Commvault

Cloud Rewind™
Formerly Appranix

eBOOK

Come raggiungere la resilienza delle applicazioni in cloud con recuperi iper-veloci.

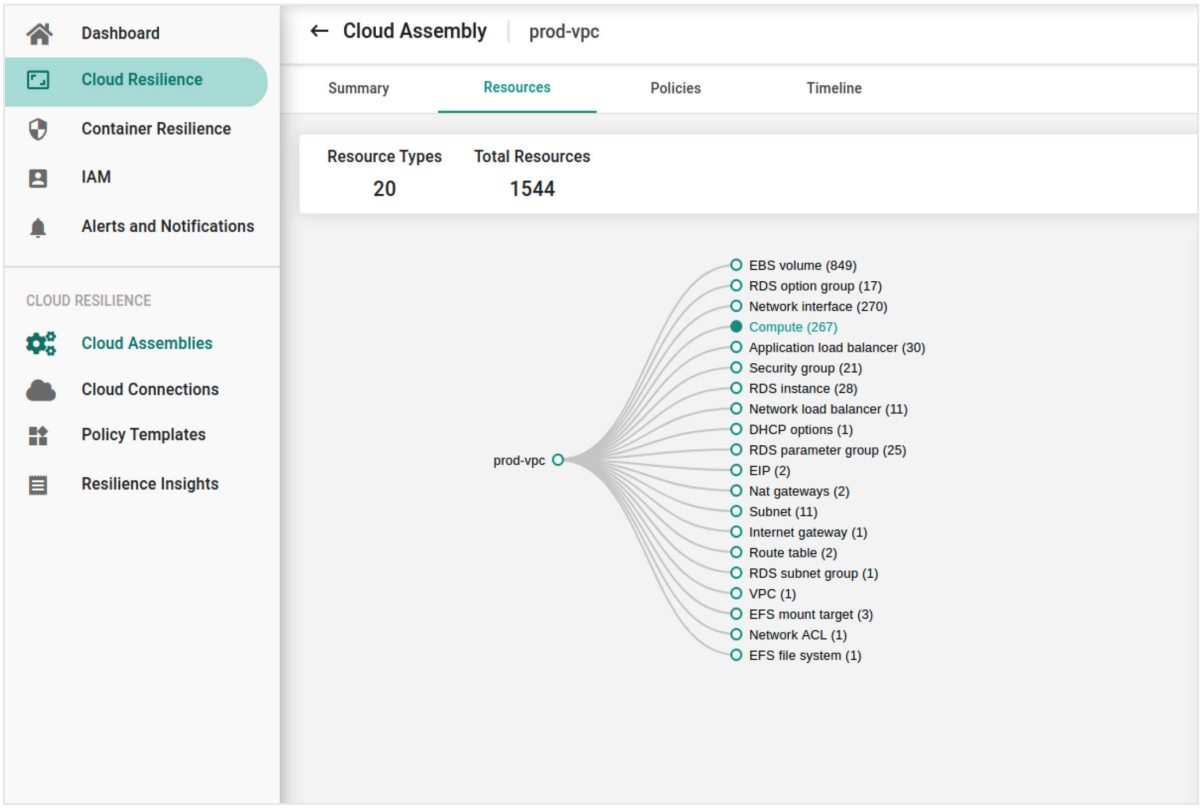
Commvault

Table of Contents

RIPRISTINO IPER-VELOCE DI AMBIENTI APPLICATIVI IN CLOUD

Le organizzazioni in al cloud sono passate rapidamente ad un modello operativo decentralizzato per le loro applicazioni e servizi. Anche le architetture software sono diventate più distribuite, facendo uso di risorse cloud prontamente disponibili in tutte le zone cloud. I Site Reliability Engineer hanno adottato cicli di rilascio più dinamici e più rapidi grazie all'uso delle pratiche DevOps, al fine di soddisfare le crescenti richieste dei clienti. Inoltre, risorse cloud programmabili hanno permesso agli ambienti di scalare automaticamente per soddisfare i requisiti di performance delle applicazioni aziendali critiche. Sul versante negativo, però, tutti questi cambiamenti hanno creato enormi sfide per i team dei servizi operativi condivisi che gestiscono la resilienza, la sicurezza e i costi. La domanda più pressante oggi, soprattutto quando gli ambienti cloud sono soggetti a un aumento dei cyberattacchi, è come questi ambienti applicativi dinamici e a scalabilità automatica possano ripristinare rapidamente da tempi di inattività utilizzando un'infrastruttura cloud-nativa, in modo da mantenere gli SLA aziendali promessi.

PERCHE' IL MODELLO TRADIZIONALE DI BCDR DEL DATA CENTER NON E' PIU' ADATTO PER LE APPLICAZIONI IN CLOUD?



Le applicazioni non si affidano più a pochi server o database critici. Si consideri il seguente esempio di una semplice applicazione cloud a tre livelli con autoscaling composta da due macchine virtuali e un database. È composta da almeno venti (20) tipi di risorse cloud e istanze distinte. I sistemi tradizionali di backup e di ripristino tradizionali sono stati progettati per proteggere solo i dischi delle macchine virtuali, i database e i file system. Per garantire la resilienza dell'intera applicazione cloud, tutte le risorse cloud devono essere protette in modo da poter ripristinare il sistema in qualsiasi momento in modo da poter effettuare il ripristino in qualsiasi momento e in qualsiasi regione del cloud. I sistemi di backup e ripristino tradizionali non sono stati costruiti per proteggere tutte queste risorse cloud utilizzate da applicazioni dinamiche e distribuite a scalabilità automatica che si basano su infrastrutture cloud definite dal software.

LA PROLIFERAZIONE DEL RANSOMWARE CAMBIA IL RIPRISTINO DELLE APPLICAZIONI

Con il proliferare degli attacchi ransomware e la loro crescente sofisticazione, i recuperi degli ambienti cloud diventano sempre più difficili. La cosa più importante è che i nuovi attacchi ransomware prendono di mira i backup e le loro console di gestione. Poiché la maggior parte dei prodotti di BCDR viene installato nello stesso account cloud dei sistemi di produzione, nel caso di un attacco ransomware che compromette l'intero account cloud, potrebbe non essere nemmeno possibile raggiungere le console dei sistemi di backup e recover per poter ripristinare gli ambienti applicativi. Questo è forse uno dei modelli critici che le organizzazioni devono riesaminare nel ridisegnare l'architettura di resilienza delle applicazioni e non solo la protezione ed il ripristino dei dati.

Poiché i sistemi di applicazioni in cloud sono composti da numerosi servizi di infrastruttura cloud, gli utenti che eseguono ripristini dopo attacchi di ransomware hanno bisogno di una profonda conoscenza per ripristinare macchine virtuali, database, reti, numerosi servizi cloud e le loro configurazioni corrispondenti. Spesso, I team di cloud operations devono compilare manualmente componenti chiave degli ambienti applicativi, come reti private virtuali (VPC), bilanciatori di carico, gateway, gruppi di sicurezza, gruppi di parametri di database, ecc., prima che i sistemi BCDR vengano utilizzati per il ripristino dei dati.

LA SCOPERTA CONTINUA DELLE RISORSE IN CLOUD È CRUCIALE PER UNA MAGGIORE RESILIENZA

Gli ambienti cloud dinamici e autoevolutivi presentano enormi sfide per gli operations team per mantenerli sicuri e resilienti. Dato che molte squadre di sviluppo gestiscono la maggior parte delle risorse di infrastruttura cloud in modo autonomo, gli ambienti applicativi in cloud si espandono più rapidamente rispetto al modello tradizionale di data center. Questi ambienti programmati e in continua evoluzione richiedono un sistema in grado di scoprire continuamente tutte le risorse appartenenti a un'applicazione. Le organizzazioni hanno inoltre molti account cloud per isolare i loro ambienti di sviluppo, produzione e test in base alle loro esigenze aziendali. Oggi, non è insolito che le organizzazioni abbiano centinaia di account cloud.

La complessità di molti account cloud, insieme ad ambienti in continua evoluzione, rende difficile per i team centralizzati dipendere da sistemi di protezione e ripristino tradizionali e non orientati alle applicazioni. Infatti, questi sistemi si limitano a richiedere agli utenti di selezionare le risorse corrette e applicare la protezione manualmente. Dall'altro lato, gli sviluppatori di applicazioni non seguono tutte le risorse di infrastruttura cloud utilizzate per le loro applicazioni, il che impedisce di aiutare gli SRE (Ingegneri di Affidabilità del Sito) nel momento cruciale del ripristino. Spesso, diverse pipeline DevOps modificano gli ambienti cloud centrali, rendendo ancora più difficile per gli SRE ripristinare le applicazioni nel momento in cui è più urgente. Pertanto, è necessario avere un sistema che scopra continuamente le risorse cloud e sia orientato alle applicazioni, con la capacità di garantire la comprensione delle risorse del sistema attraverso mappe di dipendenze automatizzate, per proteggere adeguatamente tutte le risorse cloud rilevanti. Questo consente di ripristinare o failover le applicazioni, i dati, le configurazioni, gli stati e le dipendenze rapidamente per soddisfare i requisiti di disponibilità delle applicazioni.

PROTEGGI IL TUO AMBIENTE CLOUD CON UN SISTEMA DI APPRENDIMENTO CONTINUO

Gartner stima che un ambiente cloud tipico sperimenti più di 50 modifiche di configurazione al giorno. È cruciale creare un repository immutabile di metadati di configurazione cloud per tutti gli ambienti di applicazioni critici in cloud. È anche molto importante ospitare questi metadati di configurazione in un sistema di resilienza delle applicazioni basato su un altro servizio cloud per raggiungere livelli aggiuntivi di resilienza. Questi tesori di metadati di configurazione devono essere segmentabili per i servizi di applicazioni e registrati per un ripristino a un punto specifico nel tempo in qualsiasi regione cloud. Devono essere abbastanza dettagliati da permettere agli operations team di richiedere una singola risorsa in un momento specifico, per poter ripristinare rapidamente un'istanza specifica di un servizio cloud in caso di guasto. Un sistema didiscovery continuo e l'analisi dei metadati elimina completamente la necessità di una valutazione manuale e i rischi associati a metadati separati durante il processo di ripristino.

RECUPERO IPER-VELOCE DELL'AMBIENTE CON DISASTER RECOVERY AS CODE (DR-AS-CODE)

La parte più complessa del ripristino consiste nell'identificare le risorse appropriate per il calcolo, lo storage, PaaS e l'infrastruttura di rete che appartengono a un insieme di applicazioni, e poi sequenzarle per eseguire un ripristino orchestrato. Questo è noto come "Piano Tecnico di Ripristino" o TDP. Esiste anche un aspetto non tecnico del piano di ripristino (DR) che coinvolge la fornitura di risorse umane e organizzative per validare le applicazioni dopo il ripristino.

I TDP solitamente consistono in diverse pagine e richiedono la collaborazione di molte persone operative per identificare cosa funziona in produzione in termini di configurazioni, dipendenze, sequenziazione e script. Le organizzazioni che hanno utilizzato prodotti di BCDR tradizionali possono testimoniare la complessità dei TDP e il motivo per cui spesso non eseguono prove di ripristino.

Grazie a un modello automatizzato di Infrastructure-as-Code (IaC), ora è possibile eliminare completamente i TDP complessi e manuali. In particolare, per i ripristini garantiti, è importante utilizzare un IaC cloud-native invece di un IaC cloud-neutral, in modo che la responsabilità del ripristino di grandi sistemi si trasferisca al provider cloud, che dispone di risorse scalabili dinamicamente per eseguire ripristini efficaci in caso di guasto.

GESTIONE DELLE COPIE DI DATI IN CLOUD

Le piattaforme cloud dispongono di capacità di gestione dei dati sufficienti per eseguire copie di dati molto più veloci per backup, repliche e ripristini. Non è necessario aggiungere capacità di gestione dei dati di terze parti. Non è neanche necessario convertire il formato di archiviazione dei dati nativi dell'applicazione in un formato di backup generale o passare attraverso il lungo processo di importazione ed esportazione in un sistema di file di backup neutrale.

È possibile creare copie di dati incrementali e coerenti di macchine virtuali edatabase per ridurre i costi di backup e ripristino in caso di disastro (DR). I servizi serverless dispongono di capacità di gestione dei dati integrate sufficienti per evitare copie costose verso e da piattaforme di gestione dei dati aggiuntive in un ambiente cloud.

Le piattaforme cloud iperscalabili hanno aperto la strada a una resilienza molto maggiore rispetto al modello di infrastruttura del data center. Le organizzazioni globali possono eseguire repliche di dati incrementali da una regione cloud a un'altra in pochi minuti. Questo non solo aumenta la resilienza dei dati, ma consente anche di creare copie multiple e meno costose a livello globale, il che porta a livelli di resilienza delle applicazioni molto superiori in caso di guasto.

MACCHINA DEL TEMPO PER APPLICAZIONI IN CLOUD

La macchina del tempo per applicazioni in cloud è un concetto semplice in cui un sistema automatizzato può raccogliere tutti i metadati delle applicazioni cloud da un cruscotto, l'applicazione da un repository immutabile e i dati dell'applicazione dall'archiviazione e dai database, per eseguire un ripristino sincronizzato a un punto specifico nel tempo. Si possono immaginare queste macchine del tempo come CMDB (Configuration Management Database) registrate che si aggiornano automaticamente da una prospettiva orientata alle applicazioni, utilizzando tutte le capacità native del cloud.

Tuttavia, la differenza più importante tra una macchina del tempo in cloud e le antiche CMDB (Database di Gestione della Configurazione) è che la macchina del tempo in cloud conosce le copie dei dati di un'applicazione in un punto specifico nel tempo. Con il tempo, una macchina del tempo in cloud diventa indispensabile per le organizzazioni, poiché diversi gruppi all'interno di un'organizzazione possono accedervi facilmente per eseguire varie operazioni di reversibilità, ripristino e failover. I sistemi BCDR (Business Continuity Disaster Recovery) tradizionali non hanno mai raccolto i metadati del sistema in un modo che fosse utile oltre le semplici esigenze di backup.

RIEPILOGO

La natura dinamica, la complessità e la velocità dei cambiamenti nelle applicazioni in cloud richiedono realmente un nuovo modello di resilienza orientato alle applicazioni, piuttosto che i modelli di protezione e ripristino o di ripristino da disastro tradizionali che risalgono all'era del data center. Che le applicazioni siano migrate in cloud o create nativamente su piattaforme cloud, questo nuovo modello non solo consente un rapido ripristino di applicativi completi in caso di più guasti, ma riduce anche significativamente i problemi operativi, specialmente quando gli operations team più piccoli gestiscono una quantità molto maggiore di risorse rispetto allo scorso decennio.

INFORMAZIONI SU CLOUD REWIND™

Cloud Rewind offre resilienza delle applicazioni in cloud con un backup e un ripristino completo dell'ambiente cloud, incluse le risorse, i servizi e le dipendenze, in qualsiasi momento e in qualsiasi regione cloud.