Disaster Recovery ibrido: linee guida strategiche

9 Giugno 2023 - 8 min. read

Disaster Recovery (DR) | DR Strategy

Con questo articolo proseguiamo la nostra serie sul Disaster Recovery esaminando i principali aspetti tecnici relativi al DR in uno scenario in cui le aziende stanno adottando un approccio ibrido che combina l'infrastruttura on-premise esistente con le risorse del Cloud AWS.

(Non hai ancora letto la prima parte? Puoi trovarla qui!)

La pianificazione e l'implementazione di una solida strategia di Disaster Recovery (DR) sono fondamentali per garantire la continuità operativa delle aziende in caso di eventi catastrofici o interruzioni impreviste dei sistemi. Negli ultimi anni, il Cloud Computing ha offerto nuove opportunità per migliorare l'efficienza e l'affidabilità delle soluzioni di DR.

Questa combinazione ibrida offre una serie di vantaggi che consentono alle organizzazioni di affrontare in modo efficace gli obiettivi di business continuity.

Perchè il Cloud cambia lo scenario del DR?

Partiamo analizzando quali sono i vantaggi del modello Cloud, che ci permette di realizzare progetti che altrimenti non sarebbero sostenibili.

Prima di tutto la **natura on demand** del Cloud e quindi di AWS, ovvero la scalabilità e la flessibilità che ne derivano. Nel contesto on-premises, le risorse sono limitate dalla capacità hardware e dalle infrastrutture fisiche esistenti. Nel mondo Cloud è possibile scalare verticalmente o orizzontalmente le risorse di DR in base alle esigenze, consentendo una maggiore flessibilità nel gestire picchi di carico o situazioni di emergenza.

Altri vantaggi essenziali sono l'**affidabilità e la disponibilità** in quanto ci sono servizi gestiti che ci permettono di sfruttare la ridondanza geografica, la distribuzione automatica del carico, la replicazione dei dati su più zone di disponibilità e la gestione dei failover.

Ovviamente grazie alla **natura programmatica** del Cloud possiamo automatizzare, efficientare e semplificare i processi di ripristino rendendoli più veloci ed efficaci.

Infine, ma non ultimo per importanza, va considerato l'aspetto dei **costi**. Il confronto dei costi operativi tra l'approccio on-premises e il Cloud AWS evidenzia i benefici economici di quest'ultimo. Nel modello on-premises, le aziende devono investire in hardware, software, spazio fisico, manutenzione e personale specializzato per implementare e gestire una soluzione di DR. Nel Cloud AWS, i costi sono basati sul consumo effettivo delle risorse: in pratica si paga per quello che realmente serve e viene utilizzato. Questo approccio a consumo consente alle aziende di ridurre i costi operativi legati all'infrastruttura di DR, eliminando la necessità di investimenti iniziali significativi e riducendo i costi di manutenzione.

Quest'ultimo concetto è ovviamente e linearmente correlato alla tipologia di strategia che viene adottata.

L'obiettivo principale del DR è mantenere la continuità operativa. Ciò significa che è necessario determinare quali applicazioni siano più cruciali per l'organizzazione e quali sono gli RPO e RTO richiesti. Un buona pratica prevede di classificare i workload in base ai requisiti di business continuity cercando di omogeneizzare il più possibile. In base ai requisiti di RPO e RTO, in linea di massima possiamo ragionare su tre macro categorie.

1. **Bassa criticità**: l'RPO per questi workload è di alcune ore o addirittura di alcuni giorni. L'RTO è di alcuni giorni o più. In genere, questi workload richiedono un'architettura di DR meno complessa e costosa, consentendo un periodo di ripristino più lungo.
2. **Media criticità**: l'RPO per questi workload è nell'ordine di decine di minuti, consentendo una perdita di dati accettabile. L'RTO varia da poche ore a un giorno. È comunque importante garantire la disponibilità dei dati aggiornati per limitare la perdita di informazioni e ripristinare l'applicazione entro un periodo di tempo ragionevole.
3. **Alta criticità**: questo gruppo include workload con RPO di pochi secondi o addirittura zero, il che significa che non ci si può permettere la perdita di dati. L'RTO potrebbe essere nell'ordine di minuti o di decine di minuti, in modo da ripristinare rapidamente l'applicazione in caso di interruzione.

A ogni gruppo consegue una diversa strategia. Per esempio i workload critici richiedono un sito di DR **Multi-site Active-Active**, per quelli a media criticità una strategia di tipo **Pilot Light** e per quelli a bassa criticità **Backup e Ripristino**.

Se non sono chiari i concetti di RPO/RTO e le più comuni strategie di DR, ne abbiamo parlato qui.

Tre strategie di DR e come applicarle

Unendo i concetti fino a qui espressi, è evidente che il Cloud massimizza i propri vantaggi nella strategia Backup e Ripristino. Vediamo come tecnicamente è possibile mettere a terra il backup and restore da on-premise al Cloud attraverso alcune considerazioni.

Facciamo subito focus sul dato e quindi sull'RPO. Come porto i miei dati in Cloud? E prima ancora quali sono i dati?

I dati non sono solo le informazioni salvate su database o file-server, ma anche le configurazioni del nostro ambiente. Sicuramente è importante avere sistemi che fanno backup regolari e che siano in grado di trasferirli sul sito secondario, ma abbiamo anche bisogno di strumenti che tengano allineate le configurazioni.

In questo caso servizi come Storage Gateway ed EBS ci vengono in soccorso. Storage gateway si può configurare in diverse modalità: File Gateway, Tape e Volume Gateway. Per il Backup and Restore ha senso concentrarsi maggiormente sulla modalità Volume Gateway.

Con il Volume Gateway i sistemi in locale montano i volumi iSCSI e le applicazioni interagiscono con questi ultimi come se fossero normali archivi a blocchi. I dati scritti su questi volumi vengono compressi e vengono copiati in modo asincrono come snapshot point-in-time e archiviati nel Cloud come EBS Snapshots.

Storage Gateway ci permette di sfruttare uno storage ad oggetti a basso costo ed alta retention (AWS S3) per salvare i nostri dati. Poiché si integra con EBS, ci permette di creare i volumi per le nostre EC2 da ripristinare. Contestualmente, grazie all'integrazione con AWS Backup, possiamo configurare in maniera automatica la retention e il decommissioning automatico dei nostri backup rendendo più facile mantenere il controllo e la governance del nostro processo.

L'utilizzo di Cloud Formation ci permette di creare e manutenere le nostre configurazioni in maniera automatica e consistente.

Per quanto riguarda i workload a media e ad alta criticità ci si deve appoggiare a strumenti che siano in grado di creare repliche continue dei nostri ambienti o di porzioni di essi.

Nel caso di **workload a media criticità** la replica a bassa latenza di database e file è essenziale, ma non lo è per i nodi computazionali che erogano i nostri servizi. Infatti siamo nel caso di RPO di decine di minuti e RTO di qualche ora. La strategia migliore è quella della Pilot Light, in cui alcune componenti infrastrutturali sono accese e sincronizzate nel sito di DR e altre componenti sono replicate a intervalli regolari e pronte ad entrare in gioco a tempo debito.

In questo caso ancora una volta a nostro supporto c'è Storage Gateway, ma in modalità File Gateway sincrona, che ci permette di replicare i nostri file su S3 o direttamente sul servizio gestito FSx for Windows File server. In alternativa AWS Data Sync replica i dati copiandoli su qualsiasi classe di storage S3 ed è compatibile anche con qualsiasi servizio gestito di file storage AWS (EFS ed FSx). Datasync, però, prevede una sincronizzazione a intervalli regolari e non in modalità on-going.

Per quanto riguarda i nostri database, AWS Database Migration Service (DMS) è la chiave di svolta. Grazie a DMS possiamo tenere sincronizzati i nostri database on-premise grazie alla Change Data Capture (CDC) che sincronizza gli eventi di modifica al dato (DML) tramite la lettura dei transaction log. Così è possibile tenere allineati in near-real-time i due database senza sovraccaricare i nodi di produzione.

Per i **workload ad alta criticità** AWS mette a disposizione Elastic Disaster Recovery (AWS DRS) con il quale siamo in grado di ripristinare applicazioni su AWS da infrastrutture fisiche, VMware vSphere, Microsoft Hyper-V e anche da altri Cloud provider.

In caso di disastro, è necessario eseguire un failover su AWS con l'aiuto di AWS Elastic Disaster Recovery (AWS DRS). Una volta mitigato il disastro, è poi necessario eseguire un failback sull'infrastruttura di origine. Le istanze di ripristino con AWS Elastic Disaster Recovery possono essere portate all'ultima versione disponibile o a un determinato punto nel tempo (Point-in-time - PIT).

Per la maggior parte delle organizzazioni, il sito di DR non è progettato per gestire le operazioni quotidiane e potrebbe essere necessario un notevole sforzo per spostare i dati e i servizi aziendali nell'ambiente primario una volta terminato il disastro. Potrebbe essere necessario pianificare un periodo di inattività o una parziale interruzione delle attività durante il processo di failback al sito primario.

Una volta pronti a riprendere le operazioni sul sistema primario, sarà necessario eseguire la replica del **failback**. Infatti, durante l'utilizzo del sistema di ripristino su AWS, nuovi dati vengono scritti nel sistema secondario e questi dati devono essere riportati indietro. È possibile eseguire un failback sui server di origine installando il Failback Client di AWS Elastic Disaster Recovery.

Eseguire test di ripristino (o drill) è un aspetto fondamentale per essere preparati per un disastro, in tutti i casi sopra elencati. Effettuare regolarmente test di ripristino per assicurarsi che i dati di backup siano integri e che sia possibile ripristinare il workload in modo corretto è fondamentale per valutare l'efficacia del processo di ripristino e identificare eventuali problemi o aree di miglioramento. Ad esempio, AWS DRS ci permette di automatizzare anche i drill.

Conclusioni

Molti degli argomenti espressi si basano sull'assunzione che le infrastrutture on premises siano basate su architetture classiche e, quindi, principalmente su VM. Il Cloud rimane comunque una valida scelta anche in scenari più moderni dove per esempio i container la fanno da padroni: servono tecniche diverse, ma i concetti rimangono gli stessi.

Aver implementato il DR su Cloud non ci deve fermare dal voler innovare il più possibile i nostri workload cercando di sfruttare al meglio i servizi gestiti di alto livello. Questo ci porta a ridurre l'impegno speso per il mantenimento dell'infrastruttura concentrandoci, invece, sul migliore il livello di servizio offerto e su migliori costi.

Nel prossimo articolo vedremo quali tecniche adottare in un contesto "Cloud-to-Cloud". Vedremo in particolare come cambiano gli scenari di disastro in questo scenario con un focus su Security e Automation.

Ci vediamo tra 14 giorni!

About Proud2beCloud

Proud2beCloud è il blog di beSharp, APN Premier Consulting Partner italiano esperto nella progettazione, implementazione e gestione di infrastrutture Cloud complesse e servizi AWS avanzati. Prima di essere scrittori, siamo Solutions Architect che, dal 2007, lavorano quotidianamente con i servizi AWS. Siamo innovatori alla costante ricerca della soluzione più all'avanguardia per noi e per i nostri clienti. Su Proud2beCloud condividiamo regolarmente i nostri migliori spunti con chi come noi, per lavoro o per passione, lavora con il Cloud di AWS. Partecipa alla discussione!

Nicola Ferrari

Cloud Infrastructure Line Manager @ beSharp e AWS authorized instructor champion.Vivo la vita “un livello alla volta”. Ottengo i miei superpoteri raccogliendo caffeina nascosta qua e là nella mia mappa quotidiana. Sono un Internet surfer professionale (e ho visto tutto l’Internet per intero... almeno due volte!) e un appassionato di tecnologia, computer e networking. Costruire grandi cose IT - tutte precise e ordinate - contribuisce alla mia missione principale: la ricerca della perfezione!

Simone Merlini

CEO e co-fondatore di beSharp, Cloud Ninja ed early adopter di qualsiasi tipo di soluzione *aaS. Mi divido tra la tastiera del PC e quella a tasti bianchi e neri; sono specializzato nel deploy di cene pantagrueliche e nel test di bottiglie d'annata.
