<a href="#">SDK for Kotlin</a>	예
<a href="#">.NET 4.x용 SDK</a>	예
<a href="#">SDK for .NET 3.x</a>	예
<a href="#">SDK for PHP 3.x</a>	예
<a href="#">SDK for Python (Boto3)</a>	예
<a href="#">SDK for Ruby 3.x</a>	예
<a href="#">SDK for Rust</a>	예
<a href="#">SDK for Swift</a>	예
<a href="#">PowerShell V5용 도구</a>	예
<a href="#">PowerShell V4용 도구</a>	예

## 엔드포인트 검색

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs 이 안내서의 설정 페이지의 이해](#).

SDKs 엔드포인트 검색을 사용하여 서비스 엔드포인트(URLs)를 사용하여 다양한 리소스에 액세스)에 액세스하는 동시에 필요에 따라가 URLs AWS 을 변경할 수 있는 유연성을 유지합니다. 이렇게 하면 코드가 새 엔드포인트를 자동으로 탐지할 수 있습니다. 일부 서비스에는 고정된 엔드포인트가 없습니다. 대신 런타임 중에 먼저 엔드포인트를 가져오기를 요청하여 사용 가능한 엔드포인트를 확보할 수 있습니다. 사용 가능한 엔드포인트를 검색한 후 코드는 해당 엔드포인트를 사용하여 다른 작업에 액세스합니다. 예를 들어 Amazon Timestream의 경우 SDK는 가용 엔드포인트를 검색하도록 DescribeEndpoints 요청하고 해당 엔드포인트를 사용하여 CreateDatabase 또는 CreateTable 같은 특정 작업을 완료합니다.

다음을 사용하여 이 기능을 구성하십시오.

**endpoint\_discovery\_enabled** - 공유 AWS config 파일 설정,

**AWS\_ENABLE\_ENDPOINT\_DISCOVERY** - 환경 변수, **aws.endpointDiscoveryEnabled** - JVM 시스템 속성: Java/Kotlin만 해당, 코드에서 값을 직접 구성하려면 특정 SDK를 직접 참조하십시오.

DynamoDB에 대한 엔드포인트 검색을 켜거나 끕니다.

엔드포인트 검색은 Timestream에서는 필수이며, Amazon DynamoDB에서는 선택 사항입니다. 이 설정은 서비스가 엔드포인트 검색을 필요로 하는지 여부에 따라 기본값이 true 또는 false로 설정됩니다. Timestream 요청은 기본적으로 true로 설정되며, Amazon DynamoDB 요청은 기본적으로 false로 설정됩니다.

유효한 값:

- **true**— SDK는 엔드포인트 검색이 선택사항인 서비스의 엔드포인트 검색을 자동으로 시도해야 합니다.
- **false**— SDK는 엔드포인트 검색이 선택 사항인 서비스의 엔드포인트 검색을 자동으로 시도해서는 안 됩니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 돈	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	예	공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	예	Java 2.x용 SDK는 환경 변수 이름에 <code>AWS_ENDPOINT_DISCOVERY_ENABLED</code> 를 사용합니다.
<a href="#">SDK for Java 1.x</a>	부 분 적	JVM 시스템 속성은 지원되지 않습니다.
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	예	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for Rust</a>	부 분 적	타임스트림에만 지원됩니다.
<a href="#">SDK for Swift</a>	아 니 요	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## 일반 구성 설정

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs이 안내서의 설정 페이지의 이해](#).

SDK는 전체 SDK 동작을 구성하는 몇 가지 일반 설정을 지원합니다.

다음을 사용하여 이 기능을 구성하십시오.

### **api\_versions** - 공유 AWS **config** 파일 설정

일부 AWS 서비스는 이전 버전과의 호환성을 지원하기 위해 여러 API 버전을 유지 관리합니다. 기본적으로 SDK 및 AWS CLI 작업은 최신 API 버전을 사용합니다. 요청에 사용할 특정 API 버전을 요구하려면 프로파일에 `api_versions` 설정을 포함하십시오.

기본값: 없음. (SDK에는 최신 API 버전이 사용됩니다.)

유효한 값: 중첩된 설정으로, 그 뒤에 사용할 AWS 서비스와 API 버전을 각각 식별하는 하나 이상의 들여쓰기된 줄이 옵니다. 사용 가능한 API 버전을 알아보려면 AWS 서비스 설명서를 참조하세요.

이 예제에서는 `config` 파일의 두 AWS 서비스에 대해 특정 API 버전을 설정합니다. 이러한 API 버전은 이러한 설정이 포함된 프로파일 하에서 실행되는 명령에서만 사용됩니다. 다른 서비스의 명령은 해당 서비스 API의 최신 버전을 사용합니다.

```
api_versions =
  ec2 = 2015-03-01
  cloudfront = 2015-09-017
```

## ca\_bundle - 공유 AWS config 파일 설정, AWS\_CA\_BUNDLE - 환경 변수

SSL/TLS 연결을 설정할 때 사용할 사용자 지정 인증서 번들(.pem 확장명이 있는 파일)의 경로를 지정합니다.

기본값: 없음

유효한 값: 전체 경로 또는 기본 파일 이름을 지정합니다. 기본 파일 이름이 있는 경우, 시스템은 PATH 환경 변수로 지정된 폴더 내에서 프로그램을 찾으려고 시도합니다.

config 파일에서 이 값을 설정하는 예:

```
[default]
ca_bundle = dev/apps/ca-certs/cabundle-2019mar05.pem
```

운영체제마다 경로 처리 방식과 경로 문자 이스케이프 방식이 다르기 때문에, 다음은 Windows의 config 파일에서 이 값을 설정하는 예시입니다.

```
[default]
ca_bundle = C:\\Users\\username\\.aws\\aws-custom-bundle.pem
```

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_CA_BUNDLE=/dev/apps/ca-certs/cabundle-2019mar05.pem
```

명령줄을 통해 환경 변수를 설정하는 Windows 예제:

```
setx AWS_CA_BUNDLE C:\dev\apps\ca-certs\cabundle-2019mar05.pem
```

## output - 공유 AWS config 파일 설정

AWS CLI 및 기타 AWS SDKs 및 도구에서 결과의 형식을 지정하는 방법을 지정합니다.

기본값: json

유효값:

- **json** - 출력은 [JSON](#) 문자열로 형식이 지정됩니다.
- **yaml** - 출력은 [YAML](#) 문자열로 형식이 지정됩니다.
- **yaml-stream** - 출력은 스트리밍되고 [YAML](#) 문자열로 형식이 지정됩니다. 스트리밍을 통해 대용량 데이터 유형을 빠르게 처리할 수 있습니다.
- **text** - 출력은 여러 줄의 탭으로 구분된 문자열 값으로 형식이 지정됩니다. 출력을 grep, sed 또는 awk와 같은 텍스트 프로세서로 전달하는 데 사용할 수 있습니다.
- **table** - 출력은 셀 테두리를 형성하기 위해 +- 문자를 사용하여 표로 형식이 지정됩니다. 일반적으로 읽기는 쉽지만 프로그래밍 방식으로는 유용하지 않은 '인간 친화적' 형식으로 정보를 표시합니다.

### parameter\_validation - 공유 AWS config 파일 설정

SDK 또는 도구가 AWS 서비스 엔드포인트에 보내기 전에 명령줄 파라미터를 검증할지 여부를 지정합니다.

기본값: true

유효값:

- **true** - 기본값입니다. SDK 또는 도구는 명령줄 파라미터를 클라이언트측에서 검증합니다. 이렇게 하면 SDK 또는 도구가 파라미터가 유효한지 확인하고 일부 오류를 포착하는 데 도움이 됩니다. SDK 또는 도구는 요청을 AWS 서비스 엔드포인트로 보내기 전에 유효하지 않은 요청을 거부할 수 있습니다.
- **false** - SDK 또는 도구는 AWS 서비스 엔드포인트로 전송하기 전에 명령줄 파라미터를 검증하지 않습니다. AWS 서비스 엔드포인트는 모든 요청을 검증하고 유효하지 않은 요청을 거부할 책임이 있습니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 통	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	부 분 적	api_versions 이 지원되지 않음.
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	부 분 적	api_versions 및 parameter_validation 이 지원되지 않음.
<a href="#">SDK for Go 1.x (V1)</a>	부 분 적	api_versions 및 parameter_validation 이 지원되지 않음. 공유 config 파일 설정을 사용하려면 구성 파일에서 로드를 켜야 합니다. <a href="#">세션</a> 을 참조하십시오.
<a href="#">SDK for Java 2.x</a>	아 니 요	
<a href="#">SDK for Java 1.x</a>	아 니 요	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	예	
<a href="#">SDK for Kotlin</a>	아 니 요	
<a href="#">.NET 4.x용 SDK</a>	아 니 요	

SDK	지원 톤	참고 또는 추가 정보
<a href="#">SDK for .NET 3.x</a>	아 니 요	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	아 니 요	
<a href="#">SDK for Swift</a>	아 니 요	
<a href="#">PowerShell V5용 도구</a>	아 니 요	
<a href="#">PowerShell V4용 도구</a>	아 니 요	

## 호스트 접두사 삽입

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#)이 안내서의 [설정 페이지의 이해](#).

호스트 접두사 삽입은 AWS SDKs가 특정 API 작업에 대한 서비스 엔드포인트의 호스트 이름 앞에 접두사를 자동으로 추가하는 기능입니다. 이 접두사는 정적 문자열이거나 요청 매개변수의 데이터를 포함하는 동적 값일 수 있습니다.

예를 들어 Amazon Simple Storage Service를 사용하여 Amazon S3 객체 또는 버킷에 대한 작업을 수행할 때 SDK는 최종 API 엔드포인트의 버킷 이름과 AWS 계정 ID를 대체합니다.

이 동작은 일반 AWS 서비스 엔드포인트에 필요하지만 VPC 엔드포인트 또는 로컬 테스트 도구와 같은 사용자 지정 엔드포인트를 사용할 때 문제가 발생할 수 있습니다. 이러한 경우 호스트 접두사 삽입을 비활성화해야 할 수 있습니다.

다음을 사용하여 이 기능을 구성하십시오.

**disable\_host\_prefix\_injection** - 공유 AWS **config** 파일 설정,  
**AWS\_DISABLE\_HOST\_PREFIX\_INJECTION** - 환경 변수, **aws.disableHostPrefixInjection** - JVM 시스템 속성: Java/Kotlin만 해당

이 설정은 SDK나 도구가 SDK의 클라이언트 객체나 변수에 정의된 대로 호스트 접두사를 앞에 추가하여 엔드포인트 호스트 이름을 수정할지 여부를 제어합니다.

기본값: `false`

유효한 값:

- **true** - 호스트 접두사 삽입을 비활성화합니다. SDK는 엔드포인트 호스트 이름을 수정하지 않습니다.
- **false** - 호스트 접두사 삽입을 활성화합니다. SDK는 엔드포인트 호스트 이름 앞에 호스트 접두사를 추가합니다.

config 파일에서 이 값을 설정하는 예:

```
[default]
disable_host_prefix_injection = true
```

명령 행을 통한 환경 변수 설정의 Linux/macOS 예제:

```
export AWS_DISABLE_HOST_PREFIX_INJECTION=true
```

명령줄을 통해 환경 변수를 설정하는 Windows 예제:

```
setx AWS_DISABLE_HOST_PREFIX_INJECTION true
```

## 호스트 접두사 삽입의 예

아래 예시 표는 호스트 접두사 삽입이 활성화된 경우와 비활성화된 경우, SDK가 최종 엔드포인트를 어떻게 수정하는지를 보여줍니다.

- 호스트 접두사: 코드에서 SDK의 클라이언트 객체 또는 변수에 설정되는 호스트 접두사 속성 문자열의 템플릿입니다.
- 입력: SDK의 클라이언트 객체 또는 코드의 변수에 설정된 추가 입력입니다.
- 클라이언트 엔드포인트: 클라이언트의 파생 엔드포인트입니다.
- 설정 값: 이전 설정의 해결된 값입니다.
- 결과 엔드포인트: SDK 클라이언트가 API 직접 호출에 사용하는 결과 엔드포인트입니다.

호스트 접두사	입력	클라이언트 엔드포인트	설정 값	결과 엔드포인트
"data."	{}	'https://service.us-west-2.amazonaws.com'	false	'https://data.service.us-west-2.amazonaws.com'
"{Bucket}-{AccountId}."	Bucket: "amzn-s3-demo-bucket1", AccountId: "123456789012"	'https://service.us-west-2.amazonaws.com'	false	'https://amzn-s3-demo-bucket1-123456789012.service.us-west-2.amazonaws.com'
"data."	{}	'https://override.us-west-2.amazonaws.com' (as an override endpoint)	true	'https://override.us-west-2.amazonaws.com'

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	아 니 요	설정은 지원되지 않지만 <a href="#">enableHostPrefixInjection</a> 를 사용하여 클라이언트의 코드에서 구성할 수 있습니다.
<a href="#">SDK for Go V2 (1.x)</a>	아 니 요	<a href="#">미들웨어를 사용</a> 하여 비활성화할 수 있습니다.
<a href="#">SDK for Go 1.x (V1)</a>	아 니 요	
<a href="#">SDK for Java 2.x</a>	아 니 요	설정은 지원되지 않지만 <a href="#">SdkAdvancedClientOption.DISABLE_HOST_PREFIX_INJECTION</a> 를 사용하여 클라이언트의 코드에서 구성할 수 있습니다.
<a href="#">SDK for Java 1.x</a>	아 니 요	설정은 지원되지 않지만 <a href="#">withDisableHostPrefixInjection</a> 를 사용하여 클라이언트의 코드에서 구성할 수 있습니다.
<a href="#">SDK for JavaScript 3.x</a>	아 니 요	설정은 지원되지 않지만 <a href="#">disableHostPrefix</a> 를 사용하여 클라이언트의 코드에서 구성할 수 있습니다.
<a href="#">SDK for JavaScript 2.x</a>	아 니 요	설정은 지원되지 않지만 <a href="#">hostPrefixEnabled</a> 를 사용하여 클라이언트의 코드에서 구성할 수 있습니다.

SDK	지원 통 참고 또는 추가 정보
<a href="#">SDK for Kotlin</a>	아 니 요
<a href="#">.NET 4.x용 SDK</a>	아 니 요 설정은 지원되지 않지만 <a href="#">DisableHostPrefixIn jection</a> 를 사용하여 클라이언트의 코드에서 구성할 수 있 습니다.
<a href="#">SDK for .NET 3.x</a>	아 니 요 설정은 지원되지 않지만 <a href="#">DisableHostPrefixIn jection</a> 를 사용하여 클라이언트의 코드에서 구성할 수 있 습니다.
<a href="#">SDK for PHP 3.x</a>	아 니 요 설정은 지원되지 않지만 <a href="#">disable_host_prefi x_injection</a> 를 사용하여 클라이언트의 코드에서 구성할 수 있습니다.
<a href="#">SDK for Python (Boto3)</a>	예 <a href="#">inject_host_prefix</a> 를 사용하여 클라이언트의 코드에 서 구성할 수 있습니다.
<a href="#">SDK for Ruby 3.x</a>	아 니 요 설정은 지원되지 않지만 <a href="#">disable_host_prefi x_injection</a> 를 사용하여 클라이언트의 코드에서 구성할 수 있습니다.
<a href="#">SDK for Rust</a>	아 니 요
<a href="#">SDK for Swift</a>	아 니 요
<a href="#">PowerShell V5용 도구</a>	아 니 요 설정은 지원되지 않지만 <code>-ClientConfig @{Disable HostPrefixInjection = \$true}</code> 매개변수를 사용하 여 특정 cmdlet에 포함시킬 수 있습니다.

SDK	지 운 톤 참고 또는 추가 정보
<a href="#">PowerShell V4용 도구</a>	아 니 요 설정은 지원되지 않지만 <code>-ClientConfig @{DisableHostPrefixInjection = \$true}</code> 매개변수를 사용하여 특정 cmdlet에 포함시킬 수 있습니다.

## IMDS 클라이언트

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#)이 안내서의 [설정 페이지의 이해](#).

SDK는 세션 지향 요청을 사용하여 인스턴스 메타데이터 서비스 버전 2 (IMDSv2) 클라이언트를 구현합니다. IMDSv2에 대한 자세한 내용은 <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html> Amazon EC2 사용 설명서의 IMDSv2 사용을 참조하세요. IMDS 클라이언트는 SDK 코드 베이스에서 사용할 수 있는 클라이언트 구성 객체를 통해 구성할 수 있습니다.

다음을 사용하여 이 기능을 구성하십시오.

**retries** - 클라이언트 구성 객체 멤버

실패한 요청에 대한 추가 재시도 횟수입니다.

기본값: 3

유효한 값: 0보다 큰 숫자.

**port** - 클라이언트 구성 객체 멤버

엔드포인트 포트.

기본값: 80

유효한 값: 숫자.

**token\_ttl** - 클라이언트 구성 객체 멤버

토큰의 TTL.

기본값: 21,600초(6시간, 최대 할당 시간).

유효한 값: 숫자.

**endpoint** - 클라이언트 구성 객체 멤버

IMDS 엔드포인트.

기본값: endpoint\_mode와 IPv4이 같으면 기본 엔드포인트는 http://169.254.169.254입니다. endpoint\_mode와 IPv6이 같으면 기본 엔드포인트는 http://[fd00:ec2::254]입니다.

유효한 값: 유효한 URI.

대부분의 SDK에 의해 지원되는 옵션은 다음과 같습니다. 자세한 내용은 특정 SDK 코드베이스를 참조하십시오.

**endpoint\_mode**- 클라이언트 구성 객체 멤버

IMDS의 엔드포인트 모드.

기본값: IPv4

유효한 값: IPv4, IPv6

**http\_open\_timeout**- 클라이언트 구성 객체 멤버 (이름은 다를 수 있음)

연결이 열릴 때까지 기다리는 시간 (초).

기본값: 1초.

유효한 값: 0보다 큰 숫자.

**http\_read\_timeout**- 클라이언트 구성 객체 멤버 (이름은 다를 수 있음)

데이터 청크 하나를 읽는 데 걸리는 시간 (초).

기본값: 1초.

유효한 값: 0보다 큰 숫자.

**http\_debug\_output**- 클라이언트 구성 객체 멤버 (이름은 다를 수 있음)

디버깅을 위한 출력 스트림을 설정합니다.

기본값: 없음.

유효한 값: STDOUT과 같은 유효한 I/O 스트림.

**backoff**- 클라이언트 구성 객체 멤버 (이름은 다를 수 있음)

재시도 또는 고객이 백오프 기능을 제공하여 전화를 걸 때까지 기다려야 하는 시간 (초). 이는 기본 지수 백오프 전략을 재정의 합니다.

기본값: SDK에 따라 다릅니다.

유효한 값: SDK에 따라 다릅니다. 숫자 값이거나 사용자 지정 함수 직접 호출이 될 수 있습니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	아 니 요	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	예	
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	예	
<a href="#">SDK for JavaScript 3.x</a>	예	

SDK	지원 상태	참고 또는 추가 정보
<a href="#">SDK for JavaScript 2.x</a>	예	
<a href="#">SDK for Kotlin</a>	아 니 요	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## 재시도 동작

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#) [이 안내서의 설정 페이지의 이해](#).

재시도 동작에는 SDK가 AWS 서비스에 보내진 요청으로 인한 장애 복구를 시도하는 방법에 대한 설정이 포함됩니다.

다음을 사용하여 이 기능을 구성하십시오.

**retry\_mode** - 공유 AWS **config** 파일 설정, **AWS\_RETRY\_MODE** - 환경 변수, **aws.retryMode** - JVM 시스템 속성: Java/Kotlin만 해당

SDK 또는 개발자 도구의 재시도 방법을 지정합니다.

기본값: 이 값은 SDK에 따라 달라집니다. SDK의 기본 `retry_mode` 값은 SDK별 안내서를 확인하거나 SDK의 코드 베이스를 참고하세요.

유효한 값:

- `standard` - (권장) AWS SDKs. 이 모드는 재시도 대상이 되는 표준 오류 집합을 포함하며, 가용성과 안정성을 극대화하기 위해 재시도 횟수를 자동으로 조정합니다. 이 모드는 멀티 테넌트 애플리케이션에서 사용하기에 안전합니다. 명시적으로 `max_attempts`으로 구성되어 있지 않으면 이 모드의 기본 최대 시도 횟수는 3회입니다.
- `adaptive` - 표준 모드의 기능에 더해 클라이언트 측 자동 레이트 리미팅까지 포함하는 재시도 모드로, 특수한 사용 사례에만 적합합니다. 이 재시도 모드는 애플리케이션 테넌트를 철저히 분리하지 않는 한, 멀티 테넌트 애플리케이션에서는 권장되지 않습니다. 자세한 정보는 [standard 및 adaptive 재시도 모드 중 선택](#)을 참조하세요. 이 모드는 실험적이며, 향후 동작이 변경될 수 있습니다.
- `legacy` - (비권장) 사용자의 SDK에만 적용되는 설정으로, 해당 SDK 안내서 또는 SDK의 코드 베이스를 확인해야 합니다.

**max\_attempts** - 공유 AWS **config** 파일 설정, **AWS\_MAX\_ATTEMPTS** - 환경 변수, **aws.maxAttempts** - JVM 시스템 속성: Java/Kotlin만 해당

요청에 대한 최대 시도 횟수를 지정합니다.

기본값: 이 값이 지정되지 않은 경우 기본값은 `retry_mode` 설정 값에 따라 달라집니다.

- `retry_mode`이 `legacy` 인 경우— 사용자 SDK 고유의 기본값을 사용합니다(사용자 고유 SDK 설명서 또는 `max_attempts` 기본 SDK의 코드베이스를 확인하십시오).
- `retry_mode`이 `standard`인 경우 — 세 번 시도합니다.
- `retry_mode`이 `adaptive`인 경우 — 세 번 시도합니다.

유효한 값: 0보다 큰 숫자.

## **standard** 및 **adaptive** 재시도 모드 중 선택

특히 `adaptive`가 더 적합하다고 확신하지 않는 이상, `standard` 재시도 모드를 사용할 것을 권장합니다.

**Note**

adaptive 모드에서는 백엔드 서비스가 요청을 제한할 수 있는 범위에 따라 클라이언트를 폴링한다고 가정합니다. 이렇게 하지 않으면, 동일한 클라이언트를 여러 리소스에 사용 중일 때 특정 리소스에서 발생한 스로틀링이 관련 없는 리소스의 요청까지 지연시킬 수 있습니다.

표준	적응형
애플리케이션 사용 사례: 전체.	애플리케이션 사용 사례: <ol style="list-style-type: none"> <li>1. 지연 시간에 민감하지 않습니다.</li> <li>2. 클라이언트가 단일 리소스에만 액세스하거나, 액세스하는 서비스 리소스별로 클라이언트를 개별적으로 폴링하는 로직을 제공합니다.</li> </ol>
중단 상황에서 SDK가 재시도하지 않도록 차단을 지원합니다.	중단 상황에서 SDK가 재시도하지 않도록 차단을 지원합니다.
실패 시 지터링된 지수 백오프를 사용합니다.	지연 시간이 증가할 가능성과 맞바꾸는 대신, 실패한 요청 수를 최소화하기 위해 동적 백오프 지속 시간을 사용합니다.
첫 번째 요청 시도에는 지연을 적용하지 않고, 재시도에만 지연을 적용합니다.	초기 요청 시도에도 스로틀링하거나 지연을 적용할 수 있습니다.

adaptive 모드를 사용하기로 선택한 경우, 애플리케이션은 스로틀링이 발생할 수 있는 각 리소스별로 클라이언트를 구성해야 합니다. 이 경우 리소스는 각 리소스를 생각하는 것보다 더 세밀하게 조정됩니다. AWS 서비스는 요청을 제한하는 데 사용하는 추가 차원을 가질 AWS 서비스 수 있습니다. Amazon DynamoDB 서비스를 예로 들어 보겠습니다. DynamoDB는 AWS 리전 및 액세스 중인 테이블을 사용하여 요청을 제한합니다. 이는 코드에서 액세스하는 테이블 중 하나가 다른 테이블보다 더 많이 스로틀링될 수 있다는 뜻입니다. 코드에서 모든 테이블에 동일한 클라이언트를 사용하고 있고, 그중 하나의 테이블이 스로틀링되면, 적응형 재시도 모드는 모든 테이블에 대한 요청 속도를 낮추게 됩니다. 코드는 리전과 테이블의 각 조합마다 하나의 클라이언트를 사용하도록 설계해야 합니다. adaptive 모드를 사용할 때 예기치 않은 지연 시간이 발생하는 경우 사용 중인 서비스에 대한 특정 AWS 설명서 가이드를 참조하세요.

## 재시도 모드 구현 세부 정보

AWS SDKs는 [토큰 버킷](#)을 사용하여 요청을 재시도할지 여부와 (adaptive재시도 모드의 경우) 요청을 얼마나 빨리 전송해야 하는지 결정합니다. SDK는 재시도 토큰 버킷과 요청 속도 토큰 버킷이라는 두 개의 토큰 버킷을 사용합니다.

- 재시도 토큰 버킷은 중단 시 업스트림 및 다운스트림 서비스를 보호하기 위해 SDK가 재시도를 일시적으로 비활성화해야 하는지 여부를 결정하는 데 사용됩니다. 재시도를 시도하기 전에 버킷에서 토큰을 획득하고, 요청이 성공하면 토큰이 버킷으로 반환됩니다. 재시도를 시도할 때 버킷이 비어 있는 경우 SDK가 요청을 재시도하지 않습니다.
- 요청 속도 토큰 버킷은 adaptive 재시도 모드에서만 사용되며, 요청을 전송할 속도를 결정하는 데 활용됩니다. 요청을 보내기 전에 버킷에서 토큰을 가져오며, 서비스에서 반환되는 스로틀링 응답을 기반으로 동적으로 결정된 속도에 따라 토큰이 버킷에 반환됩니다.

다음은 standard 모드와 adaptive 모드 모두에 대한 고급 의사코드입니다.

```
MakeSDKRequest() {
  attempts = 0
  loop {
    GetSendToken()
    response = SendHTTPRequest()
    RequestBookkeeping(response)
    if not Retryable(response)
      return response
    attempts += 1
    if attempts >= MAX_ATTEMPTS:
      return response
    if not HasRetryQuota(response)
      return response
    delay = ExponentialBackoff(attempts)
    sleep(delay)
  }
}
```

다음은 의사코드에 사용되는 구성 요소에 대한 자세한 내용입니다.

### GetSendToken:

이 단계는 adaptive 재시도 모드에서만 사용됩니다. 이 단계에서는 요청 속도 토큰 버킷에서 토큰을 가져옵니다. 토큰을 사용할 수 없는 경우 토큰을 사용할 수 있을 때까지 기다립니다. SDK에는 대기 대

신 요청을 즉시 실패하도록 설정할 수 있는 구성 옵션이 제공될 수도 있습니다. 버킷의 토큰은 클라이언트가 받은 스로틀링 응답 수에 따라 동적으로 결정되는 속도로 다시 채워집니다.

### **SendHTTPRequest:**

이 단계에서는 요청을 로 보냅니다 AWS. AWS SDKs HTTP 요청을 할 때 연결 풀을 사용하여 기존 연결을 재사용하는 HTTP 라이브러리를 사용합니다. 일반적으로 요청이 스로틀링 오류로 인해 실패한 경우에는 연결이 재사용되지만, 일시적 오류로 인해 실패한 경우에는 연결이 재사용되지 않습니다.

### **RequestBookkeeping:**

요청이 성공하면 토큰이 토큰 버킷에 추가됩니다. adaptive 재시도 모드에서만, 요청 속도 토큰 버킷의 충전 속도는 수신한 응답 유형에 따라 업데이트됩니다.

### **Retryable:**

이 단계에서는 다음을 기반으로 응답을 재시도할 수 있는지 여부를 결정합니다.

- HTTP 상태 코드 .
- 서비스에서 반환된 오류 코드입니다.
- 연결 오류로, 서비스로부터 HTTP 응답을 받지 못한 SDK에서 수신한 모든 오류로 정의됩니다.

일시적 오류(HTTP 상태 코드 400, 408, 500, 502, 503, 504)와 조절 오류(HTTP 상태 코드 400, 403, 429, 502, 503, 509)는 모두 재시도될 수 있습니다. SDK 재시도 동작은 서비스의 오류 코드 또는 서비스의 기타 데이터와 조합하여 결정됩니다.

### **MAX\_ATTEMPTS:**

기본 최대 시도 횟수는 `max_attempts` 설정으로 재정의되지 않는 한 `retry_mode` 설정에 의해 결정됩니다.

### **HasRetryQuota**

이 단계에서는 재시도 토큰 버킷에서 토큰을 가져옵니다. 재시도 토큰 버킷이 비어 있으면 요청이 재시도되지 않습니다.

### **ExponentialBackoff**

재시도할 수 있는 오류의 경우 잘린 지수 백오프를 사용하여 재시도 지연을 계산합니다. SDK는 지터가 있는 잘린 이진 지수 백오프를 사용합니다. 다음 알고리즘은 요청에 대한 응답의 절전 시간(초)이 어떻게 정의되는지 보여줍니다.  $i$

```
seconds_to_sleep_i = min(b*r^i, MAX_BACKOFF)
```

위 알고리즘에는 다음 값이 적용됩니다.

$b$  = random number within the range of:  $0 \leq b \leq 1$

$r = 2$

대부분의 SDK용 MAX\_BACKOFF = 20 seconds. 사용자 특정 SDK 가이드 또는 소스 코드를 참조하여 확인합니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 통	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	아 니 요	
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	예	JVM 시스템 속성: <code>aws.maxAttempts</code> 대신 <code>com.amazonaws.sdk.maxAttempts</code> 를 사용하고, <code>aws.retryMode</code> 대신 <code>com.amazonaws.sdk.retryMode</code> 를 사용합니다.
<a href="#">SDK for JavaScript 3.x</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for JavaScript 2.x</a>	아 니 요	최대 재시도 횟수, 지터가 있는 지수 백오프, 재시도 백오프를 위한 사용자 지정 방법 옵션을 지원합니다.
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## 요청 압축

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#)이 [안내서의 설정 페이지의 이해](#).

AWS SDKs페이로드 수신을 지원하는 AWS 서비스 에 요청을 보낼 때 페이로드를 자동으로 압축할 수 있습니다. 페이로드를 서비스로 보내기 전에 클라이언트에서 압축하면 데이터를 서비스로 보내는 데 필요한 전체 요청 수와 대역폭을 줄일 수 있을 뿐만 아니라 페이로드 크기에 대한 서비스 제한으로 인

해 실패한 요청도 줄일 수 있습니다. 압축을 위해 SDK 또는 도구는 서비스와 SDK에서 모두 지원하는 인코딩 알고리즘을 선택합니다. 그러나 현재 가능한 인코딩 목록은 gzip으로만 구성되어 있지만 향후 확장될 수 있습니다.

요청 압축은 애플리케이션에서 [Amazon CloudWatch](#)를 사용하는 경우 특히 유용할 수 있습니다. CloudWatch는 모니터링 및 운영 데이터를 로그, 지표 및 이벤트 형태로 수집하는 모니터링 및 관찰성 서비스입니다. 압축을 지원하는 서비스 작업의 한 예로 CloudWatch의 [PutMetricDataAPI](#) 방법을 들 수 있습니다.

다음을 사용하여 이 기능을 구성하십시오.

**disable\_request\_compression** - 공유 AWS config 파일 설정,  
**AWS\_DISABLE\_REQUEST\_COMPRESSION** - 환경 변수, **aws.disableRequestCompression** - JVM  
 시스템 속성: Java/Kotlin만 해당

요청을 보내기 전에 SDK 또는 도구가 페이로드를 압축할지 여부를 설정하거나 해제합니다.

기본값: false

유효값:

- **true** - 요청 압축을 해제합니다.
- **false** - 가능하면 요청 압축을 사용합니다.

**request\_min\_compression\_size\_bytes** - 공유 AWS config 파일 설정,  
**AWS\_REQUEST\_MIN\_COMPRESSION\_SIZE\_BYTES** - 환경 변수,  
**aws.requestMinCompressionSizeBytes** - JVM 시스템 속성: Java/Kotlin만 해당

SDK 또는 도구가 압축해야 하는 요청 본문의 최소 크기(바이트)를 설정합니다. 작은 페이로드는 압축 시 더 길어질 수 있으므로 압축을 수행하는 데 적합한 하한선이 있습니다. 이 값은 포함되며, 이 값보다 크거나 같은 요청 크기는 압축됩니다.

기본값: 10240바이트

유효값: 0~10485760바이트 사이의 정수 값.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 통	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	아 니 요	
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	아 니 요	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	아 니 요	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	

SDK	지 운 톤	참고 또는 추가 정보
<a href="#">SDK for Swift</a>	아 니 요	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## 서비스별 엔드포인트

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs](#)이 안내서의 [설정 페이지의 이해](#).

서비스별 엔드포인트 구성은 API 요청에 대해 사용자가 선택한 엔드포인트를 사용하고 선택을 유지할 수 있는 옵션을 제공합니다. 이러한 설정은 로컬 엔드포인트, VPC 엔드포인트 및 타사 로컬 AWS 개발 환경을 지원할 수 있는 유연성을 제공합니다. 테스트 환경과 프로덕션 환경에 서로 다른 엔드포인트를 사용할 수 있습니다. 개별 AWS 서비스서비스에 대한 엔드포인트 URL을 지정할 수 있습니다.

다음을 사용하여 이 기능을 구성하십시오.

**endpoint\_url** - 공유 AWS config 파일 설정, **AWS\_ENDPOINT\_URL** - 환경 변수,  
**aws.endpointUrl** - JVM 시스템 속성: Java/Kotlin만 해당

프로파일 내에서 직접 지정하거나 환경 변수로 지정하는 경우 이 설정은 모든 서비스 요청에 사용되는 엔드포인트를 지정합니다. 이 엔드포인트는 구성된 모든 서비스별 엔드포인트에 의해 재정의됩니다.

공유 AWS config 파일의 `services` 섹션 내에서 이 설정을 사용하여 특정 서비스에 대한 사용자 지정 엔드포인트를 설정할 수도 있습니다. `services` 섹션에서 사용할 모든 서비스 식별자 키 목록은 [서비스별 엔드포인트 식별자](#) 섹션을 참조하십시오.

기본값: none

**유효한 값:** 엔드포인트의 스키마와 호스트가 포함된 URL. URL에는 하나 이상의 경로 세그먼트가 포함된 경로 구성 요소가 선택적으로 포함될 수 있습니다.

**AWS\_ENDPOINT\_URL\_<SERVICE>** - 환경 변수, **aws.endpointUrl<ServiceName>** - JVM 시스템 속성: Java/Kotlin만 해당

**AWS\_ENDPOINT\_URL\_<SERVICE>**, 여기서 <SERVICE>는 AWS 서비스 식별자이며,는 특정 서비스에 대한 사용자 지정 엔드포인트를 설정합니다. 모든 서비스별 환경 변수 목록은 [서비스별 엔드포인트 식별자](#)를 참조하십시오.

이 서비스별 엔드포인트는 **AWS\_ENDPOINT\_URL**에 설정된 모든 글로벌 엔드포인트보다 우선합니다.

**기본값:** none

**유효한 값:** 엔드포인트의 스키마와 호스트가 포함된 URL. URL에는 하나 이상의 경로 세그먼트가 포함된 경로 구성 요소가 선택적으로 포함될 수 있습니다.

**ignore\_configured\_endpoint\_urls** - 공유 AWS **config** 파일 설정, **AWS\_IGNORE\_CONFIGURED\_ENDPOINT\_URLS** - 환경 변수, **aws.ignoreConfiguredEndpointUrls** - JVM 시스템 속성: Java/Kotlin만 해당

이 설정은 모든 사용자 지정 엔드포인트 구성을 무시하는 데 사용됩니다.

코드에 설정되거나 서비스 클라이언트 자체에 설정된 명시적 엔드포인트는 이 설정과 상관없이 사용된다는 점에 유의하십시오. 예를 들어 `--endpoint-url` 명령줄 파라미터를 AWS CLI 명령과 함께 포함하거나 엔드포인트 URL을 클라이언트 생성자에 전달하면 항상 적용됩니다.

**기본값:** false

**유효한 값:**

- **true**— SDK 또는 도구는 공유 config 파일 또는 환경 변수에서 엔드포인트 URL 설정을 위한 사용자 지정 구성 옵션을 읽지 않습니다.
- **false**— SDK 또는 도구는 공유 config 파일 또는 환경 변수에서 사용 가능한 사용자 제공 엔드포인트를 사용합니다.

## 환경 변수를 사용한 엔드포인트 구성

모든 서비스에 대한 요청을 사용자 지정 엔드포인트 URL로 라우팅하려면 **AWS\_ENDPOINT\_URL** 글로벌 환경 변수를 설정하십시오.

```
export AWS_ENDPOINT_URL=http://localhost:4567
```

특정에 대한 요청을 사용자 지정 엔드포인트 URL AWS 서비스 로 라우팅하려면 `AWS_ENDPOINT_URL_<SERVICE>` 환경 변수를 사용합니다. Amazon DynamoDB 에는 `serviceId`의이 있습니다 [DynamoDB](#). 이 서비스의 경우 엔드포인트 URL 환경 변수는 `AWS_ENDPOINT_URL_DYNAMODB`입니다. 이 엔드포인트는 이서비스에 대해 `AWS_ENDPOINT_URL`에 설정된 글로벌 엔드포인트보다 우선합니다.

```
export AWS_ENDPOINT_URL_DYNAMODB=http://localhost:5678
```

또 다른 예로의 `serviceId` AWS Elastic Beanstalk 가 있습니다 [Elastic Beanstalk](#). AWS 서비스 식별자는 모든 공백을 밑줄로 바꾸고 모든 문자를 대문자로 대체 `serviceId`하여 API 모델의를 기반으로 합니다. 이 서비스에 대한 엔드포인트를 설정하려면 해당 환경 변수는 `AWS_ENDPOINT_URL_ELASTIC_BEANSTALK`입니다. 모든 서비스별 환경 변수 목록은 [서비스별 엔드포인트 식별자](#)을 참조하십시오.

```
export AWS_ENDPOINT_URL_ELASTIC_BEANSTALK=http://localhost:5567
```

공유 **config** 파일을 사용하여 엔드포인트를 구성합니다.

공유 config 파일에서는 다양한 기능을 위해 여러 위치에서 `endpoint_url`이 사용됩니다.

- profile 내에서 직접 지정된 `endpoint_url`은 해당 엔드포인트를 글로벌 엔드포인트로 만듭니다.
- `services` 섹션 내의 서비스 식별자 키 아래에 중첩된 `endpoint_url`은 해당 엔드포인트가 해당 서비스에 대한 요청에만 적용되도록 만듭니다. 공유 config 파일에서 `services` 섹션을 정의하는 방법에 대한 자세한 내용은 [구성 파일 형식](#)를 참조하십시오.

다음 예제에서는 `services` 정의를 사용하여 Amazon S3에 대한 서비스별 엔드포인트 URL과 다른 모든 서비스에 사용되는 사용자 지정 글로벌 엔드포인트를 구성합니다.

```
[profile dev-s3-specific-and-global]
endpoint_url = http://localhost:1234
services = s3-specific

[services s3-specific]
s3 =
  endpoint_url = https://play.min.io:9000
```

단일 프로파일로 여러 서비스에 대한 엔드포인트를 구성할 수 있습니다. 이 예제에서는 동일한 프로파일에서 Amazon S3 및 AWS Elastic Beanstalk 에 대한 서비스별 엔드포인트 URLs을 설정하는 방법을 보여줍니다. `serviceId`의 AWS Elastic Beanstalk 가 있습니다 [Elastic Beanstalk](#). AWS 서비스 식별자는 모든 공백을 밑줄로 바꾸고 모든 문자를 소문자로 대체 `serviceId`하여 API 모델의 기반으로 합니다. 따라서 서비스 식별자 키가 `elastic_beanstalk`가 되고 이 서비스에 대한 설정이 `elastic_beanstalk = 줄에서 시작됩니다`. `services` 섹션에서 사용할 모든 서비스 식별자 키 목록은 [서비스별 엔드포인트 식별자](#)을 참조하십시오.

```
[services testing-s3-and-eb]
s3 =
  endpoint_url = http://localhost:4567
elastic_beanstalk =
  endpoint_url = http://localhost:8000

[profile dev]
services = testing-s3-and-eb
```

서비스 구성 섹션은 여러 프로파일에서 사용할 수 있습니다. 예를 들어 두 프로파일이 동일한 `services` 정의를 사용하면서 다른 프로파일 속성을 변경할 수 있습니다.

```
[services testing-s3]
s3 =
  endpoint_url = https://localhost:4567

[profile testing-json]
output = json
services = testing-s3

[profile testing-text]
output = text
services = testing-s3
```

## 역할 기반 보안 인증을 사용하여 프로파일의 엔드포인트 구성

프로파일에 역할 기반 보안 인증 정보가 IAM 가정 역할 기능에 대한 `source_profile` 파라미터를 통해 구성된 경우 SDK는 지정된 프로파일에 대한 서비스 구성만 사용합니다. 역할이 연결된 프로파일은 사용하지 않습니다. 예를 들어 다음과 같은 공유 config 파일을 사용합니다.

```
[profile A]
credential_source = Ec2InstanceMetadata
```

```

endpoint_url = https://profile-a-endpoint.aws/

[profile B]
source_profile = A
role_arn = arn:aws:iam::123456789012:role/roleB
services = profileB

[services profileB]
ec2 =
  endpoint_url = https://profile-b-ec2-endpoint.aws

```

프로파일 B를 사용하고 코드에서 Amazon EC2로 직접 호출하는 경우 엔드포인트는 `https://profile-b-ec2-endpoint.aws`로 확인됩니다. 코드에서 다른 서비스에 요청을 하는 경우 엔드포인트 확인은 사용자 지정 로직을 따르지 않습니다. 엔드포인트는 프로파일 A에 정의된 글로벌 엔드포인트로 확인되지 않습니다. 글로벌 엔드포인트가 프로파일 B에 적용되려면 프로파일 B 내에서 직접 `endpoint_url`을 설정해야 합니다. `source_profile` 설정에 대한 자세한 내용은 [역할 보안 인증제 공자 수입](#) 단원을 참조하십시오.

## 설정의 우선 순위

이 기능의 설정은 동시에 사용할 수 있지만 서비스당 하나의 값만 우선합니다. 지정된에 대한 API 호출 AWS 서비스의 경우 다음 순서가 값을 선택하는 데 사용됩니다.

1. 코드나 서비스 클라이언트 자체에 설정된 모든 명시적 설정은 다른 모든 설정보다 우선합니다.
  - 의 경우 `--endpoint-url` 명령줄 파라미터에서 제공하는 값 AWS CLI입니다. SDK의 경우 명시적 할당은 AWS 서비스 클라이언트 또는 구성 객체를 인스턴스화할 때 설정한 파라미터의 형태를 취할 수 있습니다.
2. 서비스별 환경 변수에서 제공하는 값(예: `AWS_ENDPOINT_URL_DYNAMODB`).
3. `AWS_ENDPOINT_URL` 글로벌 엔드포인트 환경 변수에 의해 제공되는 값입니다.
4. 공유 config 파일의 `services` 섹션 내에 서비스 식별자 키 아래 중첩된 `endpoint_url` 설정에서 제공하는 값.
5. 공유 config 파일의 `profile` 내에서 직접 지정된 `endpoint_url` 설정에 의해 제공되는 값.
6. 각의 기본 엔드포인트 URL AWS 서비스 이 마지막으로 사용됩니다.

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지 운 통	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	예	
<a href="#">SDK for C++</a>	예	
<a href="#">SDK for Go V2 (1.x)</a>	예	
<a href="#">SDK for Go 1.x (V1)</a>	아 니 요	
<a href="#">SDK for Java 2.x</a>	예	
<a href="#">SDK for Java 1.x</a>	아 니 요	
<a href="#">SDK for JavaScript 3.x</a>	예	
<a href="#">SDK for JavaScript 2.x</a>	아 니 요	
<a href="#">SDK for Kotlin</a>	예	
<a href="#">.NET 4.x용 SDK</a>	예	
<a href="#">SDK for .NET 3.x</a>	예	
<a href="#">SDK for PHP 3.x</a>	예	
<a href="#">SDK for Python (Boto3)</a>	예	
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	예	

SDK	자 운 톤	참고 또는 추가 정보
<a href="#">SDK for Swift</a>	예	
<a href="#">PowerShell V5용 도구</a>	예	
<a href="#">PowerShell V4용 도구</a>	예	

## 서비스별 엔드포인트 식별자

다음 표의 식별자를 사용하는 방법 및 위치에 대한 자세한 내용은 [서비스별 엔드포인트](#) 섹션을 참조하십시오.

serviceId	공 유 식 별 자	환경 변수
AccessAnalyzer	a 1	AWS_ENDPOINT_URL_ACCESSANALYZER
Account	a	AWS_ENDPOINT_URL_ACCOUNT
ACM	a	AWS_ENDPOINT_URL_ACM

serviceId	공유 서비스별 환경 변수
ACM PCA	aws_aws_endpoint_url_acm_pca
Alexa For Business	aws_aws_endpoint_url_alexa_for_business
amp	aws_aws_endpoint_url_amp
Amplify	aws_aws_endpoint_url_amplify
AmplifyBackend	aws_aws_endpoint_url_amplifybackend
AmplifyUIBuilder	aws_aws_endpoint_url_amplifyuibuilder
API Gateway	aws_aws_endpoint_url_api_gateway
ApiGatewayManagementApi	aws_aws_endpoint_url_apigatewaymanagementapi

serviceId	공유 서비스별 환경 변수
ApiGatewayV2	API_AWS_ENDPOINT_URL_APIGATEWAYV2
AppConfig	API_AWS_ENDPOINT_URL_APPCONFIG
AppConfigData	API_AWS_ENDPOINT_URL_APPCONFIGDATA
AppFabric	API_AWS_ENDPOINT_URL_APPFABRIC
Appflow	API_AWS_ENDPOINT_URL_APPFLOW
AppIntegrations	API_AWS_ENDPOINT_URL_APPINTEGRATIONS
Application Auto Scaling	API_AWS_ENDPOINT_URL_APPLICATION_AUTO_SCALING

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서비스별 자크
Application Insights	a) AWS_ENDPOINT_URL_APPLICATION_INSIGHTS 이 t:
ApplicationCostProfiler	a) AWS_ENDPOINT_URL_APPLICATIONCOSTPROFILER 이 f:
App Mesh	a) AWS_ENDPOINT_URL_APP_MESH
AppRunner	a) AWS_ENDPOINT_URL_APPRUNNER
AppStream	a) AWS_ENDPOINT_URL_APPSTREAM
AppSync	a) AWS_ENDPOINT_URL_APPS_SYNC
ARC Zonal Shift	a: AWS_ENDPOINT_URL_ARC_ZONAL_SHIFT _:
Artifact	a: AWS_ENDPOINT_URL_ARTIFACT

<b>serviceId</b>	<b>공공 유시 코드 파일 이름의 서비스별 별칭</b>	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt; 환경 변수</b>
Athena	a:	AWS_ENDPOINT_URL_ATHENA
AuditManager	a:	AWS_ENDPOINT_URL_AUDITMANAGER
Auto Scaling	a:	AWS_ENDPOINT_URL_AUTO_SCALING
Auto Scaling Plans	a:	AWS_ENDPOINT_URL_AUTO_SCALING_PLANS
b2bi	b:	AWS_ENDPOINT_URL_B2BI
Backup	b:	AWS_ENDPOINT_URL_BACKUP
Backup Gateway	b:	AWS_ENDPOINT_URL_BACKUP_GATEWAY
BackupStorage	b:	AWS_ENDPOINT_URL_BACKUPSTORAGE
Batch	b:	AWS_ENDPOINT_URL_BATCH

<b>serviceId</b>	공공 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일 시스템 별칭
BCM Data Exports	b: AWS_ENDPOINT_URL_BCM_DATA_EXPORTS e:
Bedrock	b: AWS_ENDPOINT_URL_BEDROCK
Bedrock Agent	b: AWS_ENDPOINT_URL_BEDROCK_AGENT g:
Bedrock Agent Runtime	b: AWS_ENDPOINT_URL_BEDROCK_AGENT_RUNTIME g: ir
Bedrock Runtime	b: AWS_ENDPOINT_URL_BEDROCK_RUNTIME ur
billingconductor	b: AWS_ENDPOINT_URL_BILLINGCONDUCTOR nc
Braket	b: AWS_ENDPOINT_URL_BRAKET
Budgets	b: AWS_ENDPOINT_URL_BUDGETS

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서브스택별 자크
Cost Explorer	AWS_ENDPOINT_URL_COST_EXPLORER
chatbot	AWS_ENDPOINT_URL_CHATBOT
Chime	AWS_ENDPOINT_URL_CHIME
Chime SDK Identity	AWS_ENDPOINT_URL_CHIME_SDK_IDENTITY
Chime SDK Media Pipelines	AWS_ENDPOINT_URL_CHIME_SDK_MEDIA_PIPELINES
Chime SDK Meetings	AWS_ENDPOINT_URL_CHIME_SDK_MEETINGS
Chime SDK Messaging	AWS_ENDPOINT_URL_CHIME_SDK_MESSAGING

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
Chime SDK Voice	c:\AWS_ENDPOINT_URL_CHIME_SDK_VOICE_
CleanRooms	c:\AWS_ENDPOINT_URL_CLEANROOMS
CleanRoomsML	c:\AWS_ENDPOINT_URL_CLEANROOMSML
Cloud9	c:\AWS_ENDPOINT_URL_CLOUD9
CloudControl	c:\AWS_ENDPOINT_URL_CLOUDCONTROL
CloudDirectory	c:\AWS_ENDPOINT_URL_CLOUDDIRECTORY
CloudFormation	c:\AWS_ENDPOINT_URL_CLOUDFORMATION
CloudFront	c:\AWS_ENDPOINT_URL_CLOUDFRONT

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서비스별 자크
CloudFront KeyValueStore	c: AWS_ENDPOINT_URL_CLOUDFRONT_KEYVALUESTORE_t_e:
CloudHSM	c: AWS_ENDPOINT_URL_CLOUDHSM
CloudHSM V2	c: AWS_ENDPOINT_URL_CLOUDHSM_V2_v:
CloudSearch	c: AWS_ENDPOINT_URL_CLOUDSEARCH_c:
CloudSearch Domain	c: AWS_ENDPOINT_URL_CLOUDSEARCH_DOMAIN_c:
CloudTrail	c: AWS_ENDPOINT_URL_CLOUDTRAIL_l:
CloudTrail Data	c: AWS_ENDPOINT_URL_CLOUDTRAIL_DATA_l.

<b>serviceId</b>	공 유 시 스템 의 서 버 스 별 자 크	환경 변수
CloudWatch	c h	AWS_ENDPOINT_URL_CLOUDWATCH
codeartifact	c a	AWS_ENDPOINT_URL_CODEARTIFACT
CodeBuild	c	AWS_ENDPOINT_URL_CODEBUILD
CodeCatalyst	c y	AWS_ENDPOINT_URL_CODECATALYST
CodeCommit	c t	AWS_ENDPOINT_URL_CODECOMMIT
CodeDeploy	c y	AWS_ENDPOINT_URL_CODEDEPLOY
CodeGuru Reviewer	c r	AWS_ENDPOINT_URL_CODEGURU_REVIEWER
CodeGuru Security	c s	AWS_ENDPOINT_URL_CODEGURU_SECURITY

<b>serviceId</b>	<b>공용 환경 변수</b>
	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt;</b>
CodeGuruProfiler	AWS_ENDPOINT_URL_CODEGURUPROFILER
CodePipeline	AWS_ENDPOINT_URL_CODEPIPELINE
CodeStar	AWS_ENDPOINT_URL_CODESTAR
CodeStar connections	AWS_ENDPOINT_URL_CODESTAR_CONNECTIONS
codestar notifications	AWS_ENDPOINT_URL_CODESTAR_NOTIFICATIONS
Cognito Identity	AWS_ENDPOINT_URL_COGNITO_IDENTITY
Cognito Identity Provider	AWS_ENDPOINT_URL_COGNITO_IDENTITY_PROVIDER

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
Cognito Sync	cognit sync AWS_ENDPOINT_URL_COGNITO_SYNC
Comprehend	comprehend AWS_ENDPOINT_URL_COMPREHEND
ComprehendMedical	comprehend medical AWS_ENDPOINT_URL_COMPREHENDMEDICAL
Compute Optimizer	compute optimizer AWS_ENDPOINT_URL_COMPUTE_OPTIMIZER
Config Service	config service AWS_ENDPOINT_URL_CONFIG_SERVICE
Connect	connect AWS_ENDPOINT_URL_CONNECT
Connect Contact Lens	connect contact lens AWS_ENDPOINT_URL_CONNECT_CONTACT_LENS
ConnectCampaigns	connect campaigns AWS_ENDPOINT_URL_CONNECTCAMPAIGNS

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
ConnectCases	c: AWS_ENDPOINT_URL_CONNECTCASES s:
ConnectParticipant	c: AWS_ENDPOINT_URL_CONNECTPARTICIPANT r:
ControlTower	c: AWS_ENDPOINT_URL_CONTROLTOWER w:
Cost Optimization Hub	c: AWS_ENDPOINT_URL_COST_OPTIMIZATION_HUB m: h:
Cost and Usage Report Service	c: AWS_ENDPOINT_URL_COST_AND_USAGE_REPO u: RT_SERVICE o: c:
Customer Profiles	c: AWS_ENDPOINT_URL_CUSTOMER_PROFILES p:
DataBrew	d: AWS_ENDPOINT_URL_DATABREW

serviceId	공용 서비스 디폴트 서비스 별칭 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
DataExchange	d: AWS_ENDPOINT_URL_DATAEXCHANGE
Data Pipeline	d: AWS_ENDPOINT_URL_DATA_PIPELINE
DataSync	d: AWS_ENDPOINT_URL_DATASYNC
DataZone	d: AWS_ENDPOINT_URL_DATAZONE
DAX	d: AWS_ENDPOINT_URL_DAX
Detective	d: AWS_ENDPOINT_URL_DETECTIVE
Device Farm	d: AWS_ENDPOINT_URL_DEVICE_FARM
DevOps Guru	d: AWS_ENDPOINT_URL_DEVOPS_GURU
Direct Connect	d: AWS_ENDPOINT_URL_DIRECT_CONNECT

serviceId	공공 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
Application Discovery Service	a) AWS_ENDPOINT_URL_APPLICATION_DISCOVERY_SERVICE
DLM	d) AWS_ENDPOINT_URL_DLM
Database Migration Service	d) AWS_ENDPOINT_URL_DATABASE_MIGRATION_SERVICE
DocDB	d) AWS_ENDPOINT_URL_DOCDB
DocDB Elastic	d) AWS_ENDPOINT_URL_DOCDB_ELASTIC
drs	d) AWS_ENDPOINT_URL_DRS
Directory Service	d) AWS_ENDPOINT_URL_DIRECTORY_SERVICE
DynamoDB	d) AWS_ENDPOINT_URL_DYNAMODB

serviceId	공용 엔드포인트 URL <SERVICE> 환경 변수
DynamoDB Streams	dynamodb-streams AWS_ENDPOINT_URL_DYNAMODB_STREAMS
EBS	ebs AWS_ENDPOINT_URL_EBS
EC2	ec2 AWS_ENDPOINT_URL_EC2
EC2 Instance Connect	ec2-instance-connect AWS_ENDPOINT_URL_EC2_INSTANCE_CONNECT
ECR	ecr AWS_ENDPOINT_URL_ECR
ECR PUBLIC	ecr-public AWS_ENDPOINT_URL_ECR_PUBLIC
ECS	ecs AWS_ENDPOINT_URL_ECS
EFS	efs AWS_ENDPOINT_URL_EFS
EKS	eks AWS_ENDPOINT_URL_EKS
EKS Auth	eks-auth AWS_ENDPOINT_URL_EKS_AUTH

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서비스별 자카
Elastic Inference	e: AWS_ENDPOINT_URL_ELASTIC_INFERENCE n:
ElastiCache	e: AWS_ENDPOINT_URL_ELASTICACHE h:
Elastic Beanstalk	e: AWS_ENDPOINT_URL_ELASTIC_BEANSTALK e:
Elastic Transcoder	e: AWS_ENDPOINT_URL_ELASTIC_TRANSCODER r:
Elastic Load Balancing	e: AWS_ENDPOINT_URL_ELASTIC_LOAD_BALANCING o: c:
Elastic Load Balancing v2	e: AWS_ENDPOINT_URL_ELASTIC_LOAD_BALANCING_V2 o: c:
EMR	er: AWS_ENDPOINT_URL_EMR

<b>serviceId</b>	공 유 시 드 파 일 으 서 버 스 스 별 자 크	환경 변수
EMR containers	er i:	AWS_ENDPOINT_URL_EMR_CONTAINERS
EMR Serverless	er r:	AWS_ENDPOINT_URL_EMR_SERVERLESS
EntityResolution	er o:	AWS_ENDPOINT_URL_ENTITYRESOLUTION
Elasticsearch Service	e: a: i:	AWS_ENDPOINT_URL_ELASTICSEARCH_SERVICE
EventBridge	e: g:	AWS_ENDPOINT_URL_EVENTBRIDGE
Evidently	e:	AWS_ENDPOINT_URL_EVIDENTLY
finspace	f:	AWS_ENDPOINT_URL_FINSPEACE
finspace data	f: d:	AWS_ENDPOINT_URL_FINSPEACE_DATA

serviceId	공공 유시 CIP 일 으 서 비 스 스 별 자 쿨 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
Firehose	f: AWS_ENDPOINT_URL_FIREHOSE
fis	f: AWS_ENDPOINT_URL_FIS
FMS	fr AWS_ENDPOINT_URL_FMS
forecast	fo AWS_ENDPOINT_URL_FORECAST
forecastquery	fo AWS_ENDPOINT_URL_FORECASTQUERY ur
FraudDetector	f: AWS_ENDPOINT_URL_FRAUDETECTOR cl
FreeTier	f: AWS_ENDPOINT_URL_FREETIER
FSx	f: AWS_ENDPOINT_URL_FSX
GameLift	g: AWS_ENDPOINT_URL_GAMELIFT
Glacier	g: AWS_ENDPOINT_URL_GLACIER

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서비스별 자식
Global Accelerator	g: AWS_ENDPOINT_URL_GLOBAL_ACCELERATOR c:
Glue	g: AWS_ENDPOINT_URL_GLUE
grafana	g: AWS_ENDPOINT_URL_GRAFANA
Greengrass	g: AWS_ENDPOINT_URL_GREENGRASS s
GreengrassV2	g: AWS_ENDPOINT_URL_GREENGRASSV2 s\
GroundStation	g: AWS_ENDPOINT_URL_GROUNDSTATION t:
GuardDuty	g: AWS_ENDPOINT_URL_GUARDDUTY
Health	h: AWS_ENDPOINT_URL_HEALTH

serviceId	공유 서비스별 환경 변수
HealthLake	health AWS_ENDPOINT_URL_HEALTHLAKE
Honeycode	honeycode AWS_ENDPOINT_URL_HONEYCODE
IAM	iam AWS_ENDPOINT_URL_IAM
identitystore	identitystore AWS_ENDPOINT_URL_IDENTITYSTORE
imagebuilder	imagebuilder AWS_ENDPOINT_URL_IMAGEBUILDER
ImportExport	importexport AWS_ENDPOINT_URL_IMPORTEXPORT
Inspector	inspector AWS_ENDPOINT_URL_INSPECTOR
Inspector Scan	inspector-scan AWS_ENDPOINT_URL_INSPECTOR_SCAN

serviceId	공유 서비스 디폴트 서비스별 자카 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
Inspector2	i: AWS_ENDPOINT_URL_INSPECTOR2
InternetMonitor	i: AWS_ENDPOINT_URL_INTERNETMONITOR
IoT	i: AWS_ENDPOINT_URL_IOT
IoT Data Plane	i: AWS_ENDPOINT_URL_IOT_DATA_PLANE
IoT Jobs Data Plane	i: AWS_ENDPOINT_URL_IOT_JOBS_DATA_PLANE
IoT 1Click Devices Service	i: AWS_ENDPOINT_URL_IOT_1CLICK_DEVICES_SERVICE
IoT 1Click Projects	i: AWS_ENDPOINT_URL_IOT_1CLICK_PROJECTS

<b>serviceId</b>	<b>공유 서비스별 자카</b>	<b>AWS_ENDPOINT_URL_&lt;SERVICE&gt; 환경 변수</b>
IoTAnalytics	iota	AWS_ENDPOINT_URL_IOTANALYTICS
IotDeviceAdvisor	advisor	AWS_ENDPOINT_URL_IOTDEVICEADVISOR
IoT Events	events	AWS_ENDPOINT_URL_IOT_EVENTS
IoT Events Data	events-data	AWS_ENDPOINT_URL_IOT_EVENTS_DATA
IoTFleetHub	fleet	AWS_ENDPOINT_URL_IOTFLEETHUB
IoTFleetWise	fleetwise	AWS_ENDPOINT_URL_IOTFLEETWISE
IoTSecureTunneling	secure-tunneling	AWS_ENDPOINT_URL_IOTSECURETUNNELING

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일 시스템 서비스별 자크
IoTSiteWise	i: AWS_ENDPOINT_URL_IOTSITEWISE s:
IoTThingsGraph	i: AWS_ENDPOINT_URL_IOTTHINGSGRAPH g:
IoTTwinMaker	i: AWS_ENDPOINT_URL_IOTTWINMAKER k:
IoT Wireless	i: AWS_ENDPOINT_URL_IOT_WIRELESS e:
ivs	i: AWS_ENDPOINT_URL_IVS
IVS RealTime	i: AWS_ENDPOINT_URL_IVS_REALTIME ir
ivschat	i: AWS_ENDPOINT_URL_IVSCHAT
Kafka	k: AWS_ENDPOINT_URL_KAFKA
KafkaConnect	k: AWS_ENDPOINT_URL_KAFKACONNECT e:

<b>serviceId</b>	공 유 시 드 파 일 으 서 버 스 스 별 자 크	환경 변수
kendra	k	AWS_ENDPOINT_URL_KENDRA
Kendra Ranking	k	AWS_ENDPOINT_URL_KENDRA_RANKING
Keyspaces	k	AWS_ENDPOINT_URL_KEYSPACES
Kinesis	k	AWS_ENDPOINT_URL_KINESIS
Kinesis Video Archived Media	k	AWS_ENDPOINT_URL_KINESIS_VIDEO_ARCHIVED_MEDIA
Kinesis Video Media	k	AWS_ENDPOINT_URL_KINESIS_VIDEO_MEDIA
Kinesis Video Signaling	k	AWS_ENDPOINT_URL_KINESIS_VIDEO_SIGNALING

serviceId	공유 서비스별 환경 변수
Kinesis Video WebRTC Storage	k: AWS_ENDPOINT_URL_KINESIS_VIDEO_WEBRTC i: C_STORAGE t: e
Kinesis Analytics	k: AWS_ENDPOINT_URL_KINESIS_ANALYTICS n:
Kinesis Analytics V2	k: AWS_ENDPOINT_URL_KINESIS_ANALYTICS_V2 n: v:
Kinesis Video	k: AWS_ENDPOINT_URL_KINESIS_VIDEO i:
KMS	k: AWS_ENDPOINT_URL_KMS
LakeFormation	l: AWS_ENDPOINT_URL_LAKEFORMATION t:
Lambda	l: AWS_ENDPOINT_URL_LAMBDA

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
Launch Wizard	Launch Wizard 서비스의 엔드포인트 URL을 지정하는 환경 변수입니다. 예: <code>AWS_ENDPOINT_URL_LAUNCH_WIZARD</code>
Lex Model Building Service	Lex Model Building 서비스의 엔드포인트 URL을 지정하는 환경 변수입니다. 예: <code>AWS_ENDPOINT_URL_LEX_MODEL_BUILDING_SERVICE</code>
Lex Runtime Service	Lex Runtime 서비스의 엔드포인트 URL을 지정하는 환경 변수입니다. 예: <code>AWS_ENDPOINT_URL_LEX_RUNTIME_SERVICE</code>
Lex Models V2	Lex Models V2 서비스의 엔드포인트 URL을 지정하는 환경 변수입니다. 예: <code>AWS_ENDPOINT_URL_LEX_MODELS_V2</code>
Lex Runtime V2	Lex Runtime V2 서비스의 엔드포인트 URL을 지정하는 환경 변수입니다. 예: <code>AWS_ENDPOINT_URL_LEX_RUNTIME_V2</code>
License Manager	License Manager 서비스의 엔드포인트 URL을 지정하는 환경 변수입니다. 예: <code>AWS_ENDPOINT_URL_LICENSE_MANAGER</code>

serviceId	공공 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유사 디렉토리 파일 의 서브 스 브 별 자 크
License Manager Linux Subscriptions	l: AWS_ENDPOINT_URL_LICENSE_MANAGER_LIN a: UX_SUBSCRIPTIONS n: r:
License Manager User Subscriptions	l: AWS_ENDPOINT_URL_LICENSE_MANAGER_USE a: R_SUBSCRIPTIONS e: i:
Lightsail	l: AWS_ENDPOINT_URL_LIGHTSAIL
Location	l: AWS_ENDPOINT_URL_LOCATION
CloudWatch Logs	c: AWS_ENDPOINT_URL_CLOUDWATCH_LOGS h:
LookoutEquipment	l: AWS_ENDPOINT_URL_LOOKOUTEQUIPMENT u:
LookoutMetrics	l: AWS_ENDPOINT_URL_LOOKOUTMETRICS t:

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
LookoutVision	LookoutVision: AWS_ENDPOINT_URL_LOOKOUTVISION
m2	m2: AWS_ENDPOINT_URL_M2
Machine Learning	machine-learning: AWS_ENDPOINT_URL_MACHINE_LEARNING
Macie2	macie2: AWS_ENDPOINT_URL_MACIE2
ManagedBlockchain	managed-blockchain: AWS_ENDPOINT_URL_MANAGEDBLOCKCHAIN
ManagedBlockchain Query	managed-blockchain-query: AWS_ENDPOINT_URL_MANAGEDBLOCKCHAIN_QUERY
Marketplace Agreement	marketplace-agreement: AWS_ENDPOINT_URL_MARKETPLACE_AGREEMENT

serviceId	공공 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
Marketplace Catalog	m: AWS_ENDPOINT_URL_MARKETPLACE_CATALOG c: g
Marketplace Deployment	m: AWS_ENDPOINT_URL_MARKETPLACE_DEPLOYMENT c: m
Marketplace Entitlement Service	m: AWS_ENDPOINT_URL_MARKETPLACE_ENTITLEMENT_SERVICE c: er v:
Marketplace Commerce Analytics	m: AWS_ENDPOINT_URL_MARKETPLACE_COMMERCE_ANALYTICS c: c i:
MediaConnect	m: AWS_ENDPOINT_URL_MEDIACONNECT c: e

serviceId	공유 서비스별 환경 변수
MediaConvert	AWS_ENDPOINT_URL_MEDIACONVERT
MediaLive	AWS_ENDPOINT_URL_MEDIALIVE
MediaPackage	AWS_ENDPOINT_URL_MEDIAPACKAGE
MediaPackage Vod	AWS_ENDPOINT_URL_MEDIAPACKAGE_VOD
MediaPackageV2	AWS_ENDPOINT_URL_MEDIAPACKAGEV2
MediaStore	AWS_ENDPOINT_URL_MEDIASTORE
MediaStore Data	AWS_ENDPOINT_URL_MEDIASTORE_DATA
MediaTailor	AWS_ENDPOINT_URL_MEDIATAILOR

<b>serviceId</b>	공 유 시 디 파 일 으 서 비 스 스 별 자 크	환경 변수
Medical Imaging	m: m:	AWS_ENDPOINT_URL_MEDICAL_IMAGING
MemoryDB	m:	AWS_ENDPOINT_URL_MEMORYDB
Marketplace Metering	m: c: n:	AWS_ENDPOINT_URL_MARKETPLACE_METERING
Migration Hub	m: _l	AWS_ENDPOINT_URL_MIGRATION_HUB
mgn	m:	AWS_ENDPOINT_URL_MGN
Migration Hub Refactor Spaces	m: c: e:	AWS_ENDPOINT_URL_MIGRATION_HUB_REFACTOR_SPACES
MigrationHub Config	m: h: g	AWS_ENDPOINT_URL_MIGRATIONHUB_CONFIG

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서비스별 자크
MigrationHubOrchestrator	m: AWS_ENDPOINT_URL_MIGRATIONHUBORCHESTRATOR h t:
MigrationHubStrategy	m: AWS_ENDPOINT_URL_MIGRATIONHUBSTRATEGY h g:
Mobile	m: AWS_ENDPOINT_URL_MOBILE
mq	m: AWS_ENDPOINT_URL_MQ
MTurk	m: AWS_ENDPOINT_URL_MTURK
MWAA	m: AWS_ENDPOINT_URL_MWAA
Neptune	n: AWS_ENDPOINT_URL_NEPTUNE
Neptune Graph	n: AWS_ENDPOINT_URL_NEPTUNE_GRAPH r:
neptunedata	n: AWS_ENDPOINT_URL_NEPTUNEDATA t:

serviceId	공용 유식 디파일의 서브스택별 자카	AWS_ENDPOINT_URL_<SERVICE> 환경 변수
Network Firewall	n: AWS_ENDPOINT_URL_NETWORK_FIREWALL	
NetworkManager	n: AWS_ENDPOINT_URL_NETWORKMANAGER	
NetworkMonitor	n: AWS_ENDPOINT_URL_NETWORKMONITOR	
nimble	n: AWS_ENDPOINT_URL_NIMBLE	
OAM	o: AWS_ENDPOINT_URL_OAM	
Omics	o: AWS_ENDPOINT_URL_OMICS	
OpenSearch	o: AWS_ENDPOINT_URL_OPENSEARCH	
OpenSearchServerless	o: AWS_ENDPOINT_URL_OPENSEARCHSERVERLESS	
OpsWorks	o: AWS_ENDPOINT_URL_OPSWORKS	

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
OpsWorksCM	o: AWS_ENDPOINT_URL_OPSWORKSCM
Organizations	o: AWS_ENDPOINT_URL_ORGANIZATIONS
OSIS	o: AWS_ENDPOINT_URL_OSIS
Outposts	o: AWS_ENDPOINT_URL_OUTPOSTS
p8data	p: AWS_ENDPOINT_URL_P8DATA
p8data	p: AWS_ENDPOINT_URL_P8DATA
Panorama	p: AWS_ENDPOINT_URL_PANORAMA
Payment Cryptography	p: AWS_ENDPOINT_URL_PAYMENT_CRYPTOGRAPHY
Payment Cryptography Data	p: AWS_ENDPOINT_URL_PAYMENT_CRYPTOGRAPHY_DATA

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
Pca Connector Ad	p: AWS_ENDPOINT_URL_PCA_CONNECTOR_AD
Personalize	p: AWS_ENDPOINT_URL_PERSONALIZE
Personalize Events	p: AWS_ENDPOINT_URL_PERSONALIZE_EVENTS
Personalize Runtime	p: AWS_ENDPOINT_URL_PERSONALIZE_RUNTIME
PI	p: AWS_ENDPOINT_URL_PI
Pinpoint	p: AWS_ENDPOINT_URL_PINPOINT
Pinpoint Email	p: AWS_ENDPOINT_URL_PINPOINT_EMAIL

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일 시스템 별칭
Pinpoint SMS Voice	p: AWS_ENDPOINT_URL_PINPOINT_SMS_VOICE sr
Pinpoint SMS Voice V2	p: AWS_ENDPOINT_URL_PINPOINT_SMS_VOICE_V2 sr _\'
Pipes	p: AWS_ENDPOINT_URL_PIPES
Polly	p: AWS_ENDPOINT_URL_POLLY
Pricing	p: AWS_ENDPOINT_URL_PRICING
PrivateNetworks	p: AWS_ENDPOINT_URL_PRIVATENETWORKS tv
Proton	p: AWS_ENDPOINT_URL_PROTON
QBusiness	q: AWS_ENDPOINT_URL_QBUSINESS
QConnect	q: AWS_ENDPOINT_URL_QCONNECT

<b>serviceId</b>	공 유 시 스템 의 서 버 스 스 별 자 크	환경 변수
QLDB	q	AWS_ENDPOINT_URL_QLDB
QLDB Session	q i	AWS_ENDPOINT_URL_QLDB_SESSION
QuickSight	q t	AWS_ENDPOINT_URL_QUICKSIGHT
RAM	r	AWS_ENDPOINT_URL_RAM
rbin	r	AWS_ENDPOINT_URL_RBIN
RDS	r	AWS_ENDPOINT_URL_RDS
RDS Data	r	AWS_ENDPOINT_URL_RDS_DATA
Redshift	r	AWS_ENDPOINT_URL_REDSHIFT
Redshift Data	r d	AWS_ENDPOINT_URL_REDSHIFT_DATA
Redshift Serverless	r s s	AWS_ENDPOINT_URL_REDSHIFT_SERVERLESS

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서브스택별 자크
Rekognition	r AWS_ENDPOINT_URL_REKOGNITION o
repostspace	r AWS_ENDPOINT_URL_REPOSTSPACE c
resiliencehub	r AWS_ENDPOINT_URL_RESILIENCEHUB e
Resource Explorer 2	r AWS_ENDPOINT_URL_RESOURCE_EXPLORER_2 e 2
Resource Groups	r AWS_ENDPOINT_URL_RESOURCE_GROUPS g
Resource Groups Tagging API	r AWS_ENDPOINT_URL_RESOURCE_GROUPS_TAG g: GING_API g
RoboMaker	r AWS_ENDPOINT_URL_ROBOMAKER

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일 시스템 별칭
RolesAnywhere	r AWS_ENDPOINT_URL_ROLESANYPWHERE h
Route 53	r AWS_ENDPOINT_URL_ROUTE_53
Route53 Recovery Cluster	r AWS_ENDPOINT_URL_ROUTE53_RECOVERY_CLUSTER e l
Route53 Recovery Control Config	r AWS_ENDPOINT_URL_ROUTE53_RECOVERY_CO e NTROL_CONFIG o n
Route53 Recovery Readiness	r AWS_ENDPOINT_URL_ROUTE53_RECOVERY_RE e ADINESS e
Route 53 Domains	r AWS_ENDPOINT_URL_ROUTE_53_DOMAINS d
Route53Resolver	r AWS_ENDPOINT_URL_ROUTE53RESOLVER s

serviceId	공유 서비스 디폴트 서비스별 자카 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
RUM	AWS_ENDPOINT_URL_RUM
S3	AWS_ENDPOINT_URL_S3
S3 Control	AWS_ENDPOINT_URL_S3_CONTROL
S3Outposts	AWS_ENDPOINT_URL_S3OUTPOSTS
SageMaker	AWS_ENDPOINT_URL_SAGEMAKER
SageMaker A2I Runtime	AWS_ENDPOINT_URL_SAGEMAKER_A2I_RUNTIME
Sagemaker Edge	AWS_ENDPOINT_URL_SAGEMAKER_EDGE

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수
SageMaker FeatureStore Runtime	s: AWS_ENDPOINT_URL_SAGEMAKER_FEATURESTORE_RUNTIME
SageMaker Geospatial	s: AWS_ENDPOINT_URL_SAGEMAKER_GEOSPATIAL
SageMaker Metrics	s: AWS_ENDPOINT_URL_SAGEMAKER_METRICS
SageMaker Runtime	s: AWS_ENDPOINT_URL_SAGEMAKER_RUNTIME
savingsplans	s: AWS_ENDPOINT_URL_SAVINGSPLANS
Scheduler	s: AWS_ENDPOINT_URL_SCHEDULER
schemas	s: AWS_ENDPOINT_URL_SCHEMAS

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일 시스템 서비스별 자크
SimpleDB	s: AWS_ENDPOINT_URL_SIMPLEDB
Secrets Manager	s: AWS_ENDPOINT_URL_SECRETS_MANAGER a:
SecurityHub	s: AWS_ENDPOINT_URL_SECURITYHUB u:
SecurityLake	s: AWS_ENDPOINT_URL_SECURITYLAKE a:
ServerlessApplicationRepository	s: AWS_ENDPOINT_URL_SERVERLESSAPPLICATI s: ONREPOSITORY i: t:
Service Quotas	s: AWS_ENDPOINT_URL_SERVICE_QUOTAS u:
Service Catalog	s: AWS_ENDPOINT_URL_SERVICE_CATALOG a:

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서비스별 자크
Service Catalog AppRegistry	s: AWS_ENDPOINT_URL_SERVICE_CATALOG_APP a: REGISTRY p:
ServiceDiscovery	s: AWS_ENDPOINT_URL_SERVICEDISCOVERY s:
SES	s: AWS_ENDPOINT_URL_SES
SESV2	s: AWS_ENDPOINT_URL_SESV2
Shield	s: AWS_ENDPOINT_URL_SHIELD
signer	s: AWS_ENDPOINT_URL_SIGNER
SimSpaceWeaver	s: AWS_ENDPOINT_URL_SIMSPACEWEAVER e:
SMS	s: AWS_ENDPOINT_URL_SMS

serviceId	공공 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서비스별 자카
Snow Device Management	s: AWS_ENDPOINT_URL_SNOW_DEVICE_MANAGEMENT
Snowball	s: AWS_ENDPOINT_URL_SNOWBALL
SNS	s: AWS_ENDPOINT_URL_SNS
SQS	s: AWS_ENDPOINT_URL_SQS
SSM	s: AWS_ENDPOINT_URL_SSM
SSM Contacts	s: AWS_ENDPOINT_URL_SSM_CONTACTS
SSM Incidents	s: AWS_ENDPOINT_URL_SSM_INCIDENTS
Ssm Sap	s: AWS_ENDPOINT_URL_SSM_SAP
SSO	s: AWS_ENDPOINT_URL_SSO
SSO Admin	s: AWS_ENDPOINT_URL_SSO_ADMIN

<b>serviceId</b>	<b>공유 서비스별 환경 변수</b>
SSO OIDC	s: AWS_ENDPOINT_URL_SSO_OIDC
SFN	s: AWS_ENDPOINT_URL_SFN
Storage Gateway	s: AWS_ENDPOINT_URL_STORAGE_GATEWAY a:
STS	s: AWS_ENDPOINT_URL_STS
SupplyChain	s: AWS_ENDPOINT_URL_SUPPLYCHAIN i:
Support	s: AWS_ENDPOINT_URL_SUPPORT
Support App	s: AWS_ENDPOINT_URL_SUPPORT_APP p:
SWF	s: AWS_ENDPOINT_URL_SWF
synthetics	s: AWS_ENDPOINT_URL_SYNTHETICS s:
Textract	t: AWS_ENDPOINT_URL_TEXTRACT

serviceId	공용 AWS_ENDPOINT_URL_<SERVICE> 환경 변수 유니코드 파일의 서브시스템별 자크
Timestream InfluxDB	t: AWS_ENDPOINT_URL_TIMESTREAM_INFLUXDB m_ b
Timestream Query	t: AWS_ENDPOINT_URL_TIMESTREAM_QUERY m_
Timestream Write	t: AWS_ENDPOINT_URL_TIMESTREAM_WRITE m_
tnb	t: AWS_ENDPOINT_URL_TNB
Transcribe	t: AWS_ENDPOINT_URL_TRANSCRIBE e
Transfer	t: AWS_ENDPOINT_URL_TRANSFER
Translate	t: AWS_ENDPOINT_URL_TRANSLATE
TrustedAdvisor	t: AWS_ENDPOINT_URL_TRUSTEDADVISOR v:

<b>serviceId</b>	<b>공유 서비스별 환경 변수</b>
VerifiedPermissions	<code>AWS_ENDPOINT_URL_VERIFIEDPERMISSIONS</code>
Voice ID	<code>AWS_ENDPOINT_URL_VOICE_ID</code>
VPC Lattice	<code>AWS_ENDPOINT_URL_VPC_LATTICE</code>
WAF	<code>AWS_ENDPOINT_URL_WAF</code>
WAF Regional	<code>AWS_ENDPOINT_URL_WAF_REGIONAL</code>
WAFV2	<code>AWS_ENDPOINT_URL_WAFV2</code>
WellArchitected	<code>AWS_ENDPOINT_URL_WELLARCHITECTED</code>
Wisdom	<code>AWS_ENDPOINT_URL_WISDOM</code>
WorkDocs	<code>AWS_ENDPOINT_URL_WORKDOCS</code>
WorkLink	<code>AWS_ENDPOINT_URL_WORKLINK</code>

<b>serviceId</b>	<b>공용 서비스 디폴트 엔드포인트 URL</b>	<b>환경 변수</b>
WorkMail	w: AWS_ENDPOINT_URL_WORKMAIL	
WorkMailMessageFlow	w: AWS_ENDPOINT_URL_WORKMAILMESSAGEFLOW	
WorkSpaces	w: AWS_ENDPOINT_URL_WORKSPACES	
WorkSpaces Thin Client	w: AWS_ENDPOINT_URL_WORKSPACES_THIN_CLIENT	
WorkSpaces Web	w: AWS_ENDPOINT_URL_WORKSPACES_WEB	
XRay	x: AWS_ENDPOINT_URL_XRAY	

## 스마트 구성 기본값

### Note

설정 페이지의 레이아웃을 이해하거나 다음에 나오는 [Support AWS SDKs이 안내서의 설정 페이지의 이해](#).

스마트 구성 기본값 기능을 사용하면 AWS SDKs 다른 구성 설정에 대해 사전 정의되고 최적화된 기본값을 제공할 수 있습니다.

다음을 사용하여 이 기능을 구성하십시오.

**defaults\_mode** - 공유 AWS **config** 파일 설정, **AWS\_DEFAULTS\_MODE** - 환경 변수, **aws.defaultsMode** - JVM 시스템 속성: Java/Kotlin만 해당

이 설정을 사용하면 사용자 애플리케이션 아키텍처에 맞는 모드를 선택하여 애플리케이션에 최적화된 기본값을 제공할 수 있습니다. AWS SDK 설정에 명시적으로 설정된 값이 있는 경우 해당 값이 항상 우선합니다. AWS SDK 설정에 명시적으로 설정된 값이 없고 defaults\_mode가 레거시와 같지 않은 경우 이 기능은 애플리케이션에 최적화된 다양한 설정에 대해 서로 다른 기본값을 제공할 수 있습니다. 설정에는 HTTP 통신 설정, 재시도 동작, 서비스 리전 엔드포인트 설정 및 잠재적으로 모든 SDK 관련 구성이 포함될 수 있습니다. 이 기능을 사용하는 고객은 일반 사용 시나리오에 맞게 조정된 새 구성 기본값을 얻을 수 있습니다. defaults\_mode이 legacy같지 않은 경우에 SDK를 업그레이드할 때 사용자 애플리케이션 테스트를 수행하는 것이 좋습니다. 제공된 기본값은 모범 사례가 발전함에 따라 변경될 수 있기 때문입니다.

기본값: legacy

참고: 새 주요 버전의 SDK는 standard로 기본 설정됩니다.

유효값:

- legacy— SDK에 따라 달라지고 defaults\_mode의 설정 이전에 존재했던 기본 설정을 제공합니다.
- standard— 대부분의 시나리오에서 안전하게 실행할 수 있는 최신 권장 기본값을 제공합니다.
- in-region - 표준 모드를 기반으로 하며 동일한 내에서 AWS 서비스를 호출하는 애플리케이션에 맞게 조정된 최적화를 포함합니다 AWS 리전.
- cross-region - 표준 모드를 기반으로 하며 다른 리전 AWS 서비스 에서를 호출하는 애플리케이션에 맞게 조정된 최적화를 포함합니다.

- **mobile**— 표준 모드를 기반으로 구축하며 모바일 애플리케이션에 맞게 조정된 최적화를 포함합니다.
- **auto**— 표준 모드를 기반으로 구축하며 실험적 기능을 포함합니다. SDK는 런타임 환경을 검색하여 적절한 설정을 자동으로 결정합니다. 자동 감지는 휴리스틱 기반이며 정확도가 100%는 아닙니다. 런타임 환경을 확인할 수 없는 경우 **standard** 모드가 사용됩니다. 자동 탐지는 [인스턴스 메타데이터](#)를 쿼리할 수 있으며, 이로 인해 지연이 발생할 수 있습니다. 시작 지연 시간이 애플리케이션에 중요한 경우에는 명시적 지연 시간을 `defaults_mode`을 대신 선택하는 것이 좋습니다.

config 파일에서 이 값을 설정하는 예:

```
[default]
defaults_mode = standard
```

다음 파라미터는 `defaults_mode`의 선택에 따라 최적화될 수 있습니다.

- **retryMode**— SDK 재시도 방법을 지정합니다. [재시도 동작](#)을(를) 참조하세요.
- **stsRegionalEndpoints** - SDK가 AWS Security Token Service ()와 통신하는 데 사용하는 AWS 서비스 엔드포인트를 결정하는 방법을 지정합니다AWS STS. [AWS STS 리전 엔드포인트](#)을(를) 참조하세요.
- **s3UsEast1RegionalEndpoints** - SDK가 `us-east-1` 리전의 Amazon S3와 통신하는 데 사용하는 AWS 서비스 엔드포인트를 결정하는 방법을 지정합니다.
- **connectTimeoutInMillis**— 소켓에서 처음 연결을 시도한 후 제한 시간이 초과되기까지의 시간. 클라이언트가 연결 핸드셰이크 완료를 수신하지 못하면 클라이언트는 작업을 포기하고 중단합니다.
- **tlsNegotiationTimeoutInMillis**— CLIENT HELLO 메시지가 전송된 시점부터 클라이언트와 서버가 암호를 완전히 협상하고 키를 교환할 때까지 TLS 핸드셰이크에 걸릴 수 있는 최대 시간입니다.

각 설정의 기본값은 사용자 응용 프로그램에서 선택한 `defaults_mode`에 따라 달라집니다. 이러한 값은 현재 다음과 같이 설정되어 있습니다(변경될 수 있음).

파라미터	<b>standard</b> 모드	<b>in-region</b> 모드	<b>cross-region</b> 모드	<b>mobile</b> 모드
<code>retryMode</code>	standard	standard	standard	standard

파라미터	standard 모드	in-region 모드	cross-region 모드	mobile 모드
stsRegionalEndpoints	regional	regional	regional	regional
s3UsEast1RegionalEndpoints	regional	regional	regional	regional
connectTimeoutInMillis	3100	1100	3100	30000
tlsNegotiationTimeoutInMillis	3100	1100	3100	30000

예를 들어, 선택한 `defaults_mode` 값이 `standard`이면 `standard`의 값이 같으면 `retry_mode` (유효한 `retry_mode` 옵션에서)의 값이 할당되고 `regional`의 값이 `stsRegionalEndpoints`에 할당됩니다(유효한 `stsRegionalEndpoints` 옵션에서).

## AWS SDKs 도구 지원

다음 SDK는 이 주제에서 설명하는 기능 및 설정을 지원합니다. 모든 일부 예외가 기록됩니다. 모든 JVM 시스템 속성 설정은 AWS SDK for Java 및 AWS SDK for Kotlin 에서만 지원됩니다.

SDK	지원됨	참고 또는 추가 정보
<a href="#">AWS CLI v2</a>	아니요	
<a href="#">SDK for C++</a>	예	최적화되지 않은 매개변수: <code>stsRegionalEndpoints</code> , <code>s3UsEast1RegionalEndpoints</code> , <code>tlsNegoti</code>

SDK	지원됨	참고 또는 추가 정보
		<code>ationTimeoutInMillis</code> .
<a href="#">SDK for Go V2 (1.x)</a>	예	최적화되지 않은 매개변수: <code>stsRegionalEndpoints</code> , <code>s3UsEast1RegionalEndpoints</code> , <code>retryMode</code> .
<a href="#">SDK for Go 1.x (V1)</a>	아니요	
<a href="#">SDK for Java 2.x</a>	예	최적화되지 않은 매개변수: <code>stsRegionalEndpoints</code> .
<a href="#">SDK for Java 1.x</a>	아니요	
<a href="#">SDK for JavaScript 3.x</a>	예	최적화되지 않은 매개변수: <code>stsRegionalEndpoints</code> , <code>s3UsEast1RegionalEndpoints</code> , <code>tlsNegotiationTimeoutInMillis</code> . <code>connectTimeoutInMillis</code> 가 <code>connectionTimeout</code> 직접 호출됩니다.
<a href="#">SDK for JavaScript 2.x</a>	아니요	
<a href="#">SDK for Kotlin</a>	아니요	
<a href="#">.NET 4.x용 SDK</a>	예	최적화되지 않은 매개변수: <code>connectTimeoutInMillis</code> , <code>tlsNegotiationTimeoutInMillis</code> .

SDK	지원됨	참고 또는 추가 정보
<a href="#">SDK for .NET 3.x</a>	예	최적화되지 않은 매개변수:connectTimeoutInMillis ,tlsNegotiationTimeoutInMillis .
<a href="#">SDK for PHP 3.x</a>	예	최적화되지 않은 매개변수:tlsNegotiationTimeoutInMillis .
<a href="#">SDK for Python (Boto3)</a>	예	최적화되지 않은 매개변수:tlsNegotiationTimeoutInMillis .
<a href="#">SDK for Ruby 3.x</a>	예	
<a href="#">SDK for Rust</a>	아니요	
<a href="#">SDK for Swift</a>	아니요	
<a href="#">PowerShell V5용 도구</a>	예	최적화되지 않은 매개변수:connectTimeoutInMillis ,tlsNegotiationTimeoutInMillis .
<a href="#">PowerShell V4용 도구</a>	예	최적화되지 않은 매개변수:connectTimeoutInMillis ,tlsNegotiationTimeoutInMillis .

# AWS 공통 런타임(CRT) 라이브러리

AWS 공통 런타임(CRT) 라이브러리는 SDKs. CRT는 C로 작성된 독립 패키지의 모듈식 제품군으로, 각 패키지는 우수한 성능을 제공하고 다양한 필수 기능을 위한 최소한의 설치 공간을 제공합니다. 이러한 기능은 모든 SDK에서 공통적이며 공유되므로 코드 재사용, 최적화 및 정확성이 향상됩니다. 패키지는 다음과 같습니다.

- [awslabs/aws-c-auth](#): AWS 클라이언트 측 인증(표준 자격 증명 공급자 및 서명(sigv4))
- [awslabs/aws-c-cal](#): 암호화 프리미티브 유형, 해시 (MD5, SHA256, SHA256 HMAC), 서명자, AES
- [awslabs/aws-c-common](#): 기본 데이터 구조, 스레딩/동기화 프리미티브 유형, 버퍼 관리, stdlib 관련 함수
- [awslabs/aws-c-compression](#): 압축 알고리즘 (허프만 인코딩/디코딩)
- [awslabs/aws-c-event-stream](#): 이벤트 스트림 메시지 처리 (헤더, 프렐루드, 페이로드, crc/trailer), 이벤트 스트림을 통한 원격 프로시저 직접 호출 (RPC) 구현
- [awslabs/aws-c-http](#): HTTP/1.1 및 HTTP/2 사양의 C99 구현
- [awslabs/aws-c-io](#): 소켓 (TCP, UDP), DNS, 파이프, 이벤트 루프, 채널, SSL/TLS
- [awslabs/aws-c-iot](#): 디바이스와 AWS IoT 클라우드 서비스 통합의 C99 구현
- [awslabs/aws-c-mqtt](#): 사물 인터넷 (IoT)을 위한 간단한 표준 메시징 프로토콜
- [awslabs/aws-c-s3](#): Amazon S3 서비스와의 통신을 위한 C99 라이브러리 구현으로, 고대역폭 Amazon EC2 인스턴스의 처리량을 극대화하도록 설계되었습니다
- [awslabs/aws-c-sdkutils](#): AWS 프로필 구문 분석 및 관리를 위한 유틸리티 라이브러리
- [awslabs/aws-checksums](#): 효율적인 소프트웨어 구현으로 대체되는 크로스 플랫폼 하드웨어 가속 CRC32c 및 CRC32
- [awslabs/aws-lc](#): Google BoringSSL 프로젝트 및 OpenSSL 프로젝트의 코드를 기반으로 AWS 및 고객을 위해 AWS 암호화 팀이 유지 관리하는 범용 암호화 라이브러리
- [awslabs/s2n](#): TLS/SSL 프로토콜의 C99 구현, 보안을 최우선으로 하여 작고 빠르도록 설계되었습니다

CRT는 Go and Rust를 제외한 모든 SDK를 통해 사용할 수 있습니다.

## CRT 종속성

CRT 라이브러리는 복잡한 관계와 종속성 네트워크를 형성합니다. 소스에서 직접 CRT를 구축해야 하는 경우 이러한 관계를 아는 것이 도움이 됩니다. 그러나 대부분의 사용자는 언어 SDK(예: C++용 AWS SDK 또는 Java용 AWS SDK) 또는 언어 IoT 디바이스 SDK(예: C++용 AWS IoT SDK 또는 Java용 AWS IoT SDK)를 통해 CRT 기능에 액세스합니다. 다음 다이어그램에서 언어 CRT 바인딩 상자는 특정 언어 SDK의 CRT 라이브러리를 래핑하는 패키지를 나타냅니다. 이 패키지는 다음과 같은 형식의 `aws-crt-*` 패키지 모음입니다. 여기서 '\*'는 SDK 언어 (예: [aws-crt-cpp](#) 혹은 [aws-crt-java](#))입니다.

다음은 CRT 라이브러리의 계층적 종속성을 보여줍니다.

개별 CRT 라이브러리가 서로 어떻게 상호 연관되는지를 보여주는 CRT 종속성 다이어그램.

# AWS SDKs 및 도구 유지 관리 정책

## 개요

이 문서에서는 모바일 및 IoT SDKs를 포함한 AWS 소프트웨어 개발 키트(SDKs) 및 도구에 대한 유지 관리 정책과 기본 종속성을 간략하게 설명합니다. AWS는 신규 또는 업데이트된 AWS APIs, 새로운 기능, 개선 사항, 버그 수정, 보안 패치 또는 설명서 업데이트에 대한 지원이 포함될 수 있는 업데이트를 AWS SDKs 및 도구에 제공합니다. 업데이트는 종속성, 언어 런타임 및 운영 체제의 변경 사항을 해결할 수도 있습니다. AWS SDK 릴리스는 패키지 관리자(예: Maven, NuGet, PyPI)에게 게시되며 GitHub에서 소스 코드로 사용할 수 있습니다.

최신 기능, 보안 업데이트 및 기본 종속성을 유지하려면 SDK 릴리스를 최신 상태로 유지하도록 권장됩니다. 지원되지 않는 SDK 버전을 계속 사용하는 것은 권장되지 않으며 사용자의 재량에 달려 있습니다.

## 버전 관리

AWS SDK 릴리스 버전은 X.Y.Z 형식이며, 여기서 X는 메이저 버전을 나타냅니다. SDK의 주 버전이 올라가면 이 SDK가 해당 언어의 새로운 관용구와 패턴을 지원하기 위해 상당하고 상당한 변화를 겪었다는 것을 알 수 있습니다. 메이저 버전은 공용 인터페이스(예: 클래스, 메서드, 유형 등), 동작 또는 의미가 변경될 때 도입됩니다. 애플리케이션이 최신 SDK 버전에서 작동하려면 애플리케이션을 업데이트해야 합니다. AWS가 제공하는 업그레이드 지침에 따라 메이저 버전을 신중하게 업데이트하는 것이 중요합니다.

## SDK 주요 버전 수명 주기

주요 SDK 및 도구 버전의 수명 주기는 5단계로 구성되며, 아래에 요약되어 있습니다.

- **개발자 미리 보기 (0 단계)**- 이 단계에서는 SDK가 지원되지 않으므로 프로덕션 환경에 사용해서는 안 되며 조기 액세스 및 피드백 목적으로만 사용됩니다. 향후 릴리스에서는 단절적 변경이 도입될 수 있습니다. 가 릴리스를 안정적인 제품으로 AWS 식별하면 릴리스 후보로 표시할 수 있습니다. 릴리스 후보는 중대한 버그가 나타나지 않는 한 GA 릴리스가 될 준비가 되어 있으며 완전한 AWS 지원을 받게 됩니다.
- **일반 가용성(GA)(1단계)**- 이 단계에서는 SDKs 완전히 지원됩니다. AWS는 새 서비스에 대한 지원, 기존 서비스에 대한 API 업데이트, 버그 및 보안 수정이 포함된 정기적인 SDK 릴리스를 제공합니다.

도구의 경우 AWS 는 새로운 기능 업데이트 및 버그 수정이 포함된 정기 릴리스를 제공합니다. AWS 는 최소 24개월 동안 SDK의 GA 버전을 지원합니다.

- 유지 관리 공지(2단계) - AWS SDK가 유지 관리 모드로 전환되기 최소 6개월 전에 공개적으로 공지합니다. 이 기간 동안에도 SDK는 완전히 지원됩니다. 일반적으로 유지 관리 모드는 다음 메이저 버전이 GA로 전환되는 시점에 동시 발표됩니다.
- 유지 관리 (3 단계)- 유지 관리 모드에서는 AWS 는 SDK 릴리스를 중요한 버그 수정 및 보안 문제에 한정합니다. SDK는 신규 또는 기존 서비스에 대한 API 업데이트를 수신하거나 새 리전 지역을 지원하도록 업데이트 되지 않습니다. 달리 명시되지 않는 한 유지 관리 모드의 기본 기간은 12개월입니다.
- 지원 종료 (4 단계)- SDK가 지원 종료 되면 더 이상 업데이트나 릴리스가 없습니다. 이전에 게시된 릴리스는 공개 패키지 관리자를 통해 계속 사용할 수 있으며 코드는 GitHub에 그대로 유지됩니다. GitHub 리포지토리는 보관될 수 있습니다. 사용자의 재량으로 지원 종료에 도달한 SDK를 사용할 수 있습니다. 새 메이저 버전으로 업그레이드할 것을 당사는 권장합니다.

다음은 SDK 주요 버전 수명 주기를 시각적 그림으로 나타낸 것입니다. 아래 표시된 타임라인은 예시용이며 구속력이 없다는 점에 유의하십시오.

유지 관리 정책 타임라인

## 종속성 수명 주기

AWS SDKs 언어 런타임, 운영 체제 또는 타사 라이브러리 및 프레임워크와 같은 기본 종속성이 있습니다. 이러한 종속성은 일반적으로 언어 커뮤니티 또는 해당 특정 구성 요소를 소유한 공급업체와 연동되어 있습니다. 각 커뮤니티 또는 공급업체는 해당 제품에 대한 자체 지원 종료 일정을 게시합니다.

다음 용어는 기본 타사 종속성을 분류하는 데 사용됩니다.

- 운영 체제 (OS): 아마존 리눅스 AMI, 아마존 리눅스 2, 윈도우 2008, 윈도우 2012, 윈도우 2016 등을 예로 들 수 있습니다.
- 언어 런타임: 자바 7, 자바 8, 자바 11, .NET 코어, 표준 .NET, .NET PCL 등을 예로 들 수 있습니다.
- 타사 라이브러리/프레임워크: OpenSSL, .NET 프레임워크 4.5, Java EE 등을 예로 들 수 있습니다.

커뮤니티 또는 벤더가 종속성에 대한 지원을 종료한 후에도 최소 6개월 동안 SDK 종속성을 계속 지원하는 것이 정책입니다. 하지만 이 정책은 특정 종속성에 따라 달라질 수 있습니다.

**Note**

AWS 는 메이저 SDK 버전을 늘리지 않고 기본 종속성에 대한 지원을 중지할 수 있는 권한을 보유합니다.

## 통신 메서드

유지 관리 공고는 여러 방법으로 전달됩니다.

- 영향 받는 계정에는 특정 SDK 버전에 대한 지원 종료 계획을 알리는 이메일 공지가 발송됩니다. 이 메일은 지원 종료 경로를 설명하고, 캠페인 타임 라인을 정하고, 업그레이드 지침을 제공합니다.
- AWS API 참조 설명서, 사용 설명서, SDK 제품 마케팅 페이지 및 GitHub readme(s)과 같은 SDK 설명서가 캠페인 타임라인을 표시하고 영향을 받는 애플리케이션 업그레이드에 대한 지침을 제공하도록 업데이트됩니다.
- end-of-support 경로를 간략하게 설명하고 캠페인 타임라인을 반복하는 AWS 블로그 게시물이 게시됩니다.
- 사용 중단 경고가 SDK에 추가되어 지원 종료 경로를 설명하고 SDK 설명서가 링크로 연결됩니다.

사용 가능한 AWS SDKs 및 도구의 메이저 버전 목록과 유지 관리 수명 주기의 현재 위치를 보려면 섹션을 참조하세요 [버전 수명 주기](#).

# AWS SDKs 및 도구 버전 수명 주기

아래 표에는 사용 가능한 AWS 소프트웨어 개발 키트(SDK) 메이저 버전 목록과 관련 타임라인과 함께 유지 관리 수명 주기의 현재 위치가 나와 있습니다. 주요 버전의 AWS SDKs 및 도구 수명 주기와 기본 종속성에 대한 자세한 내용은 섹션을 참조하세요 [유지 관리 정책](#).

SDK	메이저 버전	현재 단계	일반 출시 날짜	주석
<a href="#">AWS CLI</a>	1.x	유지 관리 공지	9/2/2013	세부 정보 및 날짜는 <a href="#">공지</a> 를 참조하세요.
<a href="#">AWS CLI</a>	2.x	정식 출시	2/10/2020	
<a href="#">SDK for C++</a>	1.x	정식 출시	9/2/2015	
<a href="#">SDK for Go V2</a>	V2 1.x	정식 출시	1/19/2021	
<a href="#">SDK for Go</a>	1.x	지원 종료	11/19/2015	
<a href="#">SDK for Java</a>	1.x	지원 종료	3/25/2010	
<a href="#">SDK for Java</a>	2.x	정식 출시	11/20/2018	
<a href="#">SDK for JavaScript</a>	1.x	지원 종료	5/6/2013	
<a href="#">SDK for JavaScript</a>	2.x	지원 종료	6/19/2014	
<a href="#">SDK for JavaScript</a>	3.x	정식 출시	12/15/2020	
<a href="#">SDK for Kotlin</a>	1.x	정식 출시	11/27/2023	
<a href="#">SDK for .NET</a>	1.x	지원 종료	2009년 11월	
<a href="#">SDK for .NET</a>	2.x	지원 종료	11/8/2013	
<a href="#">SDK for .NET</a>	3.x	정식 출시	7/28/2015	

SDK	메이저 버전	현재 단계	일반 출시 날짜	주석
<a href="#">SDK for .NET</a>	4.x	정식 출시	4/28/2025	
<a href="#">SDK for PHP</a>	2.x	지원 종료	11/2/2012	
<a href="#">SDK for PHP</a>	3.x	정식 출시	5/27/2015	
<a href="#">SDK for Python (Boto2)</a>	1.x	지원 종료	7/13/2011	
<a href="#">SDK for Python (Boto3)</a>	1.x	정식 출시	6/22/2015	
<a href="#">SDK for Python (Botocore)</a>	1.x	정식 출시	6/22/2015	
<a href="#">SDK for Ruby</a>	1.x	지원 종료	7/14/2011	
<a href="#">SDK for Ruby</a>	2.x	지원 종료	2/15/2015	
<a href="#">SDK for Ruby</a>	3.x	정식 출시	8/29/2017	
<a href="#">SDK for Rust</a>	1.x	정식 출시	11/27/2023	
<a href="#">SDK for Swift</a>	1.x	정식 출시	9/17/2024	
PowerShell용 도구	2.x	지원 종료	11/8/2013	
PowerShell용 도구	3.x	지원 종료	7/29/2015	
<a href="#">PowerShell용 도구</a>	4.x	정식 출시	11/21/2019	
<a href="#">PowerShell용 도구</a>	5.x	정식 출시	6/23/2025	

언급되지 않은 SDK 또는 도구를 검색하시나요? 예를 들어, Encryption SDK, IoT Device SDK, 그리고 Mobile SDK는 이 안내서에 포함되어 있지 않습니다. 이와 같은 다른 도구에 대한 문서를 찾으려면 [AWS를 기반으로 빌드할 도구](#)를 참조하세요.

# AWS SDKs 도구에 대한 문서 기록 참조 가이드

다음 표에는 AWS SDK 및 도구 참조 가이드의 중요한 추가 및 업데이트가 설명되어 있습니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드에 가입하면 됩니다.

변경 사항	설명	날짜
<a href="#">새 S3 Express One Zone 설정 추가</a>	세션 인증을 비활성화하기 위해 새 S3 Express One Zone 설정을 추가합니다.	2025년 10월 13일
<a href="#">새 인증 의사 결정 트리 추가</a>	옵션 간 인증 결정을 지원하는 새 의사 결정 트리를 추가합니다.	2025년 9월 23일
<a href="#">새 인증 체계 기능 추가</a>	새 인증 체계 기능을 추가합니다. AWS STS 리전 엔드포인트에 대한 업데이트입니다.	2025년 8월 18일
<a href="#">새 버전의 Tools for PowerShell 추가</a>	모든 설정 참조 AWS SDKs와의 호환성 테이블에 최신 버전의 Tools for PowerShell 지원을 추가합니다. 호스트 접두사 삽입 기능이 추가되었습니다.	2025년 6월 23일
<a href="#">페이지 제목 업데이트</a>	더 많은 제목, 표 제목, 초록 및 SEO 업데이트.	2025년 3월 5일
<a href="#">페이지 제목 업데이트</a>	더 설명적인 제목을 사용하도록 콘텐츠를 업데이트합니다.	2025년 2월 24일
<a href="#">설정 참조에 Swift SDK 추가</a>	모든 Setting reference Compatibility with AWS SDKs 테이블에 Swift SDK 지원을 추가합니다.	2024년 9월 17일
<a href="#">SDK for Java 1.x 시스템 속성</a>	AWS SDK for Java 1.x에서 지원되는 JVM 시스템 구성 설정	2024년 5월 30일

	에 대한 세부 정보를 추가합니다.	
<a href="#">설정 업데이트</a>	JVM 시스템 구성 설정을 추가합니다.	2024년 3월 27일
<a href="#">호환성 표 업데이트</a>	SDK 지원 호환성 관련 업데이트와 IAM Identity Center 절차 업데이트.	2024년 2월 20일
<a href="#">컨테이너 보안 인증 업데이트. IMDS 업데이트.</a>	Amazon EKS 지원 추가. IMDSv1 폴백을 비활성화하기 위한 설정 추가.	2023년 12월 29일
<a href="#">요청 압축</a>	요청 압축 기능에 대한 설정 추가.	2023년 12월 27일
<a href="#">호환성 테이블</a>	SDK 및 도구 기능에 대한 호환성 테이블이 SDK for Kotlin, SDK for Rust, AWS Tools for PowerShell등을 포함하도록 업데이트되었습니다.	2023년 12월 10일
<a href="#">인증 업데이트</a>	SDK 및 도구에 지원되는 인증 방법이 업데이트되었습니다.	2023년 7월 1일
<a href="#">IAM 모범 사례 업데이트</a>	IAM 모범 사례에 따라 가이드가 업데이트되었습니다. 자세한 내용은 <a href="#">IAM의 보안 모범 사례</a> 를 참조하십시오.	2023년 2월 27일
<a href="#">SSO 업데이트</a>	새 SSO 토큰 구성을 위한 SSO 보안 인증 업데이트.	2022년 11월 19일
<a href="#">설정 업데이트</a>	일반 구성 및 Amazon S3 다중 리전 액세스 포인트 지원 표 업데이트.	2022년 11월 17일

<a href="#"><u>설정 업데이트</u></a>	IMDS 클라이언트 및 IMDS 보안 인증의 명확성 업데이트. 환경 변수 업데이트.	2022년 11월 4일
<a href="#"><u>시작 페이지 업데이트</u></a>	Amazon CodeWhisperer 출시.	2022년 9월 22일
<a href="#"><u>싱글 사인은 서비스 이름 변경</u></a>	AWS SSO가 이제 참조됨을 반영하기 위한 업데이트입니다 AWS IAM Identity Center.	2022년 7월 26일
<a href="#"><u>설정 업데이트</u></a>	구성 파일 세부 정보 및 지원 설정에 대한 사소한 업데이트.	2022년 6월 15일
<a href="#"><u>업데이트</u></a>	이 안내서의 거의 모든 부분이 업데이트되었습니다.	2022년 2월 1일
<a href="#"><u>최초 릴리스</u></a>	이 설명서의 최초 릴리스가 일 반에 공개되었습니다.	2020년 3월 13일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.