ガードレールの確立と署名付き URLsのモニタリング

AWS 規範ガイダンス

AWS 規範ガイダンス: ガードレールの確立と署名付き URLsのモニタリング

Table of Contents

序章 1
対象者 1
目的 1
前提条件 2
署名URLs の概要 3
署名付きリクエストを使用する動機 4
一時的な AWS STS 認証情報との比較 5
署名のみのソリューションとの比較 5
署名付きリクエストの識別 6
署名付き URL を使用したリクエストの識別 6
他のタイプの署名付きリクエストの特定 7
リクエストパターンの識別 7
署名付きリクエストを使用するためのベストプラクティス 12
基本的なベストプラクティス 12
最小特権の原則を適用する 12
データ境界を実装する 13
追加のガードレール 13
s3:signatureAge のガードレール 13
リソースコントロールポリシー 17
s3:authType のガードレール 18
署名付きガードレールと例外を他のガードレールと組み合わせる 21
s3:signatureAge の制限事項 21
大規模なバケットのターゲット設定 22
インタラクションと緩和策のログ記録 22
緩和策 23
よくある質問 25
署名付きリクエストは複数回使用できますか? これはセキュリティリスクですか? 25
目的のユーザー以外のユーザーが署名付きリクエストを使用できますか? 25
承認されたユーザーは、署名付きリクエストを使用してデータを抽出できますか? 25
署名付き URL が不正な方法で共有されていると思われる場合、その URL からのアクセスを拒否できますか? 26
リソース 28
「Amazon S3 ドキュメント」 28
その他のリファレンス 7

付録 A: 署名付き URLs AWS のサービス の使用方法 29
Amazon S3 コンソール 29
Amazon S3 Object Lambda 30
AWS Lambda クロスリージョン CopyObject 31
AWS Lambda GetFunction 31
Amazon ECR 32
Amazon Redshift Spectrum 32
Amazon SageMaker AI Studio 33
付録 B: 署名付き URLs のコントロールが に与える影響 AWS のサービス 34
s3:signatureAge のガードレール 34
ネットワーク制限を使用しない場合の s3:authType のガードレール 34
ドキュメント履歴 36
..... xxxvii

ガードレールの確立と署名付き URLsのモニタリング

Ryan Baker、Amazon Web Services (AWS)

2025 年 8 月 (ドキュメント履歴)

セキュリティはすべての企業にとって重要な懸念事項であり、AWS Well-Architected フレームワークの重要な柱です。セキュリティエンジニアは、組織の統制要件に沿った管理ガードレールを実装する必要があります。 AWS Well-Architected フレームワークでは、ガードレールはアクティビティを制限する境界を定義します。

このガイドでは、Amazon Simple Storage Service (Amazon S3) オブジェクトで使用される署名付き URLs を使用するための背景情報とベストプラクティスについて説明します。署名付き URLsを使用すると、有効な認証情報にアクセスできるユーザーまたはアプリケーションは、事前に署名され、定義された有効期限まで受け入れられるリクエストを生成できます。署名付き URLs の一般的なユースケースは、これらのリクエストを共有してオブジェクトまたはリソースへのアクセスを拡張することです。共有署名付きリクエストは、特定のリクエストを実行する権限を持つシステムまたはユーザーによって生成され、他のシステムまたはユーザーに送信して、同じリクエストを実行する機能を拡張できます。

このガイドでは、以下について説明します。

- 署名付き URLsの概念
- 署名付き URLsのユースケース
- 推奨ガードレールとオプションのガードレール
- モニタリングオプション
- 署名付き URLs AWS のサービス の使用方法の例

対象者

本ガイドの対象読者は、 AWS クラウドにセキュリティコントロールを実装する作業を担当している、アーキテクトやセキュリティエンジニアです。

目的

セキュリティエンジニアとして、ソリューションビルダーがセキュリティをどのように実装しているか、およびエンドユーザーが持つアクセスのタイプを認識する必要があります。このガイドで

は、Amazon S3 でよく使用される署名付き URLs という 1 種類のアクセスについて説明します。Amazon S3 署名付き URLs は、認証メカニズムを効率的にブリッジするためのオプションをビルダーに提供します。

Amazon S3 では、署名付き URLs はリクエストの一意のカテゴリを表します。セキュリティエンジニアは、これらのリクエストをモニタリングおよび管理して、適切で必要な場合にのみ使用されるようにできます。このガイドの目的は、セキュリティエンジニアがこのタイプの高レベルの監視を提供するのを支援することです。

このガイドを読んだら、署名付き URL とは何か、通常はいつ使用されるか、その使用の動機を理解する必要があります。

前提条件

「AWS でセキュリティコントロールを実装する」ガイドで説明されているように、会社がセキュリティポリシー、コントロール目標、または標準を定義していない場合は、このガイドに進む前にこれらのガバナンスタスクを完了することをお勧めします。

開始する前に、コントロールとモニタリングに関する推奨およびオプションのベストプラクティスについても理解しておく必要があります。詳細については、以下を参照してください。

- サービスコントロールポリシー (AWS Organizations ドキュメント)
- リソースコントロールポリシー (AWS Organizations ドキュメント)
- Amazon S3 のバケットポリシー (Amazon S3 ドキュメント)
- サーバーアクセスログ記録を使用したリクエストのログ記録 (Amazon S3 ドキュメント)
- を使用した Amazon S3 API コールのログ記録 AWS CloudTrail (Amazon S3 ドキュメント)

署名URLs の概要

署名付き URL は、 AWS Identity and Access Management (IAM) サービスによって認識される HTTP リクエストの一種です。このタイプのリクエストを他の AWS すべてのリクエストと区別するのは、X-Amz-Expires クエリパラメータです。他の認証されたリクエストと同様に、署名付き URL リクエストには署名が含まれます。署名付き URL リクエストの場合、この署名は で送信されますX-Amz-Signature。署名は、署名バージョン 4 の暗号化オペレーションを使用して、他のすべてのリクエストパラメータをエンコードします。

> **注意事項**
>
> - 署名バージョン 2 は現在廃止中ですが、一部の では引き続きサポートされています AWS リージョン。このガイドは、署名バージョン 4 の署名に適用されます。
> - 受信サービスは署名なしヘッダーを処理できますが、そのオプションのサポートは、ベストプラクティスに従って制限され、ターゲットを絞ったものです。特に明記されていない限り、リクエストを受け入れるには、すべてのヘッダーに署名する必要があります。

X-Amz-Expires パラメータを使用すると、エンコードされた日時から大きく逸脱して署名を有効として処理できます。署名の有効性の その他の側面は引き続き評価されます。 署名認証情報は、一時的な場合は、署名の処理時に期限切れにすることはできません。署名認証情報は、処理時に十分な権限を持つ IAM プリンシパルにアタッチする必要があります。

署名付き URLsは、署名付きリクエストのサブセットです

署名付き URL は、将来のリクエストに署名する唯一の方法ではありません。Amazon S3 は、一般的に署名付きである POST リクエストもサポートしています。署名付き POST 署名は、署名付きポリシーに準拠し、そのポリシーに有効期限が埋め込まれているアップロードを許可します。

リクエストの署名は将来の日付になることがありますが、これはまれです。基盤となる認証情報が有効 である限り、署名アルゴリズムは将来の日付を禁止するものではありません。 ただし、これらのリクエストは有効なタイミングウィンドウまで正常に処理できないため、ほとんどのユースケースでは将来の日付が実用的ではありません。

署名付きリクエストで許可されるもの

署名付きリクエストは、リクエストの署名に使用された認証情報によって許可されたアクションのみを許可できます。認証情報が署名付きリクエストで指定されたアクションを暗黙的または明示的に拒否した場合、署名付きリクエストは送信時に拒否されます。これは、以下に適用されます。

- 認証情報に関連付けられているセッションポリシー
- 認証情報に関連付けられているプリンシパルに関連付けられているアイデンティティベースのポリシー
- セッションまたはプリンシパルに影響するリソースポリシー
- セッションまたはプリンシパルに影響するサービスコントロールポリシー
- セッションまたはプリンシパルに影響するリソースコントロールポリシー

署名付きリクエストを使用する動機

セキュリティエンジニアは、ソリューションビルダーが署名付き URLs を使用する動機となるものを認識する必要があります。必要なものとオプションを理解すると、ソリューションビルダーとの通信に役立ちます。動機には次のようなものがあります。

- Amazon S3 のスケーラビリティを活用しながら、IAM 以外の認証メカニズムをサポートする。主な動機は、Amazon S3 と直接通信して、このサービスが提供する組み込みのスケーラビリティを活用することです。この直接通信がない場合、ソリューションは PutObject および GetObject 呼び出しで送信されるバイトを再送信することによる負荷をサポートする必要があります。総負荷に応じて、この要件により、ソリューションビルダーが回避する可能性のあるスケーリングチャレンジが追加されます。

  URLs の外部で一時的な認証情報 AWS Security Token Service (AWS STS) や署名バージョン 4 の署名を使用するなど、Amazon S3 と直接通信するその他の方法は、ユースケースには適していない場合があります。Amazon S3 は認証情報を通じて AWS ユーザーを識別しますが、署名付きリクエストは AWS 認証情報以外のメカニズムによる識別を前提としています。データの直接通信を維持しながらこの違いを分割することは、署名付きリクエストを通じて達成できます。
- ブラウザが URLs。URLsはブラウザによって理解されますが、 AWS STS 認証情報と署名バージョン 4 の署名は理解されません。これは、ブラウザベースのソリューションと統合する場合に便利です。代替ソリューションにはより多くのコードが必要で、大きなファイルにはより多くのメモリが使用され、マルウェアやウイルススキャナーなどの拡張機能によって異なる処理が行われる可能性があります。

一時的な AWS STS 認証情報との比較

一時的な認証情報は、署名付きリクエストに似ています。 どちらも有効期限が切れ、アクセス範囲指定が許可され、一般的に IAM 以外の認証情報を AWS 認証情報を必要とする使用にブリッジするために使用されます。

一時的な AWS STS 認証情報を 1 つの S3 オブジェクトとアクションに厳密にスコープできますが、AWS STS APIs には制限があるため、スケーリングの課題が発生する可能性があります。(詳細については、AWS re:Post ウェブサイトの「IAM および の API スロットリングまたは「レート超過」エラーを解決する方法 AWS STS」を参照してください。) さらに、生成された各認証情報には AWS STS API コールが必要です。これにより、レイテンシーと回復力に影響を与える可能性のある新しい依存関係が追加されます。一時的な AWS STS 認証情報の最小有効期限は 15 分ですが、署名付きリクエストはより短い期間をサポートできます (適切な条件では 60 秒が実用的です) 。

署名のみのソリューションとの比較

署名付きリクエストの本質的にシークレットコンポーネントは、署名バージョン 4 の署名のみです。クライアントがリクエストの他の詳細を知っていて、その詳細に一致する有効な署名が提供されている場合は、有効なリクエストを送信できます。有効な署名がないと、署名できません。

署名付き URLs と署名のみのソリューションは、暗号的に似ています。ただし、署名のみのソリューションには、クエリ文字列パラメータの代わりに HTTP ヘッダーを使用して署名を送信する機能など、実用的な利点があります (「インタラクションと緩和のログ記録」セクションを参照) 。 管理者は、クエリ文字列がより一般的にメタデータとして扱われるのに対し、ヘッダーはそれほど一般的に扱われないと考える必要があります。

一方、 AWS SDKs、署名を直接生成して使用するためのサポートが少なくなります。署名のみのソリューションを構築するには、より多くのカスタムコードが必要です。実用的な観点からは、セキュリティのためにカスタムコードの代わりにライブラリを使用することが一般的なベストプラクティスであるため、署名のみのソリューションのコードには追加の精査が必要です。

署名のみのソリューションでは、`X-Amz-Expires`クエリ文字列は使用されず、明示的な有効期間も提供されません。IAM は、明示的な有効期限がない署名の暗黙的な有効期間を管理します。これらの暗黙的な期間は公開されません。これらは通常変更されませんが、セキュリティを念頭に置いて管理されるため、有効期間に依存しないでください。有効期限を明示的に制御することと、IAM で有効期限を管理することにはトレードオフ があります。

管理者は、署名のみのソリューションを使用することをお勧めします。ただし、実際には、構築されたソリューションをサポートする必要があります。

署名付きリクエストの識別

署名付き URL を使用したリクエストの識別

Amazon S3 には、Amazon S3 サーバーのアクセスログとデータイベントというリクエストレベルで使用状況をモニタリングするための 2 つの組み込みメカニズムが用意されています。どちらのメカニズムでも、署名付き URL の使用状況を特定できます。 Amazon S3 AWS CloudTrail

署名付き URL の使用についてログをフィルタリングするには、 認証タイプを使用できます。サーバーアクセスログについては、Authentication Type フィールド を調べます。これは、Amazon Athena テーブルで定義されているときに、通常 authtype という名前になります。については CloudTrail、 `additionalEventData`フィールドAuthenticationMethodで を調べます。どちらの場合も、署名付き URLs を使用するリクエストのフィールド値は ですが`QueryString`、`AuthHeader` は他のほとんどのリクエストの値です。

`QueryString` の使用が、署名付き URLsに常に関連しているとは限りません。検索を署名付き URL の使用のみに制限するには、クエリ文字列パラメータ を含むリクエストを検索しますX-Amz-Expires。サーバーアクセスログについては、Request-URI を調べ、クエリ文字列に `X-Amz-Expires`パラメータがあるリクエストを探します。 については CloudTrail、`requestParameters`要素の `X-Amz-Expires`要素を調べます。

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

次の Athena クエリはこのフィルターを適用します。

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

AWS CloudTrail Lake の場合、次のクエリがこのフィルターを適用します。

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

他のタイプの署名付きリクエストの特定

POST リクエストには、Amazon S3 サーバーアクセスログと HtmlFormに一意の認証タイプ もあります CloudTrail。この認証タイプはあまり一般的ではないため、これらのリクエストが環境で見つからない場合があります。

次の Athena クエリは、 のフィルターを適用しますHtmlForm。

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

CloudTrail Lake の場合、次のクエリがフィルターを適用します。

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

リクエストパターンの識別

署名付きリクエストは、前のセクションで説明した方法を使用して確認できます。ただし、そのデータを役に立てるようにするには、パターンを見つける必要があります。クエリの簡単なTOP 10結果からインサイトが得られる場合がありますが、それだけでは不十分な場合は、次の表のグループ化オプションを使用してください。

グループ化オプション	サーバーアクセスログ	CloudTrail レイク	説明
User agent	`GROUP BY useragent`	`GROUP BY userAgent`	このグループ化オプションは、リクエストのソースと目的を見つけるのに役立ちます。ユーザーエージェントはユーザー提供であり、認証または認可メカニズムとしては信頼性がありません。ただし、ほとんどのクライア

グループ化オプション	サーバーアクセスログ	CloudTrail レイク	説明
			ントは、少なくとも部分的に人間が読み取れる一意の文字列を使用しているため、パターンを探している場合は多くのことが明らかになる可能性があります。
リクエスタ	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	このグループ化オプションは、リクエストに署名した IAM プリンシパルを見つけるのに役立ちます。これらのリクエストをブロックしたり、既存のリクエストの例外を作成したりすることが目的の場合、これらのクエリはその目的に十分な情報を提供します。IAM のベストプラクティスに従ってロールを使用すると、ロールの所有者が明確に識別され、その情報を使用して詳細を確認できます。

グループ化オプション	サーバーアクセスログ	CloudTrail レイク	説明
送信元 IP アドレス	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	このオプションは、Amazon S3 に到達する前の最後のネットワーク変換ホップでグループ化します。 • トラフィックが NAT ゲートウェイを通過する場合、これは NAT ゲートウェイアドレスになります。 • トラフィックがインターネットゲートウェイを通過する場合、これはインターネットゲートウェイにトラフィックを送信したパブリック IP アドレスになります。 • トラフィックが の外部から発信された場合 AWS、これはオリジンに関連付けられているパブリックインターネットアドレスになります。

グループ化オプション	サーバーアクセスログ	CloudTrail レイク	説明
			• ゲートウェイ Virtual Private Cloud (VPC) エンドポイントを経由する場合、これは VPC 内のインスタンスの IP アドレスになります。 • パブリック仮想インターフェイス (VIF) を通過する場合、これはリクエスタのオンプレミス IP、または IP アドレスのみを公開するプロキシサーバーやファイアウォールなどの中間 IP になります。 • インターフェイス VPC エンドポイントを通過する場合、これは VPC 内のインスタンスからの IP アドレスである可能性があります。また、別の VPC またはオンプレミスネットワークの IP アドレスで

グループ化オプション	サーバーアクセスログ	CloudTrail レイク	説明
			もかまいません。パブリック VIFsと同様に、これは中間の IP アドレスである可能性があります。 このデータは、ネットワーク制御を課すことを目標としている場合に役立ちます。異なるネットワークがプライベート IP アドレスを重複させる可能性があるため、ソースを明確にするために、このオプションを `endpoint` (サーバーアクセスログの場合) や `vpcEndpointId` (CloudTrail Lake の場合) などのデータと組み合わせる必要がある場合があります。
S3 バケット名	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	このグループ化オプションは、リクエストを受信したバケットを検索するのに役立ちます。これにより、例外の必要性を特定できます。

署名付きリクエストを使用するためのベストプラクティス

このセクションでは、セキュリティエンジニアが考慮すべき署名付きリクエストを使用するためのベストプラクティスについて説明します。ガイドラインには以下が含まれます。

- すべての組織が従うべき基本的なベストプラクティス。
- 追加のガードレールは考慮すべきプラクティスですが、部分的または例外的に実装することを決定する場合があります。これらは、より詳細な制御と防御を提供することを目的としていますが、全体的な複雑さとのバランスを取る必要があります。
- ログ記録のやり取り。これは、責任共有モデルにおけるユーザーまたは顧客の責任の一部であるデバイスまたはサービスから発生する可能性があります。このセクションでは、 ログからアクセスできる情報を制限するための予防策について説明します。

基本的なベストプラクティス

他の AWS API リクエストの効果的なコントロールである一般的なベストプラクティスは、署名付きリクエストにも適用されます。このセクションでは、最小特権とデータ境界の 2 つの最も関連性の高いプラクティスを確認します。これらのプラクティスは、他のプラクティスが拡張する詳細なコントロールを作成します。

最小特権の原則を適用する

署名付きリクエストの使用を制限する最初のステップは、一般的に Amazon S3 へのアクセスを制限することです。署名付き URL は、署名付き URL の署名を生成したプリンシパルに付与されていないリソースへのアクセスを提供することはできません。また、そのプリンシパルに付与されていない方法でリソースへのアクセスを提供することはできません。そのため、ベストプラクティスを適用してこれらのプリンシパルに最小特権を付与することは、効果的なガードレールです。

署名付き URL を作成するプロセスは、署名生成のために公開された標準 (署名バージョン 4) に基づくアルゴリズムオペレーションです。したがって、署名付き URLs の生成に制限を設定することはできません。ただし、関連するには、署名付き URL が有効で、リソースへのアクセスを提供する必要があるため、署名付き URL の有効性も有効なガードレールです。

最小特権の詳細については、 AWS 「 Well-Architected フレームワーク、セキュリティの柱」の「最小特権アクセスを付与する」を参照してください。

データ境界を実装する

最小特権の拡張は、組織のニーズに沿ったデータ境界を維持することです。署名付き URLs はデータ境界と互換性があります。他のリクエスト と同様に、署名付き URL リクエストの有効性はリクエスト時に評価されます。ネットワーク、リソース、ロールセッション、およびプリンシパルのプロパティが変更された場合は、リクエストを受信する方法を使用して、その時点で評価されます。

例えば、Amazon Elastic Kubernetes Service (Amazon EKS) コンテナで実行されているサービスがリクエストに署名するとします。リクエストは、後でインターネットに接続されているユーザーのパーソナルコンピュータシステムから送信されます。この場合、aws:SourceIp 条件は、Amazon EKS コンテナ内のサービスの IP アドレスではなく、ユーザーの個人システムからのリクエストの可視パブリック IP アドレスを評価します。

同様に、リクエストの送信前にプリンシパルまたはリソースのタグが変更された場合、元の値ではなく更新された値が、aws:PrincipalTag/tag-key および aws:ResourceTag/tag-key 条件を通じてリクエストに適用されます。

追加のガードレール

署名付きリクエストがソリューションビルダーとユーザーによって適切に使用されると、データへのアクセスをユーザーに許可する安全なメカニズムが提供されます。さらに、署名付きリクエストを生成する機能は、プリンシパルにまだ持っていないアクセスを提供しません。

そのコンテキストでは、追加のコントロールが必要ですか? 追加のコントロールの根拠は、アクセスを拒否する必要性ではなく、モニタリング、使用の承認、境界の設定、およびユーザーエラーによるリスクを軽減する機能を提供することに基づいています。このようにして、使用が適切で必要であることを確認することができます。

次のガードレールは、この目標に役立ちます。これらのコントロールを有効にする前に、署名付きリクエストを識別して既存の使用状況を確認することをお勧めします。この識別は、ガードレールが既存の使用状況に与える影響に備えたり、必要に応じて例外を計画したりするのに役立ちます。

s3:signatureAge のガードレール

署名付きリクエストの定義特性の 1 つは、有効期限を記述することです。リクエストの署名には日付が含まれています。この日付は、署名付き URL のX-Amz-Dateクエリ文字列パラメータとして、および署名付き POST の日付または x-amz-date ヘッダーとして送信されます。 URLs

Amazon S3 には条件キー s3:signatureAge が用意されています。これを使用して、署名日からリクエストの有効な有効期限までの最大時間を制限できます。この条件は有効期間を延長することはできませんが、短縮できます。

次のポリシーでは、 s3:signatureAge条件キーは署名付きリクエストを 15 分の有効性に制限します。次の例では、すべて 15 分を使用して、標準署名がサポートするのと同様の期間に有効性を制限します。

ポリシーの 2 番目のステートメントは、署名バージョン 2 へのアクセスを拒否します。このバージョンの署名プロトコルは廃止されていますが、一部の では引き続きサポートされています AWS リージョン。完全に廃止する前に、明示的にブロックすることをお勧めします。

次のポリシーを AWS Organizations サービスコントロールポリシー (SCP) として適用できます。署名の生成から使用までの時間が 15 分未満であれば、ユーザーは署名付きリクエストを使用し、それらのリクエストに依存するソリューションをデプロイできます。実装によっては、この制限は影響しないか、ソリューションが使用できなくなるか、再試行できる障害が時折発生する可能性があります。

```
{
  "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"
        }
      }
```

```
    }
  ]
}
```

例外

ソリューションが有効期限より長い時間を必要とするため、前述のポリシーの影響を受ける場合は、例外を承認する方法を指定することをお勧めします。SCP で例外が列挙されないようにするには、次のポリシーのように aws:PrincipalTag を使用して、スケーラブルな方法で例外を管理します。AWS データ境界ポリシー AWS の例など、その他の例では、この戦略を使用します。 https://github.com/aws-samples/data-perimeter-policy-examples/blob/main/README.md

を使用して例外ポリシーを実装する場合はaws:PrincipalTag、プリンシパルのタグの設定へのアクセスを制御する必要があります。このタイプのタグは、設定できるタグ値を制御するこの例のように、プリンシパルから直接取得でき、SCP によって制御できます。このタイプのタグは、ID プロバイダー (IdP) または の使用時に設定されるセッションタグから取得することもできます AWS STS。へのアクセスの制御aws:PrincipalTagは複雑なトピックです。ただし、属性ベースのアクセスコントロール (ABAC) の使用経験のある組織には、このユースケースaws:PrincipalTagで を適切に使用するための経験とコントロールがあります。

次の例では、 aws:PrincipalTag条件は、名前付きタグ (long-presigned-allowed) が割り当てられ、 に設定されたすべてのプリンシパルを許可する例外を作成しますtrue。この例外を除き、署名の有効期間の制限は適用されません。

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

```
  ]
}
```

バケットポリシー

次の例のようにポリシーを使用して、バケットポリシーをすべてのバケットまたは選択したバケットに適用できます。SCP とは異なり、バケットポリシーはサービスプリンシパルの使用もターゲットにします。付録 A は、署名付きリクエストの予想されるサービスプリンシパルの使用を文書化していませんが、その制限を証明するためにコントロールを実装する場合は、次のポリシーがそのコントロールを提供します。また、SCP とは異なり、バケットポリシーは管理アカウントのプリンシパルに適用できます。

ABAC ベースの例外は、SCP と同じ方法でバケットポリシーで機能します。バケットポリシーの目標は、組織外のプリンシパルに適用される場合があるため、ABAC 例外は、ABAC コントロールが適用されるプリンシパルに制限する必要があります。

次の例では、最初のステートメントaws:PrincipalTagの条件により、名前付きタグ (long-presigned-allowed) が割り当てられ、 に設定されたプリンシパルの例外が作成されますtrue。この例外を除き、署名の有効期間の制限は適用されません。2 番目のステートメントは、バケットを所有する組織外のすべてのプリンシパルに AWS この制限を適用します。この 2 番目のステートメントの範囲は、プリンシパルの名前付きタグを設定する ABAC コントロールと一致する必要があります。

```
{
  "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}"
        }
      }
    }
  ]
}
```

リソースコントロールポリシー

リソースコントロールポリシー (RCPs) を使用して、バケットにポリシーを大規模に適用できます。SCPs やバケットポリシーとは異なり、RCPsサービスプリンシパルの使用を対象としません。RCPs、任意のアカウントのサービス以外のプリンシパルに影響しますが、管理アカウントのリソースには影響しません。詳細については、AWS Organizations のドキュメントを参照してください。

バケットポリシーと同様に、 `aws:PrincipalTags`を使用してプリンシパルの例外を作成する場合は、プリンシパルのタグ付けに関する ABAC コントロールの範囲に注意してください。

次の RCP は、署名期間を 15 分に制限することで、組織内のすべての S3 バケットで署名付き URL の使用を制限します。

```
{
  "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:authType のガードレール

署名付き URLsクエリ文字列認証を使用し、署名付き POSTs は常に POST 認証を使用します。Amazon S3 は、s3:authType 条件キーを介した認証タイプに基づくリクエストの拒否をサポートします。 REST-QUERY-STRINGはクエリ文字列s3:authTypeの値で、 POSTは POST s3:authTypeの値です。

次のポリシーを SCP として適用できます。ポリシーは を使用してs3:authType、ヘッダーベースの認証のみを許可します。また、個々のユーザーまたはロールに例外を提供するメソッドも設定します。

```
{
  "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"
        }
      }
    }
  ]
}
```

認証タイプに基づいてリクエストを拒否すると、拒否された認証タイプを使用するソリューションまたは機能に影響します。たとえば、 を拒否すると、ユーザーは Amazon S3 コンソールからアップロードまたはダウンロードを実行REST-QUERY-STRINGできなくなります。ユーザーに Amazon S3 コンソールを使用させたい場合は、このガードレールを使用したり、ユーザーに例外を設定したりしないでください。一方、ユーザーに Amazon S3 コンソールを使用しないようにする場合は、ユーザーREST-QUERY-STRINGに対して拒否できます。

Amazon S3 リソースへのユーザーの直接アクセスを既に拒否している可能性があります。この場合、認証タイプのガードレールは冗長です。ただし、直接アクセスを拒否する実装は通常、例外を含む多くのコントロールステートメントにまたがるため、s3:authType拒否ステートメントはdefense-in-depthユーティリティを提供します。

通常、ワークロードに使用されるロールは、クエリ文字列やPOST認証にアクセスする必要はありません。例外は、署名付きリクエストを使用するように設計されたサービスをサポートするロールです。これらのロールに特定の例外を作成できます。

次のようなポリシーを使用して、バケットポリシーをすべてのバケットまたは選択したバケットに適用することもできます。

```
{
  "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"
        }
      }
    }
  ]
}
```

このバケットポリシーは、CopyObject API と UploadPartCopy APIs を使用してクロスリージョンコピーを行うことを拒否する効果があります。Amazon S3 レプリケーションは、これらの APIs に依存しないため、影響を受けません。

上記のポリシーなどのバケットポリシーを使用し、引き続きクロスリージョン CopyObject または UploadPartCopy API をサポートする場合は、`aws:ViaAWSService`次のような の条件を追加します。

```
{
  "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"
        },
      }
    }
  ]
}
```

署名付きガードレールと例外を他のガードレールと組み合わせる

ユーザーとロールにガードレールを一般的に適用する予定がない場合は、他の一般的なガードレールの例外に適用して、それらの例外が署名付きリクエストをサポートしないようにすることができます。

ネットワーク制限があるが、外部パートナーまたは特別なユースケースの例外を許可する場合は、特に必要であると識別されない限り、例外が適用されるときにクエリ文字列またはPOST認証をブロックする必要があります。

s3:signatureAge の制限事項

管理者は、 の影響s3:signatureAgeをより完全に理解すると便利です。すべての署名付きリクエストにはX-Amz-Date、現在の時刻を示す が含まれます。この値はクライアントによって入力され、request signer. AWS rejects は無効な時間があると見なすリクエストを拒否します。ただし、署名者は将来の時間に署名を事前に生成できます。Amazon S3 は、送信が早すぎる場合、将来の時間を指定するリクエストを拒否します。ただし、署名にサインインするまでリクエストが送信されない場合、署名は以前に生成され、後で送信できます。

s3:signatureAge は、署名付きリクエストに対してのみ、署名X-Amz-Date内の の最大有効期間を制限します。 X-Amz-Expiresまたは POSTポリシーの有効期限が有効であると宣言した場合でも、指定された有効期間より古いリクエストは拒否されます。 s3:signatureAge は、明示的な有効期限を含まないリクエストの有効期間を変更しません。また、クライアントX-Amz-Dateが署名に使用する の値も制御しません。

システムクロックが間違っている場合、またはクライアントが意図的に将来の日付をリクエストした場合、署名時刻は署名が生成された時刻ではない可能性があります。 これにより、 がソリューションを制御s3:signatureAgeできる量が制限されます。署名を生成する現在の時刻を使用するソリューションは、予想される方法で制限されます。署名は、 で指定されたミリ秒数の間有効ですs3:signatureAge。現在の時刻を使用しない ソリューションには、異なる制限があります。1 つの制限は、署名に使用された認証情報がまだ有効であることです。管理者は、発行された一時的な認証情報の最大有効期間を制御できます。認証情報を最大 36 時間有効にすることも、15 分まで有効に制限することもできます。一時的な認証情報の有効期限は、 の値に依存しませんX-Amz-Date。

永続的な認証情報にはこの制限はありません。 一時的な認証情報のみを使用することがベストプラクティスであり、永続的な認証情報を明示的に取り消すことができます。これにより、その認証情報に基づく署名も無効になります。

s3:signatureAge はミリ秒単位で測定されますが、適切に同期されたクロックと低レイテンシーの使用量があっても、60 秒未満に設定することは実用的ではありません。60 秒未満の 設定では、有効なリクエストを拒否するリスクがあります。署名の生成とリクエストの送信の間に遅延が予想される場合、またはクロックの同期に問題がある場合は、 の管理でこれらを考慮する必要がありますs3:signatureAge。

大規模なバケットのターゲット設定

SCPsと RCPsは、 aws:PrincipalTagを使用してユーザーの例外を作成できます。バケットのタグを使用してアクセスを制御することはできませんaws:ResourceTag。アクセスコントロールにはオブジェクトタグのみが使用されます。通常、このコントロールを適用するすべてのオブジェクトにタグを追加することはスケーラブルではありません。

多くのユースケースに適した解決策は、SCP または RCP が適用されるアカウントを変更するか、aws:ResourceAccount、aws:ResourceOrgPaths、または aws:ResourceOrgID を使用して、ポリシーと例外をアカウントレベルで適用することです。たとえば、SCP または RCP を一連の本番稼働用アカウントに適用できます。

もう 1 つの解決策は、カスタム AWS Config ルールを使用して検出コントロールまたは応答コントロールを実装することです。目標は、すべてのバケットに適切なガードレールを持つバケットポリシーを含めることです。バケットポリシーの内容のテストに加えて、バケットに特定の値がタグ付けされている場合、カスタム AWS Config ルールはバケットからタグを取得し、ルールからバケットを除外できます。そのルールがコンプライアンスチェックに失敗した場合、バケットを非準拠としてマークするか、修復を呼び出してバケットのポリシーにガードレールを追加できます。

> **Note**
>
> リクエストのタグコンテンツを PutBucketTagging に制限することはできません。バケットのタグ付け方法の制御を維持するには、 PutBucketTaggingおよび DeleteBucketTagging へのアクセスを制限する必要があります。

インタラクションと緩和策の口グ記録

署名付き URL には署名が含まれており、有効期限前であれば、署名された特定の API オペレーションを実行するために使用できます。一時的なアクセス認証情報として扱う必要があります。署名は、知る必要がある当事者のみに非公開にする必要があります。ほとんどの環境では、これはリクエストを送信するクライアントとそれを受信するサーバーです。直接 HTTPS セッションの一部として署名

を送信すると、HTTPS セッションの参加者のみが署名を送信する URI を可視化できるため、そのプライベートな性質が維持されます。

署名付き URLs、署名はX-Amz-Signatureクエリ文字列パラメータとして送信されます。クエリ文字列パラメータは URI のコンポーネントです。リスクは、クライアントが URI とその署名を記録できることです。クライアントは HTTP リクエスト全体にアクセスし、リクエスト、データ、ヘッダー (認証ヘッダーを含む) の任意の部分をログに記録することができます。ただし、これは規則によって一般的ではありません。URI ログ記録はより一般的であり、アクセスログ記録などの場合に必要です。クライアントは、URIs をログに記録する前に、リダクションまたはマスキングを使用して署名を削除する必要があります。

一部の環境では、ユーザーは仲介者 (プロキシ) が HTTPS セッションを可視化できるようにします。プロキシを有効にするには、設定と信頼できる証明書が必要なため、クライアントシステムへの高レベルの特権アクセスが必要です。プロキシ設定と信頼された証明書をクライアント中間環境のローカルコンテキスト内にインストールすると、非常に高いレベルの権限が許可されます。このため、このような仲介者へのアクセスは厳重に制御する必要があります。

仲介の目的は、通常、不要な出力をブロックし、他の出力を追跡することです。そのため、このような仲介者がリクエストをログに記録するのは一般的です。仲介者は、クライアントと同様に、コンテンツ、ヘッダー、データ (すべて非常に機密性が高い) をログに記録することができますが、X-Amz-Signatureクエリ文字列パラメータを含むような URIs をログに記録する方が一般的です。

緩和策

URI ログ記録は、中間サーバーへの直接アクセスと同様に、X-Amz-Signatureクエリ文字列パラメータを編集するか、クエリ文字列全体を編集するか、情報を機密性の高いものとして扱うことをお勧めします。これらの保護は強く推奨されますが、署名付き URLsが期限切れになるという事実は、署名の有効期限が切れるのに十分な時間、公開が遅延する限り、ログ公開のリスクを軽減します。

Amazon S3 は署名も確認し、適切に処理する必要があります。Amazon S3 サーバーアクセスログにはリクエスト URI が含まれていますがX-Amz-Signature、推奨に従って を編集します。Amazon S3 の CloudTrail データイベントがログに記録される場合も同様です。カスタムデータ識別子を使用してデータをマスクするように Amazon CloudWatch Logs を設定できます。 Amazon S3

次の正規表現は、URI に表示される X-Amz-Signature と一致します。

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

次の正規表現は、より具体的に置き換えるテキストを識別するためのグループ化パターンを追加します。

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

次のようなアクセスログエントリがある場合:

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

最初の正規表現は、アクセスログエントリを次のように変換します。

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

2 番目の正規表現は、キャプチャしないグループをサポートするシステムで、アクセスログエントリを次のように変換します。

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

よくある質問

署名付きリクエストは複数回使用できますか? これはセキュリティリスクですか?

はい。署名付きリクエストの署名は複数回使用できます。これがセキュリティリスクかどうかは、コンテキストに応じた質問です。AWS のサービスにアクセスする他の方法でも、繰り返しが可能です。 AWS 認証情報を持つユーザーまたはワークロードは、多数のリクエストを に送信でき AWS のサービス、それらのリクエストは重複する可能性があります。

ユースケースで 1 回のみの実行が必要な場合は、他のメカニズムを実装して 1 回の使用を強制する必要があります。1 回の使用は、署名付きリクエストの機能ではありません。セキュリティエンジニアはユースケースと実装を確認する必要がありますが、多くの場合、複数回使用すると許容可能な使用に適します。

目的のユーザー以外のユーザーが署名付きリクエストを使用できますか?

署名付きリクエストの署名は、それを所有するすべてのユーザーが送信できます。データ境界制御など、他の形式の検証に合格した場合にのみ受け入れられます。署名の有効期限が切れている場合、署名認証情報の有効期限が切れている場合、または署名認証情報がリクエストされたリソースにアクセスできない場合、リクエストは拒否されます。

他の認証方法でも同じことが言えます AWS のサービス。不適切に共有された認証情報は、不適切なアクセスを許可します。主なベストプラクティスは、認証情報と署名を目的の対象者とのみ共有することです。プライベートデータを安全に保ち、他のユーザーと共有できないように対象者を信頼できない場合、あらゆる形式の認証が損なわれます。

承認されたユーザーは、署名付きリクエストを使用してデータを抽出できますか?

データを保護するには、堅牢なアクションが必要です。データ境界を維持しながら目的のアクセスを有効にするには、包括的なアプローチが必要です。 最小特権アクセス、データ境界制御、一時的なアクセス認証情報のみの使用は、データの保護に適用される一般的なベストプラクティスです。こ

れらのコントロールを適切に使用すると、ユーザーが生成する署名付きリクエストを通じてアクションを実行する機能も制限されます。

これは、署名付きリクエストによって提供されるアクセスが、リクエストの署名に使用される認証情報に付与されるアクセスのサブセットであるためです。このコンテキストでは、データへのアクセスに適用されるベストプラクティスは通常、署名付きリクエストに適用されますが、署名付きリクエストはデータへの新しいアクセスを作成しません。

- 最大有効期限は、署名認証情報の有効期限に制限されます。 署名認証情報が取り消された場合、認証情報に基づく署名は無効になります。
- 署名認証情報に関連付けられている IAM プリンシパルのアクセス許可に、署名付きリクエストに関連付けられたアクションの実行が含まれていない場合、署名付きリクエストを呼び出すと、「アクセス拒否」レスポンスが発生します。 レスポンスは、呼び出し時のアクセス許可の現在の状態によって異なります。この状態は、署名付きリクエストの署名が生成された時刻とは関係ありません。
- プリンシパルのプロパティは、署名認証情報に関連付けられているプリンシパルに基づいて評価されます。
- ロールセッションのプロパティは、署名認証情報に関連付けられているロールセッションに基づいて評価されます。
- ネットワークのプロパティは、通常のリクエストと同様に、リクエストの受信方法に基づいて評価されます。

このコンテキストでは、署名付きリクエストに関連するリスクの調査は、ユーザーの認証情報とは異なる認証情報で署名され、ユーザーのプリンシパルに含まれていないアクセスを提供する領域に制限されます。この調査は、署名付きリクエスト機能自体ではなく、ユーザーに代わって署名を生成するサービス、ワークロード、またはソリューションの設計に適用する必要があります。

署名付き URL が不正な方法で共有されていると思われる場合、その URL からのアクセスを拒否できますか?

はい。これには、URL が署名された認証情報を無効にする必要があります。これを実現するには、複数の方法があります。

- 認証情報が属する IAM プリンシパルからアクセス許可を削除します。その IAM プリンシパルが URL が署名されているリソースとオペレーションにアクセスできなくなった場合、URL はそのオ

ペレーションを実行できません。これは、その IAM プリンシパルからの一致するすべての使用に影響します。

- URL の署名に使用される認証情報が一時的な AWS STS 認証情報である場合は、IAM プリンシパルの特定の時間前に発行された一時的な認証情報のセッションアクセス許可を取り消すことができます。ユースケースによっては、他の有効なセッションが通常の有効期限より前に無効になる場合がありますが、新しいセッションは影響を受けません。セッションのアクセス許可を取り消すと、それらのセッションに関連付けられた認証情報を使用して署名された URLs も無効になりますが、新しいセッションに関連付けられた新しい URLs は影響を受けません。
- URL の署名に使用される認証情報が永続的な認証情報である場合は、アクセスキーを非アクティブ化します。これは、これらの認証情報に関連するすべての使用に影響します。

リソース

「Amazon S3 ドキュメント」

- リクエストの認証 (AWS 署名バージョン 4)
- リクエストの認証: クエリパラメータの使用 (AWS 署名バージョン 4)
- リクエストの認証: POST を使用したブラウザベースのアップロード (AWS 署名バージョン 4)
- Amazon S3 署名バージョン 4 認証固有のポリシーキー
- 署名付き URLs

その他のリファレンス

- AWS でのデータ境界の構築 (AWS ホワイトペーパー)
- SEC03-BP02 最小特権アクセスの付与 (AWS Well Architected Framework、セキュリティの柱)
- SEC03-BP05 組織のアクセス許可ガードレールを定義する (AWS Well Architected Framework、セキュリティの柱)

付録 A: 署名付き URLs AWS のサービス の使用方法

この付録では、署名付き URLs を使用する AWS のサービス および 機能について説明します。この情報には 2 つの目的があります。

- コントロールを実装するセキュリティエンジニアに、それらのコントロールの考えられる影響に関する情報を提供します。
- このリスクが URL ログ記録のやり取りに関連している可能性がある状況を認識する。

> **Important**
>
> この付録には、 の完全なリスト AWS のサービス や署名付き URLs。また、カスタムソリューションやサードパーティーソリューションもカバーしていません。

Amazon S3 コンソール

プリンシパル: コンソールユーザー

デフォルトの有効期限: 5 分

> **免責事項**
>
> このセクションでは、Amazon S3 コンソールの現在の動作について説明します。 AWS コンソールの動作は予告なしに変更される可能性があります。

Amazon S3 コンソールでは、オブジェクトのダウンロードとアップロードがサポートされています。 ダウンロードには、有効期限が 300 秒 (5 分) の署名済み URL が使用されます。 URL は、 へのリクエストによって生成されますhttps://<bucket-region>.console.aws.amazon.com/s3/batchOpsServlet-proxy。

このリクエストは、ユーザーがダウンロードボタンをクリックしたときに開始されるため、ダウンロードの明示的なリクエストが発生するまで URL は事前に生成されず、クライアントに送信されません。

アップロードは似ていますが、コンソールが 2 つのリクエストを送信する点が異なります。プリフライト CORS チェックOPTIONSと ですPUT。 どちらのリクエストも同じ署名を使用します。

署名に使用される認証情報は、現在ログインしているユーザーに関連付けられている一時的な認証情報です。これらの一時的な認証情報を取得する方法 に関する詳細は、このガイドの対象外です。

Amazon S3 Object Lambda

プリンシパル: アクセスポイントの発信者

デフォルトの有効期限: 61 秒

> **Note**
>
> 2025 年 11 月 7 日現在、S3 Object Lambda は、現在 サービスを使用している既存のお客様および Select AWS Partner Network (APN) パートナーのみが利用できます。S3 Object Lambda に似た機能の詳細については、Amazon S3 Object Lambda の可用性の変更」を参照してください。

Amazon S3 Object Lambda は AWS Lambda 関数を使用して、Amazon S3 から取得されるデータを自動的に処理および変換します。S3 Object Lambda が関数を呼び出すと、関数には署名付き URL (`inputS3Url`) が提供され、サポートするアクセスポイントから元のオブジェクトをダウンロードするために使用できます。

これらの署名付き URLsは、S3 Object Lambda を設定するときに提供される、サポートされている Amazon S3 アクセスポイント用に署名されています。 S3 (これは Object Lambda アクセスポイントとは異なります) 。Lambda 関数にバインドされたロールを使用する代わりに、URL は元の発信者の ID を使用して署名され、そのユーザーのアクセス許可は URL の使用時に適用されます。URL に署名付きヘッダーがある場合、Lambda 関数は Amazon S3 への呼び出しにこれらのヘッダーを含める必要があります。

返される署名付き URL の有効期限は 61 秒です (S3 Object Lambda 関数の最大期間より 1 秒長くなります) 。生成された URL は、サポートするアクセスポイントでのみ使用できます。S3 Object Lambda アクセスポイントの呼び出し元は、このアクセスポイントにアクセスできる必要があります。条件 を使用して、S3 Object Lambda のコンテキストへのアクセスを制限できます`"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]`。その条件がサポートするアクセスポイントまたはバケットにアタッチされている場合、ユーザーはサポートするアクセスポイントまたはバケットに直接アクセスできません。

このアプローチの価値は、Lambda 関数に S3 バケットまたはアクセスポイントへのアクセスを許可する必要がないことです。Lambda 関数に関連付けられているロールには WriteGetObjectResponse のアクセス許可が必要ですが、GetObject のアクセス許可は必要ありません。

S3 Object Lambda が署名付き URLs を生成する場合、ネットワーク制限は追加されないため、URL は Lambda 関数の外部で使用できます。ただし、S3 Object Lambda の呼び出し元に対する制限は引き続き適用されます。例えば、Lambda 関数が VPC で実行され、発信者を VPC エンドポイントの使用に制限する場合、署名付き URL を所有しているすべてのユーザーは、その VPC エンドポイントを介して送信する必要があります。 この制限は、SourceIp と VpcSourceIp にも適用されます。

> **Note**
>
> VPC で S3 Object Lambda 関数を使用するには、VPC に WriteGetObjectResponse を呼び出すためのパブリック S3 エンドポイントへのルートが必要です。 これは、VPC エンドポイントを使用するための要件がバケットからデータを取得するリクエストに適用されないことを示すものではありません。

AWS Lambda クロスリージョン CopyObject

プリンシパル: AWS 内部

デフォルトの有効期限: 3600 秒

CopyObject または UploadPartCopy API を使用してコピーする場合 AWS リージョン、Amazon S3 は署名付き URLs内部で使用します。これらの APIsは、 SDKs から直接呼び出すか、 AWS CLI コマンド `aws s3api copy-object`および から呼び出すことができます`aws s3api upload-part`。これらの APIs は Amazon S3 レプリケーションには使用されませんが、レプリケート元とレプリケート先が S3 バケットの場合、 コマンドと `aws s3 sync` コマンドによって AWS CLI `aws s3 cp`使用されます。また、さまざまな SDK の`TransferManager`実装でもサポートされています。AWS SDKs

AWS Lambda GetFunction

プリンシパル: AWS 内部

デフォルトの有効期限: 10 分

AWS Lambda は、Lambda チームが所有している S3 バケットにユーザーバージョンを保存します。 Lambda コンテナにデプロイされたアセットを生成する前に。関数のコードにアク

セスする 場合は、 GetFunction API を呼び出します。 この API は Code.Locationで応答します。 には、10 分間有効な署名付き URL が含まれています (この有効期限は現在の動作であり、公開された契約ではありません)。コードが必要ない場合は、 GetFunctionConfiguration、GetFunctionConcurrency、 と ListTags を使用して、 によって返される他のデータを取得しますGetFunction。

返される URL は、現在ログインしているユーザーの認証情報ではなく、Lambda によってユーザーに代わって署名されます。このため、現在ログインしているユーザーまたはユーザーの一時的なセッション認証情報に適用される条件キー (などaws:SourceIP) は、生成された URL には適用されません。これは、条件キーが GetFunction のみに適用されるか、ユーザーまたはセッションのすべてのAWS API 使用量に適用されるかにかかわらず当てはまります。

Lambda コンソールはGetFunction と返される署名付き URL も使用します。 コンソールは、現在ログインしているユーザーに関連付けられた一時的な認証情報を使用して GetFunction を呼び出します。これらの一時的な認証情報の取得に関する詳細は、このドキュメントの対象外です。

Amazon ECR

プリンシパル: AWS 内部

デフォルトの有効期限: 1 時間

Amazon Elastic Container Registry (Amazon ECR) には GetDownloadUrlForLayer API が用意されています。この API は、1 時間有効な署名付き URL を返し、Amazon ECR イメージからの単一レイヤーのダウンロードをサポートします。ただし、このオペレーションは Amazon ECR プロキシで使用され、イメージのプルとプッシュに一般的にはユーザーが使用しません。

Amazon Redshift Spectrum

プリンシパル: を介して外部スキーマの作成に渡されるロール IAM_ROLE

デフォルトの有効期限: 1 時間

Amazon Redshift Spectrum は内部で署名付き URLs を使用し、署名付き URLs。16 分のs3:signatureAge値を使用できますが、非常に低い値は信頼できません。使用できる最小値は、クエリのタイミングとサイズによって異なります。16 分未満の値は多くのシナリオで機能しますが、テストが必要です。ロールは、Redshift Spectrum によってのみ使用されるように制限できます。Redshift Spectrum は生成URLs を公開しないため、有効期限値が低いという一般的な根拠が軽減されます。

Amazon SageMaker AI Studio

Amazon SageMaker AI Studio は、CreatePresignedDomainUrl と CreatePresignedNotebookInstanceUrl の 2 つの API アクションをサポートしています。ただし、これらの APIs は署名バージョン 4 の署名付き URL 機能には関連していません。これらの APIsは、`authToken`パラメータを使用する URL を作成しますが、標準の Signature Version 4 クエリパラメータはサポートしていません。

`authToken` は別のメカニズムですが、署名付き URLs。これはクエリ文字列パラメータとして送信され、5 分の有効期限をサポートします。

SageMaker AI はネットワーク制限をサポートしています。`sagemaker:CreatePresignedDomainUrl` アクションに制限を設定すると、そのアクションは CreatePresignedDomainUrl の呼び出しと、生成された URL の使用の両方に適用されます。URL が有効なネットワークから生成され、無効なネットワークによって送信されると、URL を生成する API コールは成功しますが、URL を送信するリクエストは失敗します。CreatePresignedNotebookInstanceUrl と `sagemaker:CreatePresignedNotebookInstanceUrl`アクションも同様です。

詳細については、SageMaker AI ドキュメントを参照してください。

付録 B: 署名付き URLs のコントロールが に与える影響 AWS のサービス

この付録では、付録 A で説明 AWS のサービス されている署名付き URLs を使用する と、このガイドで前述したコントロールとのやり取りについて説明します。

s3:signatureAge のガードレール

Amazon S3 コンソールは、 `s3:signatureAge`条件キーで設定された最大有効期限の 5 分によって中断されることはありません。ダウンロードボタンを選択すると、Amazon S3 コンソールは署名 URLs を生成し、独自の 5 分の有効期限を適用します。 Amazon S3 最大時間が 2 分未満の場合、クロックの同期とレイテンシーに基づいてランダムな障害が発生する可能性があります。

Amazon S3 Object Lambda は 61 秒の有効期限を使用するため、61 秒以上の`s3:signatureAge`値に条件を設定しても中断は発生しません。期間が短いほど信頼性が低くなり、断続的な障害が発生する可能性があります。

Amazon S3 クロスリージョン CopyObject は、最大有効期限の 5 分によって中断されません。ただし、期間が短いと、クロックの同期とレイテンシーに基づいてランダムな障害が発生する可能性があります。

では AWS Lambda、GetFunction は顧客アカウント外のオブジェクトへの URL を提供するため、顧客ポリシーは生成された URLs に影響を与えません。

Amazon Redshift Spectrum は 16 分の`s3:signatureAge`条件でテストされています。ただし、期間が短いと中断が発生する可能性があります。

ネットワーク制限を使用しない場合の s3:authType のガードレール

Amazon S3 コンソールは通常、`s3:authType`ガードレールの影響を受けます。コンソールは、ローカルネットワーク設定に基づいて Amazon S3 にルーティングされます。ローカルネットワークがネットワーク制限で許可されている方法で Amazon S3 にルーティング された場合、Amazon S3 コンソールは引き続き機能します。 ただし、許可されていない方法でプロキシまたはパブリックインターネットを介してルーティングされた場合、使用はブロックされます。 ただし、使用量のブロックは、このポリシーの意図である可能性があります。 Amazon S3

Lambda 関数が適切な VPC に接続されていない場合、Amazon S3 Object Lambda に影響します。この設定では、VPC には S3 バケットにアクセスするのではなく、WriteGetObjectResponse を呼び出すための NAT ゲートウェイが必要です。

Amazon S3 クロスリージョン CopyObject は、 `aws:viaAWSService`が true の場合に推奨される例外なしで、このガードレールがバケットポリシーに適用されると中断されます。

Amazon Redshift Spectrum は、拡張 VPC `s3:authType` ルーティングが使用されていない限り、ガードレールの影響を受けます。現在、Redshift Spectrum は、プロビジョニングされたクラスターではなく、サーバーレスクラスターでのみ拡張 VPC ルーティングをサポートしています。

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
更新と明確化	「追加のガードレール」セクションに、RCPsと明確化された例外に関する情報を追加しました。	2025 年 8 月 8 日
初版発行	—	2024 年 7 月 23 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。