Las 10 mejores prácticas de seguridad para proteger las copias de seguridad en AWS

AWS Orientación prescriptiva

AWS Orientación prescriptiva: Las 10 mejores prácticas de seguridad para proteger las copias de seguridad en AWS

Table of Contents

Las 10 mejores prácticas de seguridad para proteger las copias de seguridad en AWS

Ibukun (IB) Oyewumi, Amazon Web Services (AWS)

mayo de 2022 (historial de documentos)

La seguridad es una responsabilidad compartida entre Amazon Web Services (AWS) y los clientes. Los clientes han solicitado formas de proteger sus copias de seguridad AWS. Dado que las prácticas de seguridad evolucionan de forma constante a fin de mitigar los nuevos riesgos, es importante que realice evaluaciones de riesgo periódicas para determinar la aplicabilidad de los controles de seguridad y que implemente varias capas de controles para mitigar los riesgos para los datos.

Este documento lo guiará a través de una lista seleccionada de las 10 mejores prácticas de seguridad para proteger sus datos y operaciones de respaldo AWS. Si bien esta guía se centra en las operaciones y los datos de copias de seguridad mediante el servicio AWS Backup, estas principales prácticas de seguridad recomendadas se pueden utilizar con otras soluciones de copia de seguridad, como las herramientas de copia de seguridad de AWS Marketplace.

Prácticas recomendadas

Cuando proteja las copias de seguridad AWS, le recomendamos que utilice el siguiente enfoque:

Temas

Paso 1. Implementar una estrategia de copia de seguridad

Una estrategia de copia de seguridad integral es una parte esencial del plan de protección de datos de una organización para resistir, recuperarse y reducir cualquier impacto producto de un incidente de seguridad. Crear una estrategia de copia de seguridad integral que defina qué datos se deben copiar, con qué frecuencia hacer copias de seguridad de los datos y cómo se monitorearán las tareas de copias de seguridad y de recuperación.

Cuando desarrolle una estrategia integral para realizar copias de seguridad y restaurar datos, identifique primero las interrupciones que puedan producirse y el posible impacto empresarial.

El objetivo es crear una estrategia de recuperación que recupere una carga de trabajo o evite el tiempo de inactividad dentro de los objetivos de recuperación, del objetivo de tiempo de recuperación (RTO) y del objetivo de punto de recuperación (RPO) aceptables. El RTO es la demora aceptable entre la interrupción del servicio y el restablecimiento del servicio. El RPO es la cantidad de tiempo aceptable desde el último punto de recuperación de datos. Considere una estrategia de copia de seguridad detallada que incluya todo lo siguiente:

- Cadencia de copia de seguridad continua
- Point-in-Time Recuperación (PITR)
- Recuperación a nivel de archivos
- Recuperación a nivel de datos de aplicaciones
- Recuperación a nivel de volumen
- Recuperación a nivel de instancia

Ransomware

Una estrategia de copia de seguridad bien diseñada debe incluir acciones que puedan proteger y recuperar recursos del ransomware, con requisitos de recuperación detallados para las aplicaciones y las dependencias de datos. Por ejemplo, al establecer controles preventivos y de detección para mitigar el riesgo del ransomware, asegúrese de diseñar también el nivel de granularidad adecuado para los patrones de copia y restauración entre cuentas Región de AWS o entre cuentas, a fin de garantizar que los administradores no restauren los datos de copia de seguridad corruptos tras un incidente de seguridad.

Requisitos de retención

En algunos sectores, al desarrollar una estrategia de copia de seguridad, también hay que tener en cuenta las normas relativas a los requisitos de retención de datos. Asegúrese de que la estrategia de copia de seguridad esté diseñada con requisitos de retención suficientes para cumplir con las necesidades normativas para cada nivel de clasificación de datos y tipo de recurso.

Conformidad

Consulte a los equipos de conformidad de la seguridad para validar si los recursos y operaciones de copias de seguridad deben incluirse o segmentarse dentro del alcance de los programas de conformidad. Incluir las copias de seguridad y la recuperación como partes fundamentales del programa de seguridad ayuda a comprender dónde se encuentran los datos en un entorno y a definir adecuadamente el alcance de la conformidad.

Para conocer las mejores prácticas de arquitectura para diseñar y operar cargas de trabajo confiables, seguras, eficientes y rentables en la nube, consulte Enfoques de respaldo y recuperación que utilizan el pilar de confiabilidad: AWSAWS Well-Architected Framework.

Paso 2. Incorporar las copias de seguridad en la DR y el BCP

La recuperación de desastres (DR) es el proceso de preparación, respuesta y recuperación ante un desastre. El plan de DR, una parte importante de la estrategia de resistencia, se refiere a la forma en que una carga de trabajo responde ante un desastre. Un desastre puede ser un error técnico, una acción humana o un suceso natural. El plan de continuidad empresarial (BCP) describe cómo una organización pretende continuar con las operaciones comerciales normales durante una interrupción no planificada.

Un plan de recuperación de desastres debe ser un subconjunto del BCP de la organización. El BCP también debe incluir procedimientos. AWS Backup Por ejemplo, un incidente de seguridad que afecte a los datos de producción puede requerir que recurra a un plan de recuperación ante desastres que utiliza la conmutación por error AWS Backup para hacer copias de seguridad de los datos de otra empresa. Región de AWS Asegúrese de que sus empleados estén familiarizados con los procedimientos de su organización y AWS Backup los hayan utilizado adecuadamente, de modo que, en caso de producirse un desastre, la organización pueda continuar con sus operaciones normales con una interrupción mínima o nula del servicio. Encontrará más información sobre su uso AWS Backup en otras secciones de esta guía.

Paso 3. Automatizar las operaciones de copia de seguridad

Los planes de copia de seguridad y las asignaciones de recursos de la organización deben configurarse para reflejar las políticas de protección de datos de la empresa. Al automatizar e implementar políticas de copia de seguridad o planes de copia de seguridad en toda la organización, puede estandarizar y escalar la estrategia de copia de seguridad. Puede utilizar AWS Organizations para automatizar de forma centralizada las políticas de copia de seguridad a fin de implementar, configurar, administrar y controlar la actividad de copia de seguridad en recursos de AWS Backup admitidos mediante la programación de las operaciones de copia de seguridad.

Para mejorar la productividad y controlar las operaciones de infraestructura en entornos con varias cuentas, considere implementar la infraestructura como código (IaC) y una arquitectura basada en eventos como partes esenciales de la estrategia de copia de seguridad y transformación digital. La automatización de las copias de seguridad ofrece las siguientes ventajas:

- Reduce la sobrecarga manual derivada de la laboriosa configuración de copias de seguridad
- Minimiza el riesgo de errores
- Aporta visibilidad en la detección de desviaciones

- Mejora el cumplimiento de las políticas de respaldo en múltiples AWS cargas de trabajo o cuentas

La implementación de políticas de copia de seguridad como código puede ayudar a cumplir con las normas de protección de datos al:

- Configurar diferentes requisitos para los tipos de recursos
- Escalar la estrategia de protección de datos empresariales
- Implementar reglas del ciclo de vida para especificar cuánto tiempo pasará antes de que un punto de recuperación pase a almacenamiento inactivo o se elimine, lo que puede ayudar a optimizar los costos

Al automatizar sus operaciones de respaldo, puede escalar las opciones de asignación de recursos mediante el uso de AWS etiquetas y recursos IDs para identificar automáticamente los AWS recursos que almacenan datos para sus aplicaciones esenciales para la empresa y proteger sus datos mediante copias de seguridad inmutables. Esto puede ayudar a priorizar los controles de seguridad, como los permisos de acceso y los planes o políticas de copia de seguridad.

Paso 4. Implementar mecanismos de control de acceso

Cuando piense en la seguridad en la nube, la estrategia fundamental debe comenzar con una base de identidad sólida para garantizar que el usuario tenga los permisos adecuados para acceder a los datos. La autenticación y la autorización adecuadas pueden reducir el riesgo de eventos de seguridad. El modelo de responsabilidad compartida exige que los AWS clientes implementen políticas de control de acceso. Para crear y gestionar políticas de acceso a escala, puede utilizar AWS Identity and Access Management (IAM).

Para configurar derechos y permisos de acceso, implemente el principio de privilegio mínimo, de modo que cada usuario o sistema que acceda a los datos o a los almacenes de copias de seguridad reciba únicamente los permisos necesarios para llevar a cabo su trabajo. Úselo AWS Backup para establecer políticas de acceso en las bóvedas de respaldo a fin de proteger sus cargas de trabajo en la nube.

Por ejemplo, al implementar políticas de control de acceso, puede conceder a los usuarios acceso para crear planes de copias de seguridad y copias de seguridad bajo demanda, al tiempo que limita la capacidad de eliminar puntos de recuperación. Con las políticas de acceso a los almacenes, puede compartir un almacén de respaldo de destino con una función de origen Cuenta de AWS o

de IAM, según lo requieran las necesidades de su empresa. También puede utilizar las políticas de acceso para compartir un almacén de copias de seguridad con una o varias cuentas o con toda la organización en AWS Organizations. Para obtener más información, consulte la Documentación de AWS Backup.

A medida que vaya escalando sus cargas de trabajo o migrando a AWS ellas, es posible que necesite gestionar de forma centralizada los permisos de sus almacenes y operaciones de backup. Utilice las políticas de control de servicios (SCPs) para implementar un control centralizado sobre el máximo de permisos disponibles para todas las cuentas de su organización. SCPs ofrecen una defensa exhaustiva y garantizan que sus usuarios cumplan con las directrices de control de acceso definidas. Para obtener más información, consulte Administrar el acceso a las copias de seguridad mediante políticas de control de servicios con AWS Backup.

Para mitigar los riesgos de seguridad, como el acceso no deseado a sus recursos y datos de respaldo, utilice IAM Access Analyzer para identificar cualquier función de AWS Backup IAM que comparta con lo siguiente:

- Una entidad externa, como un Cuenta de AWS
- Un usuario raíz
- Un usuario o rol de IAM
- Un usuario federado
- Una Servicio de AWS
- Un usuario anónimo
- Cualquier otra entidad que pueda utilizarse para crear un filtro

Paso 5. Cifrar los datos y el almacén de copias de seguridad

Las organizaciones necesitan mejorar cada vez más sus estrategias de seguridad de datos y es posible que se les exija cumplir con las normas de protección de datos a medida que se reducen horizontalmente en la nube. La correcta implementación de los métodos de cifrado puede aportar una capa de protección adicional sobre los mecanismos básicos de control de acceso. Esta capa adicional ofrece una reducción de riesgos en caso de que las políticas principales de control de acceso no funcionen.

Por ejemplo, si configura políticas de control de acceso demasiado permisivas en datos de AWS Backup , el sistema o el proceso de administración de claves puede reducir el máximo impacto de un

evento de seguridad. Esto se debe a que existen mecanismos de autorización independientes para acceder a los datos y a la clave de cifrado, lo que significa que los datos de las copias de seguridad solo se pueden ver como texto cifrado.

Para aprovechar al máximo el Nube de AWS cifrado, cifre los datos tanto en tránsito como en reposo. Para proteger los datos en tránsito, AWS utiliza las llamadas a la API publicadas para acceder a AWS Backup través de la red mediante el protocolo TLS a fin de proporcionar cifrado entre usted, su aplicación y el AWS Backup servicio. Para proteger los datos en reposo, puedes usar la versión AWS nativa de la nube AWS Key Management Service(AWS KMS) o. AWS CloudHSM En un modelo de seguridad de hardware (HSM) basado en la nube, AWS CloudHSM utiliza el estándar de cifrado avanzado (AES) con claves de 256 bits (AES-256), un algoritmo de cifrado de datos de gran eficacia adoptado por el sector. Evalúe requisitos normativos y de gobernanza de datos y seleccione el servicio de cifrado adecuado para cifrar datos en la nube y en almacenes de copias de seguridad.

La configuración del cifrado varía según el tipo de recurso y las operaciones de copias de seguridad en las distintas cuentas o regiones. Algunos tipos de recursos admiten la capacidad de cifrar las copias de seguridad con una clave de cifrado independiente de la clave empleada para cifrar el recurso de origen. Como usted es responsable de gestionar los controles de acceso para determinar quién puede acceder a sus AWS Backup datos o a las claves de cifrado del almacén y en qué condiciones, utilice el lenguaje normativo que ofrece AWS KMS para definir los controles de acceso de las claves. También puede utilizar AWS Backup Audit Manager para confirmar que la copia de seguridad está correctamente cifrada. Para obtener más información, consulte Cifrado de copias de seguridad en AWS Backup.

Puede utilizar claves de AWS KMS de varias regiones para replicar claves de una región a otra. Las claves de varias regiones están diseñadas para simplificar la administración del cifrado cuando los datos cifrados tienen que copiarse a otras regiones para la recuperación de desastres. Evalúe la necesidad de implementar AWS KMS claves multirregionales como parte de su estrategia general de respaldo.

Paso 6. Proteger las copias de seguridad mediante el almacenamiento inmutable

Las organizaciones pueden utilizar el almacenamiento inmutable para escribir datos en un estado Write Once Read Many (WORM). Cuando están en estado WORM, los datos pueden escribirse una vez y leerse y utilizarse tantas veces como sea necesario una vez confirmados o escritos en el medio

de almacenamiento. El almacenamiento inmutable ayuda a garantizar que se mantenga la integridad de los datos. También ofrece protección contra:

- Eliminaciones
- Sobrescritura
- Acceso involuntario y no autorizado
- Compromiso de ransomware

El almacenamiento inmutable ofrece un mecanismo eficaz para abordar los posibles eventos de seguridad que podrían tener un impacto real en las operaciones empresariales.

Puede utilizar el almacenamiento inmutable para una mejor gobernanza si se combina con fuertes restricciones de SCP. También puede utilizar el almacenamiento inmutable en un modo WORM de conformidad cuando las normas legales (por ejemplo, una retención legal) requieren el acceso a datos inmutables.

Para mantener la disponibilidad e integridad de los datos, puede utilizar AWS Backup Vault Lock para proteger las copias de seguridad. Cuando utilizas AWS Backup Vault Lock, las entidades no autorizadas no pueden borrar, alterar ni dañar los datos de tus clientes o de tu empresa durante el período de retención requerido. AWS Backup Vault Lock le ayuda a cumplir las políticas de protección de datos de su organización al evitar lo siguiente:

- Eliminaciones por parte de usuarios privilegiados (incluido el usuario Cuenta de AWS root)
- Cambios en la configuración del ciclo de vida de las copias de seguridad
- Actualizaciones que alteran el periodo de retención definido

AWS Backup Vault Lock garantiza la inmutabilidad y añade una capa de defensa adicional que protege las copias de seguridad (puntos de recuperación) de las bóvedas de copias de seguridad. Esto resulta especialmente útil en sectores altamente regulados que tienen requisitos estrictos de integridad en lo que respecta a las copias de seguridad y los archivos. AWS Backup Vault Lock se asegura de que tus datos se conserven junto con una copia de seguridad de la que poder recuperarlos en caso de que se produzcan acciones involuntarias o malintencionadas.

Important

- AWS Backup Aún no se ha evaluado el cumplimiento de la regla 17a-4 (f) de la Comisión de Bolsa y Valores (SEC) y de la Comisión de Comercio de Futuros de Productos Básicos (CFTC) en la regulación 17 del C.F.R. 1.31 (b) a (c).
- AWS Backup Vault Lock entra en vigor de forma inmediata. Cuenta con un periodo de reflexión mínimo de tres días (72 horas) para eliminar o actualizar la configuración antes de que bloquee de forma permanente el almacén. Si lo desea, puede ampliar la duración de este periodo de reflexión. Utilice este período de reflexión para probar AWS Backup Vault Lock con sus cargas de trabajo y casos de uso. Una vez transcurrido el período de reflexión, ni usted AWS Support podrá eliminar ni modificar AWS Backup Vault Lock ni el contenido de su depósito cerrado. Para obtener más información, consulte la documentación en AWS Backup Vault Lock.

Paso 7. Implementar el monitoreo y las alertas de copias de seguridad

Los trabajos de copia de seguridad pueden tener errores. Un trabajo con errores, como una tarea de copia de seguridad, restauración o copia, puede afectar a los pasos posteriores de un proceso. Cuando se produce un error en el trabajo de copia de seguridad inicial, existe una alta probabilidad de que esto también suceda en otras tareas sucesivas. En este escenario, la mejor manera de comprender el curso de los eventos es mediante el monitoreo y la notificación. El monitoreo y las alertas pueden aportar a la organización información sobre las tareas de copia de seguridad, lo cual ayuda a responder a los errores de las copias de seguridad.

Activar y configurar las notificaciones para monitorear trabajos de AWS Backup ofrece las siguientes ventajas:

- Permite que conozca sus actividades de copia de seguridad
- Ayuda a garantizar el cumplimiento de los acuerdos de nivel de servicio esenciales () SLAs
- Mejora su supervisión business-as-usual
- Ayuda a cumplir con las obligaciones de conformidad

Puede implementar el monitoreo de respaldo para sus cargas de trabajo integrándolo AWS Backup con otros sistemas Servicios de AWS y sistemas de emisión de tickets para llevar a cabo flujos automatizados de investigación y escalamiento. Por ejemplo, puede hacer lo siguiente:

- Usa Amazon CloudWatch para realizar un seguimiento de las métricas, crear alarmas y ver los paneles.
- Usa Amazon EventBridge para monitorear AWS Backup procesos y eventos.
- Utilice AWS CloudTrail para monitorear llamadas de API de AWS Backup con información detallada sobre la hora, la IP de origen, los usuarios y las cuentas que realizan estas llamadas.
- Utilice Amazon Simple Notification Service (Amazon SNS) para suscribirse AWS Backup a temas relacionados, como eventos de copia de seguridad, restauración y copia.

Puede usar AWS Backup Audit Manager para generar automáticamente evidencia de sus informes de auditoría de respaldo diarios para cada cuenta y región. También puede ampliar la supervisión de las copias de seguridad entre varias cuentas mediante un conjunto de plantillas y paneles de automatización (lo que se conoce como la solución de observación de copias de seguridad) para obtener informes agregados diarios y AWS Backup multirregionales entre cuentas.

Paso 8. Auditar la configuración de copias de seguridad

Para garantizar que el programa de respaldo funcione como debería y para identificar y corregir cualquier anomalía en los procesos de respaldo, audite el cumplimiento de AWS Backup las políticas comparándolo con los controles definidos, como la frecuencia de respaldo definida. Para encontrar e investigar las operaciones o recursos de copias de seguridad que no cumplan con los requisitos de la empresa, realice un seguimiento continuo y automático de la actividad de copias de seguridad y genere informes automáticos.

AWS Backup Audit Manager proporciona controles de conformidad integrados y personalizables que se alinean con los requisitos normativos y de conformidad de su empresa. Puede utilizar controles prediseñados y personalizables como marcos de auditoría para evaluar las prácticas de AWS Backup . Los controles incluyen:

- Recursos de copias de seguridad protegidos por planes de copia de seguridad
- Frecuencia mínima y retención mínima del plan de copia de seguridad
- Cifrado del punto de recuperación de copias de seguridad
- Eliminación manual del punto de recuperación de copias de seguridad

- Retención mínima del punto de recuperación de copias de seguridad
- Copia entre regiones
- Copia entre cuentas
- Bloqueo del almacén de copias de seguridad

Para la automatización de la infraestructura como código (IaC), puede utilizar AWS Backup Audit Manager con. AWS CloudFormation

AWS Security Hub CSPMle proporciona una visión completa del estado de su seguridad en. AWS También ayuda a verificar si un entorno cumple con las prácticas recomendadas de seguridad y los estándares del sector, como Controles fundamentales de las prácticas recomendadas de seguridad de AWS. Si utiliza Security Hub CSPM en su entorno de nube, le recomendamos que habilite el estándar AWS Foundational Security Best Practices, ya que incluye controles de detección que pueden ayudar a proteger las copias de seguridad. AWS La mayoría de los controles de detección de AWS Backup Audit Manager y Security Hub CSPM también están disponibles como reglas AWS Config gestionadas.

Paso 9. Probar las capacidades de recuperación de datos

La estrategia de copia de seguridad debe incluir la prueba de sus copias de seguridad. Una estrategia de copia de seguridad no es efectiva si los datos respaldados no se pueden restaurar. Pruebe periódicamente la capacidad para encontrar ciertos puntos de recuperación y restaurarlos.

Si bien copia AWS Backup automáticamente las etiquetas de los recursos que protege a los puntos de recuperación, las etiquetas no se copian de forma predeterminada desde los puntos de recuperación a los recursos restaurados correspondientes. Para ampliar la gestión del inventario y localizar los puntos de recuperación, considere la posibilidad de utilizar AWS Backup eventos para iniciar un proceso de replicación de etiquetas en los recursos creados por las tareas de AWS Backup restauración.

Puede iniciar un flujo de trabajo de recuperación de datos al establecer patrones de recuperación de datos y, a continuación, probarlos periódicamente. Para aumentar la confianza en su capacidad de recuperar datos de las copias de seguridad, cree un proceso básico y repetible para realizar pruebas continuas de recuperación de datos. Por ejemplo, puede crear un patrón para probar una operación de restauración entre cuentas y regiones desde un almacén central de copias de seguridad de recuperación de desastres cifrado con una clave de AWS KMS administrada por el

cliente a un almacén de copias de seguridad de una cuenta de origen cifrada con otra clave de AWS KMS administrada por el cliente.

Si no pruebas este tipo de operaciones de restauración con frecuencia, es posible que descubras que tus suposiciones sobre el AWS KMS cifrado de las operaciones entre cuentas y regiones son incorrectas. A menudo, el único patrón de recuperación de copias de seguridad que realmente funciona es la ruta que se prueba con frecuencia. Mediante pruebas rutinarias de los tipos de recursos de copias de seguridad compatibles puede detectar alertas tempranas que podrían provocar interrupciones en el futuro y la pérdida de datos críticos. Si es posible, mantenga un número limitado, pero factible de rutas y patrones de recuperación para evitar el desperdicio de espacio de almacenamiento, optimizar los costos y ahorrar tiempo. Solucionar el problema cuando se produce un error en una prueba de recuperación es más fácil que perder datos valiosos o críticos.

Paso 10. Incorporar copias de seguridad en un plan de respuesta a incidentes

Las simulaciones de respuesta a incidentes de seguridad (SIRS) son eventos internos que brindan una oportunidad estructurada para poner en práctica el plan y los procedimientos de respuesta a incidentes en un escenario realista. Resulta útil poner a prueba los datos y las operaciones de las copias de seguridad en actividades creativas de las SIRS para estar preparado ante cualquier imprevisto. Esto ayuda a validar su nivel de preparación organizacional y a sentirse cómodo ante situaciones excepcionales e inesperadas. Las simulaciones deben ser realistas y deben incluir equipos organizacionales multifuncionales que estén obligados a responder a los eventos.

Comience con ejercicios de simulación básicos y avance hacia un evento completo y complejo. Por ejemplo, puede crear un modelo realista que consista en una nube privada virtual (VPC) y los recursos asociados que simulen una sobreexposición involuntaria de información o una posible filtración de datos provocada por cambios en las políticas y en las listas de control de acceso. Para evaluar qué tan bien funcionó un plan de respuesta a incidentes, registre las lecciones aprendidas e identifique las mejoras que deben realizarse en los procedimientos de respuesta futuros.

Se puede utilizar AWS Backup para configurar copias de seguridad automatizadas a nivel de instancia como Amazon Machine Images (AMIs) y copias de seguridad a nivel de volumen como instantáneas de varios. Cuentas de AWS Esto puede ayudar a los equipos de respuesta a incidentes a mejorar los procesos de investigación, como la recopilación automatizada de discos forenses, al brindar un punto de restauración que podría reducir el alcance y el impacto de posibles eventos de seguridad, como el ransomware.

Pasos a seguir a continuación

En esta guía se describen las 10 mejores prácticas y controles de seguridad para proteger los datos de las copias de seguridad AWS. Sugerimos utilizar estas prácticas recomendadas para diseñar e implementar una estrategia y una arquitectura de copia de seguridad y recuperación, con varias capas de control, con el objetivo de escalar y satisfacer las necesidades de la empresa. Para obtener más información al respecto AWS Backup, consulte la AWS Backup documentación.

Si tiene preguntas acerca de esta guía, inicie un nuevo hilo en el foro de AWS Backup o contacte con AWS Support.

Recursos

AWS Guía prescriptiva

- Enfoques para copia de seguridad y recuperación en AWS (guía)

AWS documentación

- AWS Backup
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon EventBridge
- IAM
- AWS KMS
- AWS Organizations
- AWS Security Hub CSPM
- Amazon SNS

Publicaciones de blog

- Automatice el respaldo centralizado a escala mediante el Servicios de AWS uso AWS Backup
- Comienza la arquitectura de recuperación ante desastres (DR) AWS, primera parte: Estrategias de recuperación en la nube
- La importancia del cifrado y cómo AWS puede ayudar
- Mejore la seguridad de sus copias de seguridad con AWS Backup Vault Lock
- Supervise, evalúe y demuestre el cumplimiento de las normas de Backup con AWS Backup Audit Manager
- Cree y comparta copias de seguridad cifradas entre cuentas y regiones mediante AWS Backup

- Simplifique la auditoría de sus políticas de protección de datos con AWS Backup Audit Manager
- Gestione el acceso a las copias de seguridad mediante políticas de control de servicios con AWS Backup
- Obtenga informes agregados diarios entre cuentas y regiones AWS Backup

GitHub repositorios

Los siguientes repositorios de código le proporcionan una solución de administración e implementación para implementar el respaldo y la recuperación AWS Backup en toda su AWS Organizations organización, que abarca varias cuentas y. Regiones de AWS

- Implemente utilizando AWS BackupAWS
- Implemente AWS Backup mediante canalizaciones de CI/CD

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	—	13 de mayo de 2022

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