가드레일 설정 및 미리 서명된 URLs 모니터링

AWS 권장 가이드

AWS 권장 가이드: 가드레일 설정 및 미리 서명된 URLs 모니터링

Table of Contents

소개 1
대상 독자 1
목표 1
사전 조건 2
미리 서명된 URLs 개요 3
미리 서명된 요청 사용에 대한 동기 부여 4
임시 AWS STS 자격 증명과의 비교 4
서명 전용 솔루션과의 비교 5
사전 서명된 요청 식별 6
미리 서명된 URL을 사용한 요청 식별 6
다른 유형의 사전 서명된 요청 식별 6
요청 패턴 식별 7
미리 서명된 요청 사용 모범 사례 12
기본 모범 사례 12
최소 권한 원칙을 적용 12
데이터 경계 구현 13
추가 가드레일 13
s3:signatureAge용 가드레일 13
리소스 제어 정책 17
s3:authType용 가드레일 18
미리 서명된 가드레일 및 예외를 다른 가드레일에 결합 20
s3:signatureAge에 대한 제한 사항 20
대규모 버킷 대상 지정 21
상호작용 및 완화 조치 로깅 22
완화 22
FAQ 24
미리 서명된 요청을 여러 번 사용할 수 있습니까? 이것이 보안 위험인가요? 24
의도한 사용자 이외의 사람이 미리 서명된 요청을 사용할 수 있습니까? 24
권한이 있는 사용자가 미리 서명된 요청을 사용하여 데이터를 유출할 수 있습니까? 24
권한이 없는 방식으로 공유되었다고 의심되는 경우 미리 서명된 URL의 액세스를 거부할 수 있습니까? 25
리소스 26
Amazon S3 설명서 26
기타 참조 6

부록 A: 미리 서명된 URLs AWS 서비스 사용 방법 27
Amazon S3 콘솔 27
Amazon S3 Object Lambda 28
AWS Lambda 리전 간 CopyObject 29
AWS Lambda GetFunction 29
Amazon ECR 30
Amazon Redshift Spectrum 30
Amazon SageMaker AI Studio 30
부록 B: 미리 서명된 URLs 미치는 영향 AWS 서비스 32
s3:signatureAge용 가드레일 32
네트워크 제한을 사용하지 않는 경우 s3:authType에 대한 가드레일 32
문서 기록 34
..... xxxv

가드레일 설정 및 미리 서명된 URLs 모니터링

Ryan Baker, Amazon Web Services(AWS)

2025년 8월(문서 기록)

보안은 모든 회사에 중요한 관심사이며 AWS Well-Architected Framework의 주요 원칙입니다. 보안 엔지니어는 조직 제어 요구 사항에 맞는 관리 가드레일을 구현해야 합니다. AWS Well-Architected Framework에서 가드레일은 활동을 제한하는 경계를 정의합니다.

이 가이드에서는 Amazon Simple Storage Service(Amazon S3) 객체와 함께 사용되는 미리 서명된 URLs 사용에 대한 배경 정보와 모범 사례를 제공합니다. 미리 서명된 URLs 사용하면 유효한 자격 증명에 액세스할 수 있는 사용자 또는 애플리케이션이 미리 서명되고 정의된 만료 시간까지 수락되는 요청을 생성할 수 있습니다. 미리 서명된 URLs의 일반적인 사용 사례는 이러한 요청을 공유하여 객체 또는 리소스에 대한 액세스를 확장하는 것입니다. 미리 서명된 공유 요청은 특정 요청을 수행할 권한이 있는 시스템 또는 사용자가 생성한 다음 다른 시스템 또는 사용자에게 전송하여 동일한 요청을 수행할 수 있는 기능을 확장할 수 있습니다.

이 가이드에서는 다음을 학습합니다.

- 미리 서명된 URLs의 개념
- 미리 서명된 URLs의 사용 사례
- 권장 및 선택적 가드레일
- 모니터링 옵션
- 미리 서명된 URLs을 AWS 서비스 사용하는 방법의 예

대상 독자

이 안내서는 AWS 클라우드에서 보안 제어 구현을 담당하는 아키텍트와 보안 엔지니어를 대상으로 합니다.

목표

보안 엔지니어는 솔루션 빌더가 보안을 구현하는 방식과 최종 사용자의 액세스 유형을 알고 싶을 것입니다. 이 가이드에서는 Amazon S3에서 자주 사용되는 미리 서명된 URLs인 한 가지 유형의 액세스에 대해 설명합니다. 미리 서명된 URLs 빌더에게 인증 메커니즘을 효율적으로 브리징할 수 있는 옵션을 제공합니다.

Amazon S3에서 미리 서명된 URLs 고유한 요청 범주를 나타냅니다. 보안 엔지니어는 이러한 요청을 모니터링하고 관리하여 적절하고 필요한 경우에만 요청을 사용할 수 있습니다. 이 가이드의 목표는 보안 엔지니어가 이러한 유형의 상위 수준 감독을 제공하도록 지원하는 것입니다.

이 가이드를 읽은 후에는 미리 서명된 URL이 무엇인지, 일반적으로 사용되는 시기, 사용 동기를 이해해야 합니다.

사전 조건

AWS에서 보안 제어 구현 가이드에 설명된 대로 회사가 보안 정책, 제어 목표 또는 표준을 정의하지 않은 경우이 가이드를 진행하기 전에 해당 거버넌스 작업을 완료하는 것이 좋습니다.

시작하기 전에 제어 및 모니터링에 대한 권장 및 선택적 모범 사례도 숙지해야 합니다. 자세한 내용은 다음을 참조하세요.

- 서비스 제어 정책(AWS Organizations 문서)
- 리소스 제어 정책(AWS Organizations 문서)
- Amazon S3에 대한 버킷 정책(Amazon S3 설명서)
- 서버 액세스 로깅을 사용하여 요청 로깅(Amazon S3 설명서)
- 를 사용하여 Amazon S3 API 호출 로깅 AWS CloudTrail(Amazon S3 설명서)

미리 서명된 URLs 개요

미리 서명된 URL은 AWS Identity and Access Management (IAM) 서비스에서 인식하는 HTTP 요청 유형입니다. 이 유형의 요청을 다른 AWS 모든 요청과 구별하는 것은 X-Amz-Expires 쿼리 파라미터입니다. 다른 인증된 요청과 마찬가지로 미리 서명된 URL 요청에는 서명이 포함됩니다. 미리 서명된 URL 요청의 경우이 서명은에서 전송됩니다`X-Amz-Signature`. 서명은 서명 버전 4 암호화 작업을 사용하여 다른 모든 요청 파라미터를 인코딩합니다.

> 참고
>
> - 서명 버전 2는 현재 더 이상 사용되지 않지만 일부 에서는 여전히 지원됩니다 AWS 리전. 이 가이드는 서명 버전 4 서명에 적용됩니다.
> - 수신 서비스는 서명되지 않은 헤더를 처리할 수 있지만 모범 사례에 따라 해당 옵션에 대한 지원이 제한되고 대상으로 지정됩니다. 달리 명시되지 않는 한 요청을 수락하려면 모든 헤더에 서명해야 한다고 가정합니다.

`X-Amz-Expires` 파라미터를 사용하면 인코딩된 날짜 시간과 더 큰 편차로 서명을 유효하게 처리할 수 있습니다. 서명 유효성의 다른 측면은 여전히 평가됩니다. 임시인 경우 서명 자격 증명은 서명이 처리될 때 만료되지 않아야 합니다. 서명 자격 증명은 처리 시 충분한 권한이 있는 IAM 보안 주체에 연결되어야 합니다.

미리 서명된 URLs 미리 서명된 요청의 하위 집합입니다.

미리 서명된 URL이 향후 요청에 서명하는 유일한 방법은 아닙니다. Amazon S3는 일반적으로 미리 서명된 POST 요청도 지원합니다. 미리 서명된 POST 서명은 서명된 정책을 준수하고 해당 정책에 포함된 만료 날짜가 있는 업로드를 허용합니다.

요청에 대한 서명은 미래 날짜일 수 있지만 흔하지 않습니다. 기본 자격 증명이 유효한 한 서명 알고리즘은 미래 날짜를 금지하지 않습니다. 그러나 이러한 요청은 유효한 타이밍 기간까지 성공적으로 처리되지 않으므로 대부분의 사용 사례에서 미래 날짜는 실용적이지 않습니다.

미리 서명된 요청은 무엇을 허용하나요?

미리 서명된 요청은 요청에 서명하는 데 사용된 자격 증명에서 허용하는 작업만 허용할 수 있습니다. 자격 증명이 미리 서명된 요청에 의해 지정된 작업을 암시적으로 또는 명시적으로 거부하는 경우 미리 서명된 요청은 전송될 때 거부됩니다. 이는 다음에 적용됩니다.

- 자격 증명과 연결된 세션 정책
- 자격 증명과 연결된 보안 주체와 연결된 자격 증명 기반 정책
- 세션 또는 보안 주체에 영향을 미치는 리소스 정책
- 세션 또는 보안 주체에 영향을 미치는 서비스 제어 정책
- 세션 또는 보안 주체에 영향을 미치는 리소스 제어 정책

미리 서명된 요청 사용에 대한 동기 부여

보안 엔지니어는 솔루션 빌더가 미리 서명된 URLs을 사용하도록 동기를 부여하는 요인을 알고 있어야 합니다. 무엇이 필요하고 무엇이 선택 사항인지 이해하면 솔루션 빌더와 통신하는 데 도움이 됩니다. 동기 부여에는 다음이 포함될 수 있습니다.

- Amazon S3의 확장성을 활용하면서 비 IAM 인증 메커니즘을 지원합니다. 핵심 동기는 Amazon S3와 직접 통신하여이 서비스에서 제공하는 기본 제공 확장성의 이점을 활용하는 것입니다. 이러한 직접 통신이 없으면 솔루션은 PutObject 및 GetObject 호출로 전송되는 재전송 바이트의 로드를 지원해야 합니다. 총 부하에 따라이 요구 사항에는 솔루션 빌더가 피하고 싶을 수 있는 조정 문제가 추가됩니다.

  URLs 외부에서 임시 자격 증명 AWS Security Token Service (AWS STS) 또는 서명 버전 4 서명을 사용하는 등 Amazon S3와 직접 통신하는 다른 방법은 사용 사례에 적합하지 않을 수 있습니다. Amazon S3는 자격 증명을 통해 AWS 사용자를 식별하는 반면, 미리 서명된 요청은 AWS 자격 증명 이외의 메커니즘을 통해 식별을 수임합니다. 미리 서명된 요청을 통해 데이터에 대한 직접 통신을 유지하면서 이러한 차이를 브리징할 수 있습니다.
- 브라우저의 URL에 대한 URLs. URLs은 브라우저에서 이해되지만 자격 AWS STS 증명 및 서명 버전 4 서명은 이해되지 않습니다. 이는 브라우저 기반 솔루션과 통합할 때 유용합니다. 대체 솔루션은 더 많은 코드가 필요하고, 대용량 파일에 더 많은 메모리를 사용하며, 맬웨어 및 바이러스 스캐너와 같은 확장명으로 다르게 취급될 수 있습니다.

임시 AWS STS 자격 증명과의 비교

임시 자격 증명은 미리 서명된 요청과 유사합니다. 둘 다 만료되고, 액세스 범위 조정을 허용하며, 일반적으로 비 IAM 자격 증명을 AWS 자격 증명이 필요한 사용과 연결하는 데 사용됩니다.

임시 AWS STS 자격 증명의 범위를 단일 S3 객체 및 작업으로 엄격하게 지정할 수 있지만 AWS STS APIs에는 제한이 있기 때문에 조정 문제가 발생할 수 있습니다. (자세한 내용은 IAM 및 AWS re:Post 웹 사이트의 API 제한을 해결하려면 어떻게 해야 합니까? 또는 "Rate exceeded" 오류를 AWS STS 참

조하세요.) 또한 생성된 각 자격 증명에는 지연 시간과 복원력에 영향을 미칠 수 있는 새로운 종속성을 추가하는 AWS STS API 호출이 필요합니다. 임시 AWS STS 자격 증명은 최소 만료 시간이 15분인 반면, 미리 서명된 요청은 더 짧은 기간을 지원할 수 있습니다. (올바른 조건을 고려할 때 60초는 실용적입니다.)

서명 전용 솔루션과의 비교

미리 서명된 요청의 유일한 고유 비밀 구성 요소는 서명 버전 4 서명입니다. 클라이언트가 요청의 다른 세부 정보를 알고 있고 해당 세부 정보와 일치하는 유효한 서명이 제공된 경우 유효한 요청을 보낼 수 있습니다. 유효한 서명이 없으면 할 수 없습니다.

미리 서명된 URLs과 서명 전용 솔루션은 암호화 방식으로 유사합니다. 그러나 서명 전용 솔루션은 쿼리 문자열 파라미터 대신 HTTP 헤더를 사용하여 서명을 전송하는 기능(로깅 상호 작용 및 완화 섹션 참조)과 같은 실질적인 이점이 있습니다. 또한 관리자는 쿼리 문자열이 메타데이터로 더 일반적으로 처리되는 반면 헤더는 덜 일반적으로 처리된다는 점을 고려해야 합니다.

반면, AWS SDKs 서명을 직접 생성하고 사용하는 데 대한 지원을 덜 제공합니다. 서명 전용 솔루션을 구축하려면 더 많은 사용자 지정 코드가 필요합니다. 실제 관점에서 보안을 위해 사용자 지정 코드 대신 라이브러리를 사용하는 것이 일반적인 모범 사례이므로 서명 전용 솔루션의 코드에는 추가 조사가 필요합니다.

서명 전용 솔루션은 `X-Amz-Expires` 쿼리 문자열을 사용하지 않으며 명시적인 유효 기간을 제공하지 않습니다. IAM은 명시적 만료 시간이 없는 서명의 암시적 유효 기간을 관리합니다. 이러한 암시적 기간은 게시되지 않습니다. 일반적으로 변경되지는 않지만 보안을 염두에 두고 관리되므로 유효 기간에 종속되어서는 안 됩니다. 만료 날짜를 명시적으로 제어하는 것과 IAM이 만료를 관리하는 것 사이에는 장단점이 있습니다.

관리자는 서명 전용 솔루션을 선호할 수 있습니다. 그러나 실제적으로는 구축된 대로 솔루션을 지원해야 합니다.

사전 서명된 요청 식별

미리 서명된 URL을 사용한 요청 식별

Amazon S3는 요청 수준에서 사용을 모니터링하기 위한 두 가지 기본 제공 메커니즘, 즉 Amazon S3 서버 액세스 로그와 AWS CloudTrail 데이터 이벤트를 제공합니다. 두 메커니즘 모두 미리 서명된 URL 사용을 식별할 수 있습니다.

사전 서명된 URL 사용에 대한 로그를 필터링하려면 인증 유형을 사용할 수 있습니다. 서버 액세스 로그의 경우 인증 유형 필드를 살펴보십시오. 인증 유형 필드는 Amazon Athena 테이블에 정의될 때 일반적으로 authtype으로 지정됩니다. 예를 들어 CloudTrail, 현장에서 AuthenticationMethod확인해 보십시오. `additionalEventData` 두 경우 모두 미리 서명된 URL을 사용하는 요청의 필드 값은 이고 다른 대부분의 요청의 필드 값은 `AuthHeader` 입니다. `QueryString`

`QueryString`사용량이 항상 미리 서명된 URL과 연관되는 것은 아닙니다. 검색을 미리 서명된 URL 사용으로만 제한하려면 쿼리 문자열 파라미터가 포함된 요청을 찾아보세요. `X-Amz-Expires` 서버 액세스 로그의 경우 Request-URI를 검사하여 쿼리 문자열에 `X-Amz-Expires` 매개 변수가 있는 요청을 찾아보십시오. 의 경우 CloudTrail, `requestParameters` 요소에 요소가 있는지 검사하십시오. `X-Amz-Expires`

```
{"Records": [{…, "requestParameters": {…, "X-Amz-Expires": "300"}}, …]}
```

다음 Athena 쿼리는 이 필터를 적용합니다.

```
SELECT * FROM {athena-table} WHERE
  authtype = 'QueryString' AND
  request_uri LIKE '%X-Amz-Expires=%';
```

AWS CloudTrail Lake의 경우 다음 쿼리는 이 필터를 적용합니다.

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'QueryString' AND
  requestParameters['X-Amz-Expires'] IS NOT NULL
```

다른 유형의 사전 서명된 요청 식별

POST 요청에는 Amazon S3 서버 액세스 로그와 `HtmlForm` 같은 고유한 인증 유형도 CloudTrail 있습니다. 이 인증 유형은 덜 일반적이므로 사용자 환경에서 이러한 요청을 찾지 못할 수도 있습니다.

다음 Athena 쿼리는 다음에 대한 필터를 적용합니다. `HtmlForm`

```
SELECT * FROM {athena-table} WHERE
  authtype = 'HtmlForm';
```

CloudTrail Lake의 경우 다음 쿼리가 필터를 적용합니다.

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'HtmlForm'
```

요청 패턴 식별

이전 섹션에서 설명한 기술을 사용하여 미리 서명된 요청을 찾을 수 있습니다. 하지만 이 데이터를 유용하게 활용하려면 패턴을 찾아야 합니다. 간단한 쿼리 `TOP 10` 결과를 통해 통찰력을 얻을 수 있지만, 충분하지 않은 경우 다음 표의 그룹화 옵션을 사용하세요.

그룹화 옵션	서버 액세스 로그	CloudTrail호수	설명
사용자 에이전트	`GROUP BY useragent`	`GROUP BY userAgent`	이 그룹화 옵션은 요청의 출처와 목적을 찾는 데 도움이 됩니다. 사용자 에이전트는 사용자가 제공하며 인증 또는 권한 부여 메커니즘으로서 신뢰할 수 없습니다. 하지만 패턴을 찾아보면 많은 것을 알 수 있습니다. 왜냐하면 대부분의 클라이언트는 적어도 부분적으로는 사람이 읽을 수 있는 고유한 문자열을 사용하기 때문입니다.
요청자	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	이 그룹화 옵션은 요청에 서명한 IAM 보안 주체를 찾는 데 도움이

그룹화 옵션	서버 액세스 로그	CloudTrail호수	설명
			됩니다. 이러한 요청을 차단하거나 기존 요청에 대한 예외를 생성하는 것이 목적이라면 이러한 쿼리는 해당 목적에 필요한 충분한 정보를 제공합니다. IAM 모범 사례에 따라 역할을 사용하면 역할의 소유자가 명확하게 식별되므로 해당 정보를 사용하여 자세한 내용을 알아볼 수 있습니다.

그룹화 옵션	서버 액세스 로그	CloudTrail호수	설명
소스 IP 주소	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	이 옵션은 Amazon S3에 도달하기 전 마지막 네트워크 변환 홉을 기준으로 그룹화합니다. • 트래픽이 NAT 게이트웨이를 통과하는 경우 이 주소가 NAT 게이트웨이 주소가 됩니다. • 트래픽이 인터넷 게이트웨이를 통과하는 경우 이 주소가 인터넷 게이트웨이로 트래픽을 보낸 퍼블릭 IP 주소가 됩니다. • 트래픽이 외부에서 발생하는 AWS경우 이 주소는 오리진과 연결된 공용 인터넷 주소가 됩니다. • 게이트웨이 가상 사설 클라우드 (VPC) 엔드포인트를 통과하는 경우 이 주소는 VPC에 있는 인스턴스의 IP 주소가 됩니다.

그룹화 옵션	서버 액세스 로그	CloudTrail호수	설명
			• 퍼블릭 가상 인터페이스 (VIF) 를 통과하는 경우 이는 요청자의 온프레미스 IP 또는 IP 주소만 노출하는 프록시 서버 또는 방화벽과 같은 중개자의 IP가 됩니다. • 인터페이스 VPC 엔드포인트를 통과하는 경우 이는 VPC에 있는 인스턴스의 IP 주소일 수 있습니다. 다른 VPC 또는 온프레미스 네트워크의 IP 주소일 수도 있습니다. 퍼블릭 VIF와 마찬가지로 이 주소는 모든 중개자의 IP 주소일 수 있습니다. 이 데이터는 네트워크 제어를 적용하는 것이 목표인 경우 유용합니다. 네트워크마다 사설 IP 주소가 중복될 수 있으므로 이 옵션을 `endpoint` (서버 액세스 로그의 경우) 또는 `vpcEndpointId` (CloudTrail Lake용) 등의 데이터와 결합하

그룹화 옵션	서버 액세스 로그	CloudTrail호수	설명
			여 출처를 명확히 해야 할 수도 있습니다.
S3 버킷 이름	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	이 그룹화 옵션은 요청을 받은 버킷을 찾는 데 도움이 됩니다. 이를 통해 예외의 필요성을 파악할 수 있습니다.

미리 서명된 요청 사용 모범 사례

이 섹션에서는 보안 엔지니어가 고려해야 하는 미리 서명된 요청을 사용하는 모범 사례를 설명합니다. 지침에는 다음이 포함됩니다.

- 모든 조직이 따라야 하는 기본 모범 사례입니다.
- 고려해야 할 관행이지만 부분적으로 구현하거나 예외적으로 구현하기로 결정할 수 있는 추가 가드레일입니다. 이는 심층적인 추가 제어 및 방어를 제공하기 위한 것이지만 전반적인 복잡성과 균형을 이루어야 합니다.
- 공동 책임 모델에서 사용자 또는 고객의 책임에 속하는 디바이스 또는 서비스로 인해 발생할 수 있는 상호작용 로깅. 이 섹션에는 로그를 통해 액세스할 수 있는 정보를 제한하기 위한 예방 조치가 포함되어 있습니다.

기본 모범 사례

다른 AWS API 요청에 대한 효과적인 제어인 일반 모범 사례는 미리 서명된 요청에도 적용됩니다. 이 섹션에서는 가장 관련성이 높은 두 가지 관행인 최소 권한과 데이터 경계를 검토합니다. 이러한 관행은 다른 관행이 확장하는 심층적인 제어를 생성합니다.

최소 권한 원칙을 적용

미리 서명된 요청의 사용을 제한하는 첫 번째 단계는 일반적으로 Amazon S3에 대한 액세스를 제한하는 것입니다. 미리 서명된 URL은 미리 서명된 URL에 대한 서명을 생성한 보안 주체에게 부여되지 않은 리소스에 대한 액세스를 제공할 수 없습니다. 또한 해당 보안 주체에게 부여되지 않은 방식으로 리소스에 대한 액세스를 제공할 수 없습니다. 따라서 모범 사례를 적용하여 보안 주체에게 최소 권한을 부여하는 것이 효과적인 가드레일입니다.

미리 서명된 URL을 생성하는 프로세스는 서명 생성을 위해 게시된 표준(서명 버전 4)을 기반으로 하는 알고리즘 작업입니다. 따라서 미리 서명된 URLs 생성에는 제한을 둘 수 없습니다. 그러나 관련성이 있으려면 미리 서명된 URL이 유효하고 리소스에 대한 액세스를 제공해야 하므로 미리 서명된 URL의 유효성도 효과적인 가드레일입니다.

최소 권한에 대한 자세한 내용은 AWS Well-Architected Framework의 최소 권한 액세스 권한 부여, 보안 원칙을 참조하세요.

데이터 경계 구현

최소 권한의 확장은 조직의 요구 사항을 일관되게 충족하는 데이터 경계를 유지하는 것입니다. 미리 서명된 URLs은 데이터 경계와 호환됩니다. 다른 요청과 마찬가지로 미리 서명된 URL 요청의 유효성은 요청 시 평가됩니다. 네트워크, 리소스, 역할 세션 및 보안 주체의 속성이 변경되면 요청이 수신되는 방법을 사용하여 해당 속성을 평가합니다.

예를 들어 Amazon Elastic Kubernetes Service(Amazon EKS) 컨테이너에서 실행 중인 서비스가 요청에 서명한다고 가정해 보겠습니다. 요청은 나중에 인터넷에 연결된 사용자의 개인 컴퓨터 시스템에서 전송됩니다. 이 경우 aws:SourceIp 조건은 Amazon EKS 컨테이너에 있는 서비스의 IP 주소가 아닌 사용자의 개인 시스템에서 표시되는 요청의 퍼블릭 IP 주소를 평가합니다.

마찬가지로 요청이 전송되기 전에 보안 주체 또는 리소스의 태그가 변경되면 원본이 아닌 업데이트된 이 aws:PrincipalTag/tag-key 및 aws:ResourceTag/tag-key 조건을 통해 요청에 적용됩니다.

추가 가드레일

솔루션 빌더와 사용자가 미리 서명된 요청을 적절하게 사용하면 사용자에게 데이터에 대한 액세스 권한을 부여하는 안전한 메커니즘을 제공합니다. 또한 미리 서명된 요청을 생성하는 기능은 보안 주체에게 아직 없는 액세스 권한을 제공하지 않습니다.

이러한 맥락에서 추가 제어가 필요합니까? 추가 제어의 근거는 액세스를 거부해야 하는 필요성이 아니라 모니터링, 사용 승인 및 경계 설정, 사용자 오류로 인한 위험 감소 기능을 제공하기 위한 것입니다. 이렇게 하면 사용이 적절하고 필요한지 확인할 수 있습니다.

다음 가드레일은이 목표에 도움이 됩니다. 이러한 제어를 활성화하기 전에 미리 서명된 요청을 식별하여 기존 사용량을 확인할 수 있습니다. 이 식별은 가드레일이 기존 사용량에 미치는 영향을 준비하거나 필요한 경우 예외를 계획하는 데 도움이 됩니다.

s3:signatureAge용 가드레일

미리 서명된 요청의 한 가지 정의 특성은 만료 시간을 설명하는 것입니다. 요청에 대한 서명에는 날짜가 포함됩니다. 이 날짜는 미리 서명된 URLs의 `X-Amz-Date` 쿼리 문자열 파라미터와 미리 서명된 POST의 날짜 또는 x-amz-date 헤더로 전송됩니다.

Amazon S3는 서명된 날짜와 요청의 유효 만료 사이의 최대 시간을 제한하는 데 사용할 수 있는 조건 키 s3:signatureAge를 제공합니다. 이 조건은 유효 기간을 늘릴 수는 없지만 줄일 수는 있습니다.

다음 정책에서 s3:signatureAge 조건 키는 미리 서명된 요청을 15분의 유효성으로 제한합니다. 다음 예제에서는 모두 15분을 사용하여 표준 서명이 지원하는 것과 유사한 기간으로 유효성을 제한합니다.

정책의 두 번째 문은 서명 버전 2 액세스를 거부합니다. 이 버전의 서명 프로토콜은 더 이상 사용되지 않지만 일부 에서는 여전히 지원됩니다 AWS 리전. 완전히 사용 중지되기 전에 명시적으로 차단하는 것이 좋습니다.

다음 정책을 AWS Organizations 서비스 제어 정책(SCP)으로 적용할 수 있습니다. 사용자는 서명 생성과 사용 사이의 시간이 15분 미만인 한 미리 서명된 요청을 사용하고 이러한 요청에 의존하는 솔루션을 배포할 수 있습니다. 구현에 따라이 제한은 영향을 미치지 않거나, 솔루션을 사용할 수 없게 되거나, 가끔 재시도할 수 있는 장애가 발생할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        }
      }
    },
    {
      "Sid": "DenySignatureVersion2",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
           "s3:signatureversion": "AWS"
        }
      }
    }
  ]
}
```

예외

솔루션이 만료되기 전에 더 오랜 시간이 필요하여 이전 정책의 영향을 받는 경우 예외를 승인하는 방법을 제공하는 것이 좋습니다. SCP에서 예외를 열거하지 않으려면 다음 정책과 같이 aws:PrincipalTag를 사용하여 확장 가능한 방식으로 예외를 관리합니다. AWS 데이터 경계 정책 AWS 예제와 같은 다른 예제에서는이 전략을 사용합니다. https://github.com/aws-samples/data-perimeter-policy-examples/blob/main/README.md

를 사용하여 예외 정책을 구현하는 경우 `aws:PrincipalTag`보안 주체에 대한 태그 설정에 대한 액세스를 제어해야 합니다. 이 유형의 태그는 보안 주체에서 직접 가져올 수 있으며 설정할 수 있는 태그 값을 제어하는이 예제와 같이 SCP로 제어할 수 있습니다. 이 유형의 태그는 ID 제공업체(IdP)에서 설정하거나 사용할 때 설정하는 세션 태그에서 가져올 수도 있습니다 AWS STS. 에 대한 액세스를 제어하는 `aws:PrincipalTag` 것은 복잡한 주제입니다. 그러나 ABAC(속성 기반 액세스 제어)를 사용한 경험이 있는 조직은이 사용 사례에 `aws:PrincipalTag` 적합한 사용을 지원하는 경험과 제어를 갖게 됩니다.

다음 예제에서 `aws:PrincipalTag` 조건은 명명된 태그(`long-presigned-allowed`)가 할당되고로 설정된 모든 보안 주체를 허용하는 예외를 생성합니다`true`. 단, 서명 기간에 대한 제한은 적용되지 않습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    }
  ]
}
```

버킷 정책

다음 예제와 같이 정책을 사용하여 모든 버킷 또는 선택한 버킷에 버킷 정책을 적용할 수 있습니다. SCP와 달리 버킷 정책은 서비스 보안 주체 사용량도 대상으로 합니다. 부록 A는 미리 서명된 요청의 예상 서비스 보안 주체 사용을 문서화하지 않지만, 해당 제한을 증명하기 위해 제어를 구현하려는 경우 다음 정책이 해당 제어를 제공합니다. 또한 SCP와 달리 버킷 정책은 관리 계정의 보안 주체에게 적용될 수 있습니다.

ABAC 기반 예외는 SCP와 동일한 방식으로 버킷 정책에서 작동합니다. 버킷 정책의 목표는 조직 외부의 보안 주체에 적용하는 것일 수 있으므로 ABAC 예외는 ABAC 제어가 적용되는 보안 주체로 제한되어야 합니다.

다음 예제에서 첫 번째 문의 `aws:PrincipalTag` 조건은 명명된 태그(`long-presigned-allowed`)가 할당되고가 로 설정된 보안 주체에 대한 예외를 생성합니다`true`. 단, 서명 기간에 대한 제한은 적용되지 않습니다. 두 번째 문은 버킷을 소유한 조직 외부의 AWS 모든 보안 주체에게이 제한을 적용합니다. 이 두 번째 문의 범위는 보안 주체에 대해 명명된 태그를 설정하려면 ABAC 제어와 일치해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    },
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
```

```
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

리소스 제어 정책

리소스 제어 정책(RCPs. SCPs 및 버킷 정책과 달리 RCPs 서비스 보안 주체 사용을 대상으로 지정하지 않습니다. RCPs 모든 계정의 비서비스 보안 주체에 영향을 미치지만 관리 계정의 리소스에는 영향을 주지 않습니다. 자세한 내용은 AWS Organizations 설명서를 참조하세요.

버킷 정책과 마찬가지로 `aws:PrincipalTags`를 사용하여 보안 주체에 대한 예외를 생성하는 경우 보안 주체의 태그 지정에 대한 ABAC 제어 범위를 염두에 두세요.

다음 RCP는 서명 수명을 15분으로 제한하여 조직의 모든 S3 버킷에서 미리 서명된 URL 사용을 제한합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true",
        }
      }
    },
```

```
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

s3:authType용 가드레일

미리 서명된 URLs 쿼리 문자열 인증을 사용하고 미리 서명된 POSTs 항상 POST 인증을 사용합니다. Amazon S3는 s3:authType 조건 키를 통해 인증 유형에 따른 요청 거부를 지원합니다. `REST-QUERY-STRING`는 쿼리 문자열의 `s3:authType` 값이고 `POST`는 POST의 `s3:authType` 값입니다.

다음 정책을 SCP로 적용할 수 있습니다. 이 정책은 `s3:authType`를 사용하여 헤더 기반 인증만 허용합니다. 또한 개별 사용자 또는 역할에 예외를 제공하도록 메서드를 구성합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
```

```
}
```

인증 유형을 기반으로 요청을 거부하면 거부된 인증 유형을 사용하는 모든 솔루션 또는 기능에 영향을 미칩니다. 예를 들어 거부하면 사용자가 Amazon S3 콘솔에서 업로드 또는 다운로드를 수행할 수 REST-QUERY-STRING 없습니다. 사용자가 Amazon S3 콘솔을 사용하도록 하려면이 가드레일을 사용하지 않거나 사용자에 대해 예외를 적용합니다. 반면 사용자가 Amazon S3 콘솔을 사용하지 않도록 하려면 REST-QUERY-STRING 사용자를 거부할 수 있습니다.

Amazon S3 리소스에 대한 사용자의 직접 액세스를 이미 거부했을 수 있습니다. 이 경우 인증 유형에 대한 가드레일은 중복됩니다. 그러나 s3:authType 직접 액세스를 거부하는 구현은 일반적으로 많은 제어 문에 걸쳐 있으며 일부는 예외이므로 거부 문은 defense-in-depth 유틸리티를 제공합니다.

워크로드에 사용되는 역할은 일반적으로 쿼리 문자열 또는 POST 인증에 액세스할 필요가 없습니다. 사전 서명된 요청을 사용하도록 설계된 서비스를 지원하는 역할은 예외입니다. 이러한 역할에 대한 특정 예외를 생성할 수 있습니다.

다음과 같은 정책을 사용하여 모든 버킷 또는 선택한 버킷에 버킷 정책을 적용할 수도 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

이 버킷 정책은 리전 간 복사를 위해 CopyObject 및 UploadPartCopy APIs 사용을 거부하는 효과가 있습니다. Amazon S3 복제는 이러한 APIs에 의존하지 않으므로 영향을 받지 않습니다.

이전 정책과 같은 버킷 정책을 사용하고 교차 리전 CopyObject 또는 UploadPartCopy API를 계속 지원하려면 다음과 aws:ViaAWSService 유사한에 대한 조건을 추가합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        },
        "Bool": {
          "aws:ViaAWSService": "false"
        },
      }
    }
  ]
}
```

미리 서명된 가드레일 및 예외를 다른 가드레일에 결합

일반적으로 사용자 및 역할에 가드레일을 적용할 계획이 없는 경우 다른 일반 가드레일의 예외에 가드레일을 적용할 수 있으므로 이러한 예외는 미리 서명된 요청을 지원하지 않습니다.

네트워크 제한이 있지만 외부 파트너 또는 특수 사용 사례에 대한 예외를 허용하는 경우, 특별히 필요한 것으로 식별되지 않는 한 이러한 예외가 적용될 때 쿼리 문자열 또는 POST 인증을 차단해야 합니다.

s3:signatureAge에 대한 제한 사항

관리자는의 영향을 s3:signatureAge 더 완전히 이해하는 것이 유용할 것입니다. 서명된 모든 요청에는 현재 시간을 나타내는가 X-Amz-Date포함됩니다. 이 값은 클라이언트에 의해 채워지고 요청 signer. AWS reject는 잘못된 시간이 있는 것으로 간주되는 요청을 거부합니다. 그러나 서명자는 나중에 서명을 미리 생성할 수 있습니다. Amazon S3는 너무 일찍 전송되는 경우 미래 시간을 지정하는 요청을 거부합니다. 그러나 서명에 로그인할 때까지 요청이 전송되지 않는 경우 서명을 더 일찍 생성하고 나중에 전송할 수 있습니다.

s3:signatureAge는 미리 서명된 요청에 대해서만 서명X-Amz-Date의 최대 기간을 제한 합니다. X-Amz-Expires 또는 POST 정책에서 만료가 유효하다고 선언했더라도 지정된 기간보다 오래된 요청

은 거부됩니다. s3:signatureAge는 명시적 만료가 포함되지 않은 요청의 유효 기간을 변경하지 않습니다. 또한 클라이언트X-Amz-Date가 서명에 사용하는 값을 제어하지 않습니다.

시스템 클럭이 잘못되었거나 클라이언트가 의도적으로 미래 날짜를 요청하는 경우 서명된 시간은 서명이 생성된 시간이 아닐 수 있습니다. 이렇게 하면가 솔루션을 제어할 s3:signatureAge 수 있는 양이 제한됩니다. 서명을 생성할 때 현재 시간을 사용하는 솔루션은 예상대로 제한됩니다. 서명은에 지정된 밀리초 수만큼 유효합니다s3:signatureAge. 현재 시간을 사용하지 않는 솔루션에는 다른 제한이 있습니다. 한 가지 제한 사항은 서명 서명에 사용된 자격 증명이 여전히 유효해야 한다는 것입니다. 관리자는 발급된 임시 자격 증명의 최대 유효성을 제어할 수 있습니다. 자격 증명이 최대 36시간 동안 유효하도록 허용하거나 유효성을 최소 15분으로 제한 할 수 있습니다. 임시 자격 증명의 만료는 값에 따라 달라지지 않습니다X-Amz-Date.

영구 자격 증명에는 이러한 제한이 없습니다. 임시 자격 증명만 사용하는 것이 모범 사례이며 영구 자격 증명을 명시적으로 취소할 수 있습니다. 그러면 해당 자격 증명을 기반으로 하는 서명도 무효화됩니다.

s3:signatureAge는 밀리초 단위로 측정되지만, 클럭이 잘 동기화되고 지연 시간이 짧은 경우에도 60초 미만으로 설정하는 것은 실용적이지 않습니다. 60초 미만의 설정은 유효한 요청을 거부할 위험이 있습니다. 서명 생성과 요청 제출 사이에 지연이 예상되거나 클럭 동기화 문제가 발생하는 경우 관리에서 이를 고려해야 합니다s3:signatureAge.

대규모 버킷 대상 지정

SCPs 및 RCPs aws:PrincipalTag를 사용하여 사용자에 대한 예외를 만들 수 있습니다. 버킷의 태그를 사용하여를 통해 액세스를 제어할 수 없습니다. 액세스 제어에는 객체 태그aws:ResourceTag만 사용됩니다.https://docs.aws.amazon.com/AmazonS3/latest/userguide/tagging-and-policies.html 이 제어를 적용하려는 모든 객체에 태그를 추가하는 것은 일반적으로 확장 가능하지 않습니다.

많은 사용 사례에 적합한 솔루션은 SCP 또는 RCP가 적용되는 계정을 변경하거나 aws:ResourceAccount, aws:ResourceOrgPaths 또는 aws:ResourceOrgID를 사용하여 계정 수준에서 정책 및 예외를 적용하는 것입니다. 예를 들어 SCP 또는 RCP를 프로덕션 계정 집합에 적용할 수 있습니다.

또 다른 해결 방법은 사용자 지정 AWS Config 규칙을 사용하여 탐지 제어 또는 대응 제어를 구현하는 것입니다. 목표는 모든 버킷에 적절한 가드레일이 있는 버킷 정책을 포함하는 것입니다. 버킷 정책의 내용을 테스트하는 것 외에도 사용자 지정 AWS Config 규칙은 버킷에서 태그를 검색하고 버킷에 특정 값으로 태그가 지정된 경우 규칙에서 버킷을 제외할 수 있습니다. 해당 규칙이 규정 준수 검사에 실패하면 버킷을 규정 미준수로 표시하거나 수정을 호출하여 버킷 정책에 가드레일을 추가할 수 있습니다.

> **Note**
>
> 요청의 태그 콘텐츠를 PutBucketTagging으로 제한할 수 없습니다. 버킷에 태그를 지정하는 방법을 제어하려면 `PutBucketTagging` 및 DeleteBucketTagging에 대한 액세스를 제한해야 합니다.

상호작용 및 완화 조치 로깅

미리 서명된 URL에는 서명이 포함되며 만료 전 기간 동안 서명되었던 특정 API 작업을 수행하는 데 사용할 수 있습니다. 임시 액세스 자격 증명으로 취급해야 합니다. 서명은 이를 알아야 하는 당사자만 비공개로 유지해야 합니다. 대부분의 환경에서 이는 요청을 보내는 클라이언트와 요청을 수신하는 서버입니다. HTTPS 세션의 참가자만 서명을 전송하는 URI를 볼 수 있으므로 직접 HTTPS 세션의 일부로 서명을 전송하면 프라이빗 특성이 유지됩니다.

미리 서명된 URLs의 경우 서명은 `X-Amz-Signature` 쿼리 문자열 파라미터로 전송됩니다. 쿼리 문자열 파라미터는 URI의 구성 요소입니다. 클라이언트가 URI와 서명을 기록할 수 있다는 위험이 있습니다. 클라이언트는 전체 HTTP 요청에 액세스할 수 있으며 요청, 데이터 및 헤더(인증 헤더 포함)의 일부를 로깅할 수 있습니다. 그러나 이는 규칙상 덜 일반적입니다. URI 로깅은 보다 일반적이며 액세스 로깅과 같은 경우에 필요합니다. 클라이언트는 URIs.

일부 환경에서 사용자는 중간자(프록시)가 HTTPS 세션에 대한 가시성을 확보하도록 허용합니다. 프록시를 활성화하려면 구성 및 신뢰할 수 있는 인증서가 필요하므로 클라이언트 시스템에 대한 높은 수준의 권한 있는 액세스가 필요합니다. 클라이언트 중개 환경의 로컬 컨텍스트 내에서 프록시 구성 및 신뢰할 수 있는 인증서를 설치하면 매우 높은 수준의 권한이 허용됩니다. 이러한 이유로 이러한 중개자에 대한 액세스를 엄격하게 제어해야 합니다.

중개자의 목적은 일반적으로 원치 않는 송신을 차단하고 다른 송신을 추적하는 것입니다. 따라서 이러한 중개자는 요청을 로깅하는 것이 일반적입니다. 클라이언트와 마찬가지로 중개자는 콘텐츠, 헤더 및 데이터(모두 매우 민감함)를 로깅할 수 있지만 `X-Amz-Signature` 쿼리 문자열 파라미터를 포함하는 것과 같은 URIs를 로깅하는 것이 더 일반적입니다.

완화

URI 로깅은 중개 서버에 대한 직접 액세스와 마찬가지로 `X-Amz-Signature` 쿼리 문자열 파라미터를 수정하거나, 전체 쿼리 문자열을 수정하거나, 정보를 극비로 취급하는 것이 좋습니다. 이러한 보호는 적극 권장되지만 미리 서명된 URLs이 만료되면 서명이 만료될 때까지 노출이 충분히 오래 지연되는 한 로그 노출 위험이 완화됩니다.

Amazon S3는 서명도 보고 적절하게 처리해야 합니다. Amazon S3 서버 액세스 로그에는 요청 URI가 포함되지만 권장 사항에 `X-Amz-Signature`따라를 수정합니다. Amazon S3에 대해 CloudTrail 데이터 이벤트를 로깅할 때도 마찬가지입니다. 사용자 지정 데이터 식별자를 사용하여 데이터를 마스킹하도록 Amazon CloudWatch Logs를 구성할 수 있습니다. https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL-custom-data-identifiers.html

다음 정규식은 URI에 나타나는 `X-Amz-Signature`와 일치합니다.

```
X-Amz-Signature=[a-f0-9]{64}
```

다음 정규식은 보다 구체적으로 대체할 텍스트를 식별하는 그룹화 패턴을 추가합니다.

```
(?:X-Amz-Signature=)([a-f0-9]{64})
```

다음과 같은 액세스 로그 항목이 있는 경우:

```
X-Amz-Signature=733255ef022bec3f2a8701cd61d4b371f3f28c9f193a1f02279211d48d5193d7
```

첫 번째 정규식은 액세스 로그 항목을 다음과 같이 변환합니다.

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

캡처되지 않은 그룹을 지원하는 시스템에서 두 번째 정규식은 액세스 로그 항목을 다음과 같이 변환합니다.

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

FAQ

미리 서명된 요청을 여러 번 사용할 수 있습니까? 이것이 보안 위험인가요?

예, 미리 서명된 요청의 서명을 두 번 이상 사용할 수 있습니다. 이것이 보안 위험인지 여부는 상황에 맞는 질문입니다. AWS 서비스에 액세스하는 다른 방법도 반복을 허용합니다. AWS 자격 증명이 있는 사용자 또는 워크로드는에 많은 요청을 보낼 수 AWS 서비스있으며 이러한 요청은 중복될 수 있습니다.

사용 사례에서 한 번만 실행해야 하는 경우 단일 사용을 적용하는 다른 메커니즘을 구현해야 합니다. 일회용은 미리 서명된 요청의 기능이 아닙니다. 보안 엔지니어는 사용 사례 및 구현을 검토해야 하지만, 대부분의 경우 여러 번 사용하는 것이 허용 가능한 사용에 적합합니다.

의도한 사용자 이외의 사람이 미리 서명된 요청을 사용할 수 있습니까?

미리 서명된 요청의 서명은 해당 요청을 소유한 모든 사용자가 보낼 수 있습니다. 데이터 경계 제어와 같은 다른 형태의 검증을 통과한 경우에만 허용됩니다. 서명이 만료되었거나 서명 자격 증명이 만료되었거나 서명 자격 증명이 요청된 리소스에 액세스할 수 없는 경우 요청이 거부됩니다.

다른 인증 방법도 마찬가지입니다 AWS 서비스. 부적절하게 공유된 자격 증명은 부적절한 액세스를 허용합니다. 핵심 모범 사례는 자격 증명과 서명을 의도한 대상과만 공유하는 것입니다. 의도한 대상이 프라이빗 데이터를 안전하게 유지하고 다른 사람과 공유하지 않도록 신뢰할 수 없는 경우 어떤 형태의 인증도 약화됩니다.

권한이 있는 사용자가 미리 서명된 요청을 사용하여 데이터를 유출할 수 있습니까?

데이터를 보호하려면 강력한 조치가 필요합니다. 데이터 경계를 유지하면서 의도한 목적으로 액세스를 활성화하려면 포괄적인 접근 방식이 필요합니다. 최소 권한 액세스, 데이터 경계 제어 및 임시 액세스 자격 증명만 사용하는 것이 데이터 보안에 적용되는 일반적인 모범 사례입니다. 이러한 제어를 적절하게 사용하면 사용자가 생성하는 미리 서명된 요청을 통해 작업을 수행할 수 있는 기능도 제한됩니다.

이는 미리 서명된 요청에서 제공하는 액세스가 요청에 서명하는 데 사용되는 자격 증명에 부여된 액세스의 하위 집합이기 때문입니다. 이 맥락에서 데이터 액세스에 적용되는 모범 사례는 일반적으로 미리 서명된 요청에 적용되지만 미리 서명된 요청은 데이터에 대한 새 액세스를 생성하지 않습니다.

- 최대 만료는 서명 자격 증명의 만료로 제한됩니다. 서명 자격 증명이 취소 되면 자격 증명을 기반으로 한 서명은 더 이상 유효하지 않습니다.
- 서명 자격 증명과 연결된 IAM 보안 주체에 대한 권한에 미리 서명된 요청과 연결된 작업의 실행이 포함되지 않은 경우 미리 서명된 요청을 호출하면 "액세스 거부" 응답이 발생합니다. 응답은 호출 시점의 현재 권한 상태에 따라 달라지며, 이는 미리 서명된 요청의 서명이 생성된 시간과 관련이 없습니다.
- 보안 주체의 속성은 서명 자격 증명과 연결된 보안 주체를 기반으로 평가됩니다.
- 역할 세션의 속성은 서명 자격 증명과 연결된 역할 세션을 기반으로 평가됩니다.
- 네트워크의 속성은 일반 요청과 마찬가지로 요청이 수신된 방식에 따라 평가됩니다.

이 컨텍스트에서 미리 서명된 요청과 관련된 위험 검사는 사용자의 자격 증명과 다른 자격 증명으로 서명되고 사용자 보안 주체의 일부가 아닌 액세스를 제공하는 영역으로 제한됩니다. 이 검사는 미리 서명된 요청 기능 자체 대신 사용자를 대신하여 서명을 생성하는 서비스, 워크로드 또는 솔루션의 설계에 적용해야 합니다.

권한이 없는 방식으로 공유되었다고 의심되는 경우 미리 서명된 URL의 액세스를 거부할 수 있습니까?

예. 이렇게 하려면 URL이 서명된 자격 증명을 무효화해야 합니다. 이를 수행하는 방법에는 여러 가지가 있습니다.

- 자격 증명이 속한 IAM 보안 주체에서 권한을 제거합니다. 해당 IAM 보안 주체가 더 이상 URL이 서명된 리소스 및 작업에 액세스할 수 없는 경우 URL은 해당 작업을 실행할 수 없습니다. 이는 해당 IAM 보안 주체의 모든 일치하는 사용에 영향을 미칩니다.
- URL에 서명하는 데 사용되는 자격 증명이 임시 AWS STS 자격 증명인 경우 IAM 보안 주체의 특정 시간 이전에 발급된 임시 자격 증명에 대한 세션 권한을 취소할 수 있습니다. 사용 사례에 따라 정상 만료 시간 전에 무효화되는 다른 유효한 세션이 있을 수 있지만 새 세션은 영향을 받지 않습니다. 세션 권한을 취소하면 해당 세션과 연결된 자격 증명을 사용하여 서명된 URLs도 무효화되지만 새 세션과 연결된 새 URLs은 영향을 받지 않습니다.
- URL에 서명하는 데 사용되는 자격 증명이 영구 자격 증명인 경우 액세스 키를 비활성화합니다. 이는 해당 자격 증명에 연결된 모든 사용에 영향을 미칩니다.

리소스

Amazon S3 설명서

- 인증 요청 (AWS 서명 버전 4)
- 요청 인증: 쿼리 매개변수 사용 (AWS 서명 버전 4)
- 요청 인증: POST를 사용한 브라우저 기반 업로드 (서명 버전 4)AWS
- Amazon S3 서명 버전 4 인증 관련 정책 키
- 미리 서명된 URL 사용

기타 참조

- AWS 기반 데이터 경계 구축 (AWS 백서)
- SEC03-BP02 최소 권한 액세스 권한 부여 (AWS 잘 설계된 프레임워크, 보안 기둥)
- SEC03-BP05 조직의 권한 가드레일을 정의하십시오 (AWS 잘 설계된 프레임워크, 보안 기둥).

부록 A: 미리 서명된 URLs AWS 서비스 사용 방법

이 부록에서는 미리 서명된 URL을 사용하는 AWS 서비스 및 기능에 대한 정보를 제공합니다. URLs 이 정보는 다음 두 가지 목적으로 사용됩니다.

- 제어를 구현하는 보안 엔지니어에게 해당 제어의 가능한 영향에 대한 정보를 제공합니다.
- 이 위험이 URL 로깅 상호 작용과 관련이 있을 수 있는 상황에 대한 인식을 높입니다.

> **Important**
>
> 이 부록에서는 AWS 서비스 또는 미리 서명된 URLs 사용에 대한 전체 목록을 제공하지 않습니다. 또한 사용자 지정 또는 타사 솔루션도 다루지 않습니다.

Amazon S3 콘솔

보안 주체: 콘솔 사용자

기본 만료: 5분

> **면책 조항**
>
> 이 섹션에서는 Amazon S3 콘솔의 현재 동작을 설명합니다. AWS 콘솔 동작은 예고 없이 변경될 수 있습니다.

Amazon S3 콘솔은 객체 다운로드 및 업로드를 지원합니다. 다운로드는 만료 시간이 300초(5분)인 미리 서명된 URL을 사용합니다. URL은에 대한 요청에 의해 생성됩니다`https://<bucket-region>.console.aws.amazon.com/s3/batchOpsServlet-proxy`.

이 요청은 사용자가 다운로드 버튼을 클릭할 때 시작되므로 다운로드에 대한 명시적 요청이 발생할 때까지 URL이 미리 생성되거나 클라이언트로 전송되지 않습니다.

업로드는 콘솔이 2개의 요청을 전송한다는 점을 제외하면 비슷합니다. 하나는 사전 CORS 검사`OPTIONS`이고 다른 하나는 입니다`PUT`. 두 요청 모두 동일한 서명을 사용합니다.

서명에 사용되는 자격 증명은 현재 로그인한 사용자와 연결된 임시 자격 증명입니다. 이러한 임시 자격 증명을 얻는 방법에 대한 세부 정보는이 가이드의 범위를 벗어납니다.

Amazon S3 Object Lambda

보안 주체: 액세스 포인트 호출자

기본 만료: 61초

> **Note**
>
> 2025년 11월 7일부터 S3 객체 Lambda는 현재 서비스를 사용하고 있는 기존 고객과 선택 AWS Partner Network (APN) 파트너만 사용할 수 있습니다. S3 객체 Lambda와 유사한 기능의 경우 Amazon S3 객체 Lambda 가용성 변경에서 자세히 알아보세요.

Amazon S3 객체 Lambda는 AWS Lambda 함수를 사용하여 Amazon S3에서 검색되는 데이터를 자동으로 처리하고 변환합니다. S3 객체 Lambda가 함수를 호출하면 함수에는 지원 액세스 포인트에서 원본 객체를 다운로드하는 데 사용할 수 있는 미리 서명된 URL(`inputS3Url`)이 제공됩니다.

이러한 미리 서명된 URLs은 S3 객체 Lambda를 구성할 때 제공되는 지원 Amazon S3 액세스 포인트에 대해 서명됩니다. S3 (이는 객체 Lambda 액세스 포인트와 동일하지 않습니다.) Lambda 함수에 바인딩된 역할을 사용하는 대신 원래 호출자의 자격 증명을 사용하여 URL에 서명되며 URL을 사용할 때 해당 사용자의 권한이 적용됩니다. URL에 서명된 헤더가 있는 경우 Lambda 함수는 Amazon S3에 대한 호출에 이러한 헤더를 포함해야 합니다.

반환되는 미리 서명된 URL의 만료 시간은 61초입니다(S3 객체 Lambda 함수의 최대 기간보다 1초 더 김). 생성된 URL은 지원 액세스 포인트에서만 사용할 수 있습니다. S3 객체 Lambda 액세스 포인트의 호출자는이 액세스 포인트에 액세스할 수 있어야 합니다. 조건을 사용하여 S3 객체 Lambda의 컨텍스트에 대한 액세스를 제한할 수 있습니다`"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]`. 해당 조건이 지원 액세스 포인트 또는 버킷에 연결되면 사용자는 지원 액세스 포인트 또는 버킷에 직접 액세스할 수 없습니다.

이 접근 방식의 가치는 Lambda 함수에 S3 버킷 또는 액세스 포인트에 대한 액세스 권한을 부여할 필요가 없다는 것입니다. Lambda 함수와 연결된 역할에는 WriteGetObjectResponse에 대한 권한이 필요하지만 GetObject에 대한 권한은 필요하지 않습니다.

S3 객체 Lambda는 미리 서명된 URLs 생성할 때 네트워크 제한을 추가하지 않으므로 Lambda 함수 외부에서 URL을 사용할 수 있습니다. 그러나 S3 객체 Lambda의 호출자에게 적용되는 모든 제한은 여전히 적용됩니다. 예를 들어 Lambda 함수가 VPC에서 실행되고 호출자가 VPC 엔드포인트를 사용하도록 제한하는 경우 미리 서명된 URL을 소유한 사람은 누구나 해당 VPC 엔드포인트를 통해 전송할 수 있어야 합니다.이 제한은 SourceIp 및 VpcSourceIp에도 적용됩니다.

> **Note**
>
> VPC에서 S3 객체 Lambda 함수를 사용하려면 VPC에 WriteGetObjectResponse를 호출하는 퍼블릭 S3 엔드포인트에 대한 경로가 있어야 합니다. 이는 VPC 엔드포인트를 사용하기 위한 요구 사항이 버킷에서 데이터를 검색하기 위한 요청에 적용되지 않음을 의미하지 않습니다.

AWS Lambda 리전 간 CopyObject

보안 주체: AWS 내부

기본 만료: 3600초

CopyObject 또는 UploadPartCopy API를 사용하여 복사하는 경우 AWS 리전 Amazon S3는 내부적으로 미리 서명된 URLs 사용합니다. 이러한 APIs SDKs 또는 `aws s3api copy-object` 및 AWS CLI 명령에서 직접 호출할 수 있습니다`aws s3api upload-part`. 이러한 APIs는 Amazon S3 복제에 사용되지 않지만 소스 및 대상이 S3 버킷인 경우 및 `aws s3 sync` 명령에서 사용됩니다 AWS CLI `aws s3 cp`. 또한 variousSDK의 `TransferManager` 구현에서도 지원됩니다. AWS SDKs

AWS Lambda GetFunction

보안 주체: AWS 내부

기본 만료: 10분

AWS Lambda 는 Lambda 팀이 소유한 S3 버킷에 사용자 버전을 저장합니다. Lambda 컨테이너에 배포된 자산을 생성하기 전에 GetFunction API를 호출합니다.이 API는 로 응답합니다. `Code.Location` - 10분 동안 유효한 미리 서명된 URL을 포함합니다(이 만료 시간은 게시된 계약이 아닌 현재 동작임). 코드를 원하지 않는 경우 GetFunctionConfiguration의 조합을 사용할 수 있습니다. GetFunctionConcurrency, 및 ListTags를 사용하여에서 반환되는 다른 데이터를 검색합니다`GetFunction`.

반환된 URL은 현재 로그인한 사용자의 자격 증명으로 서명되지 않고 Lambda에서 사용자를 대신하여 서명됩니다. 따라서 현재 로그인한 사용자 또는 사용자의 임시 세션 자격 증명에 적용되는 조건 키(예: `aws:SourceIP`)는 생성된 URL에 적용되지 않습니다. 조건 키가 GetFunction에만 적용되거나 사용자 또는 세션의 모든 AWS API 사용량에 적용되는 경우에도 마찬가지입니다.

또한 Lambda 콘솔은 GetFunction과 반환되는 미리 서명된 URL을 사용합니다. 콘솔은 현재 로그인한 사용자와 연결된 임시 자격 증명을 사용하여 GetFunction을 호출합니다. 이러한 임시 자격 증명을 얻는 방법에 대한 세부 정보는이 문서의 범위를 벗어납니다.

Amazon ECR

보안 주체: AWS 내부

기본 만료: 1시간

Amazon Elastic Container Registry(Amazon ECR)는 1시간 동안 유효한 미리 서명된 URL을 반환하고 Amazon ECR 이미지에서 단일 계층 다운로드를 지원하는 GetDownloadUrlForLayer API를 제공합니다. 그러나이 작업은 Amazon ECR 프록시에서 사용되며 일반적으로 사용자가 이미지를 가져오고 푸시하는 데 사용되지 않습니다.

Amazon Redshift Spectrum

보안 주체: 를 통해 CREATE EXTERNAL SCHEMA에 전달된 역할 `IAM_ROLE`

기본 만료: 1시간

Amazon Redshift Spectrum은 내부적으로 미리 서명된 URLs 사용하며 미리 서명된 URLs을 제한하는 버킷과 Amazon Redshift 역할의 조합에 대한 제한을 금지합니다. 16분의 `s3:signatureAge` 값을 사용할 수 있지만 매우 낮은 값은 신뢰할 수 없습니다. 사용할 수 있는 최소값은 쿼리의 타이밍과 크기에 따라 다릅니다. 16분 미만의 값은 많은 시나리오에서 작동하지만 테스트가 필요합니다. 역할은 Redshift Spectrum에서만 사용하도록 제한할 수 있으며 제한해야 합니다. 그러면 생성되는 URLs이 공개되지 않으므로 만료 값이 낮은 일반적인 정당화가 완화됩니다.

Amazon SageMaker AI Studio

Amazon SageMaker AI Studio는 CreatePresignedDomainUrl과 CreatePresignedNotebookInstanceUrl이라는 두 가지 API 작업을 지원합니다. 그러나 이러한 APIs는 서명 버전 4 미리 서명된 URL 기능과 관련이 없습니다. 이러한 APIs는 `authToken` 파라미터를 사용하는 URL을 생성하지만 표준 서명 버전 4 쿼리 파라미터는 지원하지 않습니다.

`authToken`는 다른 메커니즘이지만 미리 서명된 URLs. 쿼리 문자열 파라미터로 전송되며 5분의 만료 시간을 지원합니다.

SageMaker AI는 네트워크 제한을 지원합니다. `sagemaker:CreatePresignedDomainUrl` 작업에 제한을 두면 해당 작업은 CreatePresignedDomainUrl 호출과 생성된 URL 사용에 모두 적용됩니다. 유효한 네트워크에서 URL을 생성한 다음 유효하지 않은 네트워크에서 전송하는 경우 URL을 생성하기 위한 API 호출은 성공하지만 URL을 보내는 요청은 실패합니다. CreatePresignedNotebookInstanceUrl 및 `sagemaker:CreatePresignedNotebookInstanceUrl` 작업도 마찬가지입니다.

자세한 내용은 SageMaker AI 설명서를 참조하세요.

부록 B: 미리 서명된 URLs 미치는 영향 AWS 서비스

이 부록에서는 부록 A에 설명된 대로 미리 서명된 URLs AWS 서비스 사용하는와이 가이드의 앞부분에 설명된 제어 간의 상호 작용을 설명합니다.

s3:signatureAge용 가드레일

`s3:signatureAge` 조건 키로 설정된 최대 5분의 만료로 인해 Amazon S3 콘솔이 중단되지 않습니다. 다운로드 버튼을 선택하면 Amazon S3 콘솔이 미리 서명된 URLs을 생성하고 자체 5분의 만료 시간을 적용합니다. 최대 기간이 2분보다 짧으면 클럭 동기화 및 지연 시간에 따라 무작위 실패가 발생할 수 있습니다.

Amazon S3 객체 Lambda는 61초의 만료 시간을 사용하므로 61초 이상의 `s3:signatureAge` 값으로 조건을 설정해도 중단이 발생하지 않습니다. 기간이 짧을수록 신뢰성이 떨어질 수 있으며 간헐적인 장애가 발생할 수 있습니다.

Amazon S3 리전 간 CopyObject는 최대 5분의 만료로 인해 중단되지 않습니다. 그러나 기간이 짧을수록 클럭 동기화 및 지연 시간에 따라 무작위 실패가 발생할 수 있습니다.

에서 AWS LambdaGetFunction은 고객 계정 외부의 객체에 URL을 제공하므로 고객 정책은 생성된 URLs에 영향을 주지 않습니다.

Amazon Redshift Spectrum은 16분의 `s3:signatureAge` 조건으로 테스트되었습니다. 그러나 기간이 짧을수록 중단이 발생할 수 있습니다.

네트워크 제한을 사용하지 않는 경우 s3:authType에 대한 가드레일

Amazon S3 콘솔은 일반적으로 `s3:authType` 가드레일의 영향을 받습니다. 콘솔은 로컬 네트워크 구성에 따라 Amazon S3로 라우팅됩니다. 로컬 네트워크가 네트워크 제한이 허용하는 방식으로 Amazon S3로 라우팅 되는 경우에도 Amazon S3 콘솔은 계속 작동합니다. 그러나 허용되지 않는 방식으로 프록시 또는 퍼블릭 인터넷을 통해 라우팅되는 경우 사용이 차단됩니다. 그러나 사용 차단이이 정책의 의도일 수 있습니다.

Lambda 함수가 적절한 VPC에 연결되지 않은 경우 Amazon S3 객체 Lambda가 영향을 받습니다.이 구성에서 VPC에는 S3 버킷에 액세스하지 않고 WriteGetObjectResponse를 호출하기 위한 NAT 게이트웨이가 있어야 합니다.

이 가드레일이가 true일 때 권장되는 예외 없이 버킷 정책에 적용되는 경우 Amazon S3 리전 간 CopyObject가 중단`aws:viaAWSService`됩니다.

향상된 VPC 라우팅을 사용하지 않는 한 Amazon Redshift Spectrum은 `s3:authType` 가드레일의 영향을 받습니다. 현재 Redshift Spectrum은 프로비저닝된 클러스터가 아닌 서버리스 클러스터에서만 향상된 VPC 라우팅을 지원합니다.

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
업데이트 및 설명	추가 가드레일 섹션에서 RCPs.	2025년 8월 8일
최초 게시	—	2024년 7월 23일

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