Data Protection Oracle

Enterprise applications

NetApp
January 12, 2026

Sommario

Data Protection Oracle

Data Protection con ONTAP

NetApp sa che i dati più mission-critical sono presenti nei database.

Un'azienda non può operare senza accesso ai propri dati, e a volte i dati definiscono l'azienda. Questi dati devono essere protetti; tuttavia, la protezione dei dati non è solo garanzia di un backup utilizzabile, ma consiste nell'eseguire i backup in modo rapido e affidabile, oltre a memorizzarli in modo sicuro.

L'altro lato della protezione dei dati è la recovery. Quando i dati sono inaccessibili, l'azienda ne è interessata e potrebbe non funzionare fino a quando i dati non vengono ripristinati. Questo processo deve essere rapido e affidabile. Infine, la maggior parte dei database deve essere protetta dai disastri, il che significa mantenere una replica del database. La replica deve essere sufficientemente aggiornata. Rendere la replica un database completamente operativo deve anche essere semplice e veloce.

Questa documentazione sostituisce il report tecnico precedentemente pubblicato *TR-4591: Data Protection di Oracle: Backup, recovery e replica.*

Pianificazione

La corretta architettura di protezione dei dati aziendali dipende dai requisiti di business correlati a conservazione dei dati, ripristinabilità e tolleranza per le interruzioni durante i vari eventi.

Ad esempio, consideriamo il numero di applicazioni, database e set di dati importanti inclusi nell'ambito della fornitura. La costruzione di una strategia di backup per un singolo set di dati che garantisca la conformità con gli SLA tipici è piuttosto semplice, perché non ci sono molti oggetti da gestire. Con l'aumento del numero di set di dati, il monitoraggio diventa più complicato e gli amministratori potrebbero essere costretti a spendere una crescente quantità di tempo nella risoluzione degli errori di backup. Quando un ambiente raggiunge il cloud e scala un service provider, è necessario un approccio completamente diverso.

Anche le dimensioni del set di dati influiscono sulla strategia. Ad esempio, esistono molte opzioni per il backup e il ripristino con un database da 100GB TB perché il set di dati è così piccolo. La semplice copia dei dati dai supporti di backup con gli strumenti tradizionali in genere offre un RTO sufficiente per il recovery. Un database 100TB ha normalmente bisogno di una strategia completamente diversa, a meno che l'RTO non consenta un'interruzione di più giorni, nel qual caso una tradizionale procedura di backup e ripristino basata sulla copia potrebbe essere accettabile.

Infine, vi sono alcuni fattori che esulano dal processo di backup e ripristino stesso. Ad esempio, esistono database che supportano attività di produzione critiche e che rendono il ripristino una rara eventualità che viene eseguita solo da DBA esperti? In alternativa, i database fanno parte di un grande ambiente di sviluppo in cui il ripristino è un evento frequente e gestito da un team IT generico?

RTO, RPO e pianificazione SLA

ONTAP ti consente di personalizzare facilmente una strategia di protezione dei dati dei database di Oracle in base ai tuoi requisiti di business.

Questi requisiti includono fattori quali la velocità del recovery, la perdita massima consentita di dati e le esigenze di conservazione del backup. Il piano di protezione dei dati deve anche tenere in considerazione i vari requisiti normativi per la conservazione e il ripristino dei dati. Infine, è necessario considerare diversi

scenari di ripristino dei dati, che vanno dal recupero tipico e prevedibile derivante da errori di utenti o applicazioni fino a scenari di ripristino di emergenza che includono la perdita completa di un sito.

Piccole modifiche alle policy di protezione e ripristino dei dati possono avere un effetto significativo sull'architettura generale dello storage, del backup e del ripristino. È fondamentale definire e documentare gli standard prima di iniziare il lavoro di progettazione, per evitare di complicare un'architettura di protezione dati. Le funzioni o i livelli di protezione non necessari comportano costi e costi di gestione inutili, mentre un requisito inizialmente trascurato può condurre un progetto nella direzione sbagliata o richiedere modifiche di progettazione dell'ultimo minuto.

Recovery time objective

L'obiettivo RTO (Recovery Time Objective) definisce il tempo massimo consentito per il ripristino di un servizio. Ad esempio, un database di risorse umane potrebbe avere un RTO di 24 ore perché, sebbene sarebbe molto scomodo perdere l'accesso a questi dati durante la giornata lavorativa, l'azienda può comunque operare. Al contrario, un database che supporta la contabilità generale di una banca avrebbe un RTO misurato in minuti o anche secondi. Un RTO di zero non è possibile, perché deve esserci un modo per distinguere tra un'effettiva interruzione del servizio e un evento di routine, come un pacchetto di rete perso. Tuttavia, un RTO prossimo allo zero è un requisito tipico.

Obiettivo RPO

Il recovery point objective (RPO) definisce la massima perdita di dati tollerabile. In molti casi, l'RPO è determinato unicamente dalla frequenza delle snapshot o degli aggiornamenti di snapmirror.

In alcuni casi, l'RPO può essere reso più aggressivo proteggendo determinati dati con maggiore frequenza. In un contesto di database, l'RPO è in genere una questione di quanti dati di registro possono essere persi in una situazione specifica. In uno scenario di ripristino tipico in cui un database viene danneggiato a causa di un bug del prodotto o di un errore dell'utente, l'RPO deve essere pari a zero, il che significa che non ci devono essere perdite di dati. La procedura di ripristino prevede il ripristino di una copia precedente dei file di database e la riproduzione dei file di registro per portare lo stato del database al momento desiderato. I file di registro necessari per questa operazione dovrebbero essere già presenti nella posizione originale.

In scenari insoliti, i dati del registro potrebbero andare persi. Ad esempio, un accidentale o dannoso `rm -rf *` di file di database potrebbe causare l'eliminazione di tutti i dati. L'unica opzione sarebbe il ripristino dal backup, inclusi i file di registro, e alcuni dati andrebbero inevitabilmente persi. L'unica opzione per migliorare gli RPO in un ambiente di backup tradizionale sarebbe l'esecuzione di backup ripetuti dei dati di log. Questo comporta dei limiti, tuttavia, a causa dello spostamento costante dei dati e della difficoltà di mantenere un sistema di backup come servizio in esecuzione costante. Uno dei benefici dei sistemi storage avanzati è la capacità di proteggere i dati da danni accidentali o dannosi ai file e garantire quindi un RPO migliore senza spostamento dei dati.

Disaster recovery

Il ripristino di emergenza include l'architettura IT, i criteri e le procedure necessarie per il ripristino di un servizio in caso di emergenza fisica. Tra questi, inondazioni, incendi o persone che agiscono con intento doloso o negligente.

Il disaster recovery non è solo una serie di procedure di ripristino. Si tratta del processo completo di identificazione dei vari rischi, definizione dei requisiti di ripristino dei dati e continuità del servizio e realizzazione della giusta architettura con le relative procedure.

Durante la definizione dei requisiti di protezione dei dati, è fondamentale differenziare tra i requisiti tipici di RPO e RTO e quelli di RPO e RTO necessari per il disaster recovery. Alcuni ambienti applicativi richiedono un RPO pari a zero e un RTO prossimo allo zero per situazioni di perdita di dati che vanno da errori utente

relativamente normali a incendi che distruggono un data center. Tuttavia, vi sono conseguenze amministrative e di costo per questi elevati livelli di protezione.

In generale, i requisiti di ripristino dei dati non di emergenza devono essere rigorosi per due motivi. Innanzitutto, i bug applicativi e gli errori degli utenti che danneggiano i dati sono prevedibili al punto che sono quasi inevitabili. In secondo luogo, non è difficile progettare una strategia di backup in grado di offrire un RPO pari a zero e un RTO basso finché il sistema storage non viene distrutto. Non c'è motivo di non affrontare un rischio significativo che sia facilmente risolvibile, motivo per cui gli obiettivi di RPO e RTO per il ripristino locale dovrebbero essere aggressivi.

I requisiti di RTO e RPO per il disaster recovery variano in modo più ampio in base alla probabilità di un disastro e alle conseguenze della perdita di dati associata o dell'interruzione di un business. I requisiti di RPO e RTO devono essere basati sulle effettive esigenze di business e non su principi generali. Devono tenere conto di più scenari di emergenza logici e fisici.

Disastri logici

I disastri logici includono la corruzione dei dati causata da utenti, bug delle applicazioni o del sistema operativo e malfunzionamenti del software. I disastri logici possono includere anche attacchi dannosi da parte di terzi con virus o worm o sfruttando le vulnerabilità delle applicazioni. In questi casi, l'infrastruttura fisica rimane intatta, ma i dati sottostanti non sono più validi.

Un tipo sempre più comune di disastro logico è noto come ransomware, in cui un vettore di attacco viene utilizzato per crittografare i dati. La crittografia non danneggia i dati, ma li rende non disponibili fino a quando non viene effettuato il pagamento a terzi. Un numero sempre crescente di aziende è specificatamente preso di mira con gli hack ransomware. A causa di questa minaccia, NetApp offre snapshot a prova di manomissione, in cui nemmeno l'amministratore dello storage può modificare i dati protetti prima della data di scadenza configurata.

Disastri fisici

I disastri fisici includono l'errore di componenti di un'infrastruttura che superano le sue capacità di ridondanza e causano una perdita di dati o un'estesa perdita di servizio. Ad esempio, la protezione RAID fornisce la ridondanza dell'unità disco e l'utilizzo di HBA fornisce la ridondanza di porte FC e cavi FC. I guasti hardware di tali componenti sono prevedibili e non influiscono sulla disponibilità.

In un ambiente aziendale, è generalmente possibile proteggere l'infrastruttura di un intero sito con componenti ridondanti fino al punto in cui l'unico scenario di emergenza fisica prevedibile è la perdita completa del sito. Quindi, il piano di disaster recovery dipende dalla replica sito-sito.

Protezione dei dati sincrona e asincrona

In un mondo ideale, tutti i dati verrebbero replicati in modo sincrono tra siti dispersi geograficamente. Tale replicazione non è sempre fattibile o addirittura possibile per diversi motivi:

- La replica sincrona aumenta inevitabilmente la latenza di scrittura, perché tutte le modifiche devono essere replicate in entrambe le posizioni prima che l'applicazione/database possa procedere con l'elaborazione. L'effetto sulle prestazioni risultante è talvolta inaccettabile, escludendo l'uso del mirroring sincrono.
- La maggiore adozione di storage SSD al 100% implica maggiore probabilità di ottenere una latenza di scrittura aggiuntiva, poiché le aspettative di performance includono centinaia di migliaia di IOPS e latenza sotto al millisecondo. Ottenere tutti i benefici dell'utilizzo di SSD al 100% può richiedere la revisione della strategia di disaster recovery.
- I set di dati continuano a crescere in termini di byte, creando difficoltà per garantire una larghezza di banda sufficiente a sostenere la replica sincrona.

- I set di dati crescono anche in termini di complessità, creando problemi con la gestione della replica sincrona su larga scala.
- Le strategie basate sul cloud spesso implicano maggiori distanze di replica e latenza, precludendo ulteriormente l'utilizzo di mirroring sincrono.

NetApp offre soluzioni che includono replica sincrona per le più esigenti richieste di recovery di dati e soluzioni asincrone che consentono performance e flessibilità migliori. Inoltre, la tecnologia NetApp si integra perfettamente con molte soluzioni di replica di terze parti, come Oracle DataGuard

Tempo di conservazione

L'ultimo aspetto di una strategia di protezione dei dati è il tempo di conservazione dei dati, che può variare drasticamente.

- Un requisito tipico è rappresentato da 14 giorni di backup notturni sul sito primario e 90 giorni di backup memorizzati su un sito secondario.
- Molti clienti creano archivi trimestrali autonomi archiviati su supporti diversi.
- Un database costantemente aggiornato potrebbe non richiedere i dati storici e i backup devono essere conservati solo per alcuni giorni.
- I requisiti normativi potrebbero richiedere la possibilità di recupero fino al punto in cui avviene una transazione arbitraria nell'arco di 365 giorni.

Disponibilità del database

ONTAP è progettato per garantire la massima disponibilità dei database Oracle. Una descrizione completa delle funzioni di alta disponibilità di ONTAP esula dall'ambito di questo documento. Tuttavia, come per la protezione dei dati, una conoscenza di base di questa funzionalità è importante quando si progetta un'infrastruttura di database.

Coppie HA

L'unità di base dell'alta disponibilità è la coppia ha. Ciascuna coppia contiene collegamenti ridondanti per supportare la replica dei dati nella NVRAM. NVRAM non è una cache di scrittura. La RAM all'interno del controller funge da cache di scrittura. Lo scopo della NVRAM è quello di memorizzare temporaneamente i dati come salvaguardia da errori di sistema imprevisti. A questo proposito, è simile a un log di ripristino del database.

Sia la NVRAM che il redo log del database consentono di memorizzare i dati rapidamente, consentendo il commit delle modifiche ai dati il più rapidamente possibile. L'aggiornamento ai dati persistenti sulle unità (o file di dati) viene eseguito solo in un secondo momento durante un processo chiamato checkpoint sulle piattaforme ONTAP e sulla maggior parte dei database. Durante le normali operazioni, non vengono letti i dati della NVRAM né i log di ripristino del database.

Se un controller si guasta bruscamente, è probabile che vi siano modifiche in sospeso memorizzate nella NVRAM che non sono ancora state scritte sulle unità. Il partner controller rileva il guasto, assume il controllo dei dischi e applica le modifiche richieste che sono state memorizzate nella NVRAM.

Takeover e giveback

Il takeover e il giveback fanno riferimento al processo di trasferimento della responsabilità delle risorse di

storage fra i nodi di una coppia ha. L'acquisizione e il giveback presentano due aspetti:

- Gestione della connettività di rete che consente l'accesso alle unità
- Gestione delle unità stesse

Le interfacce di rete che supportano il traffico CIFS e NFS sono configurate sia con una posizione home che di failover. Un takeover include lo spostamento delle interfacce di rete nella loro abitazione temporanea su un'interfaccia fisica situata sulla stessa subnet della posizione originale. Un giveback prevede lo spostamento delle interfacce di rete nelle posizioni originali. Il comportamento esatto può essere regolato come richiesto.

Le interfacce di rete che supportano i protocolli a blocchi SAN, come iSCSI e FC, non vengono ricollocate durante il takeover e lo giveback. È invece necessario eseguire il provisioning delle LUN attraverso percorsi che includano una coppia ha completa che si traduce in un percorso primario e un percorso secondario.

È possibile configurare anche percorsi aggiuntivi per controller aggiuntivi in modo da supportare la riallocazione dei dati tra i nodi di un cluster più grande, non facente parte del processo di ha.

Il secondo aspetto del takeover e dello sconto è il trasferimento della proprietà del disco. Il processo esatto dipende da diversi fattori, tra cui il motivo del takeover/giveback e le opzioni della riga di comando emesse. L'obiettivo è quello di eseguire l'operazione nel modo più efficiente possibile. Anche se il processo complessivo potrebbe richiedere diversi minuti, il momento effettivo in cui la proprietà dell'unità viene trasferita da nodo a nodo può generalmente essere misurato in secondi.

Tempo di takeover

L'i/o dell'host subisce una breve pausa in i/o durante le operazioni di takeover e giveback, senza tuttavia alcuna interruzione dell'applicazione in un ambiente configurato correttamente. L'effettivo processo di transizione in cui l'i/o subisce un ritardo viene generalmente misurato in secondi, ma l'host potrebbe richiedere tempo aggiuntivo per riconoscere la modifica nei percorsi di dati e inviare di nuovo le operazioni i/O.

La natura dell'interruzione dipende dal protocollo:

- Un'interfaccia di rete che supporta il traffico NFS e CIFS emette una richiesta ARP (Address Resolution Protocol) alla rete dopo la transizione a una nuova posizione fisica. Ciò fa sì che gli switch di rete aggiornino le tabelle degli indirizzi MAC (Media Access Control) e riprendano l'elaborazione i/O. Le interruzioni nel caso di takeover e giveback pianificati vengono di solito misurate in secondi e in molti casi non sono rilevabili. Alcune reti potrebbero essere più lente a riconoscere completamente la modifica del percorso di rete e alcuni sistemi operativi potrebbero mettere in coda molti i/o in un breve periodo di tempo che deve essere rieseguito. Ciò può estendere il tempo necessario per riprendere l'i/O.
- Un'interfaccia di rete che supporta i protocolli SAN non passa a una nuova posizione. Un sistema operativo host deve modificare il percorso o i percorsi in uso. La pausa in i/o osservata dall'host dipende da diversi fattori. Dal punto di vista del sistema storage, il periodo in cui non è possibile fornire i/o è di pochi secondi. Tuttavia, sistemi operativi host diversi potrebbero richiedere tempo aggiuntivo per consentire un timeout i/o prima di riprovare. I sistemi operativi più recenti sono in grado di riconoscere un cambiamento di percorso molto più rapidamente, ma i sistemi operativi più vecchi in genere richiedono fino a 30 secondi per riconoscere un cambiamento.

La seguente tabella illustra i tempi di takeover previsti durante i quali il sistema storage non può fornire i dati a un ambiente applicativo. Non dovrebbero esserci errori in alcun ambiente applicativo, il takeover dovrebbe invece apparire come una breve pausa nell'elaborazione io.

	NFS	AFF	ASA

Takeover pianificato	15 sec.	6-10 sec.	2-3 sec.
Takeover non pianificato	30 sec.	6-10 sec.	2-3 sec.

Checksum e integrità dei dati

ONTAP e i protocolli supportati includono svariate funzionalità che proteggono l'integrità del database Oracle, inclusi dati a riposo e dati trasmessi sulla rete.

La protezione dei dati logici all'interno di ONTAP è costituita da tre requisiti principali:

- I dati devono essere protetti dalla corruzione.
- I dati devono essere protetti da guasti al disco.
- Le modifiche ai dati devono essere protette dalla perdita.

Queste tre esigenze sono discusse nelle sezioni seguenti.

Corruzione della rete: Checksum

Il livello più basilare di protezione dei dati è il checksum, che è uno speciale codice di rilevamento degli errori memorizzato insieme ai dati. La corruzione dei dati durante la trasmissione di rete viene rilevata con l'utilizzo di un checksum e, in alcuni casi, di checksum multipli.

Ad esempio, un frame FC include una forma di checksum chiamata CRC (Cyclic Redundancy Check) per assicurarsi che il payload non sia corrotto durante il transito. Il trasmettitore invia sia i dati che il CRC dei dati. Il ricevitore di un frame FC ricalcola il CRC dei dati ricevuti per assicurarsi che corrisponda al CRC trasmesso. Se il CRC appena calcolato non corrisponde al CRC collegato al frame, i dati sono corrotti e il frame FC viene scartato o rifiutato. Un'operazione i/o iSCSI include checksum ai livelli TCP/IP ed Ethernet e, per una maggiore protezione, può anche includere la protezione CRC opzionale al livello SCSI. Qualsiasi corruzione di bit sul filo viene rilevata dal livello TCP o IP, che porta alla ritrasmissione del pacchetto. Come nel caso di FC, gli errori nel CRC SCSI determinano un'eliminazione o un rifiuto dell'operazione.

Corruzione dei dischi: Checksum

I checksum vengono utilizzati anche per verificare l'integrità dei dati memorizzati sui dischi. I blocchi di dati scritti sui dischi vengono memorizzati con una funzione di checksum che produce un numero imprevedibile e legato ai dati originali. Quando i dati vengono letti dall'unità, il checksum viene ricalcolato e confrontato con il checksum memorizzato. Se non corrisponde, i dati sono corrotti e devono essere recuperati dal livello RAID.

Corruzione dei dati: Scritture perse

Uno dei tipi più difficili di corruzione da rilevare è una scrittura persa o posizionata erroneamente. Quando una scrittura viene confermata, deve essere scritta sul supporto nella posizione corretta. La corruzione dei dati sul posto è relativamente semplice da rilevare utilizzando un semplice checksum memorizzato con i dati. Tuttavia, se la scrittura viene semplicemente persa, la versione precedente dei dati potrebbe ancora esistere e il checksum sarebbe corretto. Se la scrittura viene posizionata nella posizione fisica errata, il checksum associato sarebbe ancora una volta valido per i dati memorizzati, anche se la scrittura ha distrutto altri dati.

La soluzione a questa sfida è la seguente:

- Un'operazione di scrittura deve includere metadati che indicano la posizione in cui dovrebbe essere trovata la scrittura.

- Un’operazione di scrittura deve includere un tipo di identificatore di versione.

Quando ONTAP scrive un blocco, include i dati sulla posizione di appartenenza del blocco. Se una lettura successiva identifica un blocco, ma i metadati indicano che esso appartiene alla posizione 123 quando è stato trovato nella posizione 456, allora la scrittura è stata erroneamente posizionata.

Rilevare una scrittura totalmente persa è più difficile. La spiegazione è molto complicata, ma essenzialmente ONTAP memorizza i metadati in modo che un’operazione di scrittura determini aggiornamenti a due posizioni diverse sulle unità. Se una scrittura viene persa, una successiva lettura dei dati e dei metadati associati mostra due diverse identità di versione. Ciò indica che la scrittura non è stata completata dall’unità.

La corruzione in scrittura persa e posizionata erroneamente è estremamente rara, ma con il continuo aumento dei dischi e la diminuzione dei set di dati nella scala di exabyte, il rischio aumenta. Il rilevamento delle operazioni di scrittura perse deve essere incluso in qualsiasi sistema storage che supporti i carichi di lavoro del database.

Guasti del disco: RAID, RAID DP e RAID-TEC

Se un blocco di dati su un’unità viene rilevato come danneggiato o se l’intera unità si guasta e non è completamente disponibile, i dati devono essere ricostituiti. Questo viene fatto in ONTAP utilizzando unità di parità. Lo striping dei dati viene eseguito su più unità dati, quindi vengono generati i dati di parità. I dati vengono memorizzati separatamente dai dati originali.

ONTAP utilizzava in origine RAID 4, che utilizza un singolo disco di parità per ciascun gruppo di unità dati. Il risultato è che un’unità del gruppo potrebbe guastarsi senza causare una perdita di dati. Se l’unità di parità non funziona correttamente, non sono stati danneggiati dati ed è stato possibile costruire una nuova unità di parità. Se si è verificato un errore in una singola unità dati, è possibile utilizzare le unità rimanenti con l’unità di parità per rigenerare i dati mancanti.

Quando le unità erano di piccole dimensioni, la possibilità statistica di due unità che si guastavano contemporaneamente era trascurabile. Con la progressiva crescita della capacità del disco aumentano anche il tempo necessario per ricostruire i dati in seguito a un guasto al disco. Ciò ha aumentato la finestra in cui un guasto di una seconda unità causerebbe la perdita di dati. Inoltre, il processo di ricostruzione crea numerosi i/o aggiuntivi sui dischi ancora in uso. Man mano che i dischi diventano obsoleti, aumenta anche il rischio di carico aggiuntivo che potrebbe causare un guasto al secondo disco. Infine, anche se il rischio di perdita di dati non aumentasse con il continuo utilizzo di RAID 4, le conseguenze della perdita di dati diventerebbero più gravi. Maggiore è la quantità di dati che andrebbero persi in caso di guasto a un gruppo RAID, più tempo occorrerebbe per ripristinare i dati, prolungando l’interruzione del business.

Questi problemi hanno portato NetApp a sviluppare la tecnologia NetApp RAID DP, una variante di RAID 6. Questa soluzione include due unità di parità, il che significa che due unità in un gruppo RAID possono guastarsi senza creare perdite di dati. Le dimensioni dei dischi hanno continuato a crescere, portando infine NetApp a sviluppare la tecnologia NetApp RAID-TEC, che introduce un disco a terza parità.

Alcune procedure consigliate per i database storici consigliano l’uso di RAID-10, noto anche come mirroring con striping. Ciò offre una protezione dei dati inferiore rispetto a quella dei sistemi RAID DP, in quanto vi sono più scenari di guasto a due dischi, mentre in RAID DP non ve ne sono nessuno.

Esistono inoltre alcune procedure consigliate per i database storici che indicano che le opzioni RAID-10 sono preferite a quelle RAID-4/5/6 a causa di problemi di prestazioni. Queste raccomandazioni a volte fanno riferimento a una penalizzazione RAID. Sebbene queste raccomandazioni siano generalmente corrette, non sono applicabili alle implementazioni di RAID all’interno di ONTAP. Il problema di prestazioni è relativo alla rigenerazione di parità. Con le implementazioni RAID tradizionali, l’elaborazione delle random write di routine eseguite da un database richiede letture multiple del disco per rigenerare i dati di parità e completare la scrittura. La penalità viene definita come gli IOPS in lettura aggiuntivi necessari per eseguire le operazioni di

scrittura.

ONTAP non subisce alcuna penalizzazione RAID perché le scritture vengono organizzate in memoria dove la parità viene generata e quindi scritta su disco come singolo stripe RAID. Non sono richieste letture per completare l'operazione di scrittura.

In sintesi, rispetto al RAID 10, RAID DP e RAID-TEC offrono una capacità utilizzabile molto maggiore, una migliore protezione contro i guasti ai dischi e nessun compromesso in termini di performance.

Protezione da errori hardware: NVRAM

Qualsiasi storage array che gestisce un carico di lavoro del database deve eseguire le operazioni di scrittura il più rapidamente possibile. Inoltre, un'operazione di scrittura deve essere protetta dalla perdita da un evento imprevisto, come un'interruzione dell'alimentazione. Ciò significa che qualsiasi operazione di scrittura deve essere conservata in modo sicuro in almeno due posizioni.

I sistemi AFF e FAS si affidano alla NVRAM per soddisfare questi requisiti. Il processo di scrittura funziona come segue:

1. I dati di scrittura in entrata sono memorizzati nella RAM.
2. Le modifiche che devono essere apportate ai dati sul disco vengono registrate nella NVRAM sia sul nodo locale che sul nodo partner. NVRAM non è una cache di scrittura, ma un journal simile a un log di ripristino dei database. In condizioni normali, non viene letta. Viene utilizzata solo per il ripristino, ad esempio in seguito a un'interruzione dell'alimentazione durante l'elaborazione i/O.
3. La scrittura viene quindi riconosciuta all'host.

Il processo di scrittura in questa fase è completo dal punto di vista dell'applicazione e i dati sono protetti dalla perdita, perché vengono memorizzati in due posizioni diverse. Alla fine, le modifiche vengono scritte su disco, ma il processo risulta fuori banda dal punto di vista dell'applicazione perché si verifica dopo il riconoscimento della scrittura e quindi non influisce sulla latenza. Questo processo è ancora una volta simile alla registrazione del database. Una modifica al database viene registrata nei registri di ripristino il più rapidamente possibile e la modifica viene quindi riconosciuta come confermata. Gli aggiornamenti ai file di dati avvengono molto più tardi e non influenzano direttamente la velocità di elaborazione.

In caso di guasto a un controller, il partner controller assume la proprietà dei dischi richiesti e riproduce i dati registrati nella NVRAM per ripristinare le operazioni di i/o in corso quando si è verificato il guasto.

Protezione da errori hardware: NVFAIL

Come discusso in precedenza, una scrittura non viene riconosciuta fino a quando non è stata registrata nella NVRAM locale e nella NVRAM su almeno un altro controller. Questo approccio garantisce che un guasto dell'hardware o un'interruzione di corrente non comporti la perdita dell'i/o in-flight In caso di guasto della NVRAM locale o di guasto della connettività al partner di ha, i dati in-flight non verranno più mirrorati.

Se la NVRAM locale riporta un errore, il nodo si arresta. Questo arresto determina il failover su un controller partner ha. Nessun dato viene perso perché il controller che presenta il guasto non ha confermato l'operazione di scrittura.

ONTAP non consente un failover quando i dati non sono sincronizzati, a meno che il failover non sia forzato. La forzatura di una modifica delle condizioni in questo modo riconosce che i dati potrebbero essere lasciati indietro nel controllore originale e che la perdita di dati è accettabile.

I database sono particolarmente vulnerabili al danneggiamento se un failover viene forzato perché mantengono grandi cache interne di dati su disco. In caso di failover forzato, le modifiche precedentemente

riconosciute vengono effettivamente eliminate. Il contenuto dell'array di storage torna indietro nel tempo e lo stato della cache del database non riflette più lo stato dei dati su disco.

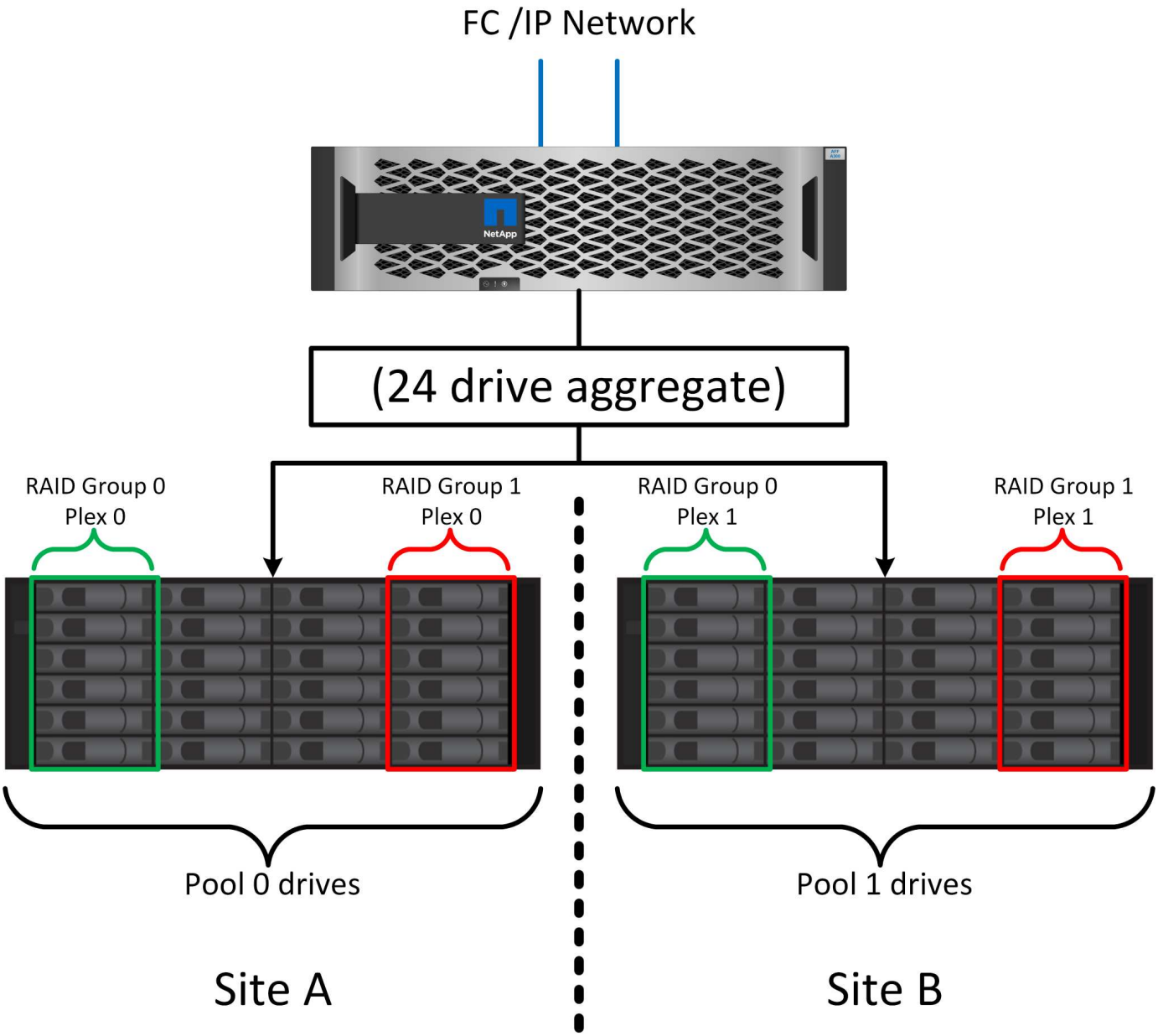
Per proteggere i dati da questa situazione, ONTAP consente di configurare i volumi per una protezione speciale contro gli errori della NVRAM. Quando attivato, questo meccanismo di protezione determina l'ingresso di un volume nello stato chiamato NVFAIL. Questo stato causa errori di i/o che causano l'arresto di un'applicazione in modo che non utilizzino dati obsoleti. I dati non devono essere persi perché qualsiasi scrittura riconosciuta deve essere presente sull'array di storage.

Solitamente, gli amministratori dovranno arrestare completamente gli host prima di riportare manualmente LUN e volumi in linea. Sebbene queste fasi possano comportare un certo lavoro, questo approccio è il modo più sicuro per garantire l'integrità dei dati. Non tutti i dati richiedono questa protezione, motivo per cui il comportamento di NVFAIL può essere configurato in base al volume.

Protezione dai guasti di shelf e siti: SyncMirror e plessi

SyncMirror è una tecnologia di mirroring che migliora, ma non sostituisce, RAID DP o RAID-TEC. Esegue il mirroring del contenuto di due gruppi RAID indipendenti. La configurazione logica è la seguente:

- I dischi sono configurati in due pool in base alla posizione. Un pool è composto da tutti i dischi sul sito A, mentre il secondo è composto da tutti i dischi sul sito B.
- Viene quindi creato un pool di storage comune, detto aggregato, in base a set di gruppi RAID con mirroring. Viene ottenuto lo stesso numero di unità per ciascun sito. Ad esempio, un aggregato SyncMirror da 20 dischi sarebbe composto da 10 dischi del sito A e 10 dischi del sito B.
- Ogni set di unità su un dato sito viene configurato automaticamente come uno o più gruppi RAID-DP o RAID-TEC completamente ridondanti, indipendentemente dall'utilizzo del mirroring. In questo modo si garantisce una protezione dei dati continua, anche dopo la perdita di un sito.



La figura precedente illustra una configurazione SyncMirror di esempio. È stato creato un aggregato di 24 dischi sul controller con 12 dischi da uno shelf allocato sul sito A e 12 dischi da uno shelf allocato sul sito B. I dischi sono stati raggruppati in due gruppi RAID con mirroring. Il gruppo RAID 0 include un plesso A 6 unità sul sito A con mirroring su un plesso A 6 unità sul sito B. Analogamente, il gruppo RAID 1 include un plesso A 6 unità sul sito A con mirroring su un plesso A 6 unità sul sito B.

Di norma, SyncMirror viene utilizzato per fornire il mirroring remoto con i sistemi MetroCluster, con una copia dei dati in ciascun sito. A volte, è stato utilizzato per fornire un livello di ridondanza extra in un unico sistema. In particolare, fornisce ridondanza a livello di shelf. Uno shelf di dischi contiene già doppi controller e alimentatori e nel complesso è poco più di una lamiera, ma in alcuni casi è consigliabile garantire una protezione extra. Ad esempio, un cliente NetApp ha implementato SyncMirror per una piattaforma mobile di analytics in tempo reale utilizzata durante i test nel settore automobilistico. Il sistema è stato separato in due rack fisici forniti da alimentatori indipendenti da sistemi UPS indipendenti.

Checksum

L'argomento dei checksum è di particolare interesse per i DBA abituati all'utilizzo dei backup in streaming Oracle RMAN che migrano a backup basati su snapshot. Una caratteristica di RMAN è che esegue controlli di integrità durante le operazioni di backup. Sebbene questa funzionalità offra un certo valore, il suo vantaggio principale è quello di un database non utilizzato su uno storage array moderno. Quando si utilizzano dischi fisici per un database Oracle, è quasi certo che il danneggiamento si verifica anche in caso di invecchiamento dei dischi, un problema che viene risolto dai checksum basati su array negli storage array reali.

Con un vero storage array, l'integrità dei dati è protetta utilizzando checksum a livelli multipli. Se i dati sono corrotti in una rete basata su IP, il livello TCP (Transmission Control Protocol) rifiuta i dati a pacchetto e richiede la ritrasmissione. Il protocollo FC include i checksum, così come i dati SCSI incapsulati. Dopo essere stato inserito nell'array, ONTAP dispone della protezione RAID e checksum. Il danneggiamento può verificarsi, ma, come nella maggior parte degli array Enterprise, viene rilevato e corretto. In genere, si verifica un guasto di un intero disco, che richiede una ricostruzione RAID e l'integrità del database rimane inalterata. È ancora possibile che i singoli byte su un'unità siano danneggiati dalla radiazione cosmica o da celle flash difettose. In questo caso, il controllo della parità non viene eseguito correttamente, l'unità viene chiusa in errore e viene avviata la ricostruzione RAID. Ancora una volta, l'integrità dei dati non viene influenzata. L'ultima linea di difesa è l'uso di checksum. Se, ad esempio, un errore catastrofico del firmware su un'unità ha danneggiato i dati in un modo che in qualche modo non è stato rilevato da un controllo di parità RAID, il checksum non corrisponderebbe e ONTAP impedirebbe il trasferimento di un blocco danneggiato prima che il database Oracle potesse riceverlo.

L'architettura dei log di ripristino e file dati di Oracle è inoltre progettata per offrire il massimo livello di integrità dei dati possibile, anche in circostanze estreme. A livello massimo, i blocchi Oracle includono il checksum e controlli logici di base con quasi ogni i/O. Se Oracle non è in crash o non ha portato offline uno spazio di tabella, i dati saranno intatti. Il grado di controllo dell'integrità dei dati è regolabile e Oracle può anche essere configurato per confermare le operazioni di scrittura. Di conseguenza, è possibile ripristinare quasi tutti gli scenari di crash e di guasto e, nel caso estremamente raro di una situazione irreversibile, viene immediatamente rilevata la corruzione.

La maggior parte dei clienti NetApp che utilizzano database Oracle interrompe l'utilizzo di RMAN e di altri prodotti di backup dopo la migrazione a backup basati su snapshot. Esistono ancora opzioni in cui RMAN può essere utilizzato per eseguire un ripristino a livello di blocco con SnapCenter. Tuttavia, ogni giorno, RMAN, NetBackup e altri prodotti vengono utilizzati solo occasionalmente per creare copie di archivio mensili o trimestrali.

Alcuni clienti scelgono di eseguire `dbv` eseguire periodicamente controlli di integrità dei database esistenti. NetApp scoraggia questa pratica perché crea un carico i/o non necessario. Come illustrato in precedenza, se il database non presentava problemi, la possibilità di `dbv` Il rilevamento di un problema è prossimo allo zero e questa utility crea un carico i/o sequenziale molto elevato sulla rete e sul sistema di storage. A meno che non vi sia motivo di ritenere che esista una corruzione, come l'esposizione a un bug Oracle noto, non c'è motivo di eseguire `dbv`.

Elementi di base di backup e recovery

Backup basati su snapshot

La base della protezione dei dati dei database Oracle su ONTAP è la tecnologia Snapshot di NetApp.

I valori chiave sono i seguenti:

- **Semplicità.** Uno snapshot è una copia di sola lettura del contenuto di un contenitore di dati in un determinato momento.
- **Efficienza.** le istantanee non richiedono spazio al momento della creazione. Lo spazio viene occupato solo quando i dati vengono modificati.
- **Gestibilità.** Una strategia di backup basata sugli snapshot è facile da configurare e gestire perché gli snapshot sono parte nativa del sistema operativo di storage. Se il sistema di archiviazione è acceso, è pronto per creare dei backup.
- **Scalabilità.** è possibile conservare fino a 1024 backup di un singolo contenitore di file e LUN. Per set di dati complessi, più container di dati possono essere protetti da un singolo set coerente di snapshot.
- Le prestazioni non sono influenzate, indipendentemente dal fatto che un volume contenga 1024 snapshot o nessuno.

Sebbene molti vendor di soluzioni storage offrano la tecnologia Snapshot, la tecnologia Snapshot all'interno di ONTAP è unica e offre benefici significativi per gli ambienti applicativi aziendali e di database:

- Le copie snapshot fanno parte del layout file WAFL (Write-Anywhere file Layout) sottostante. Non si tratta di una tecnologia aggiuntiva o esterna. Questo semplifica la gestione, perché il sistema storage è il sistema di backup.
- Le copie Snapshot non influiscono sulle prestazioni, ad eccezione di alcuni casi edge, come ad esempio quando una quantità così elevata di dati viene memorizzata nelle snapshot che il sistema storage sottostante si riempie.
- Il termine "gruppo di coerenza" viene spesso utilizzato per fare riferimento a un raggruppamento di oggetti di storage che vengono gestiti come una raccolta coerente di dati. Uno snapshot di un particolare volume ONTAP costituisce il backup del gruppo di coerenza.

Le snapshot ONTAP offrono anche una scalabilità migliore rispetto alle tecnologie della concorrenza. I clienti possono memorizzare 5, 50 o 500 snapshot senza influire sulle performance. Il numero massimo di snapshot attualmente consentiti in un volume è 1024. Se è necessaria una conservazione aggiuntiva degli snapshot, sono disponibili opzioni per trasferire gli snapshot in cascata ad altri volumi.

Di conseguenza, la protezione di un set di dati ospitato su ONTAP è semplice e altamente scalabile. I backup non richiedono lo spostamento dei dati, pertanto una strategia di backup può essere personalizzata in base alle esigenze dell'azienda piuttosto che alle limitazioni delle velocità di trasferimento di rete, del numero elevato di unità a nastro o delle aree di staging del disco.

Uno snapshot è un backup?

Una domanda comunemente posta sull'utilizzo delle istantanee come strategia di protezione dei dati è il fatto che i dati "reali" e i dati snapshot si trovano sulle stesse unità. La perdita di tali unità causerebbe la perdita sia dei dati primari che del backup.

Si tratta di un problema valido. Le snapshot locali vengono utilizzate per le esigenze di backup e ripristino quotidiane, e in questo senso la snapshot è un backup. Quasi il 99% di tutti gli scenari di ripristino in ambienti NetApp si affida alle snapshot per soddisfare anche i requisiti RTO più aggressivi.

Gli snapshot locali, tuttavia, non dovrebbero mai rappresentare l'unica strategia di backup, motivo per cui NetApp offre tecnologie come SnapMirror e la replica SnapVault per replicare in modo rapido ed efficiente le snapshot su un set indipendente di dischi. In una soluzione adeguatamente progettata con istantanee e replica snapshot, l'utilizzo del nastro può essere ridotto a icona in un archivio trimestrale o eliminato del tutto.

Backup basati su snapshot

Le copie Snapshot di ONTAP sono disponibili diverse opzioni per la protezione dei dati, mentre le snapshot sono alla base di molte altre funzionalità di ONTAP, tra cui replica, disaster recovery e cloning. Una descrizione completa della tecnologia snapshot non rientra nell'ambito di questo documento, ma le sezioni seguenti forniscono una panoramica generale.

Esistono due approcci principali per creare uno snapshot di un dataset:

- Backup coerenti con il crash
- Backup coerenti con le applicazioni

Un backup coerente con i crash di un set di dati si riferisce all'acquisizione dell'intera struttura di set di dati in un singolo point-in-time. Se il set di dati è memorizzato in un singolo volume, il processo è semplice ed è possibile creare una Snapshot in qualsiasi momento. Se un set di dati si estende tra i volumi, è necessario creare uno snapshot del gruppo di coerenza (CG). Esistono diverse opzioni per la creazione di snapshot CG, tra cui il software NetApp SnapCenter, le funzionalità native del gruppo di coerenza ONTAP e gli script gestiti dagli utenti.

I backup coerenti con i crash vengono utilizzati principalmente quando è sufficiente un ripristino point-of-the-backup. Quando è richiesto un ripristino più granulare, sono in genere necessari backup coerenti con l'applicazione.

La parola "coerente" in "coerente con l'applicazione" è spesso un nome scorretto. Ad esempio, l'inserimento di un database Oracle in modalità di backup viene definito backup coerente con l'applicazione, ma i dati non vengono resi coerenti o disattivati in alcun modo. I dati continuano a cambiare durante il backup. Al contrario, la maggior parte dei backup di MySQL e Microsoft SQL Server disattivano i dati prima di eseguire il backup. VMware può o non può rendere certi file coerenti.

Gruppi di coerenza

Il termine "gruppo di coerenza" si riferisce alla capacità di un array di archiviazione di gestire più risorse di archiviazione come una singola immagine. Ad esempio, un database può essere composto da 10 LUN. L'array deve essere in grado di eseguire il backup, il ripristino e la replica delle 10 LUN in modo coerente. Il ripristino non è possibile se le immagini dei LUN non erano coerenti nel punto di backup. La replica di queste 10 LUN richiede che tutte le repliche siano perfettamente sincronizzate l'una con l'altra.

Il termine "gruppo di coerenza" non viene spesso utilizzato quando si parla di ONTAP perché la coerenza è sempre stata una funzione di base dell'architettura di volumi e aggregati all'interno di ONTAP. Molti altri storage array gestiscono LUN o file system come unità singole. Possono quindi essere configurati facoltativamente come "gruppo di coerenza" ai fini della protezione dei dati, ma questo è un passaggio aggiuntivo nella configurazione.

ONTAP è sempre stata in grado di acquisire immagini di dati coerenti locali e replicate. Anche se i vari volumi su un sistema ONTAP non vengono in genere formalmente descritti come un gruppo di coerenza, è proprio questo lo sono. Una snapshot di tale volume è un'immagine del gruppo di coerenza, il ripristino di tale snapshot è un ripristino di un gruppo di coerenza e sia SnapMirror che SnapVault offrono la replica di un gruppo di coerenza.

Snapshot di gruppo di coerenza

Le snapshot di gruppo di coerenza (cg-Snapshot) sono un'estensione della tecnologia Snapshot di base di ONTAP. Un'operazione Snapshot standard crea un'immagine coerente di tutti i dati all'interno di un singolo volume, ma a volte è necessario creare un set coerente di Snapshot su più volumi e persino su sistemi di storage multipli. Ne risulta una serie di snapshot che possono essere utilizzate allo stesso modo di uno

snapshot di un solo volume. Possono essere utilizzati per il recovery locale dei dati, replicati a scopo di disaster recovery o clonati come una singola unità coerente.

Il più grande utilizzo noto di cg-snapshot è per un ambiente di database di circa 1PB GB su 12 controller. Le cg-Snapshot create su questo sistema sono state utilizzate per il backup, il ripristino e il cloning.

Nella maggior parte dei casi, quando un set di dati copre i volumi e l'ordine di scrittura deve essere preservato, il software di gestione scelto utilizza automaticamente uno snapshot cg. In questi casi non è necessario comprendere i dettagli tecnici delle istantanee cg. Tuttavia, in alcune situazioni, i complessi requisiti di protezione dei dati richiedono un controllo dettagliato sul processo di protezione e replica dei dati. I flussi di lavoro di automazione o l'uso di script personalizzati per richiamare le API cg-snapshot sono alcune delle opzioni disponibili. La comprensione dell'opzione migliore e del ruolo di cg-snapshot richiede una spiegazione più dettagliata della tecnologia.

La creazione di una serie di istantanee cg è un processo in due fasi:

1. Stabilire il recencing in scrittura su tutti i volumi di destinazione.
2. Creare Snapshot di tali volumi nello stato fenced (fenced).

La recinzione in scrittura viene stabilita in serie. Ciò significa che, mentre il processo di scherma viene configurato su più volumi, l'i/o in scrittura viene bloccato sul primo volume della sequenza mentre continua ad essere assegnato ai volumi che compaiono in seguito. Questo potrebbe inizialmente sembrare una violazione del requisito per il mantenimento dell'ordine di scrittura, ma ciò si applica solo all'i/o emesso in modo asincrono sull'host e non dipende da altre scritture.

Ad esempio, un database potrebbe eseguire numerosi aggiornamenti asincroni del file dati, consentendo al sistema operativo di riordinare l'i/o e completarli in base alla propria configurazione dell'utilità di pianificazione. L'ordine di questo tipo di i/o non può essere garantito perché l'applicazione e il sistema operativo hanno già rilasciato il requisito di mantenere l'ordine di scrittura.

Come esempio di contatore, la maggior parte delle attività di registrazione del database è sincrona. Il database non procede con ulteriori scritture di registro fino a quando l'i/o non viene riconosciuto e l'ordine di tali scritture deve essere conservato. Se un i/o di registro arriva su un volume fenced, non viene riconosciuto e le applicazioni vengono bloccate in ulteriori scritture. Analogamente, l'i/o di metadati del file system è di solito sincrono. Ad esempio, un'operazione di eliminazione file non deve essere persa. Se un sistema operativo con un file system xfs eliminava un file e l'i/o che aggiornava i metadati del file system xfs per rimuovere il riferimento a quel file apposto su un volume recintato, l'attività del file system si interrompeva. Ciò garantisce l'integrità del file system durante le operazioni cg-snapshot.

Dopo aver configurato la funzionalità write fencing nei volumi di destinazione, sono pronti per la creazione di snapshot. Non è necessario creare esattamente gli snapshot contemporaneamente, perché lo stato dei volumi è bloccato da un punto di vista di scrittura dipendente. Per evitare un difetto nell'applicazione che crea le istantanee cg, la recinzione iniziale include un timeout configurabile in cui ONTAP rilascia automaticamente la recinzione e riprende l'elaborazione di scrittura dopo un numero definito di secondi. Se tutte le istantanee vengono create prima dello scadere del periodo di timeout, il gruppo risultante di istantanee è un gruppo di coerenza valido.

Ordine di scrittura dipendente

Da un punto di vista tecnico, la chiave per un gruppo di coerenza è preservare l'ordine di scrittura e, nello specifico, l'ordine di scrittura dipendente. Ad esempio, un database in scrittura su 10 LUN scrive simultaneamente su tutte. Molte scritture vengono emesse in modo asincrono, il che significa che l'ordine in cui vengono completate non è importante e l'ordine effettivo in cui vengono completate varia in base al comportamento del sistema operativo e della rete.

Alcune operazioni di scrittura devono essere presenti sul disco prima che il database possa procedere con operazioni di scrittura aggiuntive. Queste operazioni critiche di scrittura sono chiamate scritture dipendenti. I/o di scrittura successivi dipendono dalla presenza di queste scritture sul disco. Qualsiasi snapshot, recovery o replica di queste 10 LUN deve garantire l'ordine di scrittura dipendente. Gli aggiornamenti del file system sono un altro esempio di scritture dipendenti dall'ordine di scrittura. L'ordine in cui vengono apportate le modifiche al file system deve essere mantenuto o l'intero file system potrebbe danneggiarsi.

Strategie

Esistono due approcci principali ai backup basati su snapshot:

- Backup coerenti con il crash
- Backup a caldo protetti dagli snapshot

Un backup coerente con i crash di un database si riferisce all'acquisizione dell'intera struttura del database, inclusi i file di dati, i log di ripristino e i file di controllo, in un singolo momento. Se il database è memorizzato in un singolo volume, il processo è semplice ed è possibile creare una Snapshot in qualsiasi momento. Se un database si estende su volumi, è necessario creare uno snapshot del gruppo di coerenza (CG). Esistono diverse opzioni per la creazione di snapshot CG, tra cui il software NetApp SnapCenter, le funzionalità native del gruppo di coerenza ONTAP e gli script gestiti dagli utenti.

I backup Snapshot coerenti con i crash vengono utilizzati principalmente quando è sufficiente un recovery point-of-the-backup. In alcune circostanze è possibile applicare i registri di archivio, ma quando è necessario un ripristino point-in-time più granulare, è preferibile un backup online.

La procedura di base per un backup online basato su snapshot è la seguente:

1. Inserire il database in `backup` modalità.
2. Creare una snapshot di tutti i volumi che ospitano file di dati.
3. Esci `backup` modalità.
4. Eseguire il comando `alter system archive log current` per forzare l'archiviazione del registro.
5. Creare snapshot di tutti i volumi che ospitano i log di archivio.

Questa procedura produce una serie di istantanee contenenti file di dati in modalità backup e i registri di archivio critici generati in modalità backup. Questi sono i due requisiti per il ripristino di un database. I file come i file di controllo dovrebbero essere protetti per comodità, ma l'unico requisito assoluto è la protezione per i file di dati e i registri di archivio.

Sebbene i diversi clienti possano avere strategie molto diverse, quasi tutte queste strategie si basano in ultima analisi sugli stessi principi delineati di seguito.

Recovery basato su Snapshot

Quando si progettano layout di volumi per database Oracle, la prima decisione è se utilizzare la tecnologia VBSR (Volume-Based NetApp SnapRestore).

La funzione SnapRestore basata su volume consente di ripristinare quasi istantaneamente un volume in un point-in-time precedente. Poiché tutti i dati sul volume vengono ripristinati, VBSR potrebbe non essere appropriato per tutti i casi di utilizzo. Ad esempio, se un intero database, inclusi file di dati, log di ripristino e log di archivio, viene memorizzato in un singolo volume e questo volume viene ripristinato con VBSR, i dati vengono persi perché i log di archivio e i dati di ripristino più recenti vengono scartati.

VBSR non è necessario per il ripristino. Molti database possono essere ripristinati utilizzando SFSR (Single-file SnapRestore) basato su file o semplicemente copiando i file dalla snapshot nel file system attivo.

VBSR è preferibile quando un database è molto grande o quando deve essere recuperato il più rapidamente possibile, e l'uso di VBSR richiede l'isolamento dei file di dati. In un ambiente NFS, i file di dati di un dato database devono essere archiviati in volumi dedicati che non sono contaminati da alcun altro tipo di file. In un ambiente SAN, i file di dati devono essere memorizzati in LUN dedicate su volumi dedicati. Se viene utilizzato un volume manager (incluso Oracle Automatic Storage Management [ASM]), il gruppo di dischi deve essere dedicato anche ai file di dati.

L'isolamento dei file di dati in questo modo consente loro di tornare a uno stato precedente senza danneggiare altri file system.

Riserva di Snapshot

Per ogni volume con i dati Oracle in un ambiente SAN, il `percent-snapshot-space` Dovrebbe essere impostato su zero perché non è utile riservare spazio per uno snapshot in un ambiente LUN. Se la riserva frazionaria è impostata su 100, uno snapshot di un volume con LUN richiede spazio libero sufficiente nel volume, esclusa la riserva snapshot, per assorbire il 100% di turnover di tutti i dati. Se la riserva frazionaria è impostata su un valore inferiore, è necessaria una quantità di spazio libero corrispondente inferiore, ma esclude sempre la riserva istantanea. Ciò significa che viene sprecato lo spazio di riserva di Snapshot in un ambiente LUN.

In un ambiente NFS, esistono due opzioni:

- Impostare `percent-snapshot-space` in base al consumo di spazio snapshot previsto.
- Impostare `percent-snapshot-space` a zero e gestire collettivamente il consumo di spazio attivo e snapshot.

Con la prima opzione, `percent-snapshot-space` è impostato su un valore diverso da zero, in genere intorno al 20%. Questo spazio viene quindi nascosto all'utente. Tuttavia, questo valore non crea un limite di utilizzo. Se un database con una prenotazione del 20% registra un fatturato del 30%, lo spazio snapshot può crescere oltre i limiti della riserva del 20% e occupare spazio non riservato.

Il vantaggio principale dell'impostazione di una riserva a un valore come 20% è verificare che una parte di spazio sia sempre disponibile per gli snapshot. Ad esempio, un volume da 1TB TB con una riserva del 20% consentirebbe all'amministratore di database (DBA) di memorizzare 800GB TB di dati. Questa configurazione garantisce almeno 200GB GB di spazio per il consumo di snapshot.

Quando `percent-snapshot-space` è impostato su zero, tutto lo spazio nel volume è disponibile per l'utente finale, il che garantisce una migliore visibilità. Un DBA deve capire che, se rileva un volume di 1TB GB che sfrutta le snapshot, questo 1TB GB di spazio viene condiviso tra i dati attivi e il turnover di Snapshot.

Non esiste una chiara preferenza tra l'opzione 1 e l'opzione 2 tra gli utenti finali.

ONTAP e snapshot di terze parti

Oracle Doc ID 604683,1 illustra i requisiti per il supporto di snapshot di terze parti e le varie opzioni disponibili per le operazioni di backup e ripristino.

Il fornitore di terze parti deve garantire che le istantanee dell'azienda siano conformi ai seguenti requisiti:

- Gli snapshot devono integrarsi con le operazioni di ripristino e ripristino consigliate da Oracle.
- Gli snapshot devono essere coerenti con il crash del database nel punto dello snapshot.

- L’ordine di scrittura viene mantenuto per ogni file all’interno di uno snapshot.

I prodotti di gestione ONTAP e NetApp di Oracle sono conformi a questi requisiti.

SnapRestore

La tecnologia NetApp SnapRestore offre il ripristino rapido dei dati in ONTAP a partire da una snapshot.

Quando un set di dati critico non è disponibile, le operazioni di business critiche non sono attive. I nastri possono interrompersi e persino i ripristini da backup basati su disco possono essere lenti da trasferire sulla rete. SnapRestore consente di evitare questi problemi grazie al ripristino quasi istantaneo dei set di dati. Anche i database di diversi petabyte possono essere ripristinati completamente con pochi minuti di lavoro.

Esistono due forme di SnapRestore: Basata su file/LUN e basata su volume.

- Singoli file o LUN possono essere ripristinati in pochi secondi, sia in una LUN da 2TB GB che in un file da 4KB GB.
- Il container di file o LUN può essere ripristinato in pochi secondi, siano essi 10GB o 100TB TB di dati.

Un "contenitore di file o LUN" generalmente si riferisce a un volume FlexVol. Ad esempio, potresti avere 10 LUN che costituiscono un gruppo di dischi LVM in un singolo volume, oppure un volume potrebbe archiviare le home directory NFS di 1000 utenti. Invece di eseguire un’operazione di ripristino per ogni singolo file o LUN, è possibile ripristinare l’intero volume come un’unica operazione. Questo processo funziona anche con container scale-out che includono volumi multipli, come FlexGroup o un gruppo di coerenza ONTAP.

Il motivo per cui SnapRestore funziona in modo così rapido ed efficiente è dovuto alla natura di uno snapshot, che è essenzialmente una vista parallela di sola lettura del contenuto di un volume in uno specifico momento. I blocchi attivi sono i blocchi reali che è possibile modificare, mentre lo snapshot è una vista di sola lettura dello stato dei blocchi che costituiscono i file e le LUN al momento della creazione dello snapshot.

ONTAP consente solo l’accesso in sola lettura ai dati snapshot, ma i dati possono essere riattivati con SnapRestore. Lo snapshot viene riabilitato come visualizzazione lettura-scrittura dei dati, riportando i dati allo stato precedente. SnapRestore può operare a livello di volume o di file. La tecnologia è essenzialmente la stessa con alcune differenze minori nel comportamento.

SnapRestore volume

La SnapRestore basata su volume riporta l’intero volume di dati a uno stato precedente. Questa operazione non richiede lo spostamento dei dati, il che significa che il processo di ripristino è essenzialmente istantaneo, sebbene l’elaborazione delle operazioni API o CLI possa richiedere alcuni secondi. Il ripristino di 1GB TB di dati non è più complicato o richiede molto tempo rispetto al ripristino di 1PB TB di dati. Questa funzionalità è il motivo principale per cui molti clienti aziendali migrano ai sistemi storage ONTAP. Offre un RTO misurato in secondi anche per i set di dati più grandi.

Uno svantaggio di SnapRestore basato su volumi è causato dal fatto che le modifiche all’interno di un volume sono cumulative nel tempo. Pertanto, ogni snapshot e i dati del file attivo dipendono dalle modifiche che hanno portato a quel punto. Ripristinare uno stato precedente di un volume significa ignorare tutte le modifiche successive apportate ai dati. Ciò che è meno ovvio, tuttavia, è che questo include gli snapshot creati successivamente. Ciò non è sempre desiderabile.

Ad esempio, uno SLA di conservazione dei dati può specificare 30 giorni di backup notturni. Il ripristino di un set di dati in uno snapshot creato cinque giorni fa con Volume SnapRestore scaricherebbe tutti gli snapshot creati nei cinque giorni precedenti, violando lo SLA.

Sono disponibili diverse opzioni per risolvere questo limite:

1. I dati possono essere copiati da una snapshot precedente, invece di eseguire un SnapRestore dell'intero volume. Questo metodo funziona meglio con set di dati più piccoli.
2. È possibile clonare una snapshot invece di ripristinarla. Il limite a questo approccio è che lo snapshot di origine è una dipendenza del clone. Pertanto, non può essere eliminato a meno che il clone non venga anch'esso eliminato o diviso in un volume indipendente.
3. Utilizzo di SnapRestore basati su file.

File SnapRestore (Stato file)

SnapRestore basato su file è un processo di ripristino più granulare e basato su snapshot. Invece di ripristinare lo stato di un intero volume, viene ripristinato lo stato di un singolo file o LUN. Non è necessario eliminare gli snapshot, né questa operazione crea alcuna dipendenza da uno snapshot precedente. Il file o LUN diventa immediatamente disponibile nel volume attivo.

Durante il ripristino di SnapRestore di un file o LUN non è necessario alcuno spostamento dei dati. Tuttavia, alcuni aggiornamenti dei metadati interni sono necessari per riflettere il fatto che i blocchi sottostanti in un file o LUN ora esistono sia in una snapshot che nel volume attivo. Non dovrebbe avere alcun effetto sulle prestazioni, ma questo processo blocca la creazione di snapshot fino al completamento. La velocità di elaborazione è di circa 5Gbps MB (18TB MB/ora) in base alla dimensione totale dei file ripristinati.

Backup in linea

Per proteggere e ripristinare un database Oracle in modalità backup sono richiesti due set di dati. Si noti che questa non è l'unica opzione di backup di Oracle, ma è la più comune.

- Un'istantanea dei file di dati in modalità di backup
- I registri di archivio creati mentre i file di dati erano in modalità backup

Se è richiesto il recupero completo, comprese tutte le transazioni impegnate, è necessario un terzo elemento:

- Una serie di registri di ripristino correnti

Esistono diversi modi per eseguire il ripristino di un backup online. Molti clienti ripristinano le snapshot utilizzando l'interfaccia CLI di ONTAP e quindi Oracle RMAN o sqlplus per completare il ripristino. Ciò è particolarmente comune negli ambienti di produzione di grandi dimensioni, in cui la probabilità e la frequenza dei ripristini dei database sono estremamente ridotte e qualsiasi procedura di ripristino viene gestita da un DBA esperto. Per un'automazione completa, soluzioni come NetApp SnapCenter includono un plug-in Oracle con interfacce sia a riga di comando che grafiche.

Alcuni clienti su larga scala hanno adottato un approccio più semplice configurando script di base sugli host per impostare i database in modalità di backup in un momento specifico in preparazione a uno snapshot pianificato. Ad esempio, pianificare il comando `alter database begin backup` alle 23:58, `alter database end backup` alle 00:02, quindi programmare le snapshot direttamente sul sistema storage a mezzanotte. Il risultato è una strategia di backup semplice e altamente scalabile che non richiede licenze o software esterni.

Layout dei dati

Il layout più semplice consiste nell'isolare i file di dati in uno o più volumi dedicati. Non devono essere

contaminati da alcun altro tipo di file. In questo modo si garantisce che i volumi dei file dati possano essere ripristinati rapidamente tramite un'operazione SnapRestore senza distruggere un log di ripristino, controlfile o un log di archivio importante.

LE SAN hanno requisiti simili per l'isolamento dei file dati all'interno di volumi dedicati. Con un sistema operativo come Microsoft Windows, un singolo volume potrebbe contenere più LUN di file dati, ciascuno con un file system NTFS. Con altri sistemi operativi, in genere esiste un volume manager logico. Ad esempio, con Oracle ASM, l'opzione più semplice sarebbe limitare i LUN di un gruppo di dischi ASM a un singolo volume che può essere sottoposto a backup e ripristinato come unità. Se per motivi di gestione delle performance o della capacità sono necessari volumi aggiuntivi, la creazione di un gruppo di dischi aggiuntivo sul nuovo volume semplifica la gestione.

Se vengono seguite queste linee guida, le snapshot possono essere pianificate direttamente sul sistema di storage, senza che sia necessario eseguire uno snapshot del gruppo di coerenza. Il motivo è che i backup Oracle non richiedono il backup dei file di dati contemporaneamente. La procedura di backup online è stata progettata per consentire ai file di dati di continuare ad essere aggiornati, poiché vengono lentamente trasmessi su nastro nel corso delle ore.

Una complicazione si verifica in situazioni come l'utilizzo di un gruppo di dischi ASM distribuito tra i volumi. In questi casi, è necessario eseguire uno snapshot cg per assicurarsi che i metadati ASM siano coerenti in tutti i volumi costituenti.

Attenzione: verificare che l'ASM `spfile` e. `passwd` i file non si trovano nel gruppo di dischi che ospita i file di dati. Ciò interferisce con la capacità di ripristinare selettivamente i dati e solo i file di dati.

Procedura di ripristino locale: NFS

Questa procedura può essere gestita manualmente o tramite un'applicazione come SnapCenter. La procedura di base è la seguente:

1. Arrestare il database.
2. Recuperare i volumi di file dati nello snapshot immediatamente prima del punto di ripristino desiderato.
3. Riprodurre i log di archivio nel punto desiderato.
4. Se si desidera completare il ripristino, riprodurre i registri di ripristino correnti.

Questa procedura presuppone che i log di archivio desiderati siano ancora presenti nel file system attivo. In caso contrario, è necessario ripristinare i log di archivio oppure è possibile indirizzare rman/sqlplus ai dati nella directory snapshot.

Inoltre, per i database di dimensioni inferiori, i file di dati possono essere recuperati da un utente finale direttamente da `.snapshot` directory senza l'assistenza di tool di automazione o amministratori dello storage per eseguire una `snaprestore` comando.

Procedura di ripristino locale: SAN

Questa procedura può essere gestita manualmente o tramite un'applicazione come SnapCenter. La procedura di base è la seguente:

1. Arrestare il database.
2. Chiudere i gruppi di dischi che ospitano i file di dati. La procedura varia a seconda del volume manager logico scelto. Con ASM, il processo richiede lo smontaggio del gruppo di dischi. Con Linux, i file system devono essere smontati e i volumi logici e i gruppi di volumi devono essere disattivati. L'obiettivo è quello di interrompere tutti gli aggiornamenti del gruppo di volumi di destinazione da ripristinare.

3. Ripristinare i gruppi di dischi del file dati nello snapshot immediatamente prima del punto di ripristino desiderato.
4. Riattivare i gruppi di dischi appena ripristinati.
5. Riprodurre i log di archivio nel punto desiderato.
6. Se si desidera eseguire il ripristino completo, riprodurre tutti i registri di ripristino.

Questa procedura presuppone che i log di archivio desiderati siano ancora presenti nel file system attivo. In caso contrario, è necessario ripristinare i registri di archivio portando i LUN del registro di archivio offline ed eseguendo un ripristino. Questo è anche un esempio in cui è utile dividere i log di archivio in volumi dedicati. Se i log dell'archivio condividono un gruppo di volumi con log di ripristino, i log di ripristino devono essere copiati in un altro punto prima di ripristinare il set complessivo di LUN. Questa fase impedisce la perdita di tali transazioni finali registrate.

Backup ottimizzati per le snapshot di storage

Il backup e il ripristino basati su Snapshot sono diventati ancora più semplici quando è stato rilasciato Oracle 12c perché non è necessario collocare un database in modalità hot backup. Il risultato è la possibilità di pianificare backup basati su snapshot direttamente in un sistema storage, preservando comunque la capacità di eseguire ripristini completi o point-in-time.

Sebbene la procedura di ripristino con backup a caldo sia più familiare per gli amministratori di database, da molto tempo è stato possibile utilizzare istantanee che non sono state create mentre il database era in modalità di backup a caldo. Per rendere il database coerente, sono stati necessari ulteriori passaggi manuali con Oracle 10g e 11g durante il ripristino. Con Oracle 12c, `sqlplus` e. `rman` contenere la logica aggiuntiva per riprodurre i log di archivio sui backup dei file dati che non erano in modalità hot backup.

Come indicato in precedenza, il ripristino di un backup a caldo basato su snapshot richiede due set di dati:

- Un'istantanea dei file di dati creati in modalità backup
- I log di archivio generati mentre i file di dati erano in modalità hot backup

Durante il ripristino, il database legge i metadati dai file di dati per selezionare i log di archivio richiesti per il ripristino.

Per ottenere gli stessi risultati, il recovery ottimizzato per le snapshot di storage richiede set di dati leggermente diversi:

- Un'istantanea dei file di dati, più un metodo per identificare l'ora in cui è stata creata l'istantanea
- Archiviare i log dall'ora del checkpoint del file dati più recente all'ora esatta dello snapshot

Durante il ripristino, il database legge i metadati dai file di dati per identificare il registro di archivio più recente richiesto. È possibile eseguire il ripristino completo o point-in-time. Quando si esegue un ripristino point-in-time, è fondamentale conoscere l'ora dello snapshot dei file di dati. Il punto di ripristino specificato deve essere successivo all'ora di creazione degli snapshot. NetApp consiglia di aggiungere almeno alcuni minuti all'ora dello snapshot per tenere conto della variazione dell'orologio.

Per informazioni dettagliate, vedere la documentazione di Oracle sull'argomento "Recovery Using Storage Snapshot Optimization" disponibile in varie versioni della documentazione di Oracle 12c. Inoltre, consultare l'ID documento Oracle Doc ID 604683,1 relativo al supporto per le istantanee di terze parti di Oracle.

Layout dei dati

Il layout più semplice consiste nell'isolare i file di dati in uno o più volumi dedicati. Non devono essere contaminati da alcun altro tipo di file. In questo modo si garantisce che i volumi dei file dati possano essere ripristinati rapidamente con un'operazione SnapRestore senza distruggere un log di ripristino, controlfile o un log di archivio importante.

LE SAN hanno requisiti simili per l'isolamento dei file dati all'interno di volumi dedicati. Con un sistema operativo come Microsoft Windows, un singolo volume potrebbe contenere più LUN di file dati, ciascuno con un file system NTFS. Con altri sistemi operativi, esiste in genere anche un volume manager logico. Ad esempio, con Oracle ASM, l'opzione più semplice sarebbe quella di limitare i gruppi di dischi a un singolo volume di cui è possibile eseguire il backup e il ripristino come unità. Se per motivi di gestione delle performance o della capacità sono necessari volumi aggiuntivi, la creazione di un gruppo di dischi aggiuntivo sul nuovo volume semplifica la gestione.

Se si seguono queste linee guida, gli snapshot possono essere pianificati direttamente su ONTAP senza che sia necessario eseguire uno snapshot del gruppo di coerenza. Il motivo è che i backup ottimizzati per le istantanee non richiedono che venga eseguito contemporaneamente il backup dei file di dati.

Una complicazione si verifica in situazioni come un gruppo di dischi ASM distribuito tra i volumi. In questi casi, è necessario eseguire uno snapshot cg per assicurarsi che i metadati ASM siano coerenti in tutti i volumi costituenti.

[Note]verificare che i file ASM spfile e passwd non siano nel gruppo di dischi che ospita i file di dati. Ciò interferisce con la capacità di ripristinare selettivamente i dati e solo i file di dati.

Procedura di ripristino locale: NFS

Questa procedura può essere gestita manualmente o tramite un'applicazione come SnapCenter. La procedura di base è la seguente:

1. Arrestare il database.
2. Recuperare i volumi di file dati nello snapshot immediatamente prima del punto di ripristino desiderato.
3. Riprodurre i log di archivio nel punto desiderato.

Questa procedura presuppone che i log di archivio desiderati siano ancora presenti nel file system attivo. In caso contrario, è necessario ripristinare i registri di archivio, o. `rman` oppure `sqlplus` può essere indirizzato ai dati in `.snapshot` directory.

Inoltre, per i database di dimensioni inferiori, i file di dati possono essere recuperati da un utente finale direttamente da `.snapshot` Senza l'assistenza di tool di automazione o di un amministratore dello storage per eseguire un comando SnapRestore.

Procedura di ripristino locale: SAN

Questa procedura può essere gestita manualmente o tramite un'applicazione come SnapCenter. La procedura di base è la seguente:

1. Arrestare il database.
2. Chiudere i gruppi di dischi che ospitano i file di dati. La procedura varia a seconda del volume manager logico scelto. Con ASM, il processo richiede lo smontaggio del gruppo di dischi. Con Linux, i file system devono essere smontati e i volumi logici e i gruppi di volumi sono disattivati. L'obiettivo è quello di interrompere tutti gli aggiornamenti del gruppo di volumi di destinazione da ripristinare.

3. Ripristinare i gruppi di dischi del file dati nello snapshot immediatamente prima del punto di ripristino desiderato.
4. Riattivare i gruppi di dischi appena ripristinati.
5. Riprodurre i log di archivio nel punto desiderato.

Questa procedura presuppone che i log di archivio desiderati siano ancora presenti nel file system attivo. In caso contrario, è necessario ripristinare i registri di archivio portando i LUN del registro di archivio offline ed eseguendo un ripristino. Questo è anche un esempio in cui è utile dividere i log di archivio in volumi dedicati. Se i log dell'archivio condividono un gruppo di volumi con i log di ripristino, i log di ripristino devono essere copiati in un altro punto prima del ripristino del set complessivo di LUN, per evitare di perdere le transazioni finali registrate.

Esempio di recupero completo

Si supponga che i file di dati siano stati corrotti o distrutti e che sia necessario un ripristino completo. La procedura da seguire è la seguente:

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover automatic;
Media recovery complete.
SQL> alter database open;
Database altered.
SQL>
```

Esempio di recupero point-in-time

L'intera procedura di ripristino è un singolo comando: `recover automatic`.

Se è necessario un ripristino point-in-time, l'indicatore data e ora degli snapshot deve essere noto e può essere identificato come segue:

```
Cluster01::> snapshot show -vserver vserver1 -volume NTAP_oradata -fields
create-time
vserver   volume        snapshot   create-time
--------  ------------  ---------  ------------------------
vserver1  NTAP_oradata  my-backup  Thu Mar 09 10:10:06 2017
```

L'ora di creazione dell'istantanea è indicata come marzo 9th e 10:10:06. Per essere sicuri, viene aggiunto un

minuto all'ora dell'istantanea:

```
[oracle@host1 ~]$ sqlplus / as sysdba
Connected to an idle instance.
SQL> startup mount;
ORACLE instance started.
Total System Global Area 1610612736 bytes
Fixed Size                  2924928 bytes
Variable Size            1040191104 bytes
Database Buffers          553648128 bytes
Redo Buffers               13848576 bytes
Database mounted.
SQL> recover database until time '09-MAR-2017 10:44:15' snapshot time '09-
MAR-2017 10:11:00';
```

Il ripristino viene avviato. È stato specificato un tempo di snapshot di 10:11:00, un minuto dopo il tempo registrato per tenere conto della possibile varianza dell'orologio e un tempo di recupero target di 10:44. Successivamente, sqlplus richiede i registri di archivio necessari per raggiungere il tempo di ripristino desiderato di 10:44.

```
ORA-00279: change 551760 generated at 03/09/2017 05:06:07 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_31_930813377.dbf
ORA-00280: change 551760 for thread 1 is in sequence #31
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 552566 generated at 03/09/2017 05:08:09 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_32_930813377.dbf
ORA-00280: change 552566 for thread 1 is in sequence #32
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 553045 generated at 03/09/2017 05:10:12 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_33_930813377.dbf
ORA-00280: change 553045 for thread 1 is in sequence #33
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
ORA-00279: change 753229 generated at 03/09/2017 05:15:58 needed for
thread 1
ORA-00289: suggestion : /oralogs_nfs/arch/1_34_930813377.dbf
ORA-00280: change 753229 for thread 1 is in sequence #34
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
Log applied.
Media recovery complete.
SQL> alter database open resetlogs;
Database altered.
SQL>
```

Completare il ripristino di un database utilizzando gli snapshot utilizzando `recover automatic` command non richiede licenze specifiche, ma utilizza un ripristino point-in-time `snapshot time` Richiede la licenza Oracle Advanced Compression.

Tool di gestione e automazione del database

Il valore primario di ONTAP in un ambiente di database Oracle deriva dalle tecnologie principali di ONTAP, come copie Snapshot istantanee, semplice replica SnapMirror e creazione efficiente dei volumi FlexClone.

In alcuni casi, una semplice configurazione di queste funzionalità chiave direttamente su ONTAP soddisfa i requisiti, ma esigenze più complesse richiedono un livello di orchestrazione.

SnapCenter

SnapCenter è il prodotto di punta della protezione dei dati di NetApp. A un livello molto basso, è simile ai prodotti SnapManager in termini di modalità di esecuzione dei backup del database, ma è stato creato da zero per fornire un singolo pannello di controllo per la gestione della protezione dati sui sistemi di storage NetApp.

SnapCenter include le funzioni di base come backup e ripristini basati su snapshot, la replica SnapMirror e SnapVault e altre funzionalità necessarie per operare su larga scala per le grandi imprese. Queste funzionalità avanzate includono una funzionalità estesa di controllo degli accessi in base al ruolo (RBAC), API RESTful per l'integrazione con prodotti di orchestrazione di terze parti, gestione centrale senza interruzioni dei plug-in SnapCenter sugli host di database e un'interfaccia utente progettata per ambienti cloud-scale.

RIPOSO

ONTAP contiene anche un ricco set di API RESTful. Questo consente a 3rd vendor di creare data Protection e altre applicazioni di gestione con una profonda integrazione con ONTAP. Inoltre, l'API RESTful è facile da utilizzare da parte dei clienti che desiderano creare i propri flussi di lavoro e utility di automazione.