Estabelecimento de grades de proteção e monitoramento para URLs pré-assinados

AWS Recomendações

AWS Recomendações: Estabelecimento de grades de proteção e monitoramento para URLs pré-assinados

Table of Contents

Estabelecimento de grades de proteção e monitoramento para pré-assinados URLs

Ryan Baker, Amazon Web Services ()AWS

Agosto de 2025 (histórico do documento)

A segurança é uma preocupação fundamental para todas as empresas e um pilar fundamental no AWS Well-Architected Framework. Como engenheiro de segurança, você desejará implementar barreiras administrativas alinhadas aos requisitos de controle organizacional. No AWS Well-Architected Framework, as grades de proteção definem os limites que limitam a atividade.

Este guia fornece informações básicas e melhores práticas para o uso de objetos pré-assinados URLs, que são usados com objetos do Amazon Simple Storage Service (Amazon S3). O pré-assinado URLs permite que usuários ou aplicativos que tenham acesso a credenciais válidas gerem solicitações assinadas com antecedência e aceitas até um prazo de expiração definido. Um caso de uso comum para presigned URLs é estender o acesso a objetos ou recursos compartilhando essas solicitações. Solicitações pré-assinadas compartilhadas são geradas por sistemas ou usuários que têm os direitos de realizar uma solicitação específica e, em seguida, podem ser enviadas a outros sistemas ou usuários para ampliar a capacidade de realizar a mesma solicitação.

Neste guia, você aprenderá:

- Os conceitos de preassinado URLs
- Casos de uso para pré-assinados URLs
- Guardrails recomendados e opcionais
- Opções de monitoramento
- Exemplos de como Serviços da AWS usar pré-assinado URLs

Público-alvo

Este guia é voltado para arquitetos e engenheiros de segurança responsáveis pela implementação de controles de segurança na Nuvem AWS.

Objetivos

Como engenheiro de segurança, você quer saber como os criadores de soluções estão implementando a segurança e o tipo de acesso que seus usuários finais têm. Este guia aborda um tipo de acesso, pré-assinado URLs, que geralmente é usado com o Amazon S3. O Presigned URLs fornece aos construtores opções para unir eficientemente os mecanismos de autenticação.

No Amazon S3, os pré-assinados URLs representam uma categoria exclusiva de solicitações. Os engenheiros de segurança podem monitorar e gerenciar essas solicitações para garantir que elas sejam usadas somente quando apropriado e necessário. O objetivo deste guia é ajudar os engenheiros de segurança a fornecer esse tipo de supervisão de alto nível.

Depois de ler este guia, você deve entender o que é um URL pré-assinado, quando normalmente é usado e as motivações para seu uso.

Pré-requisitos

Se sua empresa não definiu uma política de segurança, objetivos de controle ou padrões, conforme descrito no guia Implementando controles de segurança na AWS, recomendamos que você conclua essas tarefas de governança antes de continuar com este guia.

Antes de começar, você também deve estar familiarizado com as melhores práticas recomendadas e opcionais para controle e monitoramento. Para obter mais informações, consulte:

- Políticas de controle de serviços (AWS Organizations documentação)
- Políticas de controle de recursos (AWS Organizations documentação)
- Políticas de bucket para o Amazon S3 (documentação do Amazon S3)
- Registro de solicitações com registro de acesso ao servidor (documentação do Amazon S3)
- Registro de chamadas de API do Amazon S3 usando AWS CloudTrail(documentação do Amazon S3)

Visão geral do pré-assinado URLs

Uma URL pré-assinada é um tipo de solicitação HTTP reconhecida pelo serviço AWS Identity and Access Management (IAM). O que diferencia esse tipo de solicitação de todas as outras AWS solicitações é o parâmetro de X-Amz-Expires consulta. Assim como em outras solicitações autenticadas, as solicitações de URL pré-assinadas incluem uma assinatura. Para solicitações de URL pré-assinadas, essa assinatura é transmitida em`X-Amz-Signature`. A assinatura usa operações criptográficas do Signature Version 4 para codificar todos os outros parâmetros da solicitação.

Observações

- A versão 2 do Signature está atualmente em processo de descontinuação, mas ainda é suportada em alguns. Regiões da AWS Este guia se aplica à assinatura do Signature versão 4.
- O serviço de recebimento pode processar cabeçalhos não assinados, mas o suporte para essa opção é limitado e direcionado, de acordo com as melhores práticas. Salvo indicação em contrário, suponha que todos os cabeçalhos devem ser assinados para que uma solicitação seja aceita.

O `X-Amz-Expires` parâmetro permite que uma assinatura seja processada como válida com um desvio maior da data e hora codificada. Outros aspectos da validade da assinatura ainda são avaliados. As credenciais de assinatura, se temporárias, não devem expirar no momento em que a assinatura é processada. As credenciais de assinatura devem ser anexadas a um diretor do IAM que tenha autorização suficiente no momento do processamento.

Os pré-assinados URLs são um subconjunto de solicitações pré-assinadas

Um URL pré-assinado não é o único método para assinar uma solicitação para um horário futuro. O Amazon S3 também oferece suporte a solicitações POST, que geralmente também são pré-assinadas. Uma assinatura POST pré-assinada permite uploads que estejam em conformidade com uma política assinada e tenham uma data de expiração incorporada a essa política.

As assinaturas de solicitações podem ter data futura, embora isso seja incomum. Desde que as credenciais subjacentes sejam válidas, o algoritmo de assinatura não proíbe futuros encontros.

Contudo, essas solicitações não podem ser processadas com sucesso até a janela de tempo válida, o que torna o future dating impraticável para a maioria dos casos de uso.

O que uma solicitação pré-assinada permite?

Uma solicitação pré-assinada só pode permitir ações permitidas pelas credenciais usadas para assinar a solicitação. Se as credenciais negarem implícita ou explicitamente a ação especificada pela solicitação pré-assinada, a solicitação pré-assinada será negada quando for enviada. Isso se aplica ao seguinte:

- Políticas de sessão associadas às credenciais
- Políticas baseadas em identidade associadas ao diretor associado às credenciais
- Políticas de recursos que afetam a sessão ou o diretor
- Políticas de controle de serviço que afetam a sessão ou o diretor
- Políticas de controle de recursos que afetam a sessão ou o diretor

Motivações para usar solicitações pré-assinadas

Como engenheiro de segurança, você deve estar ciente do que motiva os criadores de soluções a usarem o presigned. URLs Entender o que é necessário e o que é opcional ajudará você a se comunicar com os criadores de soluções. As motivações podem incluir o seguinte:

- Para oferecer suporte a um mecanismo de autenticação não IAM e, ao mesmo tempo, se beneficiar da escalabilidade no Amazon S3. A principal motivação é comunicar-se diretamente com o Amazon S3 para se beneficiar da escalabilidade integrada fornecida por esse serviço. Sem essa comunicação direta, uma solução precisaria suportar a carga de retransmissão de bytes enviados PutObjecte GetObjectchamadas. Dependendo da carga total, esse requisito adiciona desafios de escalabilidade que um criador de soluções pode querer evitar.

  Outros meios de comunicação direta com o Amazon S3, como usar credenciais temporárias AWS Security Token Service em AWS STS() ou assinaturas URLs externas do Signature Version 4, podem não ser apropriados para seu caso de uso. O Amazon S3 identifica os usuários por meio de AWS credenciais, enquanto as solicitações pré-assinadas presumem a identificação por meio de mecanismos que não sejam credenciais. AWS É possível superar essa diferença e, ao mesmo tempo, manter a comunicação direta dos dados por meio de solicitações pré-assinadas.
- Para se beneficiar da compreensão nativa de um navegador sobre URLs. URLs são compreendidas pelos navegadores, enquanto AWS STS as credenciais e as assinaturas

do Signature Version 4 não são. Isso é benéfico na integração com soluções baseadas em navegador. Soluções alternativas exigem mais código, usam mais memória para arquivos grandes e podem ser tratadas de forma diferente por extensões, como verificadores de malware e vírus.

Comparação com AWS STS credenciais temporárias

As credenciais temporárias são semelhantes às solicitações pré-assinadas. Ambos expiram, permitem o escopo do acesso e são comumente usados para unir credenciais que não são do IAM a um uso que requer credenciais da AWS.

Você pode definir um escopo rigoroso de uma AWS STS credencial temporária para um único objeto e ação do S3, mas isso pode resultar em desafios de escalabilidade porque AWS STS APIs há limites. (Para obter mais informações, consulte o artigo Como posso resolver erros de limitação de API ou de “Taxa excedida” para IAM e AWS STS no site AWS re:POST.) Além disso, cada credencial gerada exige uma chamada de AWS STS API, o que adiciona latência e uma nova dependência que pode afetar a resiliência. Uma AWS STS credencial temporária também tem um tempo mínimo de expiração de 15 minutos, enquanto uma solicitação pré-assinada pode suportar durações mais curtas. (60 segundos são práticos, dadas as condições certas).

Comparação com soluções somente com assinatura

O único componente inerentemente secreto de uma solicitação pré-assinada é sua assinatura Signature Version 4. Se um cliente souber os outros detalhes de uma solicitação e receber uma assinatura válida que corresponda a esses detalhes, ele poderá enviar uma solicitação válida. Sem uma assinatura válida, não é possível.

As soluções pré-assinadas URLs e somente com assinatura são criptograficamente similares. No entanto, as soluções somente com assinatura têm vantagens práticas, como a capacidade de usar um cabeçalho HTTP em vez de um parâmetro de sequência de caracteres de consulta para transmitir a assinatura (consulte a seção Interações e mitigações de registros). Os administradores também devem considerar que as cadeias de caracteres de consulta são mais comumente tratadas como metadados, enquanto os cabeçalhos são menos comumente tratados como tal.

Por outro lado, AWS SDKs forneça menos suporte para gerar e usar assinaturas diretamente. A criação de uma solução somente com assinatura requer mais código personalizado. Do ponto de vista prático, usar bibliotecas em vez de código personalizado para fins de segurança é uma prática recomendada geral, portanto, o código para soluções somente de assinatura exige um exame mais minucioso.

As soluções somente de assinatura não usam a sequência de caracteres de `X-Amz-Expires` consulta e não fornecem um período de validade explícito. O IAM gerencia os períodos de validade implícita das assinaturas que não têm um prazo de expiração explícito. Esses períodos implícitos não são publicados. Normalmente, eles não mudam, mas são gerenciados pensando na segurança, portanto, você não deve depender dos períodos de validade. Há uma compensação entre ter controle explícito sobre a data de expiração e fazer com que o IAM gerencie a expiração.

Como administrador, talvez você prefira uma solução somente com assinatura. No entanto, em um sentido prático, você precisará oferecer suporte às soluções criadas.

Identificação de solicitações pré-assinadas

Identificação de solicitações que usaram um URL pré-assinado

O Amazon S3 fornece dois mecanismos integrados para monitorar o uso em um nível de solicitação: registros AWS CloudTrail de acesso ao servidor Amazon S3 e eventos de dados. Ambos os mecanismos podem identificar o uso de URL pré-assinado.

Para filtrar os registros de uso de URL pré-assinada, você pode usar o tipo de autenticação. Para registros de acesso ao servidor, examine o campo Tipo de autenticação, que normalmente é denominado authtype quando definido em uma tabela do Amazon Athena. Pois CloudTrail, examine AuthenticationMethodem `additionalEventData` campo. Em ambos os casos, o valor do campo para solicitações que usam URLs preassinadas é`QueryString`, enquanto `AuthHeader` é o valor para a maioria das outras solicitações.

`QueryString`o uso nem sempre está associado a URLs pré-assinados. Para restringir sua pesquisa somente ao uso de URL pré-assinada, encontre solicitações que contenham o parâmetro `X-Amz-Expires` da sequência de caracteres de consulta. Para registros de acesso ao servidor, examine Request-URI e procure solicitações que tenham um `X-Amz-Expires` parâmetro na string de consulta. Para CloudTrail, examine o `requestParameters` elemento em busca de um `X-Amz-Expires` elemento.

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

A seguinte consulta do Athena aplica esse filtro:

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

Para AWS CloudTrail Lake, a consulta a seguir aplica esse filtro:

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

Identificação de outros tipos de solicitações pré-assinadas

A solicitação POST também tem um tipo de autenticação exclusivo,`HtmlForm`, nos registros de acesso ao servidor Amazon S3 e. CloudTrail Esse tipo de autenticação é menos comum, então talvez você não encontre essas solicitações em seu ambiente.

A consulta do Athena a seguir aplica o filtro para: `HtmlForm`

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

Para CloudTrail Lake, a consulta a seguir aplica o filtro:

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

Identificação de padrões de solicitação

Você pode encontrar solicitações pré-assinadas usando as técnicas discutidas na seção anterior. No entanto, para tornar esses dados úteis, você deve encontrar padrões. `TOP 10`Os resultados simples da sua consulta podem fornecer uma visão, mas se isso não for suficiente, use as opções de agrupamento na tabela a seguir.

Opção de agrupamento	Registros de acesso ao servidor	CloudTrailLago	Descrição
Agente de usuário	`GROUP BY useragent`	`GROUP BY userAgent`	Essa opção de agrupamento ajuda você a encontrar a origem e a finalidade das solicitações. O agente do usuário é fornecido pelo usuário e não é confiável como mecanismo de autenticação ou autorização. No

Opção de agrupamento	Registros de acesso ao servidor	CloudTrailLago	Descrição
			entanto, isso pode revelar muito se você estiver procurando por padrões, porque a maioria dos clientes usa uma string exclusiva que é pelo menos parcialmente legível por humanos.
Solicitante	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	Essa opção de agrupamento ajuda a encontrar diretores do IAM que assinaram solicitações. Se sua meta é bloquear essas solicitações ou criar uma exceção para solicitações existentes, essas consultas fornecem informações suficientes para essa finalidade. Quando você usa funções de acordo com as melhores práticas do IAM, a função tem um proprietário claramente identificado, e você pode usar essas informações para saber mais.

Opção de agrupamento	Registros de acesso ao servidor	CloudTrailLago	Descrição
Endereço IP de origem	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	Essa opção é agrupada pelo último salto de tradução de rede antes de chegar ao Amazon S3. • Se o tráfego passar por um gateway NAT, esse será o endereço do gateway NAT. • Se o tráfego passar por um gateway da Internet, esse será o endereço IP público que enviou o tráfego para o gateway da Internet. • Se o tráfego tiver origem externa AWS, esse será o endereço público da Internet associado à origem. • Se ele passar por um endpoint de gateway de nuvem privada virtual

Opção de agrupamento	Registros de acesso ao servidor	CloudTrailLago	Descrição
			(VPC), esse será o endereço IP da instância na VPC. • Se passar por uma interface virtual pública (VIF), esse será o IP local do solicitante ou de qualquer intermediário, como um servidor proxy ou firewall, que expõe somente seu endereço IP. • Se ele passar por uma interface VPC endpoint, esse pode ser o endereço IP de uma instância na VPC. Também pode ser um endereço IP de outra VPC ou de uma rede local. Assim como acontece com os VIFs públicos, esse pode ser o endereço IP de

Opção de agrupamento	Registros de acesso ao servidor	CloudTrailLago	Descrição
			qualquer intermediário. Esses dados são úteis se seu objetivo é impor controles de rede. Talvez seja necessário combinar essa opção com dados como `endpoint` (para registros de acesso ao servidor) ou `vpcEndpointId` (para CloudTrail Lake) para esclarecer a origem, pois redes diferentes podem duplicar endereços IP privados.
Nome do bucket S3	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	Essa opção de agrupamento ajuda a encontrar buckets que receberam solicitações. Isso ajuda você a identificar a necessidade de exceções.

Práticas recomendadas para usar solicitações pré-assinadas

Esta seção discute as melhores práticas para o uso de solicitações pré-assinadas que um engenheiro de segurança deve considerar. As diretrizes incluem:

- Melhores práticas fundamentais, que são práticas que toda organização deve seguir.
- Proteções adicionais, que são práticas que você deve considerar, mas que pode decidir implementá-las parcialmente ou com exceções. Eles têm o objetivo de fornecer controle e defesa adicionais em profundidade, mas devem ser equilibrados em relação à complexidade geral.
- Registrar interações, que podem resultar de dispositivos ou serviços que fazem parte da sua responsabilidade ou da responsabilidade de seu cliente no modelo de responsabilidade compartilhada. Esta seção inclui precauções para limitar as informações que podem ser acessadas por meio de registros.

Práticas recomendadas fundamentais

As melhores práticas gerais que são controles eficazes para outras solicitações de AWS API também se aplicam às solicitações pré-assinadas. Esta seção analisa duas das práticas mais relevantes: privilégios mínimos e perímetros de dados. Essas práticas criam uma profundidade de controles que outras práticas ampliam.

Aplicação do princípio de privilégio mínimo

A primeira etapa para limitar o uso de solicitações pré-assinadas é limitar o acesso ao Amazon S3 em geral. Um URL pré-assinado não pode fornecer acesso a recursos que não foram concedidos ao principal que gerou a assinatura do URL pré-assinado. Também não pode fornecer acesso a um recurso de uma forma que não tenha sido concedida a esse diretor. Dessa forma, aplicar as melhores práticas para conceder a esses diretores o mínimo de privilégio é uma barreira eficaz.

O processo de criação de uma URL pré-assinada é uma operação algorítmica baseada em um padrão publicado (Signature Version 4) para geração de assinaturas. Portanto, não é possível colocar limites na geração de URLs pré-assinados. No entanto, para ser relevante, um URL pré-assinado deve ser válido e fornecer acesso aos recursos, portanto, a validade de um URL pré-assinado também é uma barreira eficaz.

Para obter mais informações sobre privilégios mínimos, consulte Conceder acesso com privilégios mínimos no pilar AWS Well-Architected Estrutura, Segurança.

Implemente um perímetro de dados

Uma extensão de menor privilégio é manter um perímetro de dados consistente com as necessidades da sua organização. Os URLs pré-assinados são compatíveis com os perímetros de dados. Assim como em outras solicitações, a validade de uma solicitação de URL pré-assinada é avaliada no momento da solicitação. Se as propriedades da rede, do recurso, da sessão de função e do principal mudarem, elas serão avaliadas no momento e usando o método pelo qual a solicitação é recebida.

Por exemplo, digamos que um serviço executado em um contêiner do Amazon Elastic Kubernetes Service (Amazon EKS) assine uma solicitação. Posteriormente, a solicitação é enviada do sistema de computador pessoal do usuário conectado à Internet. Nesse caso, a SourceIp condição aws: avalia o endereço IP público visível da solicitação do sistema pessoal do usuário, não o endereço IP do serviço no contêiner Amazon EKS.

Da mesma forma, se as tags do principal ou do recurso mudarem antes do envio da solicitação, os valores atualizados, não originais, serão aplicados à solicitação por meio das ResourceTag/tag-key condições aws: PrincipalTag/tag-key e aws:.

Guardrails adicionais

Quando as solicitações pré-assinadas são usadas adequadamente pelos criadores de soluções e pelos usuários, elas fornecem um mecanismo seguro para dar aos usuários acesso aos dados. Além disso, a capacidade de gerar solicitações pré-assinadas não fornece aos diretores um acesso que eles ainda não tinham.

Nesse contexto, controles adicionais são necessários? A justificativa para controles adicionais não se baseia na necessidade de negar o acesso, mas em fornecer a capacidade de monitorar, aprovar o uso, estabelecer limites e reduzir o risco de erros do usuário. Dessa forma, você pode ajudar a garantir que o uso seja apropriado e necessário.

As grades de proteção a seguir ajudam você a atingir esse objetivo. Antes de ativar esses controles, talvez você queira determinar o uso existente identificando solicitações pré-assinadas. Essa identificação ajuda você a se preparar para o impacto da grade de proteção no uso existente ou a planejar exceções quando necessário.

Guardrail para S3: SignatureAge

Uma característica definidora das solicitações pré-assinadas é que elas descrevem um prazo de expiração. A assinatura da solicitação contém uma data. Essa data é transmitida como um parâmetro de sequência de caracteres de `X-Amz-Date` consulta para URLs pré-assinados e como um cabeçalho de data ou x-amz-date para um POST pré-assinado.

O Amazon S3 fornece uma chave de condição, S3:SignatureAge, que você pode usar para limitar o tempo máximo entre a data de assinatura e a expiração efetiva da solicitação. Essa condição nunca pode aumentar o período de validade, mas pode reduzi-lo.

Na política a seguir, a chave de `s3:signatureAge` condição limita as solicitações pré-assinadas a 15 minutos de validade. Todos os exemplos a seguir usam 15 minutos para limitar a validade a um período de tempo semelhante ao suportado pela assinatura padrão.

A segunda declaração da política nega qualquer acesso ao Signature Version 2. Essa versão do protocolo de assinatura está sendo descontinuada, mas ainda é suportada em alguns. Regiões da AWS Recomendamos que você o bloqueie explicitamente antes que seja totalmente descontinuado.

Você pode aplicar a política a seguir como uma política AWS Organizations de controle de serviço (SCP). Os usuários ainda podem usar solicitações pré-assinadas e implantar soluções que dependam dessas solicitações, desde que o tempo entre a geração e o uso da assinatura seja inferior a 15 minutos. Dependendo da implementação, essa limitação pode não ter impacto, pode fazer com que uma solução se torne inutilizável ou pode causar falhas ocasionais que podem ser repetidas.

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

Exceções

Se uma solução precisar de mais tempo antes da expiração e, portanto, for afetada pela política anterior, recomendamos que você forneça um método para aprovar exceções. Para evitar enumerar exceções em um SCP, use aws:, como na política a seguirPrincipalTag, para gerenciar exceções de forma escalável. Outros AWS exemplos, como os exemplos de políticas de perímetro de dados da AWS, usam essa estratégia.

Se você implementar uma política de exceção usando`aws:PrincipalTag`, deverá controlar o acesso à configuração de tags nos principais. Tags desse tipo podem vir diretamente dos principais e podem ser controladas por um SCP, como neste exemplo de controle de quais valores de tag podem ser definidos. Uma tag desse tipo também pode vir de tags de sessão, que são definidas por um provedor de identidade (IdP) ou durante o uso. AWS STS Controlar o acesso ao `aws:PrincipalTag` é um tópico complexo. No entanto, uma organização com experiência no uso do controle de acesso baseado em atributos (ABAC) terá a experiência e os controles necessários para permitir o uso adequado desse caso de `aws:PrincipalTag` uso.

No exemplo a seguir, a `aws:PrincipalTag` condição cria uma exceção que permite que qualquer principal com a tag nomeada (`long-presigned-allowed`) seja atribuída e definida como`true`. Com essa exceção, a restrição de idade da assinatura não é aplicada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
```

```
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    }
  ]
}
```

Políticas de buckets

Você pode aplicar políticas de bucket a todos ou a alguns buckets usando uma política como no exemplo a seguir. Ao contrário de um SCP, uma política de bucket também visa o uso principal do serviço. O Apêndice A não documenta nenhum uso esperado do principal serviço de solicitações pré-assinadas, mas se você quisesse implementar um controle para provar esse limite, a política a seguir forneceria esse controle. Além disso, diferentemente de um SCP, uma política de bucket pode ser aplicada aos diretores em sua conta de gerenciamento.

ABAC-based as exceções funcionam nas políticas de bucket da mesma forma que um SCP. Uma meta de uma política de compartimento pode ser a aplicação a diretores fora da organização, portanto, as exceções do ABAC devem ser restritas aos diretores aos quais os controles do ABAC se aplicam.

No exemplo a seguir, a `aws:PrincipalTag` condição na primeira instrução cria uma exceção para um principal com a tag nomeada (`long-presigned-allowed`) atribuída e definida como`true`. Com essa exceção, a restrição de idade da assinatura não é aplicada. A segunda declaração aplica essa restrição a todos os diretores fora da AWS organização proprietária do bucket. O escopo dessa segunda declaração deve corresponder aos controles ABAC para definir a tag nomeada para os principais.

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

Políticas de controle de recursos

Você pode aplicar uma política a buckets em grande escala usando políticas de controle de recursos (RCPs). Assim como os SCPs e, diferentemente das políticas de bucket, os RCPs não visam o uso principal do serviço. Os RCPs afetam os diretores que não prestam serviços em nenhuma conta, mas não afetam os recursos na conta de gerenciamento. Para obter mais informações, consulte a documentação do AWS Organizations.

Assim como acontece com as políticas de bucket, se você usa `aws:PrincipalTags` para criar exceções para entidades principais, tenha em mente o escopo dos controles ABAC sobre a marcação de entidades principais.

O RCP a seguir restringe o uso de URL pré-assinado em todos os buckets do S3 em uma organização, limitando a duração da assinatura a 15 minutos.

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

Guardrail para S3:AuthType

URLs pré-assinados usam autenticação de sequência de caracteres de consulta, e POSTs pré-assinados sempre usam autenticação POST. O Amazon S3 suporta a negação de solicitações com base no tipo de autenticação por meio da chave de condição s3:AuthType. `REST-QUERY-STRING`é o `s3:authType` valor para cadeias de caracteres de consulta e `POST` é o `s3:authType` valor para POST.

Você pode aplicar a política a seguir como SCP. A política é usada `s3:authType` para permitir somente a autenticação baseada em cabeçalho. Ele também configura um método para fornecer exceções a usuários ou funções individuais.

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

Negar solicitações com base no tipo de autenticação afeta qualquer solução ou recurso que use o tipo de autenticação negada. Por exemplo, negar `REST-QUERY-STRING` impede que os usuários realizem uploads ou downloads a partir do console Amazon S3. Se você quiser que os usuários usem o console do Amazon S3, não use essa grade de proteção nem faça uma exceção para os usuários. Por outro lado, se você não quiser que os usuários usem o console Amazon S3, você pode negar `REST-QUERY-STRING` para os usuários.

Talvez você já negue aos usuários acesso direto aos recursos do Amazon S3. Nesse caso, uma grade de proteção para o tipo de autenticação é redundante. No entanto, uma declaração de

`s3:authType` negação fornece uma utilidade de defesa profunda porque as implementações para negar acesso direto geralmente abrangem muitas instruções de controle, algumas com exceções.

As funções usadas para cargas de trabalho normalmente não precisam de acesso à sequência de caracteres de consulta ou à `POST` autenticação. As exceções são funções que oferecem suporte a serviços projetados para usar solicitações pré-assinadas. Você pode criar exceções específicas para essas funções.

Você também pode aplicar uma política de bucket a todos ou a alguns buckets usando uma política como a seguinte:

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

Essa política de bucket tem o efeito de negar o uso das UploadPartCopyAPIs CopyObjecte para fazer cópias entre regiões. A replicação do Amazon S3 não é afetada porque não depende dessas APIs.

Se você quiser usar uma política de bucket, como a política anterior, e ainda oferecer suporte à UploadPartCopyAPI CopyObjectou Cross-region, adicione uma condição `aws:ViaAWSService` semelhante à seguinte:

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

Combinando grades de proteção pré-assinadas e exceções a outras grades de proteção

Se você não planeja aplicar uma barreira de proteção em geral aos seus usuários e funções, convém aplicá-la às exceções de outras grades de proteção comuns, para que essas exceções não suportem solicitações pré-assinadas.

Se você tem restrições de rede, mas permite exceções para parceiros externos ou casos de uso especiais, bloqueie a sequência de caracteres de consulta ou a `POST` autenticação quando essas exceções forem aplicadas, a menos que elas sejam especificamente identificadas como obrigatórias.

Limitações do S3: SignatureAge

Os administradores acharão útil entender `s3:signatureAge` mais detalhadamente as implicações de. Cada solicitação assinada inclui`X-Amz-Date`, o que deve indicar a hora atual. Esse valor é preenchido pelo cliente e pelo signatário da solicitação. AWS rejeita solicitações que considere ter horários inválidos. No entanto, um signatário pode gerar assinaturas com antecedência em um horário futuro. O Amazon S3 rejeita solicitações que especificam um horário futuro se forem enviadas com muita antecedência. No entanto, se a solicitação não for enviada até o momento em que você fizer login na assinatura, a assinatura poderá ser gerada mais cedo e enviada posteriormente.

`s3:signatureAge`limita a idade máxima `X-Amz-Date` de uma assinatura somente para solicitações pré-assinadas. Solicitações maiores que a idade especificada são negadas, mesmo que a expiração `X-Amz-Expires` ou uma `POST` política a tenha declarado válida. `s3:signatureAge`não altera o período válido para solicitações que não incluem uma expiração explícita. Também não controla o valor `X-Amz-Date` que um cliente usa para uma assinatura.

Se o relógio do sistema estiver errado ou se um cliente solicitar intencionalmente datas futuras, a hora assinada pode não ser a hora em que a assinatura foi gerada. Isso limita o quanto as soluções `s3:signatureAge` podem controlar. Uma solução que usa a hora atual ao gerar assinaturas é limitada da maneira esperada: as assinaturas permanecem válidas pelo número de milissegundos especificado em. `s3:signatureAge` Uma solução que não usa a hora atual terá limites diferentes. Uma restrição é que as credenciais usadas para assinar a assinatura ainda devem ser válidas. Como administrador, você pode controlar a validade máxima das credenciais temporárias emitidas. Você pode permitir que as credenciais sejam válidas por até 36 horas ou restringir a validade a até 15 minutos. A expiração das credenciais temporárias não depende do valor de`X-Amz-Date`.

As credenciais permanentes não têm essa restrição. Usar somente credenciais temporárias é uma prática recomendada, e você pode revogar explicitamente qualquer credencial permanente, o que também invalidaria qualquer assinatura com base nessa credencial.

Embora `s3:signatureAge` seja medido em milissegundos, não é prático configurá-lo para menos de 60 segundos, mesmo se você tiver um relógio bem sincronizado e baixa latência de uso. Configurações com menos de 60 segundos correm o risco de rejeitar solicitações válidas. Se você espera atrasos entre a geração da assinatura e o envio da solicitação, ou problemas com a sincronização do relógio, considere esses atrasos no gerenciamento de. `s3:signatureAge`

Segmentação de buckets em grande escala

SCPs e RCPs podem ser usados `aws:PrincipalTag` para fazer exceções para os usuários. Você não pode usar tags em um bucket para controlar o acesso por meio de `aws:ResourceTag` – somente tags de objeto são usadas para controle de acesso. Geralmente, não é escalável adicionar uma tag a cada objeto ao qual você deseja aplicar esse controle.

Uma solução adequada para muitos casos de uso é aplicar a política e a exceção no nível da conta, alterando as contas às quais o SCP ou o RCP se aplicam ou usando aws: ResourceAccount, aws: ResourceOrgPaths ou aws: ResourceOrg ID. Por exemplo, um SCP ou RCP pode ser aplicado a um conjunto de contas de produção.

Outra solução é usar uma AWS Config regra personalizada para implementar um controle de detetive ou controle responsivo. A meta seria que cada bucket contivesse uma política de bucket com a proteção apropriada. Além de testar o conteúdo de uma política de intervalo, a AWS Config regra personalizada pode recuperar as tags do intervalo e excluir o intervalo da regra se o intervalo estiver marcado com um valor específico. Se essa regra falhar na verificação de conformidade, ela poderá marcar o bucket como não compatível ou invocar uma remediação para adicionar a proteção à política do bucket.

> **Note**
>
> Você não pode restringir o conteúdo da tag das solicitações PutBucketTaggingа. Para manter o controle sobre como um bucket é marcado, você deve limitar o acesso a `PutBucketTagging` DeleteBucketTaggingе.

Registrando interações e mitigações

Um URL pré-assinado contém uma assinatura e pode ser usado, durante o período anterior à expiração, para realizar a operação de API específica para a qual foi assinado. Ela deve ser tratada como uma credencial de acesso temporário. A assinatura deve permanecer privada somente para as partes que precisam conhecê-la. Na maioria dos ambientes, é o cliente que envia a solicitação e o servidor que a recebe. Enviar a assinatura como parte de uma sessão HTTPS direta mantém sua natureza privada, pois somente um participante da sessão HTTPS tem visibilidade do URI que transmite a assinatura.

Para URLs pré-assinados, a assinatura é transmitida como o parâmetro da sequência de caracteres de `X-Amz-Signature` consulta. Os parâmetros da sequência de caracteres de consulta são um componente de um URI. O risco é que os clientes possam registrar o URI e a assinatura com ele. Os clientes têm acesso a toda a solicitação HTTP e podem registrar qualquer parte da solicitação, dos dados e dos cabeçalhos (incluindo cabeçalhos de autenticação). No entanto, isso é, por convenção, menos comum. O registro de URI é mais comum e é necessário em casos como o registro de acesso. Os clientes devem usar redação ou mascaramento para remover a assinatura antes de registrar os URIs.

Em alguns ambientes, os usuários permitem que intermediários (proxies) tenham visibilidade em suas sessões HTTPS. A habilitação de proxies requer um alto nível de acesso privilegiado aos sistemas clientes, pois eles exigem configuração e certificados confiáveis. A instalação da

configuração de proxy e certificados confiáveis, dentro do contexto local do ambiente intermediário do cliente, permite um nível muito alto de privilégio. Por esse motivo, o acesso a esses intermediários deve ser rigorosamente controlado.

O objetivo de um intermediário geralmente é bloquear saídas indesejadas e rastrear outras saídas. Dessa forma, é comum que esses intermediários registrem solicitações. Embora os intermediários possam, como os clientes, registrar qualquer conteúdo, cabeçalho e dados (todos os quais seriam muito confidenciais), é mais comum que eles registrem URIs, como aqueles que incluem o parâmetro de sequência de caracteres de `X-Amz-Signature` consulta.

Mitigações

Recomendamos que o registro de URI redija o parâmetro da sequência de caracteres de `X-Amz-Signature` consulta, redija toda a sequência de caracteres de consulta ou trate as informações como altamente confidenciais, como acontece com o acesso direto ao servidor intermediário. Embora essas proteções sejam altamente recomendadas, o fato de os URLs pré-assinados expirarem reduz os riscos de exposição dos registros, desde que a exposição seja adiada por tempo suficiente para que as assinaturas expirem.

O Amazon S3 também vê as assinaturas e deve tratá-las adequadamente. Os logs de acesso ao servidor Amazon S3 incluem o URI da solicitação, mas o editam conforme recomendado`X-Amz-Signature`. O mesmo acontece quando CloudTrail os eventos de dados são registrados para o Amazon S3. Você pode configurar o Amazon CloudWatch Logs para mascarar dados usando identificadores de dados personalizados.

A expressão regular a seguir corresponde à `X-Amz-Signature` que aparece em um URI:

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

A expressão regular a seguir adiciona padrões de agrupamento para identificar o texto a ser substituído mais especificamente:

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

Se você tiver uma entrada de registro de acesso como a seguinte:

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

A primeira expressão regular traduz a entrada do registro de acesso em:

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

A segunda expressão regular, em sistemas que oferecem suporte a grupos sem captura, traduz a entrada do registro de acesso em:

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Perguntas frequentes

Uma solicitação pré-assinada pode ser usada várias vezes? Isso é um risco de segurança?

Sim, uma assinatura em uma solicitação pré-assinada pode ser usada mais de uma vez. Se isso é um risco de segurança é uma questão contextual. Outros métodos de acesso aos serviços da AWS também permitem a repetição. Um usuário ou carga de trabalho com AWS credenciais pode enviar muitas solicitações para Serviços da AWS, e qualquer uma dessas solicitações pode ser duplicada.

Se seu caso de uso exigir uma única execução, você deverá implementar outros mecanismos para impor o uso único. O uso único não é um recurso de solicitações pré-assinadas. Como engenheiro de segurança, você deve analisar os casos de uso e as implementações, mas, em muitos casos, o uso múltiplo é adequado para uso aceitável.

Alguém que não seja o usuário pretendido pode usar uma solicitação pré-assinada?

Uma assinatura em uma solicitação pré-assinada pode ser enviada por qualquer pessoa que a possua. Ele será aceito somente se passar por outras formas de validação, como controles de perímetro de dados. Se a assinatura tiver expirado, as credenciais de assinatura expirarem ou as credenciais de assinatura não tiverem acesso aos recursos solicitados, a solicitação será negada.

O mesmo vale para outros métodos de autenticação com Serviços da AWS. Credenciais compartilhadas de forma inadequada permitem acesso inadequado. A melhor prática básica é compartilhar credenciais e assinaturas somente com o público-alvo. Se você não pode confiar em seu público-alvo para manter os dados privados seguros e não compartilhá-los com outras pessoas, isso prejudicará qualquer forma de autenticação.

Um usuário autorizado pode usar uma solicitação pré-assinada para exfiltrar dados?

Proteger os dados exige uma ação robusta. Permitir o acesso para os fins pretendidos e, ao mesmo tempo, manter um perímetro de dados requer uma abordagem abrangente. Acesso com privilégios

mínimos, controles de perímetro de dados e uso somente de credenciais de acesso temporário são as melhores práticas gerais que se aplicam à proteção de dados. O uso adequado desses controles também limita a capacidade dos usuários de realizar ações por meio das solicitações pré-assinadas que eles geram.

Isso ocorre porque o acesso fornecido por uma solicitação pré-assinada é um subconjunto do acesso concedido às credenciais usadas para assinar a solicitação. Nesse contexto, as melhores práticas que se aplicam ao acesso aos dados geralmente se aplicam às solicitações pré-assinadas, mas as solicitações pré-assinadas não criam novos acessos aos dados.

- A expiração máxima é limitada à expiração das credenciais de assinatura. Se as credenciais de assinatura forem revogadas, as assinaturas baseadas nas credenciais não serão mais válidas.
- Se as permissões para o principal do IAM associadas às credenciais de assinatura não incluírem a execução da ação associada à solicitação pré-assinada, invocar uma solicitação pré-assinada resultará em uma resposta de “acesso negado”. A resposta depende do estado atual das permissões no momento da invocação, que não tem relação com o momento em que a assinatura da solicitação pré-assinada foi gerada.
- As propriedades do principal são avaliadas com base no principal associado às credenciais de assinatura.
- As propriedades de uma sessão de função são avaliadas com base na sessão de função associada às credenciais de assinatura.
- As propriedades da rede são avaliadas com base em como a solicitação foi recebida, como acontece com as solicitações normais.

Nesse contexto, o exame dos riscos associados às solicitações pré-assinadas é restrito às áreas em que elas são assinadas com credenciais diferentes das credenciais do usuário e fornecem acesso que não fazia parte do principal do usuário. Esse exame deve ser aplicado ao design do serviço, à carga de trabalho ou à solução que gera assinaturas em nome do usuário, em vez do próprio recurso de solicitação pré-assinada.

Posso negar o acesso de um URL pré-assinado se eu suspeitar que ele foi compartilhado de forma não autorizada?

Sim. Isso requer a invalidação das credenciais com as quais o URL foi assinado. Há várias maneiras de fazer isso:

- Remova as permissões do diretor do IAM ao qual as credenciais pertencem. Se esse diretor do IAM não tiver mais acesso ao recurso e à operação para os quais o URL está assinado, o URL não poderá executar essa operação. Isso afeta todo o uso correspondente desse principal do IAM.
- Se as credenciais usadas para assinar o URL forem temporárias, você poderá revogar AWS STS as permissões de sessão para credenciais temporárias emitidas antes de um horário específico para o diretor do IAM. Dependendo do caso de uso, pode haver outras sessões válidas que sejam invalidadas antes do prazo normal de expiração, mas as novas sessões não serão afetadas. A revogação das permissões da sessão também invalida todas as URLs que foram assinadas usando credenciais associadas a essas sessões, mas as novas URLs associadas às novas sessões não serão afetadas.
- Se as credenciais usadas para assinar o URL forem permanentes, desative a chave de acesso. Isso afeta todo o uso vinculado a essas credenciais.

Recursos

Documentação do Amazon S3

- Solicitações de autenticação (AWS assinatura versão 4)
- Autenticando solicitações: usando parâmetros de consulta (AWS Signature versão 4)
- Solicitações de autenticação: uploads baseados em navegador usando POST (AWS Signature versão 4)
- Chaves de política específicas de autenticação do Amazon S3 Signature versão 4
- Trabalhando com URLs pré-assinados

Outras referências

- Construindo um perímetro de dados na AWS (AWS whitepaper)
- SEC03-BP02 Conceda acesso com privilégios mínimos (AWS Well Architected Framework, pilar de segurança)
- SEC03-BP05 Defina barreiras de permissão para sua organização (Well Architected Framework, Security Pillar)AWS

Apêndice A: Como usar o pré-assinado Serviços da AWS URLs

Este apêndice fornece informações Serviços da AWS e recursos que usam presigned. URLs Essas informações têm dois propósitos:

- Fornecer aos engenheiros de segurança que implementam controles informações sobre os possíveis impactos desses controles.
- Para conscientizar sobre situações em que esse risco pode ser relevante para interações de registro de URL.

> **Important**
>
> Este apêndice não fornece uma lista completa nem o uso de Serviços da AWS presignados. URLs Também não abrange soluções personalizadas ou de terceiros.

Console do Amazon S3

Principal: Usuário do console

Expiração padrão: 5 minutos

> **Isenção de responsabilidade**
>
> Esta seção documenta o comportamento atual do console Amazon S3. AWS os comportamentos do console estão sujeitos a alterações sem aviso prévio.

O console do Amazon S3 suporta o download e o upload de objetos. Os downloads usam um URL pré-assinado que tem um tempo de expiração de 300 segundos (5 minutos). O URL é gerado por uma solicitação para`https://<bucket-region>.console.aws.amazon.com/s3/batch0psServlet-proxy`.

Essa solicitação é iniciada quando o usuário clica em um botão de download, para que o URL não seja gerado com antecedência nem enviado ao cliente até que a solicitação explícita de download ocorra.

Os uploads são semelhantes, exceto que o console envia duas solicitações: `OPTIONS` como uma verificação CORS antes do voo e. `PUT` Ambas as solicitações usam a mesma assinatura.

As credenciais usadas para assinar são credenciais temporárias associadas ao usuário atualmente conectado. Detalhes sobre o método para obter essas credenciais temporárias estão fora do escopo deste guia.

Amazon S3 Object Lambda

Principal: Chamador de ponto de acesso

Expiração padrão: 61 segundos

> **Note**
>
> A partir de 7 de novembro de 2025, o S3 Object Lambda está disponível somente para clientes existentes que estão usando o serviço no momento, bem como para parceiros selecionados AWS Partner Network (APN). Para recursos semelhantes ao S3 Object Lambda, saiba mais aqui — Alteração na disponibilidade do Amazon S3 Object Lambda.

O Amazon S3 Object Lambda usa AWS Lambda funções para processar e transformar dados automaticamente à medida que são recuperados do Amazon S3. Quando o S3 Object Lambda invoca uma função, a função recebe uma URL pré-assinada `inputS3Url` () que pode ser usada para baixar o objeto original do ponto de acesso de suporte.

Esses pré-assinados URLs são assinados para o ponto de acesso Amazon S3 de suporte, que é fornecido quando você configura o S3 Object Lambda. (Isso não é o mesmo que o ponto de acesso do Object Lambda.) Em vez de usar uma função vinculada à função Lambda, a URL é assinada usando a identidade do chamador original, e as permissões desse usuário serão aplicadas quando a URL for usada. Se houver cabeçalhos assinados na URL, a função Lambda deve incluir esses cabeçalhos na chamada para o Amazon S3.

O URL pré-assinado que é retornado tem um tempo de expiração de 61 segundos (um segundo a mais do que a duração máxima de uma função Lambda do S3 Object). O URL gerado só pode

ser usado com o ponto de acesso de suporte. O chamador do ponto de acesso S3 Object Lambda precisa ter acesso a esse ponto de acesso. Você pode limitar esse acesso ao contexto do S3 Object Lambda usando a condição. `"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]` Quando essa condição é anexada a um ponto de acesso ou bucket de suporte, o usuário não pode acessar diretamente o ponto de acesso ou bucket de suporte.

O valor dessa abordagem é que não há necessidade de conceder acesso à função Lambda ao seu bucket ou ponto de acesso do S3. A função associada à função Lambda precisará de permissões WriteGetObjectResponse, mas não precisará de permissões para. GetObject

Quando o S3 Object Lambda gera um código URLs pré-assinado, ele não adiciona restrições de rede, portanto, um URL pode ser usado fora da função Lambda. No entanto, quaisquer restrições impostas ao chamador do S3 Object Lambda ainda se aplicam. Por exemplo, se sua função Lambda for executada em uma VPC e você restringir o chamador a usar um VPC endpoint, qualquer pessoa que possua a URL pré-assinada precisaria enviá-la por meio desse endpoint da VPC. Essa restrição também se aplica a SourceIpe. VpcSourceIp

> **Note**
>
> Para usar uma função Lambda do S3 Object em uma VPC, a VPC deve ter uma rota para os endpoints públicos do S3 para fazer a chamada. WriteGetObjectResponse Isso não indica que os requisitos para usar um VPC endpoint não se aplicariam às solicitações de recuperação de dados do bucket.

AWS Lambda Entre regiões CopyObject

Diretor:AWS interno

Expiração padrão: 3600 segundos

Quando você usa a UploadPartCopyAPI CopyObjectou para copiar Regiões da AWS, o Amazon S3 usa URLs presigned internamente. Eles APIs podem ser chamados diretamente de SDKs ou a partir dos AWS CLI comandos `aws s3api copy-object` `aws s3api upload-part` e. Eles APIs não são usados para a replicação do Amazon S3, mas são usados pelos `aws s3 sync` comandos AWS CLI `aws s3 cp` e quando a origem e o destino são buckets do S3. Eles também são suportados por `TransferManager` implementações em vários AWS SDKs.

AWS Lambda GetFunction

Diretor: AWS interno

Expiração padrão: 10 minutos

AWS Lambda armazena a versão do usuário em um bucket S3 de propriedade da equipe Lambda, antes de gerar os ativos implantados nos contêineres Lambda. Quando quiser acessar o código da sua função, você chama a GetFunctionAPI. Essa API responde com`Code.Location`, que contém um URL pré-assinado válido por 10 minutos (esse tempo de expiração é o comportamento atual e não um contrato publicado). Se você não quiser o código, você pode usar uma combinação de GetFunctionConfiguration, GetFunctionConcurrency, e ListTagspara recuperar os outros dados retornados por`GetFunction`.

O URL retornado não é assinado com as credenciais do usuário atualmente conectado, mas em nome do usuário pela Lambda. Por esse motivo, as chaves de condição (como`aws:SourceIP`) aplicadas ao usuário atualmente conectado ou às credenciais de sessão temporária do usuário não se aplicam ao URL gerado. Isso vale se as chaves de condição forem aplicadas GetFunctionsomente ou aplicadas a todo o uso da API da AWS para o usuário ou a sessão.

O console Lambda também usa GetFunctiono URL pré-assinado que ele retorna. O console usa as credenciais temporárias associadas ao usuário atualmente conectado para ligar. GetFunction Detalhes sobre a obtenção dessas credenciais temporárias estão fora do escopo deste documento.

Amazon ECR

Diretor: AWS interno

Expiração padrão: 1 hora

O Amazon Elastic Container Registry (Amazon ECR) fornece GetDownloadUrlForLayera API, que retorna uma URL pré-assinada que é válida por uma hora e suporta o download de uma única camada de uma imagem do Amazon ECR. No entanto, essa operação é usada pelo proxy Amazon ECR e geralmente não é usada pelos usuários para extrair e enviar imagens.

Amazon Redshift Spectrum

Principal: Função passada para CREATE EXTERNAL SCHEMA por meio de `IAM_ROLE`

Expiração padrão: 1 hora

O Amazon Redshift Spectrum usa URLs presigned internamente e proíbe restrições na combinação do bucket e da função do Amazon Redshift que limitariam o pré-assinado. URLs Você pode usar um `s3:signatureAge` valor de 16 minutos, mas valores muito baixos não são confiáveis. O valor mínimo que você pode usar depende do tempo e do tamanho da sua consulta. Embora um valor inferior a 16 minutos funcione para muitos cenários, ele exige testes. A função pode e deve ser restrita para ser usada somente pelo Redshift Spectrum, que não divulga o que URLs ela gera, mitigando assim a justificativa típica para valores de expiração mais baixos.

Estúdio Amazon SageMaker AI

O Amazon SageMaker AI Studio oferece suporte a duas ações de API: CreatePresignedDomainUrlCreatePresignedNotebookInstanceUrle. No entanto, eles APIs não estão relacionados ao recurso de URL pré-assinado do Signature Version 4. Eles APIs criam uma URL que usa um `authToken` parâmetro, mas não oferecem suporte a nenhum dos parâmetros de consulta padrão do Signature Version 4.

`authToken`é um mecanismo diferente, mas tem semelhanças com o URLs preassinado. Ele é enviado como um parâmetro de sequência de caracteres de consulta e suporta um tempo de expiração de 5 minutos.

SageMaker A IA suporta restrições de rede. Se você colocar uma restrição na `sagemaker:CreatePresignedDomainUrl` ação, essa ação se aplicará tanto à chamada CreatePresignedDomainUrlquanto ao uso da URL gerada. Se uma URL for gerada a partir de uma rede válida e depois enviada por uma rede inválida, a chamada de API para gerar a URL será bem-sucedida, mas a solicitação que envia a URL falhará. O mesmo se aplica CreatePresignedNotebookInstanceUrlà `sagemaker:CreatePresignedNotebookInstanceUrl` ação.

Para obter mais informações, consulte a documentação da SageMaker IA.

Apêndice B: Como os controles para presignados afetam URLs Serviços da AWS

Este apêndice descreve as interações entre Serviços da AWS esse uso preassinado URLs, conforme descrito no Apêndice A, e os controles descritos anteriormente neste guia.

Guardrail para S3: SignatureAge

O console do Amazon S3 não é interrompido pela expiração máxima de 5 minutos definida pela chave de condição. `s3:signatureAge` O console Amazon S3 gera pré-assinados URLs quando você escolhe o botão Download e aplica seu próprio prazo de expiração de 5 minutos. Uma duração máxima menor que 2 minutos pode criar falhas aleatórias com base na sincronização do relógio e nas latências.

O Amazon S3 Object Lambda usa um tempo de expiração de 61 segundos, portanto, definir condições em um `s3:signatureAge` valor de 61 segundos ou mais não causará nenhuma interrupção. Durações mais curtas podem ser menos confiáveis e causar falhas intermitentes.

A região cruzada do Amazon S3 CopyObjectnão é interrompida por uma expiração máxima de 5 minutos. No entanto, durações mais curtas podem criar falhas aleatórias com base na sincronização do relógio e nas latências.

Em AWS Lambda, GetFunctionfornece uma URL para objetos fora da conta do cliente, para que as políticas do cliente não afetem o gerado URLs.

O Amazon Redshift Spectrum foi testado com `s3:signatureAge` uma condição de 16 minutos. No entanto, durações mais curtas podem causar interrupções.

Guardrail para s3:AuthType quando não estiver usando restrições de rede

O console do Amazon S3 geralmente é afetado pela grade de proteção. `s3:authType` O console é roteado para o Amazon S3 com base na configuração da rede local. Se a rede local for roteada para o Amazon S3 de uma forma que a restrição de rede permita, o console do Amazon S3 ainda funcionará. No entanto, se for roteado por meio de um proxy ou da Internet pública de uma forma

não permitida, o uso será bloqueado. No entanto, bloquear o uso é provavelmente a intenção dessa política.

O Amazon S3 Object Lambda é afetado se a função Lambda não estiver conectada a uma VPC apropriada. Nessa configuração, a VPC deve ter um gateway NAT, não para acessar o bucket do S3, mas para fazer chamadas. WriteGetObjectResponse

A região cruzada do Amazon S3 CopyObjecté interrompida se essa grade de proteção for aplicada a uma política de bucket sem a exceção recomendada de quando for verdadeira. **`aws:viaAWSService`**

O Amazon Redshift Spectrum é afetado pelo guardrail, a menos que `s3:authType` o roteamento de VPC aprimorado seja usado. Atualmente, o Redshift Spectrum oferece suporte ao roteamento aprimorado de VPC somente com clusters sem servidor, não com clusters provisionados.

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Atualizações e esclarecimentos	Na seção Guardrails adicionais, incluiu informações RCPs e esclareceu as exceções.	8 de agosto de 2025
Publicação inicial	—	23 de julho de 2024

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.