Auditoría de instancias de SQL Server, objetos de base de datos e inicios de sesión en Amazon RDS y Amazon EC2

Recomendaciones de AWS

Recomendaciones de AWS: Auditoría de instancias de SQL Server, objetos de base de datos e inicios de sesión en Amazon RDS y Amazon EC2

Table of Contents

Auditoría de instancias de SQL Server, objetos de base de datos e inicios de sesión en Amazon RDS y Amazon EC2

Ashish Srivastava, Bhavani Akundi y Sreenivas Nettem, Amazon Web Services (AWS)

abril de 2023 (historial de documentos)

En esta guía se explica cómo implementar el proceso de auditoría de SQL Server en Amazon Elastic Compute Cloud (Amazon EC2) y Amazon Relational Database Service (Amazon RDS) para instancias de bases de datos de SQL Server.

La auditoría de bases de datos es un método de auditoría de TI para certificar que los datos de la organización están protegidos. Implica evaluar datos y registrar las principales operaciones empresariales críticas en bases de datos.

La auditoría de bases de datos se ha convertido en obligatoria, especialmente cuando los datos incluyen información de identificación personal (PII) y deben adecuarse a las directrices de seguridad y cumplimiento. Algunas directrices incluyen los tipos de datos y las recomendaciones que emiten las políticas de gobernanza de un país. Un proceso de auditoría requiere pruebas, que se pueden extraer de los registros de bases de datos. La auditoría ayuda a evitar el acceso no autorizado a los datos. Al hacer un seguimiento del uso de los datos, puede investigar si hay actividades falsas y tomar las medidas adecuadas. Las auditorías de bases de datos para garantizar la confidencialidad, integridad y accesibilidad de los datos ayudan a garantizar su protección. Para evitar infracciones de datos, la práctica recomendad es contar con la seguridad y la auditoría de bases de datos.

La auditoría de SQL Server es un requisito para cumplir con estándares de seguridad, financieros y sanitarios, como la ISO/IEC 27001, el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS), BASEL III, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, la Gobernanza de la Información (IG) y la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA).

Resultados empresariales específicos

Las organizaciones implementan la auditoría de SQL Server y bases de datos por varios motivos, entre los que se incluyen los siguientes:

- Los auditores necesitan datos contextuales y significativos para el cumplimiento y la auditoría. Los registros de auditoría de bases de datos son adecuados para los equipos de DBA, pero no para los auditores.
- La capacidad de generar alertas críticas en caso de infracción de seguridad es un requisito básico para el software a gran escala. Puede utilizar los registros de auditoría para este fin, ya que la información de registro ayuda a identificar las comprobaciones de control y hacer un seguimiento de ellas.
- La auditoría de bases de datos proporciona información como la siguiente:
  - ¿Quién accedió a los datos (por ejemplo, DBA, desarrolladores, auditores, procesos de extracción, transformación y carga (ETL) o ingenieros de DevOps)?
  - ¿Cuál era el estado previo de los datos?
  - Cuando se actualizaron los datos, ¿qué se modificó y por qué?
  - ¿Una persona autorizada aprobó la solicitud?
  - ¿Los usuarios internos utilizan sus privilegios correctamente?
- Como los registros de auditoría ayudan a identificar si hay infiltrados, ayudan a disuadir a las personas internas. Es menos probable que las personas que saben que sus acciones son objeto de escrutinio accedan a bases de datos no autorizadas o manipulen datos específicos.
- Las finanzas, la salud, la energía, los servicios de alimentación, las obras públicas y muchos otros sectores necesitan analizar el acceso a los datos y producir informes detallados con regularidad para las agencias gubernamentales. Por ejemplo, las normas de la HIPAA exigen que los proveedores de servicios sanitarios publiquen registros de auditoría en los que se detalle quién accedió a los datos de sus registros, tanto por fila como por registro. El RGPD tiene requisitos similares. La Ley Sarbanes Oxley (SOX) impone una amplia gama de normas contables a las empresas públicas. Estas organizaciones deben analizar el acceso a los datos y producir informes detallados con regularidad.

Descripción general de los niveles y procesos de auditoría de SQL Server

En las siguientes secciones se proporciona información sobre la auditoría de servidor y base de datos, los procesos de auditoría, las ventajas y las desventajas.

Niveles de auditoría

La auditoría se puede llevar a cabo en SQL Server, bases de datos (lo que implica registrar los eventos asociados a las acciones) o ambos niveles.

Auditoría de servidor

Puede utilizar el objeto de SQL Server Audit para auditar y recopilar las acciones que desee supervisar. Puede especificar una sola instancia de acciones y grupos de acciones de servidor. También puede crear varias auditorías para cada instancia de SQL Server.

La auditoría de SQL Server implica parámetros de configuración de servidor, como xp_cmdshell y max server memory. Para más información sobre las configuraciones de memoria de servidor, consulte la documentación de Microsoft SQL Server.

Auditoría de base de datos

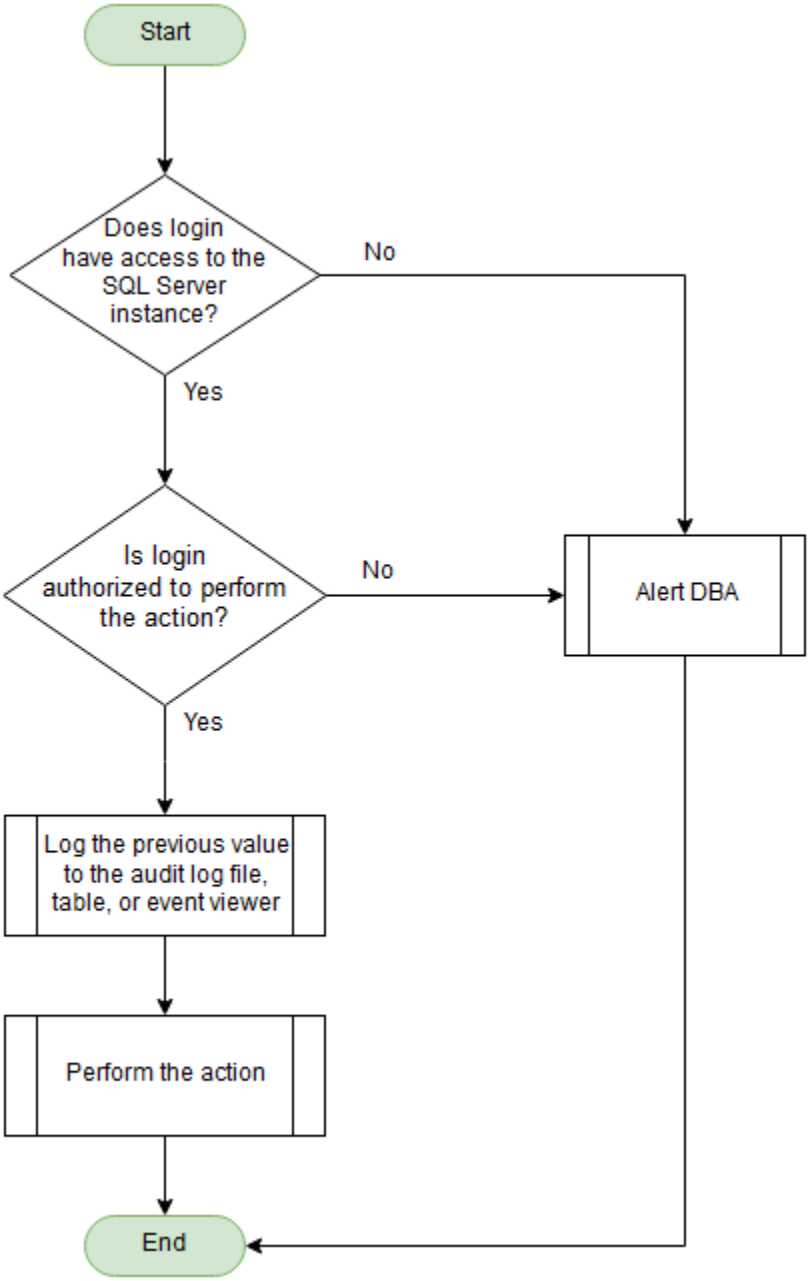
La auditoría de base de datos implica capturar las acciones de los usuarios de la base de datos por motivos de seguridad. Por ejemplo, puede utilizar la auditoría de base de datos para garantizar que los usuarios y procesos no autorizados no puedan acceder a la base de datos y para verificar que se aplican las reglas a fin de restringir cualquier actividad no autorizada. Entre los ejemplos de auditoría de base de datos, se incluyen las capturas de todas las operaciones `INSERT`, `UPDATE`, `DELETE` y `TRIGGERS` en la base de datos.

En esta guía se proporcionan instrucciones y ejemplos de ambos niveles de auditoría.

Diagrama de flujo

En el siguiente diagrama de flujo se ilustra el proceso de auditoría de SQL Server. Cuando un usuario o un proceso inicia sesión en el sistema de base de datos, se validan sus credenciales de

inicio de sesión. Si el inicio de sesión es válido, el proceso de auditoría comprueba la autorización. Si el usuario o el proceso tiene autorización para llevar a cabo la acción, puede completarla. A continuación, los datos auditados se registran en la tabla de auditoría de base de datos.



Ventajas y desventajas de la auditoría

Ventajas

- Ayuda a reducir los incidentes de infracciones de seguridad o cualquier otra acción que pueda resultar en una divulgación no autorizada de información clasificada.
- Ayuda a identificar las deficiencias y vulnerabilidades de seguridad, lo que incluye el acceso ilícito a los recursos, los datos o las operaciones de las bases de datos.
- Proporciona un registro de auditoría de las actividades para que pueda verificar y hacer un seguimiento de todos los tipos de transacciones y procesos, y rastrear las consultas a fin de analizar el rendimiento.
- Hace que las organizaciones rindan más cuentas, ya que pueden revisar la información de auditoría de la que se hizo el seguimiento y proporcionar comentarios para cumplir los objetivos de seguridad y de rendimiento.

Desventajas

- En general, el impacto en el rendimiento es mínimo. Sin embargo, si la auditoría implica un gran volumen de seguimiento de las transacciones, puede requerir recursos adicionales.
- Puede generar demasiados informes y documentos como para verlos, y puede que sea necesario enviar comentarios a distintos equipos de administración y seguridad.
- El consumo de recursos de almacenamiento para almacenar los archivos de auditoría puede ser elevado.
- Se requiere un mantenimiento adicional para archivar o purgar datos de auditoría antiguos, o para mover tablas a otros grupos de archivos de bases de datos o almacenamientos.

Auditoría de instancias de base de datos de Amazon RDS para SQL Server

En esta sección se proporciona información sobre las opciones de auditoría de SQL Server en Amazon RDS, lo que incluye la creación de auditorías, la visualización de los registros de auditorías y la supervisión de los resultados.

Requisitos previos

- Un bucket de Amazon Simple Storage Service (Amazon S3) en el que almacenar los archivos de auditoría
- Un rol de AWS Identity and Access Management (IAM) para acceder al bucket de S3
- Un inicio de sesión en bases de datos con un permiso `ALTER ANY SERVER AUDIT` o `CONTROL SERVER`

Versiones compatibles

- En el caso de Amazon RDS para SQL Server 2014, todas las ediciones admiten auditorías de servidor. La edición Enterprise también admite auditorías de base de datos.
- A partir de SQL Server 2016 (13.x) SP1, todas las ediciones admiten tanto auditorías de nivel de servidor como de nivel de base de datos.
- Amazon RDS admite actualmente las auditorías de SQL Server en todas las Regiones de AWS excepto Medio Oriente (Baréin). Para obtener la información más reciente, consulte Compatibilidad con SQL Server Audit en la documentación de Amazon RDS.

Uso del modo de auditoría C2

El modo de auditoría C2 es un parámetro del grupo de parámetros de base de datos de Amazon RDS para SQL Server. Está deshabilitado de forma predeterminada. Para activarlo, puede actualizar el valor del parámetro a 1. Cuando el modo de auditoría C2 está activado, audita eventos como los inicios de sesión de los usuarios, las llamadas a procedimientos almacenados y la creación y eliminación de objetos. Este modo puede generar grandes cantidades de datos porque lo audita todo, aunque también es posible que no se audite nada.

> **Important**
>
> Microsoft planea eliminar el modo de auditoría C2 en una versión futura de SQL Server. Le recomendamos que evite el uso de esta característica.

Creación y visualización de auditorías

Puede auditar bases de datos de Amazon RDS para SQL Server mediante mecanismos de auditoría de SQL Server integrados que implican la creación de auditorías y especificaciones de auditoría.

- Los registros de auditoría se cargan en un bucket de S3 mediante un rol de IAM que tiene los permisos necesarios para acceder al bucket.
- Puede elegir el rol de IAM, el bucket de S3, la compresión y el periodo de retención al crear el grupo de opciones. El periodo máximo de retención es de 35 días.
- Cree el grupo de opciones y adjúntelo a una instancia de base de datos de Amazon RDS para SQL Server nueva o existente. Los registros de auditoría se almacenan en `D:\rdsdbdata\SQLAudit`.
- Cuando SQL Server termina de escribir en un archivo de registro de auditoría o cuando el archivo alcanza su límite de tamaño, Amazon RDS lo carga en el bucket de S3.
- Si habilita la retención, Amazon RDS mueve el archivo a la carpeta de retención `D:\rdsdbdata\SQLAudit\transmitted`. Los registros de auditoría se conservan en la instancia de base de datos hasta que se carga el archivo de registro de auditoría.
- Para buscar registros de auditoría, también puede consultar `dbo.rds_fn_get_audit_file`.

Para las instancias Multi-AZ, los objetos de especificación de auditoría de base de datos se replican en todos los nodos. La auditoría de servidor y las especificaciones de auditoría de servidor no se replican en todos los nodos, por lo que debe crearlas manualmente.

Configuración del grupo de opciones

Siga estos pasos para configurar un grupo de opciones a fin de llevar a cabo una auditoría de SQL Server en la instancia de base de datos de Amazon RDS para SQL Server. Para obtener instrucciones detalladas, consulte SQL Server Audit en la documentación de Amazon RDS.

- Cree un grupo de opciones.

- Agregue la opción SQLSERVER_AUDIT al grupo de opciones.
- En Destino de S3, cree un nuevo bucket o seleccione uno existente para los registros de auditoría.
- En Rol de IAM, cree un nuevo rol o elija uno existente con las políticas necesarias. Para más información, consulte Creación manual de un rol de IAM para SQL Server Audit en la documentación de IAM.
- Expanda Información adicional y seleccione Habilitar compresión para comprimir los registros de auditoría (recomendado).
- Para conservar los registros de auditoría de la instancia de base de datos, seleccione Habilitar retención y especifique un periodo de retención (hasta un máximo de 35 días).
- Aplique el grupo de opciones a una instancia de base de datos de Amazon RDS para SQL Server nueva o existente.
  - Si se trata de una instancia de base de datos nueva, aplique el grupo de opciones al lanzar la instancia.
  - Para una instancia de base de datos existente, modifique la instancia y adjunte el nuevo grupo de opciones.

Creación de auditorías

Para crear una auditoría de servidor, utilice el siguiente script. Este script crea el archivo de auditoría en la ruta de archivo que especifique. Para ver la sintaxis, argumentos y ejemplos, consulte la documentación de Microsoft SQL Server. Para evitar errores, consulte la lista de limitaciones en la documentación de Amazon RDS.

```
--Creating the server audit
 use master
 GO
 CREATE SERVER AUDIT [Audit-<<servername>>]
 TO FILE  ( FILEPATH = N'D:\rdsdbdata\SQLAudit', MAXSIZE = 2 MB, RESERVE_DISK_SPACE =
 OFF)
 WITH ( QUEUE_DELAY = 1000, ON_FAILURE = CONTINUE)
 GO
-- Enabling the server audit
 ALTER SERVER AUDIT [Audit-<<servername>>] WITH (STATE = ON) ;
 GO
```

Creación de especificaciones de auditoría

Después de crear una auditoría de servidor, puede registrar los eventos de servidor mediante la creación de una especificación de auditoría de servidor con el siguiente código. Esta especificación determina qué se comprobará durante la auditoría de servidor. Para ver la sintaxis, argumentos y ejemplos, consulte la documentación de Microsoft SQL Server. La siguiente especificación audita las acciones de inicios de sesión fallidos y hace un seguimiento de la creación, la alteración y la eliminación de los objetos del servidor. Para obtener una lista de las acciones, consulte la documentación de Microsoft SQL Server.

```
--Creating server audit specification
 USE [master]
 GO
 CREATE SERVER AUDIT SPECIFICATION [Audit-Spec-<<servername>>]
 FOR SERVER AUDIT  [Audit-<<servername>>]
 ADD (FAILED_LOGIN_GROUP), ADD (SERVER_OBJECT_CHANGE_GROUP)
 GO
--Enables the audit
 ALTER SERVER AUDIT [Audit-<<servername>>]
 WITH (STATE = ON);
 GO
```

Puede usar el siguiente código para crear una especificación de auditoría de base de datos que registre eventos de base de datos. En este ejemplo, se auditan las acciones `INSERT`. Para ver la sintaxis, argumentos y más ejemplos, consulte la documentación de Microsoft SQL Server.

```
--Creating database audit specification
 USE [<<DBName>>]
 GO

 CREATE DATABASE AUDIT SPECIFICATION [DatabaseAuditSpecification-<<DBName>>]
 FOR SERVER AUDIT [Audit-<<ServerName>>]
 ADD (INSERT ON DATABASE::[<<DBName>>] BY [dbo])
 WITH (STATE = ON)
 GO
```

Visualización de registros de auditoría

Utilice la siguiente consulta para ver los registros de auditoría. Los registros de auditoría se almacenan en la instancia de base de datos hasta que se cargan en Amazon S3. Si habilita la

retención para la opción SQLSERVER_AUDIT, Amazon RDS mueve el archivo a la carpeta de retención `D:\rdsdbdata\SQLAudit\transmitted`.

También puede cambiar el filtro a `D:\rdsdbdata\SQLAudit\transmitted\*.sqlaudit` para ver los registros de auditoría de la carpeta de retención.

```
--Viewing audit logs
SELECT   *
 FROM     msdb.dbo.rds_fn_get_audit_file
              ('D:\rdsdbdata\SQLAudit\*.sqlaudit'
              , default
              , default )
--Viewing audit logs in retention folder
SELECT   *
 FROM     msdb.dbo.rds_fn_get_audit_file
              ('D:\rdsdbdata\SQLAudit\transmitted\*.sqlaudit'
              , default
              , default )
```

Las opciones adicionales para auditar bases de datos de SQL Server se describen en la siguiente documentación de AWS y Microsoft:

- Eventos extendidos de SQL Server: consulte la publicación del blog de AWS Set up Extended Events in Amazon RDS for SQL Server.
- Desencadenadores de SQL Server: consulte Creación de una regla que se desencadena en función de un evento de Amazon RDS en la documentación de Amazon RDS.
- Seguimiento de cambios: consulte Track data changes en la documentación de Microsoft SQL Server.
- Captura de datos de cambio: consulte Uso de la captura de datos de cambios en la documentación de Amazon RDS.
- Parámetro del modo de auditoría C2: consulte C2 audit mode Server Configuration Option en la documentación de Microsoft SQL Server.

Monitorización

Puede utilizar los flujos de actividad de base de datos para Amazon RDS a fin de integrar los eventos de auditoría de SQL Server con las herramientas de supervisión de la actividad de las bases de

datos de Imperva, McAfee e IBM. Para más información, consulte Auditoría en Microsoft SQL Server en la documentación de Amazon RDS.

Auditoría de SQL Server en instancias de bases de datos personalizadas de Amazon EC2 o Amazon RDS Custom

En esta sección se proporciona información sobre las opciones de auditoría de SQL Server en Amazon EC2 y Amazon RDS Custom, lo que incluye la creación de auditorías de servidores y bases de datos, la visualización de los registros de auditorías y la supervisión de los resultados.

Requisitos previos

- Inicio de sesión en bases de datos con un permiso `ALTER ANY SERVER AUDIT` o `CONTROL SERVER`

Versiones compatibles

- Cualquier edición de SQL Server, versión 2016 y posteriores

Uso del modo de auditoría C2

El modo de auditoría C2 audita eventos como los inicios de sesión de los usuarios, las llamadas a procedimientos almacenados y la creación y eliminación de objetos. Este modo puede generar grandes cantidades de datos porque lo audita todo, aunque también es posible que no se audite nada. Los registros de auditorías C2 se almacenan en el directorio de datos predeterminado de la instancia de SQL Server. El tamaño máximo de cada archivo de registro es de 200 MB Se crea automáticamente un nuevo archivo cuando se llega a este límite. Puede activar las auditorías C2 mediante SQL Server Management Studio. Para más información, consulte la documentación de Microsoft SQL Server.

> **Important**
>
> Microsoft planea eliminar el modo de auditoría C2 en una versión futura de SQL Server. Le recomendamos que evite el uso de esta característica.

Cómo usar el modo de auditoría C2 para auditar los inicios de sesión fallidos:

1. En SQL Server Management Studio, conéctese a la instancia de SQL Server para la que desea habilitar la auditoría.
2. Seleccione la instancia de SQL Server, haga clic en ella con el botón derecho del ratón, elija Propiedades y, a continuación, Seguridad.
3. En Auditorías de inicio de sesión, elija una opción de configuración. Puede auditar solo inicios de sesión fallidos, solo inicios de sesión correctos, ambos o ninguno. (El valor predeterminado es solo inicios de sesión fallidos).
4. En Opciones, seleccione Habilitar el seguimiento de auditorías C2.

Creación y visualización de auditorías

Creación de auditorías de servidor

Una auditoría de servidor en SQL Server recopila las acciones por instancia o base de datos que se deben supervisar. El resultado de la auditoría se guarda en una ruta del archivo de destino de auditorías, en un registro de seguridad de Windows o en un registro de la aplicación.

Cómo crear una auditoría de servidor:

1. En SQL Server Management Studio, en el Explorador de objetos, expanda Seguridad, haga clic con el botón derecho en Auditorías y, a continuación, elija Nueva auditoría. Se creará un nuevo objeto de auditoría de SQL Server para la auditoría del servidor.
2. En Destino de auditoría, elija un archivo, un registro de seguridad o un registro de la aplicación.
3. Si seleccionó un archivo como destino, especifique la ubicación de la carpeta.
4. Configure otras opciones y, a continuación, elija Aceptar.
5. Para activar la auditoría, haga clic con el botón derecho en la nueva configuración de auditoría y, a continuación, elija Habilitar auditoría.

Para más información, consulte la documentación de Microsoft SQL Server.

Creación de especificaciones de auditoría de servidor

La especificación de una auditoría de servidor recopila muchos grupos de acciones del servidor generados por la característica Eventos extendidos de SQL Server. Puede incluir grupos de acciones de auditoría en una especificación de auditoría de servidor. Estas acciones se envían a la auditoría, que las registra en el registro o el archivo de destino.

Cómo crear una especificación de auditoría de servidor:

1. En SQL Server Management Studio, en el Explorador de objetos, expanda Seguridad, haga clic con el botón derecho en Especificaciones de auditoría de servidor y, a continuación, elija Nueva especificación de auditoría de servidor.
2. En Auditoría, elija la auditoría de servidor que creó antes.
3. En Acciones, elija el tipo de acción de auditoría que especifique los grupos de acción de auditoría de servidor y las acciones de auditoría que desea capturar y, a continuación, elija Aceptar.
4. Para activar la especificación de auditoría de servidor, haga clic con el botón derecho en la nueva especificación y, a continuación, elija Habilitar especificación de auditoría de servidor.

Para más información, consulte Create a Server Audit and Server Audit Specification and SQL Server Audit Action Groups and Actions en la documentación de Microsoft SQL Server.

Creación de especificaciones de auditoría de base de datos

Puede crear un objeto de especificación de auditoría de base de datos para la auditoría de base de datos. Esta especificación especifica los grupos de acciones de auditoría de base de datos y las acciones de auditoría que se deben capturar.

Cómo crear una especificación de auditoría de base de datos:

1. En SQL Server Management Studio, en el Explorador de objetos, expanda la base de datos que desee auditar.
2. Expanda la carpeta Seguridad, haga clic con el botón derecho en Especificaciones de auditoría de base de datos y, a continuación, elija Nueva especificación de auditoría de base de datos.
3. En Acciones, configure uno o más tipos de acciones de auditoría de base de datos. Seleccione las instrucciones que desee auditar (como DELETE o INSERT) y la clase de objeto en la que desee llevar a cabo la acción.
4. Cuando haya terminado de seleccionar opciones, elija Aceptar.
5. Para activar la especificación de auditoría de base de datos, haga clic con el botón derecho en la nueva especificación y, a continuación, elija Habilitar especificación de auditoría de base de datos.

Para más información, consulte Create a server audit and database audit specification and SQL Server Audit Action Groups and Actions en la documentación de Microsoft SQL Server.

Visualización de registros de auditoría de SQL Server

Cómo ver registros de auditoría:

1. En SQL Server Management Studio, haga clic con el botón derecho en el objeto de auditoría de SQL Server y, a continuación, elija Ver registros de auditoría.

   El Visor de archivos de registro muestra el registro de auditoría independientemente de su ubicación (un archivo o el registro de eventos de Windows).
2. Para personalizar las entradas de registro que se muestran, elija Filtrar.
3. Para exportar el registro a un archivo de registro, elija Exportar.
4. Cuando haya terminado de ver el registro, elija Cerrar.

Para más información, consulte la documentación de Microsoft SQL Server.

Monitorización

Puede supervisar los registros de auditoría que se registran en un archivo de auditoría, en un registro de aplicaciones o eventos de seguridad o en una tabla de auditorías en la base de datos mediante soluciones de supervisión como Nagios. Una solución de supervisión integrada con un mecanismo de tickets o alertas puede generar alertas e incidentes en tiempo real para notificarlos al administrador del sistema o de la base de datos.

Requisitos de almacenamiento y computación para auditorías

Para Amazon RDS

- Los registros de auditoría se almacenan primero de forma local en la ubicación `D:\rdsdbdata\SQLAudit` del disco. A continuación, Amazon RDS carga estos archivos en un bucket de S3 configurado en el grupo de opciones `SQLSERVER_AUDIT` mediante el rol de IAM especificado.
- Si habilita la retención, Amazon RDS mueve el archivo a la carpeta de retención `D:\rdsdbdata\SQLAudit\transmitted`. Los registros de auditoría se conservan en la instancia de base de datos hasta que se carga el archivo de registro de auditoría a Amazon S3.
- Asegúrese de proporcionar suficiente espacio de almacenamiento para la instancia según el periodo de retención.
- Por lo general, el consumo de CPU para ejecutar auditorías es mínimo. Supervise el uso de CPU al ejecutar consultas de auditoría y ajuste el tamaño de la instancia de base de datos de Amazon RDS en consecuencia. Puede supervisar las métricas de Amazon RDS con Amazon CloudWatch.

Para Amazon EC2

- Asegúrese de que haya suficiente espacio de almacenamiento en la unidad que almacena los archivos de registro de auditoría según el periodo de retención.
- Por lo general, el consumo de CPU para ejecutar auditorías es mínimo. Supervise el uso de CPU al ejecutar consultas de auditoría y ajuste el tamaño de la instancia de EC2 en consecuencia. Puede usar Amazon CloudWatch para supervisar las instancias de EC2.

Prácticas recomendadas para auditorías de SQL Server en AWS

Al auditar las bases de datos de SQL Server en AWS, siga estas prácticas recomendadas.

- Comprenda los requisitos de auditoría. Compruebe si la solución de auditoría debe satisfacer los requisitos de cumplimiento, como el RGPD o la HIPAA. Por ejemplo, es posible que la solución de auditoría deba hacer un seguimiento y registrar todos los cambios hechos en datos críticos, como la información financiera y PII.
- Defina el ámbito de la auditoría. Decida si tiene que auditar todas las instancias de SQL Server o solo las instancias específicas que alojan bases de datos críticas. Determine si tiene que auditar todas las tablas o solo las que contienen datos críticos por base de datos.
- Identifique la lista de eventos que desea registrar y de los que desea hacer un seguimiento. Por ejemplo, la lista de auditoría puede incluir errores de inicio de sesión, cambios en los permisos de inicio de sesión, nuevos inicios de sesión y usuarios, así como inicios de sesión y usuarios eliminados.
- Elija la herramienta de auditoría adecuada. Por ejemplo, si solo desea auditar los eventos de inicio y cierre de sesión, puede utilizar un registro de errores o eventos ampliados. Si desea auditar los cambios en el lenguaje de manipulación de datos (DML), utilice la captura de datos de cambios (CDC), el seguimiento de cambios o las tablas temporales. Si desea auditar los cambios por instancia y base de datos, utilice la característica de auditoría de SQL Server. O bien, puede utilizar una herramienta de auditoría de terceros, como ApexSQL Audit.
- Configure alertas en tiempo real para notificar de forma proactiva a los DBA o al equipo de seguridad cuando una acción específica no satisfaga los requisitos de cumplimiento.
- Revise los datos de auditoría periódicamente mediante la creación de un simple panel o un informe en el que se lean los datos de auditoría y se filtren las acciones que le interesen.
- Configure una alerta para supervisar los cambios hechos en la solución de auditoría.
- Defina políticas de retención para los datos de auditoría en función de los requisitos de la empresa y archive los datos de auditoría antiguos.

Preguntas frecuentes

En esta sección, se proporcionan respuestas a las preguntas frecuentes sobre auditorías de instancias de SQL Server en Amazon RDS y Amazon EC2.

¿Cuáles son los componentes principales de la característica de auditoría de SQL Server?

La característica de auditoría de SQL Server tiene tres componentes principales:

- Los objetos de auditoría de SQL Server definen la ruta para almacenar la información de auditoría, el modo de sincronización de la auditoría, el mecanismo de transferencia del archivo de auditoría y la acción que se debe llevar a cabo en caso de errores de auditoría.
- Las especificaciones de auditoría de servidor hacen un seguimiento de los cambios hechos en la instancia de SQL Server y los eventos generados por la característica Eventos extendidos de SQL Server y los registran.
- Las especificaciones de auditoría de base de datos hacen un seguimiento de los diferentes tipos de acciones efectuadas en la base de datos y los eventos generados por la característica Eventos extendidos de SQL Server y los registran.

¿Cuáles son algunos de los eventos críticos que debería plantearme auditar?

Los eventos críticos incluyen inicios de sesión fallidos y cambios de inicio de sesión, de usuario, de esquema y de auditoría.

¿Por qué es importante auditar los inicios de sesión fallidos y los cambios de inicio de sesión y de usuario?

Por ejemplo, un número excesivo de intentos fallidos de inicio de sesión o cambios en los permisos de los usuarios podría indicar que se está produciendo un ataque.

¿Por qué es importante auditar los cambios de esquema?

Se recomienda hacer un seguimiento de todos los cambios de esquema de la base de datos para detectar cualquier cambio que no esté autorizado.

¿Por qué es importante auditar el sistema de auditoría?

La auditoría de los cambios en la solución de auditoría de SQL Server lo ayuda a atrapar a usuarios no autorizados que podrían estar intentando deshabilitar el proceso de auditoría para llevar a cabo actividades ilegales o no conformes. Esta auditoría también lo ayuda a cumplir con los requisitos de los auditores en cuanto a la integridad de los registros de la solución de auditoría, ya que proporciona pruebas que abarcan todos los escenarios. Otro uso sencillo de esta auditoría es recordar al administrador de la base de datos que debe volver a activar la auditoría si se desactivó por motivos de mantenimiento.

¿Cómo puedo usar los desencadenadores para auditar cambios de base de datos?

Puede crear desencadenadores en tablas que contengan datos críticos para registrar los datos modificados o insertados y comparar los datos antes y después de la modificación. Puede utilizar el desencadenador `INSTEAD OF` para evitar cambios en una tabla específica y registrar la acción fallida.

¿Cuáles son las ventajas y desventajas de usar la CDC para auditar cambios de base de datos? ¿Qué versiones admiten la CDC?

La captura de datos de cambios (CDC) se admite en todas las ediciones de SQL Server 2016 y versiones posteriores. En las versiones anteriores, solo la edición Enterprise admite la CDC.

Estas son algunas ventajas de usar la CDC para auditar los cambios de base de datos:

- Puede usar la CDC como una solución de auditoría asíncrona de SQL Server para hacer un seguimiento de las operaciones de lenguaje de manipulación de datos (DML) en las tablas.

- La CDC hace un seguimiento de las operaciones `INSERT`, `UPDATE` y `DELETE` en las tablas de bases de datos y registran información detallada sobre estos cambios en tablas reflejadas.
- La CDC depende del registro de transacciones de SQL Server como origen de cambios de datos.
- Puede configurar la CDC fácilmente mediante los comandos de Transact-SQL.

Desventajas:

- La CDC no gestiona automáticamente los cambios en el lenguaje de definición de datos (DDL) en las tablas compatibles con la CDC. Se requiere un esfuerzo adicional para reflejar los cambios en el DDL en la tabla de seguimiento.
- La CDC no ofrece ninguna opción para hacer un seguimiento de la instrucción `SELECT`.
- SQL Server mantiene los datos de seguimiento de la CDC en la tabla de cambios solo durante un número de días configurable.
- Los trabajos de la CDC no funcionarán a menos que el servicio de agente de SQL Server esté en ejecución.

Recursos

- SQL Server Audit (documentación de Amazon RDS)
- How to enable auditing for Amazon RDS for SQL Server (taller de Amazon RDS para SQL Server)
- Uso de notificaciones de eventos de Amazon RDS (documentación de Amazon RDS)
- Audit and accountability in Amazon EC2 (documentación de Amazon EC2)
- Migrating SQL Server databases to the Nube de AWS (Guía prescriptiva de AWS)
- Best practices for deploying Microsoft SQL Server on Amazon EC2 (Guía prescriptiva de AWS)

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	—	20 de abril de 2023

Glosario de las Recomendaciones de AWS

Los siguientes son términos de uso común en las estrategias, guías y patrones que se ofrecen en las Recomendaciones de AWS. 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 la base de datos de Oracle en las instalaciones a la Edición de Amazon Aurora compatible con PostgreSQL.
- 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 la base de datos de Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la 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 el sistema de administración de las 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 la base de datos de Oracle en las instalaciones a Oracle en una instancia de EC2 en la 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 en las instalaciones a un servicio en la nube para la misma plataforma. Ejemplo: migre una aplicación de Microsoft Hyper-V 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 administrados.

ACID

Consulte atomicidad, consistencia, aislamiento, 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 una 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 de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función de agregación

Función SQL que actúa en un grupo de filas y calcula un único valor de devolución para el grupo. Entre los ejemplos de funciones de agregación se incluyen `SUM` y `MAX`.

IA

Consulte inteligencia artificial.

AIOps

Consulte 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

Enfoque de seguridad que permite usar exclusivamente 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 se utiliza AIOps en la estrategia de migración de AWS, 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. A fin de obtener más información, consulte ABAC para AWS en la documentación de 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

Ubicación diferenciada de una Región de AWS que está aislada de los errores que se producen en otras zonas de disponibilidad y que brinda conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

AWS Cloud Adoption Framework (AWS CAF)

Marco de directrices y prácticas recomendadas de AWS para ayudar a las empresas a desarrollar un plan eficiente y eficaz a fin de migrar con éxito a la nube de AWS. CAF organiza la orientación en seis áreas de enfoque llamadas perspectivas: empresarial, humana, gobernanza, 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 brinda orientación para el desarrollo, la capacitación y la comunicación de las personas, con el fin de ayudar a preparar 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 Workload Qualification Framework (AWS WQF)

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y brinda 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

bot malicioso

Bot destinado a causar interrupciones o daños a personas u organizaciones.

BCP

Consulte 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. Consulte también endianidad.

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

Estrategia de implementación 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 se ejecuta en el otro entorno (verde). Esta estrategia lo ayuda a hacer reversiones 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 la información de internet. Otros bots, conocidos como bots maliciosos, tienen como objetivo causar interrupciones o daños a personas u organizaciones.

botnet

Redes de bots infectadas por malware y que están bajo el control de una sola parte, conocida como pastor de bots 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 ramas (documentación de GitHub).

acceso de emergencia

En circunstancias excepcionales y mediante un proceso aprobado, un usuario puede acceder rápidamente a una Cuenta de AWS a la que normalmente no tiene permisos para acceder. Para más información, consulte el indicador Implement break-glass procedures en la guía de AWS Well-Architected.

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 AWS Cloud Adoption Framework.

implementación canario

Lanzamiento lento e incremental de una versión para los usuarios finales. Cuando tenga mayor confianza en la nueva versión, la implementa y reemplaza la versión actual en su totalidad.

CCoE

Consulte Centro de excelencia en la nube.

CDC

Consulte 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

Introducción intencionada de fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puede usar AWS Fault Injection Service (AWS FIS) para llevar a cabo experimentos que pongan bajo estrés sus cargas de trabajo de AWS y evalúen su respuesta.

CI/CD

Consulte integración continua y entrega continua.

classification

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 de forma local, antes de que el Servicio de AWS de destino los 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 más información, consulte las publicaciones sobre el CCoE en el blog de estrategia empresarial de la Nube de AWS.

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 relacionada con la tecnología de computación de periferia.

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 siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a la Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realización de inversiones fundamentales para escalar la adopción de la nube (p. ej., crear una zona de aterrizaje, definir un CCoE, 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 publicación The Journey Toward Cloud-First & the Stages of Adoption del blog de estrategia empresarial de la Nube de AWS. Para obtener información sobre cómo se relacionan con la estrategia de migración de AWS, consulte la Guía de preparación para la migración.

CMDB

Consulte base de datos de administración de 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. Algunos repositorios en la nube comunes son GitHub o Bitbucket 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 machine learning para analizar y extraer información de formatos visuales, como imágenes y videos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

deriva de configuración

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

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

Una colección de acciones correctivas y reglas de AWS Config que puede reunir para personalizar sus controles de seguridad y conformidad. Puede implementar un paquete de conformidad como una sola entidad en una región y Cuenta de AWS, o en toda una organización, mediante una plantilla YAML. Para obtener más información, consulte Paquetes de conformidad en la documentación de AWS Config.

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, presentación y producción del proceso de lanzamiento del software. La CI/CD se describe comúnmente como una canalización. La CI/CD puede 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

Consulte 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 Marco de AWS Well-Architected. 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

Marco de arquitectura que proporciona una propiedad de datos distribuida y descentralizada con una administración y una gobernanza centralizadas.

minimización de datos

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

perímetro de datos

Conjunto de barreras de protección en su entorno de AWS que ayudan a garantizar que solo las identidades de confianza accedan a los recursos de confianza desde las redes esperadas. Para más información, consulte Building a data perimeter on 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

Sistema de administración de datos que respalda la inteligencia empresarial, como los análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para las consultas y los 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 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.

defensa en profundidad

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. Cuando se adopta esta estrategia en AWS, se suman varios controles en diferentes capas de la estructura de AWS Organizations para ayudar a proteger los recursos. Por ejemplo, un enfoque de defensa en profundidad podría combinar la autenticación multifactor, la segmentación de la red y el cifrado.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de miembro de AWS a fin de administrar las cuentas de la organización y los permisos para 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 en 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 suelen utilizar para restringir consultas, filtrarlas y etiquetar los 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)

Estrategia y proceso que utiliza para minimizar el tiempo de inactividad y la pérdida de datos a causa de un desastre. Para obtener más información, consulte Recuperación de desastres de cargas de trabajo en AWS: Recuperación en la nube en un marco Well-Architected de AWS.

DML

Consulte 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 desviaciones

Seguimiento de las desviaciones con respecto a una configuración con línea de base. Por ejemplo, puede usar AWS CloudFormation para detectar desviaciones en los recursos del sistema o puede usar AWS Control Tower para detectar cambios en la zona de aterrizaje que podrían afectar al cumplimiento de los requisitos de gobernanza.

DVSM

Consulte asignación de flujos de valor para el desarrollo.

E

EDA

Consulte análisis de datos de tipo exploratorio.

EDI

Consulte 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 la nube, la computación de periferia puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos (EDI)

Intercambio automatizado de documentos comerciales entre organizaciones. Para más información, consulte ¿Qué es el intercambio electrónico de datos?

cifrado

Proceso de computación que transforma datos de texto plano, que son 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.

endpoint

Consulte punto de conexión de 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 de conexión con AWS PrivateLink y conceder permisos a otras

Cuentas de AWS o para entidades principales de 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)

Sistema que automatiza y administra los procesos empresariales clave (como la contabilidad, MES y la administración 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 Cifrado de sobre 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 de seguridad de AWS CAF incluyen la administración 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 hechos

Tabla central de un esquema en estrella. Almacena datos cuantitativos sobre operaciones empresariales. Por lo general, 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.

respuesta rápida a los errores

Filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de los enfoques ágiles.

límite de aislamiento de errores

En la Nube de AWS, límite, como una zona de disponibilidad, una Región de AWS, un plano de control o un plano de datos, que acota el efecto de un error y ayuda a mejorar la resiliencia de las cargas de trabajo. Para más información, consulte AWS Fault Isolation Boundaries.

rama de característica

Consulte rama.

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 más información, consulte Machine learning model interpretability with 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.

peticiones con pocos pasos

Proporcionar a un LLM una pequeña cantidad de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que lleve a cabo una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, mediante el que los modelos aprenden a partir de ejemplos (pasos) incrustados en las peticiones. La técnica de peticiones con pocos pasos puede ser eficaz para las tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también peticiones desde cero.

FGAC

Consulte 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 de cambio 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 modelo fundacional.

modelo fundacional (FM)

Gran red neuronal de aprendizaje profundo que se entrenó con conjuntos de datos masivos de datos generalizados y no etiquetados. Los FM pueden hacer una amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para más información, consulte ¿Qué son los modelos fundacionales?

G

IA generativa

Subconjunto de modelos de IA que se entrenaron con grandes cantidades de datos y que pueden utilizar una simple petición de texto para crear contenido y artefactos nuevos, como imágenes, videos, texto y audio. Para más información, consulte ¿Qué es la IA generativa?

bloqueo geográfico

Consulte 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, consulte Restricción de la distribución geográfica de su contenido en la documentación de CloudFront.

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, mientras que el flujo de trabajo basado en enlaces troncales es el enfoque moderno preferido.

imagen dorada

Instantánea de un sistema o software que se usa 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 la conformidad en todas las unidades organizativas (OU). 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 el uso de AWS Config, AWS Security Hub CSPM, Amazon GuardDuty, AWS Trusted Advisor, Amazon Inspector y comprobaciones de AWS Lambda personalizadas.

H

HA

Consulte 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 de reserva

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de machine learning. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo mediante la comparación de 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, el hotfix suele realizarse fuera del flujo de trabajo típico de las versiones de 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

Consulte infraestructura como código.

políticas basadas en identidad

Una política asociada a una o más entidades principales de IAM que define sus permisos en el entorno de la Nube de AWS.

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

Modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar o modificar la infraestructura existente o aplicarle revisiones. Las infraestructuras inmutables son intrínsecamente más coherentes, fiables y predecibles que las infraestructuras mutables. Para más información, consulte la práctica recomendada Implementación mediante una infraestructura inmutable en el Marco de AWS Well-Architected.

VPC entrante (de entrada)

En una arquitectura de varias cuentas de AWS, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

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

Término que introdujo Klaus Schwab en 2016 para referirse a la modernización de los procesos de fabricación mediante los avances en la conectividad, los datos en tiempo real, la automatización, el análisis, la IA y el ML.

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 (IIoT)

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 del Internet de las cosas industrial (IIoT).

VPC de inspección

En una arquitectura de varias cuentas de AWS, una VPC centralizada que administra las inspecciones del tráfico de red entre VPC (en la misma o en diferentes Regiones de AWS), Internet y las redes en las instalaciones. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su 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 más información, consulte Machine learning model interpretability with 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 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 zona de aterrizaje es un entorno de AWS correctamente diseñado, con varias cuentas, que es 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 de gran tamaño (LLM)

Modelo de IA de aprendizaje profundo que se entrenó previamente con una gran cantidad de datos. Un LLM puede llevar a cabo varias tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para más información, consulte ¿Qué es un LLM (modelo de lenguaje de gran tamaño)?

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

Consulte Las 7 R.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Consulte también endianidad.

LLM

Consulte modelo de lenguaje de gran tamaño.

entornos inferiores

Consulte 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

Consulte rama.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware podría 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 administrados

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

sistema de ejecución de fabricación (MES)

Sistema de software para seguir, supervisar, documentar y controlar los procesos de producción que convierten las materias primas en productos acabados en la zona de producción.

MAP

Consulte Programa de aceleración de la migración.

mecanismo

Proceso completo mediante el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para hacer ajustes. Un mecanismo es un ciclo que se refuerza y mejora por sí mismo a medida que funciona. Para más información, consulte Building mechanisms en el Marco de AWS Well-Architected.

cuenta de miembro

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

MES

Consulte sistema de ejecución de fabricación.

Message Queuing Telemetry Transport (MQTT)

Protocolo de comunicación ligero de máquina a máquina (M2M) que se basa en el patrón de publicación/suscripción y está pensado para dispositivos de IoT con recursos limitados.

microservicio

Un servicio pequeño e independiente que se comunica a través de API bien definidas 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 Integración de microservicios mediante servicios sin servidor de AWS.

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 API ligeras. 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)

Programa de AWS que brinda soporte de consultoría, capacitación y servicios para ayudar a las empresas a construir una base operativa sólida para migrar a la nube y 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 la fábrica de migración suelen incluir operaciones, analistas y propietarios de negocios, ingenieros de migración, desarrolladores y profesionales de DevOps que trabajan en tiempo y forma. 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 las subredes de destino, los grupos de seguridad y las cuentas de AWS.

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: Volver a alojar la migración en Amazon EC2 con AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Herramienta en línea que proporciona información a fin de validar los argumentos comerciales necesarios para migrar a la 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 inicio de sesión) está disponible de forma gratuita para todos los consultores de AWS y los consultores asociados de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de la nube de una organización, identificar los puntos fuertes y débiles, y elaborar un plan de acción para cerrar las brechas identificadas, mediante 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

Enfoque utilizado para migrar una carga de trabajo a la Nube de AWS. Para más información, consulte la entrada Las 7 R de este glosario y también Mobilize your organization to accelerate large-scale migrations.

ML

Consulte machine learning.

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 más información, consulte Strategy for modernizing applications in the 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 más información, consulte Evaluating modernization readiness for applications in the 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.

MPA

Consulte Migration Portfolio Assessment.

MQTT

Consulte Message Queuing Telemetry Transport.

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

Modelo que actualiza y modifica la infraestructura actual para las cargas de trabajo de producción. Para mejorar la coherencia, la fiabilidad y la previsibilidad, el Marco de AWS Well-Architected recomienda usar una infraestructura inmutable.

O

OAC

Consulte control de acceso de origen.

OAI

Consulte identidad de acceso de origen.

OCM

Consulte administración 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

Consulte acuerdo de 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.

Open Process Communications: arquitectura unificada (OPC-UA)

Protocolo de comunicación de máquina a máquina (M2M) para la automatización industrial. OPC-UA establece un estándar de interoperabilidad con esquemas de autenticación, autorización y cifrado 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)

Lista de comprobación de preguntas y prácticas recomendadas asociadas que son útiles para comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles errores. Para más información, consulte Operational Readiness Reviews (ORR) en el Marco de AWS Well-Architected.

tecnología operativa (TO)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En el sector de la fabricación, 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

Registro de seguimiento creado por AWS CloudTrail que registra todos los eventos para todas las Cuentas de AWS en una organización en 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 Creación de un registro de seguimiento para una organización en la documentación de CloudTrail.

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 migración de AWS, este marco se denomina aceleración de personas, debido a la velocidad de cambio requerida en 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 a su contenido de Amazon Simple Storage Service (Amazon S3). El OAC es compatible con todos los buckets de S3 en todas las Regiones de AWS, cifrado del servidor con AWS KMS (SSE-KMS), y solicitudes `PUT` y `DELETE` dinámicas al bucket de S3.

identidad de acceso de origen (OAI)

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

ORR

Consulte revisión de la preparación operativa.

OT

Consulte tecnología operativa.

VPC saliente (de salida)

En una arquitectura de varias cuentas de AWS, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su 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 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 administración del ciclo de vida del producto.

policy

Objeto que puede definir permisos (consulte política basada en identidad), especificar las condiciones de acceso (consulte política basada en recursos) o definir los permisos máximos para todas las cuentas de una organización de AWS Organizations (consulte política de control de servicio).

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

Condición de consulta que devuelve `true` o `false`. En general, se encuentra en una cláusula `WHERE`.

inserción de predicados

Técnica de optimización de consultas en bases de datos que filtra los datos de la consulta antes de transferirlos. Esta técnica reduce la cantidad de datos de la base de datos relacional que se tienen que recuperar y procesar. Además, 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 de AWS que puede realizar acciones y obtener acceso a los recursos. Esta entidad suele ser un usuario raíz de una Cuenta de AWS, un 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

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

zonas alojadas privadas

Contenedor que aloja información acerca de cómo desea que responda Amazon Route 53 a las consultas de DNS de un dominio y sus subdominios en una o varias VPC. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Control de seguridad que se diseñó para evitar la implementación de recursos que no cumplan con la normativa. Estos controles analizan los recursos antes de aprovisionarlos. Si el recurso no cumple con los requisitos del control, no se aprovisiona. Para más información, consulte Controls reference guide en la documentación de AWS Control Tower y consulte Proactive controls en Implementing security controls on AWS.

administración del ciclo de vida del producto (PLM)

Administración 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 la reducción de su uso y su retirada.

entorno de producción

Consulte entorno.

controlador lógico programable (PLC)

En el sector de la fabricación, computadora adaptable y altamente fiable que supervisa las máquinas y automatiza los procesos de fabricación.

encadenamiento de peticiones

Uso de la salida de una petición de LLM como entrada para la siguiente petición a fin de generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en tareas secundarias 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.

publicación/suscripción (pub/sub)

Patrón que permite establecer 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 pueden suscribir otros microservicios. El sistema puede agregar 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

Consulte responsable, fiable, consultada e informada (RACI).

RAG

Consulte generación aumentada por recuperación.

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

Consulte responsable, fiable, consultada e informada (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

Consulte Las 7 R.

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

Consulte Las 7 R.

Región

Conjunto de recursos de AWS que se encuentran en un área geográfica. Cada Región de AWS está aislada y es independiente de las demás para ofrecer tolerancia a errores, estabilidad y resistencia. Para más información, consulte Specify which Regiones de AWS your account can use.

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 Las 7 R.

versión

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

reubicar

Consulte Las 7 R.

redefinir la plataforma

Consulte Las 7 R.

recomprar

Consulte Las 7 R.

resiliencia

Capacidad de una aplicación para resistir interrupciones o recuperarse de ellas. Al planificar la resiliencia en la Nube de AWS, la alta disponibilidad y la recuperación ante desastres son consideraciones comunes. Para más información, consulte Resiliencia en la Nube de AWS.

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 Las 7 R.

retirar

Consulte Las 7 R.

Generación aumentada de recuperación (RAG)

Tecnología de IA generativa mediante la que un LLM hace referencia a un origen de datos autorizado que se encuentra fuera de sus orígenes de datos de entrenamiento antes de generar una respuesta. Por ejemplo, un modelo de RAG podría hacer una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para más información, consulte ¿Qué es RAG (generación aumentada por recuperación)?

rotación

Proceso mediante el que periódicamente se actualiza un secreto para que resulte más difícil que un atacante pueda acceder 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 objetivo de punto de recuperación.

RTO

Consulte 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 identidades (IdP). Esta característica permite el inicio de sesión único (SSO) federado a fin de que los usuarios puedan iniciar sesión en la Consola de administración de AWS o llamar a la API de AWS sin necesidad de crear un usuario de IAM para cada persona 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 control de supervisión y adquisición de datos.

SCP

Consulte política de control de servicio.

secreta

En AWS Secrets Manager, información confidencial o restringida, como una contraseña o credenciales de usuario, que almacena de forma cifrada. Se compone del valor del secreto y de sus metadatos. El valor del secreto puede ser binario, una sola cadena o varias cadenas. Para más información, consulte What's in a Secrets Manager secret? en la documentación de Secrets Manager.

seguridad desde el diseño

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 de controles de seguridad principales: preventivos, de detección, 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

Acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o corregirlo. Estas automatizaciones sirven como controles de seguridad de detección o de respuesta que lo ayudan a implementar las prácticas recomendadas de seguridad de AWS. La modificación de un grupo de seguridad de VPC, la aplicación de revisiones a una instancia de Amazon EC2 o la rotación de credenciales son algunos ejemplos de acciones de respuesta automatizadas.

cifrado del servidor

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

política de control de servicio (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. Las SCP definen barreras de protección o establecen límites a las acciones que un administrador puede delegar en los usuarios o roles. Puede utilizar las SCP como listas de permitidos o rechazados, para especificar qué servicios o acciones se encuentra

permitidos o prohibidos. Para obtener más información, consulte Políticas de control de servicio en la documentación de AWS Organizations.

punto de enlace de servicio

La URL del punto de entrada para 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)

Métrica objetivo que representa el estado de un servicio medido mediante un indicador de nivel de servicio.

modelo de responsabilidad compartida

Modelo que describe la responsabilidad que comparte con AWS en cuanto a la conformidad y la seguridad en 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 sistema de administración de eventos e información de seguridad.

único punto de error (SPOF)

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

SLA

Consulte acuerdo de nivel de servicio.

SLI

Consulte indicador de nivel de servicio.

SLO

Consulte objetivo de nivel de servicio.

modelo de dividir y sembrar

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 más información, consulte Phased approach to modernizing applications in the Nube de AWS.

SPOF

Consulte único punto de error.

esquema en estrella

Estructura organizativa de una base de datos que utiliza una tabla de hechos de gran tamaño para almacenar datos transaccionales o medidos y una o varias tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para utilizarse 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.

control de supervisión y adquisición de datos (SCADA)

En el sector de la fabricación, sistema que utiliza hardware y software para supervisar 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

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

petición del sistema

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

T

etiquetas

Pares de clave y valor que funcionan como metadatos para organizar los recursos de 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

Centro de tránsito de red que puede utilizar para interconectar las VPC y las redes en las instalaciones. Para obtener más información, consulte ¿Qué es una puerta de enlace de tránsito? en la documentación de AWS Transit Gateway.

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

Concesión de permisos a un servicio que especifique para realizar tareas en su empresa en 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 Uso de AWS Organizations con otros servicios de AWS en la documentación de AWS Organizations.

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 pequeño equipo de DevOps 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

Consulte 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.

Interconexión con VPC

Conexión entre dos VPC que 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 hace un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para las tareas de procesamiento, 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.

WORM

Consulte escritura única y lectura múltiple.

WQF

Consulte AWS Workload Qualification Framework.

escritura única y lectura múltiple (WORM)

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

Z

ataque de día cero

Ataque, normalmente de malware, que se aprovecha de 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.

peticiones desde cero

Proporcionar a un LLM instrucciones para llevar a cabo una tarea, pero sin ejemplos (pasos) que puedan ayudar a guiarlo. El LLM debe usar los conocimientos del entrenamiento previo para llevar a cabo la tarea. La eficacia de la petición desde cero depende de la complejidad de la tarea y de la calidad de la petición. Consulte también peticiones con 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.