CLOUDITALIA®

Guida sul Disaster Recovery

DR negli ambienti virtualizzati

Powered by Zerto

Guida sul Disaster Recovery
DR Negli Ambienti Virtualizzati

INDICE

PREFAZIONE

Disaster recovery in un mondo Virtualizzato

Nelle aziende di oggi, in cui le attività sono basate sui dati e non conoscono interruzioni, la business continuity dipende completamente dalle infrastrutture IT, che devono restare sempre attive e operative, 24x7. I costi dei tempi di inattività sono enormi e la perdita dei dati può mettere a serio rischio l'esistenza stessa delle aziende. La perdita dei dati non è causata soltanto da calamità naturali, interruzioni di corrente, guasti dell'hardware ed errori commessi dagli utenti ma è sempre più spesso la conseguenza di problemi riscontrati con il software ed eventi nefasti correlati alla sicurezza informatica. È quindi fondamentale adottare strategie di sicurezza e business continuity intese a ridurre al minimo i rischi di perdita dei dati e tempi di inattività per le aziende moderne. Si tratta di un'esigenza di estrema attualità perché i data center sono sempre più di tipo software-defined e i private, hybrid e public cloud sono sempre più soggetti a questo tipo di minacce.

In un ambiente virtualizzato software-defined, le applicazioni vengono eseguite su virtual machine (VM), quindi non sono più basate su hardware. Sebbene queste nuove tecnologie apportino notevoli vantaggi alle aziende, che ne guadagnano sicuramente in efficienza, lo stesso discorso non vale per gli ambiti del disaster recovery (DR) e della business continuity (BC).

La maggior parte delle soluzioni di BC/DR è ancora basata su entità, appliance e array fisici, che non offrono la capacità di scalare in base alla quantità di dati attualmente prodotta dalle aziende. In più, potrebbe non essere possibile sfruttare appieno molti dei vantaggi offerti dalla virtualizzazione, a causa dell'overhead di gestione e della difficoltà ad armonizzare una strategia di virtualizzazione con gli strumenti di disaster recovery progettati per gli ambienti fisici. Per superare queste difficoltà, è necessario adottare soluzioni di BC/DR ideate appositamente per gli ambienti virtualizzati.

In questo opuscolo, sono presenti approfondimenti sulle sfide, esigenze, strategie e soluzioni disponibili per il disaster recovery e la business continuity, in special modo nei moderni ambienti virtualizzati e nel public cloud. Sono inoltre delineati i vantaggi e le caratteristiche positive offerti dalla soluzione Zerto Virtual Replication, confrontati con altre tecnologie di BC/DR. Il nostro obiettivo è fornire tutte le informazioni necessarie affinché le aziende possano scegliere la soluzione di BC/DR più adatta alle loro esigenze. Per qualsiasi domanda, non esitate a contattarci all'indirizzo email cloud@clouditalia.com.

PROVATE VOI STESSI

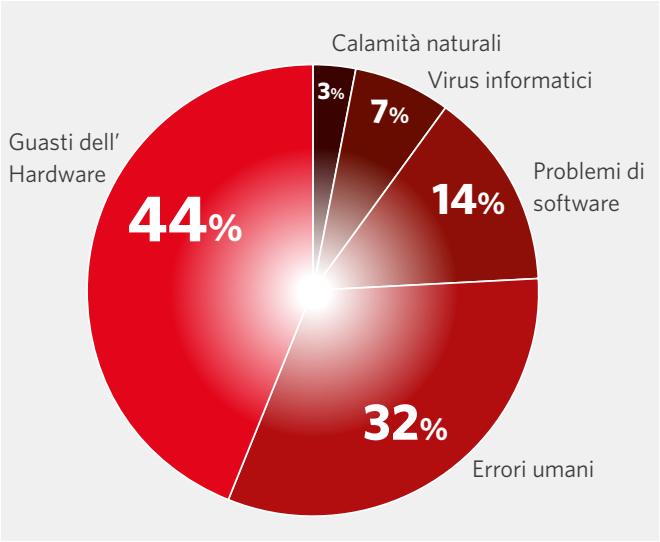
La soluzione Zerto Virtual Replication può essere installata e configurata in meno di un'ora. La replicazione basata su virtual machine offre RPO (Recovery Point Objective) di pochi secondi e RTO (Recovey Time Objective) di pochi minuti. Visitate il sito web www.zerto.com/trial e scaricate una versione di prova gratuita oggi stesso!

SEZIONE 1

Disaster Recovery: Esigenze e Tecnologie

Cause e Costi della Perdita dei Dati

Le aziende di oggi non possono permettersi di perdere dati. Qualunque sia la causa (calamità naturali, errori umani o attacchi informatici), la perdita dei dati si rivela un evento costoso ed estremamente rischioso. Ricerche condotte da vari istituti dimostrano che il volume e i costi della perdita dei dati aumentano di anno in anno. La necessità di adottare una strategia di business continuity in grado di garantire tempi di attività, diminuire la perdita dei dati e aumentare al massimo la produttività in caso di situazioni compromettenti equivale alla sottoscrizione di una polizza assicurativa digitale per qualsiasi azienda. Il rischio è più probabile di ciò che sembra: non è più questione di "*se*" si verificherà la catastrofe ma di "*quando*" avverrà concretamente.



PRINCIPALI CAUSE DI PERDITA DI DATI E TEMPI DI INATTIVITÀ

(fonte: World Backup Day 2015)

...in un mondo virtualizzato

Molte aziende hanno virtualizzato il proprio ambiente di produzione, godendo di grandi vantaggi e conseguendo notevoli e concreti risparmi in termini di costi. Tuttavia, molti di questi vantaggi non sono applicabili alla business continuity e al disaster recovery, poiché le soluzioni di BC/DR sono in genere basate su tecnologie obsolete: replica basata su array o replica basata su agent, ovvero tecnologie non ideate appositamente per gli ambienti virtualizzati. Poiché sono sempre più numerose le tecnologie sfruttate nell'ambito di una pianificazione di disaster recovery, è davvero complesso creare un piano di disaster recovery uniforme e ripetibile.

400% GROWTH

Del volume complessivo della perdita dei dati tra due anni

(Security Week)

$2.1 TRILLION

Costo complessivo delle violazioni di dati nel 2019

(IT Web)

64% OF COMPANIES

Ha subito interruzioni negli ultimi 12 mesi

(EMC)

71% OF IT DECISION MAKERS

Non sono certi della loro capacità di ripristino

(CIO Insight)

15 million APPLICATIONS

Implementate in infrastrutture virtualizzate

(CIO Insight)

86% OF ALL SERVER WORKLOADS

Sono stati virtualizzati nel 2016

(Gartner Group)

Il Concetto di Disaster Recovery

Che cos'è il disaster recovery (DR)? Con disaster recovery si intende, letteralmente, un ripristino di emergenza in seguito al verificarsi di una catastrofe, ovvero il tempo e il lavoro necessari per ritornare attivi e operativi dopo un evento di perdita di dati o inattività. Il tempo necessario varia in base alla soluzione scelta per proteggere l'azienda dalla perdita di dati. Il disaster recovery non riguarda soltanto il tempo in cui sistemi e dipendenti non riescono ad essere operativi, ma anche la quantità di dati persi quando è necessario tornare a una versione precedente dei dati. Le aziende dovrebbero porsi questa domanda: "Quanto ci costa un'ora di inattività?" E soprattutto: "È possibile ricordare e riprodurre il lavoro che i dipendenti (o i sistemi) hanno svolto nelle ultime ore?" Il 95% delle aziende non è in grado di rispondere a queste domande...

Il backup non è una soluzione di disaster recovery efficace

Il disaster recovery implica l'esistenza di diversi concetti, che potrebbero creare confusione: disaster recovery, business continuity, backup, RTO e RPO. Una soluzione ben nota ai più è il concetto di **backup dei dati**, che comporta la replica dei dati o delle virtual machine in un altro dispositivo o ubicazione, eseguita periodicamente in base a un intervallo di tempo prestabilito (ad esempio ogni 24 ore), affinché tali dati o virtual machine possano essere ripristinati o utilizzati come soluzione di conservazione a lungo termine per scopi di conformità. Tuttavia, in casi di emergenza, il backup è un concetto vuoto senza l'adozione di una soluzione di **disaster recovery (DR)** che permetta di ripristinare file, software e funzionalità. In genere, una soluzione di questo tipo non si limita a ricopiare i dati nel sistema in cui si trovavano originariamente. Se un server è inattivo, è necessario reinstallarlo, riconfigurarlo e in alcuni casi persino sostituirlo. Da soli, i backup non sono una soluzione di disaster recovery efficace. Con un backup, le virtual machine devono essere ricreate praticamente da zero, poiché i processi di backup non offrono funzionalità di automazione.

RISPOSTA AL RANSOMWARE

Negli ultimi anni è stata osservata una nuova tendenza: gli hacker tentano di estorcere denaro sia da utenti privati che aziende, tramite trojan ransomware come CryptoLocker. Questi frammenti di codice dannosi sono in grado di crittografare dati, file o addirittura interi sistemi generando una coppia di chiavi private-pubbliche. Sarà impossibile decrittografare i dati senza disporre della chiave privata, che è memorizzata nel server dell'autore degli attacchi. Sarà necessario pagarla per sbloccare il ransom.

La migliore strategia per proteggere le aziende da questo tipo di minacce è utilizzare un software antivirus e di protezione aggiornato, una soluzione di ripristino avanzata ed educare gli utenti a non aprire le email di phishing, che rappresentano spesso l'origine di questi virus. Nel malaugurato caso in cui un'azienda dovesse essere vittima di un attacco di ransomware, Zerto può aiutare ad attenuare i rischi di perdita dei dati offrendo i seguenti vantaggi:

- Ripristino dei sistemi all'ultimo point-in-time prima che l'infezione si diffonda, nel giro di pochi secondi.
- Ripristino di tutti i sistemi critici nel giro di pochi minuti, con pochi semplici clic.
- Ripristino di interi database e applicazioni in modo uniforme, ma anche ripristino di singoli file.
- Esecuzione di test di failover senza interruzioni in qualsiasi momento, per accertarsi che l'azienda possa tornare subito online quando necessario.
- Creazione di copie di dati off-site per la conservazione a lungo termine, offrendo alle aziende una soluzione di Continuous Data Protection per un massimo di 14 giorni.

BusinessContinuity

Molte aziende hanno implementato un **sito di disaster recovery** remoto, in cui i dati vengono replicati in modo continuo, pronti per essere recuperati in caso di interruzioni dell'attività. Se il sito di disaster recovery si trova in una località remota, può anche fornire **business continuity (BC)**, ovvero la capacità di un'azienda di continuare ad operare dopo una catastrofe, ad esempio un incendio, interruzioni di corrente o calamità naturali. Nel caso in cui il sito originale fosse inattivo, i servizi sul sito di produzione possono essere svolti nel sito di disaster recovery. Il processo di passaggio è denominato failover. Quando il normale sito di produzione ritorna attivo e operativo, il lavoro svolto presso il sito di disaster recovery deve essere replicato nuovamente per garantire che tutto il lavoro non vada perso. In questo caso, viene eseguito il cosiddetto **failback** delle applicazioni e dei dati dal sito di disaster recovery al sito di produzione, una caratteristica essenziale di una buona soluzione di DR.

In passato i siti di disaster recovery erano una copia del sito di produzione ubicata presso altre sedi fisiche dell'azienda, oggi invece si possono trovare presso il data center di un fornitore di servizi cloud o nel public cloud.

CONCETTI DI RTO E RPO

Tutte le aziende **quotate in borsa** devono garantire la conformità con le normative in materia di sicurezza dei dati; la perdita dei dati si traduce in perdita di guadagni, reputazione e valore per gli azionisti.

Se un'impresa che svolge **attività online** dovesse perdere 4 ore di dati aziendali potrebbe ritrovarsi con clienti infuriati che temono di subire ritardi nella consegna delle merci che hanno acquistato.

Se i sistemi di un'**azienda di trasporti** sono inattivi per qualche ora, sarà praticamente impossibile programmare consegne e ritiri in modo efficiente, con conseguenti effetti negativi sui guadagni, che di per sé sono già sotto pressione.

I processi di produzione robotizzati che restano inattivi in seguito a un guasto dell'hardware o del software causano enormi perdite in termini di produttività e fatturato.

RTO e RPO

Quando si parla di esigenze aziendali, tradotte in SLA (Service Level Agreement), il ripristino è in genere espresso in due tipi di obiettivi: RTO e RPO. **RTO (Recovery Time Objective)** indica il tempo totale in cui l'azienda può fare a meno del servizio da ripristinare, senza perdite o rischi significativi. **RPO (Recovery Point Objective)** indica il più recente point-in-time da cui è possibile ripristinare i dati. Le tecnologie di backup o snapshot tradizionali offrono RPO che variano da 15 minuti a 24 ore. Nei moderni ambienti digitali di classe enterprise, sia l'RTO che l'RPO devono essere quanto più bassi possibile, nel senso che non possono più essere espressi in ore, ma in minuti o addirittura secondi. Sebbene molte aziende si concentrano sull'RTO per far tornare operativa l'azienda nei tempi più brevi possibili, è molto più impattante la perdita dei dati (RPO) perche' dopo una catastrofe mette a rischio sul lungo termine la credibilita' aziendale.

High Availability

Un concetto che viene spesso confuso con disaster recovery e business continuity è quello di **high availability (HA)**. Si tratta di una funzionalità che permette di evitare i tempi di inattività causati da problemi dell'hardware e implica tecnologie quali RAID e parti ridondanti come alimentatori e cavi, ma che può essere applicata anche negli ambienti virtualizzati. Le tecnologie di HA sono necessarie per mantenere i sistemi in funzione, tuttavia non sono utili per eseguire un ripristino dopo una catastrofe. High availability è un concetto per lo più espresso in percentuale, intorno al 99%. Tuttavia bisogna tener presente che un tempo di attività parti al 99,9% indica che un sistema è soggetto comunque a 8 ore di tempi di inattività su un periodo di un anno.

HIGH AVAILABILITY IN % E TEMPO *(fonte: Wikipedia)*

% di availability	Tempi di inattività all'anno	A settimana
90% ("one nine")	36.5 days	16.8 hours
99% ("two nines")	3.65 days	1.68 hours
99.9% ("three nines")	8.76 hours	10.1 minutes
99.99% ("four nines")	52.56 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	6.05 seconds

Disaster Recovery Come Strategia di Business

Poiché la perdita dei dati e i tempi di inattività hanno un impatto diretto sulle aziende, il disaster recovery è una problematica che andrebbe discussa basandosi su criteri e obiettivi di business strategico. A domande quali "Quanto tempo di inattività un'azienda è in grado di sopportare?" e "Quanti dati possono essere persi?" prima di causare danni irreversibili (impostando RTO e RPO) è impossibile rispondere soltanto da una prospettiva tecnica. Le risposte variano in base ai flussi di guadagno che derivano dai sistemi IT, dal valore associato ai dati aziendali, dalla logistica e da altri processi di business che dipendono direttamente dall'IT. In breve, poiché sono coinvolte numerose tecnologie, il disaster recovery rappresenta un elemento chiave per soddisfare appieno gli obiettivi di business.

Primo Obiettivo: Decidere Cosa è Realmente Business-Critical

Quando si tratta di sviluppare una strategia di disaster recovery, è importante tenere presente che non tutti i sistemi, applicazioni e dati hanno lo stesso valore critico per un'azienda. Nel caso delle applicazioni principali, è fondamentale adottare una strategia di disaster recovery solida che preveda un sito di DR remoto, RTO/RPO bassi e un piano di ripristino collaudato. Nel caso di altre applicazioni e tipi di dati, è accettabile implementare soluzioni meno costose e RPO/RTO più elevati.

Nella pianificazione del disaster recovery, è assolutamente necessario assegnare priorità a ciò che è più importante. È necessario stabilire quanto tempo di inattività può essere tollerato per ogni applicazione discutendone con i responsabili delle linee di business. In questo modo, sarà possibile sapere quanto prima quali sono quelle che devono garantire una maggiore availability con perdite di dati minime. È molto probabile, infatti, che vi siano applicazioni di cui un'azienda può fare a meno per diverse ore. In questa fase, è essenziale stabilire i livelli di servizio su tutti i fronti, in modo da evitare brutte sorprese in una situazione di emergenza.

Un piano di BC/DR è una Decisione Finanziaria

Per progettare una soluzione di DR, sono disponibili diverse strutture e molte soluzioni. Ognuna di queste presenta un costo. La soluzione più economica è probabilmente un software di backup tradizionale, che tuttavia si rivela inadeguata a garantire la sicurezza degli ambienti moderni. Quando si implementa un sito di DR remoto, è possibile scegliere tra una replica del sito di produzione presso un'altra sede o un servizio basato su cloud (DRaaS). La scelta di una di queste due soluzioni implica anche una scelta tra CAPEX e OPEX, ovvero tra i costi in conto capitale e i costi operativi di un servizio online.

Un'altra considerazione da fare è il numero di strumenti da includere nel piano di BC/DR. Un piano di DR basato su numerose tecnologie complesse implicherà necessariamente un processo di ripristino complesso e difficoltoso. In situazioni di emergenza, l'utilizzo di diversi strumenti può causare errori e quindi ingenti spese.

Il Disaster Recovery Richiede Amministrazione

Quando si tratta di DR, le aziende di grandi dimensioni devono far fronte anche a problematiche di conformità e amministrazione. Le normative in materia di dati diventano sempre più rigorose e garantire la conformità con queste deve rientrare in una strategia di DR al pari degli altri elementi.

Per garantire la conformità, le procedure devono essere documentate e le soluzioni devono essere collaudate e affidabili. Per decidere correttamente se è possibile archiviare i dati nel cloud, tenendo presente dove si trova il servizio cloud e chi controlla tale servizio, è necessario tenere conto anche delle normative a cui un'azienda deve conformarsi.

Tecnologie di Disaster Recovery e Ambienti Virtualizzati

La virtualizzazione del data center ha realmente rivoluzionato il mondo dell'IT, offrendo maggiore flessibilità e controllo nella gestione dei carichi di lavoro di produzione, oltre a semplificare notevolmente l'implementazione e il supporto operativo. Per sfruttare appieno i vantaggi di questo ambiente software-defined (private o hybrid cloud), le aziende devono ottimizzare tutti i processi e le attività dell'IT per la sicurezza, la conformità e il binomio business continuity/disaster recovery (BC/DR) dell'ambiente virtuale. Quando si tratta di prendere decisioni in merito a BC/DR, molte aziende considerano questo aspetto come una polizza assicurativa costosa, proprio perché in molti casi le soluzioni disponibili sono estremamente costose e inadeguate in un ambiente virtualizzato.

Hardware e Software

Molte soluzioni di DR sono progettate per ridurre al minimo i tempi di inattività causati da guasti dell'hardware, interruzioni di corrente o calamità naturali. La maggior parte dei problemi dei data center non è causata interamente dalla loro interruzione. Ai reparti IT viene richiesto spesso di ripristinare un file eliminato involontariamente o una singola virtual machine che non funziona più correttamente oppure altri eventi di minore entità. In altre parole, le catastrofi non sono sempre causate da guasti dell'hardware né possono essere risolte direttamente da soluzioni hardware.

Che cosa differenzia il binomio BC/DR in un ambiente virtualizzato?

- **Software-defined** – in un ambiente virtuale, la replicazione al livello dell'hardware non è sufficiente. La replica deve essere eseguita nell'hypervisor, in modo da soddisfare sempre le esigenze aziendali in situazioni di emergenza. Gli utenti finali non cercano una storage unit logica, ma l'applicazione: Oracle, Microsoft Exchange e così via.
- **Progettati per gli ambienti virtualizzati** – l'adozione di una strategia di virtualizzazione richiede che anche la soluzione di disaster recovery sia progettata appositamente per le esigenze della virtualizzazione. In questo modo, si garantisce che le eventuali modifiche apportate nell'ambiente di produzione vengano applicate anche alla strategia di disaster recovery, senza compromettere la protezione e contando sempre sulla flessibilità e agilità offerte dalla virtualizzazione.
- **Uniformità delle applicazioni** – molte applicazioni business-critical utilizzano più virtual machine, ognuna delle quali interdipendente. In altre parole, è necessario replicarle insieme per garantirne la conformità.
- **Scalabilità** - è essenziale adottare una soluzione ideata appositamente per proteggere molte virtual machine. I dati e le applicazioni aumentano a ritmi esponenziali. La soluzione di DR deve avere la capacità di scalare con la crescita senza aggiungere complessità e overhead.
- **Trasformazione** – a causa della loro natura dinamica, gli ambienti virtuali tendono a proliferare, rendendo la business continuity e il disaster recovery più complessi.
- **Granularità** – per rispondere in modo efficiente alle principali cause di violazioni dei dati, ad esempio danneggiamento dei dati ed errori commessi accidentalmente dagli utenti, la granularità è un elemento necessario per ripristinare singole virtual machine o file.
- **Frequenza** – oggi gli ambienti IT, e non solo quelli virtualizzati, sono fondamentali per la sopravvivenza delle aziende; la replicazione delle virtual machine, dei dati e dei file deve essere eseguita con una certa frequenza. Un backup giornaliero non basta.

Soluzioni di Disaster Recovery Disponibili

Nel corso degli anni, sono state introdotte diverse soluzioni di DR di tipo disk-to-disk, ma nessuna di queste è stata progettata appositamente per la virtualizzazione. In una breve panoramica, riassumeremo le loro strutture e lacune in un ambiente virtualizzato.

Replica basata su array

I prodotti di replica basata su array sono forniti dagli storage vendor e sono implementati come moduli nello storage array. Si tratta di soluzioni distribuite da un singolo vendor, compatibili solo con la soluzione di storage specifica già in uso. La relazione tra la virtual machine e lo storage è fissa e implica la replica dell'intera LUN, indipendentemente dal fatto che venga utilizzata al 40% o al 90%.

- **Hardware-defined** – La replica basata su array è progettata per replicare entità fisiche. Non rileva le virtual machine né le modifiche alla configurazione.
- **Non indipendente** – Sebbene sia ottimizzata per il funzionamento con lo storage array esistente, vincola l'azienda a un unico vendor.
- **Più punti di gestione** – Oltre alla console di gestione dello storage array fisico, l'IT deve gestire le risorse virtuali anche da una console di gestione della virtualizzazione.
- **Crescita e trasformazione** – Tla relazione tra la virtual machine e lo storage è fissa, eliminando la flessibilità della virtualizzazione e la capacità di rispondere alle esigenze aziendali in continua evoluzione.
- **Granularità** – Replicando l'intera LUN, la replica basata su array non offre la granularità necessaria in un ambiente virtuale
- **Costi** – Viene replicata l'intera LUN, indipendentemente dal fatto che sia utilizzata al 40% o al 90%, aumentando il consumo energetico, i tempi di raffreddamento, la connettività di rete e i costi di storage.
- **Unico punto per il ripristino** – Molte soluzioni basate su array non sono in grado di archiviare una cronologia delle prestazioni della LUN. A causa di questa limitazione, nel caso in cui l'ultimo data point dovesse danneggiarsi, sarà impossibile fare riferimento all'ultimo punto che l'azienda deve utilizzare per il ripristino, rendendo la soluzione di DR inutilizzabile..
- **Tempi** – Il ripristino è un'operazione complessa che richiede molto tempo in quanto non offre automazione, quindi le virtual machine e le applicazioni devono essere ricreate da zero..

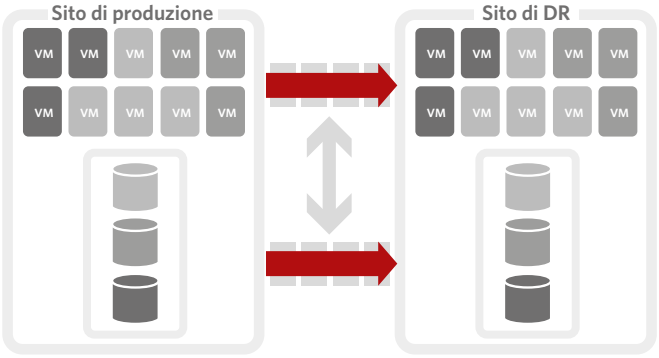


Figura 1. La replica basata su array e su appliance richiede il coordinamento di due prodotti di replica, sia per l'ambiente fisico che per quello virtualizzato. Di conseguenza, aumenta la complessità di gestione e si compromettono gli investimenti effettuati per la virtualizzazione.

Replica Basata su Appliance

Anche le soluzioni basate su appliance utilizzano hardware e sono specifiche di un'unica piattaforma. La principale differenza è che la replica viene eseguita in un appliance fisico esterno anziché nello storage array stesso. Questo tipo di replica, quindi, risulta più flessibile e consuma una quantità inferiore di risorse degli array. Tuttavia, gli svantaggi sono più o meno gli stessi della replica basata su array.

- **Hardware-defined** - È inoltre progettata per replicare entità fisiche anziché entità virtuali.
- **Non indipendente** - Sebbene sia più flessibile della replica basata su array, è comunque progettata specificamente per un'unica piattaforma.
- **Più punti di gestione** - La replica basata su appliance richiede due punti di gestione: la console di gestione fisica e la console di gestione della virtualizzazione.
- **Crescita e trasformazione** - Non rileva le modifiche alla configurazione. Di conseguenza, i piani di BC/DR non saranno armonizzati con l'attuale ambiente di produzione, eliminando la flessibilità della virtualizzazione e la capacità di rispondere alle esigenze aziendali in continua evoluzione.
- **Granularità** - La replica basata su appliance è incentrata sull'unità logica anziché sulla virtual machine. Questa assenza di granularità è in conflitto con i requisiti e le promesse della virtualizzazione.
- **Costi** - Poiché viene replicata l'intera LUN, i costi di elettricità, raffreddamento, storage e connettività di rete aumentano.

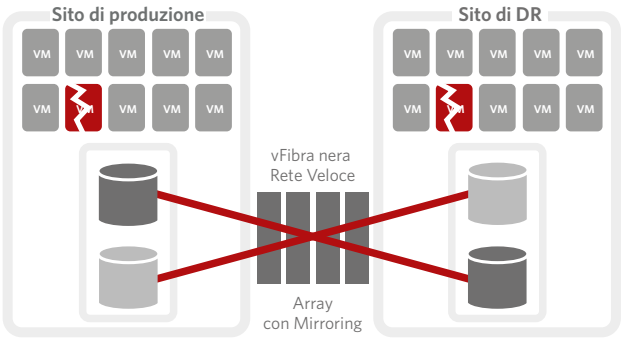


Figura 2. Eseguendo il mirroring su una rete veloce, è disponibile un'elevata high availability, tuttavia vengono replicati anche i componenti software danneggiati.

Replica Sincrona

Un'altra opzione è disporre di una copia completa di un'infrastruttura in un altro luogo, copiando o eseguendo lo striping di ogni scrittura anche in tale luogo. In caso di emergenza, viene avviato un failover automatico, facendo assumere il controllo all'infrastruttura remota. Questa opzione di replica sincrona, offerta ad esempio da MetroCluster di NetApp, sembra essere la soluzione perfetta, sebbene costosa; tuttavia è totalmente basata su hardware e si tratta più di una soluzione di high availability (HA) che di disaster recovery. Il failover si rivela utile in caso di guasto dell'hardware, interruzione di corrente o calamità naturale, ma se il problema deriva da un database danneggiato, un virus o qualsiasi altra problematica basata su software, gli errori verranno replicati anche nel sito remoto. In questo caso, la replica risulta inutile, e il team dovrà eseguire il ripristino servendosi del backup notturno.

- **Vendor lock-in**: È necessaria una copia esatta dell'hardware, offerta dallo stesso vendor e ubicata in un altro luogo.
- **Costosa** – Ovviamente, questa è una soluzione piuttosto costosa, comportando il raddoppio dei costi hardware e richiede una soluzione di connettività di rete con una notevole quantità di larghezza di banda.
- **Incompleta** – Totalmente hardware-based; in caso di catastrofe di tipo software-based, richiede il fallback tramite snapshot.

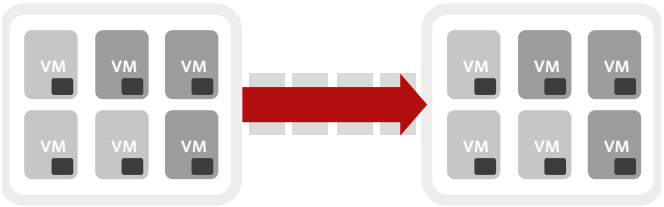


Figura 3. La replica basata su host richiede un agent in ciascuna virtual machine, aumentando notevolmente la complessità.

Replica basata su guest/sistema operativo

In una soluzione di replica basata su guest/sistema operativo, è necessario installare i componenti software in ogni singolo server fisico e virtuale. Sebbene si tratti di un metodo meno complesso rispetto alle soluzioni basate su array, le soluzioni di replica basate su guest/sistema operativo non sono adatte per le imprese.

- **Crescita e trasformazione** - La necessità di installare un modulo in ogni singolo server limita la scalabilità e rende impossibile l'implementazione e la gestione in ambienti a scalabilità elevata di classe enterprise. Inoltre, l'overhead di ciascun agent nella virtual machine potrebbe presentare problemi in termini di prestazioni per le applicazioni a cui l'azienda fa affidamento.
- **Complessità** - In molti casi, le virtual machine di tipo shadow fanno parte dell'implementazione, aumentando il carico di lavoro e la complessità di gestione.
- **Nessuna uniformità delle applicazioni** - Ogni virtual machine è protetta singolarmente, rendendo impossibile la gestione dei gruppi di virtual machine per un'applicazione e la relativa replica in modo uniforme.
- **Overhead di gestione** - Tutti gli agent devono essere gestiti e sono soggetti a manutenzione. Un ambiente composto da un numero esiguo di virtual machine non crea particolari problemi, tuttavia se nell'ambiente sono presenti oltre venti virtual machine, la gestione e la manutenzione, inclusi i riavvii dei guest, hanno un impatto decisamente più negativo sul business. Le operazioni di manutenzione e aggiornamento contemplate nella strategia di DR hanno ormai una cadenza settimanale, e spesso richiedono tempi di inattività.

Snapshot

Molte soluzioni utilizzano le snapshot come metodo per abilitare un ripristino rapido. Una snapshot è un metodo che consente di "bloccare" un sistema di storage o una virtual machine attiva in un dato momento nel tempo. In seguito all'acquisizione delle snapshot, si continua ad apportare modifiche ai file. Se le modifiche vengono apportate in seguito all'acquisizione delle snapshot e nella virtual machine o nel sistema di storage si riscontra un problema, viene data la possibilità di rifiutare tali modifiche ripristinando la virtual machine o il sistema di storage al momento della creazione delle snapshot. Una snapshot si rivela particolarmente utile quando si apportano modifiche a una singola virtual machine in cui è necessario procedere con un rollback.

Sono disponibili due tipi di snapshot: **snapshot di storage**, basate hardware, e **snapshot di hypervisor**.

Storage Snapshots: expensive

Le snapshot di storage sono istantanee del volume di storage nel suo complesso. Le dimensioni delle snapshot possono aumentare in modo esponenziale, utilizzando una grande quantità di spazio di storage di tier 1. Non e' insolito ritrovarsi con richieste di un 30% aggiuntivo sul volume dati. Ciò si verifica in special modo quando sono presenti numerose modifiche ai dati nello storage dopo aver acquisito la prima snapshot. Inoltre, la maggior parte delle tecnologie snapshot di storage è basata sul disco originale.

Snapshot di virtual machine: Incomplete

Le snapshot di virtual machine sono valide solo per le singole e specifiche virtual machine e non creano copie delle virtual machine. Si tratta semplicemente di un file che consente di ripristinare uno stato precedente di una virtual machine già esistente (analogamente alla maggior parte delle tecnologie snapshot basate su storage, tuttavia in questo caso fanno riferimento all'intero volume di storage e non a una singola virtual machine). Non sono protette in caso di guasto dell'hardware. Se si perdono i file che contengono una virtual machine, i file della snapshot associata diventano inutilizzabili.

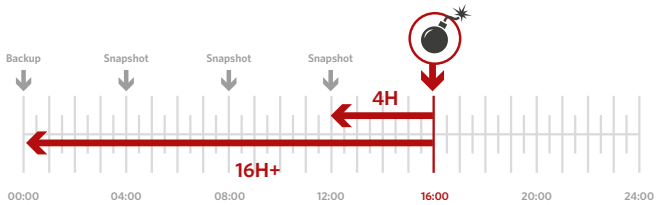


Figura 4. Sebbene le snapshot riducano l'RPO, in genere vengono acquisite ogni 4 o 8 ore (in caso contrario, influirebbero notevolmente sulle prestazioni e sullo spazio su disco disponibile). Offrono un RPO migliore rispetto a un backup tradizionale, tuttavia resta la probabilità di perdere fino a 4 o 8 ore di lavoro in caso di incidente.

La domanda da porsi è la seguente: le snapshot sono adeguate come soluzione di DR?

- **Nessun DR reale** – Sle snapshot sono utilizzate per salvare un point-in-time temporaneo, non per una soluzione a lungo termine. Per creare una copia di una virtual machine da archiviare, è necessario un backup o un sito di DR, non una snapshot.
- **Prestazioni** – Le snapshot di virtual machine hanno un enorme impatto sulle prestazioni di una virtual machine, e possono anche influire sull'intero ambiente con ulteriore overhead di hypervisor e storage.
- **Gestione** – Large numbers of snapshots are difficult to manage.
- **Frequenza** – : poiché in genere le snapshot vengono acquisite ogni 4 ore (una maggiore frequenza potrebbe avere un forte impatto sulle prestazioni e sullo storage), è possibile che 4 ore di dati vadano persi dopo il rollback (vedere figura 4). Un RPO di 15 minuti può andare bene per ambienti di piccolissime dimensioni; negli ambienti moderni è necessario adottare una soluzione di replica continua, senza influire sulle prestazioni dell'ambiente di produzione.
- **Snapshot e cloud** – Sebbene alcune soluzioni di DR utilizzino snapshot e le archivino in un ambiente cloud (DRaaS), è comunque necessario creare la snapshot nell'ambiente di produzione prima che venga replicata nel cloud. In questo modo, l'impatto su storage e prestazioni non varia. Un altro aspetto importante da conoscere è il tipo di snapshot utilizzato da tali soluzioni: è una snapshot di storage o una snapshot di virtual machine? Le tecnologie snapshot basate su storage richiedono lo stesso hardware, limitando i provider di cloud e i cicli di vita dell'hardware tra le due organizzazioni coinvolte.

Replica Basata su Hypervisor

Tutte queste categorie di tecnologie di replica presentano limitazioni critiche in un contesto virtuale. Per questo motivo, compromettono le promesse della virtualizzazione, limitandone le funzionalità. Per sfruttare appieno gli investimenti effettuati per la virtualizzazione senza compromettere la business continuity e il disaster recovery, è necessario un nuovo approccio: la replica basata su hypervisor. Zerto ha sviluppato la replica al di là dello stack, dal livello di storage, sopra il livello di astrazione delle risorse al livello di virtualizzazione/hypervisor. Nella **Sezione 2** si spiega in che modo l'innovativa soluzione di replica basata su hypervisor di Zerto offra replica virtuale e funzionalità di BC/DR di classe enterprise per il data center e il cloud.

Disaster Recovery Offerto Dagli Hypervisor

I vendor di hypervisor, ad esempio VMware, offrono le proprie soluzioni di replica basate su software, limitandole al proprio hypervisor. Una soluzione come VMware vSphere Replication (VR) offre funzionalità di replica limitate e non include tutte le funzioni di coordinamento, test, generazione di report e disaster recovery di classe enterprise necessarie. Anche se combinata con VMware Site Recovery Manager (SRM), i tempi di ripristino e la scalabilità potrebbero non essere sufficienti a soddisfare le esigenze di business. Sebbene SRM offra funzionalità di pianificazione, test ed esecuzione di un disaster recovery, non riesce a sopperire alle limitazioni di vSphere Replication, poiché quest'ultima soluzione è basata su tecnologia snapshot di virtual machine.

Disaster recovery e cloud

Il cloud computing diventa sempre più una necessità, quindi le aziende di qualsiasi dimensione stanno cercando di implementare il public, l'hybrid o il private cloud nella propria soluzione di BC/DR. La virtualizzazione ha dato vita a un'opportunità, tuttavia in base alla soluzione adottata potrebbero sussistere ancora notevoli divari tecnologici. Le applicazioni mission-critical possono essere virtualizzate e gestite in modo efficiente; tuttavia, non se ne può garantire la giusta protezione in un ambiente cloud se non vengono implementati gli strumenti appropriati.

Disaster Recovery as a Service (DRaaS)

Il cloud come soluzione di DR è una scelta intelligente, poiché offre maggiore flessibilità e in genere presenta un costo più basso rispetto all'implementazione di un sito di DR di proprietà della stessa azienda. Quando si tratta di scegliere un provider di servizi cloud e un servizio DRaaS, è importante tenere presente che DRaaS non è una tecnologia, bensì un servizio basato su una delle tecnologie menzionate sopra. La sola differenza sta nel luogo in cui vengono archiviati i file di disaster recovery. In altre parole, se una soluzione è basata su snapshot, presenterà tutti gli svantaggi associati alle snapshot, tra cui impatto su prestazioni e storage nel sito di produzione. Ma soprattutto: un RPO di 15 minuti basato su snapshot non ne fa di certo la soluzione ideale.

Quando si tratta di scegliere un servizio DRaaS, è opportuno dare un'occhiata alla tecnologia su cui si basa il servizio, controllando che RTO e RPO offerti siano realistici e collaudati, senza dover sostenere ulteriori investimenti iniziali. Per facilitare la scelta, abbiamo messo a punto una checklist dei requisiti di DR e DRaaS, disponibile alla pagina successiva.

CHECKLIST DEI REQUISITI DI DISASTER RECOVERY

sia per soluzioni in-house che DRaaS

Prestazioni

1. La soluzione di DR offre replica continua? Qual è l'impatto sul sito di produzione in base alla tecnologia utilizzata (ad esempio snapshot)?
2. Quali RTO e RPO offre la soluzione? È misurato in secondi, minuti oppure ore? Le misurazioni possono essere provate? È possibile avere informazioni dettagliate continue su questi dati?
3. Le cifre di RPO/RTO soddisfano le esigenze di business in modo realistico, e a quali sacrifici o costi?
3. Do these RPO/RTO numbers realistically meet your business requirements, and at what sacrifices or costs?
4. **DRaaS** – il provider di servizi cloud offre una soluzione di connettività di rete veloce e affidabile? La soluzione DRaaS offre funzionalità efficienti quali la compressione?

Supporto dei sistemi

5. La soluzione di DR è indipendente dalla piattaforma di storage e dall'hypervisor? In altre parole: è possibile eseguire la replica da qualsiasi ambiente nella soluzione di DR?
6. Tiene conto delle applicazioni? Offre raggruppamenti di virtual machine uniformi con le applicazioni?
7. Qual è il livello di scalabilità della soluzione (offre scalabilità sia in verticale che in orizzontale in un ambiente DRaaS)?
8. Quali sono le caratteristiche dell'installazione? È necessario riconfigurare le applicazioni, le LUN, le virtual machine?
9. Supporta le modifiche, quando le virtual machine devono essere spostate in altre ubicazioni di storage o quando si desidera eseguire una migrazione?
10. **DRaaS** – Supporta più siti ed è multi-tenant? Offre flussi di dati isolati in modo sicuro per la conformità e le applicazioni business-critical?

Funzionalità

11. È una soluzione di protezione off-site completa, che offre sia DR sia storage di archiviazione (backup), con un impatto estremamente limitato sul sito di produzione?
12. È adatta sia per i guasti dei componenti hardware che logici?
13. Offre funzionalità di failover e failback sufficienti, tra cui automazione e coordinamento dei ripristini, script di pre- e post-ripristino, regolazione automatica degli indirizzi IP ecc.?
14. In caso di failover o failback, che impatto ha sulla produzione? Quali sono le caratteristiche del processo di failback? È simile al processo di failover?

Conformità

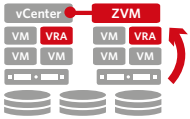
15. 15. Può essere facilmente sottoposta a test? Sono disponibili report dei test? Qual è l'impatto del test? Si tratta di attività che possono essere eseguite durante l'orario lavorativo o più adatte per i fine settimana? La produzione deve essere interrotta? La replica viene sospesa o interrotta durante i test, influendo sulla soluzione di DR nel corso di ogni test?
16. **DRaaS** – Si verificano problemi con le licenze? Sono previsti investimenti iniziali?
17. **DRaaS** – Dove vengono conservati i dati? Il provider di servizi è conforme con le normative UE?

Usabilità

18. È facile da apprendere e utilizzare? Aggiunge ulteriori punti di controllo di gestione all'ambiente oppure si integra senza problemi?
19. Offre la giusta granularità di ripristino? È possibile ripristinare un file, una singola virtual machine, una singola applicazione, un numero esiguo di applicazione o l'intero sito?
20. **DRaaS** – la soluzione DRaaS offre sia funzionalità self-service che servizi gestiti?

SEZIONE 2

La Rivoluzione di Zerto



Disaster Recovery a un Nuovo Livello

Zerto ha sviluppato la replica al di là dello stack, dal livello di storage al livello di virtualizzazione/hypervisor. Il risultato? Un'innovativa soluzione di replica progettata per ambienti virtualizzati basata su hypervisor che offre replica di classe enterprise e funzionalità di BC/DR per il data center e il cloud.

Replicazione Always-on

Zerto Virtual Replication replica continuamente gli I/O cosi' come sono stati creati in sorgente con un RPO di secondi.

Uniformità delle Applicazioni

Poiché le applicazioni sono spesso costituite da più virtual machine, Zerto ha sviluppato i cosiddetti VPG (Virtual Protection Group), una funzionalità esclusiva che abilita la replica contemporanea di più virtual machine come gruppo. La replica dei VPG consente di ripristinare l'intero gruppo da un singolo point-in-time, in modo uniforme, e rispettando l'ordine di scrittura.

Indipendente dalle Tecnologie

Zerto è indipendente da hypervisor e hardware, aprendo la strada all'innovazione e offrendo maggiore efficienza. Nessun accordo di esclusiva con un vendor, quindi è possibile utilizzare gli array e hypervisor più obsoleti o meno costosi per ridurre ulteriormente i costi. Inoltre, ora è più facile sfruttare o provare nuove e recenti tecnologie, ad esempio i flash array.

Scalabile e Granulare

Con una soluzione basata su software, scalare l'infrastruttura per supportare i processi di disaster recovery è un'operazione semplice e rapida. Quando si aggiunge un nuovo host virtuale, è sufficiente installare un nuovo appliance virtuale. Zerto Virtual Replication non si limita ad offrire la scalabilità necessaria per supportare ambienti di grandi dimensioni, ma anche lo stesso livello di granularità necessario per gli ambienti di qualsiasi dimensione, con la possibilità di ripristinare file, virtual machine, applicazioni e interi sit .

Semplicità di Gestione

La soluzione Zerto Virtual Replication può essere installata senza problemi nell'infrastruttura esistente, senza necessità di apportare modifiche alla configurazione nell'hypervisor, nell'applicazione e nello storage. La console è accessibile ovunque e offre una vista completa dell'ambiente, semplificando l'individuazione delle problematiche, che potranno essere risolte in modo decisamente più rapido. ZVR offre inoltre un avanzato pannello di controllo con un'interfaccia uniforme in tutte le piattaforme.

Semplicità di Ripristino

In caso di interruzione, è possibile avviare un semplice processo di failover e ripristino dalla stessa console. È facile testare, configurare ed eseguire l'automazione del disaster recovery. I test possono essere eseguiti senza alcun impatto sul sito di produzione o sulla replica. Sono inoltre disponibili report con i risultati del test per garantire la conformità.

Completa

Le funzionalità di Zerto si estendono a una soluzione completa per ambienti virtuali, supportando private, hybrid e public cloud con funzionalità di disaster recovery, conservazione a lungo termine, test e migrazione.

SEZIONE 3

Zerto Virtual Replication

Quando la produzione è virtualizzata, c'è un evidente divario nella strategia di protezione dei dati poiché in genere è basata su tecnologie obsolete che presentano limitazioni in termini di risorse fisiche. Zerto Virtual Replication armonizza la produzione con le strategie di disaster recovery grazie a una soluzione di replica basata su hypervisor.

In questa sezione, si descrive il funzionamento della tecnologia Zerto e i vantaggi che offre.

Architettura

La tecnologia di replica di Zerto si basa su due componenti:

- **Zerto Virtual Manager (ZVM)** – gestisce le funzionalità di disaster recovery, business continuity e off-site backup a livello del sito; si integra con VMware vCenter e/o Microsoft System Center Virtual Machine Manager, ed è dotato di un'opzione basata su browser.
- **Virtual Replication Appliance (VRA)** – replica le virtual machine e i dischi virtuali associati; per ogni host ESXi/Hyper-V, viene installata una VRA.

Come funziona la replica?

Zerto Virtual Replication Appliance (VRA) copia l'I/O creato prima che lasci l'hypervisor. La replicazione continua a livello di blocco offre RPO di pochi secondi, riducendo al minimo la perdita dei dati in caso di interruzioni.

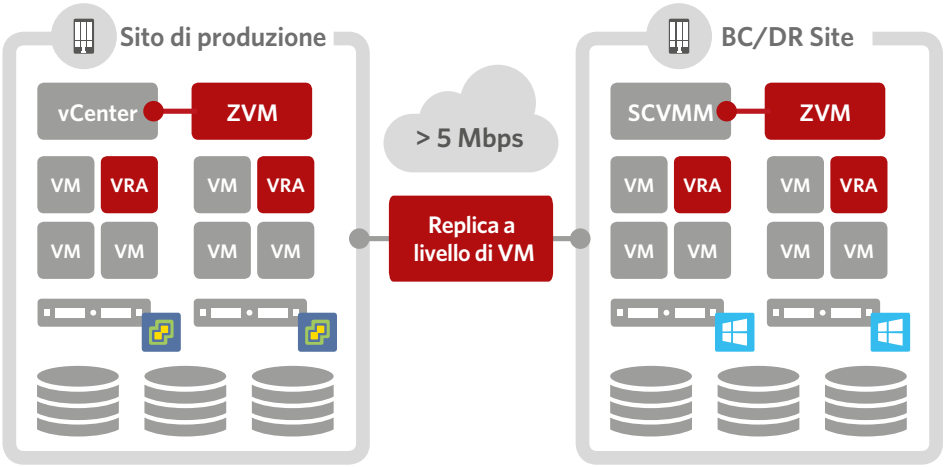


Figura 5. Architettura di Zerto

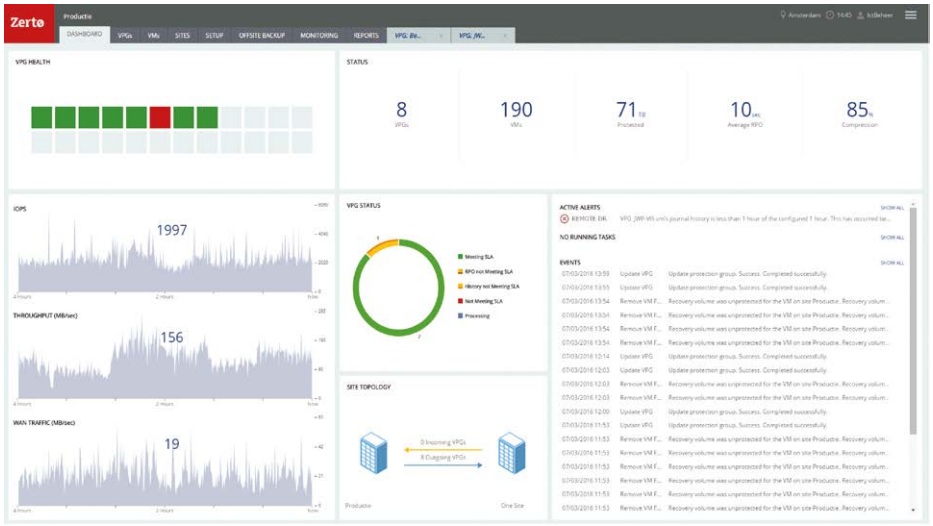


Figure 6. Zerto Virtual Manager interface

Caratteristiche e Vantaggi

- **Funzionalità di Journaling** - Offre una replicazione continua a livello di blocco senza alcun impatto sulle prestazioni delle applicazioni e con ripristino point-in-time con punti di ripristino compresi tra 1 ora ed un massimo di 30 giorni.
- **Indipendente da Hardware e Hypervisor** - Apre la strada all'innovazione con una soluzione di replica che non ha alcuna dipendenza da hardware o hypervisor.
- **Installazione Semplice e Senza Problemi** - Può essere installata facilmente nell'infrastruttura esistente senza richiedere tempi di inattività o modifiche alla configurazione.
- **Carichi di Lavoro di Produzione Protetti** - Garantisce uniformità delle applicazioni grazie ai gruppi di virtual machine protetti, gestiti, replicati e ripristinati come un'entità unica.
- **Scalabile** - Poiché si tratta di una soluzione basata su software, cresce insieme all'infrastruttura, indipendentemente dal ritmo di espansione dell'azienda.
- **Gestione Centralizzata Semplice** - Gestione centralizzata di due siti con Zerto Virtual Manager e di più siti con Zerto Cloud Manager.
- **Livelli di Servizio Estremamente Competitivi** - Offre RPO (Recovery Point Objective) di pochi secondi e RTO (Recovery Time Objective) di pochi minuti.
- **Coordinamento Completo** - Failover, failback, e protezione inversa automatizzati con pochi clic.
- **Test di DR Senza Interruzioni** - Verifica dell'intero processo di ripristino senza influire sugli ambienti di produzione o sulla replica continua, offrendo la certezza di poter ripristinare l'attività in situazioni di emergenza.
- **Supporto di Classe Enterprise** - Zerto offre servizi di assistenza di classe enterprise integrati in tutti i prodotti offerti. Tra i servizi si annoverano avvisi in tempo reale quando non si raggiungono gli obiettivi di RPO/RTO, avvertimenti in caso di riduzione delle prestazioni della rete e promemoria di verifica delle configurazioni e dei VPG. Le soluzioni Zerto sono supportate da centri di assistenza globali che offrono accesso on-demand a un team di tecnici esperti.

Gestione

Zerto Virtual Manager (ZVM) funziona tramite la console di gestione virtuale e offre una panoramica grafica delle virtual machine del sito e delle relative prestazioni. Se si verifica un problema, viene rappresentato visivamente. Vengono inoltre inviati avvisi al riguardo. Nelle schede ubicate nella parte superiore, tutte le altre funzionalità sono disponibili per il coordinamento e l'automazione dei processi di failback e ripristino, tra cui ordine di avvio, riassegnazione di indirizzi IP, test e opzioni di convalida.

Protezione incentrata sulle applicazioni: Virtual Protection Group (VPG)

Molte applicazioni di classe enterprise sono composte da più server virtuali: un web server, un application server, un database server ecc., ognuno dei quali interdipendente. Quando è necessario eseguire il ripristino, tutti i server devono essere ripristinati da un unico point-in-time uniforme. A tale scopo, Zerto ha sviluppato i cosiddetti VPG (Virtual Protection Group), che garantiscono uniformità nell'ambito di un gruppo di virtual machine. In questo modo, la soluzione Zerto garantisce che le applicazioni di classe enterprise vengano replicate e ripristinate in modo uniforme, indipendentemente dall'infrastruttura sottostante. Zerto Virtual Replication riconosce e preserva tali relazioni abilitando funzionalità di VMware importanti, tra cui DRS, vMotion e Storage vMotion.

- **Uniforme** – Replica e ripristina applicazioni basate su più virtual machine in modo uniforme.
- **Flessibile** – Consente alle aziende di implementare un'applicazione in diversi dispositivi fisici per aumentare al massimo le prestazioni e la capacità di ridurre la complessità dell'infrastruttura.
- **Granulare** – Offre tutta la granularità necessaria per ripristinare singole virtual machine e gruppi di virtual machine in diverse situazioni di emergenza.
- **Assegnazione di priorità** – Prioritize virtual protection groups for replication and recovery.
- **Supporto** – Supporta funzionalità di virtualizzazione quali vMotion, svMotion, HA ecc.

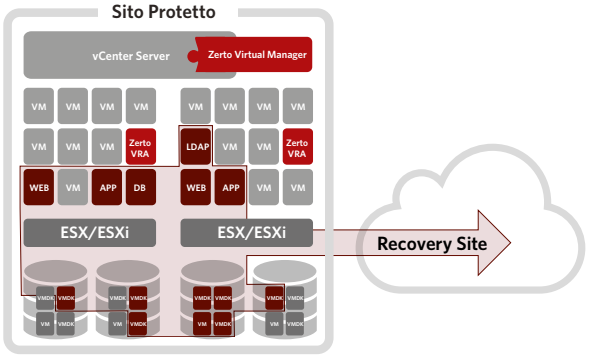


Figura 7. Le varie virtual machine che compongono un servizio applicativo si trovano in un Virtual Protection Group e sono replicate in modo uniforme anche se diffuse in più host e datastore.

Automazione e coordinamento completi

La replica dei dati nel sito di ripristino rappresenta solo una parte del problema. Le informazioni presenti nel sito, necessarie per proteggere un'azienda in caso di catastrofe, devono essere di facile utilizzo.

Zerto ha riconosciuto questa problematica e ha integrato processi automatizzati e coordinati che possono essere eseguiti con pochi clic quando il reparto IT deve affrontare una situazione di emergenza

Processo di failover completamente configurato

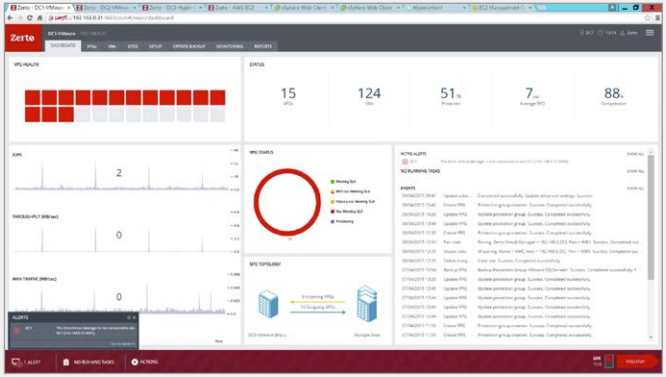
Parte della configurazione dei VPG richiede l'impostazione del processo di failover. Tra i parametri da configurare, si annoverano l'ordine di avvio, la riassegnazione di indirizzi IP in caso di failover, la lunghezza del journal e altre impostazioni. Grazie alla configurazione iniziale, si semplifica notevolmente il processo di ripristino, trasformandolo in un'operazione eseguibile con pochi clic.

Failover come decisione aziendale

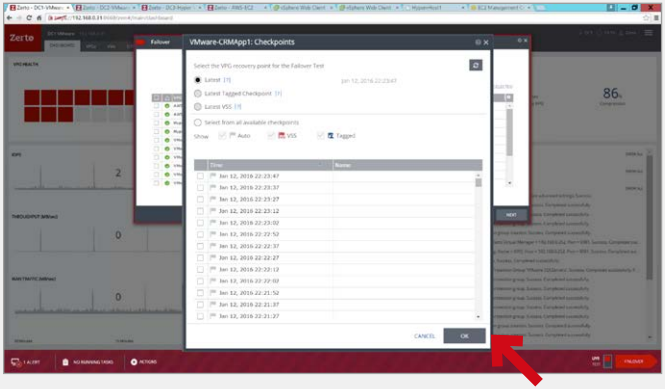
Poiché ogni catastrofe ha le proprie peculiarità, Zerto ritiene che il failover debba essere una decisione presa dall'azienda e non un processo automatizzato. Poiché è sempre possibile ripartire su un determinato istante nel tempo, questa fase di decisione è essenziale per un corretto failover. Dopo aver fatto clic sul pulsante del failover, viene avviato un processo automatizzato e coordinato per riportare i servizi online. Con una decisione a monte, è ad esempio possibile eseguire un failover con la possibilità di scegliere un point-in-time poco prima che si verifichi un danno al database.

PROCESSO DI FAILOVER IN 4 SEMPLICI PASSAGGI

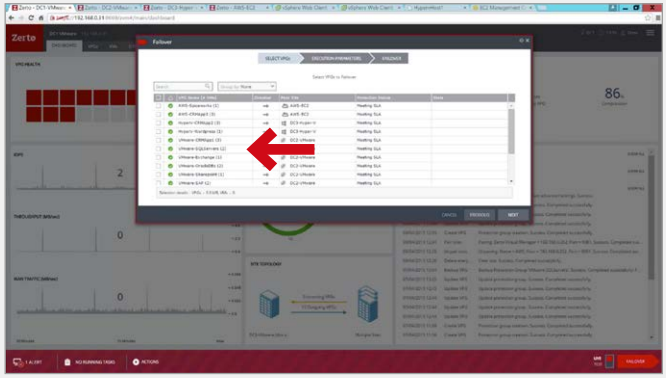
Il processo di failover si compone di quattro semplici passaggi. Dopo aver visualizzato un incidente nella console di gestione:



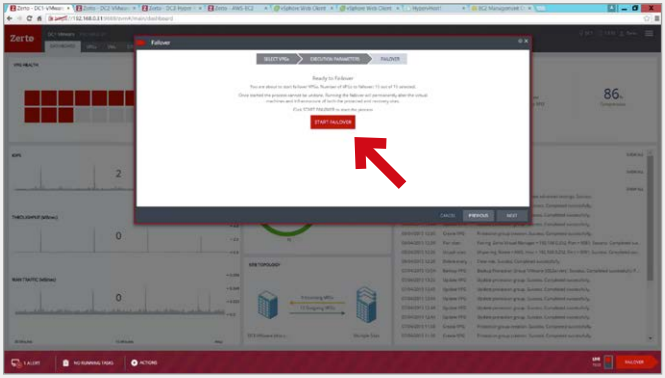
1. **Fare clic su Failover.**



3. **Verificare il point-in-time** in cui è necessario ripristinare le applicazioni. Per evitare che vengano ripristinate applicazioni danneggiate, è necessario tornare al punto in cui non erano danneggiate.



2. **Selezionare le applicazioni** (Virtual Protection Group) da recuperare dall'elenco.



4. **Avviare il processo di failover**. Il processo di failover viene avviato e le virtual machine vengono avviate e riconfigurate secondo necessità.

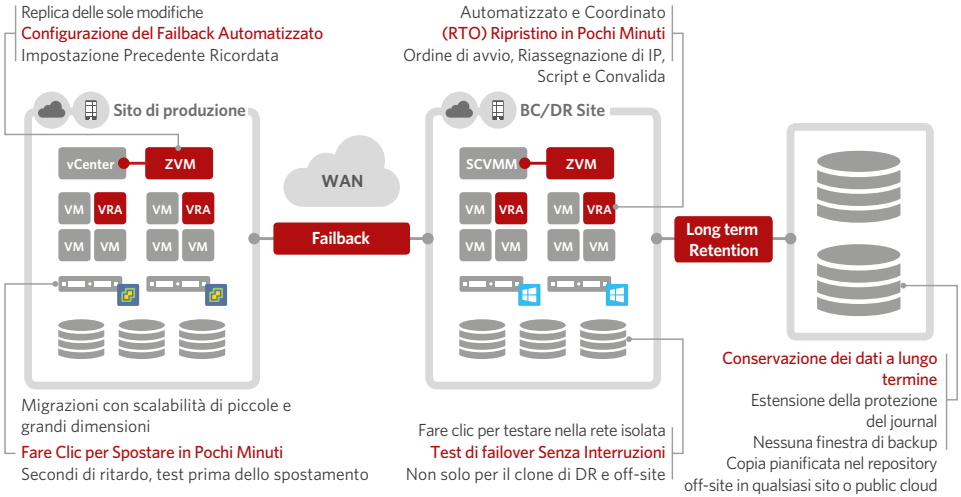


Figura 8. Per quanto riguarda il failback, l'architettura di Zerto offre automazione e coordinamento totali, oltre a test di failover senza interruzioni. La stessa funzionalità può essere utilizzata anche per il test delle sandbox e la migrazione dei dati. Per opzioni di protezione complete, i dati presso il sito di DR possono essere utilizzati anche per creare una copia di conservazione a lungo termine dei dati, senza influire sulla produzione.

Failover e Failback Automatizzati

Come già menzionato, la configurazione dei VPG permette di disporre di un piano di ripristino. Gli script di pre- e post-ripristino possono essere configurati anche in base a ogni singolo VPG. Ora, il failover e il failback possono essere eseguiti con pochi semplici clic. Anche quando il processo di disaster recovery è stato avviato, è comunque possibile eseguire il rollback del failover nel caso in cui vengano riscontrati problemi presso il sito di ripristino non correlato a Zerto, ad esempio quando una rete è inattiva. Una volta eseguito il failover, la protezione inversa semplifica ulteriormente il processo di failback. La protezione inversa inizia a sincronizzare il lavoro aggiuntivo svolto presso il sito di ripristino con il sito di produzione, quando quest'ultimo è pronto per l'utilizzo. Quando le applicazioni risultano aggiornate nel sito di produzione originale, anche in questo caso l'operazione di failback richiede pochi clic. Molte organizzazioni non procedono con il failover perché il failback è un'operazione complicata; con Zerto Virtual Replication tutto risulta più semplice.

PROVATE VOI STESSI

Scaricate una versione di valutazione gratuita all'indirizzo www.zerto.com/trial. Installate e configurate Zerto in meno di un'ora ed eseguite un test di failover in tutta autonomia con lo script di test fornito.

Test del Disaster Recovery Senza Interruzioni

Le aziende devono essere in grado di dimostrare che i processi di disaster recovery funzionino correttamente in situazioni di emergenza per garantire la conformità con i requisiti interni ed esterni. Zerto Virtual Replication consente di eseguire test senza interruzioni in un ambiente di sandbox, che dimostra nel dettaglio la buona riuscita di un'operazione di failover. Durante il test, l'ambiente risulta comunque protetto e la replica è ancora in corso. Ciò implica che il test di DR e la pianificazione delle risorse del personale non richiede più finestre di test nei fine settimana, perché nessuna parte dell'ambiente di produzione deve restare inattiva per l'intera durata del test.

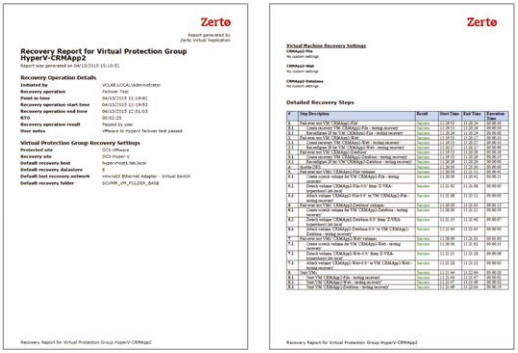


Figura 9. Risultati dei test di disaster recovery senza interruzioni nei report di audit che è possibile utilizzare per garantire conformità

Test di Sandbox

Con la funzione di test del failover, Zerto può anche creare un ambiente di test e sviluppo.

Migrazione dei Dati

Le migrazioni e i consolidamenti dei data center sono progetti che richiedono molto tempo ed enormi quantità di risorse che devono essere attentamente pianificate e programmate per tentare di ridurre al minimo i tempi di inattività e la perdita di produttività. Con la tecnologia di replica basata su hypervisor di Zerto, tuttavia, le migrazioni possono trasformarsi in attività indolori. Utilizzando gli attributi core di ZVR, le applicazioni virtualizzate possono essere verificate in anticipo e migrate nel giro di pochi minuti e con tempi di inattività ridotti al minimo.

- **Semplicità** – La migrazione delle virtual machine è un'operazione estremamente semplice, e lo stesso vale per l'associazione della replica al datastore di destinazione scelto, consentendo di replicare i dati nel nuovo sito in background dalle altre attività di business..
- **Granularità** – Le migrazioni possono essere molto granulari con la possibilità di migrare al livello di VM Disk (VMDK), che può essere associato a diversi storage tiere.
- **Flessibile** – Il supporto di un ambiente eterogeneo consente migrazioni tra diversi tipi di hardware e diverse versioni di VMware e Hyper-V, da un ambiente vCenter a un ambiente vCloud, e tra diverse versioni di ZVR.
- **Trasferimenti Automatizzati al 100%** – Sfruttando la configurazione VPG, trasferire virtual machine in una nuova posizione è un'operazione semplicissima che richiede soli pochi clic. In questo modo, si riducono notevolmente i tempi di inattività in pochi minuti, garantendo l'assenza di impatto sulle attività di generazione di utili.

Copie dei Dati con Conservazione a Lungo Termine

Poiché i dati vengono replicati nel sito di DR, è facile creare una copia off-site dei dati per la conservazione a lungo termine o per scopi di conformità. Questo processo e la relativa infrastruttura non fanno parte del sito di produzione, rimuovendo l'overhead e il carico di gestione, e possono essere gestiti dalla stessa interfaccia utente di ZVR.

Ripristino di File e Cartelle

Le situazioni di emergenza più comuni che richiedono un ripristino non sono rappresentate da calamità naturali o interruzione del sito, ma principalmente da file o cartelle persi o eliminati accidentalmente. ZVR ha risolto questa problematica offrendo la possibilità di ripristinare un unico file o cartella a una versione risalente fino a 14 giorni prima grazie al journal. La replicazione continua a livello di blocco offre punti di ripristino che permettono all'IT di risalire al punto precedente all'eliminazione o al danneggiamento del file e quindi di ripristinarlo. Questa operazione richiede solo pochi clic e il lavoro perso è davvero ridotto al minimo.

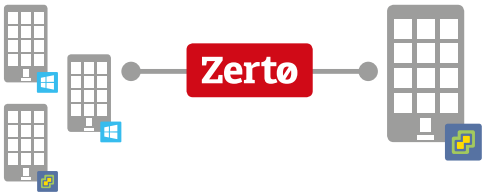
- **Rischio** – Riduce al minimo la perdita dei dati in file, folder, virtual machine, applicazioni e siti con la possibilità di ripristinare su qualsiasi livello, in qualsiasi point-in-time.
- **Semplicità** – Riduce il tempo medio di ripristino con la possibilità di usufruire di un workflow automatizzato per ripristinare file, applicazioni e dati.
- **Protezione della Produttività** - Quando si elimina involontariamente un file o una cartella, gli utenti finali non dovranno più sacrificare ore se non giorni del loro tempo per recuperare il lavoro perso, garantendo produttività continua e tenendo alto il morale dei dipendenti.

SEZIONE 4

Zerto Virtual Replication: Use Case

I vantaggi Zerto Virtual Replication sono disponibili per un'ampia gamma di use case. La tecnologia di base è indipendente dalle piattaforme di storage e supporta hypervisor misti: in altre parole, è possibile replicare qualunque sito in qualsiasi altro sito, indipendentemente dal fatto che si tratti di un private cloud, un public cloud, un fornitore di servizi o una filiale.

Da Private Cloud a Private Cloud
L'esempio più comune è configurare un sito di DR come versione remota del data center interno. Un aspetto meno tradizionale, invece, è rappresentato dalla possibilità di utilizzare qualsiasi tipo di storage, qualunque storage vendor e una combinazione di hypervisor. Zerto supporta tutto questo senza limiti di distanza.



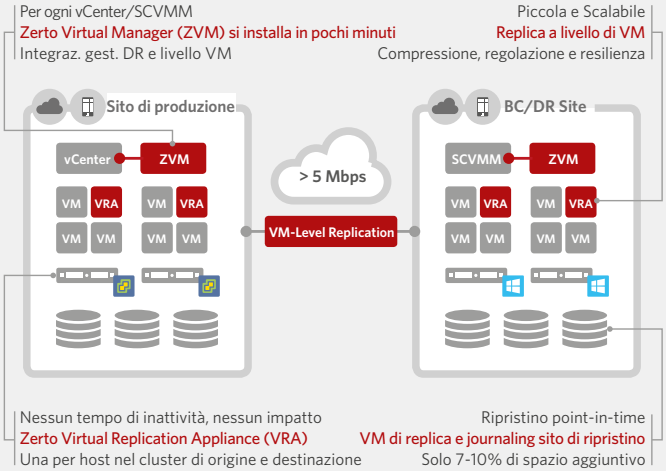
Protezione e Migrazione delle Filiali
Un altro use case prevede l'utilizzo di Zerto per la protezione o la migrazione di applicazioni tra le filiali di un'azienda. Anche in questo caso è possibile utilizzare qualsiasi tipo di storage, qualunque storage vendor e una combinazione di hypervisor.

Hybrid cloud, Disaster Recovery as a Service (DRaaS)
Diversi fornitori di servizi cloud offrono l'opportunità di utilizzare il cloud come sito di DR. In questo caso, si parla di DRaaS (Disaster Recovery as-a-Service) che, se basato su Zerto, offre tutti i vantaggi di Zerto. In questi servizi, è possibile controllare il disaster recovery da un portale self-service o gestirlo a distanza tramite il fornitore di servizi (Managed Disaster Recovery as-a-Service) o ancora utilizzare un private cloud come sito di DR per un sito di produzione basato su cloud.

DRaaS Self-Service
È inoltre possibile utilizzare un servizio di public cloud, ad esempio Amazon Web Services, come sito di DR. In tal caso, è necessario configurare autonomamente il servizio, come quando si configura un sito di DR remoto.

Zerto in Sintesi

ARCHITETTURA DI ZERTO



PERCHÉ NON PROVARE?

La soluzione Zerto Virtual Replication può essere installata, configurata e replicare virtual machine in meno di un'ora. La replica basata su virtual machine offre RPO di pochi secondi e RTO di pochi minuti. Visitate il sito web www.zerto.com/trial e fate clic per scaricare una versione di prova gratuita oggi stesso!

www.zerto.com/trial

CARATTERISTICHE

Replica basata su hypervisor - Replicazione continua a livello di blocco in hypervisor VMware e Microsoft su più siti.

Protezione granulare a livello di virtual machine - Protegge tutto quello che è necessario: virtual machine e VMDK/VHD.

Coordinamento totale - Automazione di failover, failback, protezione inversa e test di disaster recovery.

Protezione dei dati continua - Ripristino dei dati in una finestra che risale fino a 14 prima della situazione di emergenza, con checkpoint disponibili ogni paio di secondi.

Protezione dei dati completa - Un'unica soluzione per BC/DR per storage e hypervisor con conservazione a lungo termine.

Gestione semplice - Gestione centralizzata di due siti con Zerto Virtual Manager o di più siti con Zerto Cloud Manager.

Livelli di servizio estremamente competitivi - Offre RPO di pochi secondi e RTO di pochi minuti.

Installazione semplice - Richiede solo un'ora, senza apportare modifiche alle configurazioni di applicazioni e storage; progettata per offrire prestazioni impeccabili, non per il solo DR.

Carichi di lavoro di produzione protetti - Garantisce uniformità delle applicazioni grazie ai gruppi di virtual machine protetti, gestiti, replicati e ripristinati come un'entità unica.

Conservazione off-site - Aumenta l'utilità dei dati replicati con funzionalità di conservazione a lungo termine al livello del sito di replica.

Replica Indipendente dalle Piattaforme di Storage - Rimuove le barriere in ingresso con la replica indipendente dalle piattaforme di storage.

Supporto del public cloud - Replica, protezione e migrazione dei carichi di lavoro in servizi di public cloud come Amazon Web Services.

A Proposito di Clouditalia Telecomunicazioni

Clouditalia Telecomunicazioni è un'Azienda Italiana fondata nel Giugno del 2012, specializzata in servizi integrati di Telecomunicazione e Cloud Computing dedicati specificatamente ai bisogni delle piccole e medie imprese. L'Azienda dispone di una rete in fibra ottica proprietaria pari a 15.000 km lungo tutta la Nazione, e di 3 Datacenter ad Arezzo, Roma e Milano. Le filiali di Arezzo, Roma, Torino, Milano, Padova e Napoli contano ad oggi circa 250 dipendenti in totale.

Per offrire un servizio ICT che soddisfi le esigenze della piccolo e media Impresa italiana occorre una adeguata infrastruttura, un'esperienza tecnica specifica e la conoscenza approfondita di quali siano i reali bisogni dei clienti.

Clouditalia ha costruito la sua strategia su questi presupposti: la qualità dei servizi e delle tecnologie hardware e software impiegate sono amplificate dal supporto da parte dei nostri partner tecnologici, ognuno leader nel suo settore a livello globale.

CLOUDITALIA®

PERCHÉ NON PROVARE?

La soluzione Zerto Virtual Replication può essere installata, configurata e replicare virtual machine in meno di un'ora. La replica basata su virtual machine offre RPO di pochi secondi e RTO di pochi minuti. Visitate il sito web www.zerto.com/trial e fate clic per scaricare una versione di prova gratuita oggi stesso!

clouditalia.com