Strategia di disaster recovery per database su AWS

AWS Linee guida prescrittive

AWS Linee guida prescrittive: Strategia di disaster recovery per database su AWS

Table of Contents

Strategia di disaster recovery per database su AWS

Oliver Francis, Balaji Desikachari, Jitendra Kumar e Suhas Basavaraj, Amazon Web Services

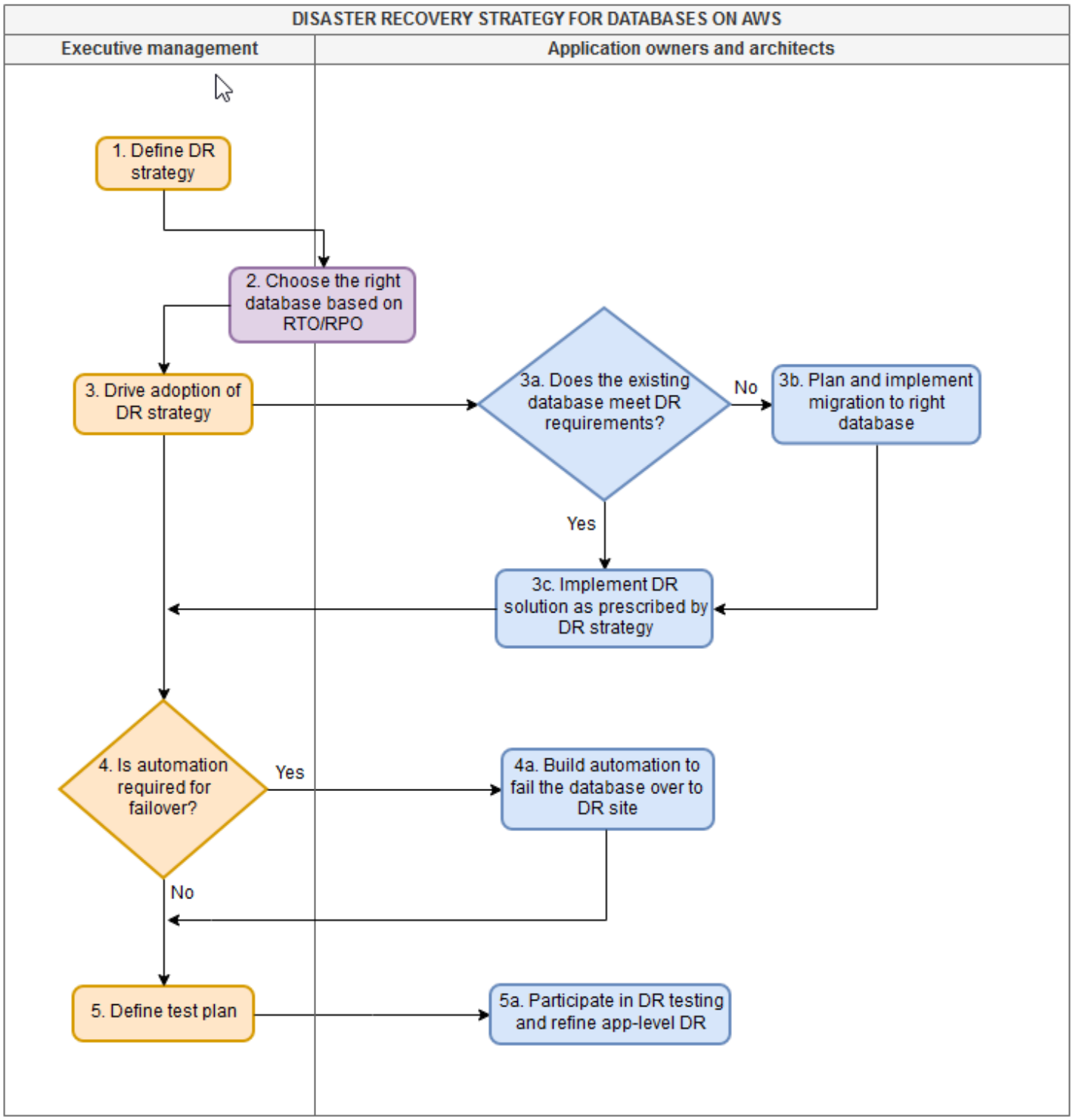
Nell'ottobre 2021, il Forbes Technology Council ha pubblicato un articolo dal titolo Why Disaster Recovery Is No Longer Optional For Today's Businesses. L' U.Sarticolo cita un. Uno studio della Federal Emergency Management Agency (FEMA) afferma che il 40% delle piccole e medie imprese negli Stati Uniti d'America fallisce dopo un disastro. Inoltre, il 25% delle imprese che riaprono chiudono di nuovo entro un anno. Data la gravità dell'argomento, è fondamentale definire un piano di continuità aziendale ben studiato che includa una strategia di ripristino di emergenza (disaster recovery, DR) per gli asset IT, al fine di garantire la crescita e il successo a lungo termine dell'azienda. Il cloud computing ha reso praticabile il ripristino di emergenza anche per le piccole e medie imprese, abbassando la barriera all'ingresso. Considerati i rischi derivanti dalla mancanza di una soluzione adeguata in caso di emergenza, un piano di continuità aziendale che includa una strategia di ripristino dovrebbe essere in cima alla lista delle priorità dei leader aziendali.

Se i tuoi carichi di lavoro sono in esecuzione AWS, indubbiamente la maggior parte dei tuoi dati risiede nei database. AWS Che si tratti di dati archiviati in un sistema di database relazionale (RDBMS) come Amazon Aurora Edition MySQL-Compatible o in un database NoSQL come Amazon DynamoDB, questi dati sono preziosi per la tua azienda. Lo sviluppo di una strategia di DR specifica per i database ti AWS aiuta a capire cosa AWS offre in termini di disaster recovery per i tuoi database e come puoi sfruttare queste informazioni nel tuo piano di DR per il. Cloud AWS

Il diagramma a corsie seguente presenta le attività di alto livello associate alla definizione e all'implementazione di una strategia di ripristino di emergenza. Le due colonne mostrano le attività del team esecutivo e le attività degli architetti e dei proprietari delle applicazioni. Il team esecutivo è responsabile del processo decisionale. Questo team definisce la strategia di ripristino di emergenza che l'organizzazione deve seguire, promuove la sua l'adozione all'interno dell'azienda, decide se adottare o meno l'automazione per raggiungere gli obiettivi del ripristino di emergenza e stabilisce il relativo piano di test.

Dopo aver implementato la strategia di ripristino di emergenza, il team esecutivo collabora con gli architetti e i proprietari delle applicazioni per scegliere i database corretti in grado di soddisfare gli obiettivi del tempo di ripristino (RTO) e gli obiettivi del punto di ripristino (RPO) derivanti dalla strategia. Mentre il team di gestione esecutivo guida l'adozione della strategia di DR, i proprietari delle applicazioni e gli architetti valutano i database utilizzati nelle loro applicazioni e migrano al database giusto se quelli esistenti non raggiungono l'RTO e l'RPO impostati per la loro applicazione.

Gli architetti e i proprietari delle applicazioni implementano inoltre l'automazione, se necessario, e partecipano ai test per perfezionare e migliorare il ripristino di emergenza a livello di applicazione.



Questo articolo è destinato ai dirigenti aziendali e ai responsabili delle decisioni che desiderano formulare una strategia di ripristino di emergenza interregionale in grado di contribuire al

raggiungimento degli obiettivi aziendali. L'articolo presuppone una certa conoscenza tecnica e una certa familiarità con la terminologia del disaster recovery, ma nessuna esperienza. AWS

Obiettivi aziendali specifici

Questa sezione illustra i risultati previsti associati alla definizione e alla creazione di un piano di ripristino di emergenza (disaster recovery, DR) per i database in AWS.

Contenimento delle perdite finanziarie

Se disponi di una soluzione di ripristino di emergenza ben progettata per i database che archiviano i dati delle applicazioni, in caso di eventi catastrofici puoi ripristinare i dati più rapidamente e con una perdita di dati minima o nulla. Ciò riduce al minimo le perdite finanziarie che possono derivare dall'indisponibilità dell'applicazione per periodi prolungati o, nel peggiore dei casi, dalla perdita permanente dei dati.

Riduzione dell'impatto sui processi aziendali critici

Identificando i servizi e i processi di livello 0 e pianificando una strategia di ripristino di emergenza in grado di ripristinarli rapidamente, è possibile ridurre l'impatto significativo su tali servizi e processi, gestendo al contempo il ripristino dei processi dipendenti.

Riduzione del coordinamento manuale durante un evento reale (automazione)

Scegliendo di automatizzare la soluzione di ripristino di emergenza, è possibile ridurre il coordinamento manuale necessario per eseguire tale soluzione quando si verifica un evento. L'automazione è utile anche quando si testa il piano di continuità aziendale (BCP), che specifica come mantenere le operazioni aziendali standard durante un'interruzione non pianificata.

Fidelizzazione dei clienti

In un mercato competitivo, la strategia di ripristino di emergenza influisce sull'acquisizione e la fidelizzazione dei clienti. Se l'organizzazione è in grado di riprendersi rapidamente dagli eventi di emergenza, è possibile creare un rapporto di fiducia con i clienti.

Ottimizzazione della sicurezza

Una strategia di ripristino di emergenza interregionale ben pianificata può aiutare a limitare l'impatto di un attacco ransomware a una sola regione Regione AWS e consentire di utilizzare liberamente i dati in un'altra regione senza perderli.

Aumento della produttività dei dipendenti

Se i tuoi dipendenti comprendono bene il processo di DR e si sentono a proprio agio con esso, un evento di DR non causerà il panico. Per implementare la soluzione di ripristino di emergenza, è possibile seguire runbook ben definiti. In questo modo, i dipendenti possono ottimizzare il tempo a loro disposizione e riportare l'azienda alla normalità.

Definizione della strategia di disaster recovery

A seconda dell'importanza delle applicazioni dell'azienda, è possibile scegliere una strategia uniforme per tutte le applicazioni o sviluppare una strategia di ripristino di emergenza più complessa basata sulla criticità di ciascuna applicazione. L'organizzazione potrebbe tollerare un periodo di inattività di diverse ore prima che tutte le applicazioni vengano ripristinate nel sito di ripristino di emergenza. In questo caso, puoi optare per una strategia di ripristino di emergenza economica basata sul backup e sul ripristino di tutti i database. D'altra parte, l'attività dell'organizzazione potrebbe dipendere dalla rapida disponibilità di alcuni servizi o applicazioni fondamentali, con requisiti RPO e RTO più stringenti, mentre altre applicazioni potrebbero tollerare esigenze meno rigorose. In questo caso, dovrai assegnare la giusta strategia di ripristino di emergenza per ogni livello di applicazioni e database.

La tabella seguente descrive quattro opzioni di DR per i carichi di lavoro eseguiti in Cloud AWS, per aiutarti a determinare e definire la strategia di DR dell'organizzazione. Gli obiettivi RPO e RTO documentati in questa tabella si riferiscono a uno stack completo che include sia i componenti dell'applicazione che quelli del database. Per ulteriori informazioni, consulta Opzioni di disaster recovery nel cloud nella documentazione del AWS Well-Architected Framework. La sezione successiva illustra le opzioni di RPO e RTO specifiche per i database.

Opzione di ripristino	RPO	RTO	Attività infrastrutturali nella regione di ripristino di emergenza	Costo
Backup e ripristino	Ore	Inferiore a 24 ore	Eseguire il provisioning di tutte le risorse applicative richieste nella regione di ripristino di emergenza e ripristinare il database da	Bassa

uno snapshot copiato.

Pilot light	Decine di minuti	Decine di minuti	Eseguire il provisioning di una copia dell'infrastruttura dell'applicazione e disattivare le risorse nel relativo stack. Replicare i dati da una regione all'altra . Mantenere i database sempre attivi e sincronizzati con i database primari. Fornire le risorse su richiesta durante il failover e l'evento di test. È inoltre necessari o implement are le modifiche apportate all'infra struttura e alle applicazioni in entrambe le regioni contempor aneamente . È possibile semplificare questa operazion e tramite la creazione di	Media

			pipeline di automazione in grado di sincronizzare codice e infrastruttura sia nelle regioni primarie che in quelle di ripristino di emergenza.	
Warm standby	Minuti	Minuti	Effettuare il provisioning di una copia dell'intera infrastruttura dell'applicazione nella regione di ripristino di emergenza, ma mantenere la copia dimensionata rispetto alla regione principale. La regione di ripristino di emergenza potrà accettare il traffico a un volume inferiore rispetto alla regione principale.	Elevata

Multi-site oppure active/active	Vicino allo zero	Zero o vicino allo zero	Effettuare il provisioning di una copia completa dell'infrastruttura nella regione di ripristino di emergenza. Tutte le risorse nella regione di ripristino di emergenza saranno equivalenti a quelle della regione principale. Inoltre, saranno in grado di servire il traffico con lo stesso dimensionamento rispetto della regione principale. Poiché non vi è alcuna interruzione nel flusso di traffico, questa opzione non richiede un'attività di failover come parte del piano di ripristino di emergenza.	Più alto

Scelta del database corretto per i requisiti RTO e RPO

Dopo aver definito la strategia di ripristino di emergenza per l'organizzazione in base alla tabella della sezione precedente, scegli i database adatti ai requisiti RPO e RTO. Per impostazione predefinita, tutti i servizi di AWS database forniscono funzionalità di backup e ripristino. Utilizza la tabella seguente per conoscere le funzionalità di ripristino di emergenza più avanzate fornite dai servizi di database AWS e adattale ai requisiti di ripristino di emergenza.

AWS servizio di database	Metodo di replica nella regione di ripristino di emergenza	Possibile classificazione in standby	RTO	RPO
Amazon RDS per MySQL	Cross-Region replica di lettura	1. Luce pilota 2. Warm standby con capacità di traffico di lettura	Di solito espresso in minuti. L'automazione può ridurre al minimo i ritardi.	In genere meno di 1 secondo
Amazon RDS per PostgreSQL	Cross-Region replica di lettura	1. Luce pilota 2. Warm standby con capacità di traffico di lettura	Di solito espresso in minuti. L'automazione può ridurre al minimo i ritardi.	In genere meno di 1 secondo
Amazon RDS per MariaDB	Cross-Region replica di lettura	1. Luce pilota 2. Warm standby con capacità di traffico di lettura	Di solito espresso in minuti. L'automazione può ridurre al minimo i ritardi.	In genere meno di 1 secondo
Edizione Amazon Aurora	Il database globale dispone di uno o più	1. Hot standby con capacità di supportare il	In genere meno di 1 minuto.	In genere meno di 1 secondo

MySQL-Compatible	cluster secondari in una regione diversa	traffico di lettura 2. Warm standby con capacità di supportare il traffico di lettura		
Edizione Amazon Aurora PostgreSQL-Compatible	Il database globale dispone di uno o più cluster secondari in una regione diversa	1. Hot standby con capacità di supportare il traffico di lettura 2. Warm standby con capacità di supportare il traffico di lettura	In genere meno di 1 minuto.	In genere meno di 1 secondo
Amazon DocumentDB (compatibile con MongoDB)	Il cluster globale dispone di uno o più cluster secondari in una regione diversa	1. Hot standby con capacità di supportare il traffico di lettura 2. Warm standby con capacità di supportare il traffico di lettura	In genere meno di 1 minuto.	Espresso in secondi
Amazon ElastiCache (sistema operativo Redis)	Il datastore globale dispone di un cluster secondario in una regione diversa	1. Hot standby con capacità di supportare il traffico di lettura 2. Warm standby con capacità di supportare il traffico di lettura	Di solito espresso in minuti. L'automazione può ridurre al minimo i ritardi.	Espresso in secondi

Amazon DynamoDB	Tabelle globali DynamoDB	Active/active la configurazione accetta operazioni di scrittura nella regione secondaria	Zero o vicino allo zero.	Sub-second
Amazon RDS per Oracle	Promozione delle repliche di letture tra regioni (Oracle Enterprise Edition e Active Data Guard)	1. Luce pilota 2. Warm standby con capacità di traffico di lettura	Di solito espresso in minuti.	In genere meno di 1 secondo
Amazon RDS per Oracle (alternativa)	Promozione delle repliche di lettura montate tra regioni (Oracle Enterprise Edition)	1. Luce pilota 2. Warm standby (non consente query di lettura)	Di solito espresso in minuti.	In genere meno di 1 secondo
Amazon RDS per SQL Server	Cross-Region leggi la replica (Microsoft SQL Server Enterprise Edition 2016-2022)	1. Luce pilota 2. Warm standby con capacità di traffico di lettura	Di solito espresso in minuti. L'automazione può ridurre al minimo i ritardi.	In genere meno di 1 secondo
Amazon Neptune	Il database globale ha cluster secondari in una regione diversa	1. Hot standby con capacità di supportare il traffico di lettura 2. Warm standby con capacità di supportare il traffico di lettura	In genere meno di 1 minuto.	In genere 1 secondo

Amazon RDS per Db2	Cross-Region replica di lettura (Amazon RDS per Db2 11.5.9 e 12.1.4)	1. Luce pilota 2. Warm standby con capacità di traffico di lettura	Di solito espresso in minuti. L'automazione può ridurre al minimo i ritardi.	In genere meno di 1 secondo
Amazon MemoryDBMulti-Region	Multi-Region cluster con replica attiva-attiva	Active/active la configurazione accetta operazioni di scrittura nella regione secondaria	Zero o vicino allo zero.	In genere meno di 1 secondo

Promuovere l'adozione della tua strategia di disaster recovery

Dopo aver implementato la strategia di ripristino di emergenza, puoi promuoverne l'adozione all'interno dell'organizzazione. Quando l'adozione sarà completa, tutte le applicazioni e i relativi database saranno in grado di gestire un evento di ripristino di emergenza negativo e potranno raggiungere la maturità attraverso i test.

Puoi collaborare con i proprietari e gli architetti delle applicazioni per promuovere l'adozione comunicando la strategia DR all'intera organizzazione e chiedendo ai dipendenti di valutare gli attuali database AWS utilizzati nelle loro applicazioni. Ciò garantisce che tutti i database attualmente utilizzati siano in grado di soddisfare le aspettative stabilite nella strategia di ripristino di emergenza. Se i proprietari e gli architetti delle applicazioni stabiliscono che il database scelto per le loro applicazioni non è in grado di soddisfare i requisiti della strategia DR, dovranno pianificare una migrazione verso un AWS database adatto in grado di soddisfare le aspettative RTO e RPO prescelte. Ad esempio, se un'applicazione fondamentale dell'azienda che richiede un RPO in secondi e un RTO in minuti utilizza attualmente un'istanza DB Amazon RDS per Oracle, Amazon RDS non sarà in grado di soddisfare queste aspettative. In questo caso, potresti prendere in considerazione la migrazione del carico di lavoro su Amazon PostgreSQL-Compatible Aurora e utilizzare un database globale per soddisfare le aspettative stabilite dalla tua strategia di disaster recovery.

Automatizzazione della strategia di disaster recovery

Puoi facoltativamente scegliere di implementare un'automazione totale o parziale per ottenere un migliore controllo del ripristino di emergenza. Se utilizzi l'opzione DR di backup e ripristino, puoi automatizzare i backup utilizzando AWS Backup, che supporta tutti i database Amazon RDS oltre alle tabelle DynamoDB, Amazon DocumentDB e Amazon Neptune.

Rilevamento di eventi di emergenza

Per ridurre i tempi di ripristino, puoi considerare la possibilità di automatizzare il rilevamento di un evento a livello regionale, che può quindi avviare il failover nella regione di ripristino di emergenza. Per implementare il rilevamento automatico e ottenere un RTO più stringente, puoi creare una soluzione basata su controlli dell'integrità. Questi controlli dell'integrità non si limitano agli heartbeat, che verificano se i moduli del piano di controllo (control-plane) e del piano dati all'interno di una rete sono in grado di comunicare tra loro, ma approfondiscono la valutazione della natura interrelata dei componenti dell'applicazione per ottenere una previsione accurata. Tuttavia, una soluzione automatizzata può comportare il rischio di falsi allarmi, che possono portare a failover non necessari. In questo caso è necessario prestare attenzione, poiché i failover non necessari introducono problemi di disponibilità per l'azienda. Puoi inoltre confermazione l'esecuzione di un failover creando sostituzioni manuali nel flusso di lavoro. Per rimanere aggiornato sulle interruzioni a livello di servizio, puoi sottoscrivere il feed RSS Service Health Dashboard. Inoltre, puoi utilizzare la AWS Health Dashboard (richiede una Account AWS) all'interno della tua regione e del tuo account principali per rimanere informato sugli eventi che possono influire sul tuo account. Questi possono aiutarti a prendere una decisione informata di fallire in caso di Region-wide evento.

Failover

Indipendentemente dalla strategia di ripristino di emergenza scelta, puoi creare soluzioni di automazione di ripristino di emergenza personalizzate per eseguire il failover nella regione interessata. Questa automazione può ridurre al minimo la necessità di interventi manuali e fornire un maggiore controllo nel testare la soluzione di ripristino di emergenza. Puoi scegliere tra le API di AWS servizio, che AWS forniscono in più lingue come Python JavaScript, PHP, .NET, Ruby, Java, Go Node.js e C++, in base alle preferenze della tua organizzazione. Per creare un'automazione che utilizzi queste API di AWS servizio, dovresti innanzitutto concentrarti sulla trasformazione dell'infrastruttura del database in codice sotto forma di modelli Terraform. AWS CloudFormation Questi modelli possono aiutarti ad automatizzare il failover di diversi database, oltre a mantenere

l'ordine in cui i componenti dell'applicazione e del database vengono ripristinati nella regione di ripristino di emergenza.

Ai fini del ripristino di emergenza, ti consigliamo di concentrarti su questi due obiettivi:

- CloudFormation Gli stack esistenti dovrebbero esportare le informazioni pertinenti sui database, inclusi i nomi delle istanze e gli endpoint. I processi di automazione possono fare riferimento a questi valori di esportazione all'interno di una regione ed eseguire operazioni per facilitare il ripristino di emergenza.
- Se disponi di risorse in produzione ma non hai uno CloudFormation stack associato, dovresti concentrarti sulla creazione di pile per tali risorse. Assicurati inoltre che questi stack coprano i valori di esportazione corretti, come indicato nel punto precedente.

Una volta raggiunti questi due obiettivi, puoi creare soluzioni di automazione nella lingua preferita dalla tua organizzazione per sfruttare CloudFormation le esportazioni ed eseguire automaticamente le azioni necessarie in caso di emergenza. Ad esempio, se disponi di un datastore globale ElastiCache (Redis OSS) distribuito come CloudFormation modello, il codice di automazione ha accesso alle CloudFormation esportazioni che forniscono dettagli sul datastore globale. In caso di emergenza, il codice può promuovere automaticamente il datastore secondario al datastore primario senza alcun intervento manuale utilizzando le API del servizio (Redis OSS). ElastiCache

In uno scenario tipico, l'automazione dovrebbe essere scalabile per più database all'interno dell'organizzazione. Puoi dimensionare le soluzioni di automazione per diversi database utilizzando AWS Step Functions o AWS Batch.

Test per ottenere affidabilità

La migliore soluzione di ripristino di emergenza per i database è quella che viene testata frequentemente e supera i controlli seguenti:

- Ripristino adeguato dei dati che soddisfi le aspettative RPO per ogni database
- Ripristino completo di un database funzionante entro l'obiettivo del tempo di ripristino (RTO) previsto, che consente alle applicazioni di connettersi al database e riprendere la piena funzionalità

I test di ripristino di emergenza devono far parte della strategia aziendale, in modo da disporre di backup funzionanti quando necessario. I test di ripristino di emergenza possono inoltre essere utilizzati nei casi in cui:

- Le dimensioni di un database sono aumentate in modo significativo e l'attuale strategia di ripristino di emergenza non soddisfa più gli accordi sul livello di servizio (SLA) dell'azienda.
- Un file di backup è danneggiato, il che potrebbe causare problemi durante il ripristino.

Aspetti da tenere in considerazione quando si testa la strategia di ripristino di emergenza

- Avere chiari gli obiettivi di continuità aziendale in termini di RPO e RTO e assicurarsi che i risultati dei test siano in linea con gli obiettivi.
- Creare un piano dettagliato per il test di ripristino di emergenza, tenendo conto dei requisiti finanziari e del fabbisogno di risorse umane per l'esecuzione del test.
- Assegnare risorse per documentare i potenziali problemi e le conoscenze acquisite.
- Aggiornare la strategia di ripristino di emergenza in base alle conoscenze acquisite e trovare una soluzione che supporti i processi e l'automazione ottimali per l'organizzazione.

Frequenza dei test per le soluzioni DR

Non esistono raccomandazioni specifiche per i cicli di test DR, a meno che non siano esplicitamente prescritte dalle normative. Ad esempio, l'audit di conformità agli standard PCI DSS (Payment Card Industry Data Security Standards, standard di sicurezza dei dati dell'industria delle carte di

pagamento) richiede alle organizzazioni di testare il proprio piano di ripristino di emergenza almeno una volta all'anno. (Vedi i requisiti di ripristino di emergenza PCI DSS sul sito Web PCI DSS.)

I team applicativi possono anche eseguire test continui delle soluzioni di ripristino di emergenza individuali nel momento in cui cambia l'applicazione o l'infrastruttura.

Rilevamento delle deviazioni

La soluzione di ripristino di emergenza deve inoltre essere in grado di gestire il rilevamento delle deviazioni. In questo modo, si garantisce che la regione primaria e la regione di ripristino di emergenza siano sincronizzate, consentendo un avanzamento regolare durante i test. AWS Config offre funzionalità di gestione della configurazione e monitoraggio della cronologia delle configurazioni nell'infrastruttura, consentendo di gestire efficacemente la deviazioni.

Osservabilità

L'ottimizzazione dell'osservabilità ha un impatto positivo sulla preparazione ai test. Tutte le soluzioni di ripristino di emergenza spostano i dati dalla regione primaria alla regione secondaria (di ripristino di emergenza). È possibile impostare avvisi per i ritardi di replica e backup oppure mettere in atto un processo per eseguire controlli giornalieri che assicurino la copia corretta dei dati nella regione di ripristino di emergenza.

Risorse e passaggi successivi

- Per ulteriori informazioni su DR on AWS, leggi il white paper Disaster Recovery of Workloads on AWS: Recovery in the Cloud.
- Esamina il pilastro dell'affidabilità nel Framework. AWS Well-Architected
- Esplora AWS Resilience Hubper tracciare e convalidare la resilienza dei tuoi carichi di lavoro. AWS
- Esamina le seguenti risorse aggiuntive:
  - Utilizzo del failover in un database globale Amazon Aurora (documentazione di Aurora)
  - Replica Regioni AWS tramite datastore globali (documentazione Amazon ElastiCache (Redis OSS))
  - Ripristino di emergenza e cluster globali di Amazon DocumentDB (documentazione di Amazon DocumentDB)
  - Preparati per un disaster recovery più rapido: implementa un database globale Amazon Aurora con Terraform (parte 1) (post sul blog)AWS
  - Tabelle globali Amazon DynamoDB (sito Web)AWS
  - Disaster Recovery su AWS, Cross-Region replica (Amazon RDS lab)
  - Cross-Region disaster recovery di Amazon RDS per SQL ServerAWS (post di blog)
  - Disaster recovery gestito con Amazon RDS for Oracle Backup automatici su più regioni — Parte 1 AWS (post sul blog)

Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida.

Modifica	Descrizione	Data
Dettagli aggiornati nella tabella di confronto	È stata aggiornata la sezione Scelta del database giusto per i requisiti RTO e RPO.	29 giugno 2026
Dettagli aggiornati nella tabella di confronto	Nella sezione Scelta del database giusto per i requisiti RTO e RPO, sono state aggiornate le informazioni su Amazon RDS for Db2 e sono stati corretti i dettagli RPO per Amazon RDS for Oracle e Amazon RDS for Oracle (alternativa).	11 giugno 2025
Aggiunto Amazon RDS per Db2	Nella sezione Scelta del database giusto per i requisiti RTO e RPO, sono state aggiunte informazioni su Amazon RDS for Db2.	4 marzo 2024
Dettagli aggiornati RTO/RPO	Nella sezione Scelta del database giusto per i requisiti RTO e RPO, sono state aggiornate le informazioni su Amazon DocumentDB, ElastiCache Amazon (Redis OSS) e Amazon RDS for SQL Server.	19 aprile 2023
Pubblicazione iniziale	—	26 ottobre 2022

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