Le 10 migliori pratiche di sicurezza per proteggere i backup in AWS

AWS Linee guida prescrittive

AWS Linee guida prescrittive: Le 10 migliori pratiche di sicurezza per proteggere i backup in AWS

Table of Contents

Le 10 migliori pratiche di sicurezza per proteggere i backup in AWS

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

Maggio 2022 (cronologia dei documenti)

La sicurezza è una responsabilità condivisa tra Amazon Web Services (AWS) e i clienti. I clienti hanno chiesto modi per proteggere i propri backup in. AWS Poiché le pratiche di sicurezza si evolvono costantemente per mitigare nuovi rischi, è importante condurre valutazioni periodiche dei rischi per determinare l'applicabilità dei controlli di sicurezza e implementare più livelli di controlli per mitigare i rischi per i dati.

Questo documento ti guiderà attraverso un elenco curato delle 10 migliori pratiche di sicurezza per proteggere i dati e le operazioni di backup. AWS Sebbene questa guida si concentri sui dati e sulle operazioni di backup utilizzando il servizio AWS Backup, queste best practice di sicurezza consigliate possono essere utilizzate con altre soluzioni di backup, come gli strumenti di backup del Marketplace AWS.

Best practice

Quando si proteggono i backup in AWS, si consiglia di utilizzare il seguente approccio:

Argomenti

Passaggio 1. Implementazione di una strategia di backup

Una strategia di backup completa è una parte essenziale del piano di protezione dei dati di un'organizzazione per resistere a, ripristinare e ridurre qualsiasi impatto che potrebbe essere sostenuto a causa di un evento di sicurezza. Crea una strategia di backup completa che definisca quali dati devono essere sottoposti a backup, con che frequenza devono essere sottoposti a backup e in che modo verranno monitorate le attività di backup e ripristino.

Quando si sviluppa una strategia completa per il backup e il ripristino dei dati, è necessario innanzitutto identificare le interruzioni che potrebbero verificarsi e il loro potenziale impatto aziendale.

Il tuo obiettivo è creare una strategia di ripristino che ripristini il carico di lavoro o eviti i tempi di inattività entro gli obiettivi di ripristino accettabili, obiettivo del tempo di ripristino (RTO) e obiettivo del punto di ripristino (RPO). L'RTO è il ritardo accettabile tra l'interruzione del servizio e il ripristino del servizio. L'RPO è il periodo di tempo accettabile dall'ultimo punto di ripristino dei dati. Prendi in considerazione una strategia di backup granulare che includa tutti i seguenti elementi:

- Cadenza di backup continua

- Point-in-Time Ripristino (PITR)
- Ripristino a livello di file
- Ripristino a livello di dati delle applicazioni
- Ripristino a livello di volume
- Ripristino a livello di istanza

Ransomware

Una strategia di backup ben progettata dovrebbe includere azioni in grado di proteggere e ripristinare le risorse dai ransomware, con requisiti di ripristino dettagliati per le applicazioni e le relative dipendenze dei dati. Ad esempio, mentre stabilisci controlli preventivi e investigativi per mitigare il rischio di ransomware, assicurati di progettare anche il livello di granularità appropriato per i modelli di copia e ripristino tra Regione AWS o più account, per garantire che gli amministratori non ripristinino i dati di backup danneggiati dopo l'evento di sicurezza.

Requisiti di conservazione

In alcuni settori, quando si sviluppa una strategia di backup, è necessario considerare anche le normative relative ai requisiti di conservazione dei dati. Assicurati che la tua strategia di backup sia progettata con requisiti di conservazione sufficienti a soddisfare le esigenze normative per ogni livello di classificazione dei dati e tipo di risorsa.

Conformità

Consulta i tuoi team addetti alla conformità alla sicurezza per verificare se le risorse e le operazioni di backup debbano essere incluse o segmentate dall'ambito dei programmi di conformità. Includere il backup e il ripristino come parte fondamentale del programma di sicurezza ti aiuterà a capire dove si trovano i dati nell'ambiente e a definire in modo appropriato l'ambito di conformità.

Per le migliori pratiche architettoniche per la progettazione e la gestione di carichi di lavoro affidabili, sicuri, efficienti ed economici nel cloud, vedi Approcci di backup e ripristino utilizzando AWS and Reliability Pillar — AWS Well-Architected Framework.

Passaggio 2. Incorporare il backup nel ripristino di emergenza e nel piano di continuità aziendale

Il ripristino di emergenza (DR) è il processo di preparazione a, risposta a e ripristino di una condizione di emergenza. Parte importante della strategia di resilienza, il piano di ripristino di emergenza riguarda la risposta del carico di lavoro in caso di emergenza. Un'emergenza potrebbe essere un guasto tecnico, un'azione umana o un evento naturale. Il Piano di continuità aziendale (BCP) descrive in che modo un'organizzazione intende continuare le normali operazioni aziendali durante un'interruzione non pianificata.

Il piano di ripristino di emergenza deve essere un sottoinsieme del piano di continuità aziendale dell'organizzazione. Il BCP dovrebbe includere anche delle procedure. AWS Backup Ad esempio, un evento di sicurezza che influisce sui dati di produzione potrebbe richiedere l'attivazione di un piano di DR che utilizzi il failover AWS Backup per eseguire il backup dei dati da un altro. Regione AWS Assicuratevi che i vostri dipendenti conoscano le procedure organizzative e ne abbiano fatto pratica, in modo che, in caso di emergenza, l' AWS Backup organizzazione possa continuare le normali operazioni con interruzioni del servizio minime o nulle. Ulteriori informazioni sull'utilizzo AWS Backup sono disponibili in altre sezioni di questa guida.

Fase 3. Automatizzazione delle attività di backup

I piani di backup e l'assegnazione delle risorse dell'organizzazione devono essere configurati in modo da riflettere le policy di protezione dei dati aziendali. Automatizzando e implementando policy di backup o piani di backup a livello di organizzazione, è possibile standardizzare e dimensionare la strategia di backup. Puoi utilizzare AWS Organizations per automatizzare centralmente le policy di backup per implementare, configurare, gestire e governare le attività di backup tra risorse di AWS Backup supportate pianificando le operazioni di backup.

Per migliorare la produttività e gestire le operazioni dell'infrastruttura in ambienti con più account, prendi in considerazione l'implementazione dell'infrastruttura come codice (IaC) e dell'architettura basata sugli eventi come parti essenziali della tua strategia di trasformazione digitale e backup. L'automazione dei backup offre i seguenti vantaggi:

- Riduce la gestione manuale della configurazione onerosa in termini di tempo dei backup
- Riduce al minimo il rischio di errori
- Fornisce visibilità sul rilevamento delle deviazioni

- Migliora la conformità alle policy di backup su più AWS carichi di lavoro o account

L'implementazione delle policy di backup sotto forma di codice può aiutarti a rispettare le normative sulla protezione dei dati effettuando le seguenti operazioni:

- Configurare requisiti diversi per i tipi di risorse
- Dimensionare la strategia di protezione dei dati aziendali
- Implementare regole del ciclo di vita per specificare quanto tempo occorre prima che un punto di ripristino passi alla conservazione a freddo o venga eliminato, il che può contribuire a ottimizzare i costi

Quando si automatizzano le operazioni di backup, è possibile scalare le opzioni di assegnazione delle risorse utilizzando AWS tag e risorse IDs per identificare automaticamente AWS le risorse che archiviano i dati per le applicazioni aziendali critiche e proteggere i dati utilizzando backup immutabili. Questo può aiutarti a dare priorità ai controlli di sicurezza, come le autorizzazioni di accesso e i piani o le policy di backup.

Passaggio 4. Implementazione di meccanismi di controllo dell'accesso

Quando si pensa alla sicurezza nel cloud, la strategia di base dovrebbe iniziare con una solida base di identità per garantire che l'utente disponga delle autorizzazioni giuste per accedere ai dati. L'autenticazione e l'autorizzazione appropriate possono mitigare il rischio di eventi di sicurezza. Il modello di responsabilità condivisa richiede AWS ai clienti di implementare politiche di controllo degli accessi. Per creare e gestire policy di accesso su larga scala, puoi usare AWS Identity and Access Management (IAM).

Per gli scopi di configurazione dei diritti di accesso e delle autorizzazioni, implementa il principio del privilegio minimo e assicurati che a ogni utente o sistema che accede ai dati di backup o al vault vengano fornite solo le autorizzazioni necessarie per svolgere il lavoro. Utilizzalo AWS Backup per impostare le policy di accesso negli archivi di backup per proteggere i carichi di lavoro nel cloud.

Ad esempio, implementando policy di controllo dell'accesso, puoi concedere agli utenti l'accesso per creare piani di backup e backup su richiesta, limitando al contempo la loro capacità di eliminare i punti di ripristino. Utilizzando le policy di accesso al vault, è possibile condividere un vault di backup di destinazione con un ruolo di origine Account AWS o IAM, in base alle esigenze aziendali.

Puoi anche utilizzare le policy di accesso per condividere un archivio di backup con uno o più account o con l'intera organizzazione in AWS Organizations. Per ulteriori informazioni, consulta la documentazione relativa ad AWS Backup.

Man mano che ridimensionate i carichi di lavoro o effettuate la migrazione AWS, potrebbe essere necessario gestire centralmente le autorizzazioni per i vault e le operazioni di backup. Utilizza le policy di controllo dei servizi (SCPs) per implementare il controllo centralizzato sulle autorizzazioni massime disponibili per tutti gli account dell'organizzazione. SCPs offrono una difesa approfondita e garantiscono che gli utenti rispettino le linee guida definite per il controllo degli accessi. Per ulteriori informazioni, consulta la sezione Gestione dell'accesso ai backup utilizzando le policy di controllo del servizio con AWS Backup.

Per mitigare i rischi per la sicurezza, come l'accesso involontario alle risorse e ai dati di backup, utilizza IAM Access Analyzer per identificare qualsiasi ruolo AWS Backup IAM condiviso con quanto segue:

- Un'entità esterna come Account AWS
- Un utente root
- Un utente o ruolo IAM
- Un utente federato
- Un Servizio AWS
- Un utente anonimo
- Qualsiasi altra entità che potrebbe essere utilizzata per creare un filtro

Fase 5. Crittografia dei dati di backup e del vault

Le organizzazioni hanno sempre più bisogno di migliorare la propria strategia di sicurezza dei dati e potrebbe essere richiesto loro di rispettare le normative sulla protezione dei dati man mano che si ridimensionano nel cloud. La corretta implementazione dei metodi di crittografia possono offrire un ulteriore livello di protezione rispetto ai meccanismi di controllo degli accessi di base. Questo livello aggiunto consente la mitigazione in caso di fallimento delle policy di controllo dell'accesso principali.

Ad esempio, se configuri policy di controllo dell'accesso eccessivamente permissive sui tuoi dati di AWS Backup , il sistema o il processo di gestione delle chiavi possono mitigare l'impatto massimo di un evento di sicurezza. Questo perché esistono meccanismi di autorizzazione separati per accedere

ai dati e alla chiave di crittografia, il che significa che i dati di backup sono visualizzabili solo come testo cifrato.

Per ottenere il massimo dalla Cloud AWS crittografia, crittografa i dati sia in transito che a riposo. Per proteggere i dati in transito, AWS utilizza chiamate API pubblicate per accedere AWS Backup attraverso la rete utilizzando il protocollo TLS per fornire la crittografia tra l'utente, l'applicazione e il AWS Backup servizio. Per proteggere i dati inattivi, puoi utilizzare AWS cloud-native AWS Key Management Service()AWS KMS o. AWS CloudHSM Un modello di sicurezza hardware (HSM) basato sul cloud, AWS CloudHSM utilizza Advanced Encryption Standard (AES) con chiavi a 256 bit (AES-256), un potente algoritmo adottato dal settore per la crittografia dei dati. Valuta i requisiti normativi e di governance dei dati e seleziona il servizio di crittografia appropriato per crittografare i dati cloud e gli archivi di backup.

La configurazione della crittografia varia a seconda del tipo di risorsa e delle operazioni di backup tra account o regioni. Alcuni tipi di risorse supportano la possibilità di crittografare i backup con una chiave di crittografia separata da quella usata per crittografare la risorsa di origine. Poiché sei responsabile della gestione dei controlli di accesso per determinare chi può accedere ai tuoi AWS Backup dati o alle chiavi di crittografia del vault e a quali condizioni, utilizza il linguaggio delle policy offerto da AWS KMS per definire i controlli di accesso sulle chiavi. Puoi anche utilizzare AWS Backup Audit Manager per confermare che il backup sia crittografato correttamente. Per ulteriori informazioni, consulta la sezione Crittografia dei backup in AWS Backup.

Puoi utilizzare le chiavi multi-regione di AWS KMS per replicare le chiavi da una regione all'altra. Le chiavi multi-regione sono progettate per semplificare la gestione della crittografia quando i dati crittografati devono essere copiati in altre regioni per il ripristino di emergenza. Valuta la necessità di implementare AWS KMS chiavi multiregionali come parte della tua strategia di backup complessiva.

Fase 6. Protezione dei backup utilizzando un archivio immutabile

Le organizzazioni possono utilizzare l'archivio immutabile per scrivere dati in uno stato WORM (Write Once Read Many). In uno stato WORM, i dati possono essere scritti una sola volta e letti e utilizzati tutte le volte che è necessario dopo il commit o la scrittura sul supporto di archiviazione. L'archivio immutabile ti aiuta a garantire il mantenimento dell'integrità dei dati. Fornisce inoltre protezione da quanto segue:

- Eliminazioni
- Sovrascritture
- Accesso involontario e non autorizzato

- Compromissione del ransomware

L'archivio immutabile offre un meccanismo efficiente per affrontare potenziali eventi di sicurezza che potrebbero avere un impatto reale sulle operazioni aziendali.

È possibile utilizzare l'archivio immutabile per una migliore governance se abbinato a forti restrizioni delle SCP. Puoi anche utilizzare l'archivio immutabile in modalità WORM di conformità quando la legge (ad esempio in caso di controversia legale) richiede l'accesso a dati immutabili.

Per mantenere la disponibilità e l'integrità dei dati, è possibile utilizzare AWS Backup Vault Lock per proteggere i backup. Quando utilizzi AWS Backup Vault Lock, le entità non autorizzate non possono cancellare, alterare o danneggiare i dati aziendali o dei clienti durante il periodo di conservazione richiesto. AWS Backup Vault Lock ti aiuta a soddisfare le politiche di protezione dei dati della tua organizzazione impedendo quanto segue:

- Eliminazioni da parte di utenti privilegiati (incluso l' Account AWS utente root)
- Modifiche alle impostazioni del ciclo di vita del backup
- Aggiornamenti che modificano il periodo di conservazione definito

AWS Backup Vault Lock garantisce l'immutabilità e aggiunge un ulteriore livello di difesa che protegge i backup (punti di ripristino) nelle casseforti di backup. Ciò è particolarmente utile in settori altamente regolamentati che hanno requisiti di integrità rigorosi per backup e archivi. AWS Backup Vault Lock assicura la conservazione dei dati insieme a un backup da cui eseguire il ripristino in caso di azioni involontarie o dannose.

Important

- AWS Backup Non è stata ancora valutata la conformità di Vault Lock alla regola 17a-4 (f) della Securities and Exchange Commission (SEC) e alla Commodity Futures Trading Commission (CFTC) nel regolamento 17 C.F.R. 1.31 (b) - (c).
- AWS Backup Vault Lock ha effetto immediato. Prevede un periodo minimo in cui esercitare il diritto di recesso di tre giorni (72 ore) per eliminare o aggiornare la configurazione prima di bloccare definitivamente il vault. Se lo desideri, puoi prolungare la durata di questo periodo di diritto di recesso. Usa questo periodo di riflessione per testare AWS Backup Vault Lock rispetto ai tuoi carichi di lavoro e ai tuoi casi d'uso. Dopo la scadenza del periodo di riflessione, né l'utente né l'utente Supporto AWS possono eliminare o modificare

in altro modo AWS Backup Vault Lock o il contenuto del vault chiuso a chiave. Per ulteriori informazioni, consulta la documentazione su AWS Backup Vault Lock.

Fase 7. Implementazione del monitoraggio e degli avvisi di backup

I processi di backup possono fallire. Un processo non riuscito, ad esempio un'operazione di backup, ripristino o copia, potrebbe influire sulle fasi successive di un processo. Quando il processo di backup iniziale fallisce, vi è un'alta probabilità che anche altre attività successive abbiano esito negativo. In uno scenario di questo tipo, è possibile comprendere meglio il corso degli eventi tramite il monitoraggio e la notifica. Il monitoraggio e l'invio di avvisi possono fornire informazioni organizzative sui processi di backup, aiutando a rispondere agli errori di backup.

L'attivazione e la configurazione delle notifiche per monitorare i processi AWS Backup offre i seguenti vantaggi:

- Ti consente di conoscere le tue attività di backup
- Contribuisce a garantire il rispetto degli accordi critici sui livelli di servizio () SLAs
- Migliora il monitoraggio business-as-usual
- Ti aiuta a rispettare gli obblighi di conformità

È possibile implementare il monitoraggio dei backup per i carichi di lavoro integrandosi AWS Backup con altri sistemi di ticketing per eseguire indagini automatizzate Servizi AWS e flussi di escalation. Ad esempio, puoi eseguire le operazioni seguenti:

- Usa Amazon CloudWatch per tenere traccia delle metriche, creare allarmi e visualizzare dashboard.
- Usa Amazon EventBridge per monitorare AWS Backup processi ed eventi.
- Usare AWS CloudTrail per monitorare le chiamate AWS Backup API con informazioni dettagliate sull'ora, l'IP di origine, gli utenti e gli account che effettuano tali chiamate.
- Usa Amazon Simple Notification Service (Amazon SNS) per iscriverti AWS Backup ad argomenti correlati come eventi di backup, ripristino e copia.

È possibile utilizzare AWS Backup Audit Manager per generare automaticamente prove dei report di audit di backup giornalieri per ogni account e regione. È inoltre possibile scalare il monitoraggio

dei backup su più account utilizzando una serie di modelli e dashboard di automazione (noti come soluzione backup observer) per ottenere report giornalieri aggregati su più account e più regioni. AWS Backup

Fase 8. Verifica della configurazione del backup

Per garantire che il programma di backup funzioni come dovrebbe e per identificare e correggere eventuali anomalie dei processi di backup, verifica la conformità delle AWS Backup politiche rispetto a controlli definiti, come la frequenza di backup definita. Per individuare e analizzare le operazioni o le risorse di backup non conformi ai requisiti aziendali, monitora in modo continuo e automatico l'attività di backup e genera report automatici.

AWS Backup Audit Manager offre controlli di conformità integrati e personalizzabili che si allineano ai requisiti normativi e di conformità aziendali. Puoi utilizzare i controlli predefiniti e personalizzabili come framework di audit per valutare le tue pratiche AWS Backup . I controlli comprendono:

- Risorse di backup protette da piani di backup
- Frequenza minima e conservazione minima del piano di backup
- Punto di ripristino dei backup crittografato
- Eliminazione manuale del punto di ripristino dei backup
- Conservazione minima dei punti di ripristino dei backup
- Copia tra regioni
- Copia tra account
- Vault Lock di backup

Per l'automazione dell'infrastruttura come codice (IaC), puoi utilizzare AWS Backup Audit Manager con. AWS CloudFormation

AWS Security Hub CSPMti offre una visione completa del tuo stato di sicurezza in. AWS Inoltre, consente di verificare la conformità dell'ambiente alle best practice di sicurezza e agli standard di settore, ad esempio i controlli di AWS Foundational Security Best Practices. Se utilizzi Security Hub CSPM nel tuo ambiente cloud, ti consigliamo di abilitare lo standard AWS Foundational Security Best Practices, poiché include controlli investigativi che possono aiutarti a proteggere i backup in ingresso. AWS La maggior parte dei controlli AWS Backup investigativi in Audit Manager e Security Hub CSPM sono disponibili anche come regole AWS Config gestite.

Fase 9. Test delle funzionalità di ripristino dei dati

La tua strategia di backup deve includere il test dei backup. Una strategia di backup non è efficace se i dati di backup non possono essere ripristinati. Verifica regolarmente la tua capacità di trovare determinati punti di ripristino e ripristinarli.

Sebbene AWS Backup copi automaticamente i tag dalle risorse che protegge ai punti di ripristino, per impostazione predefinita i tag non vengono copiati dai punti di ripristino alle risorse ripristinate corrispondenti. Per scalare la gestione dell'inventario e individuare i punti di ripristino, prendi in considerazione l'utilizzo AWS Backup degli eventi per avviare un processo di replica dei tag sulle risorse create dai AWS Backup processi di ripristino.

Puoi avviare il flusso di lavoro di ripristino dei dati stabilendo modelli di ripristino dei dati e quindi testandoli regolarmente. Per aumentare la fiducia nella tua capacità di ripristinare i dati di backup, crea un processo di base e ripetibile per eseguire test continui di ripristino dei dati. Ad esempio, puoi creare un modello per testare un'operazione di ripristino tra account e regioni diversi da un vault di backup di ripristino di emergenza centrale crittografato con una chiave AWS KMS gestita dal cliente a un vault di backup dell'account di origine crittografato con un'altra chiave AWS KMS gestita dal cliente.

Se non testate spesso tali operazioni di ripristino, potreste scoprire che le vostre ipotesi sulla AWS KMS crittografia per le operazioni tra account e regioni non sono corrette. Spesso, l'unico modello di ripristino del backup che funziona davvero è il percorso testato frequentemente. Attraverso i test di routine dei tipi di risorse di backup supportati, puoi individuare avvisi tempestivi che potrebbero causare future interruzioni e perdita di dati critici. Se possibile, mantieni un numero limitato ma fattibile di percorsi e modelli di ripristino per evitare sprechi di spazio di archiviazione, ottimizzare i costi e risparmiare tempo. Risolvere il problema quando un test di ripristino fallisce è più facile che perdere dati importanti o critici.

Fase 10. Incorporare il backup nel piano di risposta agli incidenti

Le simulazioni di risposta agli incidenti di sicurezza (SIRS) sono eventi interni che offrono un'opportunità strutturata per mettere in pratica il piano e le procedure di risposta agli incidenti in uno scenario realistico. È utile testare i dati e le operazioni di backup nelle attività creative di SIRS per mettersi alla prova contro gli imprevisti. Questo ti aiuta a confermare la tua preparazione organizzativa e a sentirti a tuo agio con ciò che è raro e inaspettato. Le simulazioni devono essere realistiche e devono coinvolgere team organizzativi interfunzionali che sono tenuti a rispondere agli eventi.

Inizia con esercizi di simulazione di base e procedi con un evento completo e complesso. Ad esempio, puoi creare un modello realistico costituito da un cloud privato virtuale (VPC) e risorse associate che simula la sovraesposizione involontaria di informazioni o una potenziale violazione dei dati causata da modifiche alle policy e agli elenchi di controllo dell'accesso. Per valutare l'efficacia del piano di risposta agli incidenti, documenta le lezioni apprese e identifica i miglioramenti da apportare alle future procedure di risposta.

Puoi utilizzarlo AWS Backup per configurare backup automatici a livello di istanza come Amazon Machine Images AMIs () e backup a livello di volume come istantanee su più istanze. Account AWS Questo può aiutare il team di risposta agli incidenti a migliorare i propri processi forensi, come la raccolta forense automatizzata su disco, fornendo un punto di ripristino in grado di ridurre la portata e l'impatto di potenziali eventi di sicurezza come il ransomware.

Passaggi successivi

Questa guida illustra le 10 migliori pratiche e controlli di sicurezza per proteggere i dati di backup AWS. Ti consigliamo di utilizzare queste best practice per progettare e implementare una strategia e un'architettura di backup e ripristino, con più livelli di controllo, in grado di dimensionare e soddisfare le tue esigenze aziendali. Per ulteriori informazioni in merito AWS Backup, consulta la AWS Backup documentazione.

Se hai domande su questa guida, apri un nuovo thread sul forum AWS Backup o contatta Supporto AWS.

Risorse

AWS Guida prescrittiva

- Approcci di backup e ripristino su AWS (guida)

AWS documentazione

- 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

Post del blog

- Automatizza il backup centralizzato su larga scala in tutti gli utilizzi Servizi AWSAWS Backup
- Architettura di Disaster Recovery (DR) su AWS, Parte I: Strategie per il ripristino nel cloud
- L'importanza della crittografia e come AWS può aiutarla
- Migliora il livello di sicurezza dei tuoi backup con AWS Backup Vault Lock
- Monitora, valuta e dimostra la conformità del backup con AWS Backup Audit Manager
- Crea e condividi backup crittografati tra account e regioni utilizzando AWS Backup
- Semplifica il controllo delle politiche di protezione dei dati con AWS Backup Audit Manager

- Gestione dell'accesso ai backup utilizzando le politiche di controllo del servizio con AWS Backup
- Ottieni report giornalieri aggregati su più account e più regioni AWS Backup

GitHub archivi

I seguenti archivi di codice forniscono una soluzione di gestione e implementazione per implementare il backup e il ripristino AWS Backup in tutta l' AWS Organizations organizzazione, su più account e. Regioni AWS

- Implementa utilizzando AWS BackupAWS
- Implementazione AWS Backup utilizzando pipeline CI/CD

Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	—	13 maggio 2022

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.