



Approcci di backup e ripristino su AWS

AWS Linee guida prescrittive



AWS Linee guida prescrittive: Approcci di backup e ripristino su AWS

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Introduzione	1
Perché utilizzarla AWS come piattaforma di protezione dei dati?	2
Obiettivi aziendali specifici	4
Scelta AWS dei servizi	5
Progettazione di una soluzione di backup e ripristino	7
AWS Backup	8
Simple Storage Service (Amazon S3)	10
Utilizzo delle classi di storage di Amazon S3	10
Creazione di bucket S3 standard	12
Utilizzo del controllo delle versioni di Amazon S3	12
Backup e ripristino di file di configurazione personalizzati per AMIs	12
Backup e ripristino personalizzati	13
Protezione dei dati di backup	13
Amazon EC2 con volumi EBS	14
Backup e ripristino di Amazon EC2	16
AMI o istantanee	16
Volumi del server	18
Volumi di server separati	19
Volumi di archivio dell'istanza	19
Etichettatura e applicazione degli standard	20
Crea backup di volumi EBS	21
Preparazione di un volume EBS	21
Creazione di istantanee dalla console	23
Creazione di AMI	23
Amazon Data Lifecycle Manager	24
AWS Backup	25
Multi-volume backup	25
Protezione dei backup	27
Archiviazione delle istantanee	28
Automatizzazione della creazione di istantanee e AMI	28
Ripristina un volume o un'istanza	29
Ripristino di file e directory dalle istantanee EBS	30
Ripristino di un volume EBS da uno snapshot Amazon EBS	30
Creazione o ripristino di un'istanza EC2 da uno snapshot EBS	32

Ripristino di un'istanza in esecuzione da un'AMI	33
Backup e ripristino da locale	34
Gateway di file	35
Gateway di volumi	35
Gateway di nastri virtuali	36
Backup e ripristino delle applicazioni	38
Servizi nativi per il cloud AWS	39
Amazon RDS	39
Utilizzo di DNS CNAME	40
DynamoDB	42
Architetture ibride	44
Spostamento delle soluzioni centralizzate di gestione dei backup	45
Ripristino di emergenza	47
On-premises DR a AWS	47
DR per carichi di lavoro nativi del cloud	49
DR in un'unica zona di disponibilità	50
DR in caso di errore regionale	50
Pulizia dei backup	52
Domande frequenti	53
Quale pianificazione di backup devo selezionare?	53
Devo creare backup nei miei account di sviluppo?	53
Posso aggiornare le applicazioni e continuare a utilizzare un volume EBS mentre viene creata un'istanza senza alcun impatto?	53
Passaggi successivi	54
Resources	55
Cronologia dei documenti	56
.....	lix

Approcci di backup e ripristino su AWS

Khurram Nizami, Amazon Web Services (AWS)

Giugno 2024 [\(cronologia del documento\)](#)

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

Questa guida è destinata ai responsabili tecnici responsabili della protezione dei dati nei propri 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 dell'architettura.

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

- Serverless con AWS Lambda
- Contenitori con Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) e AWS Fargate
- Amazon Machine Images (AMIs) 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 servizi per la protezione dei dati](#)
- [Progettazione di una soluzione di backup e ripristino](#)
- [Backup e ripristino tramite AWS Backup](#)

- [Backup e ripristino con Amazon S3](#)
- [Backup e ripristino per Amazon EC2 con volumi EBS](#)
- [Backup e ripristino dall'infrastruttura locale a AWS](#)
- [Backup e ripristino delle applicazioni dal AWS data center](#)
- [Backup e ripristino di servizi nativi del cloud AWS](#)
- [Backup e ripristino per architetture ibride](#)
- [Disaster recovery con AWS](#)
- [Pulizia dei backup](#)

Perché utilizzarla AWS come piattaforma di protezione dei dati?

AWS è una piattaforma di cloud computing sicura, ad alte prestazioni, flessibile, che consente di risparmiare denaro. easy-to-use AWS si occupa del lavoro indifferenziato necessario per creare, implementare e gestire soluzioni di backup e ripristino scalabili.

L'utilizzo AWS come parte della strategia di protezione dei dati presenta molti vantaggi:

- **Durabilità:** Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e S3 Glacier Deep Archive sono progettati per una durabilità del 99,999999999% (11 nove). Entrambe le piattaforme offrono un backup affidabile dei dati, con replica degli oggetti su almeno tre zone di disponibilità geograficamente distribuite. Molti AWS servizi utilizzano Amazon S3 per lo storage e export/import le operazioni. Ad esempio, Amazon Elastic Block Store (Amazon EBS) utilizza Amazon S3 per lo storage di snapshot.
- **Sicurezza:** AWS offre una serie di opzioni per il controllo degli accessi e la crittografia dei dati in transito e a riposo.
- **Infrastruttura globale:** AWS i servizi sono disponibili in tutto il mondo, quindi è possibile eseguire il backup e l'archiviazione dei dati nella regione che soddisfa i requisiti di conformità e carico di lavoro.
- **Conformità:** L'AWS infrastruttura è certificata per la conformità ai seguenti standard, quindi è possibile 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: con AWS, non devi preoccuparti della capacità. Man mano che le tue esigenze cambiano, puoi aumentare o ridurre i consumi senza sovraccarichi amministrativi.
- Riduzione del costo totale di proprietà (TCO): la scalabilità delle AWS operazioni riduce i costi dei servizi e aiuta a ridurre il TCO dei servizi. AWS trasferisce questi risparmi sui costi ai clienti attraverso riduzioni dei prezzi.
- Pay-as-you-go prezzi: acquisti AWS i servizi quando ne hai bisogno e solo per il periodo in cui prevedi di utilizzarli. AWS i 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 dei AWS servizi che è possibile utilizzare per supportare gli approcci di backup e ripristino per quanto segue:

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

Le migliori pratiche e considerazioni sono trattate insieme a una panoramica dei servizi. Questa guida illustra anche i compromessi tra l'utilizzo di un approccio rispetto a un altro per il backup e il ripristino.

Scelta AWS 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](#) è adatto per casi d'uso ibridi e nativi per il cloud. Fornisce soluzioni di storage di oggetti generiche e altamente durevoli, adatte per il backup di singoli file, server o di un intero data center.
- [Gateway di archiviazione AWS](#) è 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:
 - File system di rete (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:

- Simple Storage Service (Amazon S3)
- 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 Backup](#) è 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

- Volumi Storage Gateway

Il costo di si AWS Backup basa sullo storage utilizzato, ripristinato e trasferito in un mese. Per ulteriori informazioni, consulta i [AWS Backup prezzi](#).

- [AWS Elastic Disaster Recovery](#) replica i computer in una sottorete dell'area di gestione temporanea nella regione di destinazione Account AWS e preferita. Il design dell'area di staging riduce i costi utilizzando uno storage conveniente e risorse di elaborazione minime per mantenere una replica continua. Puoi utilizzare Elastic Disaster Recovery for DR dall'ambiente on-premise al cloud e per il DR. in più regioni
- [AWS Config](#) fornisce 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 Lambda](#) può 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 usare [Amazon EventBridge](#) per eseguire le tue 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 errore o di emergenza e il loro potenziale impatto aziendale. In alcuni settori, è necessario prendere in considerazione 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 EC2 livello di volume Amazon (ad esempio, un volume EBS)
- EC2 ripristino a livello di istanza. (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, coordinate il backup e il ripristino tra i vari componenti dell'architettura.

I seguenti argomenti descrivono gli approcci di backup e ripristino basati sull'organizzazione dell'infrastruttura. L'infrastruttura IT può essere generalmente classificata come locale, ibrida o nativa per il cloud.

Backup e ripristino tramite AWS Backup

AWS Backup è un servizio di backup completamente gestito che centralizza e automatizza il backup dei dati tra i servizi. AWS Backup fornisce un livello di orchestrazione che integra CloudWatch, Amazon CloudTrail, AWS Identity and Access Management (IAM) e AWS Organizations e altri servizi. Questa soluzione centralizzata e nativa del AWS cloud offre funzionalità di backup globali che possono aiutarti a soddisfare i requisiti di disaster recovery e conformità. Utilizzando AWS Backup, è possibile configurare centralmente le politiche di backup e monitorare l'attività di backup AWS delle risorse.

AWS Backup è la soluzione ideale per implementare piani di backup standard per le AWS risorse in tutti gli account e le regioni. Poiché AWS Backup supporta più tipi di AWS risorse, semplifica la manutenzione e l'implementazione di una strategia di backup per i carichi di lavoro che utilizzano più AWS risorse di cui è necessario eseguire il backup collettivamente. AWS Backup consente inoltre di monitorare collettivamente un'operazione di backup e ripristino che coinvolge più risorse. AWS

Se hai requisiti di conformità e audit, puoi utilizzare la funzionalità [AWS Backup Audit Manager](#) per creare framework e report di audit a supporto dei tuoi requisiti di conformità. La funzionalità [AWS Backup Vault Lock](#) supporta anche i requisiti di conformità applicando una configurazione WORM (Write-Once, Read-Many) per tutti i backup archiviati in un archivio di backup in AWS Backup.

Un elemento chiave di differenziazione AWS Backup è il supporto per Organizzazioni. Utilizzando questo supporto, è possibile definire e gestire le politiche di backup a livello di organizzazione o unità organizzativa e far sì che tali politiche vengano implementate automaticamente per ogni AWS account e regione correlati. Durante l'onboarding di nuovi AWS account e regioni, non è necessario definire e gestire i piani di backup separatamente.

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

Ad esempio, è possibile creare un piano di backup giornaliero che avvii un backup alle 05:00 UTC su base giornaliera e abbia una politica di conservazione di 35 giorni. Questo piano di backup può includere un'[assegnazione di risorse di backup](#) che specifichi che tutte le AWS risorse supportate con il tag «backup, chiave» e «tag value» verranno sottoposte giornalmente a backup in base a questo piano. Inoltre, è possibile creare un piano di backup mensile che inizi alle 05:00 UTC del primo giorno di ogni mese e abbia una politica di conservazione di 366 giorni. Questo piano di backup

può includere un'assegnazione di risorse di backup che specifichi che ogni AWS risorsa supportata con il tag, key backup e tag value verrà sottoposto mensilmente a un backup in base a questo piano.

È quindi possibile utilizzare le politiche di tag e la AWS Config regola [required-tags](#) per garantire che tutte le risorse AWS supportate abbiano questa chiave di tag e uno di questi valori di tag. Questo approccio può aiutarvi a implementare e mantenere in modo coerente un approccio di backup standard AWS per le risorse supportate. AWS Backup È possibile estendere questo approccio per standardizzare i backup per le applicazioni e i livelli architetturici che hanno requisiti RPO (Recovery Point Objective) diversi.

Ti consigliamo di adottare misure per proteggere il tuo archivio di backup. Ad esempio, è possibile implementare una policy di controllo dei servizi (SCP) dell'Organizations che impedisce l'eliminazione del backup vault o la condivisione con account AWS indesiderati. Per ulteriori dettagli e altre importanti considerazioni sulla sicurezza, consulta le [10 migliori pratiche di sicurezza per proteggere i backup nel post del blog](#). AWS

AWS Backup può semplificare l'implementazione del piano di disaster recovery (DR) AWS perché supporta più AWS risorse che possono essere gestite collettivamente. Ad esempio, è possibile implementare il backup [tra regioni](#) e più [account](#) per la maggior parte dei tipi di AWS risorse supportati da AWS 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 dettagliate sui tipi di AWS risorse supportati, consulta la tabella [Disponibilità delle funzionalità per risorsa](#).

È possibile utilizzare l'esempio [Backup and Recovery con soluzione AWS Backup open source](#) per implementare un approccio Infrastructure as Code (IaC) e un approccio di integrazione continua e distribuzione continua (CI/CD) per la gestione dei backup per l'organizzazione. AWS Organizations Questa soluzione include funzionalità personalizzate, come la riapplicazione automatica dei AWS tag sulle AWS risorse ripristinate e la creazione di un archivio di backup secondario in un account e in una regione separati per scopi di disaster recovery.

Backup e ripristino con Amazon S3

Puoi utilizzare Amazon Simple Storage Service (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 o. AWS SDKs

Servizi AWS usa 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 di 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.

Utilizzo delle classi di storage Amazon S3 per ridurre i costi di storage dei dati di backup

Amazon S3 offre più classi di storage da utilizzare in architetture locali, ibride e native per il cloud. Tutte le classi di storage offrono una capacità scalabile che non richiede 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 unità GB/month rendono le classi di storage Amazon S3 adatte a un'ampia gamma

di casi d'uso di protezione dei dati. Le classi di storage Amazon S3 sono progettate per diversi casi d'uso, incluse le seguenti categorie:

- [Classi di storage ad accesso frequente](#) per l'archiviazione generica dei dati a cui si accede di frequente (ad esempio, file di configurazione, backup non pianificati, backup giornalieri). Ciò include la classe di storage S3 Standard, che è l'impostazione predefinita per tutti gli oggetti Amazon S3.
- [Classi di storage ad accesso poco frequente](#) per dati di lunga durata ma a cui si accede raramente (ad esempio, backup mensili). Ciò include la classe di storage S3 Standard-IA. IA è l'acronimo di Infrequent Access.
- [Classi di storage S3 Glacier](#) per dati estremamente longevi a cui è necessario accedere raramente (ad esempio, backup annuali). Ciò include S3 Glacier Deep Archive, che offre lo storage a più basso costo. AWS

[Per i backup con modelli di accesso sconosciuti o modificati, puoi utilizzare la classe di storage S3 Intelligent-Tiering.](#) S3 Intelligent-Tiering trasferisce automaticamente gli oggetti al livello più conveniente in base a quanti giorni fa è stato effettuato l'ultimo accesso a un oggetto.

 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

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 automaticamente 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

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 AMIs

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 AWS Marketplace 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 le operazioni AWS CLI AWS SDKs, e 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, puoi utilizzarlo 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.

Protezione dei dati di backup in Amazon S3

La sicurezza dei dati è una preoccupazione universale e AWS prende molto sul serio la sicurezza. La sicurezza è alla base di ogni Servizio AWS. Amazon S3 offre funzionalità per il controllo degli accessi e la crittografia sia a riposo che in transito. Tutti gli endpoint Amazon S3 supportano SSL/TLS per la crittografia dei dati in transito. Puoi configurare la crittografia per gli oggetti inattivi effettuando le seguenti operazioni:

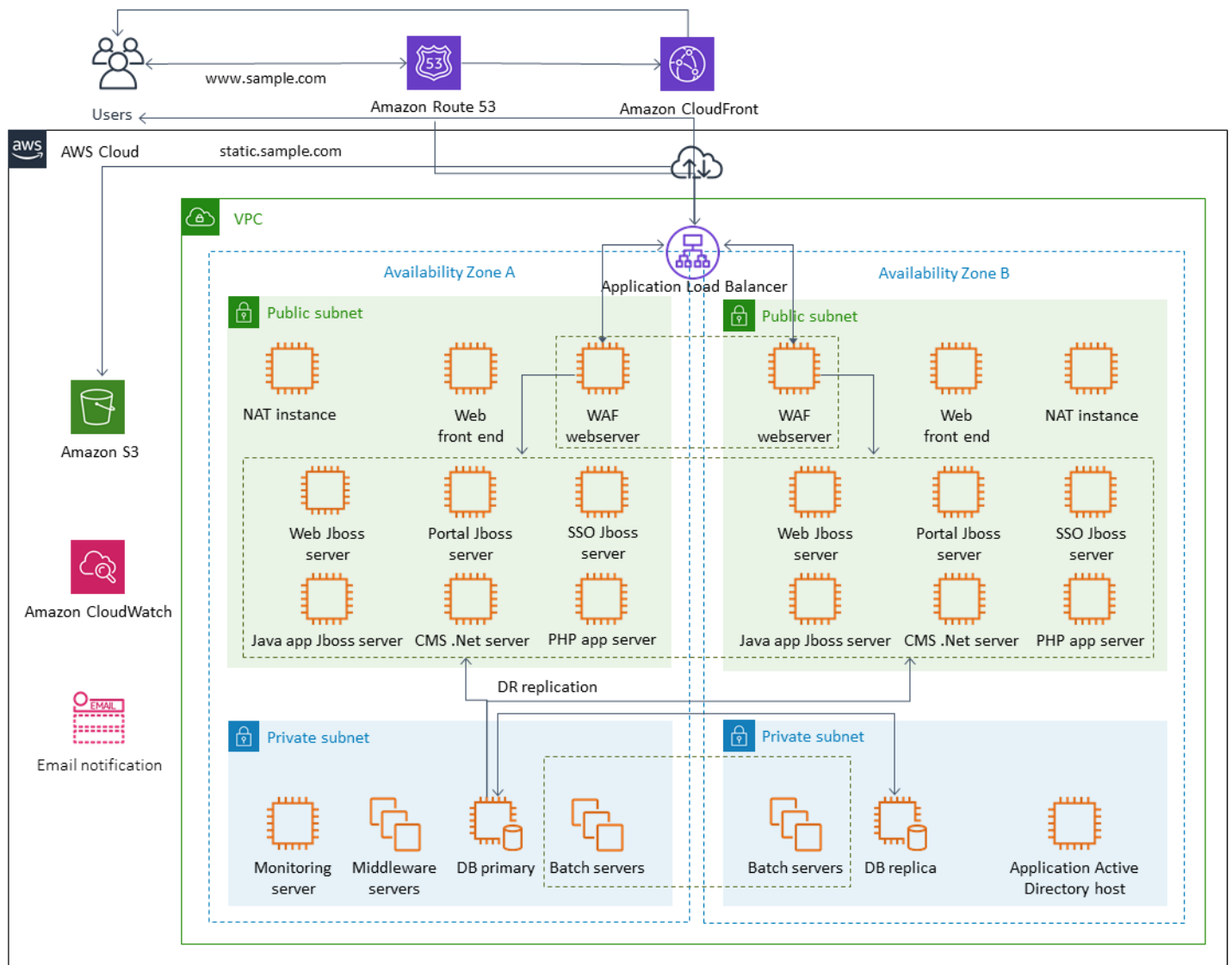
- Utilizzo della [crittografia lato server con chiavi di crittografia gestite di Amazon S3 \(impostazione predefinita\)](#)
- Utilizzo della [crittografia lato server con AWS Key Management Service](#) chiavi () archiviate in AWS KMS AWS KMS
- [Utilizzo della crittografia lato client](#)

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, Active Directory e replica di disaster recovery (DR).



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](#)
- [Creazione di backup di volumi EBS con AMI e snapshot EBS](#)
- [Ripristino di un volume Amazon EBS o di un'istanza EC2](#)

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. Instance-store-backed Le 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.

Note

Nella maggior parte dei casi, le AMI per Windows, Red Hat, SUSE e SQL Server richiedono la presenza delle informazioni di licenza corrette sull'AMI. Per ulteriori informazioni, consulta [Comprendere le informazioni di fatturazione AMI](#). Quando si crea un'AMI da uno snapshot, l'operazione `RegisterImage` ricava le informazioni di fatturazione corrette dai metadati dello snapshot, ma ciò richiede la presenza dei metadati appropriati. Per verificare se sono state applicate le informazioni di fatturazione corrette, controlla il campo `Dettagli della piattaforma` sulla nuova AMI. Se il campo è vuoto o non corrisponde al codice del sistema operativo previsto (ad esempio, Windows, Red Hat, SUSE o SQL), la creazione dell'AMI non è riuscita e dovresti scattare l'AMI e seguire le istruzioni in [Creare un'AMI da un'istanza](#).

È possibile 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 AWS Marketplace 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 AWS Marketplace 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](#). 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 per cento. 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 backup point-in-time 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 EBS](#) 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 EBS.](#)

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 i dati dal volume Instance Store al volume EBS su base periodica. [Per ulteriori informazioni, consulta il Knowledge Center.AWS](#)

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>CreateSnapshotoperazione 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 AWS Config tenere costantemente traccia delle modifiche alla configurazione tra le tue risorse, verifica se tali modifiche violano alcune delle condizioni delle tue 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'istananea o un AMI

Prima di scattare un'istananea 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'istananea 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. Una procedura ottimale consiste nell'avere il sistema in uno stato in cui non esegue alcuna I/O operazione. Idealmente, la macchina non accetta traffico e si trova in uno stato di arresto, ma ciò è raro in quanto le operazioni 24/7 IT 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'istananea, l'istananea 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 di 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. VSS-aware 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 univoche 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'istanza prima di aggiornare o applicare patch al software dell'applicazione o del sistema sull'istanza.

È possibile creare un'istanza 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 istanza. Puoi cercare i volumi collegati a un'istanza specifica inserendo l'ID dell'istanza nella casella del filtro.

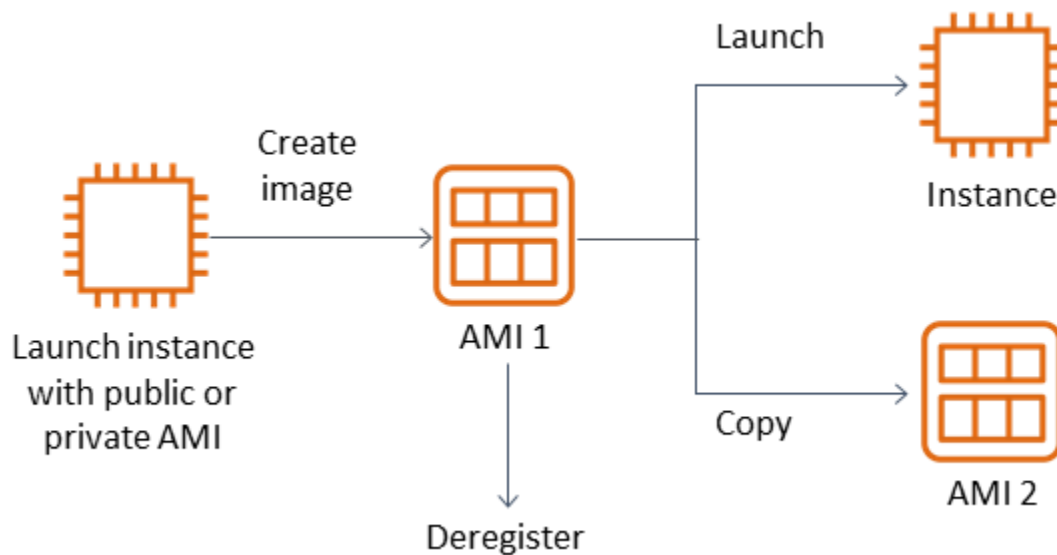
Inserisci una descrizione e aggiungi i tag appropriati. Aggiungi un Name tag per facilitare la ricerca del volume in un secondo momento. Aggiungi qualsiasi altro tag appropriato in base alla tua strategia di tagging.

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 tramite AWS 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 [CreateSnapshots](#) API o accedi alla console Amazon EC2 e scegli Elastic Block Store, Snapshots, Create Snapshot.

[Snapshots](#) > Create Snapshot

Create Snapshot

Select resource type ☐ Volume ☒ Instance

Instance ID*  

Description 

Exclude root volume ☐

Volume ID	Volume Type	Encryption
vol-1111111	Root	Encrypted
vol-2222222	EBS	Not Encrypted
vol-3333333	EBS	Not Encrypted
vol-4444444	EBS	Not Encrypted

Copy tags from volume ☒

Key	Value
(127 characters maximum)	(255 characters maximum)

This resource currently has no tags

Choose the Add tag button or [click to add a Name tag](#)

50 remaining (Up to 50 tags maximum)

* Required

Le istantanee delle istanze che hanno più volumi collegati in una configurazione RAID vengono prese collettivamente come istantanee multivolume. Multi-volume le istantanee forniscono istantanee point-in-time, coordinate dai dati e 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 relativa ad 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 [AWS Marketplace](#)

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 AWS account, puoi designare un account separato come account di archiviazione in cui tutti gli altri account possono copiare i backup. Ad esempio, è possibile eseguire questa operazione con un backup in più account. [AWS Backup](#)

Il piano di disaster recovery potrebbe inoltre richiedere la possibilità di riprodurre istanze EC2 in un'altra istanza 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 EBS 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 fase di fine del ciclo di vita 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 e AWS SDK

L'approccio di backup potrebbe richiedere operazioni prima e dopo la creazione di un'istananea 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 [AWS- CreateSnapshot e AWS- CreateImage](#) runbook per creare istantanee e AMI oppure puoi concedere ad altri utenti le autorizzazioni per utilizzarli. Systems Manager include anche i [AWS- UpdateLinuxAmi e AWS- UpdateWindowsAmi](#) runbook per automatizzare l'applicazione di patch e la creazione di AMI.

È inoltre possibile utilizzare AWS CLI and [AWS Tools for Windows PowerShell](#) per automatizzare il processo di creazione di istantanee e AMI. Puoi utilizzare il AWS CLI comando [aws ec2 create-snapshot](#) per creare un'istanza 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 esatta in un determinato momento del volume originale utilizzato per creare l'istanza. Per ripristinare singoli file o cartelle, devi fare quanto segue:

1. [Innanzitutto, ripristina il volume dall'istanza 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 istanza e collegandolo all'istanza. Puoi utilizzare la console, le operazioni dell' AWS CLI API o dell'API per creare un volume da un'istanza 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 precedente backup point-in-time 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.

Note

Nella maggior parte dei casi, le AMI per Windows, Red Hat, SUSE e SQL Server richiedono la presenza delle informazioni di licenza corrette sull'AMI. Per ulteriori informazioni, consulta [Comprendere le informazioni di fatturazione AMI](#). Quando si crea un'AMI da uno snapshot, l'operazione RegisterImage ricava le informazioni di fatturazione corrette dai metadati dello snapshot, ma ciò richiede la presenza dei metadati appropriati. Per verificare se sono state applicate le informazioni di fatturazione corrette, controlla il campo Dettagli della piattaforma sulla nuova AMI. Se il campo è vuoto o non corrisponde al codice del sistema operativo previsto (ad esempio, Windows, Red Hat, SUSE o SQL), la creazione dell'AMI non è riuscita e dovresti scartare l'AMI e seguire le istruzioni in Creare [un'AMI da un'istanza](#).

Se devi utilizzare uno snapshot EBS per ripristinare un'istanza, crea prima un'AMI da un'istanza 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.
5. (Solo Windows, Red Hat, SUSE e SQL Server) Per verificare se sono state applicate le informazioni di fatturazione corrette, controlla il campo Dettagli della piattaforma sulla nuova AMI. Se il campo è vuoto o non corrisponde al codice del sistema operativo previsto (ad esempio, Windows o Red Hat), la creazione dell'AMI non è riuscita e dovresti scartare l'AMI e seguire le istruzioni in [Creare un'AMI da un'istanza](#).

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. Quindi sostituisci 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, è possibile che si verifichino 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 a AWS

È possibile utilizzarli AWS per l'archiviazione duratura e fuori sede dei backup dell'infrastruttura locale. Utilizzando i servizi AWS di storage in questo scenario, è possibile concentrarsi sulle attività di backup e archiviazione. Non è necessario preoccuparsi del provisioning, della scalabilità o della capacità dell'infrastruttura di storage per le attività di backup.

Amazon S3 offre ampie operazioni API e SDK per l'integrazione nei tuoi approcci di backup e ripristino nuovi ed esistenti. Ciò offre inoltre ai fornitori di software di backup la possibilità di integrare direttamente le proprie applicazioni con le soluzioni di storage. AWS

In questo scenario, il software di backup e archiviazione utilizzato nell'infrastruttura locale si interfaccia direttamente con AWS le operazioni API. Poiché il software di backup è AWS-aware, esegue il backup dei dati dai server locali direttamente su Amazon S3.

Se il software di backup esistente non supporta nativamente il AWS Cloud, puoi utilizzare Storage Gateway. Storage Gateway è un servizio di cloud storage che offre ai sistemi locali l'accesso 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. Puoi utilizzare Storage Gateway come parte di un approccio di backup e ripristino per i carichi di lavoro di storage basati su blocchi locali.

Storage Gateway è utile negli 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. Lo Storage Gateway viene distribuito come macchina virtuale o appliance hardware dedicata. Questa guida si concentra su come lo 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 SMB-based o NFS-based accedendo.
- Un gateway di volumi per presentare volumi di storage a blocchi iSCSI basati sul cloud alle applicazioni locali. Un gateway di volumi fornisce una cache locale o volumi completi in locale, archiviando al contempo copie complete dei volumi nel cloud. AWS
- Un gateway a nastro per indirizzare un software di backup affidabile verso un gateway di storage locale che, a sua volta, si connette ad Amazon S3. Questa opzione offre la scalabilità e la durabilità del cloud per una conservazione sicura e a lungo termine senza interrompere gli investimenti o i processi esistenti.

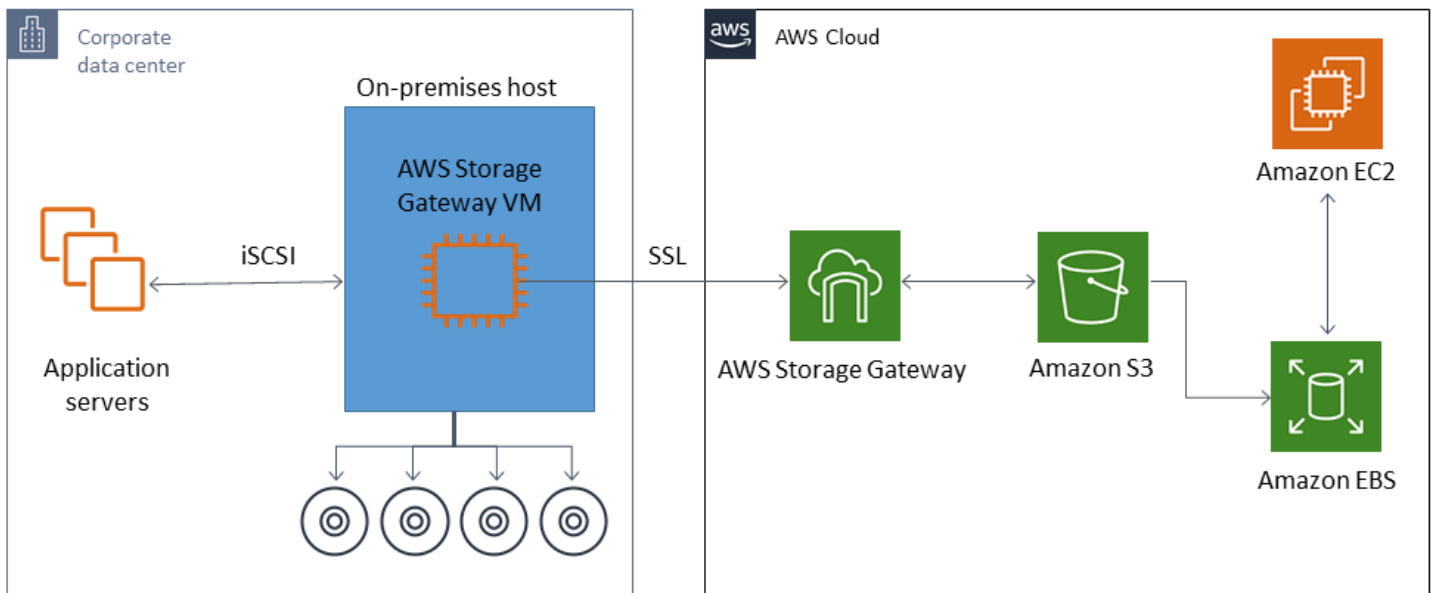
Gateway di file

Molte organizzazioni iniziano il loro percorso verso il cloud spostando dati secondari e terziari, come i backup, nel cloud. Il supporto delle interfacce SMB e NFS di un gateway di file offre ai gruppi IT un modo per trasferire i lavori 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 gateway di file 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. Long-term le esigenze di conservazione vengono soddisfatte suddividendo i backup su più livelli nelle classi di storage S3 Access e Standard-Infrequent Amazon Glacier a basso costo.

Il gateway di file fornisce una rampa di accesso per lo storage basato su blocchi su Amazon S3 per backup offsite altamente durevoli. È particolarmente utile negli scenari in cui un file di cui è stato eseguito il backup recente 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, puoi ripristinare le versioni precedenti degli oggetti di un file e quindi accedervi facilmente utilizzando SMB o NFS.

Gateway di volumi

Un volume gateway 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 volume gateway facilita l'acquisizione di istantanee point-in-time complete dei volumi e l'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 DR basata sul cloud. I volumi possono anche essere ripristinati su Storage Gateway, consentendo alle applicazioni locali di tornare allo stato precedente.



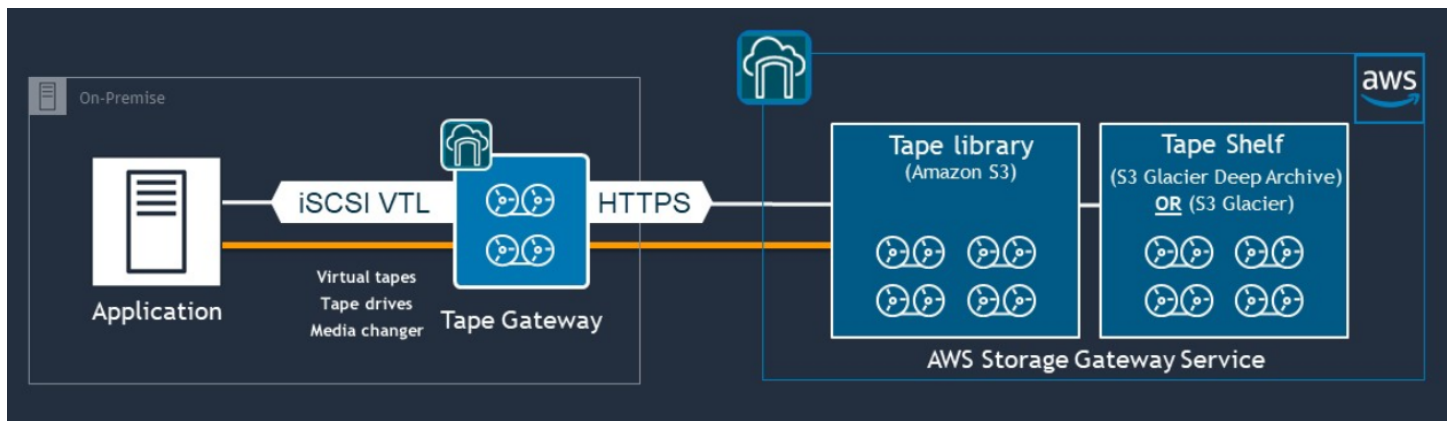
Poiché un gateway di volume si integra con la funzionalità di volume Amazon EBS di Amazon EC2, puoi AWS Backup utilizzarlo per automatizzare e pianificare il processo di snapshot. Un volume gateway offre i vantaggi aggiuntivi di snapshot e funzionalità di tagging di Amazon EBS durevoli e supportati da Amazon S3. Per ulteriori informazioni, consulta la documentazione relativa agli [snapshot di Amazon EBS](#).

Gateway di nastri virtuali

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

AWS esegue inoltre controlli di fissità su base regolare per confermare che i dati possano essere letti e che non siano stati introdotti errori. Tutti i nastri archiviati in Amazon S3 sono protetti da crittografia lato server utilizzando chiavi predefinite o le tue chiavi. AWS KMS Inoltre, si evitano i rischi di sicurezza fisica associati alla portabilità dei nastri. Con un gateway a nastro, si ottengono dati corretti, rispetto allo stoccaggio dei nastri fuori sede, in cui è possibile ricevere un nastro errato o rotto durante il ripristino.

Puoi risparmiare sui costi di storage mensili archiviando i dati in Amazon S3. Puoi risparmiare ancora di più per le tue esigenze 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 come uno standard aperto i SCSI-based VTL, con un lettore di supporti virtuali e unità a 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 a scalabilità elevata. Quando non è più necessario l'accesso immediato o frequente ai dati su un nastro virtuale, l'applicazione di backup può archivarli 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 i tape per accedere ai nastri virtuali. SCSI-based Considerate anche la dimensione di storage minima di 100 GB per nastro. Per ulteriori informazioni, consulta l'elenco delle [applicazioni di backup di terze parti](#) che supportano i gateway a nastro.

Backup e ripristino delle applicazioni dal AWS data center

Potresti avere una policy che richieda l'implementazione di uno scenario come il DR o la continuità aziendale per i carichi di lavoro basati sul cloud e l'infrastruttura locale. Se disponi già di un framework di backup dei dati per i tuoi server locali, puoi estenderlo alle tue AWS risorse tramite una connessione VPN o tramite AWS Direct Connect. Puoi installare l'agente di backup sulle EC2 istanze ed eseguire il backup dei dati e delle applicazioni in base alle tue politiche di protezione dei dati. Puoi anche utilizzare Amazon S3 come servizio intermedio per archiviare i backup a livello di applicazione. Puoi quindi utilizzare le operazioni API o ripristinare i SDKs dati nel tuo AWS CLI ambiente locale.

Per eseguire il backup dei dati in AWS servizi diversi da Amazon EC2 AWS CLI, utilizza le operazioni SDKs, e API per estrarre i dati nel formato desiderato. Quindi copia i dati su Amazon S3 e copiali da Amazon S3 al tuo ambiente locale. Alcuni servizi forniscono l'esportazione diretta in Amazon S3. Ad esempio, Amazon RDS supporta il [backup nativo](#) dei database Microsoft SQL Server su Amazon S3.

Backup e ripristino di servizi nativi del cloud AWS

Il tuo approccio al backup e al ripristino dovrebbe riguardare i AWS servizi utilizzati nei tuoi carichi di lavoro. AWS offre funzionalità e opzioni specifiche del servizio per la gestione e l'interazione con i dati. È possibile utilizzare la console AWS CLI SDKs, le operazioni e le API per implementare il backup e il ripristino per i AWS servizi in uso. Questa guida illustra [Amazon RDS e Amazon DynamoDB](#) a titolo di esempio. AWS Backup supporta sia DynamoDB che Amazon RDS e dovrebbe essere usato 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 del volume di storage dell'istanza di database, eseguendo il backup dell'intera istanza DB, non solo dei singoli database. Utilizzando Amazon RDS, puoi stabilire una finestra di backup per 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 il point-in-time 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 dei dati durante una finestra di backup definita al momento della creazione dell'istanza DB. Puoi configurare un periodo di conservazione fino a 35 giorni per il backup automatico. Amazon RDS carica inoltre i log delle transazioni per le istanze DB su Amazon S3 ogni 5 minuti. Amazon RDS utilizza i backup giornalieri insieme ai log delle transazioni del database per ripristinare l'istanza DB. Puoi ripristinare l'istanza in qualsiasi momento durante il periodo di conservazione, fino a `LatestRestorableTime` (in genere, gli ultimi cinque minuti).

Per conoscere l'orario di ripristino più recente per le tue istanze DB, utilizza la chiamata `DescribeDBInstances` API. Oppure consulta la scheda Descrizione per il database sulla console Amazon RDS.

Quando avvii un PITR, i log delle transazioni vengono combinati con il backup giornaliero più appropriato per ripristinare l'istanza DB all'ora richiesta.

- Le istantanee DB sono backup avviati dall'utente che è possibile utilizzare per ripristinare l'istanza DB in uno stato noto con la frequenza desiderata. È quindi possibile ripristinare tale stato in

qualsiasi momento. Puoi utilizzare la console Amazon RDS o la chiamata `CreateDBSnapshot` API per creare snapshot DB. Queste istantanee vengono conservate fino a quando non utilizzi la console o la chiamata `DeleteDBSnapshot` API per eliminarle esplicitamente.

Entrambe queste opzioni di backup sono supportate per Amazon RDS in AWS Backup, che fornisce anche altre funzionalità. Prendi in considerazione l'idea di AWS Backup impostare un piano di backup standard per i tuoi database Amazon RDS e utilizza le opzioni di backup delle istanze avviate dall'utente quando i tuoi 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 di backup e ripristino native utilizzando le utilità client. Ad esempio, puoi utilizzare il comando [mysqldump con un database Amazon RDS MySQL per esportare un database](#) sul tuo computer client locale. In alcuni casi, Amazon RDS offre anche opzioni aumentate per eseguire un backup e un ripristino nativi di un database. Ad esempio, Amazon RDS fornisce procedure memorizzate per [esportare e importare backup di database RDS di database SQL Server](#).

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

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

Quando si ripristina un database utilizzando PITR o uno snapshot di un'istanza DB RDS, viene creata una nuova istanza DB con un nuovo endpoint. In questo modo, è possibile creare più istanze DB da uno specifico snapshot o point-in-time del database. Quando si ripristina un'istanza DB RDS per sostituire un'istanza DB RDS attiva, sono necessarie considerazioni particolari. Ad esempio, è necessario determinare come reindirizzare i client di 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 l'ora di ripristino dei dati e il tempo di ripristino quando la nuova istanza inizia a ricevere le scritture.

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

Imposta il Time to Live (TTL) per il tuo record CNAME su un valore appropriato. 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 per un periodo più lungo del TTL. Per Amazon Route 53, se si specifica un valore più lungo (ad esempio 172800 secondi o due giorni), si riduce il numero di chiamate che i resolver ricorsivi DNS devono effettuare a Route 53 per ottenere le informazioni più recenti in questo record. Ciò riduce la latenza e riduce la bolletta per il servizio Route 53. Per ulteriori informazioni, consulta [Come Amazon Route 53 indirizza il traffico per il tuo dominio](#).

Le applicazioni e i sistemi operativi client potrebbero inoltre memorizzare nella cache le informazioni DNS che devi cancellare 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 sull'istanza ripristinata, verifica che tutti i 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 sull'istanza ripristinata e quindi la correzione di eventuali dati che potrebbero essere ancora scritti sull'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 ad alcuni client di database che è possibile gestire singolarmente. Per ridurre l'impatto sul client, è possibile eseguire il ripristino del database durante una finestra di manutenzione.

Scrivete le vostre applicazioni in modo da gestire senza problemi gli errori di connessione al database, riprovando utilizzando il backoff esponenziale. Ciò consente all'applicazione di eseguire il ripristino quando una connessione al database diventa non disponibile durante un ripristino senza causare un arresto anomalo imprevisto dell'applicazione.

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

Backup e ripristino per DynamoDB

DynamoDB fornisce PITR, che esegue backup quasi continui dei dati delle 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 DynamoDB, o l'API DynamoDB. AWS CLI Per ulteriori informazioni, consulta [Backup di una tabella DynamoDB](#). È possibile pianificare backup periodici o futuri utilizzando AWS Backup, oppure personalizzare e automatizzare l'approccio di backup utilizzando le funzioni Lambda. Per ulteriori informazioni sull'utilizzo delle funzioni Lambda per il backup di DynamoDB, consulta il post del blog [Una soluzione serverless per pianificare il backup on-demand di Amazon](#) DynamoDB. Se non desideri creare script di pianificazione e processi di pulizia, puoi utilizzarli per creare piani di backup. AWS Backup I piani di backup includono pianificazioni e politiche di conservazione per le tabelle DynamoDB. AWS Backup crea i backup ed elimina i backup precedenti in base alla pianificazione di conservazione. AWS Backup include 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 più regioni. Per ulteriori informazioni, consulta [Backup DynamoDB avanzato](#).

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

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

È possibile ripristinare solo i dati dell'intera tabella in una nuova tabella da un backup. È possibile scrivere sulla tabella ripristinata solo dopo che è diventata attiva.

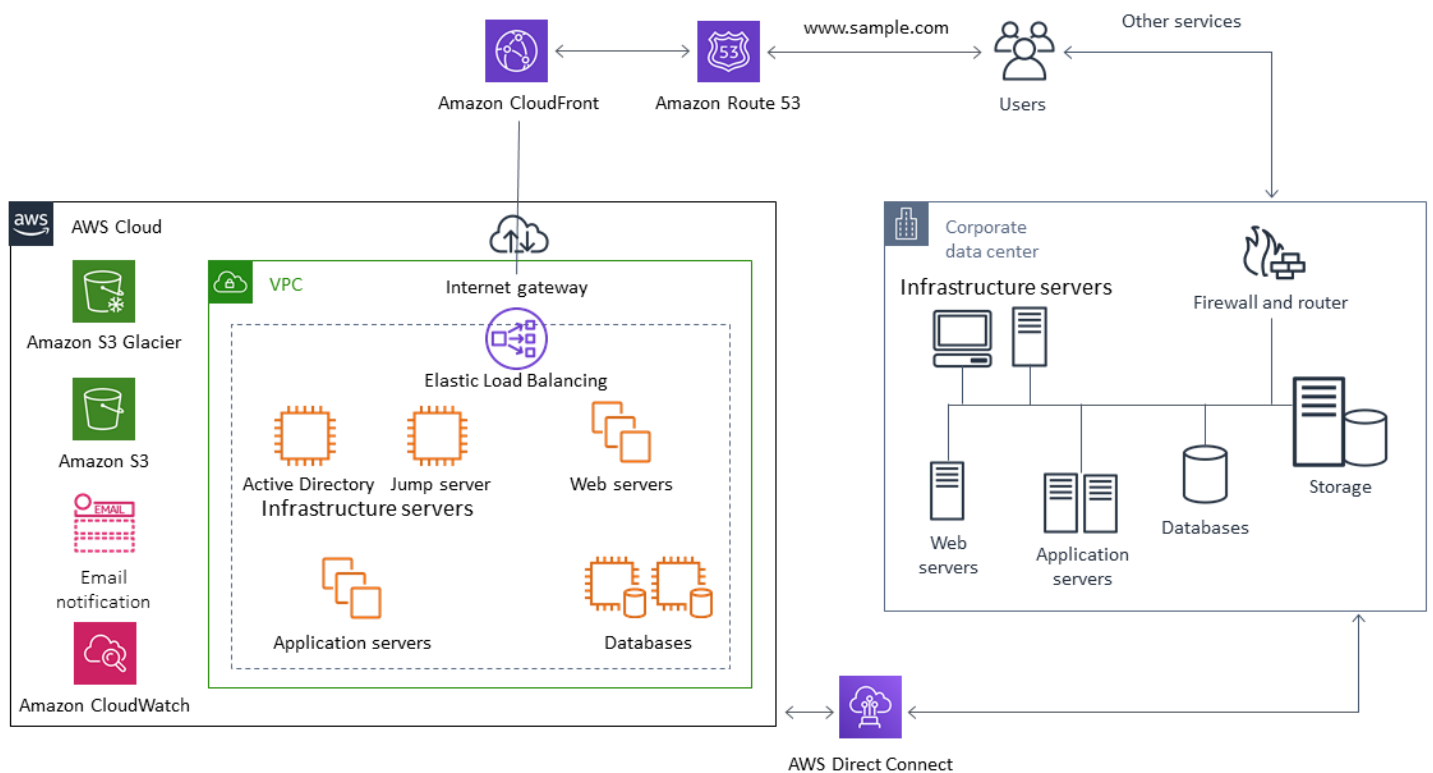
Il processo di ripristino deve considerare in che modo i client verranno indirizzati a utilizzare il nome della tabella appena ripristinata. È possibile configurare le applicazioni e i client per recuperare il nome della tabella DynamoDB da un file di configurazione AWS Systems Manager, dal valore Parameter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

Come parte del processo di ripristino, è necessario considerare attentamente il processo di passaggio al digitale. 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 riconciliare le differenze tra la tabella DynamoDB esistente e la tabella DynamoDB appena ripristinata.

Backup e ripristino per architetture ibride

Le implementazioni native per il cloud e locali discusse in questa guida possono essere combinate in scenari ibridi in cui l'ambiente del carico di lavoro include componenti locali e infrastrutturali. AWS Le risorse, inclusi server Web, server delle applicazioni, server di monitoraggio, database e Microsoft Active Directory, sono ospitate nel data center del cliente o su AWS. Le applicazioni in esecuzione nel AWS cloud sono connesse alle applicazioni eseguite in locale.

Questo sta diventando uno scenario comune per i carichi di lavoro aziendali. Molte aziende dispongono di centri dati propri e li utilizzano AWS per aumentare la capacità. Questi data center per i clienti sono spesso collegati alla AWS rete tramite collegamenti di rete ad alta capacità. Ad esempio, con [Direct Connect](#), puoi stabilire una connettività privata e dedicata dal tuo data center locale a. AWS Ciò fornisce la larghezza di banda e una latenza costante per caricare i dati sul cloud ai fini della protezione dei dati. Fornisce inoltre prestazioni e latenza costanti per carichi di lavoro ibridi. Il diagramma seguente fornisce un esempio di approccio all'ambiente ibrido.



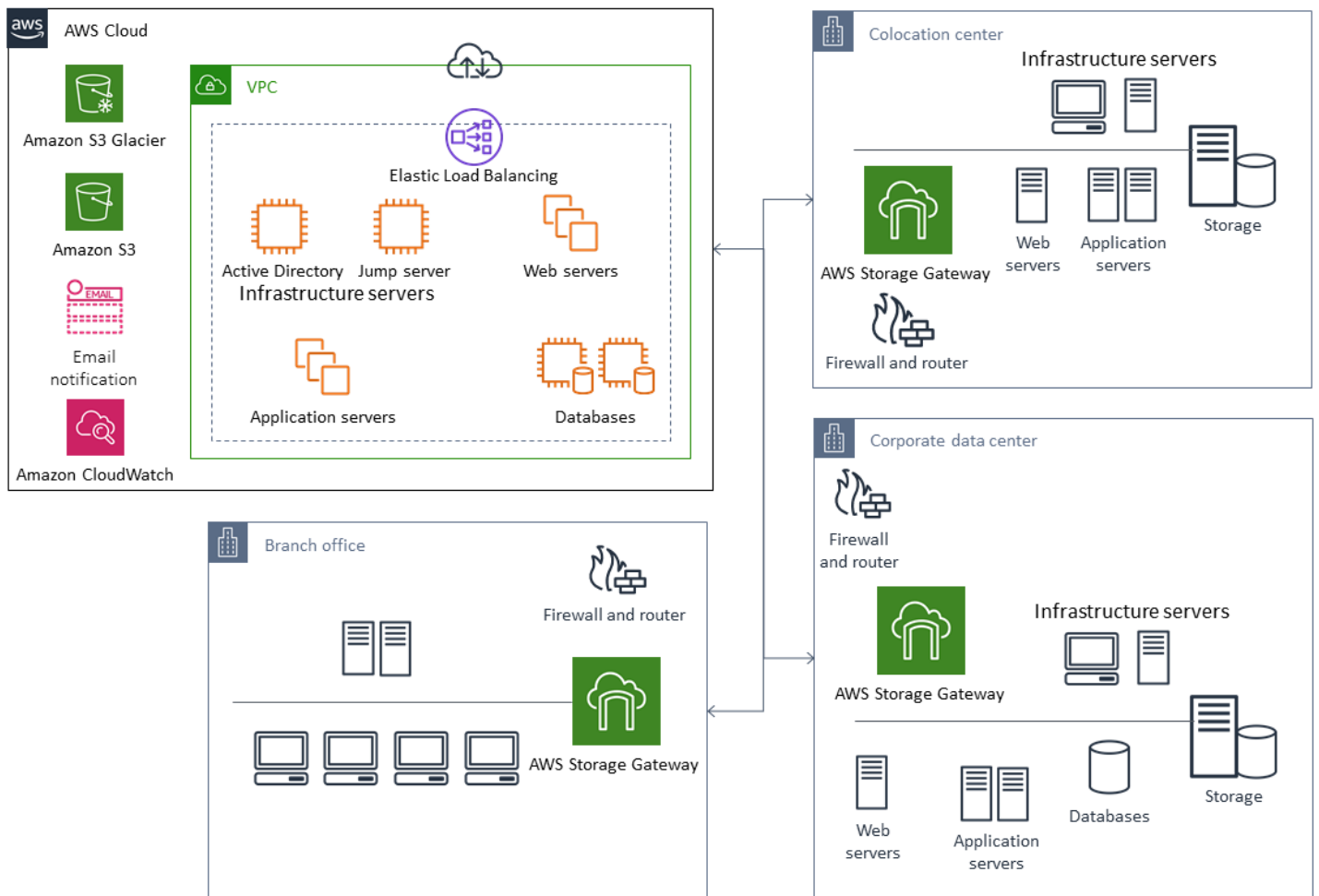
Well-designed Le soluzioni di protezione dei dati utilizzano in genere una combinazione delle opzioni descritte nelle soluzioni native per il cloud e locali di questa guida. Molti ISV forniscono soluzioni di backup e ripristino leader di mercato per l'infrastruttura locale e hanno ampliato le proprie soluzioni per supportare approcci ibridi.

Spostamento delle soluzioni centralizzate di gestione dei backup sul cloud per una maggiore disponibilità

Utilizzando gli investimenti esistenti nelle soluzioni di gestione del backup con AWS, è possibile migliorare la resilienza e l'architettura del proprio approccio. È possibile disporre di un server di backup principale e di uno o più server multimediali o di archiviazione ubicati in sede in più sedi vicine ai server e ai servizi che proteggono. In questo caso, valuta la possibilità di 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, puoi creare uno o più server multimediali su istanze EC2 nella stessa regione dei server che proteggeranno. I server multimediali vicini alle istanze EC2 ti consentono di risparmiare denaro sui trasferimenti via Internet. Quando esegui il backup su Amazon S3, i server multimediali aumentano le prestazioni complessive di backup e ripristino.

Puoi anche utilizzare Storage Gateway per fornire un accesso cloud centralizzato ai dati provenienti da data center e uffici geograficamente distribuiti. Ad esempio, un gateway di file offre un accesso su richiesta e a bassa latenza ai dati archiviati per i flussi di lavoro delle applicazioni che possono estendersi in tutto AWS il mondo. Puoi utilizzare funzionalità come l'aggiornamento della cache per aggiornare i dati in posizioni geograficamente distribuite in modo che i contenuti possano essere facilmente condivisi tra i tuoi uffici.



Disaster recovery con AWS

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 utilizzano il AWS cloud per il backup e il ripristino e come sito di disaster recovery. AWS fornisce una serie di servizi e funzionalità che supportano il DR e la continuità aziendale.

Argomenti

- [On-premises DR a AWS](#)
- [DR per carichi di lavoro nativi del cloud](#)

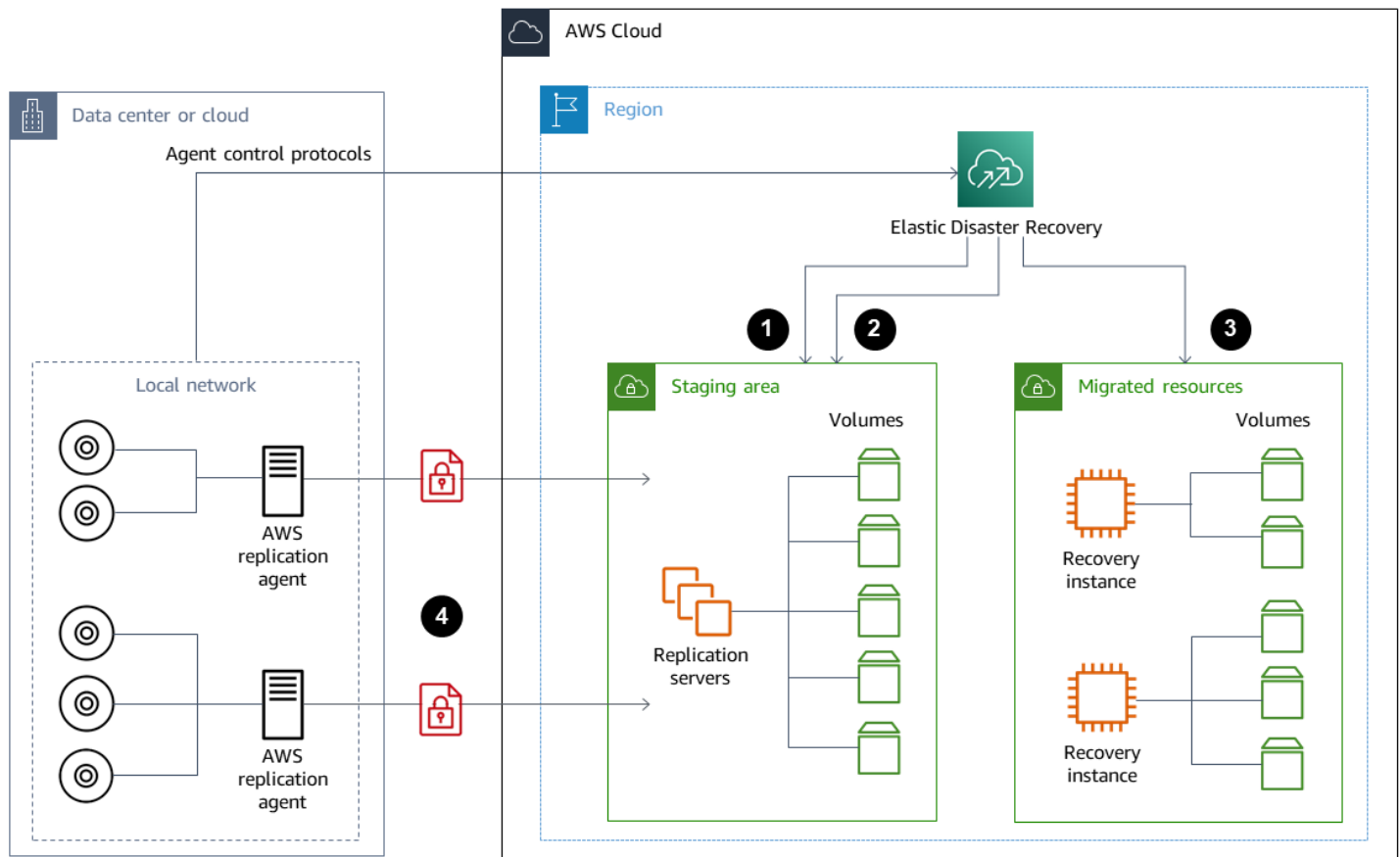
On-premises DR a AWS

L'utilizzo AWS come ambiente di disaster recovery (DR) offsite per carichi di lavoro locali è uno scenario ibrido comune. Definisci i tuoi obiettivi di disaster recovery, inclusi i tempi di ripristino e gli obiettivi dei punti di ripristino richiesti, prima di selezionare le tecnologie da utilizzare. Per facilitare questa definizione, puoi utilizzare la [checklist del piano DR](#).

Sono disponibili diverse opzioni per aiutarti a configurare e fornire rapidamente un ambiente DR. AWS Assicurati di tenere conto di tutte le dipendenze del carico di lavoro e testa il piano e la soluzione di DR in modo accurato e regolare per verificarne l'integrità.

AWS consente [AWS Elastic Disaster Recovery](#) di creare una replica completa dei server locali, inclusi il volume root e il sistema operativo, su. AWS Elastic Disaster Recovery replica continuamente le tue macchine in un'area di staging a basso costo nell'account AWS di destinazione e preferito. Regione AWS La replica a livello di blocco è una replica esatta dello storage dei server, inclusi 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 di completo provisioning in pochi minuti.

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



1. Segnalazione dello stato del server di replica
2. Le risorse dell'area di staging vengono create e terminate automaticamente
3. Istanze di ripristino avviate con RTO in minuti e RPO in secondi
4. Replica continua a livello di blocco (compressa e crittografata)

È importante testare il processo di disaster recovery 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 disaster recovery locale, di staging e avviato. Verifica inoltre che tutti i processi di tipo worker che potrebbero eseguire il polling e recuperare il 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 da eseguire prima che le istanze del server di ripristino siano online. Includi anche i passaggi da eseguire dopo che le istanze del server di ripristino sono online e disponibili. È possibile utilizzare soluzioni come la [soluzione AWS Elastic Disaster Recovery Plan Automation](#) o un altro approccio per automatizzare i piani di disaster recovery.

È possibile utilizzare un [gateway di volume Storage Gateway](#) per fornire ai server locali volumi basati sul cloud. È inoltre possibile effettuare rapidamente il provisioning di questi volumi per l'uso con Amazon EC2 utilizzando le istantanee di Amazon EBS. In particolare, gli Stored Volume Gateway forniscono alle applicazioni locali un accesso a bassa latenza a interi set di dati. I Volume Gateway forniscono anche backup durevoli basati su snapshot che possono essere ripristinati per l'uso in locale o per l'uso con Amazon EC2. Puoi pianificare istantanee point-in-time in base al Recovery Point Objective (RPO) per il tuo 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 un'Amazon Machine Image (AMI) di Amazon EC2 con una configurazione che corrisponde ai tuoi server locali e specifica i volumi di dati separatamente. Dopo aver configurato e testato l'AMI, esegui il provisioning delle istanze EC2 dall'AMI insieme ai volumi di dati basati sulle istantanee del gateway del volume. Questo approccio richiede un test approfondito dell'ambiente per verificare che l'istanza EC2 funzioni correttamente, in particolare per i carichi di lavoro Windows.

DR per carichi di lavoro nativi del cloud

Valuta in che modo i tuoi carichi di lavoro nativi del cloud si allineano ai tuoi obiettivi di disaster recovery. AWS offre diverse zone di disponibilità in regioni di tutto il mondo. Molte aziende che utilizzano il AWS cloud allineano le proprie architetture di carico di lavoro e gli obiettivi di DR per far fronte alla perdita di una zona di disponibilità. L'[Reliability Pillar](#) del AWS Well-Architected Framework supporta questa best practice. È possibile progettare i carichi di lavoro e le relative dipendenze tra servizi e applicazioni in modo da utilizzare più zone di disponibilità. È quindi possibile automatizzare il DR e raggiungere gli obiettivi di DR con un intervento minimo o nullo.

In pratica, tuttavia, potreste scoprire di non essere in grado di stabilire un'architettura ridondante, attiva e automatizzata per tutti i componenti. Esamina ogni livello della tua architettura per determinare i processi di DR necessari per raggiungere i tuoi obiettivi. Ciò può variare da carico di lavoro a carico di lavoro, con requisiti di architettura e servizio diversi. Questa guida illustra considerazioni e opzioni per Amazon EC2. Per altri AWS servizi, puoi fare riferimento alla [AWS documentazione](#) per determinare l'alta disponibilità e le opzioni di DR.

DR per Amazon EC2 in un'unica zona di disponibilità

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

Se la tua architettura ha istanze EC2 che non possono essere bilanciate dal carico e possono avere una sola 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 possa essere usato 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 e fornire il servizio automaticamente. 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 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 dell'istanza attiva e utilizzi l'AMI per effettuare 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 l'istanza interrotta precedente. 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.

Testa a fondo la tua soluzione simulando il guasto da cui la soluzione è stata progettata per proteggerti. Considera anche gli aggiornamenti necessari alla tua soluzione DR man mano che l'architettura del carico di lavoro cambia.

DR per Amazon EC2 in un guasto regionale

I clienti con requisiti di disponibilità molto elevati (ad esempio, applicazioni mission-critical che non possono tollerare alcun downtime) possono utilizzare AWS in più regioni per fornire ulteriore resilienza contro i problemi a livello di regione. 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. AWS fornisce 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.

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

[AWS Elastic Disaster Recovery](#) può essere utilizzato per automatizzare e replicare continuamente i server Amazon EC2 in una regione in una regione DR alternativa. Elastic Disaster Recovery può semplificare il tuo approccio al 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 pochi minuti e l'RPO nell'intervallo inferiore al secondo.

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

Pulizia dei backup

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

Una strategia di tagging è un prerequisito per una strategia di pulizia. Utilizza i tag per identificare le risorse da pulire, informare i proprietari in modo appropriato e automatizzare il processo di pulizia. Ai backup creati da AWS sono associate le date di creazione, 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 delle istantanee utilizzando l'automazione. Ad esempio, è possibile eseguire la scansione dell'account alla ricerca di istantanee e determinare se i volumi corrispondenti si trovano in uno stato allegato o disponibile. È possibile filtrare ulteriormente i risultati in base a una soglia temporale specificata dall'utente. Utilizzando i tag allegati al volume, è possibile inviare automaticamente messaggi di posta elettronica ai proprietari delle istantanee e avvisarli che è stata pianificata l'eliminazione delle relative istantanee. Questa riparazione automatica può essere implementata utilizzando AWS Config regole, uno script che utilizza o una funzione Lambda utilizzando l' AWS SDK. AWS CLI

Systems Manager fornisce [AWS-Delete EBSVolume Snapshot](#) e [AWS- DeleteSnapshot](#) documenti per aiutarti ad avviare e automatizzare la pulizia degli snapshot di Amazon EBS. Puoi anche utilizzare l' AWS SDK AWS CLI and per automatizzare la pulizia di altre AWS risorse come gli snapshot di Amazon RDS.

Domande frequenti su backup e ripristino

Quale pianificazione di backup devo selezionare?

Definisci una frequenza di pianificazione del backup in linea con il tuo Recovery Point Objective (RPO). Definisci un periodo di backup quando il carico di lavoro è al di sotto della quantità di carico minima e quando è possibile ridurre l'impatto sull'utente. Crea un'istantanea point-in-time ogni volta che intendi apportare una modifica significativa al tuo carico di lavoro.

Devo creare backup nei miei account di sviluppo?

Verifica le modifiche potenzialmente irreversibili negli account di sviluppo per i tuoi carichi di lavoro e crea backup prima di eseguire modifiche sostanziali. Potresti avere molti più backup di point-in-time ripristino (PITR) nei tuoi account di sviluppo e non di produzione derivanti dalle 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; la point-in-time snapshot viene creata immediatamente, ma lo stato della snapshot 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](#).

Passaggi successivi

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

Testa il processo di ripristino per un singolo componente dell'architettura oltre a tutti i componenti dell'architettura. Convalida il tempo di ripristino per ciascuno di essi. Convalida anche l'impatto del processo di backup e ripristino sulle dipendenze a monte e a valle. Verifica l'impatto di qualsiasi interruzione del servizio sulle dipendenze a monte e conferma l'impatto a valle sui backup.

Risorse aggiuntive

AWS resources

- [AWS Guida prescrittiva](#)
- [AWS documentazione](#)
- [AWS riferimento generale](#)
- [AWS glossario](#)

AWS servizi

- [AWS Backup](#)
- [Amazon CloudWatch](#)
- [AWS Config](#)
- [Amazon DynamoDB](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [Amazon EventBridge](#)
- [IAM](#)
- [Amazon RDS](#)
- [Amazon S3](#)
- [Storage Gateway](#)
- [AWS Systems Manager](#)

Altre risorse

- [Backup e ripristino con AWS Backup](#) (soluzione)
- [Disaster recovery dei carichi di lavoro su AWS: ripristino nel cloud](#) (white paper)
- [Serie Disaster Recovery](#) (post del blog sull'architettura)AWS
- [Elenco di controllo del piano di disaster recovery IT](#)
- [Utilizzo di approcci di backup e ripristino AWS](#) (paper tecnico — archiviato)
- [Guida introduttiva con AWS Backup](#)

Cronologia dei documenti

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

Modifica	Descrizione	Data
Informazioni aggiornate	Linee guida aggiornate nella sezione Amazon S3 .	28 giugno 2024
Informazioni aggiornate	Informazioni aggiornate nella AWS sezione On-premises DR to .	13 aprile 2023
È stata aggiunta una sezione	Sono state aggiunte linee guida e passaggi per la creazione o il ripristino di un'istanza da un'istantanea .	7 marzo 2023
Sono state aggiunte informazioni su Elastic Disaster Recovery e ulteriori chiarimenti	Nelle sezioni Disaster recovery with AWS e AWS Choosing services for data protection , sono state aggiunte informazioni su AWS Elastic Disaster Recovery. Nelle sezioni EC2 Backup e ripristino con istantanee di Amazon e AMIs , Preparazione di un volume EBS prima di creare uno snapshot o AMI e Ripristino da uno snapshot di Amazon EBS o un AMI , sono stati aggiunti ulteriori chiarimenti. Aggiunto alle domande frequenti su Backup e ripristino .	19 gennaio 2023

È stato aggiunto un collegamento	È stato aggiunto un collegamento alla documentazione di Amazon Data Lifecycle Manager nella sezione Amazon Data Lifecycle Manager .	31 ottobre 2022
Informazioni aggiornate	Sono state aggiornate le informazioni sul ripristino dei volumi .	30 agosto 2022
Informazioni aggiornate e aggiunta una nuova sezione	Nella sezione Scelta dei AWS servizi per la protezione dei dati , servizi aggiunti. È stata aggiunta la sezione Backup e ripristino utilizzando AWS Backup . Nella sezione Backup e ripristino con Amazon S3 e Amazon Glacier, sono state aggiunte informazioni sulle nuove classi di storage Amazon Glacier. Nella sezione Backup e ripristino per Amazon EC2 con volumi EBS , sono stati aggiunti collegamenti alla documentazione e informazioni aggiuntive. Nella sezione Backup e ripristino dei AWS servizi nativi del cloud , è stato aggiunto un consiglio d'uso. AWS 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 EC2 backup e ripristino di Amazon con istantanee e AMIs	9 settembre 2021
Informazioni aggiornate	Nella AWS Backup sezione, sono state aggiunte informazioni sui AWS servizi che AWS Backup supporta.	1 giugno 2021
Pubblicazione iniziale	—	29 luglio 2020

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.