콘솔 관리 가이드

# AWS re:포스트 프라이빗

# AWS re:포스트 프라이빗: 콘솔 관리 가이드

# Table of Contents

# AWS re:Post 프라이빗이란 무엇입니까?

AWS re:Post Private은 엔터프라이즈 지원 또는 엔터프라이즈 온램프 지원 플랜을 보유한 엔터프라이즈용 AWS re:Post의 프라이빗 버전입니다. 지식과 전문가에 대한 액세스를 제공하여 클라우드 채택을 가속화하고 개발자 생산성을 높입니다. 조직별 비공개 re:Post를 사용하면 대규모 효율성을 높이고 귀중한 지식 리소스에 액세스할 수 있는 조직별 개발자 커뮤니티를 구축할 수 있습니다. 또한 re:Post Private은 신뢰할 수 있는 AWS 기술 콘텐츠를 중앙 집중화하고 비공개 토론 포럼을 제공하여 팀이 내부 및 AWS와 협업하여 기술적 장애물을 제거하고 혁신을 가속화하며 클라우드에서 더 효율적으로 확장하는 방식을 개선합니다.

자세한 내용은 AWS re:Post 프라이빗을 참조하십시오.

## re:Post 프라이빗에 액세스

관리자는 AWS re:Post 프라이빗 콘솔을 사용하여 조직별 프라이빗 re:Post를 생성합니다. 관리자는 프라이빗 re:Post를 생성할 때 프라이빗 re:Post라는 이름을 지정하고 아래에 하위 도메인을 정의할 수 있습니다. `*.private.repost.aws` 조직의 비공개 re:Post의 관리자는 인증을 위한 ID 센터 디렉터리, Active Directory 또는 외부 ID 공급자 중 하나를 사용하여 사용자 액세스를 AWS IAM Identity Center 구성하고 지정할 수 있습니다. 사용자를 구성한 후 콘솔 관리자는 한 명 이상의 사용자에게 re:Post Private 관리자 역할을 할당할 수 있습니다. re:Post Private 관리자는 조직의 브랜딩 및 지식 요구 사항에 따라 개인 re:Post 응용 프로그램을 사용자 정의할 수 있습니다. 조직의 아키텍처와 워크로드에 익숙한 기술 계정 관리자와 같은 계정 팀 구성원은 협업을 위해 조직의 비공개 re:Post에 자동으로 추가됩니다. AWS

re:Post Private 애플리케이션 관리자는 브랜딩을 사용자 지정하고, 태그를 추가하여 콘텐츠를 분류하고, 개발자가 관심 있는 주제를 선택하여 교육 및 기술 콘텐츠를 자동으로 채울 수 있습니다. 또한 사용자를 비공개 re:Post에 가입하도록 초대하여 협업을 강화할 수도 있습니다. 자세한 내용은 AWS re:Post 프라이빗 관리 안내서를 참조하십시오.

관리자가 아닌 사용자는 re:Post Private 애플리케이션을 사용하여 관리자가 구성한 자격 증명을 사용하여 로그인합니다. 비공개 re:Post에 로그인한 후 사용자는 관심 주제에 맞는 맞춤형 교육 및 기술 콘텐츠를 비롯한 기존 콘텐츠를 찾아보거나 검색할 수 있습니다. 또한 사용자는 비공개 re:Post에서 직접 AWS 공개 기술 콘텐츠를 검색하고 공개 콘텐츠에 대한 내부 토론을 위한 비공개 스레드를 만들 수 있습니다. AWS 사용자는 질문을 하거나 답변을 제공하거나 기사를 게시하여 다른 비공개 re:Post 사용자로부터 AWS 기술 문제를 공동으로 해결하고 기술 지침을 얻을 수 있습니다. 사용자는 토론 스레드를 케이스로 전환할 수도 있습니다. AWS Support 사용자는 비공개 re:Post의 응답을 AWS Support 선택하여 추가할 수 있습니다. 자세한 내용은 AWS re:Post 프라이빗 사용 설명서를 참조하십시오.

# 요금

엔터프라이즈 지원 (ES) 및 엔터프라이즈 온램프 (EOP) 지원 플랜을 보유한 고객만 re:Post Private 서비스를 구독할 수 있습니다. 사용 가능한 두 가지 요금 계층, 즉 프리 티어와 표준 티어 중에서 선택할 수 있습니다. 프리 티어는 유료 티어로 원활하게 전환하기 전에 6개월 동안 표준 티어 기능을 충분히 살펴보고 시험해 볼 수 있는 기능을 제공합니다. 표준 등급을 사용하는 경우 사용자 요금별로 월간 구독료를 지불하여 re:Post Private를 사용할 수 있습니다. 자세한 내용은 요금을 참조하세요.

# 시작하는 방법

re:Post 비공개를 시작하려면 을 참조하십시오. 필수 조건

# 필수 조건

AWS re:Post Private에서 새 프라이빗 re:Post를 생성하거나 기존 프라이빗 re:Post를 관리하려면 먼저 다음 사전 요구 사항을 충족해야 합니다.

- 엔터프라이즈 또는 엔터프라이즈 On-Ramp 지원 플랜에 가입해야 합니다.
- 비공개 re:Post를 설정하려는 지역과 동일한 AWS IAM Identity Center 지역에서 활성화해야 합니다.
- AWS Support케이스를 생성, 관리, 해결하는 데 필요한 권한이 있는 AWS Identity and Access Management 역할을 생성해야 합니다. re:Post Private 서비스는 이 역할을 사용하여 API를 호출합니다. AWS Support 자세한 정보는 re:Post AWS Support Private에서 사례 생성 및 관리에 대한 액세스 관리 단원을 참조하세요.

# IAM 아이덴티티 센터를 통해 re:Post 비공개로 온보딩

re:Post Private는 와 통합되어 직원에게 ID AWS IAM Identity Center 페더레이션을 제공합니다. IAM Identity Center를 통해 사용자는 기존 회사 디렉터리로 리디렉션되어 기존 자격 증명으로 로그인할 수 있습니다. 그러면 개인 re:Post에 원활하게 로그인할 수 있습니다. 이렇게 하면 암호 정책 및 2단계 인증과 같은 보안 설정이 적용됩니다. IAM ID 센터를 사용해도 기존 IAM 구성에는 영향을 미치지 않습니다.

기존 사용자 디렉터리가 없거나 페더레이션을 원하지 않는 경우, IAM Identity Center는 re:Post Private의 사용자 및 그룹을 생성하는 데 사용할 수 있는 통합 사용자 디렉터리를 제공합니다. re:Post Private는 IAM 사용자 및 역할을 사용하여 프라이빗 re:Post 내에서 권한을 할당하는 것을 지원하지 않습니다. 프라이빗 re:Post 내의 사용자 권한은 관리자가 프라이빗 re:Post 애플리케이션에서 구성합니다.

IAM 자격 증명 센터에 대한 자세한 내용은 AWS IAM 자격 증명 센터란? (AWS Single Sign-On의 후속)을 참조하십시오. IAM ID 센터를 시작하는 방법에 대한 자세한 내용은 시작하기를 참조하십시오. IAM ID 센터를 사용하려면 해당 계정도 AWS Organizations 활성화해야 합니다.

> **Important**
>
> re:Post Private은 IAM ID 센터의 조직 인스턴스만 지원합니다.

# re:Post 비공개에서의 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처를 활용할 수 있습니다.

보안은 기업과 기업 간의 공동 책임입니다. AWS 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. AWS re:Post Private에 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스 규정 준수 참조하십시오.
- 클라우드에서의 보안 — 사용하는 AWS 서비스에 따라 책임이 결정됩니다. 또한 사용자는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 re:Post Private를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 re:Post Private를 구성하는 방법을 보여줍니다. 또한 re:Post Private 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- AWS re:Post 프라이빗에서의 데이터 보호
- re:Post 프라이빗이 IAM과 연동되는 방식
- AWS re:Post Private에 대한 규정 준수 검증
- AWS re:포스트 프라이빗에서의 레질리언스
- AWS re:포스트 프라이빗의 인프라 보안

## AWS re:Post 프라이빗에서의 데이터 보호

AWS 공동 책임 모델 공동 책임 모델 이 모델에 설명된 대로, AWS 는 모든 모델을 실행하는 글로벌 인프라를 보호할 책임이 있습니다. AWS 클라우드사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그에서 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API 또는 SDK를 AWS 서비스 사용하여 re:Post Private 또는 기타 작업을 수행하는 경우가 포함됩니다. AWS CLI AWS 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

## 암호화로 데이터 보호

### 저장 중 암호화

re:Post Private는 Amazon 심플 스토리지 서비스 버킷, Amazon DynamoDB 데이터베이스, Amazon Neptune 데이터베이스 OpenSearch 및 Amazon 서비스 도메인을 사용합니다. Amazon 서비스 도메인은 Amazon 관리 키 또는 고객 관리 키를 사용하여 유휴 상태에서 암호화됩니다.

## 전송 중 암호화

re:Post Private은 HTTPS 프로토콜을 사용하여 클라이언트 애플리케이션과 통신합니다. HTTPS와 AWS 서명을 사용하여 애플리케이션을 대신하여 다른 서비스와 통신합니다.

## 키 관리

re:Post Private은 키와 통합되어 있으며 키를 지원합니다 AWS Key Management Service . AWS KMS 비공개 re:Post를 생성할 때 데이터 암호화 설정을 사용자 지정할 수 있습니다. 이렇게 하려면 기존 AWS KMS 키를 선택하거나 새 AWS KMS 키를 생성하면 됩니다.

# re:Post 프라이빗이 IAM과 연동되는 방식

IAM을 사용하여 AWS re:Post Private에 대한 액세스를 관리하기 전에 re:Post Private과 함께 사용할 수 있는 IAM 기능을 이해해야 합니다. re:Post Private 및 기타 AWS 서비스가 IAM과 어떻게 연동되는지 자세히 알아보려면 IAM 사용 설명서에서 IAM과 연동되는 AWS 서비스를 참조하십시오.

## re:Post 프라이빗 자격 증명 기반 정책

IAM 자격 증명 기반 정책을 사용하면 허용 또는 거부 작업을 지정할 수 있습니다. re:Post Private은 특정 작업을 지원합니다. JSON 정책에서 사용하는 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

### 작업

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

re:Post Private의 정책 작업은 작업 앞에 다음 접두사를 사용합니다. `repostspace:` 예를 들어 누군가에게 re:Post Private `CreateSpace` API 작업을 실행할 권한을 부여하려면 해당 작업을 해당 사용자의 정책에 포함해야 합니다`repostspace:CreateSpace`. 정책 설명에는 `Action` OR `NotAction` 요소가 포함되어야 합니다. re:Post Private은 이 서비스로 수행할 수 있는 작업을 설명하는 자체 작업 세트를 정의합니다.

명령문 하나에 여러 태스크를 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "repostspace:CreateSpace",
```

```
        "repostspace:DeleteSpace"
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Describe라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "repostspace:Describe*"
```

re:Post Private 작업 목록을 보려면 IAM 사용 설명서의 re:Post Private에서 정의한 작업을 참조하십시오.

### 리소스

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 타입을 지원하는 작업에 대해 이 작업을 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

### 조건 키

re:Post Private은 서비스별 조건 키를 제공하지 않지만 글로벌 조건 키 사용을 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

### 예제

re:Post 프라이빗 ID 기반 정책의 예를 보려면 을 참조하십시오. AWS re:Post 프라이빗 자격 증명 기반 정책 예제

## re:Post 프라이빗 리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는

이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 또는 서비스가 포함될 수 있습니다. AWS 리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

re:Post Private은 리소스 기반 정책을 지원하지 않습니다.

## 태그 기반 인증

re:Post Private은 리소스에 태그를 지정하거나 태그를 기반으로 액세스를 제어할 수 있습니다. 자세한 내용은 태그를 사용한 AWS 리소스 액세스 제어를 참조하십시오.

## re:POST 프라이빗 IAM 역할

IAM 역할은 AWS 계정 내에서 특정 권한을 가진 엔티티입니다.

### re:Post Private에서 임시 자격 증명 사용

임시 보안 인증을 사용하여 페더레이션을 통해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 것을 강력히 권장합니다. 또는 와 같은 AWS STS AssumeRoleAPI 작업을 호출하여 임시 보안 자격 증명을 얻을 수 있습니다. GetFederationToken

re:Post Private은 임시 자격 증명 사용을 지원합니다.

## 서비스 연결 역할

서비스 연결 역할을 사용하면 AWS 서비스가 다른 서비스의 리소스에 액세스하여 사용자를 대신하여 작업을 완료할 수 있습니다. 서비스 연결 역할은 IAM 계정에 나타나고 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집할 수 없습니다.

## 서비스 역할

이 기능을 사용하면 서비스가 사용자를 대신하여 서비스 역할을 맡을 수 있습니다. 이 역할을 통해 서비스는 다른 서비스의 리소스에 액세스하여 사용자를 대신하여 작업을 완료할 수 있습니다. 자세한 내용은 AWS 서비스에 권한을 위임하기 위한 역할 생성을 참조하십시오. 서비스 역할은 IAM 계정에 나타나고, 해당 계정이 소유합니다. 즉, IAM 관리자가 이 역할에 대한 권한을 변경할 수 있습니다. 그러나 권한을 변경하면 서비스의 기능이 손상될 수 있습니다.

# re:Post Private의 서비스 연결 역할 사용

AWS re:Post 프라이빗 사용 AWS Identity and Access Management (IAM) 서비스 연결 역할. 서비스 연결 역할은 re:Post Private에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 re:Post Private에 의해 미리 정의되며 서비스가 사용자를 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 re:Post Private를 더 쉽게 설정할 수 있습니다. re:Post Private는 서비스 연결 역할의 권한을 정의하며, 달리 정의하지 않는 한 re:Post Private만 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할(Service-linked roles) 열에 예(Yes)가 있는 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

## re:Post Private에 대한 서비스 연결 역할 권한

re:Post Private는 이름이 지정된 서비스 연결 역할을 사용합니다 AWSServiceRoleForrePostPrivate. re:Post Private는 이 서비스 연결 역할을 사용하여 데이터를 게시합니다. CloudWatch

AWSServiceRoleForrePostPrivate 서비스 연결 역할은 역할을 맡을 수 있는 다음 서비스를 신뢰합니다.

- `repostspace.amazonaws.com`

이름이 지정된 역할 권한 정책을 `AWSrePostPrivateCloudWatchAccess` 사용하면 re:Post Private가 지정된 리소스에서 다음 작업을 완료할 수 있습니다.

- 조치 대상: `cloudwatch PutMetricData`

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하십시오.

자세한 정보는 AWSrePostPrivateCloudWatchAccess을 참조하세요.

## re:Post 비공개를 위한 서비스 연결 역할 만들기

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API에서 첫 번째 비공개 re:Post를 만들면 re:Post가 서비스 연결 역할을 자동으로 생성합니다.

> **Important**
>
> 이러한 서비스 연결 역할은 해당 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다. 또한 서비스 연결 역할을 지원하기 시작한 2023년 12월 1일 이전에 re:Post Private 서비스를 사용하고 있었다면 re:Post Private이 사용자 계정에 역할을 생성한 것입니다. `AWSServiceRoleForrePostPrivate` 자세히 알아보려면 내 역할에 새 역할이 생겼음을 참조하십시오. AWS 계정

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 첫 번째 비공개 re:Post를 생성하면 re:Post Private가 서비스 연결 역할을 다시 생성합니다.

AWS CLI 또는 AWS API에서 서비스 이름을 사용하여 서비스 연결 역할을 생성합니다. `repostspace.amazonaws.com` 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 생성을 참조하십시오. 이 서비스 연결 역할을 삭제하면 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

## re:Post Private의 서비스 연결 역할 편집

re:Post Private에서는 서비스에 연결된 역할을 편집할 수 없습니다. `AWSServiceRoleForrePostPrivate` 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

## re:Post Private의 서비스 연결 역할 삭제

`AWSServiceRoleForrePostPrivate` 역할은 수동으로 삭제할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API에서 비공개 re:Post를 삭제하면 re:Post가 서비스 연결 역할을 자동으로 삭제합니다.

IAM 콘솔 AWS CLI, 또는 API를 사용하여 서비스 연결 역할을 수동으로 삭제할 수도 있습니다. AWS

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 서비스 연결 역할을 삭제합니다. AWSServiceRoleForrePostPrivate 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

# re:Post 프라이빗 서비스 연결 역할이 지원되는 지역

re:Post Private은 서비스가 제공되는 지역에서 서비스 연결 역할을 사용할 수 있도록 지원합니다. AWS

| 지역명 | 리전 자격 증명 | re:Post 비공개 지원 |
|---|---|---|
| 미국 동부(버지니아 북부) | us-east-1 | 예 |
| 미국 동부(오하이오) | us-east-2 | 아니요 |
| 미국 서부(캘리포니아 북부) | us-west-1 | 아니요 |
| 미국 서부(오레곤) | us-west-2 | 예 |
| 아프리카(케이프타운) | af-south-1 | 아니요 |
| 아시아 태평양(홍콩) | ap-east-1 | 아니요 |
| 아시아 태평양(자카르타) | ap-southeast-3 | 아니요 |
| 아시아 태평양(뭄바이) | ap-south-1 | 아니요 |
| 아시아 태평양(오사카) | ap-northeast-3 | 아니요 |
| 아시아 태평양(서울) | ap-northeast-2 | 아니요 |
| 아시아 태평양(싱가포르) | ap-southeast-1 | 예 |
| 아시아 태평양(시드니) | ap-southeast-2 | 예 |
| 아시아 태평양(도쿄) | ap-northeast-1 | 아니요 |
| 캐나다(중부) | ca-central-1 | 예 |
| 유럽(프랑크푸르트) | eu-central-1 | 예 |
| 유럽(아일랜드) | eu-west-1 | 예 |
| 유럽(런던) | eu-west-2 | 아니요 |
| 유럽(밀라노) | eu-south-1 | 아니요 |

| 지역명 | 리전 자격 증명 | re:Post 비공개 지원 |
|---|---|---|
| 유럽(파리) | eu-west-3 | 아니요 |
| 유럽(스톡홀름) | eu-north-1 | 아니요 |
| 중동(바레인) | me-south-1 | 아니요 |
| 중동(UAE) | me-central-1 | 아니요 |
| 남아메리카(상파울루) | sa-east-1 | 아니요 |

## AWS re:Post 프라이빗 자격 증명 기반 정책 예제

> **Note**
>
> 보안을 강화하려면 가급적 IAM 사용자 대신 페더레이션 사용자를 생성하세요.

기본적으로 AWS Identity and Access Management 사용자와 역할은 AWS re:Post 프라이빗 리소스를 생성하거나 수정할 권한이 없습니다. 또한 AWS Management Console AWS CLI, 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. IAM 관리자는 지정된 리소스에서 특정 API 작업을 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

### 정책 모범 사례

ID 기반 정책은 누군가가 계정에서 re:Post Private 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

## 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## 인라인 정책

인라인 정책은 사용자가 만들고 관리하는 정책입니다. 인라인 정책을 사용자, 그룹 또는 역할에 직접 내장할 수 있습니다. 다음 정책 예제는 AWS re:Post 프라이빗 작업을 수행할 권한을 할당하는 방법을 보여줍니다. 인라인 정책에 대한 일반 정보는 AWS IAM 사용 설명서의 IAM 정책 관리를 참조하십시오. AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS Identity and Access Management API를 사용하여 인라인 정책을 생성하고 내장할 수 있습니다.

주제

- re:Post 프라이빗에 대한 읽기 전용 액세스 권한
- re:Post 비공개에 대한 전체 액세스 권한

## re:Post 프라이빗에 대한 읽기 전용 액세스 권한

다음 정책은 IAM ID 센터 및 re:Post Private 콘솔에 대한 읽기 권한을 사용자에게 부여합니다. 이 정책을 통해 사용자는 읽기 전용인 re:Post Private 작업을 수행할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",

                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "repostspace:GetSpace",
                "repostspace:ListSpaces",
                "repostspace:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

## re:Post 비공개에 대한 전체 액세스 권한

다음 정책은 사용자에게 IAM ID 센터 및 re:Post Private 콘솔에 대한 전체 액세스 권한을 부여합니다. 이 정책을 통해 사용자는 모든 re:Post Private 작업을 수행할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",

                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:AssociateProfile",
                "sso:DisassociateProfile",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "kms:ListAliases",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant",

                "repostspace:*"
            ],
            "Resource": "*"
        }
    ]
}
```

# AWS AWS re:Post 프라이빗 관리형 정책

AWS 관리형 정책을 사용하면 정책을 직접 작성하는 것보다 사용자, 그룹 및 역할에 권한을 더 쉽게 추가할 수 있습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. AWS 관리형 정책을 사용하면 빠르게 시작할 수 있습니다. 이러한 정책은 일반적인 사용 사례를 다루며 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의AWS 관리형 정책을 참조하십시오.

AWS 서비스는 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스가 새 기능을 지원하기 위해 AWS 관리형 정책에 권한을 추가하는 경우가 있습니다. 이 타입의 업데이트는 정책이 연결된 모든 보안 인증(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새 기능이 출시되거나 새 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한 여러 서비스에 걸친 작업 기능에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 `ReadOnlyAccess` AWS 관리형 정책은 모든 AWS 서비스와 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면 새 작업 및 리소스에 대한 읽기 전용 권한이 AWS 추가됩니다. 자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

주제

- AWS 관리형 정책: AWSRepostSpaceSupportOperationsPolicy
- AWS 관리형 정책: AWSrePostPrivateCloudWatchAccess
- AWS re:POST 관리형 정책에 대한 AWS 프라이빗 업데이트

## AWS 관리형 정책: AWSRepostSpaceSupportOperationsPolicy

이 정책은 AWS re:Post Private 서비스가 re:Post Private 웹 애플리케이션을 통해 생성된 AWS Support 사례를 생성, 관리 및 해결할 수 있도록 허용합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
```

```
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
   ],
   "Resource": "*"
  }
 ]
}
```

## AWS 관리형 정책: AWSrePostPrivateCloudWatchAccess

이 정책은 re:Post Private 서비스가 데이터를 게시할 수 있도록 허용합니다. CloudWatch

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CloudWatchPublishMetrics",
   "Effect": "Allow",
   "Action": [
    "cloudwatch:PutMetricData"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "cloudwatch:namespace": [
      "AWS/rePostPrivate",
      "AWS/Usage"
     ]
    }
   }
  }
 ]
}
```

## AWS re:POST 관리형 정책에 대한 AWS 프라이빗 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 re:Post Private의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 문서 이력 페이지에서 RSS 피드를 구독하십시오.

다음 표에는 2023년 11월 26일 이후 re:Post Private 관리형 정책에 대한 중요 업데이트가 설명되어 있습니다.

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 새 정책 - AWSrePostPrivateCloudWatchAccess | 에 데이터를 게시하기 위한 새로운 관리형 정책 CloudWatch | 2023년 11월 26일 |
| 새 정책 - AWSRepostSpaceSupportOperationsPolicy | AWS re:Post Private의 AWS Support 기능에 대한 새로운 관리형 정책 | 2023년 11월 26일 |
| re:Post Private는 변경 사항을 추적하기 시작했습니다. | re:Post Private는 관리형 정책의 변경 사항을 추적하기 시작했습니다. AWS | 2023년 11월 26일 |

## AWS re:Post 프라이빗 자격 증명 및 액세스 문제 해결

다음 정보를 사용하면 re:Post Private 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 re:Post Private에서 작업을 수행할 권한이 없습니다.
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 제 re:Post 비공개 리소스에 외부 사용자가 액세스할 수 AWS 계정 있도록 허용하고 싶습니다.

### 저는 re:Post Private에서 작업을 수행할 권한이 없습니다.

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 `mateojackson`IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`*리소스에 대한 세부 정보를 보려고 하지만 가상 `repostPrivate:`*`GetWidget`*권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 repostPrivate:GetWidget on resource: my-example-widget
```

이 경우 `repostPrivate:GetWidget`작업을 사용하여 `my-example-widget`리소스에 액세스할 수 있도록 `mateojackson`사용자 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

## 저는 IAM을 수행할 권한이 없습니다. PassRole

작업을 수행할 권한이 없다는 오류가 발생하는 경우 re:Post Private에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다. `iam:PassRole`

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 이라는 IAM 사용자가 re:Post Private에서 콘솔을 사용하여 작업을 `marymajor` 수행하려고 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우 Mary가 `iam:PassRole`작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

## 제 re:Post 비공개 리소스에 외부 사용자가 액세스할 수 AWS 계정 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- re:Post Private이 이러한 기능을 지원하는지 알아보려면 을 참조하십시오. re:Post 프라이빗이 IAM 과 연동되는 방식
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.

- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

## AWS re:Post Private에 대한 규정 준수 검증

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.

- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

# AWS re:포스트 프라이빗에서의 레질리언스

AWS 글로벌 인프라는 가용 영역을 중심으로 구축됩니다. AWS 리전 AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

# AWS re:포스트 프라이빗의 인프라 보안

관리형 서비스인 AWS re:Post Private는 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차에 따라 보호됩니다.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 re:Post Private에 액세스할 수 있습니다. 클라이언트가 전송 계층 보안(TLS) 1.0 이상을 지원해야 합니다. TLS 1.2 이상을 권장합니다. 클라이언트는 DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID 및 보안 주체와 연결된 비밀 액세스 키를 사용하여 요청에 서명해야 합니다. AWS Identity and Access Management 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

# re:비공개 할당량 게시

AWS re:Post Private은 특정 지역의 계정에서 사용할 수 있는 비공개 re:Post를 제공합니다. AWS re:Post Private에 가입하면 생성할 수 있는 비공개 re:Post의 수와 프라이빗 re:Post의 크기에 대한 기본 할당량 (이전에는 한도라고 함) 을 AWS 설정합니다.

## 서비스 할당량

계정의 re:Post Private의 기본 할당량은 다음과 같습니다. AWS Service Quotas 콘솔을 사용하여 기본 할당량을 볼 수 있습니다. 이러한 할당량 중 어느 것도 조정할 수 없습니다. 할당량 증가를 요청할 수 없습니다.

| 리소스 | 기본값 | 설명 | 조정 가능 |
|---|---|---|---|
| 비공개 re:게시물 수 | 3 | 현재 지역에서 이 계정의 비공개 re:Post의 최대 개수 | 아니요 |
| 무료 비공개 re:Post 크기 | 10 | 무료 프라이빗 re:Post의 최대 크기 (GB). | 아니요 |
| 표준 사설 re:Post 크기 | 100 | 표준 사설 re:Post의 최대 크기 (GB). | 아니요 |

## API 스로틀링 한도

re:Post Private에서는 계정별, 지역별로 다음과 같은 제한 제한이 적용됩니다. 이러한 할당량은 늘릴 수 없습니다.

| 작업 | 토큰 리필 비율 | 요청 비율 | |
|---|---|---|---|
| CreateSpace | 1 | 1 | |
| ListSpaces | 10 | 10 | |
| GetSpace | 10 | 10 | |

| 작업 | 토큰 리필 비율 | 요청 비율 |
| --- | --- | --- |
| UpdateSpace | 10 | 10 |
| DeleteSpace | 1 | 1 |
| RegisterAdmin | 10 | 100 |
| DeRegisterAdmin | 10 | 100 |
| SendInvites | 1 | 1 |
| TagResource | 10 | 10 |
| UnTagResource | 10 | 10 |
| ListTagsForResource | 10 | 10 |

# 개인 re:Post를 생성, 구성 및 사용자 정의하십시오.

주제

- 새 비공개 re:Post를 만드세요.
- re:Post AWS Support Private에서 사례 생성 및 관리에 대한 액세스 관리
- 를 사용하여 사용자 액세스를 설정하고 관리합니다. AWS IAM Identity Center
- 프라이빗 re:Post를 사용자 지정하세요.
- 사용자를 비공개 re:Post에 초대하십시오.

## 새 비공개 re:Post를 만드세요.

새 비공개 re:Post를 만들려면 다음 단계를 따르세요.

1. https://console.aws.amazon.com/repost-private/ 에서 re:Post 프라이빗 콘솔을 엽니다.
2. 콘솔 홈페이지에서 비공개 re:Post 생성을 선택합니다.
3. 계정에 IAM ID 센터를 아직 구성하지 않은 경우 ID 센터 열기를 선택하십시오. AWS IAM ID 센터 사용 설명서의 시작하기에 나와 있는 지침을 따르십시오.
4. 프라이빗 re:Post 생성 페이지에서 요금을 보려면 사용 사례에 따라 프리 티어 또는 스탠다드 티어를 선택하십시오. 계정에 이미 프리 티어를 사용한 경우 프리 티어 옵션을 사용할 수 없습니다.
5. 세부 정보에서 다음을 수행하십시오.

   이름에는 비공개 re:Post의 고유한 이름을 입력합니다.

   (선택 사항) 설명에 비공개 re:Post에 대한 간략한 설명을 입력합니다.

   사용자 지정 하위 도메인의 경우 하위 도메인의 사용자 지정 이름을 입력합니다.
6. (선택 사항) 데이터 암호화 설정을 사용자 지정하려면 데이터 암호화에서 암호화 설정 사용자 지정을 선택합니다. 그런 다음 다음 작업 중 하나를 수행하십시오.

   AWS KMS 키 선택에서 AWS Key Management Service 키 또는 Amazon 리소스 이름 (ARN) 을 선택합니다.

   -또는-

   AWS KMS 키 생성을 선택합니다. 그런 다음 AWS KMS 키를 생성합니다.

7. (선택 사항) Support 사례 통합을 위한 서비스 액세스에서 이 re:Post에 대한 서비스 액세스 활성화를 선택합니다.

> **Note**
>
> 비공개 re:Post를 만든 후에도 이 옵션을 켤 수 있습니다.

   아래에서 기존 IAM 역할을 선택하거나 IAM 콘솔에서 새 역할을 생성하려면 검색 창을 사용하여 기존 IAM 역할을 찾으십시오.

   -또는-

   IAM 콘솔에서 새 역할 생성을 선택합니다.

   새 역할을 생성하려면 의 IAM 역할 생성 지침을 따르십시오.

   기존 서비스 역할을 사용하기로 선택한 경우 검색창에 사용하려는 역할의 ARN을 입력합니다. 드롭다운 목록에서 역할을 선택합니다.

   자세한 설명은 re:Post AWS Support Private에서 사례 생성 및 관리에 대한 액세스 관리 섹션을 참조하세요.

8. (선택 사항) 태그에서 새 태그 추가를 선택합니다. 그런 다음 다음 정보를 입력합니다.

   키에 사용자 지정 태그 키를 입력합니다.

   값에 사용자 지정 태그 값을 입력합니다.

   태그를 더 추가하려면 새 태그 추가를 선택합니다.

9. 이 re:Post 만들기를 선택합니다.

확인 페이지에서 비공개 re:Post가 생성되고 있음을 알 수 있습니다. 상태 필드에서 비공개 re:Post의 상태를 확인할 수 있습니다. 비공개 re:Post가 생성되면 상태 필드에 작성 중이라는 메시지가 표시됩니다.

비공개 re:Post를 생성하는 데 약 30분이 소요됩니다. 비공개 re:Post가 준비되면 상태 필드에 온라인이 표시됩니다. 설정 탭 아래에 나열된 프라이빗 re:Post에 대해 AWS에서 생성한 하위 도메인을 사용하여 프라이빗 re:Post에 액세스할 수 있습니다. 검토가 완료되면 설정 탭에서 프라이빗 re:Post의 사용자 지정 하위 도메인을 확인할 수 있습니다.

# re:Post AWS Support Private에서 사례 생성 및 관리에 대한 액세스 관리

AWS re:Post Private에서 AWS Support 사례 생성 및 관리에 대한 액세스를 관리하려면 AWS Identity and Access Management (IAM) 역할을 생성해야 합니다. 이 역할은 다음 AWS Support 작업을 대신 수행합니다.

- CreateCase
- AddCommunicationToCase
- ResolveCase

IAM 역할을 생성한 후 이 역할에 IAM 정책을 연결하여 해당 역할이 이러한 작업을 완료하는 데 필요한 권한을 갖도록 하십시오. re:Post 프라이빗 콘솔에서 프라이빗 re:Post를 생성할 때 이 역할을 선택합니다.

프라이빗 re:Post의 사용자는 IAM 역할에 부여한 것과 동일한 권한을 가집니다.

> **Important**
>
> IAM 역할 또는 IAM 정책을 변경하면 구성한 프라이빗 re:POST에 변경 내용이 적용됩니다.

다음 절차에 따라 IAM 역할 및 정책을 생성합니다.

주제

- 관리형 정책을 사용하거나 AWS 고객 관리형 정책을 생성하십시오.
- IAM 정책 예제
- IAM 역할 생성
- 문제 해결

## 관리형 정책을 사용하거나 AWS 고객 관리형 정책을 생성하십시오.

역할 권한을 부여하려면 AWS 관리형 정책 또는 고객 관리형 정책을 사용할 수 있습니다.

> **Tip**
>
> 정책을 수동으로 생성하지 않으려면 AWS 관리형 정책을 대신 사용하고 이 절차를 건너뛰는 것이 좋습니다. 관리형 정책에는 필요한 AWS Support권한이 자동으로 부여됩니다. 정책을 수동으로 업데이트할 필요가 없습니다. 자세한 설명은 AWS 관리형 정책: AWSRepostSpaceSupportOperationsPolicy 섹션을 참조하세요.

다음 절차에 따라 역할에 맞는 고객 관리형 정책을 생성합니다. 이 절차에서는 IAM 콘솔에서 JSON 정책 편집기를 사용합니다.

re:Post Private에 대한 고객 관리형 정책을 만들려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. JSON 탭을 선택합니다.
5. JSON을 입력한 다음 편집기에서 기본 JSON을 교체합니다. 예제 정책을 사용할 수 있습니다.
6. Next: Tags(다음: 태그)를 선택합니다.
7. (선택 사항) 태그를 키 값 페어로 사용하여 메타데이터를 정책에 추가할 수 있습니다.
8. Next: Review(다음: 검토)를 선택합니다.
9. Review Policy(정책 검토) 페이지에서 Name(이름)(예: *rePostPrivateSupportPolicy*) 및 Description(설명)(선택 사항)을 입력합니다(선택 사항).
10. 요약 페이지를 검토하여 정책이 허용하는 권한을 확인한 다음 Create policy (정책 생성) 를 선택합니다.

이 정책은 이 역할이 수행할 수 있는 작업을 정의합니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

## IAM 정책 예제

IAM 역할에 다음 예제 정책을 연결할 수 있습니다. 이 정책을 통해 역할은 필요한 모든 작업에 대한 전체 권한을 가질 수 AWS Support있습니다. 역할과 함께 비공개 re:Post를 구성한 후에는 비공개 re:Post의 모든 사용자에게 동일한 권한이 부여됩니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
   ],
   "Resource": "*"
  }
 ]
}
```

> **Note**
>
> re:Post Private의 AWS 관리형 정책 목록은 을 참조하십시오. AWS AWS re:Post 프라이빗 관리형 정책

정책을 업데이트하여 권한을 제거할 수 있습니다. AWS Support

각 작업에 대한 설명은 서비스 승인 참조에서 다음 항목을 참조하세요.

- AWS Support에 사용되는 작업, 리소스 및 조건 키
- Service Quotas에 사용되는 작업, 리소스 및 조건 키
- 에 대한 작업, 리소스 및 조건 키 AWS Identity and Access Management

## IAM 역할 생성

정책을 생성한 후 IAM 역할을 생성한 다음 이 정책을 해당 역할에 연결해야 합니다. re:Post Private 콘솔에서 비공개 re:Post를 생성할 때 이 역할을 선택합니다.

사례 생성 및 관리를 위한 AWS Support 역할을 만들려면

1. https://console.aws.amazon.com/iam/ 에서 AWS Management Console 로그인하고 IAM 콘솔을 엽니다.
2. 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. Trusted entity type(신뢰할 수 있는 엔터티 유형)에서 Custom trust policy(사용자 지정 정책)를 선택합니다.
4. 사용자 지정 신뢰 정책에 다음을 입력합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "Service": "repostspace.amazonaws.com"
   },
   "Action": [
    "sts:AssumeRole",
    "sts:SetSourceIdentity"
   ]
  }
 ]
}
```

5. 다음을 선택합니다.
6. 권한 정책 아래의 검색 창에 직접 만든 AWS 관리형 정책 또는 고객 관리형 정책 (예:) 을 입력합니다 *rePostPrivateSupportPolicy*. 서비스에 적용하려는 권한 정책 옆에 있는 확인란을 선택합니다.
7. 다음을 선택합니다.
8. 이름, 검토 및 생성 페이지에서 역할 이름에 이름을 입력합니다 (예:) *rePostPrivateSupportRole*.
9. (선택 사항)설명에 역할에 대한 설명을 입력합니다.
10. 신뢰 정책 및 권한을 검토하십시오.
11. (선택 사항) 태그를 키 값 페어로 사용하여 메타데이터를 역할에 추가할 수 있습니다. IAM에서 태그를 사용하는 방법에 대한 자세한 내용은 IAM 리소스 태깅을 참조하세요.
12. 역할 생성을 선택합니다. 이제 re:Post Private 콘솔에서 비공개 re:Post를 구성할 때 이 역할을 선택할 수 있습니다. 새 비공개 re:Post를 만드세요. 섹션을 참조하십시오.

자세한 내용은 IAM 사용 설명서의 AWS 서비스 (콘솔) 역할 생성을 참조하십시오.

# 문제 해결

re:Post Private에 대한 액세스를 관리하려면 다음 주제를 참조하십시오.

목차



## 비공개 re:Post의 특정 사용자가 특정 작업을 수행하지 못하도록 제한하고 싶습니다.

기본적으로 프라이빗 re:Post의 사용자는 생성한 IAM 역할에 연결하는 IAM 정책에 지정된 것과 동일한 권한을 가집니다. 즉, 비공개 re:Post에 있는 모든 사용자는 IAM 사용자가 있든 없든 관계없이 AWS Support 사례를 생성하고 관리할 수 있는 읽기 또는 쓰기 권한을 가집니다. AWS 계정

다음 모범 사례를 따르는 것이 좋습니다.

- 필요한 최소 권한이 있는 IAM 정책을 사용하십시오. AWS SupportAWS 관리형 정책: AWSRepostSpaceSupportOperationsPolicy 섹션을 참조하십시오.

## 프라이빗 re:Post를 구성할 때 생성한 IAM 역할이 보이지 않습니다.

re:Post Private; 목록의 IAM 역할에 IAM 역할이 나타나지 않는다면 이는 해당 역할에 re:Post Private이 신뢰할 수 있는 주체로 등록되어 있지 않거나 역할이 삭제되었음을 의미합니다. 기존 추적을 업데이트하거나 다른 역할을 생성할 수 있습니다. IAM 역할 생성 섹션을 참조하십시오.

## 내 IAM 역할에 권한이 없습니다

프라이빗 re:Post용으로 생성한 IAM 역할에는 원하는 작업을 수행할 수 있는 권한이 필요합니다. 예를 들어, 비공개 re:Post의 사용자가 지원 사례를 생성하도록 하려면 역할에 `support:CreateCase` 권한이 있어야 합니다. re:Post Private는 이 역할을 맡아 이러한 작업을 대신 수행합니다.

권한 누락에 대한 오류 메시지가 표시되는 경우 역할에 연결된 정책에 필요한 AWS Support권한이 있는지 확인하세요.

이전 IAM 정책 예제을 참조하세요.

내 IAM 역할이 유효하지 않다는 오류 메시지가 표시됩니다.

프라이빗 re:Post 구성에 맞는 역할을 선택했는지 확인하세요.

## 를 사용하여 사용자 액세스를 설정하고 관리합니다. AWS IAM Identity Center

re:Post Private는 와 통합되어 조직의 AWS IAM Identity Center 직원에게 ID 페더레이션을 제공합니다. IAM Identity Center를 사용하여 조직의 사용자를 만들거나 연결하고 모든 계정과 애플리케이션에 대한 액세스를 중앙에서 관리할 수 있습니다. AWS IAM 자격 증명 센터에 대한 자세한 내용은 AWS IAM 자격 증명 센터란? (AWS Single Sign-On의 후속) 을 참조하십시오. IAM ID 센터를 시작하는 방법에 대한 자세한 내용은 시작하기를 참조하십시오. IAM ID 센터를 사용하려면 해당 계정도 AWS Organizations 활성화해야 합니다.

## 프라이빗 re:Post를 사용자 지정하세요.

비공개 re:Post를 만든 후 한 명 이상의 관리자를 추가할 수 있습니다. 관리자는 re:Post Private 애플리케이션을 사용하여 비공개 re:Post를 시작하고 해당 애플리케이션 내에서 사용자를 관리합니다. 비공개 re:Post의 브랜딩을 사용자 정의하고, 태그를 추가하여 콘텐츠를 분류하고, 콘텐츠 자동 채우기를 위해 관심 주제를 선택할 수 있습니다. 자세한 내용은 AWS re:Post 프라이빗 관리 가이드를 참조하십시오.

## 사용자를 비공개 re:Post에 초대하십시오.

비공개 re:Post를 만든 후 한 명 이상의 사용자를 추가할 수 있습니다. 비공개 re:Post에서 사용자를 초대하여 협업할 수 있습니다. 사용자는 re:Post Private 애플리케이션을 사용하여 구성한 자격 증명을 사용하여 로그인합니다. 비공개 re:Post에 로그인한 후 사용자는 관심 주제에 맞는 맞춤형 교육 및 기술 콘텐츠를 비롯한 기존 콘텐츠를 찾아보거나 검색할 수 있습니다. 자세한 내용은 AWS re:Post 프라이빗 사용 설명서를 참조하십시오.

# re:Post 프라이빗 콘솔에서 비공개 re:Post를 관리하세요

이 섹션에서는 AWS re:Post 프라이빗 콘솔에서 프라이빗 re:Post를 관리하는 방법을 설명합니다.

주제



## 프라이빗 re:Post에 사용자 및 그룹을 추가합니다.

관리자인 경우 프라이빗 re:Post에 사용자와 그룹을 추가할 수 있습니다.

비공개 re:Post에 사용자 추가

1. https://console.aws.amazon.com/repost-private/ 에서 re:Post 프라이빗 콘솔을 엽니다.
2. 탐색 창에서 내 비공개 re:Posts 전체를 선택합니다.
3. 관리하려는 비공개 re:Post를 선택합니다.
4. 사용자(Users) 탭을 선택합니다.
5. 사용자에서 사용자 및 그룹 추가를 선택합니다.
6. 목록에서 비공개 re:Post에 추가할 사용자를 선택합니다. 그런 다음 [Assign] 을 선택합니다.

선택한 사용자가 비공개 re:Post에 추가되고 사용자 탭 아래에 나열됩니다.

비공개 re:Post에 그룹을 추가하세요

1. https://console.aws.amazon.com/repost-private/ 에서 re:Post 프라이빗 콘솔을 엽니다.
2. 탐색 창에서 내 비공개 re:Posts 전체를 선택합니다.
3. 관리하려는 비공개 re:Post를 선택합니다.
4. 그룹 탭을 선택합니다.

5. [사용자 및 그룹 추가] 를 선택합니다.
6. 목록에서 비공개 re:Post에 추가할 그룹을 선택합니다. 그런 다음 Assign을 선택합니다.

선택한 그룹이 비공개 re:Post에 추가되고 그룹 탭 아래에 나열됩니다.

## 비공개 re:Post의 그룹에 사용자를 추가합니다.

IAM ID 센터를 사용하여 프라이빗 re:Post의 기존 그룹에 새 사용자를 추가할 수 있습니다. 자세한 내용은 AWS IAM ID 센터 사용 설명서의 그룹에 사용자 추가를 참조하십시오.

## 비공개 re:Post에 사용자 및 그룹을 초대하십시오.

다음 단계에 따라 AWS re:Post Private의 프라이빗 re:Post에 사용자와 그룹을 초대하십시오.

1. https://console.aws.amazon.com/repost-private/ 에서 re:Post 프라이빗 콘솔을 엽니다.
2. 탐색 창에서 내 비공개 re:Posts 전체를 선택합니다.
3. 관리하려는 비공개 re:Post를 선택합니다.
4. 사용자를 비공개 re:Post에 초대하려면 사용자 탭을 선택합니다.

   목록에서 비공개 re:Post에 초대할 사용자를 선택합니다. 그런 다음 re:POST를 실행할 사용자 온보딩을 선택합니다.
5. 이 비공개 re:Post에 사용자 등록 대화 상자에 다음 정보를 입력합니다.

   제목에는 보내는 이메일 메시지의 제목을 입력합니다.

   Body에는 비공개 re:Post를 위한 환영 메시지를 입력합니다.

   온보딩 이메일 보내기를 선택합니다.
6. 그룹을 비공개 re:Post에 초대하려면 그룹 탭을 선택합니다.

   목록에서 비공개 re:Post에 초대할 그룹을 선택합니다. 그런 다음 re:Post를 실행할 온보드 그룹을 선택합니다.
7. 이 비공개 re:Post에 그룹 등록하기 대화 상자에 다음 정보를 입력합니다.

   제목에는 보내는 이메일 메시지의 제목을 입력합니다.

   Body에는 비공개 re:Post를 위한 환영 메시지를 입력합니다.

온보딩 이메일 보내기를 선택합니다.

비공개 re:Post에 로그인하는 방법에 대한 정보가 포함된 환영 메시지가 선택된 모든 사용자 및 그룹에게 전송됩니다.

# 비공개 re:Post에 있는 사용자를 관리자로 승격시킵니다.

프라이빗 re:POST 사용자를 관리자로 승격하려면 다음 단계를 따르십시오.

1. https://console.aws.amazon.com/repost-private/ 에서 re:Post Private 콘솔을 엽니다.
2. 탐색 창에서 내 비공개 re:Posts 전체를 선택합니다.
3. 관리하려는 비공개 re:Post를 선택합니다.
4. 사용자(Users) 탭을 선택합니다.
5. 관리자로 승격시킬 사용자를 한 명 이상 선택합니다.
6. 역할 편집을 선택한 다음 관리자로 지정을 선택합니다.

선택한 사용자는 관리자로 승격됩니다. 사용자 탭에서 해당 사용자의 역할이 관리자로 업데이트됩니다.

# 비공개 re:Post에서 사용자 또는 그룹을 삭제하세요

관리자인 경우 프라이빗 re:Post에서 사용자 또는 그룹을 제거할 수 있습니다.

비공개 re:Post에서 사용자를 삭제하세요

1. https://console.aws.amazon.com/repost-private/ 에서 re:Post 프라이빗 콘솔을 엽니다.
2. 탐색 창에서 내 비공개 re:Posts 전체를 선택합니다.
3. 관리하려는 비공개 re:Post를 선택합니다.
4. 사용자 아래의 목록에서 비공개 re:Post에서 제거하려는 사용자를 선택합니다. 그런 다음 제거를 선택합니다.

선택한 사용자가 비공개 re:Post에서 제거됩니다. 제거된 사용자에 대한 정보는 더 이상 사용자 탭 아래에 표시되지 않습니다.

비공개 re:Post에서 그룹을 삭제하세요

1. https://console.aws.amazon.com/repost-private/ 에서 re:Post 프라이빗 콘솔을 엽니다.
2. 탐색 창에서 내 비공개 re:Posts 전체를 선택합니다.
3. 관리하려는 비공개 re:Post를 선택합니다.
4. 그룹 탭을 선택합니다.
5. 목록에서 비공개 re:Post에서 제거하려는 그룹을 선택합니다. 그런 다음 삭제를 선택합니다.

선택한 그룹이 비공개 re:Post에서 제거됩니다. 제거된 그룹에 대한 정보는 더 이상 그룹 탭 아래에 표시되지 않습니다.

## 비공개 re:Post에 AWS 직원 추가 또는 삭제

엔터프라이즈 또는 엔터프라이즈 온램프 지원 플랜을 보유한 경우 프라이빗 re:Post에서 AWS 직원을 추가하거나 제거할 수 있습니다. 자세한 내용은 컨시어지 지원 또는 기술 계정 관리자 (TAM) 에게 문의하십시오.

## re:Post 비공개에서 비공개 re:Post를 삭제하세요

AWS re:Post 프라이빗에서 프라이빗 re:Post를 삭제하려면 다음 단계를 따르십시오.

1. https://console.aws.amazon.com/repost-private/ 에서 re:Post 프라이빗 콘솔을 엽니다.
2. 탐색 창에서 내 비공개 re:Posts 전체를 선택합니다.
3. 관리하려는 비공개 re:Post를 선택한 다음 삭제를 선택합니다.
4. 모든 옵션을 선택하여 비공개 re:Post와 이와 관련된 데이터를 영구 삭제할 것인지 확인하고 확인합니다.

> **Important**
>
> 비공개 re:POST를 삭제하면 비공개 re:POST와 관련된 모든 구성 정보가 삭제됩니다. 비공개 re:Post를 삭제한 후에는 해당 re:Post에서 콘텐츠를 복원할 수 없습니다.

5. 추가 서면 동의를 요구하는 메시지가 표시되면 비공개 re:Post의 이름을 입력하세요. 그런 다음 [삭제(Delete)]를 선택합니다.

비공개 re:Post가 삭제되는 데 약 30분이 소요됩니다.

# AWS re:포스트 프라이빗 모니터링

모니터링은 AWS re:Post Private 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWSre:Post Private를 감시하고, 문제 발생 시 보고하고, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon은 실행 중인 AWS 리소스와 애플리케이션을 AWS 실시간으로 CloudWatch 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 CloudWatch 추적하고 필요할 때 새 인스턴스를 자동으로 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.
- AWS CloudTrail사용자 또는 사용자를 위해 이루어진 API 호출 AWS 계정 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자 및 계정이 AWS를 직접 호출했는지, 어떤 소스 IP 주소에 직접 호출이 이루어졌는지, 언제 직접 호출이 발생했는지 확인할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

## 아마존을 통한 AWS re:POST 프라이빗 모니터링 CloudWatch

원시 데이터를 수집하여 읽기 쉬운 거의 실시간 지표로 처리하는 CloudWatch Amazon을 사용하여 AWS re:Post Private를 모니터링할 수 있습니다. 이러한 통계는 15개월 동안 보관되므로 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스 성능을 더 잘 파악할 수 있습니다. 특정 임계값을 주시하다가 해당 임계값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

re:Post Private 서비스는 네임스페이스에 다음과 같은 지표를 보고합니다`AWS/rePostPrivate`.

| 지표 | 설명 |
| --- | --- |
| `NumberOfSpaces` | 현재 계정에 있는 비공개 re:Posts의 수입니다.<br><br>단위: 개수 |
| `NumberOfUsers` | 비공개 re:Post의 사용자 수 이 지표는 spaceID를 측정기준으로 사용합니다.<br><br>단위: 개수 |

| 지표 | 설명 |
| --- | --- |
| ContentSize | 비공개 re:Post에 있는 콘텐츠의 양 이 지표는 spaceID를 측정기준으로 사용합니다.<br><br>단위: 바이트 |

re:Post Private 지표에는 다음과 같은 측정기준이 지원됩니다.

| 차원 | 설명 |
| --- | --- |
| spaceId | 비공개 re:Post의 고유 식별자입니다. |

# 를 사용하여 AWS re:POST 프라이빗 API 호출 로깅 AWS CloudTrail

AWS re:Post Private은 re:Post Private에서 사용자, 역할 또는 서비스가 수행한 작업에 대한 기록을 제공하는 AWS 서비스인 서비스와 통합되어 있습니다. AWS CloudTrail CloudTrail re:Post Private에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 re:Post 프라이빗 콘솔에서의 호출 및 re:Post 프라이빗 API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 re:Post Private용 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 re:Post Private에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail사용 설명서를 참조하십시오.

## re:개인 정보 게시 CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. re:Post Private에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록 작업을 참조하십시오.

re:Post Private의 이벤트를 포함하여 내 이벤트의 진행 중인 기록을 보려면 트레일을 생성하십시오 AWS 계정. 트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 콘솔에

서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- AWS 계정에 대한 추적 생성
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 re:Post 프라이빗 작업은 AWS re:Post 프라이빗 API 레퍼런스에 의해 CloudTrail 기록되고 문서화됩니다. re:Post Private은 다음 작업을 로그 파일에 이벤트로 기록할 수 있도록 지원합니다. CloudTrail

- CreateSpace
- DeleteSpace
- DeregisterAdmin
- GetSpace
- ListSpaces
- ListTagsForResource
- RegisterAdmin
- SendInvites
- TagResource
- UntagResource
- UpdateSpace

re:Post Private은 다음 작업을 로그 파일에 이벤트로 기록하는 것을 지원합니다. AWS Support CloudTrail

- CreateCase
- AddCommunicationToCase
- ResolveCase

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 했는지.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

## re:Post 프라이빗 로그 파일 항목에 대한 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `CreateSpace` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.


```
{
   "eventVersion": "1.08",
   "userIdentity": {
       "type": "AssumedRole",
       "principalId": "AROAQM47QIR7WLEXAMPLE:user",
       "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
       "accountId": "123456789012",
       "accessKeyId": "EXAMPLE_KEY_ID",
       "sessionContext": {
           "sessionIssuer": {
               "type": "Role",
               "principalId": "AROAQM47QIR7WLEXAMPLE",
               "arn": "arn:aws:iam::123456789012:role/User",
               "accountId": "123456789012",
               "userName": "User"
           },
           "webIdFederationData": {},
           "attributes": {
               "creationDate": "2023-11-06T19:24:39Z",
               "mfaAuthenticated": "false"
           }
```

```
        }
    },
    "eventTime": "2023-11-06T21:37:44Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "CreateSpace",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
    "requestParameters": {
        "spaceName": "Test space name",
        "spaceSubdomain": "customsubdomain",
        "tagSet": {},
        "tier": "2000",
        "roleArn": "",
        "spaceDescription": "Test space description"
    },
    "responseElements": {
        "spaceId": "SPLPWvQmv9SIWYF30EXAMPLE",
        "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
    },
    "requestID": "71d815e0-6632-4ec9-9fac-92af3e4a86dc",
    "eventID": "30a6c3da-ce2e-4931-ba5d-b3cc7cf16ec8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. `RegisterAdmin`


```
 {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR7WLEXAMPLE:user",
        "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-07T21:17:19Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-07T21:24:23Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "RegisterAdmin",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
    "requestParameters": {
        "adminId": "08612310-a0f1-7063-3e54-fb2960444dd1",
        "spaceId": "SPlYNZE-ylQEmAXpmEXAMPLE"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
    },
    "requestID": "9939ebbe-8599-4f9a-827b-4995e3006001",
    "eventID": "e1873b18-f80c-4934-9ff2-bf5b35c78031",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. `ListSpaces`

```
 {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR7WLEXAMPLE:user",
        "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-09T22:28:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-09T22:38:34Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "ListSpaces",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "95be587b-c04f-4eb0-9269-12fee33ae2e3",
    "eventID": "9777da32-545f-44c4-af0b-1d9109b8cbc3",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. `ResolveCase` 이 로그 항목의 `sourceIdentity` 요소를 사용하여 사례를 해결한 사용자를 식별할 수 있습니다.


```
 {
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR76DQZ7N5WX:create-support-case-
Uk1iHNTWQEOLmR2BR1FDJQ",
        "arn": "arn:aws:sts::123456789012:assumed-role/AWSRepostSpaceRole/create-
support-case-Uk1iHNTWQEOLmR2BR1FDJQ",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR76DQZ7N5WX",
                "arn": "arn:aws:iam::123456789012:role/AWSRepostSpaceRole",
                "accountId": "123456789012",
                "userName": "AWSRepostSpaceRole"
            },
            "attributes": {
                "creationDate": "2023-11-17T21:46:42Z",
                "mfaAuthenticated": "false"
            },
            "sourceIdentity": "28e17330-10f1-705d-7cba-3a62a6b10e2e"
        }
    },
    "eventTime": "2023-11-17T21:46:44Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "ResolveCase",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.68.27.29",
    "userAgent": "aws-sdk-nodejs/2.1363.0 linux/v16.20.2 exec-env/AWS_ECS_FARGATE
 promise",
    "requestParameters": {
        "caseId": "case-123456789012-muen-2023-75d2c35481b96357"
    },
    "responseElements": {
        "initialCaseStatus": "unassigned",
        "finalCaseStatus": "resolved"
    },
    "requestID": "594b91c6-df1c-47e4-a834-d67d67f34b9d",
```

```
    "eventID": "7fc9cbe4-c8d5-4d61-a016-e076de272fff",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "support.us-west-2.amazonaws.com"
    }
}
```

# re:Post 비공개 문제 해결

다음 정보는 AWS re:Post Private와 관련된 문제를 해결하는 데 도움이 될 수 있습니다.

주제



## 특정 지역에서 프라이빗 re:Post를 설정할 수 없습니다. AWS

re:Post Private은 미국 동부 (버지니아 북부), 미국 서부 (오레곤), 유럽 (프랑크푸르트), 아시아 태평양 (싱가포르), 아시아 태평양 (시드니), 캐나다 (중부), 유럽 (아일랜드) 지역에서만 사용할 수 있습니다. 다음 지역 중 하나에서 비공개 re:Post를 만들고 있는지 확인하세요.

## 내 계정에서 비공개 re:Post를 설정할 수 없어요

계정을 AWS IAM Identity Center 활성화하고 프라이빗 re:Post를 생성하려는 지역과 동일한 지역에 IAM ID 센터를 설정했는지 확인하십시오. 자세한 정보는 필수 조건을 참조하세요.

## 비공개 re:Post에서는 사용자 또는 그룹을 관리할 수 없습니다.

비공개 re:Post를 편집하고 비공개 re:Post에서 사용자와 그룹을 관리하는 데 필요한 권한이 있는지 확인하세요. 자세한 내용은 AWS re:Post 프라이빗 자격 증명 기반 정책 예제을(를) 참조하세요.

# 문서 이력

다음 표에는 AWS re:Post Private의 설명서 릴리스가 설명되어 있습니다.

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 업데이트 | 미국 동부 (버지니아 북부), 아시아 태평양 (시드니), 캐나다 (중부), 유럽 (아일랜드) 을 지원 지역에 추가 | 2024년 5월 10일 |
| 업데이트 | 지원 지역에 아시아 태평양 (싱가포르) 추가 | 2024년 3월 6일 |
| 신규 리소스 | AWS re:Post Private용 AWS 관리형 정책에 대한 설명서가 추가되었습니다. | 2023년 11월 26일 |
| 최초 릴리스 | re:Post 프라이빗 콘솔 관리 가이드의 최초 릴리스 | 2023년 11월 26일 |

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.