Elementi di base di backup e recovery

Enterprise applications

NetApp
May 09, 2024

This PDF was generated from https://docs.netapp.com/it-it/ontap-apps-dbs/oracle/oracle-dp-snapshots.html on May 09, 2024. Always check docs.netapp.com for the latest.

Sommario

Elementi di base di backup e recovery

Database Oracle e 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 NetApp FlexVol, 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 NetApp FlexVol, 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 FlexVol 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.

Recovery rapida dei database Oracle con 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 online dei database Oracle

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 istantanee dello storage dei database Oracle

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 Oracle

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.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.