Establecer barandas y monitorear los prefirmados URLs

AWS Guía prescriptiva

AWS Guía prescriptiva: Establecer barandas y monitorear los prefirmados URLs

Table of Contents

Establecer barandas y monitorear las URL prefirmadas

Ryan Baker, Amazon Web Services (AWS)

Julio de 2024 (historial del documento)

La seguridad es una preocupación fundamental para todas las empresas y un pilar clave del AWS Well-Architected Framework. Como ingeniero de seguridad, querrá implementar barreras administrativas que estén alineadas con los requisitos de control de la organización. En el AWS Well-Architected Framework, las barandas definen los límites que limitan la actividad.

Esta guía proporciona información básica y prácticas recomendadas para el uso de URL prefirmadas, que se utilizan con objetos de Amazon Simple Storage Service (Amazon S3). Las URL prefirmadas permiten a los usuarios o las aplicaciones que tienen acceso a credenciales válidas generar solicitudes que se firman previamente y se aceptan hasta un tiempo de caducidad definido. Un caso de uso habitual de las URL prefirmadas consiste en ampliar el acceso a objetos o recursos mediante el uso compartido de estas solicitudes. Las solicitudes prefirmadas compartidas las generan sistemas o usuarios que tienen los derechos para realizar una solicitud específica y, a continuación, pueden enviarse a otros sistemas o usuarios para ampliar la capacidad de realizar esa misma solicitud.

En esta guía, aprenderá lo siguiente:

- Los conceptos de las URL prefirmadas
- Casos de uso de direcciones URL prefirmadas
- Barandillas recomendadas y opcionales
- Opciones de monitoreo
- Ejemplos de cómo Servicios de AWS utilizar las URL prefirmadas

Destinatarios previstos

Esta guía se ha diseñado para arquitectos e ingenieros de seguridad responsables de implementar los controles de seguridad en la Nube de AWS.

Objetivos

Como ingeniero de seguridad, querrá saber cómo los creadores de soluciones implementan la seguridad y el tipo de acceso que tienen sus usuarios finales. Esta guía cubre un tipo de acceso, las URL prefirmadas, que se utilizan a menudo con Amazon S3. Las URL prefirmadas ofrecen a los creadores opciones para unir de manera eficiente los mecanismos de autenticación.

En Amazon S3, las URL prefirmadas representan una categoría única de solicitudes. Los ingenieros de seguridad pueden supervisar y gestionar estas solicitudes para garantizar que se utilicen únicamente cuando sea adecuado y necesario. El objetivo de esta guía es ayudar a los ingenieros de seguridad a proporcionar este tipo de supervisión de alto nivel.

Después de leer esta guía, debe comprender qué es una URL prefirmada, cuándo se usa normalmente y las motivaciones para su uso.

Requisitos previos

Si su empresa no ha definido una política de seguridad, objetivos de control o estándares, tal como se describe en la guía Implementación de controles de seguridad en AWS, le recomendamos que complete esas tareas de gobierno antes de continuar con esta guía.

Antes de empezar, también debe familiarizarse con las prácticas recomendadas y opcionales de control y supervisión. Para obtener más información, consulte:

- Políticas de control de servicios (AWS Organizations documentación)
- Políticas de bucket para Amazon S3 (documentación de Amazon S3)
- Registro de solicitudes con registro de acceso al servidor (documentación de Amazon S3)
- Registro de llamadas a la API de Amazon S3 mediante AWS CloudTrail (documentación de Amazon S3)

Descripción general de las URL prefirmadas

Una URL prefirmada es un tipo de solicitud HTTP que reconoce el servicio AWS Identity and Access Management (IAM). Lo que diferencia a este tipo de solicitud de todas las demás es el parámetro de consulta AWS X-Amz-Expires. Al igual que con otras solicitudes autenticadas, las solicitudes de URL prefirmadas incluyen una firma. En el caso de las solicitudes de URL prefirmadas, esta firma se transmite en. `X-Amz-Signature` La firma utiliza las operaciones criptográficas de la versión 4 de Signature para codificar todos los demás parámetros de la solicitud.

> **Notas**
>
> - La versión 2 de Signature se encuentra actualmente en proceso de quedar obsoleta, pero algunas todavía la admiten. Regiones de AWS Esta guía se aplica a la firma de la versión 4 de Signature.
> - El servicio de recepción podría procesar encabezados sin firmar, pero el soporte para esa opción es limitado y específico, de acuerdo con las mejores prácticas. A menos que se indique lo contrario, suponga que todos los encabezados deben estar firmados para que se acepte una solicitud.

El `X-Amz-Expires` parámetro permite procesar una firma como válida con una desviación mayor de la fecha y hora codificada. Aún se están evaluando otros aspectos de la validez de la firma. Las credenciales de firma, si son temporales, no deben caducar en el momento en que se procese la firma. Las credenciales de firma deben adjuntarse a un director de IAM que cuente con la autorización suficiente en el momento del procesamiento.

Las URL prefirmadas son un subconjunto de solicitudes prefirmadas

Una URL prefirmada no es el único método para firmar una solicitud en el futuro. Amazon S3 también admite solicitudes POST, que también suelen estar prefirmadas. Una firma POST prefirmada permite realizar cargas que cumplan con una política firmada y que tenga una fecha de caducidad incluida en dicha política.

Las firmas de las solicitudes pueden estar fechadas en el futuro, aunque esto es poco común. Mientras las credenciales subyacentes sean válidas, el algoritmo de firma no prohíbe las citas futuras. sin embargo, estas solicitudes no se pueden procesar correctamente hasta su período de

tiempo válido, lo que hace que las citas futuras no sean prácticas para la mayoría de los casos de uso.

¿Qué permite una solicitud prefirmada?

Una solicitud prefirmada solo puede permitir acciones que estén permitidas por las credenciales que se usaron para firmar la solicitud. Si las credenciales deniegan implícita o explícitamente la acción especificada en la solicitud prefirmada, la solicitud prefirmada se deniega cuando se envía. Esto se aplica a lo siguiente:

- Políticas de sesión asociadas a las credenciales
- Políticas asociadas al principal que está asociado a las credenciales
- Políticas de recursos que afectan a la sesión o al director
- Políticas de control de servicios que afectan a la sesión o al principal

Motivaciones para usar solicitudes prefirmadas

Como ingeniero de seguridad, debe saber qué motiva a los creadores de soluciones a utilizar direcciones URL prefirmadas. Entender lo que es necesario y lo que es opcional le ayudará a comunicarse con los creadores de soluciones. Las motivaciones pueden incluir las siguientes:

- Respaldar un mecanismo de autenticación que no sea de IAM y, al mismo tiempo, beneficiarse de la escalabilidad de Amazon S3. Una de las principales motivaciones es comunicarse directamente con Amazon S3 para aprovechar la escalabilidad integrada que ofrece este servicio. Sin esta comunicación directa, una solución tendría que soportar la carga que supone la retransmisión de los bytes que se envían PutObjecty GetObjectlas llamadas. En función de la carga total, este requisito añade desafíos de escalado que un creador de soluciones podría querer evitar.

  Es posible que otros medios de comunicación directa con Amazon S3, como el uso de credenciales temporales en AWS Security Token Service (AWS STS) o firmas de la versión 4 de Signature fuera de las URL, no sean adecuados para su caso de uso. Amazon S3 identifica a los usuarios mediante AWS credenciales, mientras que las solicitudes prefirmadas suponen la identificación mediante mecanismos distintos AWS de las credenciales. Se puede salvar esta diferencia y, al mismo tiempo, mantener la comunicación directa de los datos mediante solicitudes prefirmadas.
- Aprovechar la comprensión nativa de un navegador sobre las URL. Los navegadores entienden las URL, mientras que AWS STS las credenciales y las firmas de la versión 4 de Signature no. Esto

resulta beneficioso cuando se integra con soluciones basadas en navegadores. Las soluciones alternativas requieren más código, utilizan más memoria para archivos de gran tamaño y pueden recibir un tratamiento diferente con extensiones como los escáneres de malware y virus.

Comparación con credenciales temporales AWS STS

Las credenciales temporales son similares a las solicitudes prefirmadas. Ambos caducan, permiten establecer el alcance del acceso y se suelen utilizar para vincular las credenciales que no son de IAM con el uso que requiere credenciales de AWS.

Puede limitar estrictamente una AWS STS credencial temporal a un único objeto y acción de S3, pero esto puede provocar problemas de escalado, ya AWS STS que las API tienen límites. (Para obtener más información, consulte el artículo Cómo resolver la limitación de API o los errores de «tasa excedida» para IAM y en AWS STS el sitio web de AWS Re:post). Además, cada credencial generada requiere una llamada a la AWS STS API, lo que añade latencia y crea una nueva dependencia que podría afectar a la resiliencia. Una AWS STS credencial temporal también tiene un tiempo de caducidad mínimo de 15 minutos, mientras que una solicitud prefirmada puede admitir duraciones más cortas (60 segundos es práctico si se dan las condiciones adecuadas).

Comparación con soluciones que solo utilizan firmas

El único componente intrínsecamente secreto de una solicitud prefirmada es su firma de la versión 4 de firma. Si un cliente conoce los demás detalles de una solicitud y se le proporciona una firma válida que coincide con esos detalles, puede enviar una solicitud válida. Sin una firma válida, no puede hacerlo.

Las direcciones URL prefirmadas y las soluciones de solo firma son criptográficamente similares. Sin embargo, las soluciones que solo utilizan firmas tienen ventajas prácticas, como la posibilidad de utilizar un encabezado HTTP en lugar de un parámetro de cadena de consulta para transmitir la firma (consulte la sección sobre el registro de interacciones y mitigaciones). Los administradores también deben tener en cuenta que las cadenas de consulta se tratan más comúnmente como metadatos, mientras que los encabezados se tratan con menos frecuencia como tales.

Por otro lado, AWS los SDK ofrecen menos soporte para generar y usar firmas directamente. La creación de una solución que solo utilice firmas requiere más código personalizado. Desde una perspectiva práctica, el uso de bibliotecas en lugar de código personalizado por motivos de seguridad es una buena práctica general, por lo que el código para las soluciones que solo utilizan firmas requiere un análisis más exhaustivo.

Las soluciones que solo utilizan firmas no utilizan la cadena de `X-Amz-Expires` consulta ni proporcionan ningún período de validez explícito. IAM gestiona los períodos de validez implícita de las firmas que no tienen una fecha de caducidad explícita. Esos períodos implícitos no se publican. No suelen cambiar, pero se administran teniendo en cuenta la seguridad, por lo que no debes depender de los períodos de validez. Existe un equilibrio entre tener un control explícito sobre la fecha de caducidad y dejar que IAM gestione la caducidad.

Como administrador, es posible que prefiera una solución que solo utilice firmas. Sin embargo, en un sentido práctico, necesitará respaldar las soluciones tal como están diseñadas.

Identificación de solicitudes prefirmadas

Identificar las solicitudes que utilizaban una URL prefirmada

Amazon S3 proporciona dos mecanismos integrados para supervisar el uso a nivel de solicitud: los registros de acceso al servidor Amazon S3 y AWS CloudTrail los eventos de datos. Ambos mecanismos pueden identificar el uso de URL prefirmadas.

Para filtrar los registros en función del uso de URL prefirmadas, puede utilizar el tipo de autenticación. Para los registros de acceso al servidor, examine el campo Tipo de autenticación, que normalmente se denomina authtype cuando se define en una tabla de Amazon Athena. Para CloudTrail, examine AuthenticationMethoden el `additionalEventData` campo. En ambos casos, el valor del campo para las solicitudes que utilizan direcciones URL prefirmadas es`QueryString`, mientras que `AuthHeader` es el valor para la mayoría de las demás solicitudes.

`QueryString`el uso no siempre está asociado a las URL prefirmadas. Para restringir la búsqueda únicamente al uso de URL prefirmadas, busca las solicitudes que contengan el parámetro de cadena de consulta. `X-Amz-Expires` Para los registros de acceso al servidor, examina el URI de la solicitud y busca las solicitudes que tengan un `X-Amz-Expires` parámetro en la cadena de consulta. Para CloudTrail, examine el `requestParameters` elemento en busca de un `X-Amz-Expires` elemento.

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

La siguiente consulta de Athena aplica este filtro:

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

Para AWS CloudTrail Lake, la siguiente consulta aplica este filtro:

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

Identificar otros tipos de solicitudes prefirmadas

La solicitud POST también tiene un tipo de autenticación únicoHtmlForm, en los registros de acceso al servidor Amazon S3 y CloudTrail. Este tipo de autenticación es menos común, por lo que es posible que no encuentre estas solicitudes en su entorno.

La siguiente consulta de Athena aplica el filtro para: HtmlForm

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

En el caso de CloudTrail Lake, la siguiente consulta aplica el filtro:

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

Identificar los patrones de solicitud

Puede encontrar las solicitudes prefirmadas mediante las técnicas descritas en la sección anterior. Sin embargo, para que esos datos sean útiles, querrás buscar patrones. TOP 10Los resultados simples de la consulta pueden proporcionarte una idea, pero si eso no es suficiente, usa las opciones de agrupación de la siguiente tabla.

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
Agente usuario	GROUP BY useragent	GROUP BY userAgent	Esta opción de agrupación le ayuda a encontrar el origen y el propósito de las solicitudes. El agente de usuario lo proporciona el usuario y no es fiable como mecanismo de autenticación o autorización. Sin

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
			embargo, puede revelar muchas cosas si se buscan patrones, ya que la mayoría de los clientes utilizan una cadena única que es, al menos parcialmente, legible por humanos.
Solicitante	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	Esta opción de agrupación ayuda a encontrar a los directores de IAM que firmaron las solicitudes. Si su objetivo es bloquear estas solicitudes o crear una excepción para las solicitudes existentes, estas consultas proporcionan suficiente información para ello. Si utilizas los roles de acuerdo con las mejores prácticas de IAM, el rol tiene un propietario claramente identificado y puedes usar esa información para obtener más información.

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
Dirección IP de origen	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	Esta opción se agrupa por el último salto de traducción de red antes de llegar a Amazon S3. • Si el tráfico pasa por una puerta de enlace NAT, esta será la dirección de la puerta de enlace NAT. • Si el tráfico pasa por una puerta de enlace de Internet, será la dirección IP pública que envió el tráfico a la puerta de enlace de Internet. • Si el tráfico se origina desde fuera AWS, será la dirección pública de Internet asociada al origen. • Si pasa por un punto final de nube privada virtual (VPC) de puerta

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
			de enlace, será la dirección IP de la instancia en la VPC. • Si pasa a través de una interfaz virtual pública (VIF), será la IP local del solicitante o de cualquier intermediario, como un servidor proxy o un firewall, que solo exponga su dirección IP. • Si pasa a través de un punto final de la VPC de la interfaz, podría ser la dirección IP de una instancia de la VPC. También puede ser una dirección IP de otra VPC o de una red local. Al igual que ocurre con los VIF públicos, puede ser la dirección IP de cualquier intermediario.

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
			Estos datos son útiles si su objetivo es imponer controles de red. Puede que tengas que combinar esta opción con datos como `endpoint` (para los registros de acceso al servidor) o `vpcEndpointId` (para CloudTrail Lake) para aclarar la fuente, ya que diferentes redes pueden duplicar las direcciones IP privadas.
Nombre del bucket de S3	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	Esta opción de agrupación ayuda a encontrar los depósitos que recibieron solicitudes. Esto le ayuda a identificar la necesidad de excepciones.

Mejores prácticas para usar solicitudes prefirmadas

En esta sección se describen las mejores prácticas para el uso de solicitudes prefirmadas que un ingeniero de seguridad debería tener en cuenta. Las directrices incluyen:

- Las mejores prácticas fundamentales, que son prácticas que toda organización debe seguir.
- Restricciones adicionales, prácticas que debería tener en cuenta, pero que podría decidir implementar parcialmente o con excepciones. Su objetivo es proporcionar un control y una defensa adicionales en profundidad, pero deben equilibrarse teniendo en cuenta la complejidad general.
- Registra las interacciones, que pueden ser el resultado de dispositivos o servicios que son parte de tu responsabilidad o la de tu cliente en el modelo de responsabilidad compartida. Esta sección incluye precauciones para limitar la información a la que se puede acceder a través de los registros.

Mejores prácticas fundamentales

Las mejores prácticas generales que son controles efectivos para otras solicitudes de AWS API también se aplican a las solicitudes prefirmadas. En esta sección, se analizan dos de las prácticas más relevantes: los privilegios mínimos y los perímetros de datos. Estas prácticas crean una profundidad de controles que otras prácticas amplían.

Aplique el principio del mínimo privilegio

El primer paso para limitar el uso de solicitudes prefirmadas es limitar el acceso a Amazon S3 en general. Una URL prefirmada no puede proporcionar acceso a recursos que no se hayan otorgado a la entidad principal que generó la firma de la URL prefirmada. Tampoco puede proporcionar acceso a un recurso de una manera que no se haya otorgado a ese director. Por lo tanto, aplicar las mejores prácticas para conceder a esos directores el menor privilegio es una barrera eficaz.

El proceso de creación de una URL prefirmada es una operación algorítmica que se basa en un estándar publicado (Signature versión 4) para la generación de firmas. Por lo tanto, no es posible poner límites a la generación de prefirmados. URLs Sin embargo, para que sea relevante, una URL prefirmada debe ser válida y proporcionar acceso a los recursos, por lo que la validez de una URL prefirmada también es una barrera eficaz.

Para obtener más información sobre los privilegios mínimos, consulte Otorgar acceso con privilegios mínimos en el pilar Seguridad del AWS Well-Architected Framework.

Implemente un perímetro de datos

Una extensión de privilegios mínimos es mantener un perímetro de datos que sea coherente con las necesidades de su organización. Los prefirmados URLs son compatibles con los perímetros de datos. Al igual que con otras solicitudes, la validez de una solicitud de URL prefirmada se evalúa en el momento de la solicitud. Si las propiedades de la red, el recurso, la sesión de rol y el principal cambian, se evalúan en el momento y mediante el método con el que se recibe la solicitud.

Por ejemplo, supongamos que un servicio que se ejecuta en un contenedor de Amazon Elastic Kubernetes Service (Amazon EKS) firma una solicitud. La solicitud se envía posteriormente desde el sistema informático personal del usuario que está conectado a Internet. En este caso, la SourceIp condición aws: evalúa la dirección IP pública visible de la solicitud del sistema personal del usuario, no la dirección IP del servicio en el contenedor EKS de Amazon.

Del mismo modo, si las etiquetas del principal o recurso cambian antes de que se envíe la solicitud, los valores actualizados, no los originales, se aplicarán a la solicitud mediante las condiciones aws: PrincipalTag /tag-key y aws: /tag-key. ResourceTag

Barandillas adicionales

Cuando los creadores de soluciones y los usuarios utilizan adecuadamente las solicitudes prefirmadas, proporcionan un mecanismo seguro para que los usuarios accedan a los datos. Además, la capacidad de generar solicitudes prefirmadas no proporciona a los directores un acceso que aún no tenían.

En ese contexto, ¿son necesarios controles adicionales? La justificación de los controles adicionales no se basa en la necesidad de denegar el acceso, sino en ofrecer la posibilidad de supervisar, aprobar el uso y establecer límites, además de reducir el riesgo de que los usuarios cometan errores. De esta forma, puede ayudar a garantizar que el uso sea adecuado y necesario.

Las siguientes barandillas le ayudan a lograr este objetivo. Antes de activar estos controles, es posible que desee determinar el uso actual identificando las solicitudes prefirmadas. Esta identificación le ayuda a prepararse para el impacto de la barandilla en el uso actual o a planificar excepciones cuando sea necesario.

Barandilla para S3: Signature Age

Una característica que define a las solicitudes prefirmadas es que describen un tiempo de caducidad. La firma de la solicitud contiene una fecha. Esta fecha se transmite como parámetro de cadena de

`X-Amz-Date` consulta para un POST prefirmado URLs y como fecha o x-amz-date encabezado para un POST prefirmado.

Amazon S3 proporciona una clave de condición, s3:SignatureAge, que puede utilizar para limitar el tiempo máximo entre la fecha de firma y el vencimiento efectivo de la solicitud. Esta condición nunca puede aumentar el período de validez, pero sí puede reducirlo.

En la siguiente política, la clave de `s3:signatureAge` condición limita las solicitudes prefirmadas a 15 minutos de validez. Todos los ejemplos siguientes utilizan 15 minutos para limitar la validez a un período de tiempo similar al que admite la firma estándar.

La segunda declaración de la política deniega cualquier acceso a la versión 2 de Signature. Esta versión del protocolo de firma está en desuso, pero algunas Regiones de AWS aún la admiten. Le recomendamos que la bloquee de forma explícita antes de que quede totalmente obsoleta.

Puede aplicar la siguiente política como política de control de AWS Organizations servicios (SCP). Los usuarios pueden seguir utilizando solicitudes prefirmadas e implementar soluciones que dependan de esas solicitudes, siempre que el tiempo entre la generación de la firma y el uso sea inferior a 15 minutos. Según la implementación, es posible que esta limitación no tenga ningún impacto, que la solución quede inutilizable o que se produzcan errores ocasionales que se puedan volver a intentar.

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

Excepciones

Si una solución requiere más tiempo antes de caducar y, por lo tanto, se ve afectada por la política anterior, le recomendamos que proporcione un método para aprobar las excepciones. Para evitar enumerar las excepciones en un SCP, utilice aws: PrincipalTag, como en la siguiente política, para gestionar las excepciones de forma escalable. Otros AWS ejemplos, como los ejemplos de políticas perimetrales de datos de AWS, utilizan esta estrategia.

Si implementa una política de excepciones mediante el usoaws:PrincipalTag, debe controlar el acceso a las etiquetas de configuración en las entidades principales. Las etiquetas de este tipo pueden provenir directamente de los directores y pueden ser controladas por un SCP, como en este ejemplo de control de los valores de las etiquetas que se pueden establecer. Una etiqueta de este tipo también puede provenir de etiquetas de sesión, que establece un proveedor de identidad (IdP) o cuando se utilizan. AWS STS Controlar el acceso a `aws:PrincipalTag` es un tema complejo. Sin embargo, una organización que tenga experiencia en el uso del control de acceso basado en atributos (ABAC) tendrá la experiencia y los controles necesarios para permitir el uso adecuado en este caso de `aws:PrincipalTag` uso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
--- Example exception ---
        "StringNotEquals": {
```

```
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
--- Example exception end ---
      }
    }
  ]
}
```

Políticas de buckets

Puede aplicar políticas de bucket a todos los buckets o a algunos de ellos mediante una política como la que se muestra en el siguiente ejemplo. A diferencia de una SCP, una política de bucket también se centra en el uso principal del servicio. El apéndice A no documenta ningún uso principal esperado de las solicitudes prefirmadas, pero si quisieras implementar un control para demostrar ese límite, la siguiente política proporcionaría ese control. Además, a diferencia de un SCP, se puede aplicar una política de grupos a los principales de tu cuenta de administración. Las excepciones basadas en ABAC funcionan en las políticas de bucket de la misma manera que en un SCP.

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

Guardrail para S3: AuthType

Los prefirmados URLs utilizan la autenticación de cadenas de consulta y los prefirmados siempre utilizan la autenticación POST. POSTs Amazon S3 admite la denegación de solicitudes en función del tipo de autenticación mediante la clave de condición s3:AuthType. `REST-QUERY-STRING`es el `s3:authType` valor de las cadenas de consulta y `POST` es el `s3:authType` valor de POST.

Puede aplicar la siguiente política como SCP. La política se utiliza `s3:authType` para permitir únicamente la autenticación basada en encabezados. También configura un método para proporcionar excepciones a usuarios o roles individuales.

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

La denegación de solicitudes en función del tipo de autenticación afecta a cualquier solución o función que utilice el tipo de autenticación denegada. Por ejemplo, la denegación `REST-QUERY-STRING` impide que los usuarios realicen cargas o descargas desde la consola Amazon S3. Si desea que los usuarios utilicen la consola Amazon S3, no utilice esta barandilla o haga una excepción para los usuarios. Por otro lado, si no desea que los usuarios usen la consola Amazon S3, puede denegársela a `REST-QUERY-STRING` los usuarios.

Quizás ya deniegue a los usuarios el acceso directo a los recursos de Amazon S3. En este caso, una barrera para el tipo de autenticación es redundante. Sin embargo, una sentencia de `s3:authType` denegación es defense-in-depth útil porque las implementaciones para denegar el acceso directo suelen incluir muchas sentencias de control, algunas con excepciones.

Los roles que se utilizan para las cargas de trabajo no suelen necesitar acceso a la cadena de consulta ni POST a la autenticación. Las excepciones son las funciones que respaldan los servicios diseñados para usar solicitudes prefirmadas. Puede crear excepciones específicas para esas funciones.

También puedes aplicar una política de grupos a todos los grupos o a algunos de ellos mediante una política como la siguiente:

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

Esta política de depósitos tiene el efecto de denegar el uso de los depósitos CopyObjecty de UploadPartCopy APIs realizar copias entre regiones. La replicación de Amazon S3 no se ve afectada porque no depende de ellos APIs.

Si desea utilizar una política de bucket como la política anterior y seguir siendo compatible con la UploadPartCopyAPI CopyObjecto entre regiones, añada una condición `aws:ViaAWSService` similar a la siguiente:

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

Combinación de barandas prefirmadas y excepciones a otras barandillas

Si no tiene previsto aplicar una barrera de protección en general a sus usuarios y funciones, puede que le interese aplicarla a las excepciones de otras barreras de protección comunes, de forma que esas excepciones no admitan las solicitudes prefirmadas.

Si tienes restricciones de red, pero permites excepciones para socios externos o para casos de uso especiales, debes bloquear la cadena de consulta o la `POST` autenticación cuando se apliquen esas excepciones, a menos que se identifique específicamente que son obligatorias.

Limitaciones de S3: SignatureAge

A los administradores les resultará útil comprender sus implicaciones con mayor detalle. `s3:signatureAge` Cada solicitud firmada incluye`X-Amz-Date`, en la que se debe indicar, la hora actual. Este valor lo rellenan el cliente y el firmante de la solicitud. AWS rechaza las solicitudes que considera que tienen tiempos no válidos. Sin embargo, un firmante podría generar firmas por adelantado en future time. Amazon S3 rechaza las solicitudes que especifiquen una hora futura si se envían con demasiada antelación. Sin embargo, si la solicitud no se envía hasta el momento en que se inicia sesión en la firma, la firma podría generarse antes y enviarse más tarde.

`s3:signatureAge`limita la antigüedad máxima de `X-Amz-Date` una firma solo para las solicitudes prefirmadas. Se rechazan las solicitudes con una antigüedad superior a la especificada, incluso si han caducado `X-Amz-Expires` o si una `POST` política las hubiera declarado válidas. `s3:signatureAge`no cambia el período de validez de las solicitudes que no incluyen un vencimiento explícito. Tampoco controla el valor `X-Amz-Date` que un cliente utiliza como firma.

Si el reloj del sistema es incorrecto o si un cliente solicita intencionalmente fechas futuras, es posible que la hora firmada no sea la hora en que se generó la firma. Esto limita en qué medida `s3:signatureAge` pueden controlar las soluciones. Una solución que utiliza la hora actual para generar firmas está limitada de la forma esperada: las firmas siguen siendo válidas durante el número de milisegundos especificado en`s3:signatureAge`. Una solución que no utilice la hora actual tendrá límites diferentes. Una restricción es que las credenciales que se usaron para firmar la firma deben seguir siendo válidas. Como administrador, puede controlar la validez máxima de las credenciales temporales emitidas. Puede permitir que las credenciales sean válidas durante un máximo de 36 horas o restringir la validez a un mínimo de 15 minutos. La caducidad de las credenciales temporales no depende del valor de`X-Amz-Date`.

Las credenciales permanentes no tienen esta restricción. Usar solo credenciales temporales es una práctica recomendada, y puedes revocar de forma explícita cualquier credencial permanente, lo que también invalidaría cualquier firma basada en esa credencial.

Aunque `s3:signatureAge` se mide en milisegundos, no es práctico configurarlo en menos de 60 segundos, incluso si el reloj está bien sincronizado y el uso de la latencia es bajo. Los ajustes inferiores a 60 segundos conllevan el riesgo de que se rechacen las solicitudes válidas. Si prevé demoras entre la generación de la firma y el envío de la solicitud, o si hay problemas con la sincronización del reloj, debe tener en cuenta estos problemas en la gestión de los `s3:signatureAge` mismos.

Dirigirse a los grupos a gran escala

SCPs se puede utilizar `aws:PrincipalTag` para hacer excepciones para los usuarios. No puedes usar etiquetas en un depósito para controlar el acceso`aws:ResourceTag`; solo se usan etiquetas de objetos para el control de acceso. Por lo general, no es escalable añadir una etiqueta a cada objeto al que quieras aplicar este control.

Una solución que se adapta a muchos casos de uso es aplicar la política y la excepción a nivel de cuenta, ya sea cambiando las cuentas a las que se aplica el SCP o utilizando aws: ResourceAccount, aws: ResourceOrgPaths o aws: ResourceOrg ID. Por ejemplo, un SCP podría aplicarse a un conjunto de cuentas de producción.

Otra solución consiste en utilizar una AWS Config regla personalizada para implementar un control detectivesco o un control responsivo. El objetivo sería que cada grupo contuviera una política de grupo con la barrera de protección adecuada. Además de probar el contenido de una política de bucket, la AWS Config regla personalizada puede recuperar las etiquetas del bucket y excluirlo de

la regla si el bucket está etiquetado con un valor específico. Si esa regla no supera la comprobación de conformidad, podría marcar el depósito como no conforme o solicitar una solución para añadir el elemento de protección a la política del depósito.

> **Note**
>
> No puedes restringir el contenido de las etiquetas de las solicitudes a. PutBucketTagging Para mantener el control sobre cómo se etiqueta un depósito, debes limitar el acceso a `PutBucketTagging` y DeleteBucketTagging.

Registrar las interacciones y las mitigaciones

Una URL prefirmada contiene una firma y se puede usar, durante el período anterior a la caducidad, para realizar la operación de API específica para la que se firmó. Debe tratarse como una credencial de acceso temporal. La firma debe permanecer privada solo para las partes que necesiten conocerla. En la mayoría de los entornos, este es el cliente que envía la solicitud y el servidor que la recibe. El envío de la firma como parte de una sesión HTTPS directa mantiene su naturaleza privada, ya que solo un participante de la sesión HTTPS puede ver el URI que transmite la firma.

En el caso de los prefirmados URLs, la firma se transmite como parámetro de cadena de `X-Amz-Signature` consulta. Los parámetros de la cadena de consulta son un componente de un URI. El riesgo es que los clientes registren el URI y la firma con él. Los clientes tienen acceso a toda la solicitud HTTP y pueden registrar cualquier parte de la solicitud, los datos y los encabezados (incluidos los encabezados de autenticación). Sin embargo, por convención, esto es menos común. El registro de URI es más común y obligatorio en casos como el registro de acceso. Los clientes deben utilizar la redacción o el enmascaramiento para eliminar la firma antes de iniciar sesión. URIs

En algunos entornos, los usuarios permiten que los intermediarios (proxies) obtengan visibilidad en sus sesiones HTTPS. La activación de los proxies requiere un alto nivel de acceso privilegiado a los sistemas cliente, ya que requieren configuración y certificados de confianza. La instalación de una configuración de proxy y de certificados de confianza, dentro del contexto local del entorno intermediario del cliente, permite un nivel de privilegios muy alto. Por esta razón, el acceso a dichos intermediarios debe estar estrictamente controlado.

El propósito de un intermediario suele ser bloquear las salidas no deseadas y rastrear otras salidas. Por ello, es habitual que estos intermediarios registren las solicitudes. Si bien los intermediarios podrían, como los clientes, registrar cualquier contenido, encabezados y datos (todos los cuales

serían muy confidenciales), es más común que registren URIs, como los que incluyen el parámetro de cadena de `X-Amz-Signature` consulta.

Mitigaciones

Se recomienda que al registrar el URI se redacte el parámetro de la cadena de `X-Amz-Signature` consulta, se redacte toda la cadena de consulta o se trate la información de forma altamente confidencial, como ocurre con el acceso directo al servidor intermediario. Si bien estas protecciones son muy recomendables, el hecho de que la fecha de URLs caducidad prefirmada mitiga los riesgos de exposición de los registros, siempre y cuando la exposición se retrase lo suficiente como para que las firmas caduquen.

Amazon S3 también ve las firmas y debe gestionarlas de forma adecuada. Los registros de acceso al servidor Amazon S3 incluyen el URI de la solicitud`X-Amz-Signature`, pero lo redactan como se recomienda. Lo mismo ocurre cuando se registran eventos de CloudTrail datos para Amazon S3. Puedes configurar Amazon CloudWatch Logs para que oculte los datos mediante identificadores de datos personalizados.

La siguiente expresión regular coincide con la `X-Amz-Signature` forma en que aparece en un URI:

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

La siguiente expresión regular agrega patrones de agrupamiento para identificar el texto que se va a reemplazar de manera más específica:

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

Si tiene una entrada en el registro de acceso como la siguiente:

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

La primera expresión regular traduce la entrada del registro de acceso a:

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

La segunda expresión regular, en los sistemas que admiten grupos que no capturan, traduce la entrada del registro de acceso a:

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Preguntas frecuentes

¿Se puede utilizar una solicitud prefirmada varias veces? ¿Es un riesgo para la seguridad?

Sí, la firma de una solicitud prefirmada se puede usar más de una vez. Si se trata de un riesgo de seguridad es una cuestión contextual. Otros métodos de acceso a los servicios de AWS también permiten la repetición. Un usuario o una carga de trabajo con AWS credenciales pueden enviar muchas solicitudes Servicios de AWS, y cualquiera de ellas podría estar duplicada.

Si su caso de uso requiere una ejecución única y solo una vez, debe implementar otros mecanismos para imponer el uso único. El uso único no es una característica de las solicitudes prefirmadas. Como ingeniero de seguridad, debe revisar los casos de uso y las implementaciones, pero en muchos casos, el uso múltiple es adecuado para un uso aceptable.

¿Puede otra persona que no sea el usuario previsto utilizar una solicitud prefirmada?

Cualquier persona que esté en posesión de la misma puede enviar la firma de una solicitud prefirmada. Solo se aceptará si supera otras formas de validación, como los controles perimetrales de datos. Si la firma ha caducado, las credenciales de firma han caducado o las credenciales de firma no tienen acceso a los recursos solicitados, se denegará la solicitud.

Lo mismo ocurre con otros métodos de autenticación con Servicios de AWS. Las credenciales que se comparten de forma inapropiada permiten un acceso inapropiado. La mejor práctica básica es compartir las credenciales y firmas solo con el público al que van dirigidas. Si no puedes confiar en el público al que estás dirigido para proteger los datos privados y no compartirlos con otras personas, esto socavará cualquier forma de autenticación.

¿Puede un usuario autorizado utilizar una solicitud prefirmada para filtrar datos?

Proteger los datos requiere una acción sólida. Permitir el acceso para los fines previstos y, al mismo tiempo, mantener un perímetro de datos requiere un enfoque integral. El acceso con privilegios

mínimos, los controles del perímetro de los datos y el uso exclusivo de credenciales de acceso temporales son las mejores prácticas generales que se aplican a la protección de los datos. El uso adecuado de estos controles también limita la capacidad de los usuarios para realizar acciones a través de las solicitudes prefirmadas que generan.

Esto se debe a que el acceso que proporcionan las solicitudes prefirmadas es un subconjunto del acceso otorgado a las credenciales que se utilizan para firmar la solicitud. En este contexto, las mejores prácticas que se aplican al acceso a los datos generalmente se aplican a las solicitudes prefirmadas, pero las solicitudes prefirmadas no crean ningún acceso nuevo a los datos.

- La caducidad máxima se limita a la caducidad de las credenciales de firma. Si se revocan las credenciales de firma, las firmas basadas en las credenciales dejarán de ser válidas.
- Si los permisos de la entidad principal de IAM asociada a las credenciales de firma no incluyen la ejecución de la acción asociada a la solicitud prefirmada, al invocar una solicitud prefirmada se obtiene una respuesta de «acceso denegado». La respuesta depende del estado actual de los permisos en el momento de la invocación, que no tiene relación con el momento en que se generó la firma de la solicitud prefirmada.
- Las propiedades del principal se evalúan en función del principal asociado a las credenciales de firma.
- Las propiedades de una sesión de rol se evalúan en función de la sesión de rol asociada a las credenciales de firma.
- Las propiedades de la red se evalúan en función de cómo se recibió la solicitud, como ocurre con las solicitudes normales.

En este contexto, el examen de los riesgos asociados a las solicitudes prefirmadas se limita a las áreas en las que se firman con credenciales diferentes de las credenciales del usuario y proporcionan un acceso que no formaba parte del principal del usuario. Este examen debería aplicarse al diseño del servicio, la carga de trabajo o la solución que genera firmas en nombre del usuario, y no a la propia capacidad de solicitud prefirmada.

¿Puedo denegar el acceso desde una URL prefirmada si sospecho que se ha compartido de forma no autorizada?

Sí. Esto requiere invalidar las credenciales con las que se firmó la URL. Existen varias formas de lograrlo:

- Elimine los permisos del principal de IAM al que pertenecen las credenciales. Si ese principal de IAM ya no tiene acceso al recurso y la operación para los que está firmada la URL, la URL no podrá ejecutar esa operación. Esto afecta a todos los usos coincidentes de ese principal de IAM.
- Si las credenciales utilizadas para firmar la URL son temporales AWS STS , puede revocar los permisos de sesión para las credenciales temporales que se emitieron antes de una hora específica para el principal de IAM. Según el caso de uso, es posible que haya otras sesiones válidas que se invaliden antes de su fecha de caducidad normal, pero las sesiones nuevas no se verán afectadas. La revocación de los permisos de sesión también invalida cualquier URL que se haya firmado con las credenciales asociadas a esas sesiones, pero las nuevas URL asociadas a las nuevas sesiones no se verán afectadas.
- Si las credenciales utilizadas para firmar la URL son credenciales permanentes, desactive la clave de acceso. Esto afecta a todo el uso vinculado a esas credenciales.

Recursos

Documentación de Amazon S3

- Solicitudes de autenticación (AWS firma, versión 4)
- Autenticación de solicitudes: uso de parámetros de consulta (AWS firma, versión 4)
- Solicitudes de autenticación: cargas basadas en el navegador mediante POST (versión de firma 4)AWS
- Claves de política de autenticación específicas de Amazon S3 Signature versión 4
- Trabajar con direcciones URL prefirmadas

Otras referencias

- Creación de un perímetro de datos en AWS (AWS documento técnico)
- SEC03-BP02 Otorgue el acceso con privilegios mínimos (marco AWS bien diseñado, pilar de seguridad)
- SEC03-BP05 Defina las barreras de permisos para su organización (Well Architected Framework, pilar de seguridad)AWS

Apéndice A: Cómo Servicios de AWS usar prefirmado URLs

En este apéndice se proporciona información Servicios de AWS y funciones que utilizan URLs prefirmados. Esta información tiene dos propósitos:

- Proporcionar a los ingenieros de seguridad que implementan los controles información sobre los posibles impactos de esos controles.
- Para crear conciencia sobre las situaciones en las que este riesgo podría ser relevante para el URL registro de las interacciones.

> **Important**
>
> Este apéndice no proporciona una lista completa Servicios de AWS ni su uso de los prefirmadosURLs. Tampoco cubre las soluciones personalizadas o de terceros.

Consola de Amazon S3

Principal: usuario de consola

Caducidad predeterminada: 5 minutos

> **Exención de responsabilidad**
>
> En esta sección se documenta el comportamiento actual de la consola Amazon S3. AWS El comportamiento de la consola está sujeto a cambios sin previo aviso.

La consola Amazon S3 admite la descarga y carga de objetos. Las descargas utilizan un prefirmado URL que tiene un tiempo de caducidad de 300 segundos (5 minutos). URLSe genera mediante una solicitud a`https://<bucket-region>.console.aws.amazon.com/s3/batchOpsServlet-proxy`.

Esa solicitud se inicia cuando el usuario hace clic en un botón de descarga, por lo que URL no se genera con antelación ni se envía al cliente hasta que se produce la solicitud explícita de descarga.

Las subidas son similares, excepto que la consola envía dos solicitudes: `OPTIONS` como CORS control previo al vuelo, y. `PUT` Ambas solicitudes utilizan la misma firma.

Las credenciales utilizadas para firmar son credenciales temporales que están asociadas al usuario que ha iniciado sesión actualmente. Los detalles sobre el método para obtener esas credenciales temporales están fuera del ámbito de esta guía.

Amazon S3 Object Lambda

Principal: Persona que llama al punto de acceso

Caducidad predeterminada: 61 segundos

Amazon S3 Object Lambda utiliza AWS Lambda funciones para procesar y transformar automáticamente los datos a medida que se recuperan de Amazon S3. Cuando S3 Object Lambda invoca una función, la función recibe un prefirmado URL (`inputS3Url`) que puede utilizar para descargar el objeto original desde el punto de acceso compatible.

Estos prefirmados URLs están firmados para el punto de acceso Amazon S3 compatible, que se proporciona al configurar S3 Object Lambda. (No es lo mismo que el punto de acceso de Object Lambda). En lugar de utilizar un rol vinculado a la función Lambda, URL se firma con la identidad de la persona que llama originalmente y los permisos de ese usuario se aplicarán cuando se utilice. URL Si hay encabezados firmados enURL, la función Lambda debe incluir estos encabezados en la llamada a Amazon S3.

El prefirmado URL que se devuelve tiene un tiempo de caducidad de 61 segundos (un segundo más que la duración máxima de una función de Objeto Lambda de S3). El generado solo se URL puede usar con el punto de acceso compatible. La persona que llama al punto de acceso S3 Object Lambda debe tener acceso a este punto de acceso. Puede limitar ese acceso al contexto de S3 Object Lambda mediante la condición. `"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]` Cuando esa condición está asociada a un punto de acceso o depósito de soporte, el usuario no puede acceder directamente al punto de acceso o depósito de soporte.

El valor de este enfoque es que no es necesario conceder a la función Lambda acceso a su bucket o punto de acceso de S3. El rol que está asociado a la función Lambda necesitará permisos WriteGetObjectResponse, pero no los necesitará. GetObject

Cuando S3 Object Lambda genera un objeto prefirmadoURLs, no añade restricciones de red, por lo que se URL puede utilizar fuera de la función Lambda. Sin embargo, se seguirán aplicando las restricciones impuestas a la persona que llama a S3 Object Lambda. Por ejemplo, si la función Lambda se ejecuta en un punto final VPC y restringe a la persona que llama a usar un VPC punto

final, cualquier persona que posea el prefirmado necesitará poder enviarlo a través de URL ese punto final. VPC Esta restricción también se aplica a y. SourceIpVpcSourceIp

> **Note**
>
> Para utilizar una función Object Lambda de S3 en unVPC, VPC debe tener una ruta a los puntos finales públicos de S3 a los que llamar. WriteGetObjectResponse Esto no indica que los requisitos de uso de un VPC punto final no se apliquen a las solicitudes de recuperación de datos del depósito.

AWS Lambda Entre regiones CopyObject

Principal: internoAWS

Caducidad predeterminada: 3600 segundos

Cuando usa CopyObjecto UploadPartCopyAPIpara copiar de forma transversal Regiones de AWS, Amazon S3 usa prefirmados URLs internamente. Se APIs pueden llamar directamente desde SDKs o desde los AWS CLI comandos `aws s3api copy-object` y`aws s3api upload-part`. APIsNo se utilizan para la replicación de Amazon S3, pero los utilizan los `aws s3 sync` comandos AWS CLI `aws s3 cp` y cuando el origen y el destino son buckets de S3. También son compatibles con `TransferManager` implementaciones en varios. AWS SDKs

AWS Lambda GetFunction

Principal: interno AWS

Caducidad predeterminada: 10 minutos

AWS Lambda almacena la versión de usuario en un bucket de S3 propiedad del equipo de Lambda antes de generar los activos desplegados en los contenedores de Lambda. Cuando desee acceder al código de su función, llame a. GetFunctionAPI Esto API responde con`Code.Location`, que contiene un prefirmado URL que es válido durante 10 minutos (este tiempo de caducidad es el comportamiento actual y no un contrato publicado). Si no quieres el código, puedes usar una combinación de GetFunctionConfigurationGetFunctionConcurrency, y ListTagspara recuperar el resto de datos devueltos por`GetFunction`.

Lo devuelto URL no está firmado con las credenciales del usuario que ha iniciado sesión actualmente, sino que Lambda lo firma en nombre del usuario. Por este motivo, las claves de condición (por ejemplo`aws:SourceIP`) que se aplican al usuario que ha iniciado sesión actualmente o a las credenciales de sesión temporales del usuario no se aplican a las generadasURL. Esto es cierto tanto si las claves de condición se aplican GetFunctionúnicamente al uso del usuario o la sesión como si se aplican a todos los AWS API usos del usuario o de la sesión.

La consola Lambda también usa GetFunctiony devuelve lo prefirmadoURL. La consola utiliza las credenciales temporales asociadas al usuario que ha iniciado sesión actualmente para realizar la llamada. GetFunction Los detalles sobre la obtención de esas credenciales temporales están fuera del ámbito de este documento.

Amazon ECR

Director: AWS interno

Caducidad predeterminada: 1 hora

Amazon Elastic Container Registry (AmazonECR) proporciona el GetDownloadUrlForLayerAPI, que devuelve un prefirmado URL que es válido durante una hora y permite la descarga de una sola capa de una ECR imagen de Amazon. Sin embargo, el ECR proxy de Amazon utiliza esta operación y, por lo general, los usuarios no la utilizan para extraer y empujar imágenes.

Amazon Redshift Spectrum

Director: Función transferida a CREATEEXTERNALSCHEMAtravés `IAM_ROLE`

Caducidad predeterminada: 1 hora

Amazon Redshift Spectrum usa URLs prefirmados internamente y prohíbe las restricciones en la combinación del bucket y la función de Amazon Redshift que limitarían los prefirmados. URLs Puede utilizar un `s3:signatureAge` valor de 16 minutos, pero los valores muy bajos no son fiables. El valor mínimo que puede utilizar depende de la duración y el tamaño de la consulta. Si bien un valor inferior a 16 minutos funciona en muchos escenarios, es necesario probarlo. La función puede y debe restringirse para que la utilice únicamente Redshift Spectrum, que no revela lo que genera, URLs lo que mitiga la típica justificación de valores de caducidad más bajos.

Amazon SageMaker AI Studio

Amazon SageMaker AI Studio admite dos API acciones: CreatePresignedDomainUrly CreatePresignedNotebookInstanceUrl. Sin embargo, no APIs están relacionadas con la URL función prefirmada de la versión 4 de Signature. APIsCrean una URL que usa un `authToken` parámetro, pero no admiten ninguno de los parámetros de consulta estándar de Signature Version 4.

`authToken`es un mecanismo diferente, pero tiene similitudes con el prefirmadoURLs. Se envía como parámetro de cadena de consulta y admite un tiempo de caducidad de 5 minutos.

SageMaker La IA admite las restricciones de red. Si restringes la `sagemaker:CreatePresignedDomainUrl` acción, esa acción se aplica tanto a la llamada CreatePresignedDomainUrlcomo al uso de lo generadoURL. Si a URL se genera desde una red válida y, a continuación, se envía desde una red no válida, la API llamada para generarla URL tiene éxito, pero la solicitud que envía el URL error. Lo mismo puede decirse de la acción CreatePresignedNotebookInstanceUrly de la `sagemaker:CreatePresignedNotebookInstanceUrl` misma.

Para obtener más información, consulte la documentación sobre SageMaker IA.

Apéndice B: Cómo afectan los controles de las URL prefirmadas Servicios de AWS

En este apéndice se describen las interacciones entre los Servicios de AWS que utilizan direcciones URL prefirmadas, tal como se describe en el apéndice A, y los controles descritos anteriormente en esta guía.

Guardrail para S3: SignatureAge

La consola Amazon S3 no se ve afectada por la caducidad máxima de 5 minutos establecida por la clave de `s3:signatureAge` condición. La consola Amazon S3 genera URL prefirmadas al seleccionar el botón Descargar y aplica su propio tiempo de caducidad de 5 minutos. Una duración máxima inferior a 2 minutos puede provocar errores aleatorios en función de la sincronización del reloj y las latencias.

Amazon S3 Object Lambda utiliza un tiempo de caducidad de 61 segundos, por lo que establecer condiciones en un `s3:signatureAge` valor de 61 segundos o más no provocará ninguna interrupción. Las duraciones más cortas pueden ser menos fiables y provocar fallos intermitentes.

Amazon S3 Cross-Region CopyObjectno se ve interrumpido por una caducidad máxima de 5 minutos. Sin embargo, las duraciones más cortas pueden provocar errores aleatorios en función de la sincronización del reloj y las latencias.

En AWS Lambda, GetFunctionproporciona una URL a objetos ajenos a la cuenta del cliente, de modo que las políticas del cliente no afecten a las URL generadas.

Se probó Amazon Redshift Spectrum durante 16 minutos. `s3:signatureAge` Sin embargo, una duración más corta podría provocar interrupciones.

Barandilla para S3: AuthType cuando no se utilizan restricciones de red

La consola Amazon S3 suele verse afectada por la `s3:authType` barandilla. La consola se enruta a Amazon S3 en función de la configuración de la red local. Si la red local se enruta a Amazon S3 de la manera que lo permita la restricción de red, la consola Amazon S3 seguiría funcionando. Sin

embargo, si se enruta a través de un proxy o de la Internet pública de una manera no permitida, se bloqueará su uso. Sin embargo, bloquear el uso es probablemente la intención de esta política.

El objeto Lambda de Amazon S3 se ve afectado si la función Lambda no está conectada a una VPC adecuada. En esta configuración, la VPC debe tener una puerta de enlace NAT, no para acceder al bucket de S3, sino para realizar una llamada. WriteGetObjectResponse

Amazon S3 Cross-Region CopyObjectse interrumpe si esta barrera de protección se aplica a una política de bucket sin la excepción recomendada cuando **`aws:viaAWSService`** es verdadera.

Amazon Redshift Spectrum se ve afectado por `s3:authType` la barandilla, a menos que se utilice el enrutamiento de VPC mejorado. Actualmente, Redshift Spectrum admite el enrutamiento de VPC mejorado solo con clústeres sin servidor, no con clústeres aprovisionados.

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Publicación inicial	—	23 de julio de 2024

AWS Glosario de orientación prescriptiva

Los siguientes son términos de uso común en las estrategias, guías y patrones proporcionados por la Guía AWS prescriptiva. Para sugerir entradas, utilice el enlace Enviar comentarios al final del glosario.

Números

Las 7 R

Siete estrategias de migración comunes para trasladar aplicaciones a la nube. Estas estrategias se basan en las 5 R que Gartner identificó en 2011 y consisten en lo siguiente:

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: migre su base de datos Oracle local a la edición compatible con PostgreSQL de Amazon Aurora.
- Redefinir la plataforma (transportar y redefinir): traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Amazon Relational Database Service (Amazon RDS) para Oracle en el. Nube de AWS
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: migre su sistema de gestión de relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Oracle en una EC2 instancia del. Nube de AWS
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma local a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

- Retirar: retire o elimine las aplicaciones que ya no sean necesarias en un entorno de origen.

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas (mediante una herramienta de replicación bidireccional o mediante operaciones de escritura doble) y ambas bases de datos gestionan las transacciones de las aplicaciones conectadas durante la migración. Este método permite la migración en lotes pequeños y controlados, en lugar de requerir una transición única. Es más flexible, pero requiere más trabajo que la migración activa-pasiva.

migración activa-pasiva

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas, pero solo la base de datos de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la base de datos de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función agregada

Función SQL que opera en un grupo de filas y calcula un único valor de retorno para el grupo. Algunos ejemplos de funciones agregadas incluyen `SUM` y`MAX`.

IA

Véase inteligencia artificial.

AIOps

Consulte las operaciones de inteligencia artificial.

anonimización

El proceso de eliminar permanentemente la información personal de un conjunto de datos. La anonimización puede ayudar a proteger la privacidad personal. Los datos anonimizados ya no se consideran datos personales.

antipatrones

Una solución que se utiliza con frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa.

control de aplicaciones

Un enfoque de seguridad que permite el uso únicamente de aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

cartera de aplicaciones

Recopilación de información detallada sobre cada aplicación que utiliza una organización, incluido el costo de creación y mantenimiento de la aplicación y su valor empresarial. Esta información es clave para el proceso de detección y análisis de la cartera y ayuda a identificar y priorizar las aplicaciones que se van a migrar, modernizar y optimizar.

inteligencia artificial (IA)

El campo de la informática que se dedica al uso de tecnologías informáticas para realizar funciones cognitivas que suelen estar asociadas a los seres humanos, como el aprendizaje, la resolución de problemas y el reconocimiento de patrones. Para más información, consulte ¿Qué es la inteligencia artificial?

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo AIOps se utiliza en la estrategia de AWS migración, consulte la guía de integración de operaciones.

cifrado asimétrico

Algoritmo de cifrado que utiliza un par de claves, una clave pública para el cifrado y una clave privada para el descifrado. Puede compartir la clave pública porque no se utiliza para el descifrado, pero el acceso a la clave privada debe estar sumamente restringido.

atomicidad, consistencia, aislamiento, durabilidad (ACID)

Conjunto de propiedades de software que garantizan la validez de los datos y la fiabilidad operativa de una base de datos, incluso en caso de errores, cortes de energía u otros problemas.

control de acceso basado en atributos (ABAC)

La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte ABAC AWS en la documentación AWS Identity and Access Management (IAM).

origen de datos fidedigno

Ubicación en la que se almacena la versión principal de los datos, que se considera la fuente de información más fiable. Puede copiar los datos del origen de datos autorizado a otras ubicaciones con el fin de procesarlos o modificarlos, por ejemplo, anonimizarlos, redactarlos o seudonimizarlos.

Zona de disponibilidad

Una ubicación distinta dentro de una Región de AWS que está aislada de los fallos en otras zonas de disponibilidad y que proporciona una conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

AWS Marco de adopción de la nube (AWS CAF)

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la Página web de AWS CAF y el Documento técnico de AWS CAF.

AWS Marco de calificación de la carga de trabajo (AWS WQF)

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQF se incluye con AWS

Schema Conversion Tool ().AWS SCT Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

B

Un bot malo

Un bot destinado a interrumpir o causar daño a personas u organizaciones.

BCP

Consulte la planificación de la continuidad del negocio.

gráfico de comportamiento

Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las llamadas sospechosas a la API y acciones similares. Para obtener más información, consulte Datos en un gráfico de comportamiento en la documentación de Detective.

sistema big-endian

Un sistema que almacena primero el byte más significativo. Véase también endianness.

clasificación binaria

Un proceso que predice un resultado binario (una de las dos clases posibles). Por ejemplo, es posible que su modelo de ML necesite predecir problemas como “¿Este correo electrónico es spam o no es spam?” o “¿Este producto es un libro o un automóvil?”.

filtro de floración

Estructura de datos probabilística y eficiente en términos de memoria que se utiliza para comprobar si un elemento es miembro de un conjunto.

implementación azul/verde

Una estrategia de despliegue en la que se crean dos entornos separados pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación en el otro entorno (verde). Esta estrategia le ayuda a revertirla rápidamente con un impacto mínimo.

bot

Aplicación de software que ejecuta tareas automatizadas a través de Internet y simula la actividad o interacción humana. Algunos bots son útiles o beneficiosos, como los rastreadores web que indexan información en Internet. Algunos otros bots, conocidos como bots malos, tienen como objetivo interrumpir o causar daños a personas u organizaciones.

botnet

Redes de bots que están infectadas por malware y que están bajo el control de una sola parte, conocida como pastor u operador de bots. Las botnets son el mecanismo más conocido para escalar los bots y su impacto.

branch

Área contenida de un repositorio de código. La primera rama que se crea en un repositorio es la rama principal. Puede crear una rama nueva a partir de una rama existente y, a continuación, desarrollar características o corregir errores en la rama nueva. Una rama que se genera para crear una característica se denomina comúnmente rama de característica. Cuando la característica se encuentra lista para su lanzamiento, se vuelve a combinar la rama de característica con la rama principal. Para obtener más información, consulte Acerca de las sucursales (GitHub documentación).

acceso con cristales rotos

En circunstancias excepcionales y mediante un proceso aprobado, un usuario puede acceder rápidamente a un sitio para el Cuenta de AWS que normalmente no tiene permisos de acceso. Para obtener más información, consulte el indicador Implemente procedimientos de rotura de cristales en la guía Well-Architected AWS .

estrategia de implementación sobre infraestructura existente

La infraestructura existente en su entorno. Al adoptar una estrategia de implementación sobre infraestructura existente para una arquitectura de sistemas, se diseña la arquitectura en función de las limitaciones de los sistemas y la infraestructura actuales. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

caché de búfer

El área de memoria donde se almacenan los datos a los que se accede con más frecuencia.

capacidad empresarial

Lo que hace una empresa para generar valor (por ejemplo, ventas, servicio al cliente o marketing). Las arquitecturas de microservicios y las decisiones de desarrollo pueden estar impulsadas por las capacidades empresariales. Para obtener más información, consulte la sección Organizado en torno a las capacidades empresariales del documento técnico Ejecutar microservicios en contenedores en AWS.

planificación de la continuidad del negocio (BCP)

Plan que aborda el posible impacto de un evento disruptivo, como una migración a gran escala en las operaciones y permite a la empresa reanudar las operaciones rápidamente.

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

El lanzamiento lento e incremental de una versión para los usuarios finales. Cuando está seguro, despliega la nueva versión y reemplaza la versión actual en su totalidad.

CCoE

Consulte Cloud Center of Excellence.

CDC

Consulte la captura de datos de cambios.

captura de datos de cambio (CDC)

Proceso de seguimiento de los cambios en un origen de datos, como una tabla de base de datos, y registro de los metadatos relacionados con el cambio. Puede utilizar los CDC para diversos fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

ingeniería del caos

Introducir intencionalmente fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puedes usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estresen tus AWS cargas de trabajo y evalúen su respuesta.

CI/CD

Consulte la integración continua y la entrega continua.

clasificación

Un proceso de categorización que permite generar predicciones. Los modelos de ML para problemas de clasificación predicen un valor discreto. Los valores discretos siempre son distintos entre sí. Por ejemplo, es posible que un modelo necesite evaluar si hay o no un automóvil en una imagen.

cifrado del cliente

Cifrado de datos localmente, antes de que el objetivo los Servicio de AWS reciba.

Centro de excelencia en la nube (CCoE)

Equipo multidisciplinario que impulsa los esfuerzos de adopción de la nube en toda la organización, incluido el desarrollo de las prácticas recomendadas en la nube, la movilización de recursos, el establecimiento de plazos de migración y la dirección de la organización durante las transformaciones a gran escala. Para obtener más información, consulte las publicaciones de CCo E en el blog de estrategia Nube de AWS empresarial.

computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar conectada a la tecnología de computación perimetral.

modelo operativo en la nube

En una organización de TI, el modelo operativo que se utiliza para crear, madurar y optimizar uno o más entornos de nube. Para obtener más información, consulte Creación de su modelo operativo de nube.

etapas de adopción de la nube

Las cuatro fases por las que suelen pasar las organizaciones cuando migran a Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCo E, establecer un modelo de operaciones)
- Migración: migración de aplicaciones individuales
- Reinvención: optimización de productos y servicios e innovación en la nube

Stephen Orban definió estas etapas en la entrada del blog The Journey Toward Cloud-First & the Stages of Adoption en el blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de preparación para la migración.

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Los repositorios en la nube más comunes incluyen GitHub oBitbucket Cloud. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola canalización de CI/CD puede utilizar varios repositorios.

caché en frío

Una caché de búfer que está vacía no está bien poblada o contiene datos obsoletos o irrelevantes. Esto afecta al rendimiento, ya que la instancia de la base de datos debe leer desde la memoria principal o el disco, lo que es más lento que leer desde la memoria caché del búfer.

datos fríos

Datos a los que se accede con poca frecuencia y que suelen ser históricos. Al consultar este tipo de datos, normalmente se aceptan consultas lentas. Trasladar estos datos a niveles o clases de almacenamiento de menor rendimiento y menos costosos puede reducir los costos.

visión artificial (CV)

Campo de la IA que utiliza el aprendizaje automático para analizar y extraer información de formatos visuales, como imágenes y vídeos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

desviación de configuración

En el caso de una carga de trabajo, un cambio de configuración con respecto al estado esperado. Puede provocar que la carga de trabajo deje de cumplir las normas y, por lo general, es gradual e involuntario.

base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, los

datos de una CMDB se utilizan en la etapa de detección y análisis de la cartera de productos durante la migración.

paquete de conformidad

Conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus comprobaciones de conformidad y seguridad. Puede implementar un paquete de conformidad como una entidad única en una región Cuenta de AWS y, o en una organización, mediante una plantilla YAML. Para obtener más información, consulta los paquetes de conformidad en la documentación. AWS Config

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD is commonly described as a pipeline. CI/CDpuede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Vea la visión artificial.

D

datos en reposo

Datos que están estacionarios en la red, como los datos que se encuentran almacenados.

clasificación de datos

Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de datos es un componente del pilar de seguridad del AWS Well-Architected Framework. Para obtener más información, consulte Clasificación de datos.

desviación de datos

Una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de machine learning, o un cambio significativo en los datos de entrada

a lo largo del tiempo. La desviación de los datos puede reducir la calidad, la precisión y la imparcialidad generales de las predicciones de los modelos de machine learning.

datos en tránsito

Datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red.

malla de datos

Un marco arquitectónico que proporciona una propiedad de datos distribuida y descentralizada con una administración y un gobierno centralizados.

minimización de datos

El principio de recopilar y procesar solo los datos estrictamente necesarios. Practicar la minimización de los datos Nube de AWS puede reducir los riesgos de privacidad, los costos y la huella de carbono de la analítica.

perímetro de datos

Un conjunto de barreras preventivas en su AWS entorno que ayudan a garantizar que solo las identidades confiables accedan a los recursos confiables desde las redes esperadas. Para obtener más información, consulte Crear un perímetro de datos sobre. AWS

preprocesamiento de datos

Transformar los datos sin procesar en un formato que su modelo de ML pueda analizar fácilmente. El preprocesamiento de datos puede implicar eliminar determinadas columnas o filas y corregir los valores faltantes, incoherentes o duplicados.

procedencia de los datos

El proceso de rastrear el origen y el historial de los datos a lo largo de su ciclo de vida, por ejemplo, la forma en que se generaron, transmitieron y almacenaron los datos.

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

Un sistema de administración de datos que respalde la inteligencia empresarial, como el análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para consultas y análisis.

lenguaje de definición de datos (DDL)

Instrucciones o comandos para crear o modificar la estructura de tablas y objetos de una base de datos.

lenguaje de manipulación de datos (DML)

Instrucciones o comandos para modificar (insertar, actualizar y eliminar) la información de una base de datos.

DDL

Consulte el lenguaje de definición de bases de datos.

conjunto profundo

Combinar varios modelos de aprendizaje profundo para la predicción. Puede utilizar conjuntos profundos para obtener una predicción más precisa o para estimar la incertidumbre de las predicciones.

aprendizaje profundo

Un subcampo del ML que utiliza múltiples capas de redes neuronales artificiales para identificar el mapeo entre los datos de entrada y las variables objetivo de interés.

defense-in-depth

Un enfoque de seguridad de la información en el que se distribuyen cuidadosamente una serie de mecanismos y controles de seguridad en una red informática para proteger la confidencialidad, la integridad y la disponibilidad de la red y de los datos que contiene. Al adoptar esta estrategia AWS, se añaden varios controles en diferentes capas de la AWS Organizations estructura para ayudar a proteger los recursos. Por ejemplo, un defense-in-depth enfoque podría combinar la autenticación multifactorial, la segmentación de la red y el cifrado.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de ese servicio. Esta cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte Servicios que funcionan con AWS Organizations en la documentación de AWS Organizations .

Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar

cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

entorno de desarrollo

Consulte entorno.

control de detección

Un control de seguridad que se ha diseñado para detectar, registrar y alertar después de que se produzca un evento. Estos controles son una segunda línea de defensa, ya que lo advierten sobre los eventos de seguridad que han eludido los controles preventivos establecidos. Para obtener más información, consulte Controles de detección en Implementación de controles de seguridad en AWS.

asignación de flujos de valor para el desarrollo (DVSM)

Proceso que se utiliza para identificar y priorizar las restricciones que afectan negativamente a la velocidad y la calidad en el ciclo de vida del desarrollo de software. DVSM amplía el proceso de asignación del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

gemelo digital

Representación virtual de un sistema del mundo real, como un edificio, una fábrica, un equipo industrial o una línea de producción. Los gemelos digitales son compatibles con el mantenimiento predictivo, la supervisión remota y la optimización de la producción.

tabla de dimensiones

En un esquema en estrella, tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos de una tabla de hechos. Los atributos de la tabla de dimensiones suelen ser campos de texto o números discretos que se comportan como texto. Estos atributos se utilizan habitualmente para restringir consultas, filtrar y etiquetar conjuntos de resultados.

desastre

Un evento que impide que una carga de trabajo o un sistema cumplan sus objetivos empresariales en su ubicación principal de implementación. Estos eventos pueden ser desastres naturales, fallos técnicos o el resultado de acciones humanas, como una configuración incorrecta involuntaria o un ataque de malware.

recuperación de desastres (DR)

La estrategia y el proceso que se utilizan para minimizar el tiempo de inactividad y la pérdida de datos ocasionados por un desastre. Para obtener más información, consulte Recuperación ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

Un enfoque para desarrollar un sistema de software complejo mediante la conexión de sus componentes a dominios en evolución, o a los objetivos empresariales principales, a los que sirve cada componente. Este concepto lo introdujo Eric Evans en su libro, Diseño impulsado por el dominio: abordando la complejidad en el corazón del software (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

detección de deriva

Seguimiento de las desviaciones con respecto a una configuración de referencia. Por ejemplo, puedes usarlo AWS CloudFormation para detectar desviaciones en los recursos del sistema o puedes usarlo AWS Control Tower para detectar cambios en tu landing zone que puedan afectar al cumplimiento de los requisitos de gobierno.

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

EDI

Véase intercambio electrónico de datos.

computación en la periferia

La tecnología que aumenta la potencia de cálculo de los dispositivos inteligentes en la periferia de una red de IoT. En comparación con la computación en nube, la computación perimetral puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos (EDI)

El intercambio automatizado de documentos comerciales entre organizaciones. Para obtener más información, consulte Qué es el intercambio electrónico de datos.

cifrado

Proceso informático que transforma datos de texto plano, legibles por humanos, en texto cifrado.

clave de cifrado

Cadena criptográfica de bits aleatorios que se genera mediante un algoritmo de cifrado. Las claves pueden variar en longitud y cada una se ha diseñado para ser impredecible y única.

endianidad

El orden en el que se almacenan los bytes en la memoria del ordenador. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian almacenan primero el byte menos significativo.

punto de conexión

Consulte el punto final del servicio.

servicio de punto de conexión

Servicio que puede alojar en una nube privada virtual (VPC) para compartir con otros usuarios. Puede crear un servicio de punto final AWS PrivateLink y conceder permisos a otros directores Cuentas de AWS o a AWS Identity and Access Management (IAM). Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte Creación de un servicio de punto de conexión en la documentación de Amazon Virtual Private Cloud (Amazon VPC).

planificación de recursos empresariales (ERP)

Un sistema que automatiza y gestiona los procesos empresariales clave (como la contabilidad, el MES y la gestión de proyectos) de una empresa.

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte el cifrado de sobres en la documentación de AWS Key Management Service (AWS KMS).

entorno

Una instancia de una aplicación en ejecución. Los siguientes son los tipos de entornos más comunes en la computación en la nube:

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.
- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En una canalización de CI/CD, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las epopeyas AWS de seguridad de CAF incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la Guía de implementación del programa.

ERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (EDA)

El proceso de analizar un conjunto de datos para comprender sus características principales. Se recopilan o agregan datos y, a continuación, se realizan las investigaciones iniciales para

encontrar patrones, detectar anomalías y comprobar las suposiciones. El EDA se realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

F

tabla de datos

La tabla central de un esquema en forma de estrella. Almacena datos cuantitativos sobre las operaciones comerciales. Normalmente, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

fallan rápidamente

Una filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de un enfoque ágil.

límite de aislamiento de fallas

En el Nube de AWS, un límite, como una zona de disponibilidad Región de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para obtener más información, consulte Límites de AWS aislamiento de errores.

rama de característica

Consulte la sucursal.

características

Los datos de entrada que se utilizan para hacer una predicción. Por ejemplo, en un contexto de fabricación, las características pueden ser imágenes que se capturan periódicamente desde la línea de fabricación.

importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, esto se expresa como una puntuación numérica que se puede calcular mediante diversas técnicas, como las explicaciones aditivas de Shapley (SHAP) y los gradientes integrados. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con AWS.

transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

indicaciones de unos pocos pasos

Proporcionar a un LLM un pequeño número de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que realice una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, en el que los modelos aprenden a partir de ejemplos (planos) integrados en las instrucciones. Las indicaciones con pocas tomas pueden ser eficaces para tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también el apartado de mensajes sin intervención.

FGAC

Consulte el control de acceso detallado.

control de acceso preciso (FGAC)

El uso de varias condiciones que tienen por objetivo permitir o denegar una solicitud de acceso.

migración relámpago

Método de migración de bases de datos que utiliza la replicación continua de datos mediante la captura de datos modificados para migrar los datos en el menor tiempo posible, en lugar de utilizar un enfoque gradual. El objetivo es reducir al mínimo el tiempo de inactividad.

FM

Consulte el modelo básico.

modelo de base (FM)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMs son capaces de realizar una amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para obtener más información, consulte Qué son los modelos básicos.

G

IA generativa

Un subconjunto de modelos de IA que se han entrenado con grandes cantidades de datos y que pueden utilizar un simple mensaje de texto para crear contenido y artefactos nuevos, como imágenes, vídeos, texto y audio. Para obtener más información, consulte Qué es la IA generativa.

bloqueo geográfico

Consulta las restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

En Amazon CloudFront, una opción para impedir que los usuarios de países específicos accedan a las distribuciones de contenido. Puede utilizar una lista de permitidos o bloqueados para especificar los países aprobados y prohibidos. Para obtener más información, consulta Restringir la distribución geográfica del contenido en la CloudFront documentación.

Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, y el flujo de trabajo basado en enlaces troncales es el enfoque moderno preferido.

imagen dorada

Instantánea de un sistema o software que se utiliza como plantilla para implementar nuevas instancias de ese sistema o software. Por ejemplo, en la fabricación, una imagen dorada se puede utilizar para aprovisionar software en varios dispositivos y ayuda a mejorar la velocidad, la escalabilidad y la productividad de las operaciones de fabricación de dispositivos.

estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como implementación sobre infraestructura existente. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y el cumplimiento en todas las unidades organizativas (OUs). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de permisos de IAM. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

HA

Consulte la alta disponibilidad.

migración heterogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que utilice un motor de base de datos diferente (por ejemplo, de Oracle a Amazon Aurora). La migración heterogénea suele ser parte de un esfuerzo de rediseño de la arquitectura y convertir el esquema puede ser una tarea compleja. AWS ofrece AWS SCT, lo cual ayuda con las conversiones de esquemas.

alta disponibilidad (HA)

La capacidad de una carga de trabajo para funcionar de forma continua, sin intervención, en caso de desafíos o desastres. Los sistemas de alta disponibilidad están diseñados para realizar una conmutación por error automática, ofrecer un rendimiento de alta calidad de forma constante y gestionar diferentes cargas y fallos con un impacto mínimo en el rendimiento.

modernización histórica

Un enfoque utilizado para modernizar y actualizar los sistemas de tecnología operativa (TO) a fin de satisfacer mejor las necesidades de la industria manufacturera. Un histórico es un tipo de base de datos que se utiliza para recopilar y almacenar datos de diversas fuentes en una fábrica.

datos retenidos

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de aprendizaje automático. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo comparando las predicciones del modelo con los datos de reserva.

migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS para SQL Server). La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

datos recientes

Datos a los que se accede con frecuencia, como datos en tiempo real o datos traslacionales recientes. Por lo general, estos datos requieren un nivel o una clase de almacenamiento de alto rendimiento para proporcionar respuestas rápidas a las consultas.

hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, las revisiones suelen realizarse fuera del flujo de trabajo habitual de las versiones. DevOps

periodo de hiperatención

Periodo, inmediatamente después de la transición, durante el cual un equipo de migración administra y monitorea las aplicaciones migradas en la nube para solucionar cualquier problema. Por lo general, este periodo dura de 1 a 4 días. Al final del periodo de hiperatención, el equipo de migración suele transferir la responsabilidad de las aplicaciones al equipo de operaciones en la nube.

I

IaC

Vea la infraestructura como código.

políticas basadas en identidad

Política asociada a uno o más directores de IAM que define sus permisos en el Nube de AWS entorno.

aplicación inactiva

Aplicación que utiliza un promedio de CPU y memoria de entre 5 y 20 por ciento durante un periodo de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

Un modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, aplicar parches o modificar la infraestructura existente. Las infraestructuras inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables. Para obtener más información, consulte las prácticas recomendadas para implementar con una infraestructura inmutable en Well-Architected Framework AWS .

VPC entrante (de entrada)

En una arquitectura de AWS cuentas múltiples, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

migración gradual

Estrategia de transición en la que se migra la aplicación en partes pequeñas en lugar de realizar una transición única y completa. Por ejemplo, puede trasladar inicialmente solo unos pocos microservicios o usuarios al nuevo sistema. Tras comprobar que todo funciona correctamente, puede trasladar microservicios o usuarios adicionales de forma gradual hasta que pueda retirar su sistema heredado. Esta estrategia reduce los riesgos asociados a las grandes migraciones.

Industria 4.0

Un término que Klaus Schwab introdujo en 2016 para referirse a la modernización de los procesos de fabricación mediante avances en la conectividad, los datos en tiempo real, la automatización, el análisis y la inteligencia artificial/aprendizaje automático.

infraestructura

Todos los recursos y activos que se encuentran en el entorno de una aplicación.

infraestructura como código (IaC)

Proceso de aprovisionamiento y administración de la infraestructura de una aplicación mediante un conjunto de archivos de configuración. La IaC se ha diseñado para ayudarlo a centralizar la administración de la infraestructura, estandarizar los recursos y escalar con rapidez a fin de que los entornos nuevos sean repetibles, fiables y consistentes.

Internet de las cosas industrial (T) IIo

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte Creación de una estrategia de transformación digital de la Internet de las cosas (IIoT) industrial.

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red VPCs entre Internet y las redes locales (en una misma o Regiones de AWS diferente). La arquitectura AWS de referencia de seguridad recomienda configurar su cuenta de red con entrada, salida e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

Internet de las cosas (IoT)

Red de objetos físicos conectados con sensores o procesadores integrados que se comunican con otros dispositivos y sistemas a través de Internet o de una red de comunicación local. Para obtener más información, consulte ¿Qué es IoT?.

interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con. AWS

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. La ITIL proporciona la base para la ITSM.

administración de servicios de TI (ITSM)

Actividades asociadas con el diseño, la implementación, la administración y el soporte de los servicios de TI para una organización. Para obtener información sobre la integración de las operaciones en la nube con las herramientas de ITSM, consulte la Guía de integración de operaciones.

ITIL

Consulte la biblioteca de información de TI.

ITSM

Consulte Administración de servicios de TI.

L

control de acceso basado en etiquetas (LBAC)

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

zona de aterrizaje

Una landing zone es un AWS entorno multicuenta bien diseñado, escalable y seguro. Este es un punto de partida desde el cual las empresas pueden lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura. Para obtener más información sobre las zonas de aterrizaje, consulte Configuración de un entorno de AWS seguro y escalable con varias cuentas.

modelo de lenguaje grande (LLM)

Un modelo de IA de aprendizaje profundo que se entrena previamente con una gran cantidad de datos. Un LLM puede realizar múltiples tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para obtener más información, consulte Qué son. LLMs

migración grande

Migración de 300 servidores o más.

LBAC

Consulte control de acceso basado en etiquetas.

privilegio mínimo

La práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Aplicar permisos de privilegio mínimo en la documentación de IAM.

migrar mediante lift-and-shift

Ver 7 Rs.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Véase también endianness.

LLM

Véase un modelo de lenguaje amplio.

entornos inferiores

Véase entorno.

M

machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte Machine learning.

rama principal

Ver sucursal.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware puede interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los registradores de pulsaciones de teclas.

servicios gestionados

Servicios de AWS para los que AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y usted accede a los puntos finales para almacenar y recuperar datos. Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB son ejemplos de servicios gestionados. También se conocen como servicios abstractos.

sistema de ejecución de fabricación (MES)

Un sistema de software para rastrear, monitorear, documentar y controlar los procesos de producción que convierten las materias primas en productos terminados en el taller.

MAP

Consulte Migration Acceleration Program.

mecanismo

Un proceso completo en el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para realizar ajustes. Un mecanismo es un ciclo que se refuerza y mejora a sí mismo a medida que funciona. Para obtener más información, consulte Creación de mecanismos en el AWS Well-Architected Framework.

cuenta de miembro

Todas las Cuentas de AWS demás cuentas, excepto la de administración, que forman parte de una organización. AWS Organizations Una cuenta no puede pertenecer a más de una organización a la vez.

MES

Consulte el sistema de ejecución de la fabricación.

Transporte telemétrico de Message Queue Queue (MQTT)

Un protocolo de comunicación ligero machine-to-machine (M2M), basado en el patrón de publicación/suscripción, para dispositivos de IoT con recursos limitados.

microservicio

Un servicio pequeño e independiente que se comunica a través de una red bien definida APIs y que, por lo general, es propiedad de equipos pequeños e independientes. Por ejemplo, un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte Integrar microservicios mediante AWS servicios sin servidor.

arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de una interfaz bien definida mediante un uso ligero. APIs Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte Implementación de microservicios en. AWS

Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

migración a escala

Proceso de transferencia de la mayoría de la cartera de aplicaciones a la nube en oleadas, con más aplicaciones desplazadas a un ritmo más rápido en cada oleada. En esta fase, se utilizan las prácticas recomendadas y las lecciones aprendidas en las fases anteriores para implementar una fábrica de migración de equipos, herramientas y procesos con el fin de agilizar la migración de las cargas de trabajo mediante la automatización y la entrega ágil. Esta es la tercera fase de la estrategia de migración de AWS.

fábrica de migración

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de las fábricas de migración suelen incluir a analistas y propietarios de operaciones, empresas, ingenieros de migración, desarrolladores y DevOps profesionales que trabajan a pasos agigantados. Entre el 20 y el 50 por ciento de la cartera de aplicaciones empresariales se compone de patrones repetidos que pueden optimizarse mediante un enfoque de fábrica. Para obtener más información, consulte la discusión sobre las fábricas de migración y la Guía de fábricas de migración a la nube en este contenido.

metadatos de migración

Información sobre la aplicación y el servidor que se necesita para completar la migración. Cada patrón de migración requiere un conjunto diferente de metadatos de migración. Algunos ejemplos de metadatos de migración son la subred de destino, el grupo de seguridad y AWS la cuenta.

patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: realoje la migración a Amazon EC2 con AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Una herramienta en línea que proporciona información para validar el modelo de negocio para migrar a. Nube de AWS La MPA ofrece una evaluación detallada de la cartera (adecuación del

tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores asociados de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar sus puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas mediante el AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. La MRA es la primera fase de la estrategia de migración de AWS.

estrategia de migración

El enfoque utilizado para migrar una carga de trabajo a. Nube de AWS Para obtener más información, consulte la entrada de las 7 R de este glosario y consulte Movilice a su organización para acelerar las migraciones a gran escala.

ML

Consulte el aprendizaje automático.

modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia y aprovechar las innovaciones. Para obtener más información, consulte Estrategia para modernizar las aplicaciones en el Nube de AWS.

evaluación de la preparación para la modernización

Evaluación que ayuda a determinar la preparación para la modernización de las aplicaciones de una organización; identifica los beneficios, los riesgos y las dependencias; y determina qué tan bien la organización puede soportar el estado futuro de esas aplicaciones. El resultado de la evaluación es un esquema de la arquitectura objetivo, una hoja de ruta que detalla las fases de desarrollo y los hitos del proceso de modernización y un plan de acción para abordar las brechas identificadas. Para obtener más información, consulte Evaluación de la preparación para la modernización de las aplicaciones en el Nube de AWS.

aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la

aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar una arquitectura de microservicios. Para obtener más información, consulte Descomposición de monolitos en microservicios.

MAPA

Consulte la evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

Un proceso que ayuda a generar predicciones para varias clases (predice uno de más de dos resultados). Por ejemplo, un modelo de ML podría preguntar "¿Este producto es un libro, un automóvil o un teléfono?" o "¿Qué categoría de productos es más interesante para este cliente?".

infraestructura mutable

Un modelo que actualiza y modifica la infraestructura existente para las cargas de trabajo de producción. Para mejorar la coherencia, la fiabilidad y la previsibilidad, el AWS Well-Architected Framework recomienda el uso de una infraestructura inmutable como práctica recomendada.

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

Método de migración en el que la carga de trabajo de origen se elimina durante el proceso de migración. Este método implica un tiempo de inactividad prolongado y, por lo general, se utiliza para cargas de trabajo pequeñas y no críticas.

OI

Consulte integración de operaciones.

OLA

Véase el acuerdo a nivel operativo.

migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

Comunicaciones de proceso abierto: arquitectura unificada (OPC-UA)

Un protocolo de comunicación machine-to-machine (M2M) para la automatización industrial. El OPC-UA proporciona un estándar de interoperabilidad con esquemas de cifrado, autenticación y autorización de datos.

acuerdo de nivel operativo (OLA)

Acuerdo que aclara lo que los grupos de TI operativos se comprometen a ofrecerse entre sí, para respaldar un acuerdo de nivel de servicio (SLA).

revisión de la preparación operativa (ORR)

Una lista de preguntas y las mejores prácticas asociadas que le ayudan a comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles fallos. Para obtener más información, consulte Operational Readiness Reviews (ORR) en AWS Well-Architected Framework.

tecnología operativa (OT)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En la industria manufacturera, la integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la industria 4.0.

integración de operaciones (OI)

Proceso de modernización de las operaciones en la nube, que implica la planificación de la preparación, la automatización y la integración. Para obtener más información, consulte la Guía de integración de las operaciones.

registro de seguimiento organizativo

Un registro creado por el AWS CloudTrail que se registran todos los eventos para todos Cuentas de AWS los miembros de una organización AWS Organizations. Este registro de seguimiento se crea en cada Cuenta de AWS que forma parte de la organización y realiza un seguimiento de la actividad en cada cuenta. Para obtener más información, consulte Crear un registro para una organización en la CloudTrail documentación.

administración del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. La OCM ayuda a las empresas a prepararse para nuevos sistemas y estrategias y a realizar la transición a ellos, al acelerar la adopción de cambios, abordar los problemas de transición e impulsar cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de personal, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la Guía de OCM.

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). El OAC admite todos los buckets de S3 Regiones de AWS, el cifrado del lado del servidor AWS KMS (SSE-KMS) y las solicitudes dinámicas `PUT` y `DELETE` dirigidas al bucket de S3.

identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando utiliza OAI, CloudFront crea un principal con el que Amazon S3 puede autenticarse. Los directores autenticados solo pueden acceder al contenido de un bucket de S3 a través de una distribución específica. CloudFront Consulte también el OAC, que proporciona un control de acceso más detallado y mejorado.

ORR

Consulte la revisión de la preparación operativa.

OT

Consulte la tecnología operativa.

VPC saliente (de salida)

En una arquitectura de AWS cuentas múltiples, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

P

límite de permisos

Una política de administración de IAM que se adjunta a las entidades principales de IAM para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte Límites de permisos en la documentación de IAM.

información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos de información de identificación personal son los nombres, las direcciones y la información de contacto.

PII

Consulte la información de identificación personal.

manual de estrategias

Conjunto de pasos predefinidos que capturan el trabajo asociado a las migraciones, como la entrega de las funciones de operaciones principales en la nube. Un manual puede adoptar la forma de scripts, manuales de procedimientos automatizados o resúmenes de los procesos o pasos necesarios para operar un entorno modernizado.

PLC

Consulte controlador lógico programable.

PLM

Consulte la gestión del ciclo de vida del producto.

policy

Un objeto que puede definir los permisos (consulte la política basada en la identidad), especifique las condiciones de acceso (consulte la política basada en los recursos) o defina los permisos máximos para todas las cuentas de una organización AWS Organizations (consulte la política de control de servicios).

persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades. Para obtener más información, consulte Habilitación de la persistencia de datos en los microservicios.

evaluación de cartera

Proceso de detección, análisis y priorización de la cartera de aplicaciones para planificar la migración. Para obtener más información, consulte la Evaluación de la preparación para la migración.

predicate

Una condición de consulta que devuelve `true` o`false`, por lo general, se encuentra en una cláusula. `WHERE`

pulsar un predicado

Técnica de optimización de consultas de bases de datos que filtra los datos de la consulta antes de transferirlos. Esto reduce la cantidad de datos que se deben recuperar y procesar de la base de datos relacional y mejora el rendimiento de las consultas.

control preventivo

Un control de seguridad diseñado para evitar que ocurra un evento. Estos controles son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Para obtener más información, consulte Controles preventivos en Implementación de controles de seguridad en AWS.

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz para un Cuenta de AWS rol de IAM o un usuario. Para obtener más información, consulte Entidad principal en Términos y conceptos de roles en la documentación de IAM.

privacidad desde el diseño

Un enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de desarrollo.

zonas alojadas privadas

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno o más VPCs. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Un control de seguridad diseñado para evitar el despliegue de recursos no conformes. Estos controles escanean los recursos antes de aprovisionarlos. Si el recurso no cumple con el control, significa que no está aprovisionado. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en Implementación de controles de seguridad en AWS.

gestión del ciclo de vida del producto (PLM)

La gestión de los datos y los procesos de un producto a lo largo de todo su ciclo de vida, desde el diseño, el desarrollo y el lanzamiento, pasando por el crecimiento y la madurez, hasta el rechazo y la retirada.

entorno de producción

Consulte el entorno.

controlador lógico programable (PLC)

En la fabricación, una computadora adaptable y altamente confiable que monitorea las máquinas y automatiza los procesos de fabricación.

encadenamiento rápido

Utilizar la salida de una solicitud de LLM como entrada para la siguiente solicitud para generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en subtareas o para

refinar o ampliar de forma iterativa una respuesta preliminar. Ayuda a mejorar la precisión y la relevancia de las respuestas de un modelo y permite obtener resultados más detallados y personalizados.

seudonimización

El proceso de reemplazar los identificadores personales de un conjunto de datos por valores de marcadores de posición. La seudonimización puede ayudar a proteger la privacidad personal. Los datos seudonimizados siguen considerándose datos personales.

publish/subscribe (pub/sub)

Un patrón que permite las comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un MES basado en microservicios, un microservicio puede publicar mensajes de eventos en un canal al que se puedan suscribir otros microservicios. El sistema puede añadir nuevos microservicios sin cambiar el servicio de publicación.

Q

plan de consulta

Serie de pasos, como instrucciones, que se utilizan para acceder a los datos de un sistema de base de datos relacional SQL.

regresión del plan de consulta

El optimizador de servicios de la base de datos elige un plan menos óptimo que antes de un cambio determinado en el entorno de la base de datos. Los cambios en estadísticas, restricciones, configuración del entorno, enlaces de parámetros de consultas y actualizaciones del motor de base de datos PostgreSQL pueden provocar una regresión del plan.

R

Matriz RACI

Véase responsable, responsable, consultado, informado (RACI).

RAG

Consulte Retrieval Augmented Generation.

ransomware

Software malicioso que se ha diseñado para bloquear el acceso a un sistema informático o a los datos hasta que se efectúe un pago.

Matriz RASCI

Véase responsable, responsable, consultado, informado (RACI).

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

Una copia de una base de datos que se utiliza con fines de solo lectura. Puede enrutar las consultas a la réplica de lectura para reducir la carga en la base de datos principal.

rediseñar

Ver 7 Rs.

objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

objetivo de tiempo de recuperación (RTO)

La demora máxima aceptable entre la interrupción del servicio y el restablecimiento del servicio.

refactorizar

Ver 7 Rs.

Región

Una colección de AWS recursos en un área geográfica. Cada uno Región de AWS está aislado e independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para obtener más información, consulte Regiones de AWS Especificar qué cuenta puede usar.

regresión

Una técnica de ML que predice un valor numérico. Por ejemplo, para resolver el problema de “¿A qué precio se venderá esta casa?”, un modelo de ML podría utilizar un modelo de regresión lineal para predecir el precio de venta de una vivienda en función de datos conocidos sobre ella (por ejemplo, los metros cuadrados).

volver a alojar

Consulte 7 Rs.

versión

En un proceso de implementación, el acto de promover cambios en un entorno de producción.

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resiliencia

La capacidad de una aplicación para resistir las interrupciones o recuperarse de ellas. La alta disponibilidad y la recuperación ante desastres son consideraciones comunes a la hora de planificar la resiliencia en el. Nube de AWS Para obtener más información, consulte Nube de AWS Resiliencia.

política basada en recursos

Una política asociada a un recurso, como un bucket de Amazon S3, un punto de conexión o una clave de cifrado. Este tipo de política especifica a qué entidades principales se les permite el acceso, las acciones compatibles y cualquier otra condición que deba cumplirse.

matriz responsable, confiable, consultada e informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina matriz RASCI y, si la excluye, se denomina matriz RACI.

control receptivo

Un control de seguridad que se ha diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Para obtener más información, consulte Controles receptivos en Implementación de controles de seguridad en AWS.

retain

Consulte 7 Rs.

jubilarse

Ver 7 Rs.

Generación aumentada de recuperación (RAG)

Tecnología de inteligencia artificial generativa en la que un máster hace referencia a una fuente de datos autorizada que se encuentra fuera de sus fuentes de datos de formación antes de generar una respuesta. Por ejemplo, un modelo RAG podría realizar una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para obtener más información, consulte Qué es el RAG.

rotación

Proceso de actualizar periódicamente un secreto para dificultar el acceso de un atacante a las credenciales.

control de acceso por filas y columnas (RCAC)

El uso de expresiones SQL básicas y flexibles que tienen reglas de acceso definidas. El RCAC consta de permisos de fila y máscaras de columnas.

RPO

Consulte el objetivo del punto de recuperación.

RTO

Consulte el objetivo de tiempo de recuperación.

manual de procedimientos

Conjunto de procedimientos manuales o automatizados necesarios para realizar una tarea específica. Por lo general, se diseñan para agilizar las operaciones o los procedimientos repetitivos con altas tasas de error.

S

SAML 2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta función permite el inicio de sesión único (SSO) federado, de modo que los usuarios pueden iniciar sesión AWS

Management Console o llamar a las operaciones de la AWS API sin tener que crear un usuario en IAM para todos los miembros de la organización. Para obtener más información sobre la federación basada en SAML 2.0, consulte Acerca de la federación basada en SAML 2.0 en la documentación de IAM.

SCADA

Consulte el control de supervisión y la adquisición de datos.

SCP

Consulte la política de control de servicios.

secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener más información, consulta ¿Qué hay en un secreto de Secrets Manager? en la documentación de Secrets Manager.

seguridad desde el diseño

Un enfoque de ingeniería de sistemas que tiene en cuenta la seguridad durante todo el proceso de desarrollo.

control de seguridad

Barrera de protección técnica o administrativa que impide, detecta o reduce la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Existen cuatro tipos principales de controles de seguridad: preventivos, de detección, con capacidad de respuesta y proactivos.

refuerzo de la seguridad

Proceso de reducir la superficie expuesta a ataques para hacerla más resistente a los ataques. Esto puede incluir acciones, como la eliminación de los recursos que ya no se necesitan, la implementación de prácticas recomendadas de seguridad consistente en conceder privilegios mínimos o la desactivación de características innecesarias en los archivos de configuración.

sistema de información sobre seguridad y administración de eventos (SIEM)

Herramientas y servicios que combinan sistemas de administración de información sobre seguridad (SIM) y de administración de eventos de seguridad (SEM). Un sistema de SIEM

recopila, monitorea y analiza los datos de servidores, redes, dispositivos y otras fuentes para detectar amenazas y brechas de seguridad y generar alertas.

automatización de la respuesta de seguridad

Una acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o remediarlo. Estas automatizaciones sirven como controles de seguridad detectables o adaptables que le ayudan a implementar las mejores prácticas AWS de seguridad. Algunos ejemplos de acciones de respuesta automatizadas incluyen la modificación de un grupo de seguridad de VPC, la aplicación de parches a una EC2 instancia de Amazon o la rotación de credenciales.

cifrado del servidor

Cifrado de los datos en su destino, por parte de quien Servicio de AWS los recibe.

política de control de servicio (SCP)

Política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPs defina barreras o establezca límites a las acciones que un administrador puede delegar en usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados para especificar qué servicios o acciones están permitidos o prohibidos. Para obtener más información, consulte las políticas de control de servicios en la AWS Organizations documentación.

punto de enlace de servicio

La URL del punto de entrada de un Servicio de AWS. Para conectarse mediante programación a un servicio de destino, puede utilizar un punto de conexión. Para obtener más información, consulte Puntos de conexión de Servicio de AWS en Referencia general de AWS.

acuerdo de nivel de servicio (SLA)

Acuerdo que aclara lo que un equipo de TI se compromete a ofrecer a los clientes, como el tiempo de actividad y el rendimiento del servicio.

indicador de nivel de servicio (SLI)

Medición de un aspecto del rendimiento de un servicio, como la tasa de errores, la disponibilidad o el rendimiento.

objetivo de nivel de servicio (SLO)

Una métrica objetivo que representa el estado de un servicio, medido mediante un indicador de nivel de servicio.

modelo de responsabilidad compartida

Un modelo que describe la responsabilidad que compartes con respecto a la seguridad y AWS el cumplimiento de la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el Modelo de responsabilidad compartida.

SIEM

Consulte la información de seguridad y el sistema de gestión de eventos.

punto único de fallo (SPOF)

Una falla en un único componente crítico de una aplicación que puede interrumpir el sistema.

SLA

Consulte el acuerdo de nivel de servicio.

SLI

Consulte el indicador de nivel de servicio.

SLO

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para obtener más información, consulte Enfoque gradual para modernizar las aplicaciones en el. Nube de AWS

SPOF

Consulte el punto único de falla.

esquema en forma de estrella

Estructura organizativa de una base de datos que utiliza una tabla de hechos grande para almacenar datos medidos o transaccionales y una o más tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para usarse en un almacén de datos o con fines de inteligencia empresarial.

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado. Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue presentado por Martin Fowler como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo con la aplicación de este patrón, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

Un intervalo de direcciones IP en la VPC. Una subred debe residir en una sola zona de disponibilidad.

supervisión, control y adquisición de datos (SCADA)

En la industria manufacturera, un sistema que utiliza hardware y software para monitorear los activos físicos y las operaciones de producción.

cifrado simétrico

Un algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar los datos.

pruebas sintéticas

Probar un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o monitorear el rendimiento. Puede usar Amazon CloudWatch Synthetics para crear estas pruebas.

indicador del sistema

Una técnica para proporcionar contexto, instrucciones o pautas a un LLM para dirigir su comportamiento. Las indicaciones del sistema ayudan a establecer el contexto y las reglas para las interacciones con los usuarios.

T

etiquetas

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. Para obtener más información, consulte Etiquetado de los recursos de AWS.

variable de destino

El valor que intenta predecir en el ML supervisado. Esto también se conoce como variable de resultado. Por ejemplo, en un entorno de fabricación, la variable objetivo podría ser un defecto del producto.

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

Consulte entorno.

entrenamiento

Proporcionar datos de los que pueda aprender su modelo de ML. Los datos de entrenamiento deben contener la respuesta correcta. El algoritmo de aprendizaje encuentra patrones en los datos de entrenamiento que asignan los atributos de los datos de entrada al destino (la respuesta que desea predecir). Genera un modelo de ML que captura estos patrones. Luego, el modelo de ML se puede utilizar para obtener predicciones sobre datos nuevos para los que no se conoce el destino.

puerta de enlace de tránsito

Un centro de tránsito de red que puede usar para interconectar sus VPCs redes con las locales. Para obtener más información, consulte Qué es una pasarela de tránsito en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

Un enfoque en el que los desarrolladores crean y prueban características de forma local en una rama de característica y, a continuación, combinan esos cambios en la rama principal. Luego, la rama principal se adapta a los entornos de desarrollo, preproducción y producción, de forma secuencial.

acceso de confianza

Otorgar permisos a un servicio que especifique para realizar tareas en su organización AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración

por usted. Para obtener más información, consulte AWS Organizations Utilización con otros AWS servicios en la AWS Organizations documentación.

ajuste

Cambiar aspectos de su proceso de formación a fin de mejorar la precisión del modelo de ML. Por ejemplo, puede entrenar el modelo de ML al generar un conjunto de etiquetas, incorporar etiquetas y, luego, repetir estos pasos varias veces con diferentes ajustes para optimizar el modelo.

equipo de dos pizzas

Un DevOps equipo pequeño al que puedes alimentar con dos pizzas. Un equipo formado por dos integrantes garantiza la mejor oportunidad posible de colaboración en el desarrollo de software.

U

incertidumbre

Un concepto que hace referencia a información imprecisa, incompleta o desconocida que puede socavar la fiabilidad de los modelos predictivos de ML. Hay dos tipos de incertidumbre: la incertidumbre epistémica se debe a datos limitados e incompletos, mientras que la incertidumbre aleatoria se debe al ruido y la aleatoriedad inherentes a los datos. Para más información, consulte la guía Cuantificación de la incertidumbre en los sistemas de aprendizaje profundo.

tareas indiferenciadas

También conocido como tareas arduas, es el trabajo que es necesario para crear y operar una aplicación, pero que no proporciona un valor directo al usuario final ni proporciona una ventaja competitiva. Algunos ejemplos de tareas indiferenciadas son la adquisición, el mantenimiento y la planificación de la capacidad.

entornos superiores

Ver entorno.

V

succión

Una operación de mantenimiento de bases de datos que implica limpiar después de las actualizaciones incrementales para recuperar espacio de almacenamiento y mejorar el rendimiento.

control de versión

Procesos y herramientas que realizan un seguimiento de los cambios, como los cambios en el código fuente de un repositorio.

Emparejamiento de VPC

Una conexión entre dos VPCs que le permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulte ¿Qué es una interconexión de VPC? en la documentación de Amazon VPC.

vulnerabilidad

Defecto de software o hardware que pone en peligro la seguridad del sistema.

W

caché caliente

Un búfer caché que contiene datos actuales y relevantes a los que se accede con frecuencia. La instancia de base de datos puede leer desde la caché del búfer, lo que es más rápido que leer desde la memoria principal o el disco.

datos templados

Datos a los que el acceso es infrecuente. Al consultar este tipo de datos, normalmente se aceptan consultas moderadamente lentas.

función de ventana

Función SQL que realiza un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para procesar tareas, como calcular una media móvil o acceder al valor de las filas en función de la posición relativa de la fila actual.

carga de trabajo

Conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.

flujo de trabajo

Grupos funcionales de un proyecto de migración que son responsables de un conjunto específico de tareas. Cada flujo de trabajo es independiente, pero respalda a los demás flujos de trabajo del proyecto. Por ejemplo, el flujo de trabajo de la cartera es responsable de priorizar las aplicaciones, planificar las oleadas y recopilar los metadatos de migración. El flujo de trabajo de la cartera entrega estos recursos al flujo de trabajo de migración, que luego migra los servidores y las aplicaciones.

GUSANO

Mira, escribe una vez, lee muchas.

WQF

Consulte el marco AWS de calificación de la carga de trabajo.

escribe una vez, lee muchas (WORM)

Un modelo de almacenamiento que escribe los datos una sola vez y evita que los datos se eliminen o modifiquen. Los usuarios autorizados pueden leer los datos tantas veces como sea necesario, pero no pueden cambiarlos. Esta infraestructura de almacenamiento de datos se considera inmutable.

Z

ataque de día cero

Un ataque, normalmente de malware, que aprovecha una vulnerabilidad de día cero.

vulnerabilidad de día cero

Un defecto o una vulnerabilidad sin mitigación en un sistema de producción. Los agentes de amenazas pueden usar este tipo de vulnerabilidad para atacar el sistema. Los desarrolladores suelen darse cuenta de la vulnerabilidad a raíz del ataque.

aviso de tiro cero

Proporcionar a un LLM instrucciones para realizar una tarea, pero sin ejemplos (imágenes) que puedan ayudar a guiarla. El LLM debe utilizar sus conocimientos previamente entrenados para

realizar la tarea. La eficacia de las indicaciones cero depende de la complejidad de la tarea y de la calidad de las indicaciones. Consulte también las indicaciones de pocos pasos.

aplicación zombi

Aplicación que utiliza un promedio de CPU y memoria menor al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.