Approcci di backup e ripristino su AWS

AWS Guida prescrittiva

AWS Guida prescrittiva: Approcci di backup e ripristino su AWS

Table of Contents

Approcci di backup e ripristino suAWS

Khurram Nizami, Amazon Web Services (AWS)

aprile 2023(cronologia dei documenti)

Questa guida spiega come implementare approcci di backup e ripristino utilizzando Amazon Web Services (AWS) servizi per architetture locali, native per il cloud e ibride. Questi approcci offrono costi inferiori, maggiore scalabilità e maggiore durata per soddisfare i requisiti di Recovery Time Objective (RTO), Recovery Point Objective (RPO) e di conformità.

Questa guida è destinata ai responsabili tecnici responsabili della protezione dei dati negli ambienti IT e cloud aziendali.

Questa guida copre diverse architetture di backup (applicazioni native del cloud, ambienti ibridi e locali). Copre anche i servizi Amazon Web Services (AWS) associati che possono essere utilizzati per creare soluzioni di protezione dei dati scalabili e affidabili per i componenti non immutabili della tua architettura.

Un altro approccio consiste nel modernizzare i carichi di lavoro per utilizzare architetture immutabili, riducendo la necessità di backup e ripristino dei componenti.AWSfornisce una serie di servizi per implementare architetture immutabili e ridurre la necessità di backup e ripristino, tra cui:

- Serverless conAWS Lambda
- Contenitori con Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) eAWS Fargate
- Amazon Machine Images (AMI) con Amazon Elastic Compute Cloud (Amazon EC2)

Con l'accelerazione della crescita dei dati aziendali, il compito di proteggerli diventa sempre più impegnativo. Le domande sulla durabilità e la scalabilità degli approcci di backup sono all'ordine del giorno, inclusa questa: in che modo il cloud aiuta a soddisfare le mie esigenze di backup e ripristino?

Questa guida include i seguenti argomenti:

- Scelta AWS dei servizi per la protezione dei dati
- Progettazione di una soluzione di backup e ripristino
- Backup e ripristino tramiteAWS Backup

- Backup e ripristino con Amazon S3 e Amazon S3 Glacier
- Backup e ripristino per Amazon EC2 con volumi EBS
- Backup e ripristino dall'infrastruttura locale aAWS
- Backup e ripristino delle applicazioni daAWSal tuo data center
- Backup e ripristino diAWS servizi nativi per il cloud
- Backup e ripristino per architetture ibride
- Disaster recovery conAWS
- Pulizia dei backup

Perché usareAWScome piattaforma di protezione dei dati?

AWS è un sistema sicuro, ad alte prestazioni, flessibile, che consente di risparmiare denaro eeasy-to-usepiattaforma di cloud computing.AWSsi occupa delle operazioni indifferenziate necessarie per creare, implementare e gestire soluzioni di backup e ripristino scalabili.

Ci sono molti vantaggi nell'utilizzoAWScome parte della tua strategia di protezione dei dati:

- Durata: Amazon Simple Storage Service (Amazon S3), Amazon S3 Glacier e S3 Glacier Deep Archive sono progettati per il 99,999999999 percento (11 nove) di durata. Entrambe le piattaforme offrono un backup affidabile dei dati, con replica degli oggetti su almeno tre zone di disponibilità distribuite geograficamente. MoltiAWSi servizi utilizzano Amazon S3 per lo storage e le operazioni di esportazione/importazione. Ad esempio, Amazon Elastic Block Store (Amazon EBS) utilizza Amazon S3 per lo storage delle istantanee.
- Sicurezza:AWSoffre una serie di opzioni per il controllo degli accessi e la crittografia dei dati in transito e a riposo.
- Infrastruttura globale:AWSi servizi sono disponibili in tutto il mondo, quindi puoi eseguire il backup e l'archiviazione dei dati nella regione che soddisfa i requisiti di conformità e di carico di lavoro.
- Conformità:AWSl'infrastruttura è certificata per la conformità ai seguenti standard, in modo da poter adattare facilmente la soluzione di backup al regime di conformità esistente:
  - Controlli dell'organizzazione dei servizi (SOC)
  - Dichiarazione sugli standard per gli impegni di attestazione (SSAE) 16
  - Organizzazione internazionale per la standardizzazione (ISO) 27001
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Health Insurance Portability and Accountability Act (HIPAA)

  - SEC1
  - Federal Risk and Authorization Management Program (FedRAMP)
- Scalabilità: ConAWS, non devi preoccuparti della capacità. Man mano che le tue esigenze cambiano, puoi aumentare o diminuire i tuoi consumi senza costi amministrativi.
- Costo totale di proprietà (TCO) inferiore: La scala diAWSle operazioni riducono i costi di servizio e aiutano a ridurre il TCO diAWSservizi.AWStrasferisce questi risparmi sui costi ai clienti attraverso riduzioni di prezzo.
- Pay-as-you-goprezzi: AcquistaAWSservizi quando ne hai bisogno e solo per il periodo in cui prevedi di utilizzarli.AWSi prezzi non prevedono commissioni anticipate, penali di risoluzione o contratti a lungo termine.

Obiettivi aziendali specifici

L'obiettivo di questa guida è fornire una panoramica diAWSservizi che è possibile utilizzare per supportare gli approcci di backup e ripristino per quanto segue:

- Architetture locali
- Architetture native per il cloud
- Architetture ibride
- Servizi nativi AWS
- Disaster recovery (DR)

Vengono illustrate le migliori pratiche e considerazioni insieme a una panoramica dei servizi. Questa guida fornisce anche i compromessi tra l'utilizzo di un approccio rispetto a un altro per il backup e il ripristino.

Scelta AWS dei servizi per la protezione dei dati

AWS fornisce una serie di servizi di storage e complementari che possono essere utilizzati come parte dell'approccio di backup e ripristino. Questi servizi possono supportare architetture native per il cloud e ibride. Servizi diversi sono più efficaci per diversi casi d'uso.

- Amazon S3 e Amazon S3 Glacier e S3 Glacier Deep Archive sono adatti per casi d'uso ibridi e nativi del cloud. Questi servizi forniscono soluzioni di storage di oggetti generiche e altamente durevoli, adatte per il backup di singoli file, server o di un intero data center.
- AWS Storage Gatewayè ideale per casi d'uso ibridi. Storage Gateway sfrutta la potenza di Amazon S3 per i comuni requisiti di backup e storage locali. Le tue applicazioni si connettono al servizio tramite una macchina virtuale (VM) o un'appliance gateway hardware utilizzando i seguenti protocolli di storage standard:
  - Network File System (NFS)
  - Server Message Block (SMB)
  - Interfaccia Internet per piccoli computer (iSCSI)

  Il gateway collega questi protocolli locali comuni a servizi di AWS storage come i seguenti:
  - Amazon S3
  - Amazon S3 Glacier
  - S3 Glacier Deep Archive
  - Amazon EBS

  Storage Gateway semplifica la fornitura di storage elastico e ad alte prestazioni per file, volumi, istantanee e nastri virtuali. AWS
- AWS Backupè un servizio di backup completamente gestito per centralizzare e automatizzare il backup dei dati tra i servizi. AWS Utilizzando AWS Backup, è possibile configurare centralmente le politiche di backup e monitorare l'attività di backup AWS delle risorse, come le seguenti:
  - Volumi EBS
  - Istanze EC2 (incluse le applicazioni Windows)
  - Database Amazon RDS e Amazon Aurora
  - Tabelle DynamoDB
  - Database Amazon Neptune
  - Database di Amazon DocumentDB database (con compatibilità MongoDB)

  - File system di Amazon EFS
  - File system Amazon FSx for Lustre e file system Amazon FSx for Windows File Server
  - Carichi di lavoro VMware in locale e in VMware Cloud on AWS
  - Volumi Storage Gateway

  Il costo di AWS Backup si basa sullo storage che consumi, ripristini e trasferisci in un mese. Per ulteriori informazioni, consulta i AWS Backup prezzi.
- AWS Elastic Disaster Recoveryreplica continuamente le tue macchine in un'area di gestione a basso costo nell' AWS account di destinazione e nella regione preferita. È possibile utilizzare Elastic Disaster Recovery per il ripristino di emergenza e il ripristino di emergenza premises-to-cloud interregionale
- AWS Configfornisce una visualizzazione dettagliata della configurazione delle AWS risorse del tuo AWS account. Ciò include il modo in cui le risorse sono correlate tra loro e come sono state configurate in passato. In questa visualizzazione, puoi vedere come la configurazione e le relazioni delle risorse sono cambiate nel tempo.

  Quando si attiva la registrazione AWS Config della configurazione per le AWS risorse, si mantiene una cronologia delle relazioni tra le risorse nel tempo. Ciò consente di identificare e tenere traccia AWS delle relazioni tra le risorse (comprese le risorse eliminate) per un massimo di sette anni. Ad esempio, AWS Config può tracciare la relazione tra un volume snapshot Amazon EBS e l'istanza EC2 a cui è stato collegato il volume.
- AWS Lambdapuò essere utilizzato per definire e automatizzare a livello di codice le procedure di backup e ripristino per i carichi di lavoro. Puoi utilizzare gli AWS SDK per interagire con AWS i servizi e i relativi dati. Puoi anche utilizzare Amazon CloudWatch Events per eseguire le funzioni Lambda in base a una pianificazione.

AWS i servizi forniscono funzionalità specifiche per il backup e il ripristino. Per ogni AWS servizio in uso, consulta la AWS documentazione per determinare le funzionalità di backup, ripristino e protezione dei dati fornite dal servizio. Puoi utilizzare AWS Command Line Interface (AWS CLI), gli AWS SDK e le operazioni API per automatizzare le funzionalità AWS specifiche del servizio per il backup e il ripristino dei dati.

Progettazione di una soluzione di backup e ripristino

Quando si sviluppa una strategia completa per il backup e il ripristino dei dati, è necessario innanzitutto identificare possibili situazioni di guasto o di emergenza e il loro potenziale impatto aziendale. In alcuni settori, è necessario considerare i requisiti normativi per la sicurezza dei dati, la privacy e la conservazione dei record.

I processi di backup e ripristino devono includere il livello di granularità appropriato per soddisfare il Recovery Time Objective (RTO) e il Recovery Point Objective (RPO) per il carico di lavoro e i relativi processi aziendali di supporto, tra cui:

- Ripristino a livello di file (ad esempio, file di configurazione per un'applicazione)
- Ripristino a livello di dati dell'applicazione (ad esempio, un database specifico all'interno di MySQL)
- Ripristino a livello di applicazione (ad esempio, una versione specifica dell'applicazione del server Web)
- Ripristino a livello di volume di Amazon EC2 (ad esempio, un volume EBS)
- Ripristino a livello di istanza EC2. (ad esempio, un'istanza EC2)
- Ripristino del servizio gestito (ad esempio, una tabella DynamoDB)

Assicurati di considerare tutti i requisiti di ripristino per la tua soluzione e le dipendenze dei dati tra i vari componenti della tua architettura. Per facilitare il corretto processo di ripristino, è necessario coordinare il backup e il ripristino tra i vari componenti dell'architettura.

Gli argomenti seguenti descrivono gli approcci di backup e ripristino basati sull'organizzazione dell'infrastruttura. L'infrastruttura IT può essere ampiamente classificata come on-premise, ibrida o nativa per il cloud.

Backup e ripristino tramiteAWS Backup

AWS Backupè un servizio di backup completamente gestito che centralizza e automatizza il backup dei datiAWSServizi .AWS Backupfornisce un livello di orchestrazione che integra Amazon CloudWatch,AWS CloudTrail,AWS Identity and Access Management(IAM),AWS Organizationse altri servizi. Questo centralizzato,AWSLa soluzione cloud native offre funzionalità di backup globali che possono aiutarti a raggiungere i requisiti di disaster recovery e conformità. Utilizzo diAWS Backup, è possibile configurare in modo centralizzato le policy di backup e monitorare le attività di backup perAWSrisorse AWS.

AWS Backupè una soluzione ideale per implementare piani di backup standard per il tuoAWSrisorse in tutto il tuoAWSaccount e regioni PoichéAWS Backupsupporta piùAWStipi di risorse, semplifica la manutenzione e l'implementazione di una strategia di backup per carichi di lavoro utilizzando piùAWSrisorse che devono essere sottoposte a backup collettivo.AWS Backupconsente inoltre di monitorare collettivamente un'operazione di backup e ripristino che coinvolge piùAWSrisorse AWS.

Se si dispone di requisiti di conformità e controllo, è possibile utilizzare ilAWS BackupAudit Managerfunzionalità per creare framework di audit e report per supportare i requisiti di conformità. LaAWS BackupVault Locksupporta anche i requisiti di conformità applicando una configurazione WORM (write-once, read-many) per tutti i backup archiviati in un vault di backup inAWS Backup.

Un differenziatore chiave perAWS Backupè il supporto per le Organizations. Utilizzando questo supporto, è possibile definire e gestire le policy di backup a livello di organizzazione o unità organizzativa e implementare automaticamente tali criteri per ogni correlato.AWSaccount e regione Come sei a bordo nuovoAWSaccount e regioni, non è necessario definire e gestire separatamente i piani di backup.

AWS Backuppuò semplificare l'implementazione di una politica di backup a livello di organizzazione utilizzando i tag. È possibile creare piani di backup separati con impostazioni di frequenza e conservazione univoche e quindi creare tag di coppia chiave-valore univoci che selezionano le risorse da includere per il backup.

Ad esempio, è possibile creare un piano di backup giornaliero che avvia un backup alle 05:00 UTC su base giornaliera e dispone di un criterio di conservazione di 35 giorni. Questo piano di backup può includere unassegnazione delle risorse di backupche specifica che qualsiasi supportoAWSrisorsa con il tag keydi riservavalore tagquotidianoverrà eseguito il backup secondo questo piano. Inoltre, è possibile creare un piano di backup mensile che inizia alle 05:00 UTC del primo giorno di ogni mese e che dispone di una politica di conservazione di 36 giorni. Questo piano di backup può includere

un'assegnazione di risorse di backup che specifica che qualsiasi supportoAWSrisorsa con il tag keydi riservavalore tagmensileverrà eseguito il backup secondo questo piano.

È quindi possibile utilizzare i criteri per i tag e ilrequired-tags AWS Configregola per garantire che tutto il tuoAWSle risorse supportate hanno questa chiave tag e uno di questi valori di tag. Questo approccio può aiutarti a implementare e mantenere in modo coerente un approccio di backup standard inAWSper supportatoAWS Backuprisorse AWS. È possibile estendere questo approccio per standardizzare i backup per le applicazioni e i livelli architettonici con requisiti RPO (Recovery Point Objective) diversi.

Consigliamo di adottare misure per proteggere il vault di backup. Ad esempio, è possibile implementare un criterio di controllo del servizio Organizations (SCP) che impedisce l'eliminazione o la condivisione del vault di backup non intenzionale.AWSconti. Per maggiori dettagli e altre importanti considerazioni sulla sicurezza, consulta ilLe 10 best practice di sicurezza per proteggere i backup inAWSpost di blog.

AWS Backuppuò semplificare l'implementazione del piano di disaster recovery (DR) perAWSperché supporta piùAWSrisorse che possono essere affrontate collettivamente. Ad esempio, è possibile implementareTra regionietra accountbackup per la maggior parte delleAWStipi di risorsa supportati daAWS Backup. Il backup su più account migliora la sicurezza del backup perché una copia è disponibile in un account separato. Il backup tra regioni migliora la disponibilità perché i backup sono disponibili in più di una regione. Per informazioni dettagliateAWStipi di risorse, vedere ilDisponibilità delle funzionalità per risorsatavolo.

Puoi utilizzare l'esempioBackup e ripristino conAWS Backupsoluzione open sourceimplementare un'infrastruttura come codice (iAC) e un approccio CI/CD (Continuous Integration and Continuous Delivery) alla gestione dei backup per il tuoAWS Organizationsorganizzazione. Questa soluzione include funzionalità personalizzate, come la riapplicazione automaticaAWStag su restauratoAWSrisorse e creazione di un archivio di backup secondario in un account separato e in una regione per scopi di DR.

Backup e ripristino con Amazon S3 e Amazon S3 Glacier

Amazon S3 e Amazon S3 Glacier sono servizi di storage ideali per l'uso in architetture locali, ibride e native per il cloud. Questi servizi forniscono piattaforme di storage durevoli e a basso costo che offrono capacità scalabile e non richiedono la gestione di volumi o supporti man mano che i set di dati di backup crescono. Il modello pay-for-what-you di utilizzo e il basso costo per GB/mese rendono questi servizi adatti a un'ampia gamma di casi d'uso di protezione dei dati.

> **Note**
>
> Alcune classi di archiviazione prevedono un costo minimo di durata. Per i dettagli, consulta i prezzi di Amazon S3 e utilizza la ricerca nella pagina Web per trovare. `duration`

Argomenti

Amazon S3

Puoi usare Amazon S3 per archiviare e recuperare qualsiasi quantità di dati, in qualsiasi momento. Puoi utilizzare Amazon S3 come archivio durevole per i dati delle applicazioni e i processi di backup e ripristino a livello di file. Ad esempio, puoi copiare i backup del database da un'istanza di database ad Amazon S3 con uno script di backup utilizzando AWS CLI gli SDK o.

AWS i servizi utilizzano Amazon S3 per uno storage altamente durevole e affidabile, come negli esempi seguenti:

- Amazon EC2 utilizza Amazon S3 per archiviare gli snapshot di Amazon EBS per i volumi EBS e per gli archivi di istanze EC2.
- Storage Gateway si integra con Amazon S3 per fornire ambienti locali con condivisioni di file, volumi e librerie a nastro supportate da Amazon S3.
- Amazon RDS utilizza Amazon S3 per gli snapshot del database.

Molte soluzioni di backup di terze parti utilizzano anche Amazon S3. Ad esempio, Arcserve Unified Data Protection supporta Amazon S3 per il backup durevole di server locali e nativi del cloud.

Puoi utilizzare le funzionalità integrate in Amazon S3 di questi servizi per semplificare l'approccio al backup e al ripristino. Allo stesso tempo, puoi trarre vantaggio dall'elevata durabilità e disponibilità fornite da Amazon S3.

Amazon S3 archivia i dati come oggetti all'interno di risorse chiamate bucket. Puoi archiviare tutti gli oggetti che desideri in un bucket. Puoi scrivere, leggere ed eliminare oggetti nel tuo bucket con un controllo degli accessi preciso. I singoli oggetti possono avere dimensioni fino a 5 TB.

Amazon S3 offre una gamma di classi di storage progettate per diversi casi d'uso, incluse le seguenti classi:

- S3 Standard per l'archiviazione generica dei dati a cui si accede di frequente (ad esempio, file di configurazione, backup non pianificati, backup giornalieri).
- S3 Standard-IA per dati di lunga durata ma con accesso meno frequente (ad esempio, backup mensili). IA è l'acronimo di Infrequent Access.

Amazon S3 offre politiche del ciclo di vita che puoi configurare per gestire i dati durante tutto il loro ciclo di vita. Dopo aver impostato una policy, i dati verranno migrati nella classe di storage appropriata senza alcuna modifica all'applicazione. Per ulteriori informazioni, consulta la documentazione sulla gestione del ciclo di vita degli oggetti di Amazon S3.

Per ridurre i costi di backup, utilizza un approccio basato su classi di storage su più livelli basato sul Recovery Time Objective (RTO) e sul Recovery Point Objective (RPO), come nell'esempio seguente:

- Backup giornalieri delle ultime 2 settimane utilizzando S3 Standard
- Backup settimanali degli ultimi 3 mesi utilizzando S3 Standard-IA
- Backup trimestrali dello scorso anno su S3 Glacier Flexible Retrieval
- Backup annuali degli ultimi 5 anni su S3 Glacier Deep Archive
- Backup eliminati da S3 Glacier Deep Archive dopo 5 anni

È possibile automatizzare la transizione dei backup utilizzando la gestione del ciclo di vita degli oggetti.

> **Note**
>
> Alcune classi di storage prevedono un costo minimo di durata. Per i dettagli, consulta i prezzi di Amazon S3 e utilizza la ricerca nella pagina Web per trovare. `duration`

Creazione di bucket S3 standard per il backup e l'archiviazione

Puoi creare un bucket S3 standard per il backup e l'archiviazione con la politica di backup e conservazione della tua azienda implementata tramite le policy del ciclo di vita di S3. L'allocazione dei costi, i tag e i report per la AWS fatturazione si basano sui tag assegnati a livello di bucket. Se l'allocazione dei costi è importante, crea bucket S3 di backup e archiviazione separati per ogni progetto o unità aziendale in modo da poter allocare i costi di conseguenza.

Gli script e le applicazioni di backup possono utilizzare il bucket S3 di backup e archiviazione creato da te per archiviare point-in-time istantanee per i dati delle applicazioni e dei carichi di lavoro. Puoi creare un prefisso s3 standard per aiutarti a organizzare le istantanee dei dati. point-in-time Ad esempio, se crei backup ogni ora, prendi in considerazione l'utilizzo di un prefisso di backup come. `YYYY/MM/DD/HH/<WorkloadName>/<files...>` In questo modo, è possibile recuperare rapidamente i point-in-time backup manualmente o programmaticamente.

Utilizzo del controllo delle versioni di Amazon S3 per mantenere automaticamente la cronologia di rollback

Puoi abilitare il controllo delle versioni degli oggetti S3 per mantenere una cronologia delle modifiche agli oggetti, inclusa la possibilità di ripristinare una versione precedente. Ciò è utile per i file di configurazione e altri oggetti che potrebbero cambiare più frequentemente rispetto alla pianificazione del backup point-in-time . È utile anche per i file che devono essere ripristinati singolarmente.

Utilizzo di Amazon S3 per il backup e il ripristino di file di configurazione personalizzati per le AMI

Amazon S3 con controllo delle versioni degli oggetti può diventare il tuo sistema di registrazione per la configurazione del carico di lavoro e i file di opzioni. Ad esempio, è possibile utilizzare un'immagine Marketplace AWS Amazon EC2 standard gestita da un ISV. Questa immagine potrebbe contenere software la cui configurazione è gestita in diversi file di configurazione. Puoi gestire i tuoi file di configurazione personalizzati in Amazon S3. All'avvio dell'istanza, puoi copiare questi

file di configurazione nell'istanza come parte dei dati utente dell'istanza. Quando si applica questo approccio, non è necessario personalizzare e ricreare un'AMI per utilizzare una versione aggiornata.

Utilizzo di Amazon S3 nel processo di backup e ripristino personalizzato

Amazon S3 offre un archivio di backup generico che puoi integrare rapidamente nei processi di backup personalizzati esistenti. Puoi utilizzare gli AWS CLI AWS SDK e le operazioni API per integrare gli script e i processi di backup e ripristino che utilizzano Amazon S3. Ad esempio, potresti avere uno script di backup del database che esegue esportazioni notturne del database. Puoi personalizzare questo script per copiare i tuoi backup notturni su Amazon S3 per lo storage fuori sede. Consulta il tutorial sul caricamento in batch dei file sul cloud per una panoramica su come eseguire questa operazione.

Puoi adottare un approccio simile per l'esportazione e il backup dei dati per diverse applicazioni in base ai rispettivi RPO individuali. Inoltre, è possibile utilizzare AWS Systems Manager per eseguire gli script di backup sulle istanze gestite. Systems Manager fornisce automazione, controllo degli accessi, pianificazione, registrazione e notifica per i singoli processi di backup.

Amazon S3 Glacier

Amazon S3 Glacier è un servizio di archiviazione cloud a basso costo che fornisce uno storage sicuro e duraturo per l'archiviazione dei dati e il backup online. Per mantenere bassi i costi, S3 Glacier offre tre classi di storage da pochi millisecondi a ore. S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive offrono opzioni aggiuntive in base alla velocità con cui è necessario ripristinare i dati. Con S3 Glacier, puoi archiviare in modo affidabile grandi o piccole quantità di dati con risparmi significativi rispetto alle soluzioni locali. S3 Glacier è ideale per l'archiviazione di dati di backup con requisiti di conservazione a lungo o indefinito e per l'archiviazione dei dati a lungo termine. S3 Glacier offre le seguenti classi di storage:

- S3 Glacier Instant Retrieval per l'archiviazione dei dati che potrebbero essere necessari una volta al trimestre e che devono essere ripristinati rapidamente (millisecondi)
- S3 Glacier Flexible Retrieval per l'archiviazione di dati che potrebbero dover essere ripristinati raramente, una o due volte all'anno, entro poche ore
- S3 Glacier Deep Archive per l'archiviazione dei dati del ciclo di backup a lungo termine che potrebbero dover essere ripristinati raramente entro 12 ore

La tabella seguente riepiloga le opzioni di recupero archivi.

Classe di storage	Expedited	Standard	Bulk
S3 Glacier Instant Retrieval	Non applicabile	Non applicabile	Non applicabile
S3 Glacier Flexible Retrieval	1 - 5 minuti	3 - 5 ore	5 - 12 ore
S3 Glacier Deep Archive	Non disponibile	Entro 12 ore	Entro 48 ore

Utilizzando Amazon S3, puoi impostare la classe di storage per ogni oggetto nel tuo bucket S3 al momento della creazione. Dopo aver creato l'oggetto, puoi modificare la classe di storage copiando l'oggetto su un nuovo oggetto con una classe di storage diversa. In alternativa, è possibile abilitare una configurazione del ciclo di vita che modifichi automaticamente la classe di archiviazione degli oggetti in base alle regole specificate.

Per automatizzare i processi di backup e ripristino, puoi accedere ad Amazon S3 Glacier e S3 Glacier Deep Archive tramite, e SDK. AWS Management Console AWS CLI AWS Per ulteriori informazioni, consulta Amazon S3 Glacier.

> **Note**
>
> Le classi di storage S3 Glacier hanno una durata minima. Per i dettagli, consulta i prezzi di Amazon S3 e utilizza la ricerca nella pagina Web per trovare. `duration`

Utilizzo della transizione di oggetti Amazon S3 Lifecycle ad Amazon S3 Glacier rispetto alla gestione degli archivi Amazon S3 Glacier

Amazon S3 offre una comoda transizione degli oggetti S3 nelle classi di storage Amazon S3 Glacier, in modo da poter gestire il ciclo di vita e i costi dei backup. Tuttavia, a seconda delle dimensioni degli oggetti e della necessità o meno di ripristinare una raccolta di oggetti per diversi componenti dell'architettura, potresti voler gestire questo processo da solo.

Se avete un gran numero di oggetti di piccole dimensioni che devono essere ripristinati collettivamente, considerate le implicazioni in termini di costi delle seguenti opzioni:

- Utilizzo di una politica del ciclo di vita per trasferire automaticamente gli oggetti singolarmente ad Amazon S3 Glacier
- Compressione di oggetti in un unico file e archiviazione in Amazon S3 Glacier

Amazon S3 Glacier prevede costi di capacità minimi per ogni oggetto a seconda della classe di storage utilizzata. Ad esempio, S3 Glacier Instant Retrieval ha una capacità minima di 128 KB per ogni oggetto. Consulta il grafico delle prestazioni per la maggior parte delle informazioni. up-to-date

Per ogni oggetto archiviato su S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, Amazon S3 utilizza 8 KB di storage per il nome dell'oggetto e altri metadati. Amazon S3 memorizza questi metadati per consentire di generare tramite l'API Amazon S3 un elenco in tempo reale degli oggetti archiviati. Questo spazio di archiviazione aggiuntivo viene addebitato secondo le tariffe di S3 Standard.

Amazon S3 aggiunge inoltre 32 KB di storage per l'indice e i relativi metadati per ogni oggetto archiviato nelle classi di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Questi dati aggiuntivi sono necessari per identificare e ripristinare l'oggetto desiderato. Ti vengono addebitate le tariffe di Amazon S3 Glacier o S3 Glacier Deep Archive per questo storage aggiuntivo.

Comprimendo gli oggetti in un unico file, puoi ridurre lo storage aggiuntivo utilizzato da Amazon S3 Glacier ed evitare costi minimi di capacità per molti oggetti di piccole dimensioni.

Un'altra considerazione importante è che le politiche del ciclo di vita vengono applicate agli oggetti singolarmente. Ciò può influire sull'integrità del backup se una raccolta di oggetti deve essere ripristinata collettivamente da un momento specifico. Non è garantito che tutti gli oggetti effettuino la transizione contemporaneamente, anche con lo stesso tempo di scadenza e di transizione del ciclo di vita impostato tra gli oggetti. Potrebbe verificarsi un ritardo tra il momento in cui la regola del ciclo di vita viene soddisfatta e il completamento dell'azione per la regola. Per ulteriori informazioni, consulta l'AWS Knowledge Center.

Infine, considera lo sforzo di ripristino tra l'utilizzo degli archivi derivanti dalle politiche del ciclo di vita e la gestione di un archivio separato da te creato. È necessario avviare un ripristino per ogni oggetto da Amazon S3 Glacier separatamente. Ciò richiede la scrittura di uno script o l'utilizzo di uno strumento per avviare un ripristino di molti oggetti collettivamente. Puoi utilizzare S3 Batch Operations per ridurre il numero di richieste individuali oppure puoi utilizzare la console Amazon S3.

Protezione dei dati di backup in Amazon S3 e Amazon S3 Glacier

La sicurezza dei dati è una preoccupazione universale e prende molto sul serio la sicurezza. AWS La sicurezza è alla base di ogni AWS servizio. I servizi di storage come Amazon S3 offrono solide funzionalità per il controllo degli accessi e la crittografia sia a riposo che in transito. Tutti gli endpoint API Amazon S3 e Amazon S3 Glacier supportano Secure Sockets Layer/Transport Layer Security (SSL/TLS) per la crittografia dei dati in transito. Amazon S3 Glacier crittografa tutti i dati inattivi per impostazione predefinita. Con Amazon S3, puoi scegliere la crittografia lato server per gli oggetti inattivi effettuando le seguenti operazioni:

- Utilizzo della crittografia lato server con chiavi di crittografia gestite da Amazon S3
- Utilizzo della crittografia lato server con chiavi () archiviate in AWS Key Management Service AWS KMS AWS KMS

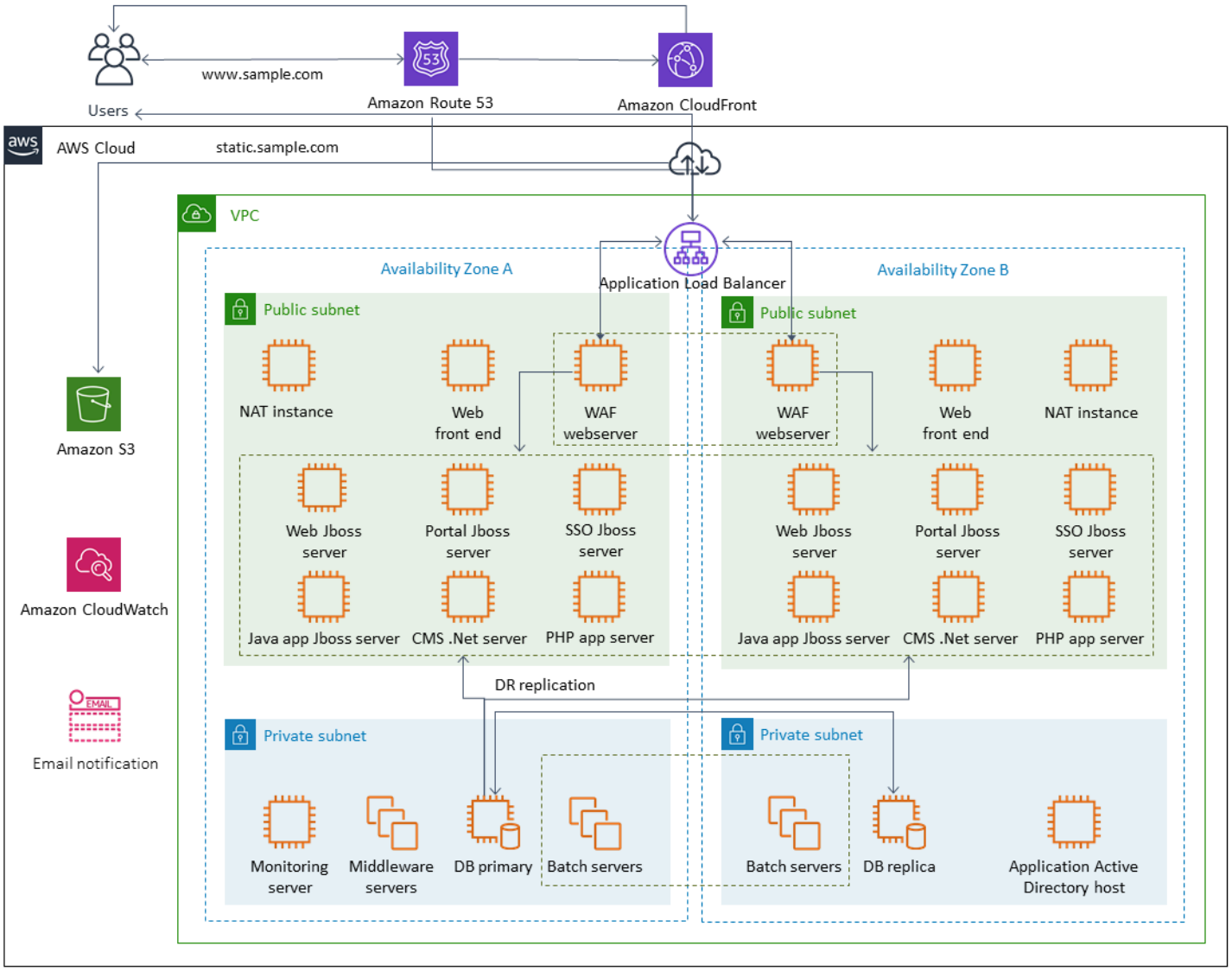
In alternativa, puoi crittografare i tuoi dati prima di caricarli su. AWS Per ulteriori informazioni, consulta la documentazione sulla crittografia lato client.

Puoi usare AWS Identity and Access Management (IAM) per controllare l'accesso agli oggetti S3. IAM fornisce il controllo sulle autorizzazioni per singoli oggetti e percorsi di prefissi specifici all'interno di un bucket S3. Puoi controllare l'accesso agli oggetti S3 utilizzando la registrazione a livello di oggetto con. AWS CloudTrail

Backup e ripristino per Amazon EC2 con volumi EBS

AWS offre diversi metodi per eseguire il backup delle istanze Amazon EC2. Questa sezione tratta diversi aspetti del backup dei volumi Amazon Elastic Block Store (Amazon EBS) o dei volumi di instance store per lo storage. Considerala AWS Backup la tua prima scelta per la gestione dei backup AWS se soddisfa i tuoi requisiti. Ricorda che i backup sono validi solo se possono essere ripristinati alla funzione per cui erano destinati. La funzione di ripristino e ripristino deve essere testata regolarmente per confermarlo.

L'architettura della soluzione nel diagramma seguente descrive un ambiente di carico di lavoro che esiste interamente AWS con la maggior parte dell'architettura basata su Amazon EC2. Come illustrato nella figura seguente, lo scenario include server Web, server di applicazioni, server di monitoraggio, database e Active Directory.



AWS fornisce molti servizi completi per molti dei server Amazon EC2 rappresentati in questa architettura per eseguire il lavoro indifferenziato di creazione, provisioning, backup, ripristino e ottimizzazione delle istanze e dello storage. Valuta se questi servizi sono utili nella tua architettura per ridurre la complessità e la gestione. AWS fornisce anche servizi per migliorare la disponibilità delle architetture basate su Amazon EC2. In particolare, prendi in considerazione Amazon EC2 Auto Scaling ed Elastic Load Balancing per integrare i tuoi carichi di lavoro su Amazon EC2. L'utilizzo di questi servizi può migliorare la disponibilità e la tolleranza ai guasti della tua architettura e aiutarti a ripristinare le istanze danneggiate con un impatto minimo sull'utente.

Le istanze EC2 utilizzano principalmente volumi Amazon EBS per lo storage persistente. Amazon EBS offre una serie di funzionalità per il backup e il ripristino, illustrate in dettaglio in questa sezione.

Argomenti

Backup e ripristino di Amazon EC2 con snapshot e AMI

Valuta se devi creare un backup completo di un'istanza EC2 con un'Amazon Machine Image (AMI) o scattare uno snapshot di un singolo volume.

Utilizzo di AMI o snapshot Amazon EBS per i backup

Un'AMI include i seguenti elementi:

- Una o più istantanee. Le nstance-store-backed AMI includono un modello per il volume principale dell'istanza (ad esempio, un sistema operativo, un server di applicazioni e applicazioni).
- Autorizzazioni di avvio che controllano quali AWS account possono utilizzare l'AMI per avviare le istanze.
- Una mappatura dei dispositivi a blocchi che specifica i volumi da collegare all'istanza al momento dell'avvio.

Puoi utilizzare le AMI per avviare nuove istanze con software e dati preconfigurati. È possibile creare AMI quando si desidera stabilire una linea di base, ovvero una configurazione riutilizzabile per avviare più istanze. Quando crei un'AMI di un'istanza EC2 esistente, viene scattata un'istantanea per tutti i volumi collegati all'istanza. L'istantanea include le mappature dei dispositivi.

Non è possibile utilizzare le istantanee per avviare una nuova istanza, ma è possibile utilizzarle per sostituire i volumi su un'istanza esistente. Se si verifica un danneggiamento dei dati o un errore di volume, è possibile creare un volume da un'istantanea scattata e sostituire il volume precedente. È inoltre possibile utilizzare le istantanee per effettuare il provisioning di nuovi volumi e collegarli durante il lancio di una nuova istanza.

Se utilizzi AMI di piattaforme e applicazioni gestite e pubblicate da AWS o da Marketplace AWS È possibile eseguire il backup dei volumi di dati come istantanee separate dai volumi del sistema operativo e delle applicazioni. Utilizza quindi le istantanee del volume di dati con le AMI appena aggiornate pubblicate da AWS o da. Marketplace AWS Questo approccio richiede test e pianificazione accurati per il backup e il ripristino di tutti i dati personalizzati, incluse le informazioni di configurazione, sulle AMI appena pubblicate.

Il processo di ripristino è influenzato dalla scelta tra backup AMI o backup istantanei. Se crei AMI per fungere da backup delle istanze, devi avviare un'istanza EC2 dall'AMI come parte del processo di ripristino. Potrebbe anche essere necessario chiudere l'istanza esistente per evitare potenziali collisioni. Un esempio di potenziale collisione sono gli identificatori di sicurezza (SID) per le istanze di Windows aggiunte al dominio. Il processo di ripristino delle istantanee potrebbe richiedere lo scollegamento del volume esistente e il collegamento del volume appena ripristinato. In alternativa, potrebbe essere necessario apportare una modifica alla configurazione per indirizzare le applicazioni verso il volume appena collegato.

AWS Backup supporta sia i backup a livello di istanza come AMI sia i backup a livello di volume come istantanee separate:

- Per un backup completo di tutti i volumi EBS sull'istanza, crea un'AMI dell'istanza EC2 in esecuzione su Linux o Windows. Quando desideri eseguire il rollback, utilizza la procedura guidata di avvio dell'istanza per creare un'istanza. Nella procedura guidata di avvio dell'istanza, scegli Le mie AMI.
- Per eseguire il backup di un singolo volume, crea un'istantanea. Per ripristinare l'istantanea, consulta Creare un volume da un'istantanea. Puoi usare il AWS Management Console o il AWS Command Line Interface ()AWS CLI.

Il costo di un'AMI di istanza è l'archiviazione di tutti i volumi dell'istanza, ma non dei metadati. Il costo di uno snapshot EBS è lo storage del singolo volume. Per ulteriori informazioni sui costi di storage di volume, consulta la pagina dei prezzi di Amazon EBS.

Volumi del server

I volumi EBS sono l'opzione di storage persistente principale per Amazon EC2. Puoi utilizzare questo storage a blocchi per dati strutturati, come database, o dati non strutturati, come file in un file system su un volume.

I volumi EBS sono collocati in una zona di disponibilità specifica. I volumi vengono replicati su più server per evitare la perdita di dati a causa del guasto di un singolo componente. Per errore si intende una perdita totale o parziale del volume, a seconda delle dimensioni e delle prestazioni del volume.

I volumi EBS sono progettati per un tasso di fallimento annuo (AFR) dello 0,1-0,2 percento. Ciò rende i volumi EBS 20 volte più affidabili rispetto alle unità disco tipiche di uso comune, che si guastano

con un AFR di circa il 4%. Ad esempio, se hai 1.000 volumi EBS in esecuzione per 1 anno, dovresti aspettarti che uno o due volumi abbiano un errore.

Amazon EBS supporta anche una funzionalità di snapshot per eseguire il point-in-time backup dei dati. Tutti i tipi di volume EBS offrono funzionalità di snapshot durevoli e sono progettati per una disponibilità del 99,999%. Per ulteriori informazioni, consulta l'Amazon Compute Service Level Agreement.

Amazon EBS offre la possibilità di creare istantanee (backup) di qualsiasi volume EBS. Un'istantanea è una funzionalità di base per la creazione di backup dei volumi EBS. Uno snapshot acquisisce una copia del volume EBS e lo colloca in Amazon S3, dove viene archiviato in modo ridondante in più zone di disponibilità. Lo snapshot iniziale è una copia completa del volume; gli snapshot in corso archiviano solo le modifiche incrementali a livello di blocco. Consulta la documentazione di Amazon EC2 per dettagli su come creare snapshot di Amazon EBS.

Puoi eseguire un'operazione di ripristino, eliminare uno snapshot o aggiornare i metadati dello snapshot, come i tag, associati allo snapshot dalla console Amazon EC2 nella stessa regione in cui hai scattato lo snapshot.

Il ripristino di uno snapshot crea un nuovo volume Amazon EBS con un volume completo di dati. Se è necessario solo un ripristino parziale, è possibile collegare il volume all'istanza in esecuzione con un nome di dispositivo diverso. Quindi montalo e usa i comandi di copia del sistema operativo per copiare i dati dal volume di backup al volume di produzione.

Gli snapshot di Amazon EBS possono anche essere copiati tra AWS regioni utilizzando la funzionalità di copia degli snapshot di Amazon EBS, come descritto nella documentazione di Amazon EC2. Puoi utilizzare questa funzionalità per archiviare il backup in un'altra regione senza dover gestire la tecnologia di replica sottostante.

Stabilire volumi di server separati

È già possibile utilizzare un set standard di volumi separati per il sistema operativo, i registri, le applicazioni e i dati. Stabilendo volumi di server separati, è possibile ridurre l'ambito di impatto in caso di guasti delle applicazioni o della piattaforma causati dall'esaurimento dello spazio su disco. Questo rischio è in genere maggiore con i dischi rigidi fisici, perché non si dispone della flessibilità necessaria per espandere rapidamente i volumi. Con le unità fisiche, è necessario acquistare le nuove unità, eseguire il backup dei dati e quindi ripristinare i dati sulle nuove unità. Inoltre AWS, questo rischio è notevolmente ridotto perché è possibile utilizzare Amazon EBS per espandere i volumi assegnati. Per ulteriori informazioni, consulta la documentazione relativa ad AWS.

Mantieni volumi separati per i dati delle applicazioni, i dati utente, i log e i file di scambio in modo da poter utilizzare politiche di backup e ripristino separate per queste risorse. Separando i volumi per i dati, puoi anche utilizzare diversi tipi di volume in base ai requisiti di prestazioni e archiviazione dei dati. È quindi possibile ottimizzare e ottimizzare i costi per diversi carichi di lavoro.

Considerazioni, ad esempio, i volumi di archiviazione

Un instance store fornisce un'archiviazione temporanea di livello per le istanze. L'archiviazione è collocata all'interno dei dischi fisicamente collegati al computer host. Gli instance store sono ideali per l'archiviazione temporanea di informazioni che cambiano frequentemente, come buffer, cache, dati scratch e altri contenuti temporanei. Sono inoltre preferibili per i dati replicati su una flotta di istanze, ad esempio un pool di server Web con bilanciamento del carico.

I dati all'interno di un instance store persistono solo durante la durata delle istanze associate. Se un'istanza si riavvia (intenzionalmente o involontariamente), i dati nell'instance store persistono. Tuttavia, i dati nell'Instance Store vengono persi in una delle seguenti circostanze.

- L'unità sottostante si guasta.
- Arresto dell'istanza.
- Terminazione dell'istanza.

Pertanto, non fate affidamento su un instance store per dati preziosi a lungo termine. È invece consigliabile l'utilizzo di un'archiviazione dei dati più duratura, come Amazon S3, Amazon EBS o Amazon EFS.

Una strategia comune con i volumi di archiviazione delle istanze consiste nel mantenere i dati necessari su Amazon S3 regolarmente secondo necessità, in base al Recovery Point Objective (RPO) e al Recovery Time Objective (RTO). Puoi quindi scaricare i dati da Amazon S3 sul tuo instance store quando viene lanciata una nuova istanza. Puoi anche caricare i dati su Amazon S3 prima che un'istanza venga interrotta. Per garantire la persistenza, crea un volume EBS, collegalo alla tua istanza e copia periodicamente i dati dal volume dell'Instance Store al volume EBS. Per ulteriori informazioni, consulta l'AWS Knowledge Center.

Etichettatura e applicazione degli standard per le istantanee e le AMI EBS

L'etichettatura di tutte le AWS risorse è una pratica importante per l'allocazione dei costi, il controllo, la risoluzione dei problemi e la notifica. L'etichettatura è importante per i volumi EBS in modo che siano presenti le informazioni pertinenti necessarie per gestire e ripristinare i volumi. I tag non

vengono copiati automaticamente dalle istanze EC2 alle AMI o dai volumi di origine alle istantanee. Assicurati che il processo di backup includa i tag pertinenti provenienti da queste fonti. Ciò consente di impostare i metadati dell'istantanea, come le politiche di accesso, le informazioni sugli allegati e l'allocazione dei costi, per utilizzare questi backup in futuro. Per ulteriori informazioni sull'etichettatura AWS delle risorse, consulta il paper tecnico sulle migliori pratiche di etichettatura.

Oltre ai tag che utilizzi per tutte le AWS risorse, utilizza i seguenti tag specifici per il backup:

- ID dell'istanza di origine
- ID del volume di origine (per le istantanee)
- Descrizione del punto di ripristino

È possibile applicare le politiche di tagging utilizzando AWS Config regole e autorizzazioni IAM. IAM supporta l'uso forzato dei tag, quindi puoi scrivere policy IAM che impongono l'uso di tag specifici quando agisci sugli snapshot di Amazon EBS. Se viene tentata un'`CreateSnapshot`operazione senza che i tag definiti nella politica di autorizzazione IAM concedessero i diritti, la creazione dello snapshot fallisce e l'accesso è negato. Per ulteriori informazioni, consulta il post del blog sull'etichettatura degli snapshot di Amazon EBS sulla creazione e l'implementazione di politiche di sicurezza più solide.

Puoi utilizzare AWS Config le regole per valutare automaticamente le impostazioni di configurazione delle tue AWS risorse. Per aiutarti a iniziare, AWS Config fornisce regole personalizzabili e predefinite denominate regole gestite. Puoi anche creare regole personalizzate. Oltre a tenere AWS Config costantemente traccia delle modifiche alla configurazione tra le risorse, verifica se tali modifiche violano alcune delle condizioni delle regole. Se una risorsa viola una regola, AWS Config contrassegna la risorsa e la regola come non conformi. Tieni presente che la regola gestita dei tag obbligatori attualmente non supporta istantanee e AMI.

Creazione di backup di volumi EBS con AMI e snapshot EBS

AWS offre una vasta gamma di opzioni per la creazione e la gestione di AMI e istantanee. È possibile utilizzare l'approccio più adatto alle proprie esigenze. Un problema comune che molti clienti devono affrontare è la gestione del ciclo di vita delle istantanee e l'allineamento chiaro delle istantanee in base allo scopo, alla politica di conservazione, ecc. Senza un'etichettatura adeguata, esiste il rischio che le istantanee vengano eliminate accidentalmente o come parte di un processo di pulizia automatico. Potresti anche finire per pagare per istantanee obsolete che vengono conservate perché non si capisce chiaramente se siano ancora necessarie.

Preparazione di un volume EBS prima di creare un'istantanea o un AMI

Prima di scattare un'istantanea o creare un AMI, effettua i preparativi necessari per il volume EBS. La creazione di un'AMI comporta la creazione di una nuova istantanea per ogni volume EBS collegato all'istanza, quindi questi preparativi si applicano anche alle AMI.

Puoi scattare un'istantanea di un volume EBS collegato utilizzato da un'istanza EC2 accesa. Tuttavia, le istantanee acquisiscono solo i dati che sono stati scritti sul volume EBS al momento dell'emissione del comando snapshot. Ciò potrebbe escludere tutti i dati che sono stati memorizzati nella cache dalle applicazioni o dal sistema operativo. È consigliabile che il sistema si trovi in uno stato in cui non esegua alcun I/O. Idealmente, la macchina non accetta traffico e si trova in uno stato di arresto, ma ciò è raro in quanto le operazioni IT 24 ore su 24, 7 giorni su 7, diventano la norma. Se è possibile scaricare i dati dalla memoria di sistema sul disco utilizzato dalle applicazioni e sospendere la scrittura di qualsiasi file sul volume per un periodo sufficiente a scattare un'istantanea, l'istantanea dovrebbe essere completa.

Per eseguire un backup pulito, è necessario disattivare il database o il file system. Il modo in cui eseguire questa operazione dipende dal database o dal file system in uso.

Il processo per un database è il seguente:

1. Se possibile, imposta il database in modalità di backup a caldo.
2. Esegui i comandi snapshot di Amazon EBS.
3. Disattiva il database dalla modalità di backup a caldo o, se utilizzi una replica di lettura, interrompi l'istanza di replica di lettura.

Il processo per un file system è simile, ma dipende dalle funzionalità del sistema operativo o del file system. Ad esempio, XFS è un file system in grado di cancellare i dati per un backup coerente. Per ulteriori informazioni, vedere xfs_freeze. In alternativa, è possibile facilitare questo processo utilizzando un gestore di volumi logico che supporti il congelamento degli I/O.

Tuttavia, se non riesci a cancellare o mettere in pausa tutte le scritture di file sul volume, procedi come segue:

1. Smonta il volume dal sistema operativo.
2. Esegui il comando snapshot.
3. Rimontate il volume per ottenere un'istantanea coerente e completa. È possibile rimontare e utilizzare il volume mentre lo stato dell'istantanea è in sospeso.

Il processo di creazione delle istantanee continua in background e la creazione delle istantanee è rapida e cattura un momento nel tempo. I volumi di cui stai eseguendo il backup vengono smontati solo per pochi secondi. È possibile pianificare una piccola finestra di backup in cui è prevista un'interruzione e gestirla dai clienti con garbo.

Quando crei un'istantanea per un volume EBS che funge da dispositivo root, interrompi l'istanza prima di scattare l'istantanea. Windows fornisce il Volume Shadow Copy Service (VSS) per aiutare a creare istantanee coerenti con l'applicazione. AWS fornisce un documento Systems Manager che è possibile eseguire per eseguire backup a livello di immagine delle applicazioni compatibili con VSS. Gli snapshot includono dati delle transazioni in sospeso tra queste applicazioni e il disco. Non è necessario chiudere le istanze o disconnetterle quando si esegue il backup di tutti i volumi collegati. Per ulteriori informazioni, consulta la documentazione relativa ad AWS.

> **Note**
>
> Se stai creando un'AMI Windows in modo da poter distribuire un'altra istanza simile, usa EC2Config o EC2Launch per Sysprep la tua istanza. Quindi crea un AMI dall'istanza interrotta. Sysprep rimuove informazioni univoche dall'istanza Amazon EC2 di Windows, inclusi i SID, il nome del computer e i driver. I SID duplicati possono causare problemi con Active Directory, Windows Server Update Services (WSUS), problemi di accesso, attivazione delle chiavi di volume di Windows, Microsoft Office e prodotti di terze parti. Non utilizzare Sysprep con l'istanza se l'AMI è a scopo di backup e si desidera ripristinare la stessa istanza con tutte le sue informazioni uniche intatte.

Creazione manuale di istantanee dei volumi EBS dalla console

Crea istantanee dei volumi appropriati o dell'intera istanza prima di apportare modifiche importanti che non sono state completamente testate sull'istanza. Ad esempio, potresti voler creare un'istantanea prima di aggiornare o applicare patch al software dell'applicazione o del sistema sull'istanza.

È possibile creare un'istantanea manualmente dalla console. Sulla console Amazon EC2, nella pagina Elastic Block Store Volumes, seleziona il volume di cui desideri eseguire il backup. Quindi, nel menu Azioni, scegli Crea istantanea. Puoi cercare i volumi collegati a un'istanza specifica inserendo l'ID dell'istanza nella casella del filtro.

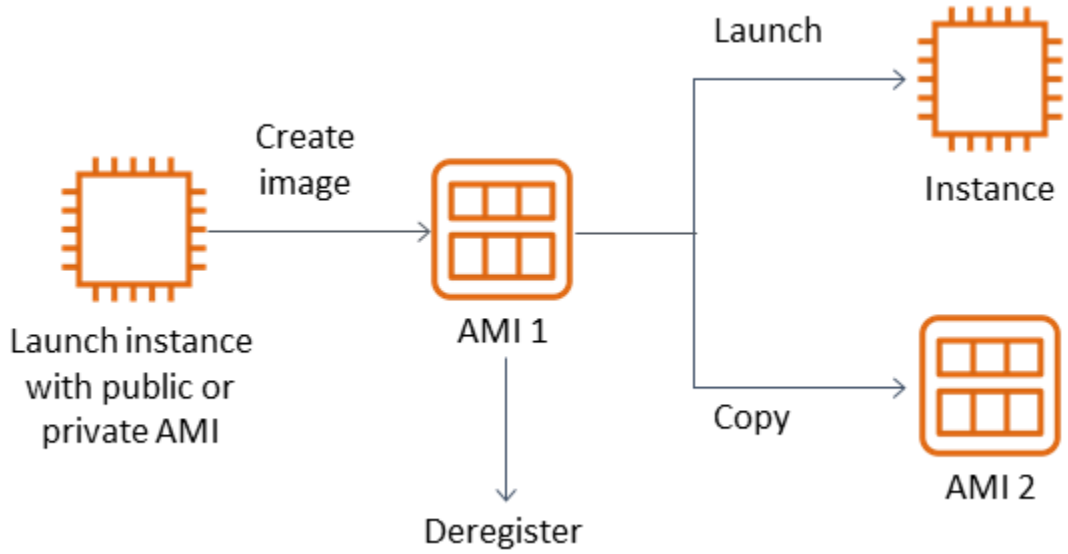
Inserisci una descrizione e aggiungi i tag appropriati. Aggiungi un `Name` tag per facilitare la ricerca del volume in un secondo momento. Aggiungi qualsiasi altro tag appropriato in base alla tua strategia di tagging.

Creazione di AMI

Un AMI fornisce le informazioni necessarie per avviare un'istanza. L'AMI include il volume root e le istantanee dei volumi EBS collegati all'istanza al momento della creazione dell'immagine. Non puoi avviare nuove istanze solo dalle istantanee EBS; devi avviare nuove istanze da un'AMI.

Quando crei un'AMI, questa viene creata nell'account e nella regione che stai utilizzando. Il processo di creazione dell'AMI crea istantanee Amazon EBS per ogni volume collegato all'istanza e l'AMI fa riferimento a queste istantanee di Amazon EBS. Queste istantanee risiedono in Amazon S3 e sono estremamente resistenti.

Dopo aver creato un'AMI della tua istanza EC2, puoi utilizzare l'AMI per ricreare l'istanza o avviare altre copie dell'istanza. Puoi anche copiare le AMI da una regione all'altra per la migrazione delle applicazioni o il DR.



È necessario creare un'AMI da un'istanza EC2 a meno che non si stia migrando una macchina virtuale, ad esempio una macchina virtuale VMWARE, verso. AWS Per creare un'AMI dalla console Amazon EC2, seleziona l'istanza, scegli Azioni, scegli Immagine, quindi scegli Crea immagine.

Amazon Data Lifecycle Manager

Per automatizzare la creazione, la conservazione e l'eliminazione degli snapshot di Amazon EBS, puoi utilizzare Amazon Data Lifecycle Manager. L'automazione della gestione degli snapshot ti aiuta a fare quanto segue:

- Proteggere i dati importanti applicando una pianificazione regolare di backup.
- Conservare i backup come richiesto dai revisori o dalla conformità interna.
- Ridurre i costi di archiviazione eliminando i backup obsoleti.

Utilizzando Amazon Data Lifecycle Manager, puoi automatizzare il processo di gestione degli snapshot per le istanze EC2 (e i relativi volumi EBS collegati) o volumi EBS separati. Supporta opzioni come la copia tra regioni, in modo da poter copiare automaticamente le istantanee in altre regioni. AWS La copia delle istantanee in regioni alternative è un approccio per supportare le attività di DR e le opzioni di ripristino in una regione alternativa. Puoi anche utilizzare Amazon Data Lifecycle Manager per creare una policy sul ciclo di vita degli snapshot che supporti il ripristino rapido degli snapshot.

Amazon Data Lifecycle Manager è una funzionalità inclusa di Amazon EC2 e Amazon EBS. Amazon Data Lifecycle Manager è gratuito.

AWS Backup

AWS Backup è unico di Amazon Data Lifecycle Manager perché puoi creare un piano di backup che include risorse su più servizi. AWS Puoi coordinare il backup per coprire le risorse che utilizzi insieme anziché coordinare i backup delle risorse singolarmente.

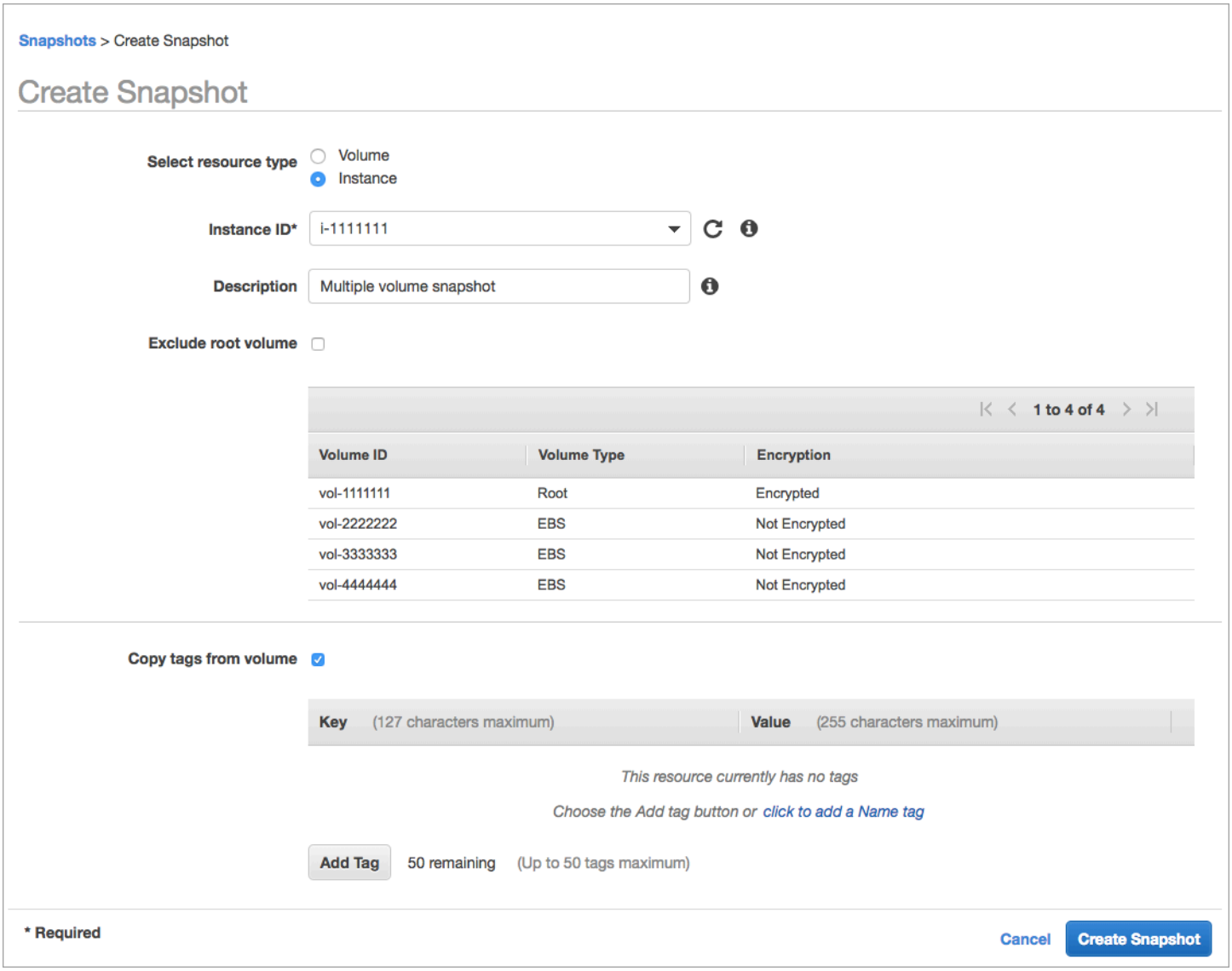
AWS Backup include anche il concetto di archivi di backup, che possono limitare l'accesso ai punti di ripristino per i backup completati. Le operazioni di ripristino possono essere avviate AWS Backup anziché procedere su ogni singola risorsa e ripristinare il backup creato. AWS Backup include anche una serie di funzionalità aggiuntive, come la gestione degli audit e la reportistica. Per ulteriori informazioni, consulta la sezione Backup e ripristino tramiteAWS Backup di questa guida.

Esecuzione di backup a più volumi

Se si desidera eseguire il backup dei dati sui volumi EBS in un array RAID utilizzando istantanee, le istantanee devono essere coerenti. Ciò è necessario perché gli snapshot di questi volumi

vengono creati in modo indipendente. Il ripristino dei volumi EBS in un array RAID da istantanee non sincronizzate riduce l'integrità dell'array.

Per creare un set coerente di istantanee per il tuo array RAID, utilizza l'operazione CreateSnapshotsAPI o accedi alla console Amazon EC2 e scegli Elastic Block Store, Snapshots, Create Snapshot.



Le istantanee delle istanze che hanno più volumi collegati in una configurazione RAID vengono prese collettivamente come istantanee multivolume. Le istantanee multivolume forniscono istantanee coordinate dai dati e point-in-time coerenti con gli arresti anomali su più volumi EBS collegati a un'istanza EC2. Non è necessario impedire all'istanza di coordinarsi tra i volumi per ottenere coerenza, poiché le istantanee vengono acquisite automaticamente su più volumi EBS. Dopo l'avvio

dello snapshot per i volumi (in genere uno o due secondi), il file system può continuare le sue operazioni.

Dopo che gli snapshot vengono creati, ogni snapshot viene considerato come uno snapshot singolo. È possibile eseguire tutte le operazioni di istantanea, come il ripristino, l'eliminazione e la copia tra aree geografiche e account, come si farebbe con un'istantanea a volume singolo. È inoltre possibile contrassegnare le istantanee a più volumi come se si trattasse di un'istantanea a volume singolo. Ti consigliamo di etichettare le istantanee multivolume per gestirle collettivamente durante il ripristino, la copia o la conservazione. Per ulteriori informazioni, consulta la documentazione di AWS.

È inoltre possibile eseguire questi backup da un gestore di volumi logico o da un backup a livello di file system. In questi casi, l'utilizzo di un agente di backup tradizionale consente il backup dei dati sulla rete. Diverse soluzioni di backup basate su agenti sono disponibili su Internet e in. Marketplace AWS

Un approccio alternativo consiste nel creare una replica dei volumi di sistema primari esistenti su un unico volume di grandi dimensioni. Ciò semplifica il processo di backup, poiché è necessario eseguire il backup di un solo volume di grandi dimensioni e il backup non viene eseguito sul sistema principale. Tuttavia, è necessario innanzitutto determinare se il singolo volume è in grado di fornire prestazioni sufficienti durante il backup e se la dimensione massima del volume è appropriata per l'applicazione.

Protezione dei backup di Amazon EC2

È importante considerare la sicurezza dei backup e prevenire l'eliminazione accidentale o dolosa dei backup. A tal fine è possibile utilizzare diversi approcci collettivamente. Per evitare la perdita dei backup critici a causa di una violazione della sicurezza, si consiglia di copiare i backup su un altro account. AWS Se disponi di più account AWS, puoi designare un account separato come account di archiviazione in cui tutti gli altri account possono copiare i backup. Ad esempio, puoi farlo con un backup su più account. AWS Backup

Il tuo piano di disaster recovery potrebbe anche richiedere la possibilità di riprodurre istanze EC2 in un'altra regione AWS in caso di guasto regionale. Puoi raggiungere questo obiettivo copiando i backup in un'altra regione all'interno dello stesso account. Ciò può fornire un ulteriore livello di protezione dall'eliminazione accidentale e supportare gli obiettivi di disaster recovery (DR). AWS Backup fornisce supporto per backup interregionali.

Prendi in considerazione la possibilità di bloccare le autorizzazioni IAM per le azioni ec2: DeleteSnapshot ed ec2:. DeregisterImage Puoi invece lasciare che le tue politiche e i tuoi metodi di conservazione gestiscano il ciclo di vita degli snapshot EBS e delle AMI Amazon EC2. Il blocco delle

azioni di eliminazione è un modo per implementare una strategia WORM (Write-Once, Read-Many) per gli snapshot EBS. Puoi anche utilizzare AWS Backup Vault Lock, che fornisce supporto per le istantanee EBS e altre risorse. AWS

Inoltre, valuta la possibilità di bloccare la possibilità per gli utenti di condividere AMI e snapshot EBS bloccando le azioni ec2: ed ec2: IAM. ModifyImageAttribute ModifySnapshotAttribute Ciò impedirà che le AMI e le istantanee vengano condivise con AWS account esterni all'organizzazione. Se lo utilizzi AWS Backup, limita gli utenti a eseguire operazioni simili sugli archivi di backup. Per ulteriori informazioni, consulta la sezione AWS Backup di questa guida.

Amazon EC2 include una funzionalità Recycle Bin che può aiutarti a ripristinare istantanee EBS eliminate accidentalmente. Se consenti ai tuoi utenti di eliminare le istantanee, attiva questa funzionalità in modo che le istantanee necessarie non vengano eliminate definitivamente. Gli utenti devono prestare particolare attenzione all'eliminazione di più istantanee, poiché la console Amazon EC2 consente di selezionare più istantanee ed eliminarle in un'unica operazione. Inoltre, fai attenzione quando usi gli script di pulizia e l'automazione in modo da non eliminare involontariamente le istantanee di cui hai bisogno. La funzione Recycle Bin aiuta a fornire protezione da questo tipo di situazioni.

Archiviazione delle istantanee EBS

L'archiviazione delle istantanee EBS può essere un metodo conveniente per conservare una copia di un volume a scopo di riferimento che non intendi ripristinare per 90 o più giorni. Questo può essere un buon passaggio intermedio prima di eliminare definitivamente tutte le istantanee correlate per un volume EBS. Ad esempio, potresti prendere in considerazione l'archiviazione delle istantanee come end-of-lifecycle passaggio per i volumi EBS che non vengono più utilizzati. L'archiviazione anziché l'eliminazione può anche essere un metodo di conservazione delle eliminazioni più conveniente rispetto all'utilizzo del Cestino.

Automatizzazione della creazione di snapshot e AMI con Systems Manager AWS CLI, gli e gli SDK AWS

L'approccio di backup potrebbe richiedere operazioni prima e dopo la creazione di un'istantanea o di un'AMI. Ad esempio, potrebbe essere necessario interrompere e avviare i servizi per disattivare il file system. Oppure potresti dover interrompere e avviare l'istanza durante la creazione dell'AMI. Potrebbe anche essere necessario creare collettivamente backup di più componenti dell'architettura, ciascuno con le proprie fasi precedenti e successive alla creazione.

È possibile ridurre i tempi di manutenzione dei backup automatizzando il processo e verificando che il processo di backup venga applicato in modo coerente. Per automatizzare le operazioni personalizzate di pre-creazione e post-creazione, crea uno script per il processo di backup utilizzando e l'SDK. AWS CLI

L'automazione può essere definita in un runbook di Systems Manager che può essere eseguito su richiesta o durante una finestra di manutenzione di Systems Manager. Puoi concedere ai tuoi utenti l'accesso per eseguire i runbook di Systems Manager senza dover concedere loro le autorizzazioni per i comandi dirompenti di Amazon EC2. Questo può anche aiutarti a verificare che il processo di backup e i tag vengano applicati in modo coerente dagli utenti. Puoi usare i CreateImage runbook AWS CreateSnapshot e AWS per creare snapshot e AMI oppure puoi concedere ad altri utenti le autorizzazioni per utilizzarli. Systems Manager include anche i UpdateWindowsAmi runbook AWS UpdateLinuxAmi e AWS per automatizzare l'applicazione di patch e la creazione di AMI.

È inoltre possibile utilizzare AWS CLI and AWS Tools for Windows PowerShellper automatizzare il processo di creazione di istantanee e AMI. Puoi utilizzare il AWS CLI comando aws ec2 create-snapshot per creare un'istantanea di un volume EBS come fase iniziale dell'automazione. Puoi utilizzare il comando aws ec2 create-snapshots per creare istantanee sincronizzate e coerenti con gli arresti anomali di tutti i volumi collegati alla tua istanza EC2.

Puoi usare la AWS CLI per creare nuove AMI. Puoi usare il comando aws ec2 register-image per creare una nuova immagine per la tua istanza EC2. Per automatizzare lo spegnimento, la creazione di immagini e il riavvio delle istanze, combina questo comando con i comandi aws ec2 stop-instances e aws ec2 start-instances.

Ripristino di un volume Amazon EBS o di un'istanza EC2

Se devi ripristinare solo un singolo volume collegato a un'istanza EC2, puoi ripristinare quel volume separatamente, scollegare il volume esistente e collegare il volume ripristinato all'istanza EC2. Se devi ripristinare un'intera istanza EC2, inclusi tutti i volumi associati, devi utilizzare un backup Amazon Machine Image (AMI) dell'istanza.

Per ridurre i tempi di ripristino e l'impatto sulle applicazioni e sui processi dipendenti, il processo di ripristino deve considerare la risorsa che sta sostituendo. Per ottenere risultati ottimali, testate regolarmente il processo di ripristino in ambienti inferiori (ad esempio, non di produzione) per verificare che soddisfi il Recovery Point Objective (RPO) e il Recovery Time Objective (RTO) e che il processo di ripristino funzioni come previsto. Considerate l'impatto del processo di ripristino sulle applicazioni e sui servizi che dipendono dall'istanza che state ripristinando, quindi coordinate il

ripristino secondo necessità. Cercate di automatizzare e testare il processo di ripristino il più possibile per ridurre il rischio che il processo di ripristino fallisca o venga implementato in modo incoerente.

Se utilizzi Elastic Load Balancing, con più istanze che gestiscono il traffico, puoi mettere fuori servizio un'istanza guasta o danneggiata. Quindi puoi ripristinare una nuova istanza per sostituirla mentre le altre istanze continuano a servire il traffico senza interruzioni per gli utenti.

I seguenti processi di ripristino descritti si riferiscono alle istanze che non utilizzano Elastic Load Balancing:

- Ripristino di singoli file e directory dalle istantanee EBS
- Ripristino di un volume EBS da uno snapshot Amazon EBS
- Creazione o ripristino di un'istanza EC2 da uno snapshot EBS
- Ripristino di un'istanza in esecuzione da un'AMI

Ripristino di file e directory dalle istantanee EBS

Le istantanee EBS forniscono una replica point-in-time esatta del volume originale utilizzato per creare l'istantanea. Per ripristinare singoli file o cartelle, devi fare quanto segue:

1. Innanzitutto, ripristina il volume dall'istantanea EBS che contiene i file o le directory.
2. Collega il volume all'istanza EC2 in cui desideri ripristinare i file.
3. Copia i file dal volume ripristinato al volume dell'istanza EC2.
4. Scollega ed elimina il volume ripristinato.

Ripristino di un volume EBS da uno snapshot Amazon EBS

Puoi ripristinare un volume collegato a un'istanza EC2 esistente creando un volume dalla relativa istantanea e collegandolo all'istanza. Puoi utilizzare la console, le operazioni dell' AWS CLIAPI o dell'API per creare un volume da un'istantanea esistente. È quindi possibile montare il volume sull'istanza utilizzando il sistema operativo.

Tieni presente che i dati di uno snapshot di Amazon EBS vengono caricati in modo asincrono in un volume EBS. Se un'applicazione accede al volume in cui i dati non vengono caricati, la latenza è superiore al normale durante il caricamento dei dati da Amazon S3. Per evitare questo impatto per le applicazioni sensibili alla latenza, sono disponibili due opzioni:

- È possibile inizializzare il volume EBS.
- A un costo aggiuntivo, Amazon EBS supporta il ripristino rapido degli snapshot, che elimina la necessità di inizializzare il volume.

Se stai sostituendo un volume che deve utilizzare lo stesso punto di montaggio, smonta quel volume in modo da poter montare il nuovo volume al suo posto. Per smontare il volume, interrompete innanzitutto tutti i processi che utilizzano il volume. Se state sostituendo il volume principale, dovete arrestare l'istanza prima di poter scollegare il volume principale.

Ad esempio, segui questi passaggi per ripristinare un volume su un point-in-time backup precedente utilizzando la console:

1. Sulla console Amazon EC2, nel menu Elastic Block Store, scegli Snapshots.
2. Cerca lo snapshot che desideri ripristinare e selezionalo.
3. Scegli Azioni, quindi scegli Crea volume.
4. Crea il nuovo volume nella stessa zona di disponibilità dell'istanza EC2.
5. Nella console Amazon EC2, seleziona l'istanza.
6. Nei dettagli dell'istanza, prendi nota del nome del dispositivo che desideri sostituire nella voce Root device o Block Devices.
7. Allega il volume. Il processo è diverso per i volumi root e per i volumi non root.

   Per i volumi root:

   a. Arrestare l'istanza EC2.
   b. Nel menu EC2 Elastic Block Store Volumes, seleziona il volume radice che desideri sostituire.
   c. Scegli Azioni, quindi scegli Scollega volume.
   d. Nel menu EC2 Elastic Block Store Volumes, seleziona il nuovo volume.
   e. Scegli Azioni, quindi scegli Allega volume.
   f. Seleziona l'istanza a cui desideri collegare il volume e usa lo stesso nome di dispositivo che hai annotato in precedenza.

   Per i volumi non root:

   a. Nel menu EC2 Elastic Block Store Volumes, seleziona il volume non root che desideri sostituire.
   b. Scegli Azioni, quindi scegli Scollega volume.

c. Collega il nuovo volume selezionandolo nel menu EC2 Elastic Block Store Volumes e quindi scegliendo Azioni, Allega volume. Seleziona l'istanza a cui desideri collegarlo, quindi seleziona il nome di un dispositivo disponibile.

d. Utilizzando il sistema operativo dell'istanza, smonta il volume esistente, quindi monta il nuovo volume al suo posto.

   In Linux, puoi usare il `umount` comando. In Windows, è possibile utilizzare un gestore di volumi logici (LVM) come l'utilità di sistema Disk Management.

e. Scollega tutti i volumi precedenti che potresti sostituire selezionandoli nel menu EC2 Elastic Block Store Volumes e quindi scegliendo Azioni, Scollega volume.

Puoi anche utilizzarlo AWS CLI in combinazione con i comandi del sistema operativo per automatizzare questi passaggi.

Creazione o ripristino di un'istanza EC2 da uno snapshot EBS

Per creare un backup che verrà utilizzato per ripristinare un'intera istanza EC2, consigliamo di creare un'Amazon Machine Image (AMI). Le AMI acquisiscono informazioni sulla macchina, ad esempio il tipo di virtualizzazione. Inoltre, creano istantanee per ogni volume collegato all'istanza EC2, incluse le mappature dei dispositivi, in modo che possano essere ripristinati nella stessa configurazione.

Tuttavia, se devi utilizzare uno snapshot EBS per ripristinare un'istanza, crea prima un'AMI da un'istantanea EBS che diventerà il volume root per la tua nuova istanza EC2:

1. Sulla console Amazon EC2, nel menu Elastic Block Store, scegli Snapshots.
2. Cerca lo snapshot che verrà utilizzato per creare il volume root per la tua nuova istanza EC2 e selezionalo.
3. Scegli Azioni, quindi scegli Crea immagine da istantanea.
4. Immettete un nome per l'immagine (ad esempio,`YYYYMMDD-restore-for-i-012345678998765de`) e scegliete le opzioni appropriate per la nuova immagine.

Dopo che l'immagine è stata creata e resa disponibile, puoi avviare una nuova istanza EC2 che utilizzerà lo snapshot EBS per il volume root.

Ripristino di un'istanza in esecuzione da un'AMI

Puoi richiamare una nuova istanza dal backup dell'AMI per sostituire un'istanza esistente e in esecuzione. Un approccio consiste nel fermare l'istanza esistente, mantenerla offline mentre si avvia una nuova istanza dall'AMI ed eseguire gli aggiornamenti necessari. Questo approccio riduce il rischio di conflitti dovuti all'esecuzione simultanea di entrambe le istanze. È un approccio accettabile se i servizi forniti dall'istanza non sono disponibili o se si esegue il ripristino durante una finestra di manutenzione. Dopo aver testato la nuova istanza, puoi riassegnare tutti gli indirizzi IP elastici allocati alla vecchia istanza. Quindi puoi aggiornare qualsiasi record DNS (Domain Name Service) in modo che punti alla nuova istanza.

Tuttavia, se durante un ripristino devi ridurre al minimo i tempi di inattività dell'istanza in servizio, prendi in considerazione l'avvio e il test di una nuova istanza dal backup dell'AMI. Sostituisci quindi l'istanza esistente con la nuova istanza.

Mentre entrambe le istanze sono in esecuzione, è necessario evitare che la nuova istanza provochi collisioni a livello di piattaforma o di applicazione. Ad esempio, potrebbero verificarsi problemi con le istanze di Windows aggiunte al dominio che vengono eseguite con gli stessi SID e lo stesso nome di computer. È possibile riscontrare problemi simili con le applicazioni e i servizi di rete che richiedono identificatori univoci.

Per evitare che altri server e servizi si connettano alla nuova istanza prima che sia pronta, utilizza i gruppi di sicurezza per bloccare temporaneamente tutte le connessioni in entrata per la nuova istanza ad eccezione del tuo indirizzo IP per l'accesso e il test. Puoi anche bloccare temporaneamente le connessioni in uscita per la nuova istanza per impedire a servizi e applicazioni di avviare connessioni o aggiornamenti ad altre risorse. Quando la nuova istanza è pronta, interrompi l'istanza esistente, avvia servizi e processi sulla nuova istanza, quindi sblocca tutte le connessioni di rete in entrata o in uscita che hai implementato.

Backup e ripristino dall'infrastruttura locale aAWS

Puoi usareAWSper l'archiviazione durevole e fuori sede dei backup dell'infrastruttura locale. UsandoAWScon i servizi di storage in questo scenario, è possibile concentrarsi sulle attività di backup e archiviazione. Non devi preoccuparti della fornitura, della scalabilità o della capacità dell'infrastruttura di storage per le tue attività di backup.

Amazon S3 e Amazon S3 Glacier forniscono ampie operazioni API e SDK per integrare questi servizi nei tuoi approcci di backup e ripristino nuovi ed esistenti. Ciò offre inoltre ai fornitori di software di backup modi per integrare direttamente le proprie applicazioni conAWSsoluzioni di archiviazione.

In questo scenario, il software di backup e archiviazione utilizzato nell'infrastruttura locale si interfaccia direttamente conAWStramite le operazioni API. Perché il software di backup èAWS-consapevole, esegue il backup dei dati dai server locali direttamente su Amazon S3 o Amazon S3 Glacier.

Se il software di backup esistente non supporta in modo nativoAWSCloud, puoi usare Storage Gateway. Storage Gateway, un servizio di cloud storage, consente ai sistemi locali di accedere a uno storage cloud scalabile. Supporta protocolli di storage standard aperti che funzionano con le applicazioni esistenti, archiviando al contempo in modo sicuro i dati crittografati in Amazon S3 o Amazon S3 Glacier. È possibile utilizzare Storage Gateway come parte di un approccio di backup e ripristino per i carichi di lavoro di storage locali basati su blocchi.

Storage Gateway è utile in scenari ibridi in cui si desidera passare allo storage basato sul cloud per i backup. Storage Gateway consente inoltre di ridurre gli investimenti di capitale nello storage locale. Storage Gateway viene implementato come VM o appliance hardware dedicata. Questa guida si concentra su come Storage Gateway si applica al backup e al ripristino.

Storage Gateway offre tre diverse opzioni per soddisfare requisiti diversi:

- Un gateway di file per archiviare i file di dati delle applicazioni e le immagini di backup come oggetti durevoli sullo storage cloud Amazon S3 utilizzando l'accesso basato su SMB o NFS.
- Un gateway di volume per presentare volumi di storage a blocchi iSCSI basati su cloud alle applicazioni locali. Un gateway di volumi fornisce una cache locale o volumi completi in locale, archiviando al contempo copie complete dei volumi nelAWSNuvola.
- Un gateway su nastro per indirizzare un software di backup affidabile a un gateway di storage locale che, a sua volta, si connette ad Amazon S3 e Amazon S3 Glacier. Questa opzione offre

la scalabilità e la durabilità del cloud per una conservazione sicura a lungo termine senza interrompere gli investimenti o i processi esistenti.

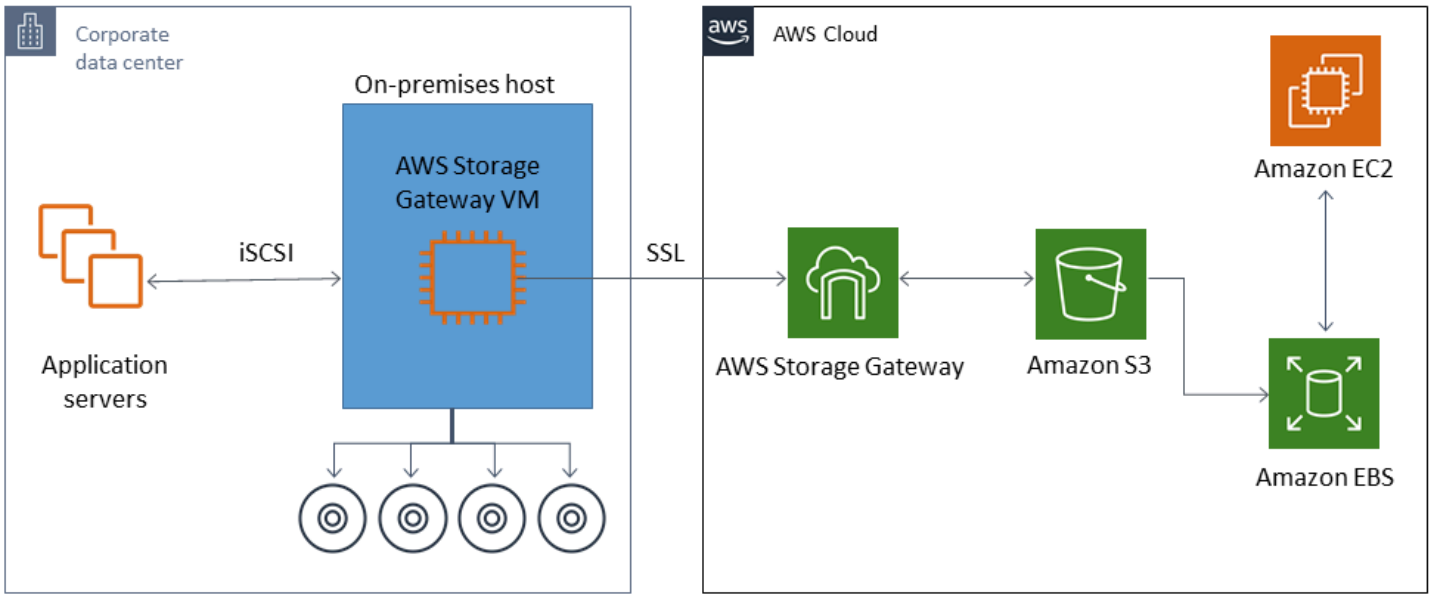
Gateway di file

Molte organizzazioni iniziano il loro percorso verso il cloud trasferendo dati secondari e terziari, come i backup, nel cloud. Il supporto delle interfacce SMB e NFS di un file gateway consente ai gruppi IT di trasferire i processi di backup dai sistemi di backup locali esistenti al cloud. Le applicazioni di backup, gli strumenti di database nativi o gli script in grado di scrivere su SMB o NFS possono scrivere su un gateway di file. Il file gateway archivia i backup come oggetti Amazon S3 di dimensioni fino a 5 TiB. Con una cache locale di dimensioni adeguate, i backup recenti possono essere utilizzati per ripristini rapidi in loco. Le esigenze di conservazione a lungo termine vengono soddisfatte suddividendo i backup su livelli di storage a basso costo di S3 Standard-Infrequent Access e Amazon S3 Glacier.

File gateway fornisce una rampa d'accesso per lo storage basato su blocchi su Amazon S3 per backup offsite estremamente duraturi. È particolarmente utile per gli scenari in cui un file di recente backup deve essere ripristinato rapidamente. Poiché un file gateway supporta i protocolli SMB e NFS, gli utenti possono accedere ai file nello stesso modo in cui accederebbero a una condivisione di file di rete. Puoi anche sfruttare le funzionalità di controllo delle versioni degli oggetti di Amazon S3. Utilizzando il controllo delle versioni degli oggetti, è possibile ripristinare le versioni precedenti degli oggetti di un file e quindi accedervi facilmente utilizzando SMB o NFS.

Gateway di volumi

Un gateway di volume consente di effettuare il provisioning di volumi di storage a blocchi iSCSI basati sul cloud per i server locali. Il volume gateway archivia i dati del volume su Amazon S3 per uno storage offsite durevole e scalabile basato sul cloud. Un gateway di volume facilita l'acquisizione completapoint-in-timeistantanee dei tuoi volumi e archiviazione nel cloud come istantanee di Amazon EBS. Dopo essere stati archiviati come istantanee, interi volumi possono essere ripristinati come volumi EBS e collegati a istanze EC2, accelerando una soluzione di ripristino di emergenza basata su cloud. I volumi possono anche essere ripristinati su Storage Gateway, consentendo alle applicazioni locali di tornare allo stato precedente.



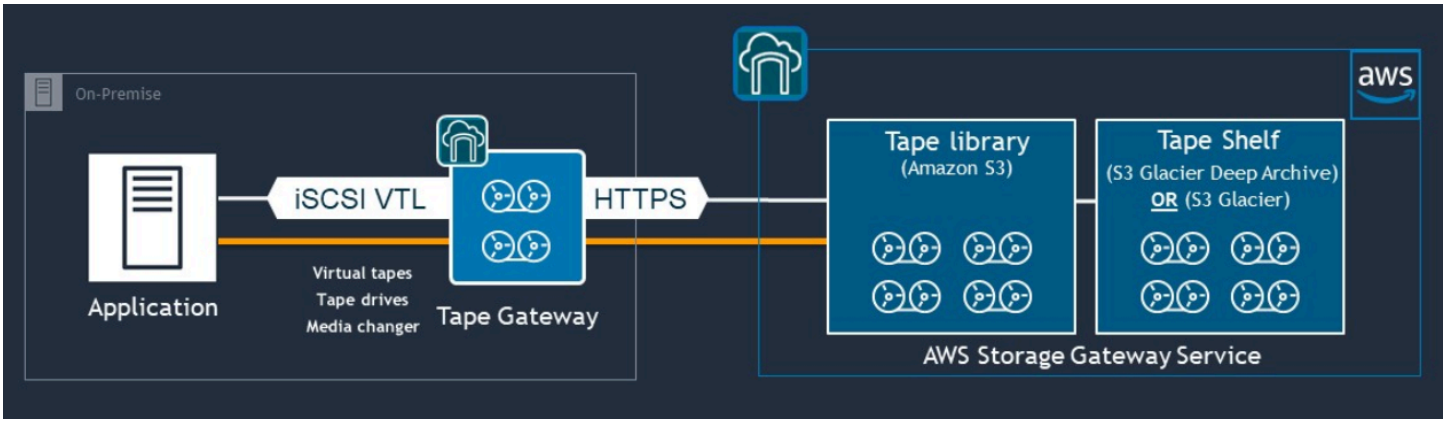
Poiché un gateway di volume si integra con la funzionalità di volume Amazon EBS di Amazon EC2, puoi usareAWS Backupper automatizzare e pianificare il processo di creazione di istantanee. Un gateway di volume offre i vantaggi aggiuntivi di snapshot e funzionalità di etichettatura di Amazon EBS durevoli supportati da Amazon S3. Per ulteriori informazioni, vedereDocumentazione relativa alle istantanee di Amazon EBS.

Gateway di nastri

Un gateway su nastro offre l'elevata durata, lo storage su più livelli a basso costo e le funzionalità complete di Amazon S3 e Amazon S3 Glacier per il tuo negozio di backup su nastro virtuale esterno. Tutti i nastri virtuali archiviati in Amazon S3 e Amazon S3 Glacier vengono replicati e archiviati in almeno tre zone di disponibilità distribuite geograficamente. I tuoi nastri virtuali sono protetti da una durata di 11".

AWSesegue inoltre controlli di stabilità su base regolare per confermare che i dati possono essere letti e che non sono stati introdotti errori. Tutti i nastri archiviati in Amazon S3 sono protetti mediante crittografia lato server utilizzando chiavi predefinite oAWS KMSchiavi. Inoltre, si evitano i rischi di sicurezza fisica associati alla portabilità dei nastri. Con un gateway a nastro si ottengono dati corretti, rispetto all'archiviazione fuori sede dei nastri, dove è possibile ricevere un nastro errato o rotto durante il ripristino.

Puoi risparmiare sui costi di archiviazione mensili quando archivi i tuoi dati in Amazon S3. Puoi risparmiare ancora di più per i tuoi requisiti di archiviazione a lungo termine utilizzando S3 Glacier Deep Archive.



Un gateway a nastro funge da libreria a nastro virtuale (VTL) che si estende dall'ambiente locale a servizi di storage altamente scalabili, ridondanti e durevoli: Amazon S3, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive.

Il tape gateway presenta Storage Gateway all'applicazione di backup esistente sotto forma di VTL basato su iSCSI a standard aperto, con un convertitore multimediale virtuale e unità nastro virtuali. Puoi continuare a utilizzare le applicazioni e i flussi di lavoro di backup esistenti mentre scrivi su una raccolta di nastri virtuali archiviati su Amazon S3 estremamente scalabile. Quando non è più necessario l'accesso immediato o frequente ai dati su un nastro virtuale, l'applicazione di backup può archiviarli in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive, riducendo ulteriormente i costi di storage.

È possibile recuperare un nastro archiviato in S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive in genere in 3-5 ore o 12 ore, rispettivamente. Il tape gateway può essere utilizzato con un'applicazione di backup compatibile con l'interfaccia della libreria a nastro basata su iSCSI per l'accesso ai nastri virtuali. Considera anche la dimensione minima di archiviazione di 100 GB per nastro. Per ulteriori informazioni, consulta l'elenco diapplicazioni di backup di terze partiche supportano gateway a nastro.

Backup e ripristino delle applicazioni daAWSal tuo data center

Potresti avere una politica che richiede l'implementazione di uno scenario come DR o Business Continuity per i tuoi carichi di lavoro basati su cloud e l'infrastruttura locale. Se hai già un framework di backup dei dati per i server locali, puoi estenderlo al tuoAWSrisorse su una connessione VPN o tramiteAWS Direct Connect. È possibile installare l'agente di backup sulle istanze EC2 e eseguire il backup dei dati e delle applicazioni in base alle policy di protezione dei dati. Puoi anche utilizzare Amazon S3 come servizio intermedio per archiviare i backup a livello di applicazione. È quindi possibile utilizzare le operazioni API, gli SDK o ilAWS CLIper ripristinare i dati nell'ambiente locale.

Per eseguire il backup dei dati inAWSservizi diversi da Amazon EC2, utilizzare ilAWS CLI, SDK e operazioni API per estrarre i dati nel formato desiderato. Quindi copiare i dati in Amazon S3 e copiarli da Amazon S3 al tuo ambiente locale. Alcuni servizi forniscono esportazione diretta in Amazon S3. Amazon RDS supporta ad esempiobackup nativodei database Microsoft SQL Server in Amazon S3.

Backup e ripristino diAWS servizi nativi per il cloud

L'approccio di backup e ripristino dovrebbe coprire iAWS servizi utilizzati nei carichi di lavoro. AWSoffre funzionalità e opzioni specifiche del servizio per la gestione e l'interazione con i dati. Puoi utilizzare la consoleAWS CLI, gli SDK e le operazioni API per implementare il backup e il ripristino perAWS i servizi che stai utilizzando. Questa guida tratta Amazon RDS e Amazon DynamoDB come esempi. AWS Backupsupporta sia DynamoDB che Amazon RDS e deve essere utilizzato se soddisfa i tuoi requisiti.

Backup e ripristino per Amazon RDS

Amazon RDS include funzionalità per automatizzare i backup dei database. Amazon RDS crea uno snapshot dei volumi di storage dell'istanza database, eseguendo il backup dell'intera istanza database anziché dei singoli database. Utilizzando Amazon RDS, puoi creare una finestra di backup per i backup automatici, creare istantanee di istanze di database e condividere e copiare istantanee tra regioni e account.

Amazon RDS offre due diverse opzioni per il backup e il ripristino delle istanze DB:

- I backup automatici forniscono point-in-time il ripristino (PITR) dell'istanza DB. I backup automatici sono attivati per impostazione predefinita quando si crea una nuova istanza DB.

  Amazon RDS esegue un backup giornaliero completo dei dati durante una finestra di backup che definisci quando crei l'istanza DB. È possibile configurare un periodo di mantenimento di massimo 35 giorni per il backup automatico. Amazon RDS carica inoltre i log delle transazioni per le istanze database in Amazon S3 ogni 5 minuti. Amazon RDS utilizza i backup giornalieri insieme ai registri delle transazioni del database per ripristinare l'istanza DB. Puoi ripristinare l'istanza in qualsiasi momento durante il periodo di conservazione, fino agli ultimi cinque minuti`LatestRestorableTime` (in genere, gli ultimi cinque minuti).

  Per trovare l'ultima ora ripristinabile per le tue istanze DB, usa la chiamata`DescribeDBInstances` API. Oppure cerca il database nella scheda Descrizione sulla console Amazon RDS.

  Quando si avvia un PITR, i registri delle transazioni vengono combinati con il backup giornaliero più appropriato per ripristinare l'istanza DB all'ora richiesta.
- Le snapshot DB di sono backup avviati dall'utente che puoi utilizzare per ripristinare la tua istanza database in uno stato noto con la frequenza che preferisci. È quindi possibile ripristinare tale stato

in qualsiasi momento. Puoi usare la console Amazon RDS o la chiamata`CreateDBSnapshot` API per creare istantanee DB. Queste istantanee vengono conservate finché non si utilizza la console o la chiamata`DeleteDBSnapshot` API per eliminarle in modo esplicito.

Entrambe queste opzioni di backup sono supportate per Amazon RDS inAWS Backup, che offre anche altre funzionalità. Prendi in considerazione l'idea diAWS Backup configurare un piano di backup standard per i tuoi database Amazon RDS e di utilizzare le opzioni di backup delle istanze avviate dall'utente quando i piani di backup per un determinato database sono unici.

Amazon RDS impedisce l'accesso diretto allo storage sottostante utilizzato dall'istanza DB. Ciò impedisce inoltre di esportare direttamente il database su un'istanza DB RDS sul relativo disco locale. In alcuni casi, è possibile utilizzare le funzioni native di backup e ripristino utilizzando le utilità client. Ad esempio, puoi utilizzare il comando mysqldump con un database MySQL Amazon RDS per esportare un database sul tuo computer client locale. In alcuni casi, Amazon RDS offre anche opzioni avanzate per eseguire un backup e un ripristino nativi di un database. Ad esempio, Amazon RDS fornisce procedure archiviate per esportare e importare i backup dei database RDS dei database SQL Server.

Assicurati di testare a fondo il processo di ripristino del database e il suo impatto sui client del database come parte del tuo approccio generale di backup e ripristino.

Utilizzo dei record DNS CNAME per ridurre l'impatto sul client durante il ripristino del database

Quando si ripristina un database utilizzando PITR o un'istantanea dell'istanza DB RDS, viene creata una nuova istanza DB con un nuovo endpoint. In questo modo, è possibile creare più istanze DB da un'istantanea o da un momento specifico del database. Esistono considerazioni particolari quando si ripristina un'istanza DB RDS per sostituire un'istanza DB RDS attiva. Ad esempio, è necessario determinare in che modo reindirizzare i client del database esistenti alla nuova istanza con interruzioni e modifiche minime. È inoltre necessario garantire la continuità e la coerenza dei dati all'interno del database considerando il tempo di ripristino dei dati e il tempo di ripristino quando la nuova istanza inizia a ricevere scritture.

Puoi creare un record DNS CNAME separato che punti all'endpoint dell'istanza DB e fare in modo che i tuoi clienti utilizzino questo nome DNS. È quindi possibile aggiornare il CNAME in modo che punti a un nuovo endpoint ripristinato senza dover aggiornare i client del database.

Imposta il valore del tuo record CNAME (Time to Live) (TTL) per il tuo record CNAME su un valore elevato. Il TTL specificato determina per quanto tempo il record viene memorizzato nella cache con i resolver DNS prima che venga effettuata un'altra richiesta. È importante notare che alcuni resolver o applicazioni DNS potrebbero non rispettare il TTL e potrebbero memorizzare nella cache il record più a lungo del TTL. Per Amazon Route 53, specifichi un valore elevato (ad esempio, 172.800 secondi, o due giorni), il numero di chiamate che i resolver ricorsivi DNS devono effettuare a Route 53 per ottenere le informazioni aggiornate in questo record. Ciò riduce la latenza e riduce la fattura per il servizio Route 53. Per ulteriori informazioni, consulta Come Amazon Route 53 instrada il traffico per il tuo dominio.

Le applicazioni e i sistemi operativi client potrebbero anche memorizzare nella cache le informazioni DNS che è necessario svuotare o riavviare per avviare una nuova richiesta di risoluzione DNS e recuperare il record CNAME aggiornato.

Quando avvii un ripristino del database e sposti il traffico verso l'istanza ripristinata, verifica che tutti i tuoi client stiano scrivendo sull'istanza ripristinata anziché sull'istanza precedente. L'architettura dei dati potrebbe supportare il ripristino del database, l'aggiornamento del DNS per spostare il traffico verso l'istanza ripristinata e quindi la correzione di eventuali dati che potrebbero essere ancora scritti nell'istanza precedente. In caso contrario, puoi interrompere l'istanza esistente prima di aggiornare il record DNS CNAME. Quindi tutti gli accessi provengono dall'istanza appena ripristinata. Ciò può causare temporaneamente problemi di connessione per alcuni client del database che è possibile gestire singolarmente. Per ridurre l'impatto sul client, è possibile eseguire il ripristino del database durante una finestra di manutenzione.

Scrivi le tue applicazioni per gestire gli errori di connessione al database in modo corretto, ripetendo i tentativi utilizzando il backoff esponenziale. Ciò consente all'applicazione di ripristinarsi quando una connessione al database non è disponibile durante un ripristino senza causare un arresto imprevisto dell'applicazione.

Dopo aver completato il processo di ripristino, è possibile mantenere l'istanza precedente in uno stato di interruzione. In alternativa, puoi utilizzare le regole dei gruppi di sicurezza per limitare il traffico all'istanza precedente fino a quando non sarai sicuro che non sia più necessario. Per un approccio di smantellamento graduale, è necessario innanzitutto limitare l'accesso a un database in esecuzione da parte del gruppo di sicurezza. Alla fine, puoi interrompere l'istanza quando non è più necessaria. Infine, crea uno snapshot dell'istanza del database ed eliminala.

Backup e ripristino per DynamoDB

DynamoDB fornisce PITR, che esegue backup pressoché continui dei dati contenuti nelle tabelle DynamoDB. Se abilitato, DynamoDB mantiene i backup incrementali della tabella negli ultimi 35 giorni fino a quando non la disattivi esplicitamente.

Puoi anche creare backup su richiesta della tua tabella DynamoDB utilizzando la console DynamoDBAWS CLI, o l'API DynamoDB. Per ulteriori informazioni, consulta Backup di una tabella DynamoDB. È possibile pianificare backup periodici o future utilizzandoAWS Backup, o personalizzare e automatizzare il tuo approccio di backup utilizzando le caratteristiche di Lambda. Per ulteriori informazioni sull'utilizzo delle funzioni Lambda per il Backup di DynamoDB, consulta il post di blog Una soluzione serverless per programmare il tuo backup on demand di Amazon DynamoDB. Se non desideri creare script di pianificazione e processi di pulizia, puoi utilizzareAWS Backup per creare piani di backup. I piani di backup includono pianificazioni e politiche di conservazione per le tabelle DynamoDB. AWS Backupcrea i backup ed elimina i backup precedenti in base al programma di conservazione. AWS Backupinclude anche opzioni di backup avanzate di DynamoDB che non sono disponibili nel servizio DynamoDB, tra cui lo storage su più livelli a basso costo e la copia tra account e tra regioni. Per ulteriori informazioni, consulta Backup avanzato di DynamoDB.

È necessario configurare manualmente quanto segue su una tabella DynamoDB ripristinata:

- Criteri di scalabilità automatica
- Policy IAM
- CloudWatch Parametri e allarmi di Amazon
- Tag
- Impostazioni flusso
- Impostazioni TTL

È possibile ripristinare solo i dati dell'intera tabella in una nuova tabella da un backup. Puoi scrivere nella tabella ripristinata solo dopo che si attiva.

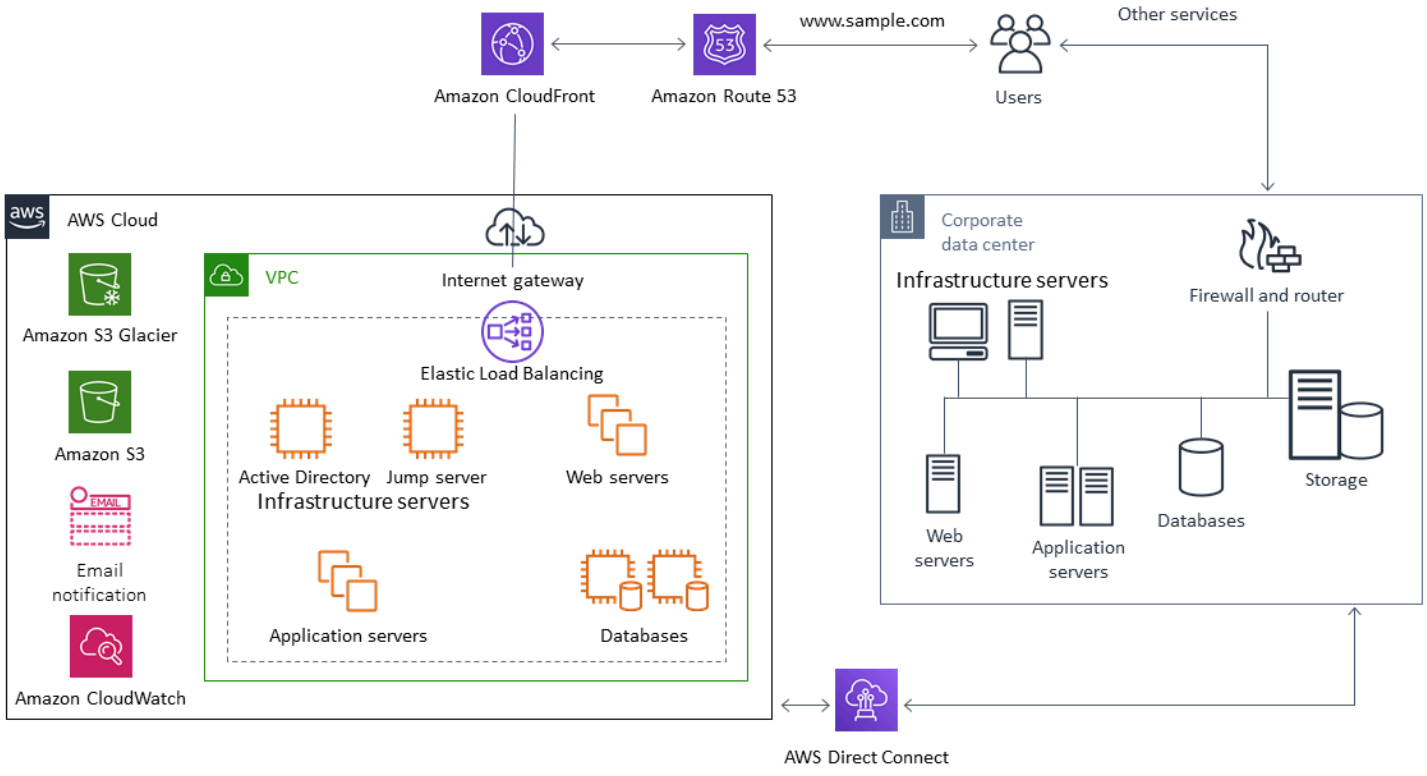
Il processo di ripristino deve considerare in che modo i client verranno indirizzati a utilizzare il nome della tabella appena ripristinata. Puoi configurare le tue applicazioni e i tuoi client per recuperare il nome della tabella DynamoDB da un file di configurazione, dal valore delAWS Systems Manager Parameter Store o da un altro riferimento che può essere aggiornato dinamicamente per riflettere il nome della tabella che il client deve usare.

Come parte del processo di ripristino, è necessario considerare attentamente il processo di commutazione. Potresti scegliere di negare l'accesso alla tua tabella DynamoDB esistente tramite le autorizzazioni IAM e consentire l'accesso alla tua nuova tabella. È quindi possibile aggiornare la configurazione dell'applicazione e del client per utilizzare la nuova tabella. Potrebbe anche essere necessario conciliare le differenze tra la tabella DynamoDB esistente e la tabella DynamoDB appena ripristinata.

Backup e ripristino per architetture ibride

Le distribuzioni cloud-native e on-premise discusse in questa guida possono essere combinate in scenari ibridi in cui l'ambiente di carico di lavoro è in locale eAWScomponenti dell'infrastruttura. Le risorse, inclusi server Web, server applicazioni, server di monitoraggio, database e Microsoft Active Directory, sono ospitate nel data center del cliente o suAWS. Applicazioni in esecuzione nelAWSIl cloud è connesso alle applicazioni in esecuzione on-premise.

Questo sta diventando uno scenario comune per i carichi di lavoro aziendali. Molte aziende dispongono di data center propri e utilizzanoAWSper aumentare la capacità. Questi data center per i clienti sono spesso collegati alAWSrete tramite collegamenti di rete ad alta capacità. Ad esempio, conAWS Direct Connect, è possibile stabilire una connettività privata e dedicata dal tuo data center locale aAWS. Ciò fornisce la larghezza di banda e la latenza coerente per caricare i dati sul cloud ai fini della protezione dei dati. Fornisce inoltre prestazioni e latenza coerenti per i carichi di lavoro ibridi. Il seguente diagramma fornisce un esempio di approccio all'ambiente ibrido.



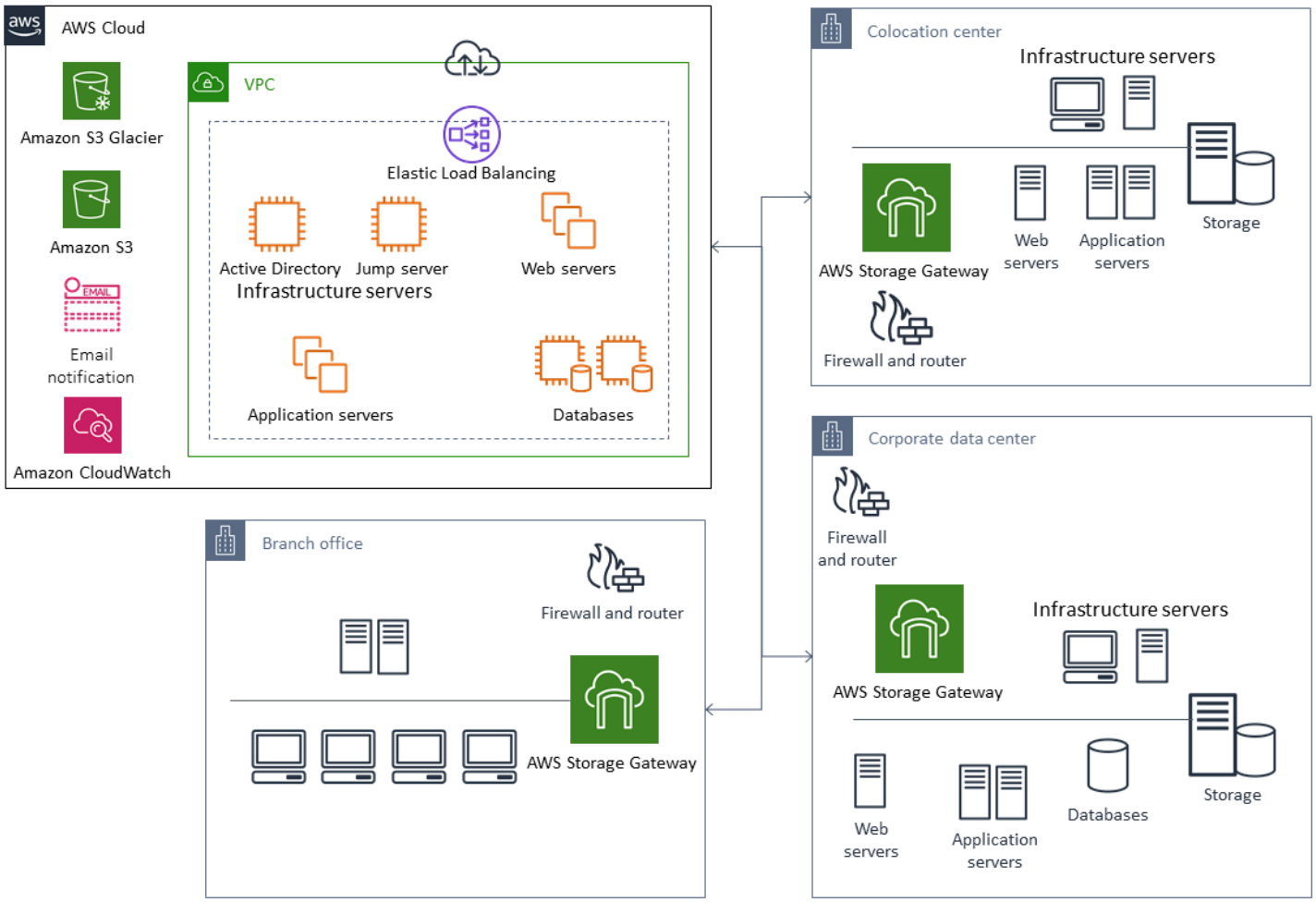
Solitamente le soluzioni di protezione dei dati ben progettate utilizzano una combinazione delle opzioni descritte nelle soluzioni cloud-native e on-premise in questa guida. Molti ISV forniscono soluzioni di backup e ripristino leader di mercato per l'infrastruttura locale e hanno ampliato le loro soluzioni per supportare gli approcci ibridi.

Spostamento delle soluzioni di gestione centralizzata del backup sul cloud per una maggiore disponibilità

Utilizzando gli investimenti esistenti nella soluzione di gestione del backup conAWS, puoi migliorare la resilienza e l'architettura del tuo approccio. È possibile che si disponga di un server di backup principale e di uno o più server multimediali o di storage situati in locale in più posizioni vicine ai server e ai servizi che proteggono. In questo caso, è consigliabile spostare il server di backup principale su un'istanza EC2 per proteggerlo dai disastri locali e per garantire un'elevata disponibilità.

Per gestire i flussi di dati di backup, è possibile creare uno o più server multimediali su istanze EC2 nella stessa regione dei server che proteggeranno. I server multimediali vicino alle istanze EC2 consentono di risparmiare denaro sul trasferimento su Internet. Quando esegui il backup su Amazon S3 o Amazon S3 Glacier, i media server aumentano le prestazioni complessive di backup e ripristino.

È inoltre possibile utilizzare Storage Gateway per fornire accesso cloud centralizzato ai dati provenienti da centri dati e uffici dislocati geograficamente. Ad esempio, un gateway di file offre accesso su richiesta e a bassa latenza ai dati archiviati inAWSper flussi di lavoro applicativi che possono attraversare il globo. È possibile utilizzare funzioni come l'aggiornamento della cache per aggiornare i dati in posizioni geograficamente distribuite in modo che i contenuti possano essere facilmente condivisi nei tuoi uffici.


AWS Cloud
Amazon S3 Glacier
Amazon S3
Email notification
Amazon CloudWatch
VPC
Elastic Load Balancing
Active Directory
Jump server
Web servers
Infrastructure servers
Application servers
Databases
Colocation center
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Storage
Firewall and router
Corporate data center
Firewall and router
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Databases
Storage
Branch office
Firewall and router
AWS Storage Gateway

Disaster recovery conAWS

Gli approcci di backup e ripristino e i servizi e le tecnologie di supporto possono essere utilizzati per implementare la soluzione di disaster recovery (DR). Molte aziende utilizzanoAWSCloud per il backup e il ripristino e come sito di DR.AWSfornisce una serie di servizi e funzionalità che supportano il ripristino di emergenza e la continuità aziendale.

Argomenti

- DR locale aAWS
- DR per carichi di lavoro nativi del cloud

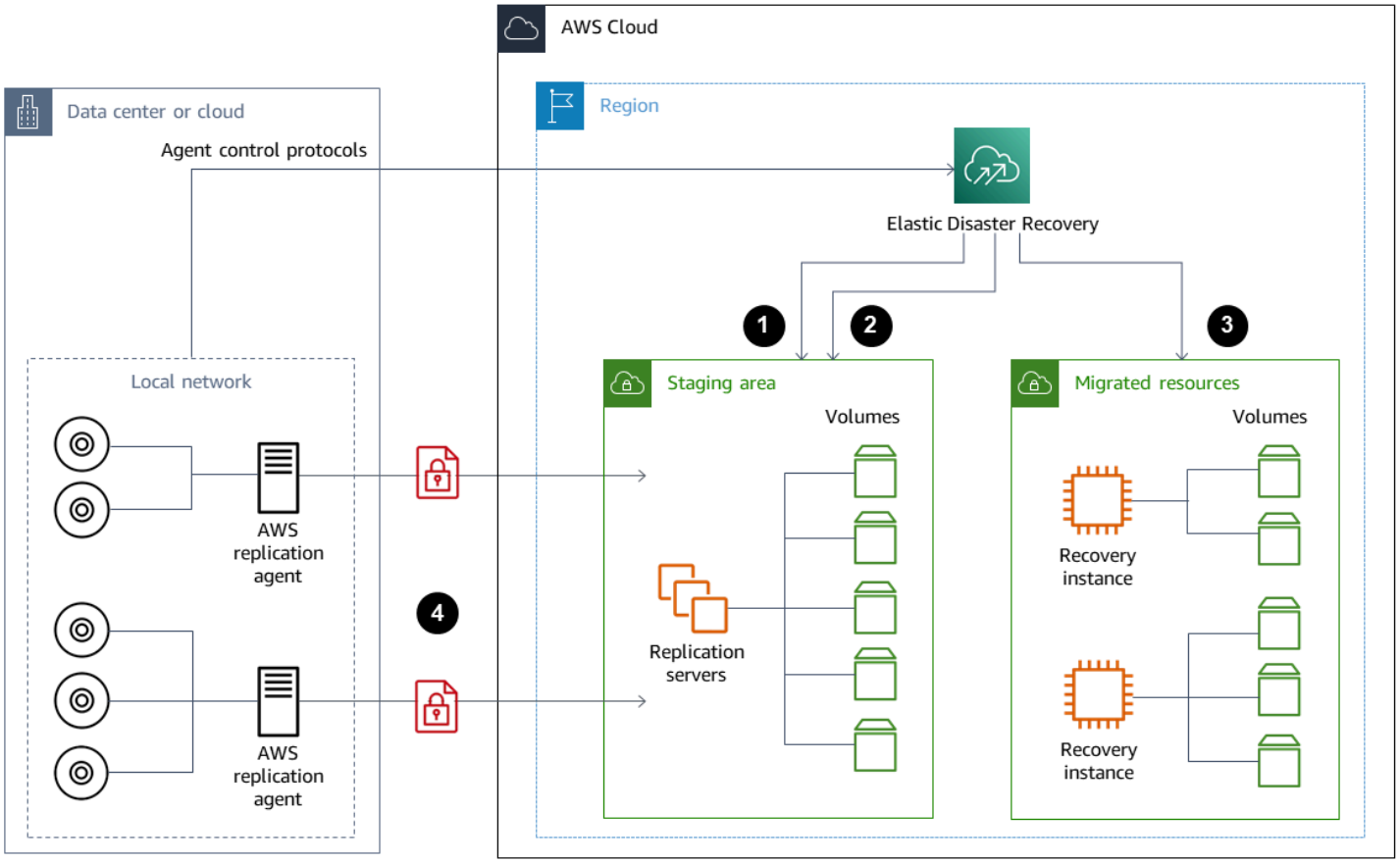
DR locale aAWS

UsandoAWScome ambiente di disaster recovery (DR) fuori sede per carichi di lavoro locali è uno scenario ibrido comune. Definisci gli obiettivi di ripristino di emergenza, inclusi i tempi di ripristino e gli obiettivi dei punti di ripristino richiesti, prima di selezionare le tecnologie da utilizzare. Per aiutarti con questa definizione, puoi usareLista di controllo del piano DR.

Sono disponibili diverse opzioni per aiutarti a configurare e fornire rapidamente un ambiente di ripristino di emergenza suAWS. Assicurati di tenere conto di tutte le dipendenze dal carico di lavoro e testa il piano e la soluzione di ripristino di emergenza in modo completo e regolare per verificarne l'integrità.

AWSforniscеAWS Elastic Disaster Recoveryper creare una replica completa dei server locali, inclusi il volume root e il sistema operativo, suAWS. Elastic Disaster Recovery replica continuamente le tue macchine in un'area di staging a basso costo nell'account AWS di destinazione e preferitoRegione AWS. La replica a livello di blocco è una replica esatta dello storage dei server, incluso il sistema operativo, la configurazione dello stato del sistema, i database, le applicazioni e i file. In caso di emergenza, puoi indicare a Elastic Disaster Recovery di avviare rapidamente migliaia di macchine nello stato completamente fornito in pochi minuti.

Elastic Disaster Recovery utilizza un agente installato su ciascuno dei tuoi server locali. Gli agenti sincronizzano lo stato dei tuoi server locali con gli equivalenti Amazon EC2 a basso consumo in esecuzione suAWS. Puoi anche automatizzare il tuo processo di failover e failback del DR con Elastic Disaster Recovery. L'automazione dei processi di failover e failback può aiutarti a raggiungere un obiettivo di tempo di ripristino (RTO) più basso e coerente.



1. Rapporti sullo stato del server di replica
2. Risorse dell'area di staging create e terminate automaticamente
3. Istanze di ripristino avviate con RTO di minuti e RPO di secondi
4. Replica continua a livello di blocco (compressa e crittografata)

È importante testare il processo di ripristino di emergenza e verificare che l'ambiente di live staging non crei conflitti con l'ambiente locale. Ad esempio, verifica che le licenze appropriate siano disponibili e funzionanti nell'ambiente di ripristino di emergenza locale, di staging e avviato. Verifica inoltre che tutti i processi di tipo worker che potrebbero eseguire sondaggi ed estrarre lavoro da un database centrale siano configurati in modo appropriato per evitare sovrapposizioni o conflitti. Nel processo di ripristino di emergenza, includi tutti i passaggi necessari che devono essere eseguiti prima che le istanze del server di ripristino vengano online. Includi anche i passaggi da eseguire dopo che le istanze del server di ripristino sono online e disponibili. È possibile utilizzare soluzioni comeAWS Elastic Disaster RecoverySoluzione Plan Automationo un altro approccio per aiutarti ad automatizzare i tuoi piani di ripristino di emergenza.

Puoi usare unGateway di volume Storage Gatewayper fornire ai tuoi server locali volumi basati sul cloud. Questi volumi possono anche essere rapidamente forniti per l'uso con Amazon EC2 utilizzando gli snapshot di Amazon EBS. In particolare, i gateway di volume archiviati forniscono alle applicazioni locali l'accesso a bassa latenza all'intero set di dati. I gateway di volume forniscono anche backup durevoli basati su istantanee che possono essere ripristinati per l'uso in locale o per l'uso con Amazon EC2. Puoi programmarepoint-in-timeistantanee basate sull'obiettivo del punto di ripristino (RPO) per il carico di lavoro.

> **Important**
>
> I volumi Volume Gateway sono pensati per essere utilizzati come volumi di dati e non come volumi di avvio.

Puoi utilizzare Amazon Machine Image (AMI) Amazon EC2 con una configurazione che corrisponde ai tuoi server locali e specifica separatamente i volumi di dati. Dopo aver configurato e testato l'AMI, esegui il provisioning delle istanze EC2 dall'AMI insieme ai volumi di dati in base alle istantanee del gateway di volume. Questo approccio richiede di testare accuratamente l'ambiente per verificare che l'istanza EC2 funzioni correttamente, in particolare per i carichi di lavoro di Windows.

DR per carichi di lavoro nativi del cloud

Valuta in che modo i tuoi carichi di lavoro nativi per il cloud si allineano ai tuoi obiettivi di ripristino di emergenza.AWSfornisce più zone di disponibilità nelle regioni di tutto il mondo. Molte aziende utilizzanoAWSIl cloud allinea le architetture dei carichi di lavoro e gli obiettivi di ripristino di emergenza per resistere alla perdita di una zona di disponibilità. LaPilastro dell'affidabilitànelAWSWell-Architected Framework supporta questa best practice. Puoi progettare i tuoi carichi di lavoro e le relative dipendenze tra servizi e applicazioni per utilizzare più zone di disponibilità. Puoi quindi automatizzare il tuo DR e raggiungere i tuoi obiettivi di DR con un intervento minimo o nullo.

In pratica, tuttavia, potresti scoprire di non essere in grado di stabilire un'architettura ridondante, attiva e automatizzata per tutti i tuoi componenti. Esamina ogni livello della tua architettura per determinare i processi di ripristino di emergenza necessari per raggiungere i tuoi obiettivi. Questo può variare da carico di lavoro a carico di lavoro, con requisiti architettonici e di servizio diversi. Questa guida illustra considerazioni e opzioni per Amazon EC2. Per altroAWSservizi, puoi fare riferimento alAWSdocumentazioneper determinare l'alta disponibilità e le opzioni di ripristino di emergenza.

DR per Amazon EC2 in un'unica zona di disponibilità

Prova a progettare i tuoi carichi di lavoro per supportare e fornire assistenza attiva ai clienti provenienti da più zone di disponibilità. Puoi utilizzare Amazon EC2 Auto Scaling ed Elastic Load Balancing per realizzare un'architettura server Multi-AZ per Amazon EC2 e altri servizi.

Se la tua architettura ha istanze EC2 che non possono essere bilanciate dal carico e possono avere solo una singola istanza in esecuzione in un dato momento, puoi utilizzare una delle seguenti opzioni.

- Crea un gruppo Auto Scaling con una dimensione minima, massima e desiderata di 1 e configurato per più zone di disponibilità. Crea un'AMI che può essere utilizzata per sostituire l'istanza in caso di errore. Assicurati di definire l'automazione e la configurazione corrette in modo che un'istanza appena fornita dall'AMI possa essere configurata automaticamente e fornire assistenza. Crea un sistema di bilanciamento del carico che punti al gruppo Auto Scaling e sia configurato per più zone di disponibilità. Facoltativamente, crea un alias Amazon Route 53 che punti all'endpoint del sistema di bilanciamento del carico.
- Crea un record Route 53 per la tua istanza attiva e fai in modo che i tuoi clienti si connettano utilizzando questo record. Crea uno script che crei una nuova AMI della tua istanza attiva e utilizzi l'AMI per eseguire il provisioning di una nuova istanza EC2 nello stato interrotto in una zona di disponibilità separata. Configura lo script per l'esecuzione periodica e per terminare la precedente istanza interrotta. Se si verifica un errore nella zona di disponibilità, avvia l'istanza di backup nella zona di disponibilità alternativa. Quindi aggiorna il record Route 53 in modo che punti a questa nuova istanza.

Testate a fondo la vostra soluzione simulando il guasto da cui la soluzione è stata progettata per proteggere. Considera anche gli aggiornamenti di cui avrà bisogno la tua soluzione di ripristino di emergenza man mano che l'architettura del carico di lavoro cambia.

DR per Amazon EC2 in caso di errore regionale

SebbeneAWSi fallimenti regionali sono rari, è possibile che unAWSLa regione potrebbe fallire in futuro. I clienti devono valutare attentamente la complessità, i costi e gli sforzi necessari per stabilire e mantenere un piano di ripristino di emergenza multiregionale rispetto ai vantaggi.AWSfornisce funzionalità che supportano architetture multiregionali per la disponibilità globale, il failover e il DR. Questa guida illustra alcune delle funzionalità disponibili specifiche per il backup e il ripristino per Amazon EC2.

AWSLe AMI e gli snapshot di Amazon EBS sono risorse regionali che possono essere utilizzate per fornire nuove istanze all'interno di una singola regione. Tuttavia, puoi copiare le tue istantanee e le AMI in un'altra regione e utilizzarle per eseguire il provisioning di nuove istanze in quella regione. Per supportare un piano regionale di ripristino dei guasti, puoi automatizzare il processo di copia delle AMI e delle istantanee in altre regioni.AWS Backupe Amazon Data Lifecycle Manager supportano la copia tra regioni come parte della configurazione di backup.

AWS Elastic Disaster Recoverypuò essere utilizzato per automatizzare e replicare continuamente i server Amazon EC2 in una regione di ripristino di emergenza alternativa. Elastic Disaster Recovery può semplificare il tuo approccio di ripristino di emergenza multiregionale e aiutarti a testare regolarmente il tuo piano di ripristino di emergenza Amazon EC2 interregionale utilizzando esercitazioni. Elastic Disaster Recovery può aiutarti quando il backup e il ripristino non sono in grado di soddisfare gli obiettivi RTO e RPO. Elastic Disaster Recovery può aiutarti a ridurre l'RTO a minuti e l'RPO a meno di un secondo.

Qualunque sia la soluzione utilizzata, è necessario determinare il processo di provisioning, failover e failback da utilizzare in caso di interruzione. Puoi utilizzare Route 53 con controlli di integrità e failover del Domain Name System per supportare la tua soluzione.

Pulizia dei backup

Per ridurre i costi, ripulisci i backup che non sono più necessari per scopi di ripristino o conservazione. Puoi usareAWS Backupe Amazon Data Lifecycle Manager per automatizzare la tua politica di conservazione per una parte dei tuoi backup. Tuttavia, anche con questi strumenti, è comunque necessario un approccio di pulizia per i backup che vengono eseguiti separatamente.

Una strategia di etichettatura è un prerequisito per una strategia di pulizia. Usa i tag per identificare le risorse da ripulire, informare i proprietari in modo appropriato e automatizzare il processo di pulizia. Backup creati daAWSle date di creazione sono allineate ad esse, ma l'etichettatura è importante per correlare i backup ai carichi di lavoro, ai requisiti di conservazione e all'identificazione dei punti di ripristino.

È possibile implementare un processo di pulizia per le istantanee utilizzando l'automazione. Ad esempio, puoi scansionare il tuo account alla ricerca di istantanee e determinare se i volumi corrispondenti sono in uno stato allegato o disponibile. Puoi filtrare ulteriormente i risultati in base a una soglia temporale specificata. Utilizzando i tag allegati al volume, puoi inviare automaticamente e-mail ai proprietari delle istantanee e avvisarli che è stata pianificata l'eliminazione delle loro istantanee. Questa correzione automatica può essere implementata utilizzandoAWS Configrules, uno script che utilizzaAWS CLI, o una funzione Lambda che utilizzaAWSSDK.

Systems Manager fornisceAWS - Elimina EBSVolumeSnapshotseSEGHE-DeleteSnapshotdocumenti per aiutarti ad avviare e automatizzare la pulizia delle istantanee di Amazon EBS. Puoi anche usareAWS CLIeAWSSDK per automatizzare la pulizia degli altriAWSrisorse come le istantanee di Amazon RDS.

Domande frequenti su backup e ripristino

Quale pianificazione di backup devo selezionare?

Definisci una frequenza di pianificazione dei backup in linea con il tuo obiettivo del punto di ripristino (RPO). Definisci un tempo di backup quando il carico di lavoro è inferiore alla quantità minima di carico e quando l'impatto sugli utenti può essere ridotto. Crea unpoint-in-timeistantanea ogni volta che intendi apportare una modifica significativa al tuo carico di lavoro.

Devo creare dei backup nei miei account di sviluppo?

Testa le modifiche potenzialmente irreversibili nei tuoi account di sviluppo per i tuoi carichi di lavoro e crea backup prima di eseguire modifiche sostanziali. Potresti averne molti altripoint-in-timebackup di ripristino (PITR) negli account di sviluppo e non di produzione derivanti da attività di sviluppo e test.

Posso aggiornare le applicazioni e continuare a utilizzare un volume EBS mentre viene creata un'istantanea senza alcun impatto?

Le istantanee vengono eseguite in modo asincrono;point-in-timeLo snapshot viene creato immediatamente, ma lo stato dell'istantanea è in sospeso fino al trasferimento di tutti i blocchi modificati su Amazon S3. Per istantanee iniziali di grandi dimensioni o istantanee successive in cui sono stati modificati molti blocchi, il trasferimento può richiedere diverse ore. Durante il trasferimento, un'istantanea in corso non è influenzata dalle letture e scritture in corso sul volume. Per ulteriori informazioni, consulta la documentazione relativa ad AWS.

Fasi successive

Inizia valutando, implementando e testando il tuo approccio di backup e ripristino in un ambiente non di produzione. È importante testare accuratamente il processo di ripristino e verificare che i carichi di lavoro ripristinati funzionino come previsto.

Testa il processo di ripristino per un singolo componente della tua architettura oltre a tutti i componenti della tua architettura. Convalida il tempo di ripristino per ciascuno di essi. Verifica anche l'impatto del tuo processo di backup e ripristino sulle dipendenze a monte e a valle. Conferma l'impatto di eventuali interruzioni del servizio sulle dipendenze upstream e conferma l'impatto a valle sui backup.

Risorse aggiuntive

Risorse AWS

- AWSGuida prescrittiva
- Documentazione AWS
- Riferimento generale AWS
- Glossario AWS

Servizi AWS

- AWS Backup
- AmazonCloudWatch
- AmazonCloudWatchEventi
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- IAM
- Amazon RDS
- Amazon S3
- Amazon S3 Glacier
- Gateway di storage
- AWS Systems Manager

Altre risorse

- Backup e ripristino conAWS Backup(soluzione)
- Disaster recovery dei carichi di lavoro suAWS: Ripristino nel cloud(libro bianco)
- Serie Disaster Recovery(post sul blog di AWS Architecture)
- Lista di controllo del piano DR
- Approcci di backup e ripristino che utilizzanoAWS(documento tecnico — archiviato)

- Nozioni di base suAWS Backup
- AWSMarketplace: backup e ripristino

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti apportate a questa guida. Se desideri ricevere una notifica sugli aggiornamenti future, puoi iscriverti a un feed RSS.

Modifica	Descrizione	Data
Informazioni aggiornate	Informazioni aggiornate nellaAWS sezione DR to locale.	13 Aprile 2023
Aggiunta una sezione	Sono state aggiunte istruzioni e passaggi per creare o ripristinare un'istanza da un'istantanea.	7 marzo 2023
Sono state aggiunte informazioni su Elastic Disaster Recovery e ulteriori chiarimenti	Nelle sezioni Disaster recovery withAWS and AWSChoosing services for data protection, sono state aggiunte informazioni suAWS Elastic Disaster Recovery. Per quanto riguarda il backup e il ripristino di Amazon EC2 con istantanee e AMI, la preparazione di un volume EBS prima di creare uno snapshot o un'AMI e il ripristino da un'istantanea Amazon EBS o dalle sezioni AMI, sono stati aggiunti dei chiarimenti. Aggiunto alle domande frequenti Backup e ripristino.	19 gennaio 2023
Aggiunto un link	È stato aggiunto un collegamento alla documentazione di Amazon Data Lifecycle	31 ottobre 2022

	Manager nella sezione Amazon Data Lifecycle Manager.	
Informazioni aggiornate	Sono state aggiornate le informazioni sul ripristino dei volumi.	30 agosto 2022
Informazioni aggiornate e aggiunta una nuova sezione	Nella sezione Scelta deiAWS servizi per la protezione dei dati, sono stati aggiunti servizi. È stata aggiunta la sezione Backup e ripristino tramite AWS Backup. Nella sezione Backup e ripristino con Amazon S3 e Amazon S3 Glacier, sono state aggiunte informazioni sulle nuove classi di storage Amazon S3 Glacier. Nella sezione Backup e ripristino per Amazon EC2 con volumi EBS, sono stati aggiunti collegamenti alla documentazione e informazi oni aggiuntive. Nella sezione Backup e ripristino deiAWS servizi nativi del cloud, è stata aggiunta una raccomand azione da utilizzareAWS Backup. Nella sezione Risorse aggiuntive, risorse aggiunte.	28 gennaio 2022

Informazioni aggiornate	Sono state aggiunte informazioni sull'impostazione delle classi di archiviazione nella sezione S3 Glacier Flexible Retrieval. Sono state aggiunte informazioni sul recupero delle istantanee nella sezione di backup e ripristino di Amazon EC2 con istantanee e AMI.	9 settembre 2021
Informazioni aggiornate	Nella AWS Backupsezione, sono state aggiunte informazioni suiAWS serviziAWS Backup supportati.	1° giugno 2021
Pubblicazione iniziale	—	29 luglio 2020

Glossario del Prontuario AWS

I seguenti termini sono comunemente utilizzati in strategie, guide e pattern forniti dal Prontuario AWS. Per suggerire voci, utilizza il link Fornisci feedback alla fine del glossario.

Numeri

7 R

Sette strategie di migrazione comuni per trasferire le applicazioni sul cloud. Queste strategie si basano sulle 5 R identificate da Gartner nel 2011 e sono le seguenti:

- Rifattorizzare/riprogettare: trasferisci un'applicazione e modifica la sua architettura sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: esegui la migrazione del database Oracle on-premise ad Amazon Aurora edizione compatibile con PostgreSQL.
- Ridefinire la piattaforma (lift and reshape): trasferisci un'applicazione nel cloud e introduci un certo livello di ottimizzazione per sfruttare le funzionalità del cloud. Esempio: esegui la migrazione del database Oracle on-premise ad Amazon Relational Database Service (Amazon RDS) per Oracle nel cloud AWS.
- Riacquistare (drop and shop): passa a un prodotto diverso, in genere effettuando la transizione da una licenza tradizionale a un modello SaaS. Esempio: esegui la migrazione del tuo sistema di gestione delle relazioni con i clienti (CRM) su Salesforce.com.
- Eseguire il rehosting (lift and shift): trasferisci un'applicazione sul cloud senza apportare modifiche per sfruttare le funzionalità del cloud. Esempio: esegui la migrazione del tuo database Oracle on-premise su Oracle su un'istanza EC2 nel cloud AWS.
- Trasferire (eseguire il rehosting a livello hypervisor): trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Questo scenario di migrazione è specifico di VMware Cloud su AWS, che supporta la compatibilità delle macchine virtuali (VM) e la portabilità del carico di lavoro tra l'ambiente on-premise e AWS. È possibile utilizzare le tecnologie VMware Cloud Foundation dai data center on-premise durante la migrazione dell'infrastruttura a VMware Cloud su AWS. Esempio: trasferisci l'hypervisor che ospita il database Oracle su VMware Cloud su AWS.
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a

un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.

- Ritirare: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

Un metodo di migrazione del database in cui i database di origine e di destinazione vengono mantenuti sincronizzati (utilizzando uno strumento di replica bidirezionale o operazioni di doppia scrittura) ed entrambi i database gestiscono le transazioni provenienti dalle applicazioni di connessione durante la migrazione. Questo metodo supporta la migrazione in piccoli batch controllati anziché richiedere una conversione una tantum. È più flessibile ma richiede più lavoro rispetto alla migrazione attiva-passiva.

migrazione attiva-passiva

Un metodo di migrazione di database in cui i database di origine e di destinazione vengono mantenuti sincronizzati, ma solo il database di origine gestisce le transazioni provenienti dalle applicazioni di connessione mentre i dati vengono replicati nel database di destinazione. Il database di destinazione non accetta alcuna transazione durante la migrazione.

funzione aggregata

Una funzione SQL che opera su un gruppo di righe e calcola un singolo valore restituito per il gruppo. Esempi di funzioni aggregate includono `SUM` e. `MAX`

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

Il processo di eliminazione permanente delle informazioni personali in un set di dati. L'anonimizzazione può aiutare a proteggere la privacy personale. I dati anonimi non sono più considerati dati personali.

anti-modello

Una soluzione utilizzata di frequente per un problema ricorrente in cui la soluzione è controproducente, inefficace o meno efficace di un'alternativa.

controllo delle applicazioni

Un approccio alla sicurezza che consente l'uso solo di applicazioni approvate per proteggere un sistema dal malware.

portfolio di applicazioni

Una raccolta di informazioni dettagliate su ogni applicazione utilizzata da un'organizzazione, compresi i costi di creazione e manutenzione dell'applicazione e il relativo valore aziendale. Queste informazioni sono fondamentali per il processo di scoperta e analisi del portfolio e aiutano a identificare e ad assegnare la priorità alle applicazioni da migrare, modernizzare e ottimizzare.

intelligenza artificiale (IA)

Il campo dell'informatica dedicato all'uso delle tecnologie informatiche per svolgere funzioni cognitive tipicamente associate agli esseri umani, come l'apprendimento, la risoluzione di problemi e il riconoscimento di schemi. Per ulteriori informazioni, consulta la sezione Che cos'è l'intelligenza artificiale?

operazioni di intelligenza artificiale (AIOps)

Il processo di utilizzo delle tecniche di machine learning per risolvere problemi operativi, ridurre gli incidenti operativi e l'intervento umano e aumentare la qualità del servizio. Per ulteriori informazioni su come viene utilizzato AIOps nella strategia di migrazione AWS, consulta la guida all'integrazione delle operazioni.

crittografia asimmetrica

Un algoritmo di crittografia che utilizza una coppia di chiavi, una chiave pubblica per la crittografia e una chiave privata per la decrittografia. Puoi condividere la chiave pubblica perché non viene utilizzata per la decrittografia, ma l'accesso alla chiave privata deve essere altamente limitato.

atomicità, consistenza, isolamento, durabilità (ACID)

Un insieme di proprietà del software che garantiscono la validità dei dati e l'affidabilità operativa di un database, anche in caso di errori, interruzioni di corrente o altri problemi.

Controllo degli accessi basato su attributi (ABAC)

La pratica di creare autorizzazioni dettagliate basate su attributi utente, come reparto, ruolo professionale e nome del team. Per ulteriori informazioni, consulta ABAC per AWS nella documentazione di AWS Identity and Access Management (IAM).

fonte di dati autorevole

Una posizione in cui è archiviata la versione principale dei dati, considerata la fonte di informazioni più affidabile. È possibile copiare i dati dalla fonte di dati autorevole in altre posizioni allo scopo di elaborarli o modificarli, ad esempio anonimizzandoli, oscurandoli o pseudonimizzandoli.

Zona di disponibilità

Posizione separata all'interno di una Regione AWS isolata dagli errori che si verificano in altre zone di disponibilità che offre connettività di rete non costosa e a bassa latenza ad altre zone di disponibilità nella stessa regione.

Framework per l'adozione del cloud AWS (AWS CAF)

Un framework di linee guida e buone pratiche di AWS per aiutare le organizzazioni a sviluppare un piano efficiente ed efficace per passare con successo al cloud. AWS CAF organizza le linee guida in sei aree di interesse chiamate prospettive: azienda, persone, governance, piattaforma, sicurezza e operazioni. Le prospettive relative ad azienda, persone e governance si concentrano sulle competenze e sui processi aziendali; le prospettive relative alla piattaforma, alla sicurezza e alle operazioni si concentrano sulle competenze e sui processi tecnici. Ad esempio, la prospettiva relativa alle persone si rivolge alle parti interessate che gestiscono le risorse umane (HR), le funzioni del personale e la gestione del personale. Per questa prospettiva, AWS CAF fornisce linee guida per lo sviluppo del personale, la formazione e le comunicazioni per aiutare l'organizzazione nell'adozione efficace del cloud. Per ulteriori informazioni, consulta il sito web di AWS CAF e il white paper AWS CAF.

AWS Workload Qualification Framework (AWS WQF)

Uno strumento che valuta i carichi di lavoro di migrazione dei database, consiglia strategie di migrazione e fornisce stime del lavoro. AWS WQF è incluso in AWS Schema Conversion Tool (AWS SCT). Analizza gli schemi di database e gli oggetti di codice, il codice dell'applicazione, le dipendenze e le caratteristiche delle prestazioni e fornisce report di valutazione.

B

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

Una vista unificata, interattiva dei comportamenti delle risorse e delle interazioni nel tempo. Puoi utilizzare un grafico comportamentale con Amazon Detective per esaminare tentativi di accesso non riusciti, chiamate API sospette e azioni simili. Per ulteriori informazioni, consulta Dati in un grafico comportamentale nella documentazione di Detective.

sistema big-endian

Un sistema che memorizza per primo il byte più importante. Vedi anche endianness.

Classificazione binaria

Un processo che prevede un risultato binario (una delle due classi possibili). Ad esempio, il modello di machine learning potrebbe dover prevedere problemi come "Questa e-mail è spam o non è spam?" o "Questo prodotto è un libro o un'auto?"

filtro Bloom

Una struttura di dati probabilistica ed efficiente in termini di memoria che viene utilizzata per verificare se un elemento fa parte di un set.

ramo

Un'area contenuta di un repository di codice. Il primo ramo creato in un repository è il ramo principale. È possibile creare un nuovo ramo a partire da un ramo esistente e quindi sviluppare funzionalità o correggere bug al suo interno. Un ramo creato per sviluppare una funzionalità viene comunemente detto ramo di funzionalità. Quando la funzionalità è pronta per il rilascio, il ramo di funzionalità viene ricongiunto al ramo principale. Per ulteriori informazioni, vedere About branch (GitHub documentazione).

accesso break-glass

In circostanze eccezionali e tramite una procedura approvata, un mezzo rapido per consentire a un utente di accedere a un sito a Account AWS cui in genere non dispone delle autorizzazioni necessarie. Per ulteriori informazioni, vedere l'indicatore Implementate break-glass procedures nella guida Well-ArchitectedAWS.

strategia brownfield

L'infrastruttura esistente nell'ambiente. Quando si adotta una strategia brownfield per un'architettura di sistema, si progetta l'architettura in base ai vincoli dei sistemi e dell'infrastruttura attuali. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

cache del buffer

L'area di memoria in cui sono archiviati i dati a cui si accede con maggiore frequenza.

capacità di business

Azioni intraprese da un'azienda per generare valore (ad esempio vendite, assistenza clienti o marketing). Le architetture dei microservizi e le decisioni di sviluppo possono essere guidate dalle capacità aziendali. Per ulteriori informazioni, consulta la sezione Organizzazione in base alle funzionalità aziendali del whitepaper Esecuzione di microservizi containerizzati su AWS.

pianificazione della continuità operativa (BCP)

Un piano che affronta il potenziale impatto di un evento che comporta l'interruzione dell'attività, come una migrazione su larga scala, sulle operazioni e consente a un'azienda di riprendere rapidamente le operazioni.

C

CAF

Vedi AWSCloud Adoption Framework.

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

Il processo di tracciamento delle modifiche a un'origine dati, ad esempio una tabella di database, e di registrazione dei metadati relativi alla modifica. È possibile utilizzare CDC per vari scopi, ad esempio il controllo o la replica delle modifiche in un sistema di destinazione per mantenere la sincronizzazione.

ingegneria del caos

Introduzione intenzionale di guasti o eventi dirompenti per testare la resilienza di un sistema. Puoi usare AWS Fault Injection Service(AWS FIS) per eseguire esperimenti che stressano i tuoi AWS carichi di lavoro e valutarne la risposta.

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

Un processo di categorizzazione che aiuta a generare previsioni. I modelli di ML per problemi di classificazione prevedono un valore discreto. I valori discreti sono sempre distinti l'uno dall'altro. Ad esempio, un modello potrebbe dover valutare se in un'immagine è presente o meno un'auto.

crittografia lato client

Crittografia dei dati in locale, prima che vengano ricevuti dal Servizio AWS di destinazione.

centro di eccellenza del cloud (CCoE)

Un team multidisciplinare che guida le iniziative di adozione del cloud in tutta l'organizzazione, tra cui lo sviluppo di best practice per il cloud, la mobilitazione delle risorse, la definizione delle tempistiche di migrazione e la guida dell'organizzazione attraverso trasformazioni su larga scala. Per ulteriori informazioni, consulta i post sul CCoE sul blog AWS Cloud Enterprise Strategy.

cloud computing

La tecnologia cloud generalmente utilizzata per l'archiviazione remota di dati e la gestione dei dispositivi IoT. Il cloud computing è comunemente collegato alla tecnologia di edge computing.

modello operativo cloud

In un'organizzazione IT, il modello operativo utilizzato per creare, maturare e ottimizzare uno o più ambienti cloud. Per ulteriori informazioni, consulta Building your Cloud Operating Model.

fasi di adozione del cloud

Le quattro fasi che le organizzazioni in genere attraversano quando migrano verso il cloud AWS:

- Progetto: esecuzione di alcuni progetti relativi al cloud per scopi di dimostrazione e apprendimento
- Fondamento: effettuare investimenti fondamentali per dimensionare l'adozione del cloud (ad esempio, creazione di una zona di destinazione, definizione di un CCoE, definizione di un modello operativo)

- Migrazione: migrazione di singole applicazioni
- Reinvenzione: ottimizzazione di prodotti e servizi e innovazione nel cloud

Queste fasi sono state definite da Stephen Orban nel post del blog The Journey Toward Cloud-First & the Stages of Adoption sul blog AWS Cloud Enterprise Strategy. Per informazioni su come si relazionano alla strategia di migrazione AWS, consulta la guida di preparazione alla migrazione.

CMDB

Vedi database di gestione della configurazione.

repository di codice

Una posizione in cui il codice di origine e altri asset, come documentazione, esempi e script, vengono archiviati e aggiornati attraverso processi di controllo delle versioni. Gli archivi cloud più comuni includono GitHub oAWS CodeCommit. Ogni versione del codice è denominata ramo. In una struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola pipeline CI/CD può utilizzare più repository.

cache fredda

Una cache del buffer vuota, non ben popolata o contenente dati obsoleti o irrilevanti. Ciò influisce sulle prestazioni perché l'istanza di database deve leggere dalla memoria o dal disco principale, il che richiede più tempo rispetto alla lettura dalla cache del buffer.

dati freddi

Dati a cui si accede raramente e che in genere sono storici. Quando si eseguono interrogazioni di questo tipo di dati, le interrogazioni lente sono in genere accettabili. Lo spostamento di questi dati su livelli o classi di storage meno costosi e con prestazioni inferiori può ridurre i costi.

visione artificiale

Un campo dell'intelligenza artificiale utilizzato dalle macchine per identificare persone, luoghi e cose nelle immagini con una precisione pari o superiore ai livelli umani. Spesso costruito con modelli di deep learning, automatizza l'estrazione, l'analisi, la classificazione e la comprensione di informazioni utili da una singola immagine o da una sequenza di immagini.

database di gestione della configurazione (CMDB)

Un repository che archivia e gestisce le informazioni su un database e il relativo ambiente IT, inclusi i componenti hardware e software e le relative configurazioni. In genere si utilizzano i dati di un CMDB nella fase di individuazione e analisi del portafoglio della migrazione.

Pacchetto di conformità

Una serie di regole di AWS Config e azioni correttive che puoi riunire per personalizzare i controlli di conformità e sicurezza. Puoi distribuire un pacchetto di conformità come singola entità in un Account AWS e in una regione, o all'interno di un'organizzazione, utilizzando un modello YAML. Per ulteriori informazioni, consulta Pacchetti di conformità nella documentazione di AWS Config.

integrazione e distribuzione continua (continuous integration and continuous delivery, CI/CD)

Il processo di automazione delle fasi di origine, creazione, test, gestione temporanea e produzione del processo di rilascio del software. Il processo CI/CD è comunemente descritto come una pipeline. CI/CD può aiutare ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le distribuzioni. Per ulteriori informazioni, consulta Vantaggi della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

Un processo per identificare e classificare i dati nella rete in base alla loro criticità e sensibilità. È un componente fondamentale di qualsiasi strategia di gestione dei rischi di sicurezza informatica perché consente di determinare i controlli di protezione e conservazione appropriati per i dati. La classificazione dei dati è un componente del pilastro della sicurezza nel Framework AWS Well-Architected. Per ulteriori informazioni, consulta Classificazione dei dati.

deriva dei dati

Una variazione significativa tra i dati di produzione e i dati utilizzati per addestrare un modello di machine learning o una modifica significativa dei dati di input nel tempo. La deriva dei dati può ridurre la qualità, l'accuratezza e l'equità complessive nelle previsioni dei modelli ML.

dati in transito

Dati che si spostano attivamente attraverso la rete, ad esempio tra le risorse di rete.

riduzione al minimo dei dati

Il principio della raccolta e del trattamento dei soli dati strettamente necessari. Praticare la riduzione al minimo dei dati in the Cloud AWS può ridurre i rischi per la privacy, i costi e l'impronta di carbonio delle analisi.

perimetro dei dati

Una serie di barriere preventive nell'AWSambiente che aiutano a garantire che solo le identità attendibili accedano alle risorse attendibili delle reti previste. Per ulteriori informazioni, consulta Building a data perimeter on. AWS

pre-elaborazione dei dati

Trasformare i dati grezzi in un formato che possa essere facilmente analizzato dal modello di ML. La pre-elaborazione dei dati può comportare la rimozione di determinate colonne o righe e l'eliminazione di valori mancanti, incoerenti o duplicati.

provenienza dei dati

Il processo di tracciamento dell'origine e della cronologia dei dati durante il loro ciclo di vita, ad esempio il modo in cui i dati sono stati generati, trasmessi e archiviati.

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

Un sistema di gestione dei dati che supporta la business intelligence, come l'analisi. I data warehouse contengono in genere grandi quantità di dati storici e vengono generalmente utilizzati per interrogazioni e analisi.

linguaggio di definizione del database (DDL)

Istruzioni o comandi per creare o modificare la struttura di tabelle e oggetti in un database.

linguaggio di manipolazione del database (DML)

Istruzioni o comandi per modificare (inserire, aggiornare ed eliminare) informazioni in un database.

DDL

Vedi linguaggio di definizione del database.

deep ensemble

Combinare più modelli di deep learning per la previsione. È possibile utilizzare i deep ensemble per ottenere una previsione più accurata o per stimare l'incertezza nelle previsioni.

deep learning

Un sottocampo del ML che utilizza più livelli di reti neurali artificiali per identificare la mappatura tra i dati di input e le variabili target di interesse.

defense-in-depth

Un approccio alla sicurezza delle informazioni in cui una serie di meccanismi e controlli di sicurezza sono accuratamente stratificati su una rete di computer per proteggere la riservatezza, l'integrità e la disponibilità della rete e dei dati al suo interno. Quando adotti questa strategia in AWS, puoi aggiungere più controlli a diversi livelli della struttura AWS Organizations per proteggere le risorse. Ad esempio, un defense-in-depth approccio potrebbe combinare l'autenticazione a più fattori, la segmentazione della rete e la crittografia.

amministratore delegato

In AWS Organizations, un servizio compatibile può registrare un account membro di AWS per amministrare gli account dell'organizzazione e gestire le autorizzazioni per quel servizio. Questo account è denominato amministratore delegato per quel servizio specifico. Per ulteriori informazioni e un elenco di servizi compatibili, consulta Servizi che funzionano con AWS Organizations nella documentazione di AWS Organizations.

implementazione

Il processo di creazione di un'applicazione, di nuove funzionalità o di correzioni di codice disponibili nell'ambiente di destinazione. L'implementazione prevede l'applicazione di modifiche in una base di codice, seguita dalla creazione e dall'esecuzione di tale base di codice negli ambienti applicativi.

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

Un controllo di sicurezza progettato per rilevare, registrare e avvisare dopo che si è verificato un evento. Questi controlli rappresentano una seconda linea di difesa e avvisano l'utente in caso di eventi di sicurezza che aggirano i controlli preventivi in vigore. Per ulteriori informazioni, consulta Controlli di rilevamento in Implementazione dei controlli di sicurezza in AWS.

mappatura del flusso di valore dello sviluppo (DVSM)

Un processo utilizzato per identificare e dare priorità ai vincoli che influiscono negativamente sulla velocità e sulla qualità nel ciclo di vita dello sviluppo del software. DVSM estende il processo di mappatura del flusso di valore originariamente progettato per pratiche di produzione snella. Si concentra sulle fasi e sui team necessari per creare e trasferire valore attraverso il processo di sviluppo del software.

gemello digitale

Una rappresentazione virtuale di un sistema reale, ad esempio un edificio, una fabbrica, un'attrezzatura industriale o una linea di produzione. I gemelli digitali supportano la manutenzione predittiva, il monitoraggio remoto e l'ottimizzazione della produzione.

tabella delle dimensioni

In uno schema a stella, una tabella più piccola che contiene gli attributi dei dati quantitativi in una tabella dei fatti. Gli attributi della tabella delle dimensioni sono in genere campi di testo o numeri discreti che si comportano come testo. Questi attributi vengono comunemente utilizzati per il vincolo delle query, il filtraggio e l'etichettatura dei set di risultati.

disastro

Un evento che impedisce a un carico di lavoro o a un sistema di raggiungere gli obiettivi aziendali nella sua sede principale di implementazione. Questi eventi possono essere disastri naturali, guasti tecnici o il risultato di azioni umane, come errori di configurazione involontari o attacchi di malware.

disaster recovery (DR)

La strategia e il processo utilizzati per ridurre al minimo i tempi di inattività e la perdita di dati causati da un disastro. Per ulteriori informazioni, consulta Disaster Recovery of Workloads suAWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

Un approccio allo sviluppo di un sistema software complesso collegandone i componenti a domini in evoluzione, o obiettivi aziendali principali, perseguiti da ciascun componente. Questo concetto è stato introdotto da Eric Evans nel suo libro,Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Per informazioni su come

utilizzare la progettazione basata sul dominio con il modello del fico strangolatore (Strangler Fig), consulta la sezione Modernizzazione incrementale dei servizi Web Microsoft ASP.NET (ASMX) legacy utilizzando container e il Gateway Amazon API.

DOTT.

Vedi disaster recovery.

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, è possibile AWS CloudFormation utilizzarlo per rilevare deviazioni nelle risorse di sistema oppure AWS Control Tower per rilevare cambiamenti nella landing zone che potrebbero influire sulla conformità ai requisiti di governance.

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

edge computing

La tecnologia che aumenta la potenza di calcolo per i dispositivi intelligenti all'edge di una rete IoT. Rispetto al cloud computing, l'edge computing può ridurre la latenza di comunicazione e migliorare i tempi di risposta.

crittografia

Un processo di elaborazione che trasforma i dati in chiaro, leggibili dall'uomo, in testo cifrato.

chiave crittografica

Una stringa crittografica di bit randomizzati generata da un algoritmo di crittografia. Le chiavi possono variare di lunghezza e ogni chiave è progettata per essere imprevedibile e univoca.

endianità

L'ordine in cui i byte vengono archiviati nella memoria del computer. I sistemi big-endian memorizzano per primo il byte più importante. I sistemi little-endian memorizzano per primo il byte meno importante.

endpoint

Vedi service endpoint.

servizio endpoint

Un servizio che puoi ospitare in un cloud privato virtuale (VPC) da condividere con altri utenti. Puoi creare un servizio endpoint con AWS PrivateLink e concedere le autorizzazioni ad altri Account AWS o ai principali AWS Identity and Access Management (IAM). Questi account o principali possono connettersi al servizio endpoint in privato creando endpoint VPC di interfaccia. Per ulteriori informazioni, consulta Creazione di un servizio endpoint nella documentazione di Amazon Virtual Private Cloud (Amazon VPC).

crittografia envelope

Il processo di crittografia di una chiave di crittografia con un'altra chiave di crittografia. Per ulteriori informazioni, consulta Crittografia a busta nella documentazione di AWS Key Management Service (AWS KMS).

ambiente

Un'istanza di un'applicazione in esecuzione. Di seguito sono riportati i tipi di ambiente più comuni nel cloud computing:

- ambiente di sviluppo: un'istanza di un'applicazione in esecuzione disponibile solo per il team principale responsabile della manutenzione dell'applicazione. Gli ambienti di sviluppo vengono utilizzati per testare le modifiche prima di promuoverle negli ambienti superiori. Questo tipo di ambiente viene talvolta definito ambiente di test.
- ambienti inferiori: tutti gli ambienti di sviluppo di un'applicazione, ad esempio quelli utilizzati per le build e i test iniziali.
- ambiente di produzione: un'istanza di un'applicazione in esecuzione a cui gli utenti finali possono accedere. In una pipeline CI/CD, l'ambiente di produzione è l'ultimo ambiente di implementazione.
- ambienti superiori: tutti gli ambienti a cui possono accedere utenti diversi dal team di sviluppo principale. Si può trattare di un ambiente di produzione, ambienti di preproduzione e ambienti per i test di accettazione da parte degli utenti.

epica

Nelle metodologie agili, categorie funzionali che aiutano a organizzare e dare priorità al lavoro. Le epiche forniscono una descrizione di alto livello dei requisiti e delle attività di implementazione. Ad esempio le epiche di sicurezza AWS CAF includono la gestione delle identità e degli accessi,

i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS, consulta la guida all'implementazione del programma.

analisi esplorativa dei dati (EDA)

Il processo di analisi di un set di dati per comprenderne le caratteristiche principali. Si raccolgono o si aggregano dati e quindi si eseguono indagini iniziali per trovare modelli, rilevare anomalie e verificare ipotesi. L'EDA viene eseguita calcolando statistiche di riepilogo e creando visualizzazioni di dati.

F

tabella dei fatti

Il tavolo centrale in uno schema a stella. Memorizza dati quantitativi sulle operazioni aziendali. In genere, una tabella dei fatti contiene due tipi di colonne: quelle che contengono misure e quelle che contengono una chiave esterna per una tabella di dimensioni.

fallire velocemente

Una filosofia che utilizza test frequenti e incrementali per ridurre il ciclo di vita dello sviluppo. È una parte fondamentale di un approccio agile.

limite di isolamento dei guasti

NelCloud AWS, un limite come una zona di disponibilitàRegione AWS, un piano di controllo o un piano dati che limita l'effetto di un errore e aiuta a migliorare la resilienza dei carichi di lavoro. Per ulteriori informazioni, consulta AWSFault Isolation Boundaries.

ramo di funzionalità

Vedi filiale.

caratteristiche

I dati di input che usi per fare una previsione. Ad esempio, in un contesto di produzione, le caratteristiche potrebbero essere immagini acquisite periodicamente dalla linea di produzione.

importanza delle caratteristiche

Quanto è importante una caratteristica per le previsioni di un modello. Di solito viene espresso come punteggio numerico che può essere calcolato con varie tecniche, come Shapley Additive

Explanations (SHAP) e gradienti integrati. Per ulteriori informazioni, vedere Interpretabilità del modello di machine learning con: AWS.

trasformazione delle funzionalità

Per ottimizzare i dati per il processo di machine learning, incluso l'arricchimento dei dati con fonti aggiuntive, il dimensionamento dei valori o l'estrazione di più set di informazioni da un singolo campo di dati. Ciò consente al modello di ML di trarre vantaggio dai dati. Ad esempio, se suddividi la data "2021-05-27 00:15:37" in "2021", "maggio", "giovedì" e "15", puoi aiutare l'algoritmo di apprendimento ad apprendere modelli sfumati associati a diversi componenti dei dati.

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

L'uso di più condizioni per consentire o rifiutare una richiesta di accesso.

migrazione flash-cut

Un metodo di migrazione del database che utilizza la replica continua dei dati tramite l'acquisizione dei dati delle modifiche per migrare i dati nel più breve tempo possibile, anziché utilizzare un approccio graduale. L'obiettivo è ridurre al minimo i tempi di inattività.

G

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

In Amazon CloudFront, un'opzione per impedire agli utenti di determinati paesi di accedere alle distribuzioni di contenuti. Puoi utilizzare un elenco consentito o un elenco di blocco per specificare i paesi approvati e vietati. Per ulteriori informazioni, consulta Limitare la distribuzione geografica dei contenuti nella CloudFront documentazione.

Flusso di lavoro di GitFlow

Un approccio in cui gli ambienti inferiori e superiori utilizzano rami diversi in un repository di codice di origine. Il flusso di lavoro Gitflow è considerato obsoleto e il flusso di lavoro basato su trunk è l'approccio moderno e preferito.

strategia greenfield

L'assenza di infrastrutture esistenti in un nuovo ambiente. Quando si adotta una strategia greenfield per un'architettura di sistema, è possibile selezionare tutte le nuove tecnologie senza il vincolo della compatibilità con l'infrastruttura esistente, nota anche come brownfield. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

guardrail

Una regola di livello elevato che consente di governare risorse, policy e conformità tra le unità organizzative (OU). I guardrail preventivi applicano le policy per garantire l'allineamento agli standard di conformità. Vengono implementati utilizzando le policy di controllo dei servizi e i limiti delle autorizzazioni IAM. I guardrail di rilevamento rilevano le violazioni delle policy e i problemi di conformità e generano avvisi per porvi rimedio. Sono implementati utilizzando Amazon AWS Config AWS Security Hub GuardDutyAWS Trusted Advisor, Amazon Inspector e controlli personalizzatiAWS Lambda.

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

Migrazione del database di origine in un database di destinazione che utilizza un motore di database diverso (ad esempio, da Oracle ad Amazon Aurora). La migrazione eterogenea fa in genere parte di uno sforzo di riprogettazione e la conversione dello schema può essere un'attività complessa. AWS offre AWS SCT che aiuta con le conversioni dello schema.

alta disponibilità (HA)

La capacità di un carico di lavoro di funzionare in modo continuo, senza intervento, in caso di sfide o disastri. I sistemi HA sono progettati per il failover automatico, fornire costantemente prestazioni di alta qualità e gestire carichi e guasti diversi con un impatto minimo sulle prestazioni.

modernizzazione storica

Un approccio utilizzato per modernizzare e aggiornare i sistemi di tecnologia operativa (OT) per soddisfare meglio le esigenze dell'industria manifatturiera. Uno storico è un tipo di database utilizzato per raccogliere e archiviare dati da varie fonti in una fabbrica.

migrazione di database omogenea

Migrazione del database di origine in un database di destinazione che condivide lo stesso motore di database (ad esempio, da Microsoft SQL Server ad Amazon RDS per SQL Server). La migrazione omogenea fa in genere parte di un'operazione di rehosting o ridefinizione della piattaforma. Per migrare lo schema è possibile utilizzare le utilità native del database.

dati caldi

Dati a cui si accede frequentemente, come dati in tempo reale o dati di traduzione recenti. Questi dati richiedono in genere un livello o una classe di storage ad alte prestazioni per fornire risposte rapide alle query.

hotfix

Una soluzione urgente per un problema critico in un ambiente di produzione. A causa della sua urgenza, un hotfix viene in genere creato al di fuori del tipico DevOps flusso di lavoro di rilascio.

periodo di hypercare

Subito dopo la conversione, il periodo di tempo in cui un team di migrazione gestisce e monitora le applicazioni migrate nel cloud per risolvere eventuali problemi. In genere, questo periodo dura da 1 a 4 giorni. Al termine del periodo di hypercare, il team addetto alla migrazione in genere trasferisce la responsabilità delle applicazioni al team addetto alle operazioni cloud.

I

IaC

Considera l'infrastruttura come codice.

Policy basata su identità

Una policy collegata a uno o più principali IAM che definisce le relative autorizzazioni all'interno dell'ambiente Cloud AWS.

applicazione inattiva

Un'applicazione che prevede un uso di CPU e memoria medio compreso tra il 5% e il 20% in un periodo di 90 giorni. In un progetto di migrazione, è normale ritirare queste applicazioni o mantenerle on-premise.

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

Un modello che implementa una nuova infrastruttura per i carichi di lavoro di produzione anziché aggiornare, applicare patch o modificare l'infrastruttura esistente. Le infrastrutture immutabili sono intrinsecamente più coerenti, affidabili e prevedibili delle infrastrutture mutabili. Per ulteriori informazioni, consulta la best practice Deploy using immutable infrastructure in Well-Architected AWS Framework.

VPC in ingresso (ingress)

In un'architettura multi-account AWS, un VPC che accetta, ispeziona e instrada le connessioni di rete dall'esterno di un'applicazione. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

migrazione incrementale

Una strategia di conversione in cui si esegue la migrazione dell'applicazione in piccole parti anziché eseguire una conversione singola e completa. Ad esempio, inizialmente potresti spostare solo alcuni microservizi o utenti nel nuovo sistema. Dopo aver verificato che tutto funzioni correttamente, puoi spostare in modo incrementale microservizi o utenti aggiuntivi fino alla disattivazione del sistema legacy. Questa strategia riduce i rischi associati alle migrazioni di grandi dimensioni.

infrastruttura

Tutte le risorse e gli asset contenuti nell'ambiente di un'applicazione.

infrastruttura come codice (IaC)

Il processo di provisioning e gestione dell'infrastruttura di un'applicazione tramite un insieme di file di configurazione. Il processo IaC è progettato per aiutarti a centralizzare la gestione dell'infrastruttura, a standardizzare le risorse e a dimensionare rapidamente, in modo che i nuovi ambienti siano ripetibili, affidabili e coerenti.

Internet delle cose industriale (IIoT)

L'uso di sensori e dispositivi connessi a Internet nei settori industriali, come quello manifatturiero, energetico, automobilistico, sanitario, delle scienze della vita e dell'agricoltura. Per ulteriori informazioni, consulta Creazione di una strategia di trasformazione digitale dell'Internet delle cose industriale (IIoT).

VPC di ispezione

In un'architettura multi-account AWS, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPC (in Regioni AWS uguali o diverse), Internet e le reti on-premise. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

Internet of Things (IoT)

La rete di oggetti fisici connessi con sensori o processori incorporati che comunicano con altri dispositivi e sistemi tramite Internet o una rete di comunicazione locale. Per ulteriori informazioni, consulta Cos'è l'IoT?

interpretabilità

Una caratteristica di un modello di machine learning che descrive il grado in cui un essere umano è in grado di comprendere in che modo le previsioni del modello dipendono dai suoi input. Per ulteriori informazioni, consulta la sezione Interpretabilità dei modelli di machine learning con AWS.

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

Una serie di best practice per offrire servizi IT e allinearli ai requisiti aziendali. ITIL fornisce le basi per ITSM.

gestione dei servizi IT (ITSM)

Attività associate alla progettazione, implementazione, gestione e supporto dei servizi IT per un'organizzazione. Per informazioni sull'integrazione delle operazioni cloud con gli strumenti ITSM, consulta la guida all'integrazione delle operazioni.

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

Un'implementazione del controllo di accesso obbligatorio (MAC) in cui agli utenti e ai dati stessi viene assegnato esplicitamente un valore di etichetta di sicurezza. L'intersezione tra l'etichetta di sicurezza utente e l'etichetta di sicurezza dei dati determina quali righe e colonne possono essere visualizzate dall'utente.

zona di destinazione

Una zona di destinazione è un ambiente AWS multi-account ben progettato, scalabile e sicuro. Questo è un punto di partenza dal quale le organizzazioni possono avviare e distribuire rapidamente carichi di lavoro e applicazioni con fiducia nel loro ambiente di sicurezza e infrastruttura. Per ulteriori informazioni sulle zone di destinazione, consulta la sezione Configurazione di un ambiente AWS multi-account sicuro e scalabile.

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

La best practice di sicurezza per la concessione delle autorizzazioni minime richieste per eseguire un'attività. Per ulteriori informazioni, consulta Applicazione delle autorizzazioni del privilegio minimo nella documentazione di IAM.

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

Un sistema che memorizza per primo il byte meno importante. Vedi anche endianità.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

Un tipo di intelligenza artificiale che utilizza algoritmi e tecniche per il riconoscimento e l'apprendimento di schemi. Il machine learning analizza e apprende dai dati registrati, come i dati dell'Internet delle cose (IoT), per generare un modello statistico basato su modelli. Per ulteriori informazioni, consulta la sezione Machine learning.

ramo principale

Vedi filiale.

servizi gestiti

Servizi AWSper cui AWS gestisce il livello di infrastruttura, il sistema operativo e le piattaforme e si accede agli endpoint per archiviare e recuperare i dati. Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e Amazon DynamoDB sono esempi di servizi gestiti. Questi sono noti anche come servizi astratti.

MAP

Vedi Migration Acceleration Program.

meccanismo

Un processo completo in cui si crea uno strumento, si promuove l'adozione dello strumento e quindi si esaminano i risultati per apportare le modifiche. Un meccanismo è un ciclo che si rafforza e si migliora man mano che funziona. Per ulteriori informazioni, consulta Creazione di meccanismi nel AWS Well-Architected Framework.

account membro

Tutti gli Account AWS diversi dall'account di gestione che fanno parte di un'organizzazione in AWS Organizations. Un account può essere membro di una sola organizzazione alla volta.

microservizio

Un piccolo servizio indipendente che comunica tramite API ben definite ed è in genere di proprietà di piccoli team autonomi. Ad esempio, un sistema assicurativo potrebbe includere microservizi che si riferiscono a funzionalità aziendali, come vendite o marketing, o sottodomini, come acquisti, reclami o analisi. I vantaggi dei microservizi includono agilità, dimensionamento flessibile, facilità di implementazione, codice riutilizzabile e resilienza. Per ulteriori informazioni, consulta la sezione Integrazione dei microservizi utilizzando servizi serverless AWS.

architettura di microservizi

Un approccio alla creazione di un'applicazione con componenti indipendenti che eseguono ogni processo applicativo come microservizio. Questi microservizi comunicano tramite un'interfaccia ben definita utilizzando API leggere. Ogni microservizio in questa architettura può essere aggiornato, distribuito e dimensionato per soddisfare la richiesta di funzioni specifiche di un'applicazione. Per ulteriori informazioni, consulta la sezione Implementazione di microservizi su AWS.

Programma di accelerazione della migrazione (MAP)

Un programma AWS che offre consulenza, formazione e servizi per aiutare le organizzazioni a costruire una solida base operativa per il passaggio al cloud e per contribuire a compensare il costo iniziale delle migrazioni. MAP include una metodologia di migrazione per eseguire le migrazioni precedenti in modo metodico e un set di strumenti per automatizzare e accelerare gli scenari di migrazione comuni.

migrazione su larga scala

Il processo di trasferimento della maggior parte del portfolio di applicazioni sul cloud avviene a ondate, con più applicazioni trasferite a una velocità maggiore in ogni ondata. Questa fase utilizza le migliori pratiche e le lezioni apprese nelle fasi precedenti per implementare una fabbrica di migrazione di team, strumenti e processi per semplificare la migrazione dei carichi di lavoro attraverso l'automazione e la distribuzione agile. Questa è la terza fase della strategia di migrazione AWS.

fabbrica di migrazione

Team interfunzionali che semplificano la migrazione dei carichi di lavoro attraverso approcci automatizzati e agili. I team di Migration Factory includono in genere operazioni, analisti e proprietari aziendali, ingegneri addetti alla migrazione, sviluppatori e DevOps professionisti che lavorano negli sprint. Tra il 20% e il 50% di un portfolio di applicazioni aziendali è costituito da schemi ripetuti che possono essere ottimizzati con un approccio di fabbrica. Per ulteriori informazioni, consulta la discussione sulle fabbriche di migrazione e la Guida alla fabbrica di migrazione al cloud in questo set di contenuti.

metadati di migrazione

Le informazioni sull'applicazione e sul server necessarie per completare la migrazione. Ogni modello di migrazione richiede un set diverso di metadati di migrazione. Esempi di metadati di migrazione includono la sottorete di destinazione, il gruppo di sicurezza e l'account AWS.

modello di migrazione

Un'attività di migrazione ripetibile che descrive in dettaglio la strategia di migrazione, la destinazione della migrazione e l'applicazione o il servizio di migrazione utilizzati. Esempio: eseguire il rehosting della migrazione ad Amazon EC2 con AWS Application Migration Service.

Valutazione del portfolio di migrazione (MPA)

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione al cloud AWS. MPA offre una valutazione dettagliata del portfolio (dimensionamento corretto dei server, prezzi, confronto del TCO, analisi dei costi di migrazione) e pianificazione della migrazione (analisi e raccolta dei dati delle applicazioni, raggruppamento delle applicazioni, prioritizzazione delle migrazioni e pianificazione delle ondate). Lo strumento MPA (richiede il login) è disponibile gratuitamente per tutti i consulenti AWS e i consulenti partner APN.

valutazione della preparazione alla migrazione (MRA)

Il processo di acquisizione di informazioni sullo stato di idoneità al cloud di un'organizzazione, l'identificazione dei punti di forza e di debolezza e la creazione di un piano d'azione per colmare le lacune identificate, utilizzando AWS CAF. Per ulteriori informazioni, consulta la guida di preparazione alla migrazione. MRA è la prima fase della strategia di migrazione AWS.

strategia di migrazione

L'approccio utilizzato per eseguire la migrazione di un carico di lavoro verso il cloud AWS. Per ulteriori informazioni, consulta la voce 7 R in questo glossario e consulta Mobilita la tua organizzazione per accelerare le migrazioni su larga scala.

ML

Vedi machine learning.

MAPPA

Vedi Migration Portfolio Assessment.

modernizzazione

Trasformazione di un'applicazione obsoleta (legacy o monolitica) e della relativa infrastruttura in un sistema agile, elastico e altamente disponibile nel cloud per ridurre i costi, aumentare l'efficienza e sfruttare le innovazioni. Per ulteriori informazioni, consulta la sezione Strategia per modernizzare le applicazioni nel cloud AWS.

valutazione della preparazione alla modernizzazione

Una valutazione che aiuta a determinare la preparazione alla modernizzazione delle applicazioni di un'organizzazione, identifica vantaggi, rischi e dipendenze e determina in che misura l'organizzazione può supportare lo stato futuro di tali applicazioni. Il risultato della valutazione è uno schema dell'architettura di destinazione, una tabella di marcia che descrive in dettaglio le fasi di sviluppo e le tappe fondamentali del processo di modernizzazione e un piano d'azione per colmare le lacune identificate. Per ulteriori informazioni, consulta la sezione Valutazione della preparazione alla modernizzazione per le applicazioni nel cloud AWS.

applicazioni monolitiche (monoliti)

Applicazioni eseguite come un unico servizio con processi strettamente collegati. Le applicazioni monolitiche presentano diversi inconvenienti. Se una funzionalità dell'applicazione registra un picco di domanda, l'intera architettura deve essere dimensionata. L'aggiunta o il miglioramento delle funzionalità di un'applicazione monolitica diventa inoltre più complessa man mano che la base di codice cresce. Per risolvere questi problemi, puoi utilizzare un'architettura di microservizi. Per ulteriori informazioni, consulta la sezione Scomposizione dei monoliti in microservizi.

classificazione multiclasse

Un processo che aiuta a generare previsioni per più classi (prevedendo uno o più di due risultati). Ad esempio, un modello di machine learning potrebbe chiedere "Questo prodotto è un libro, un'auto o un telefono?" oppure "Quale categoria di prodotti è più interessante per questo cliente?"

infrastruttura mutabile

Un modello che aggiorna e modifica l'infrastruttura esistente per i carichi di lavoro di produzione. Per migliorare la coerenza, l'affidabilità e la prevedibilità, il AWS Well-Architected Framework consiglia l'uso di un'infrastruttura immutabile come best practice.

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

Un metodo di migrazione in cui il carico di lavoro di origine viene eliminato durante il processo di migrazione. Questo metodo prevede tempi di inattività prolungati e viene in genere utilizzato per carichi di lavoro piccoli e non critici.

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

Un metodo di migrazione in cui il carico di lavoro di origine viene copiato sul sistema di destinazione senza essere messo offline. Le applicazioni connesse al carico di lavoro possono continuare a funzionare durante la migrazione. Questo metodo comporta tempi di inattività pari a zero o comunque minimi e viene in genere utilizzato per carichi di lavoro di produzione critici.

accordo a livello operativo (OLA)

Un accordo che chiarisce quali sono gli impegni reciproci tra i gruppi IT funzionali, a supporto di un accordo sul livello di servizio (SLA).

revisione della prontezza operativa (ORR)

Un elenco di domande e best practice associate che aiutano a comprendere, valutare, prevenire o ridurre la portata degli incidenti e dei possibili guasti. Per ulteriori informazioni, vedere Operational Readiness Reviews (ORR) nel Well-Architected AWS Framework.

integrazione delle operazioni (OI)

Il processo di modernizzazione delle operazioni nel cloud, che prevede la pianificazione, l'automazione e l'integrazione della disponibilità. Per ulteriori informazioni, consulta la guida all'integrazione delle operazioni.

trail organizzativo

Un trail creato da AWS CloudTrail che registra tutti gli eventi per tutti gli Account AWS in un'organizzazione di AWS Organizations. Questo percorso viene creato in ogni Account AWS che

fa parte dell'organizzazione e tiene traccia dell'attività in ogni account. Per ulteriori informazioni, vedere Creazione di un percorso per un'organizzazione nella documentazione. CloudTrail

gestione del cambiamento organizzativo (OCM)

Un framework per la gestione di trasformazioni aziendali importanti e che comportano l'interruzione delle attività dal punto di vista delle persone, della cultura e della leadership. OCM aiuta le organizzazioni a prepararsi e passare a nuovi sistemi e strategie accelerando l'adozione del cambiamento, affrontando i problemi di transizione e promuovendo cambiamenti culturali e organizzativi. Nella strategia di migrazione AWS, questo framework si chiama accelerazione delle persone, a causa della velocità di cambiamento richiesta nei progetti di adozione del cloud. Per ulteriori informazioni, consultare la Guida OCM.

controllo dell'accesso all'origine (OAC)

In CloudFront, un'opzione avanzata per limitare l'accesso per proteggere i contenuti di Amazon Simple Storage Service (Amazon S3). OAC supporta tutti i bucket S3 in tutte le Regioni AWS, crittografia lato server con AWS KMS (SSE-KMS) e richieste `PUT` e `DELETE` dinamiche al bucket S3.

identità di accesso origine (OAI)

Nel CloudFront, un'opzione per limitare l'accesso per proteggere i tuoi contenuti Amazon S3. Quando usi OAI, CloudFront crea un principale con cui Amazon S3 può autenticarsi. I principali autenticati possono accedere ai contenuti in un bucket S3 solo tramite una distribuzione specifica. CloudFront Vedi anche OAC, che fornisce un controllo degli accessi più granulare e avanzato.

O

Vedi la revisione della prontezza operativa.

VPC in uscita (egress)

In un'architettura multi-account AWS, un VPC che gestisce le connessioni di rete avviate dall'interno di un'applicazione. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

P

limite delle autorizzazioni

Una policy di gestione IAM collegata ai principali IAM per impostare le autorizzazioni massime che l'utente o il ruolo possono avere. Per ulteriori informazioni, consulta Limiti delle autorizzazioni nella documentazione di IAM.

informazioni di identificazione personale (PII)

Informazioni che, se visualizzate direttamente o abbinate ad altri dati correlati, possono essere utilizzate per dedurre ragionevolmente l'identità di un individuo. Esempi di informazioni personali includono nomi, indirizzi e informazioni di contatto.

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

Una serie di passaggi predefiniti che raccolgono il lavoro associato alle migrazioni, come l'erogazione delle funzioni operative principali nel cloud. Un playbook può assumere la forma di script, runbook automatici o un riepilogo dei processi o dei passaggi necessari per gestire un ambiente modernizzato.

policy

Un oggetto in grado di definire le autorizzazioni (vedere la politica basata sull'identità), specificare le condizioni di accesso (vedere la politicabasata sulle risorse) o definire le autorizzazioni massime per tutti gli account di un'organizzazione in (vedere la politica di controllo dei servizi). AWS Organizations

persistenza poliglotta

Scelta indipendente della tecnologia di archiviazione di dati di un microservizio in base ai modelli di accesso ai dati e ad altri requisiti. Se i microservizi utilizzano la stessa tecnologia di archiviazione di dati, possono incontrare problemi di implementazione o registrare prestazioni scadenti. I microservizi vengono implementati più facilmente e ottengono prestazioni e scalabilità migliori se utilizzano l'archivio dati più adatto alle loro esigenze. Per ulteriori informazioni, consulta la sezione Abilitazione della persistenza dei dati nei microservizi.

valutazione del portfolio

Un processo di scoperta, analisi e definizione delle priorità del portfolio di applicazioni per pianificare la migrazione. Per ulteriori informazioni, consulta la pagina Valutazione della preparazione alla migrazione.

predicate

Una condizione di interrogazione che restituisce o, in genere, si trova in una clausola `WHERE` che restituisce `true` o `false`.

predicato pushdown

Una tecnica di ottimizzazione delle query del database che filtra i dati della query prima del trasferimento. Ciò riduce la quantità di dati che devono essere recuperati ed elaborati dal database relazionale e migliora le prestazioni delle query.

controllo preventivo

Un controllo di sicurezza progettato per impedire il verificarsi di un evento. Questi controlli sono la prima linea di difesa per impedire accessi non autorizzati o modifiche indesiderate alla rete. Per ulteriori informazioni, consulta Controlli preventivi in Implementazione dei controlli di sicurezza in AWS.

principale

Un'entità in AWS che può eseguire operazioni e accedere alle risorse. Questa entità è in genere un utente root per un Account AWS, un ruolo IAM o un utente. Per ulteriori informazioni, consulta Principali in Termini e concetti dei ruoli nella documentazione di IAM.

Privacy fin dalla progettazione

Un approccio all'ingegneria dei sistemi che tiene conto della privacy durante l'intero processo di progettazione.

zone ospitate private

Un container che contiene informazioni su come si desidera che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più VPC. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private nella documentazione di Route 53.

controllo proattivo

Un controllo di sicurezza progettato per impedire l'implementazione di risorse non conformi. Questi controlli analizzano le risorse prima del loro provisioning. Se la risorsa non è conforme al

controllo, non viene fornita. Per ulteriori informazioni, consulta la guida di riferimento sui controlli nella AWS Control Tower documentazione e consulta Controlli proattivi in Implementazione dei controlli di sicurezza su. AWS

Ambiente di produzione

Vedi ambiente.

pseudonimizzazione

Il processo di sostituzione degli identificatori personali in un set di dati con valori segnaposto. La pseudonimizzazione può aiutare a proteggere la privacy personale. I dati pseudonimizzati sono ancora considerati dati personali.

Q

Piano di query

Una serie di passaggi, come le istruzioni, utilizzati per accedere ai dati in un sistema di database relazionale SQL.

regressione del piano di query

Quando un ottimizzatore del servizio di database sceglie un piano non ottimale rispetto a prima di una determinata modifica all'ambiente di database. Questo può essere causato da modifiche a statistiche, vincoli, impostazioni dell'ambiente, associazioni dei parametri di query e aggiornamenti al motore di database.

R

Matrice RACI

Vedi responsabile, responsabile, consultato, informato (RACI).

ransomware

Un software dannoso progettato per bloccare l'accesso a un sistema informatico o ai dati fino a quando non viene effettuato un pagamento.

Matrice RASCI

Vedi responsabile, responsabile, consultato, informato (RACI).

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

Una copia di un database utilizzata per scopi di sola lettura. È possibile indirizzare le query alla replica di lettura per ridurre il carico sul database principale.

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

Il periodo di tempo massimo accettabile dall'ultimo punto di ripristino dei dati. Ciò determina quella che viene considerata una perdita di dati accettabile tra l'ultimo punto di ripristino e l'interruzione del servizio.

obiettivo del tempo di ripristino (RTO)

Il ritardo massimo accettabile tra l'interruzione del servizio e il ripristino del servizio.

rifattorizzare

Vedi 7 R.

Regione

Una raccolta di risorse AWS in un'area geografica. Ogni Regione AWS è isolata e indipendente dalle altre per fornire tolleranza agli errori, stabilità e resilienza. Per ulteriori informazioni, consulta Gestione delle Regioni AWS nei Riferimenti generali di AWS.

regressione

Una tecnica di ML che prevede un valore numerico. Ad esempio, per risolvere il problema "A che prezzo verrà venduta questa casa?" un modello di ML potrebbe utilizzare un modello di regressione lineare per prevedere il prezzo di vendita di una casa sulla base di dati noti sulla casa (ad esempio, la metratura).

riospitare

Vedi 7 R.

rilascio

In un processo di implementazione, l'atto di promuovere modifiche a un ambiente di produzione.

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

policy basata su risorse

Una policy associata a una risorsa, ad esempio un bucket Amazon S3, un endpoint o una chiave di crittografia. Questo tipo di policy specifica a quali principali è consentito l'accesso, le azioni supportate e qualsiasi altra condizione che deve essere soddisfatta.

matrice di assegnazione di responsabilità (RACI)

Una matrice che definisce i ruoli e le responsabilità di tutte le parti coinvolte nelle attività di migrazione e nelle operazioni cloud. Il nome della matrice deriva dai tipi di responsabilità definiti nella matrice: responsabile (R), responsabile (A), consultato (C) e informato (I). Il tipo di supporto (S) è facoltativo. Se includi il supporto, la matrice viene chiamata matrice RASCI e, se la escludi, viene chiamata matrice RACI.

controllo reattivo

Un controllo di sicurezza progettato per favorire la correzione di eventi avversi o deviazioni dalla baseline di sicurezza. Per ulteriori informazioni, consulta Controlli reattivi in Implementazione dei controlli di sicurezza in AWS.

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

rotazione

Processo di aggiornamento periodico di un segreto per rendere più difficile l'accesso alle credenziali da parte di un utente malintenzionato.

controllo dell'accesso a righe e colonne (RCAC)

L'uso di espressioni SQL di base e flessibili con regole di accesso definite. RCAC è costituito da autorizzazioni di riga e maschere di colonna.

RPO

Vedi l'obiettivo del punto di ripristino.

RTO

Vedi l'obiettivo del tempo di ripristino.

runbook

Un insieme di procedure manuali o automatizzate necessarie per eseguire un'attività specifica. In genere sono progettati per semplificare operazioni o procedure ripetitive con tassi di errore elevati.

S

SAML 2.0

Uno standard aperto utilizzato da molti provider di identità (IdPs). Questa funzionalità consente l'autenticazione unica (SSO) federata, grazie alla quale gli utenti possono accedere alla AWS Management Console o eseguire chiamate alle operazioni delle API AWS. In questo modo non è necessario creare un utente IAM per tutti gli utenti nell'organizzazione. Per ulteriori informazioni sulla federazione basata su SAML 2.0, consulta Informazioni sulla federazione basata su SAML 2.0 nella documentazione di IAM.

SCP

Vedi la politica di controllo del servizio.

Secret

InAWS Secrets Manager, informazioni riservate o riservate, come una password o le credenziali utente, archiviate in forma crittografata. È costituito dal valore segreto e dai relativi metadati. Il valore segreto può essere binario, una stringa singola o più stringhe. Per ulteriori informazioni, consulta Secret nella documentazione di Secrets Manager.

controllo di sicurezza

Un guardrail tecnico o amministrativo che impedisce, rileva o riduce la capacità di un autore di minacce di sfruttare una vulnerabilità di sicurezza. Esistono quattro tipi principali di controlli di sicurezza: preventivi, investigativi, reattivi e proattivi.

rafforzamento della sicurezza

Il processo di riduzione della superficie di attacco per renderla più resistente agli attacchi. Può includere azioni come la rimozione di risorse che non sono più necessarie, l'implementazione di best practice di sicurezza che prevedono la concessione del privilegio minimo o la disattivazione di funzionalità non necessarie nei file di configurazione.

sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM)

Strumenti e servizi che combinano sistemi di gestione delle informazioni di sicurezza (SIM) e sistemi di gestione degli eventi di sicurezza (SEM). Un sistema SIEM raccoglie, monitora e analizza i dati da server, reti, dispositivi e altre fonti per rilevare minacce e violazioni della sicurezza e generare avvisi.

automazione della risposta alla sicurezza

Un'azione predefinita e programmata progettata per rispondere o porre rimedio automaticamente a un evento di sicurezza. Queste automazioni fungono da controlli di sicurezza investigativi o reattivi che aiutano a implementare le migliori pratiche di sicurezza. AWS Esempi di azioni di risposta automatizzate includono la modifica di un gruppo di sicurezza VPC, l'applicazione di patch a un'istanza Amazon EC2 o la rotazione delle credenziali.

Crittografia lato server

Crittografia dei dati a destinazione, da parte del Servizio AWS che li riceve.

Policy di controllo dei servizi (SCP)

Una policy che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in AWS Organizations. Le SCP definiscono i guardrail o fissano i limiti alle azioni che un amministratore può delegare a utenti o ruoli. Puoi utilizzare le SCP come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per ulteriori informazioni, consulta Policy di sicurezza dei servizi nella documentazione di AWS Organizations.

endpoint del servizio

L'URL del punto di accesso per un Servizio AWS. Puoi utilizzare l'endpoint per connetterti a livello di programmazione al servizio di destinazione. Per ulteriori informazioni, consulta Endpoint del Servizio AWS nei Riferimenti generali di AWS.

accordo sul livello di servizio (SLA)

Un accordo che chiarisce ciò che un team IT promette di offrire ai propri clienti, ad esempio l'operatività e le prestazioni del servizio.

indicatore del livello di servizio (SLI)

Misurazione di un aspetto prestazionale di un servizio, ad esempio il tasso di errore, la disponibilità o la velocità effettiva.

obiettivo a livello di servizio (SLO)

Una metrica target che rappresenta lo stato di un servizio, misurato da un indicatore del livello di servizio.

Modello di responsabilità condivisa

Un modello che descrive la responsabilità condivisa con AWS per la sicurezza e la conformità del cloud. AWS è responsabile della sicurezza del cloud, mentre l'utente è responsabile della sicurezza nel cloud. Per ulteriori informazioni, consulta Modello di responsabilità condivisa.

SIEM

Vedi il sistema di gestione delle informazioni e degli eventi sulla sicurezza.

punto di errore singolo (SPOF)

Un guasto in un singolo componente critico di un'applicazione che può disturbare il sistema.

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

Un modello per dimensionare e accelerare i progetti di modernizzazione. Man mano che vengono definite nuove funzionalità e versioni dei prodotti, il team principale si divide per creare nuovi team di prodotto. Questo aiuta a dimensionare le capacità e i servizi dell'organizzazione, migliora la produttività degli sviluppatori e supporta una rapida innovazione. Per ulteriori informazioni, vedere Approccio graduale alla modernizzazione delle applicazioni in. Cloud AWS

SPOF

Vedi punto di errore singolo.

schema a stella

Una struttura organizzativa di database che utilizza un'unica tabella dei fatti di grandi dimensioni per archiviare i dati transazionali o misurati e utilizza una o più tabelle dimensionali più piccole per memorizzare gli attributi dei dati. Questa struttura è progettata per l'uso in un data warehouse o per scopi di business intelligence.

modello del fico strangolatore

Un approccio alla modernizzazione dei sistemi monolitici mediante la riscrittura e la sostituzione incrementali delle funzionalità del sistema fino alla disattivazione del sistema legacy. Questo modello utilizza l'analogia di una pianta di fico che cresce fino a diventare un albero robusto e alla fine annienta e sostituisce il suo ospite. Il modello è stato introdotto da Martin Fowler come metodo per gestire il rischio durante la riscrittura di sistemi monolitici. Per un esempio di come applicare questo modello, consulta Modernizzazione incrementale dei servizi Web legacy di Microsoft ASP.NET (ASMX) mediante container e Gateway Amazon API.

sottorete

Un intervallo di indirizzi IP nel VPC. Una sottorete deve risiedere in una singola zona di disponibilità.

crittografia simmetrica

Un algoritmo di crittografia che utilizza la stessa chiave per crittografare e decrittografare i dati.

test sintetici

Test di un sistema in modo da simulare le interazioni degli utenti per rilevare potenziali problemi o monitorare le prestazioni. Puoi usare Amazon CloudWatch Synthetics per creare questi test.

T

tags

Coppie chiave-valore che fungono da metadati per l'organizzazione delle risorse. AWS Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare le risorse. Per ulteriori informazioni, consulta Tagging delle risorse AWS.

variabile di destinazione

Il valore che stai cercando di prevedere nel machine learning supervisionato. Questo è indicato anche come variabile di risultato. Ad esempio, in un ambiente di produzione la variabile di destinazione potrebbe essere un difetto del prodotto.

elenco di attività

Uno strumento che viene utilizzato per tenere traccia dei progressi tramite un runbook. Un elenco di attività contiene una panoramica del runbook e un elenco di attività generali da completare. Per ogni attività generale, include la quantità stimata di tempo richiesta, il proprietario e lo stato di avanzamento.

Ambiente di test

Vedi ambiente.

training

Fornire dati da cui trarre ispirazione dal modello di machine learning. I dati di training devono contenere la risposta corretta. L'algoritmo di apprendimento trova nei dati di addestramento i pattern che mappano gli attributi dei dati di input al target (la risposta che si desidera prevedere). Produce un modello di ML che acquisisce questi modelli. Puoi quindi utilizzare il modello di ML per creare previsioni su nuovi dati di cui non si conosce il target.

Transit Gateway

Un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti on-premise. Per ulteriori informazioni, consulta Che cos'è un Transit Gateway? nella documentazione di AWS Transit Gateway.

flusso di lavoro basato su trunk

Un approccio in cui gli sviluppatori creano e testano le funzionalità localmente in un ramo di funzionalità e quindi uniscono tali modifiche al ramo principale. Il ramo principale viene quindi integrato negli ambienti di sviluppo, preproduzione e produzione, in sequenza.

Accesso attendibile

La concessione di autorizzazioni a un servizio specificato dall'utente per eseguire attività all'interno dell'organizzazione in AWS Organizations e nei relativi account per conto dell'utente. Il servizio attendibile crea un ruolo collegato al servizio in ogni account, quando tale ruolo è necessario, per eseguire attività di gestione per conto dell'utente. Per ulteriori informazioni,

consulta Utilizzo di AWS Organizations con altri servizi AWS nella documentazione di AWS Organizations.

regolazione

Modificare alcuni aspetti del processo di training per migliorare la precisione del modello di ML. Ad esempio, puoi addestrare il modello di ML generando un set di etichette, aggiungendo etichette e quindi ripetendo questi passaggi più volte con impostazioni diverse per ottimizzare il modello.

team da due pizze

Una piccola DevOps squadra che puoi sfamare con due pizze. Un team composto da due persone garantisce la migliore opportunità possibile di collaborazione nello sviluppo del software.

U

incertezza

Un concetto che si riferisce a informazioni imprecise, incomplete o sconosciute che possono minare l'affidabilità dei modelli di machine learning predittivi. Esistono due tipi di incertezza: l'incertezza epistemica, che è causata da dati limitati e incompleti, mentre l'incertezza aleatoria è causata dal rumore e dalla casualità insiti nei dati. Per ulteriori informazioni, consulta la guida Quantificazione dell'incertezza nei sistemi di deep learning.

compiti indifferenziati

Conosciuto anche come sollevamento di carichi pesanti, è un lavoro necessario per creare e far funzionare un'applicazione, ma che non apporta valore diretto all'utente finale né offre vantaggi competitivi. Esempi di attività indifferenziate includono l'approvvigionamento, la manutenzione e la pianificazione della capacità.

ambienti superiori

Vedi ambiente.

V

vacuum

Un'operazione di manutenzione del database che prevede la pulizia dopo aggiornamenti incrementali per recuperare lo spazio di archiviazione e migliorare le prestazioni.

controllo delle versioni

Processi e strumenti che tengono traccia delle modifiche, ad esempio le modifiche al codice di origine in un repository.

Peering VPC

Una connessione tra due VPC che consente di instradare il traffico tramite indirizzi IP privati. Per ulteriori informazioni, consulta Che cos'è il peering VPC? nella documentazione di Amazon VPC.

vulnerabilità

Un difetto software o hardware che compromette la sicurezza del sistema.

W

cache calda

Una cache del buffer che contiene dati correnti e pertinenti a cui si accede frequentemente. L'istanza di database può leggere dalla cache del buffer, il che richiede meno tempo rispetto alla lettura dalla memoria dal disco principale.

dati caldi

Dati a cui si accede raramente. Quando si eseguono interrogazioni di questo tipo di dati, in genere sono accettabili interrogazioni moderatamente lente.

funzione finestra

Una funzione SQL che esegue un calcolo su un gruppo di righe che si riferiscono in qualche modo al record corrente. Le funzioni della finestra sono utili per l'elaborazione di attività, come il calcolo di una media mobile o l'accesso al valore delle righe in base alla posizione relativa della riga corrente.

Carico di lavoro

Una raccolta di risorse e codice che fornisce valore aziendale, ad esempio un'applicazione rivolta ai clienti o un processo back-end.

flusso di lavoro

Gruppi funzionali in un progetto di migrazione responsabili di una serie specifica di attività. Ogni flusso di lavoro è indipendente ma supporta gli altri flussi di lavoro del progetto. Ad esempio, il flusso di lavoro del portfolio è responsabile della definizione delle priorità delle applicazioni,

della pianificazione delle ondate e della raccolta dei metadati di migrazione. Il flusso di lavoro del portfolio fornisce queste risorse al flusso di lavoro di migrazione, che quindi migra i server e le applicazioni.

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

Un modello di storage che scrive i dati una sola volta e ne impedisce l'eliminazione o la modifica. Gli utenti autorizzati possono leggere i dati tutte le volte che è necessario, ma non possono modificarli. Questa infrastruttura di archiviazione dei dati è considerata immutabile.

Z

exploit zero-day

Un attacco, in genere malware, che sfrutta una vulnerabilità zero-day.

vulnerabilità zero-day

Un difetto o una vulnerabilità assoluta in un sistema di produzione. Gli autori delle minacce possono utilizzare questo tipo di vulnerabilità per attaccare il sistema. Gli sviluppatori vengono spesso a conoscenza della vulnerabilità causata dall'attacco.

applicazione zombie

Un'applicazione che prevede un utilizzo CPU e memoria inferiore al 5%. In un progetto di migrazione, è normale ritirare queste applicazioni.

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.