Concetti di ONTAP

ONTAP 9

NetApp
April 24, 2024

Sommario

Concetti di ONTAP

Panoramica dei concetti

I seguenti concetti informano il software di gestione dei dati ONTAP, inclusi storage in cluster, alta disponibilità, virtualizzazione, protezione dei dati, Efficienza dello storage, sicurezza e FabricPool. Prima di configurare la soluzione di storage, è necessario conoscere la gamma completa di funzionalità e vantaggi di ONTAP.

Per ulteriori informazioni, consultare quanto segue:

- "Amministrazione di cluster e SVM"
- "Coppie ad alta disponibilità (ha)"
- "Gestione di rete e LIF"
- "Gestione di dischi e aggregati"
- "FlexVol Volumes, tecnologia FlexClone e funzionalità di efficienza dello storage"
- "Provisioning host SAN"
- Accesso al file NAS
  - "Gestione NFS"
  - "Gestione delle PMI"
- "Disaster recovery e archiviazione"

Piattaforme ONTAP

Il software per la gestione dei dati ONTAP offre storage unificato per le applicazioni che leggono e scrivono i dati su protocolli di accesso a blocchi o file, in configurazioni storage che spaziano dalla flash ad alta velocità, ai supporti rotanti a basso prezzo, allo storage a oggetti basato sul cloud.

Le implementazioni di ONTAP vengono eseguite su piattaforme FAS, AFF A-Series e C-Series e All-SAN Flash Array ASA, oltre che su commodity hardware (ONTAP Select) e in cloud privati, pubblici o ibridi (Cloud Volumes ONTAP). Un'implementazione specializzata offre un'infrastruttura convergente Best-in-class (data center FlexPod).

Insieme, queste implementazioni formano il framework di base del *data fabric NetApp*, con un approccio comune software-defined alla gestione dei dati e una replica rapida ed efficiente tra le piattaforme.

Storage in cluster

L'attuale iterazione di ONTAP è stata originariamente sviluppata per l'architettura storage scale-out di NetApp. Questa è l'architettura che di solito si trova nelle implementazioni dei data center di ONTAP. Poiché questa implementazione esercita la maggior parte delle funzionalità di ONTAP, è un buon punto di partenza per comprendere i concetti che informano la tecnologia ONTAP.

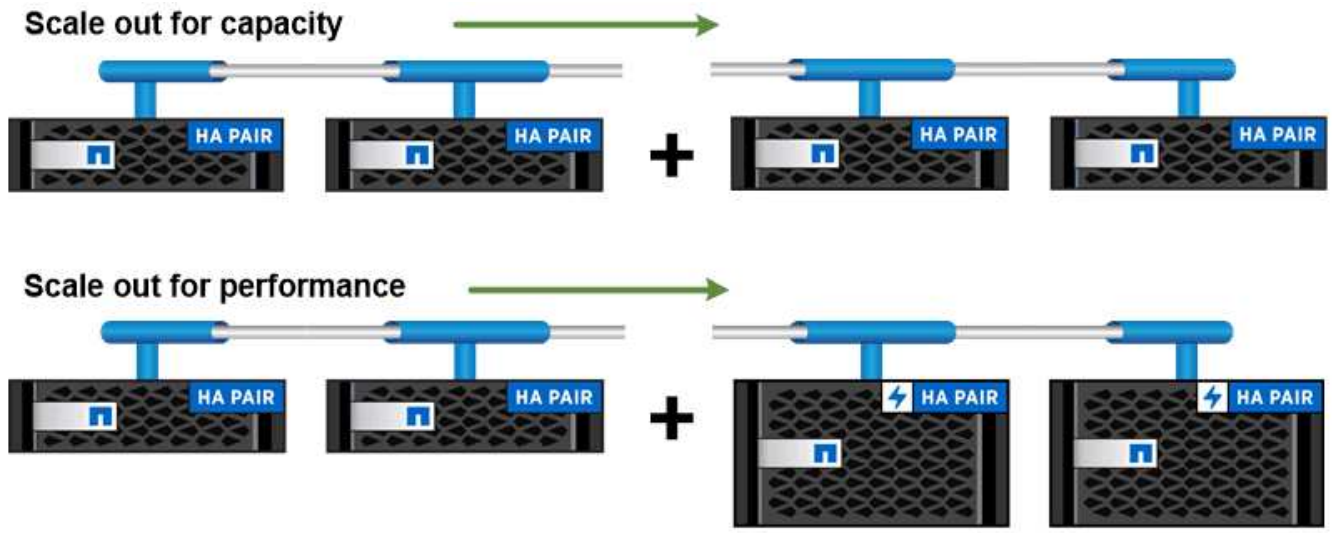
Le architetture dei data center in genere implementano controller FAS o AFF dedicati che eseguono il software di gestione dei dati ONTAP. Ciascun controller, il relativo storage, la connettività di rete e l'istanza di ONTAP in esecuzione sul controller sono denominati *node.*

I nodi sono accoppiati per l'alta disponibilità (ha). Insieme, queste coppie (fino a 12 nodi per SAN, fino a 24 nodi per NAS) comprendono il cluster. I nodi comunicano tra loro tramite un'interconnessione cluster dedicata privata.

A seconda del modello di controller, lo storage a nodi è costituito da dischi flash, dischi di capacità o entrambi. Le porte di rete sul controller forniscono l'accesso ai dati. Le risorse di storage fisico e di connettività di rete sono virtualizzate, visibili solo agli amministratori del cluster, non ai client NAS o agli host SAN.

I nodi di una coppia ha devono utilizzare lo stesso modello di array di storage. In caso contrario, è possibile utilizzare qualsiasi combinazione di controller supportata. Puoi scalare in base alla capacità aggiungendo nodi con modelli di storage array simili o per le performance aggiungendo nodi con storage array di fascia superiore.

Naturalmente è possibile scalare in alto anche in tutti i modi tradizionali, aggiornando dischi o controller in base alle esigenze. L'infrastruttura di storage virtualizzata di ONTAP semplifica lo spostamento dei dati senza interruzioni, consentendoti di scalare verticalmente o orizzontalmente senza downtime.



You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

Coppie ad alta disponibilità

I nodi del cluster sono configurati in *coppie ad alta disponibilità (ha)* per la fault tolerance e le operazioni senza interruzioni. Se un nodo si guasta o se è necessario interrompere un nodo per la manutenzione ordinaria, il partner può *assumere* il proprio storage e continuare a fornire i dati da esso. Il partner _restituisce lo storage quando il nodo viene riportato in linea.

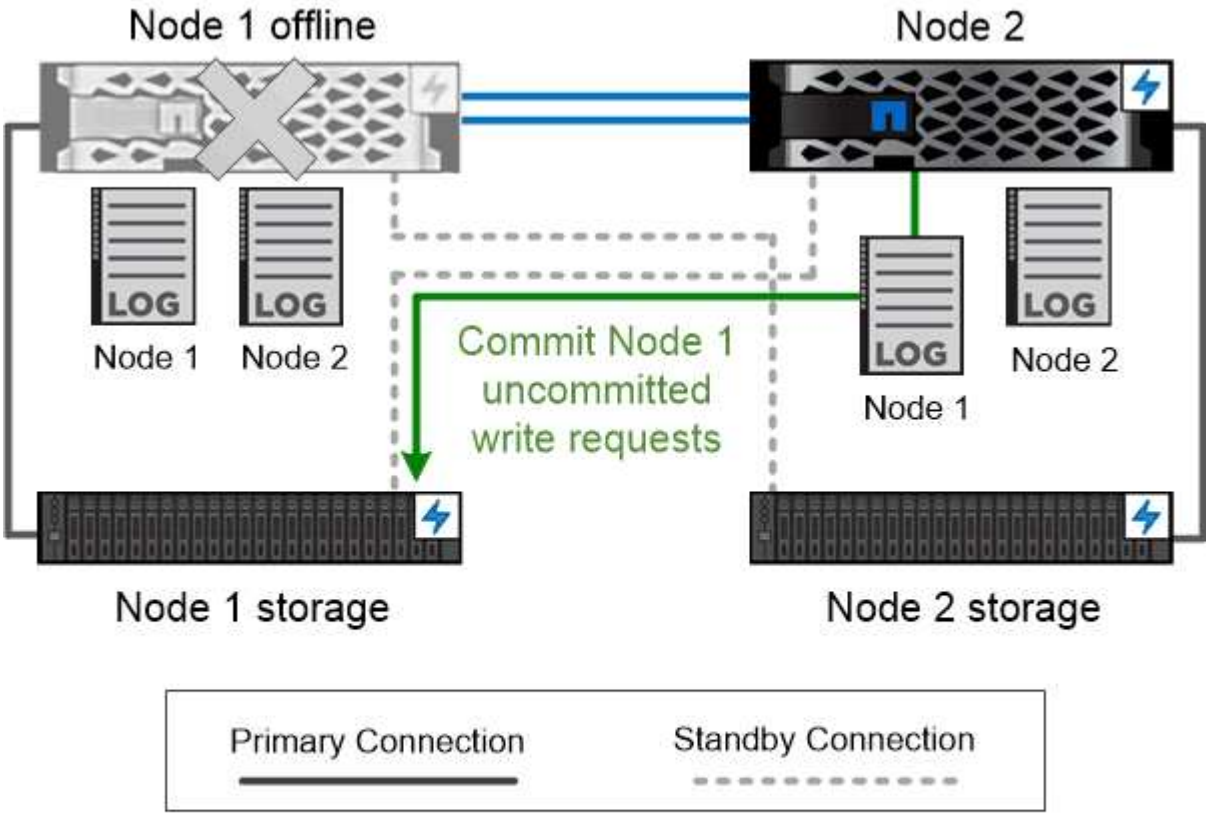
Le coppie HA sono sempre costituite da modelli di controller simili. In genere, i controller risiedono nello stesso chassis con alimentatori ridondanti.

Le coppie ha sono nodi con tolleranza agli errori in grado di comunicare tra loro in modi diversi per consentire

a ciascun nodo di verificare continuamente se il proprio partner funziona e di mirrorare i dati di registro per la memoria non volatile dell'altro. Quando una richiesta di scrittura viene effettuata a un nodo, viene registrata nella NVRAM su entrambi i nodi prima che una risposta venga rinviata al client o all'host. In caso di failover, il partner superstite impegna le richieste di scrittura non assegnate del nodo guasto sul disco, garantendo la coerenza dei dati.

Le connessioni ai supporti di storage dell'altro controller consentono a ciascun nodo di accedere allo storage dell'altro in caso di takeover. I meccanismi di failover del percorso di rete garantiscono che client e host continuino a comunicare con il nodo esistente.

Per garantire la disponibilità, è necessario mantenere l'utilizzo della capacità delle performance su entrambi i nodi al 50% per adattarsi al carico di lavoro aggiuntivo nel caso di failover. Per lo stesso motivo, è possibile configurare non più del 50% del numero massimo di interfacce di rete virtuale NAS per un nodo.



On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

Takeover e giveback nelle implementazioni virtualizzate di ONTAP

Lo storage non viene condiviso tra nodi in implementazioni ONTAP virtualizzate "hared-nothing `s`" come Cloud Volumes ONTAP per AWS o ONTAP Select. Quando un nodo non funziona, il suo partner continua a fornire i dati da una copia sincrona dei dati del nodo con mirroring. Non prende il controllo dello storage del nodo, ma solo della funzione di data serving.

Consulente digitale AutoSupport e Active IQ

ONTAP offre il monitoraggio e il reporting dei sistemi basati sull'intelligenza artificiale attraverso un portale web e un'app mobile. Il componente AutoSupport di ONTAP invia la telemetria che viene analizzata dal consulente digitale Active IQ.

Active IQ ti consente di ottimizzare la tua infrastruttura dati nel tuo cloud ibrido globale offrendo analisi predittive e supporto proattivo attraverso un portale basato sul cloud e un'app mobile. Le informazioni e i consigli di Active IQ basati sui dati sono disponibili per tutti i clienti NetApp con un contratto SupportEdge attivo (le funzionalità variano in base al prodotto e al livello di supporto).

Ecco alcune cose che puoi fare con Active IQ:

- Pianificare gli aggiornamenti. Active IQ identifica i problemi dell'ambiente che possono essere risolti eseguendo l'aggiornamento a una versione più recente di ONTAP e il componente preparazione aggiornamento consente di pianificare un aggiornamento corretto.
- Visualizza lo stato di salute del sistema. La dashboard di Active IQ segnala eventuali problemi relativi allo stato di salute e ti aiuta a correggerli. Monitorare la capacità del sistema per assicurarsi di non esaurire mai lo spazio di storage.
- Gestire le performance. Active IQ mostra le performance del sistema in un periodo più lungo di quello che puoi vedere in Gestione sistema. Identificare i problemi di configurazione e di sistema che influiscono sulle performance.
- Massimizza l'efficienza. Visualizza le metriche di efficienza dello storage e identifica i modi per memorizzare più dati in meno spazio.
- Visualizza l'inventario e la configurazione. Active IQ visualizza l'inventario completo e le informazioni di configurazione software e hardware. Verificare la scadenza dei contratti di servizio per garantire la garanzia di una copertura.

Informazioni correlate

"Documentazione NetApp: Consulente digitale Active IQ"

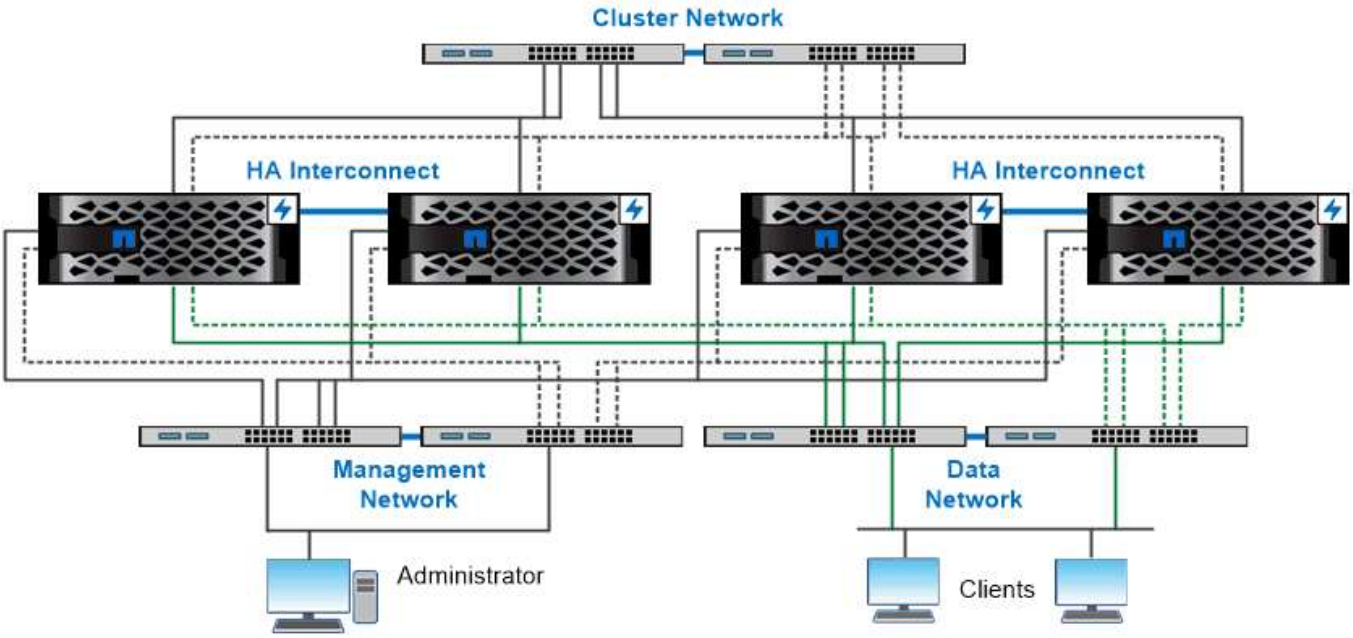
"Avviare Active IQ"

"Servizi SupportEdge"

Architettura di rete

Panoramica dell'architettura di rete

L'architettura di rete per un'implementazione di un data center ONTAP in genere è costituita da un'interconnessione cluster, una rete di gestione per l'amministrazione del cluster e una rete dati. Le schede di interfaccia di rete (NIC) forniscono porte fisiche per le connessioni Ethernet. Gli HBA (host bus adapter) forniscono porte fisiche per le connessioni FC.



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

Porte logiche

Oltre alle porte fisiche fornite su ciascun nodo, è possibile utilizzare *porte logiche* per gestire il traffico di rete. Le porte logiche sono gruppi di interfacce o VLAN.

Gruppi di interfacce

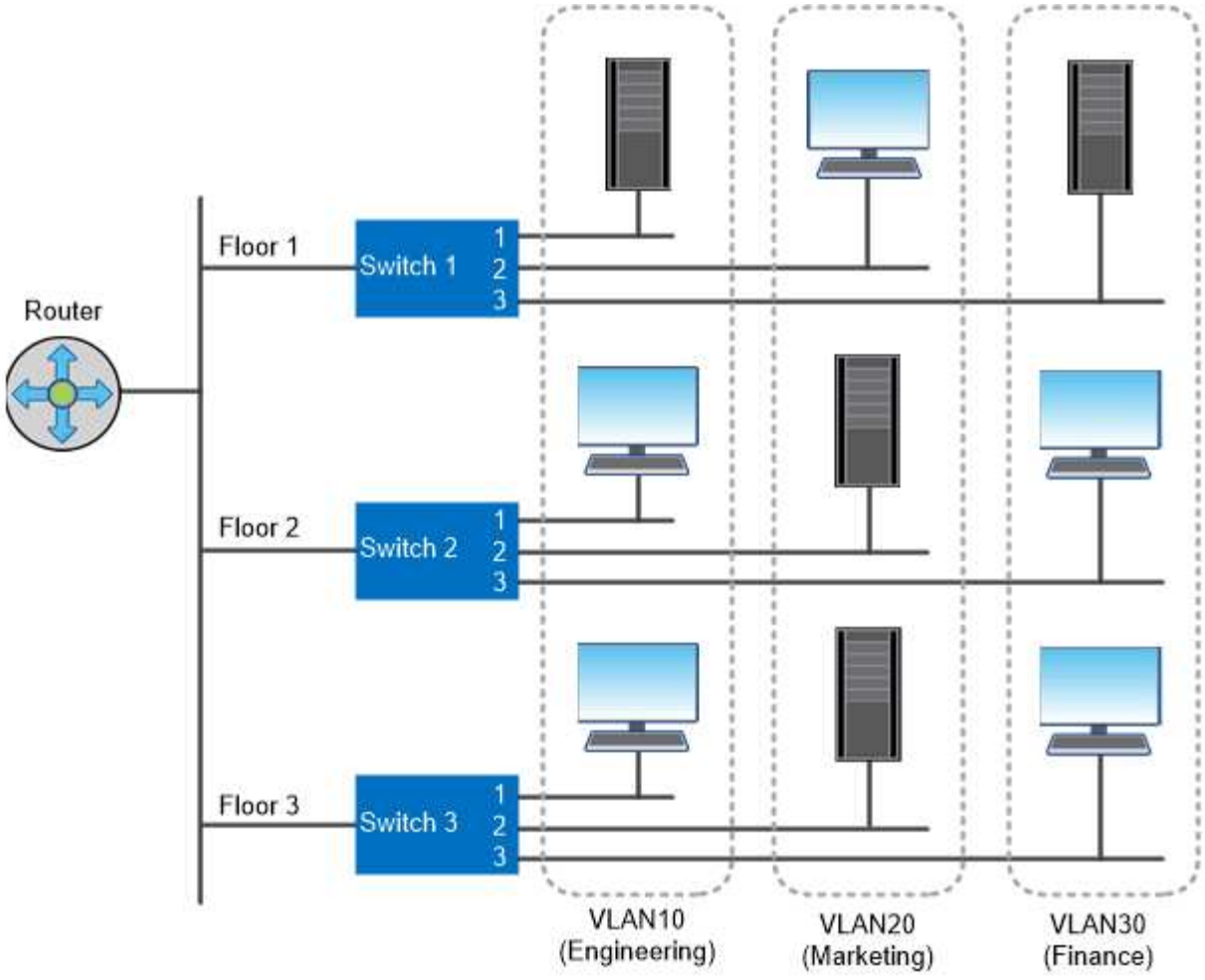
Gruppi di interfacce combina più porte fisiche in una singola “porta trunk” logica. È possibile creare un gruppo di interfacce costituito da porte provenienti da NIC in slot PCI diversi per evitare un errore di slot che riduce il traffico business-critical.

Un gruppo di interfacce può essere monomodale, multimodale o multimodale dinamica. Ogni modalità offre diversi livelli di tolleranza agli errori. Per bilanciare il carico del traffico di rete, è possibile utilizzare entrambi i tipi di gruppo di interfacce multimodali.

VLAN

VLAN separa il traffico da una porta di rete (che potrebbe essere un gruppo di interfacce) in segmenti logici definiti in base alla porta dello switch, piuttosto che in base ai confini fisici. Le *stazioni finali* appartenenti a una VLAN sono correlate in base alla funzione o all’applicazione.

È possibile raggruppare le stazioni finali per reparto, ad esempio Engineering and Marketing, o per progetto, ad esempio release1 e release2. Poiché la prossimità fisica delle stazioni finali è irrilevante in una VLAN, le stazioni finali possono essere geograficamente remote.



You can use VLANs to segregate traffic by department.

Supporto per tecnologie di rete standard di settore

ONTAP supporta tutte le principali tecnologie di rete standard di settore. Le tecnologie chiave includono IPspaces, bilanciamento del carico DNS e trap SNMP.

I domini di broadcast, i gruppi di failover e le subnet sono descritti nella Failover del percorso NAS.

IPspaces

È possibile utilizzare un *IPSpace* per creare uno spazio di indirizzi IP distinto per ciascun server di dati virtuale in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

Un provider di servizi, ad esempio, potrebbe configurare diversi spazi IP per i tenant utilizzando gli stessi indirizzi IP per accedere a un cluster.

Bilanciamento del carico DNS

È possibile utilizzare *bilanciamento del carico DNS* per distribuire il traffico di rete degli utenti tra le porte disponibili. Un server DNS seleziona dinamicamente un'interfaccia di rete per il traffico in base al numero di client montati sull'interfaccia.

Trap SNMP

È possibile utilizzare *trap SNMP* per controllare periodicamente la presenza di soglie operative o errori. I trap SNMP catturano le informazioni di monitoraggio del sistema inviate in modo asincrono da un agente SNMP a un gestore SNMP.

Conformità FIPS

ONTAP è conforme agli standard federali sull'elaborazione delle informazioni (FIPS) 140-2 per tutte le connessioni SSL. È possibile attivare e disattivare la modalità SSL FIPS, impostare i protocolli SSL a livello globale e disattivare le crittografie deboli come RC4.

Panoramica di RDMA

Le offerte Remote Direct Memory Access (RDMA) di ONTAP supportano carichi di lavoro sensibili alla latenza e a elevata larghezza di banda. RDMA consente di copiare i dati direttamente tra la memoria del sistema di storage e la memoria del sistema host, eludendo le interruzioni della CPU e l'overhead.

NFS su RDMA

A partire da ONTAP 9.10.1, è possibile eseguire la configurazione "NFS su RDMA" Per consentire l'utilizzo dello storage NVIDIA GPUDirect per carichi di lavoro con accelerazione GPU su host con GPU NVIDIA supportate.

Interconnessione del cluster RDMA

L'interconnessione del cluster RDMA riduce la latenza, riduce i tempi di failover e accelera la comunicazione tra i nodi di un cluster.

A partire da ONTAP 9.10.1, cluster Interconnect RDMA è supportato per determinati sistemi hardware, se utilizzato con le schede di rete del cluster X1151A. A partire da ONTAP 9.13.1, le schede di rete X91153A supportano anche la interconnessione in cluster RDMA. Consultare la tabella per sapere quali sistemi sono supportati nelle diverse versioni di ONTAP.

Sistemi	Versioni di ONTAP supportate
• R400 • ASA A400	ONTAP 9.10.1 e versioni successive
• AFF A900 • ASA A900 • FAS9500	ONTAP 9.13.1 e versioni successive

Data l'impostazione appropriata del sistema di storage, non è necessaria alcuna configurazione aggiuntiva per utilizzare l'interconnessione RDMA.

Protocolli client

ONTAP supporta tutti i principali protocolli client standard di settore: NFS, SMB, FC,

FCoE, iSCSI, NVMe/FC e S3.

NFS

NFS è il protocollo di accesso ai file tradizionale per i sistemi UNIX e LINUX. I client possono accedere ai file in volumi ONTAP utilizzando i seguenti protocolli.

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- PNFS

È possibile controllare l'accesso ai file utilizzando permessi di stile UNIX, permessi di stile NTFS o una combinazione di entrambi.

I client possono accedere agli stessi file utilizzando i protocolli NFS e SMB.

PMI

SMB è il protocollo di accesso ai file tradizionale per i sistemi Windows. I client possono accedere ai file nei volumi ONTAP utilizzando i protocolli SMB 2.0, SMB 2.1, SMB 3.0 e SMB 3.1.1. Come per NFS, sono supportati diversi stili di permesso.

SMB 1.0 è disponibile ma disattivato per impostazione predefinita in ONTAP 9.3 e versioni successive.

FC

Fibre Channel è il protocollo a blocchi di rete originale. Al posto dei file, un protocollo a blocchi presenta un intero disco virtuale a un client. Il protocollo FC tradizionale utilizza una rete FC dedicata con switch FC specializzati e richiede che il computer client disponga di interfacce di rete FC.

Un LUN rappresenta il disco virtuale e uno o più LUN vengono memorizzati in un volume ONTAP. È possibile accedere allo stesso LUN attraverso i protocolli FC, FCoE e iSCSI, ma più client possono accedere allo stesso LUN solo se fanno parte di un cluster che impedisce collisioni in scrittura.

FCoE

FCoE è fondamentalmente lo stesso protocollo di FC, ma utilizza una rete Ethernet di livello datacenter al posto del trasporto FC tradizionale. Il client richiede ancora un'interfaccia di rete specifica per FCoE.

ISCSI

ISCSI è un protocollo a blocchi che può essere eseguito su reti Ethernet standard. La maggior parte dei sistemi operativi client offre un iniziatore software che viene eseguito su una porta Ethernet standard. ISCSI è una buona scelta quando è necessario un protocollo a blocchi per una particolare applicazione, ma non è disponibile una rete FC dedicata.

NVMe/FC

Il più recente protocollo a blocchi, NVMe/FC, è progettato specificamente per funzionare con lo storage basato

su flash. Offre sessioni scalabili, una significativa riduzione della latenza e un aumento del parallelismo, il che lo rende ideale per applicazioni a bassa latenza e throughput elevato, come database in-memory e analytics.

A differenza di FC e iSCSI, NVMe non utilizza LUN. Utilizza invece spazi dei nomi, memorizzati in un volume ONTAP. È possibile accedere agli spazi dei nomi NVMe solo tramite il protocollo NVMe.

S3

A partire da ONTAP 9.8, è possibile attivare un server S3 (Simple Storage Service) di ONTAP in un cluster ONTAP, consentendo di fornire i dati nello storage a oggetti utilizzando i bucket S3.

ONTAP supporta due scenari di casi d'utilizzo on-premise per il servizio dello storage a oggetti S3:

- Tier FabricPool per un bucket su cluster locale (Tier to a local bucket) o cluster remoto (Tier cloud).
- Accesso dell'applicazione client S3 a un bucket sul cluster locale o su un cluster remoto.

> ONTAP S3 è adatto per le funzionalità S3 sui cluster esistenti senza hardware e gestione aggiuntivi. Per implementazioni superiori a 300 TB, il software NetApp StorageGRID continua a essere la soluzione di punta per lo storage a oggetti. Scopri di più "StorageGRID".

Dischi e aggregati

= :allow-uri-read:

Tier locali (aggregati) e gruppi RAID

Le moderne tecnologie RAID proteggono dai guasti dei dischi ricostruendo i dati di un disco guasto su un disco spare. Il sistema confronta le informazioni di indice su un "disco di parità" con i dati sui dischi integri rimanenti per ricostruire i dati mancanti, il tutto senza downtime o costi significativi per le performance.

Un Tier locale (aggregato) è costituito da uno o più *gruppi RAID*. Il *tipo RAID* del livello locale determina il numero di dischi di parità nel gruppo RAID e il numero di guasti simultanei dei dischi da cui la configurazione RAID protegge.

Il tipo RAID predefinito, RAID-DP (RAID-Double Parity), richiede due dischi di parità per gruppo RAID e protegge dalla perdita di dati in caso di guasto di due dischi contemporaneamente. Per RAID-DP, la dimensione del gruppo RAID consigliata è compresa tra 12 e 20 HDD e tra 20 e 28 SSD.

È possibile distribuire il costo di overhead dei dischi di parità creando gruppi RAID all'estremità più alta della raccomandazione di dimensionamento. Questo vale soprattutto per gli SSD, che sono molto più affidabili dei dischi con capacità. Per i Tier locali che utilizzano HDD, è necessario bilanciare la necessità di massimizzare lo storage su disco rispetto a fattori compensativi come il tempo di ricostruzione più lungo richiesto per gruppi RAID più grandi.

Tier locali mirrorati e senza mirror (aggregati)

ONTAP dispone di una funzionalità opzionale denominata *SyncMirror* che è possibile utilizzare per eseguire il mirroring sincrono dei dati del Tier locale (aggregato) nelle copie, o *plex*, memorizzate in diversi gruppi RAID. I plex garantiscono la protezione contro la perdita di dati in caso di guasti di più dischi rispetto al tipo RAID o in caso di perdita di

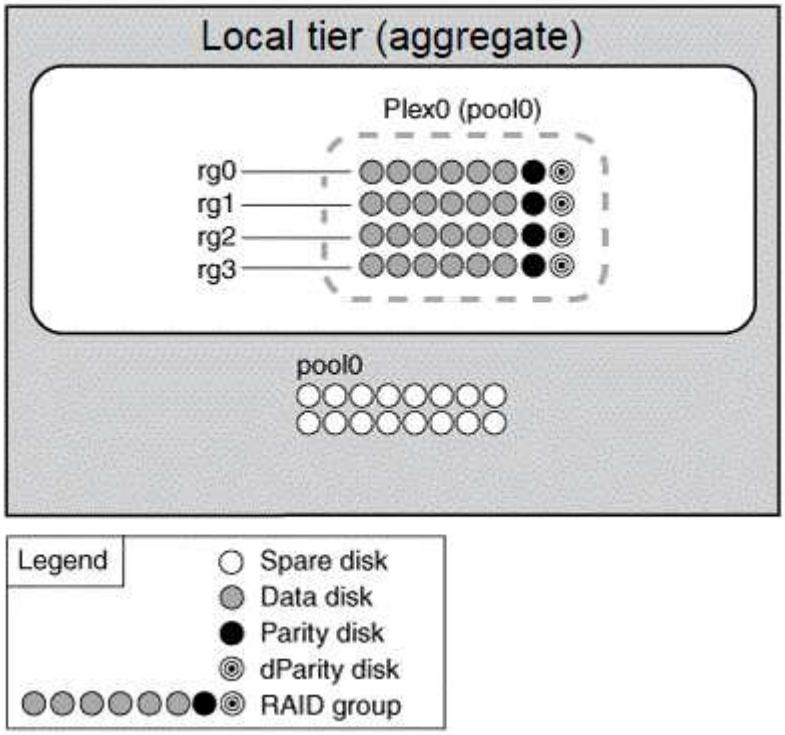
connettività ai dischi del gruppo RAID.

Quando si crea un Tier locale con System Manager o utilizzando la CLI, è possibile specificare che il Tier locale sia mirrorato o senza mirror.

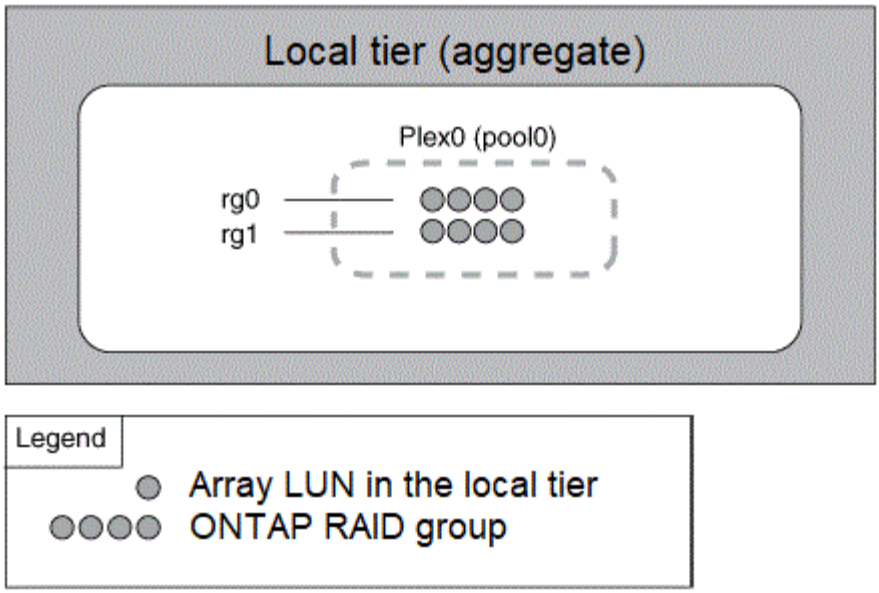
Come funzionano i Tier locali senza mirror (aggregati)

Se non si specifica il mirroring dei Tier locali, questi vengono creati come Tier locali senza mirror (aggregati). I Tier locali senza mirror dispongono di un solo *plex* (una copia dei dati), che contiene tutti i gruppi RAID appartenenti a quel Tier locale.

Il diagramma seguente mostra un Tier locale senza mirror composto da dischi, con il suo unico plex. Il Tier locale dispone di quattro gruppi RAID: Rg0, rg1, rg2 e rg3. Ciascun gruppo RAID dispone di sei dischi dati, un disco di parità e un disco di parità doppia. Tutti i dischi utilizzati dal Tier locale provengono dallo stesso pool, “pool0”.



Il seguente diagramma mostra un Tier locale senza mirror con LUN di array, con un unico plex. Ha due gruppi RAID, rg0 e rg1. Tutte le LUN degli array utilizzate dal Tier locale provengono dallo stesso pool, “pool0”.



Come funzionano i Tier locali mirrorati (aggregati)

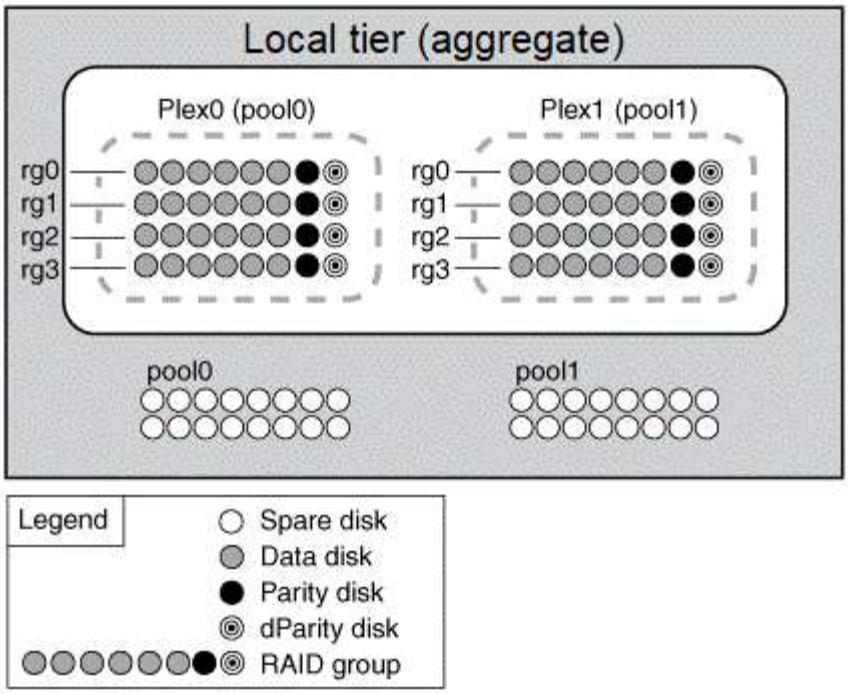
Gli aggregati mirrorati hanno due *plex* (copie dei dati), che utilizzano la funzionalità SyncMirror per duplicare i dati e fornire ridondanza.

Quando si crea un Tier locale, è possibile specificare che si tratta di un Tier locale mirrorato. Inoltre, è possibile aggiungere un secondo plex a un Tier locale senza mirror esistente per renderlo un Tier mirrorato. Utilizzando la funzionalità SyncMirror, ONTAP copia i dati nel plesso originale (plex0) nel nuovo plesso (plex1). I plex sono fisicamente separati (ogni plesso ha i propri gruppi RAID e il proprio pool) e i plex vengono aggiornati simultaneamente.

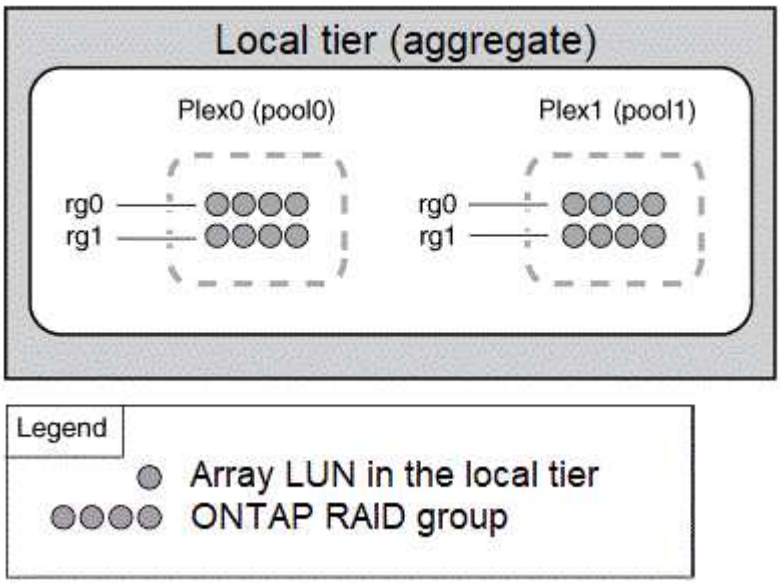
Questa configurazione offre una protezione aggiuntiva contro la perdita di dati in caso di guasti di più dischi rispetto al livello RAID dell'aggregato, in quanto il plex non interessato continua a fornire dati mentre si corregge la causa dell'errore. Una volta risolto il problema, i due plessi risincronizzano e ristabiliscono la relazione di mirroring.

I dischi e le LUN degli array sul sistema sono divisi in due pool: "pool0" e "pool1". Plex0 ottiene lo storage dal pool0 e Plex1 lo ottiene dal pool1.

Il seguente diagramma mostra un Tier locale composto da dischi con la funzionalità SyncMirror attivata e implementata. È stato creato un secondo plex per il Tier locale, "plex1". I dati in plex1 sono una copia dei dati in plex0 e anche i gruppi RAID sono identici. I 32 dischi spare vengono allocati al pool 0 o pool1 utilizzando 16 dischi per ciascun pool.



Il diagramma seguente mostra un Tier locale composto da LUN array con la funzionalità SyncMirror attivata e implementata. È stato creato un secondo plex per il Tier locale, “plex1”. Plex1 è una copia di plex0 e anche i gruppi RAID sono identici.



Si consiglia di mantenere almeno il 20% di spazio libero per gli aggregati con mirroring, per performance e disponibilità dello storage ottimali. Sebbene il suggerimento sia del 10% per gli aggregati non speculari, il 10% di spazio aggiuntivo può essere utilizzato dal filesystem per assorbire le modifiche incrementali. I cambiamenti incrementali aumentano l’utilizzo dello spazio per gli aggregati con mirroring grazie all’architettura copy-on-write basata su Snapshot di ONTAP. Il mancato rispetto di queste Best practice può avere un impatto negativo sulle prestazioni.

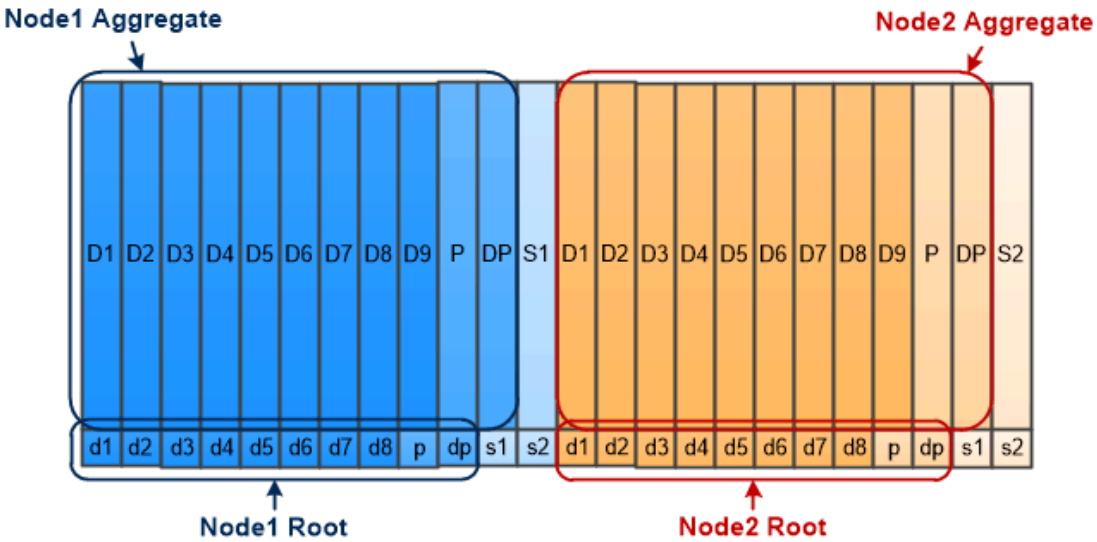
Partizione dei dati root

Ogni nodo deve disporre di un aggregato root per i file di configurazione del sistema storage. L'aggregato root ha il tipo RAID dell'aggregato di dati.

System Manager non supporta la partizione root-data o root-data-data.

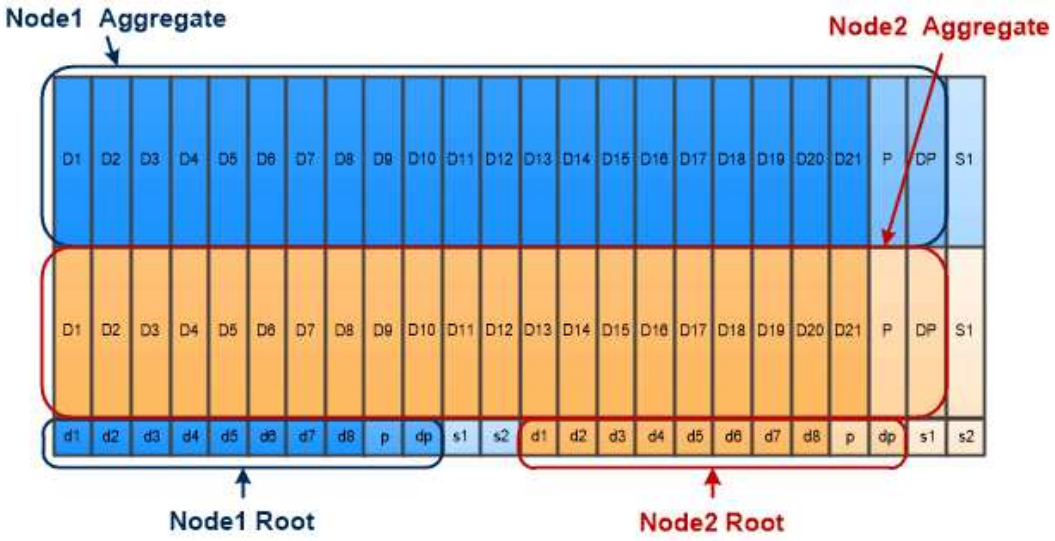
Un aggregato root di tipo RAID-DP è generalmente costituito da un disco dati e da due dischi di parità. Si tratta di una "tassa di parità" significativa da pagare per i file del sistema di storage, quando il sistema sta già riservando due dischi come dischi di parità per ciascun gruppo RAID nell'aggregato.

Partizione dei dati root riduce la tassa di parità suddividendo l'aggregato root tra le partizioni del disco, riservando una piccola partizione su ciascun disco come partizione root e una grande partizione per i dati.



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.

Come suggerisce l'illustrazione, maggiore è il numero di dischi utilizzati per memorizzare l'aggregato root, minore è la partizione root. Questo è anche il caso di una forma di partizione dei dati root denominata *root-data-data partitioning*, che crea una partizione piccola come partizione root e due partizioni più grandi e di pari dimensioni per i dati.



Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

Entrambi i tipi di partizione dei dati root fanno parte della funzione di *partizione avanzata dei dischi (ADP)* di ONTAP. Entrambi sono configurati in fabbrica: Partizione dei dati root per sistemi entry-level FAS2xxx, FAS9000, FAS8200, FAS80xx e AFF, partizione dei dati root solo per sistemi AFF.

Scopri di più "Partizione avanzata dei dischi".

Dischi partizionati e utilizzati per l'aggregato root

I dischi partizionati per l'utilizzo nell'aggregato root dipendono dalla configurazione del sistema.

Conoscere il numero di dischi utilizzati per l'aggregato root consente di determinare la quantità di capacità dei dischi riservata alla partizione root e la quantità disponibile per l'utilizzo in un aggregato di dati.

La funzionalità di partizione dei dati root è supportata per piattaforme entry-level, piattaforme All Flash FAS e piattaforme FAS con solo SSD collegati.

Per le piattaforme entry-level, vengono partizionati solo i dischi interni.

Per tutte le piattaforme Flash FAS e FAS con solo SSD collegati, tutti i dischi collegati al controller al momento dell'inizializzazione del sistema vengono partizionati, fino a un limite di 24 per nodo. Le unità aggiunte dopo la configurazione del sistema non vengono partizionate.

Volumi, qtree, file e LUN

ONTAP fornisce dati a client e host da container logici denominati *volumi FlexVol.* poiché questi volumi sono solo accoppiati in modo lasco con il loro aggregato contenente, offrono una maggiore flessibilità nella gestione dei dati rispetto ai volumi tradizionali.

È possibile assegnare più volumi FlexVol a un aggregato, ciascuno dedicato a un'applicazione o servizio diverso. È possibile espandere e contrarre un volume FlexVol, spostare un volume FlexVol ed eseguire copie efficienti di un volume FlexVol. È possibile utilizzare *qtree* per partizionare un volume FlexVol in unità più gestibili e *quote* per limitare l'utilizzo delle risorse dei volumi.

I volumi contengono file system in un ambiente NAS e LUN in un ambiente SAN. Un LUN (Logical Unit

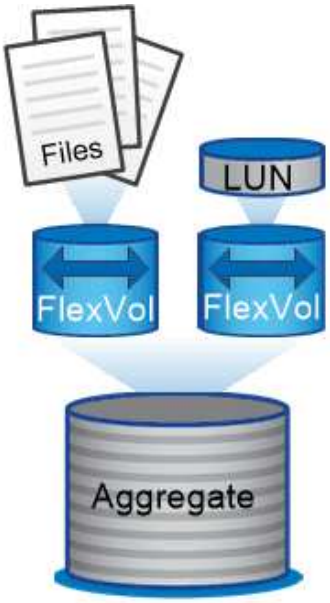
Number) è un identificatore di un dispositivo chiamato *unità logica* indirizzato da un protocollo SAN.

I LUN sono l'unità di storage di base in una configurazione SAN. L'host Windows vede le LUN del sistema storage come dischi virtuali. È possibile spostare le LUN in volumi diversi senza interruzioni in base alle esigenze.

Oltre ai volumi di dati, è necessario conoscere alcuni volumi speciali:

- Un *volume root del nodo* (in genere "vol0") contiene le informazioni di configurazione del nodo e i registri.
- Un *volume root SVM* funge da punto di ingresso allo spazio dei nomi fornito da SVM e contiene informazioni sulla directory dello spazio dei nomi.
- I *volumi di sistema* contengono metadati speciali come i registri di audit del servizio.

Non è possibile utilizzare questi volumi per memorizzare i dati.



Volumes contain files in a NAS environment and LUNs in a SAN environment.

volumi FlexGroup

In alcune aziende, un singolo namespace potrebbe richiedere petabyte di storage, superando di gran lunga anche la capacità di 100 TB di un volume FlexVol.

Un *volume FlexGroup* supporta fino a 400 miliardi di file con 200 volumi membri costitutivi che lavorano in modo collaborativo per bilanciare dinamicamente l'allocazione di carico e spazio in modo uniforme tra tutti i membri.

Con un volume FlexGroup non è necessario alcun overhead di gestione o manutenzione. È sufficiente creare il volume FlexGroup e condividerlo con i client NAS. ONTAP fa il resto.

Virtualizzazione dello storage

Panoramica sulla virtualizzazione dello storage

Utilizzate *macchine virtuali storage (SVM)* per fornire dati a client e host. Come una macchina virtuale in esecuzione su un hypervisor, una SVM è un'entità logica che astratta le risorse fisiche. I dati a cui si accede tramite SVM non sono legati a una posizione nello storage. L'accesso di rete alla SVM non è vincolato a una porta fisica.

> In precedenza, le SVM erano chiamate "vserver". L'interfaccia della riga di comando di ONTAP utilizza ancora il termine "vserver".

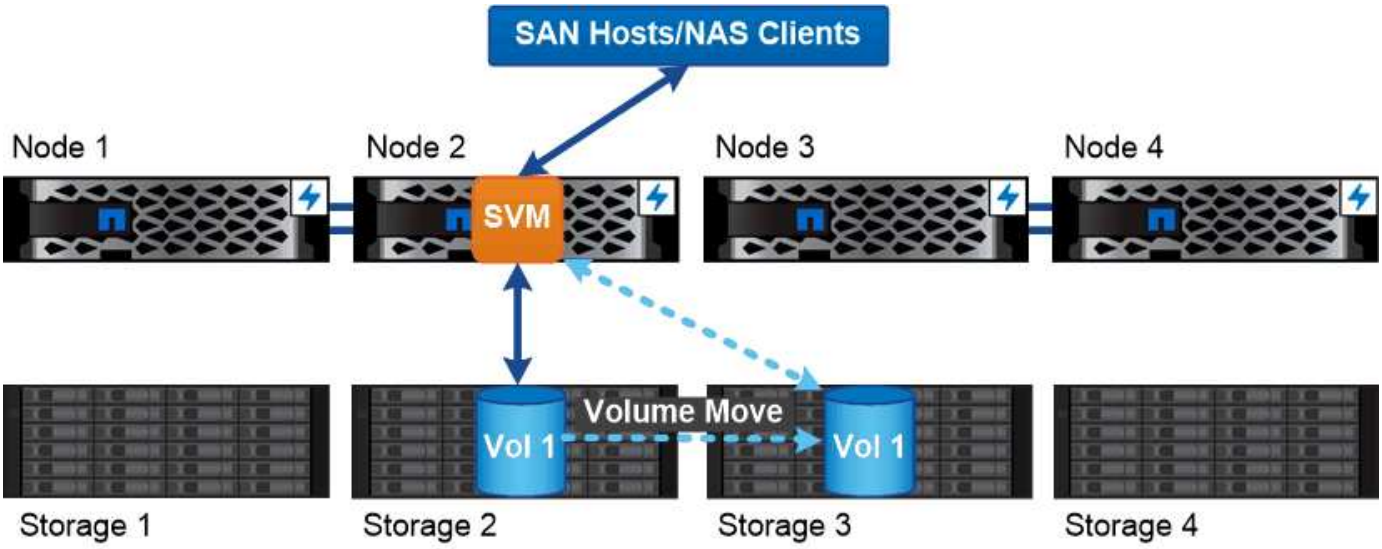
Una SVM fornisce i dati a client e host da uno o più volumi, attraverso una o più *interfacce logiche (LIF)* di rete. I volumi possono essere assegnati a qualsiasi aggregato di dati nel cluster. Le LIF possono essere ospitate da qualsiasi porta fisica o logica. Sia i volumi che le LIF possono essere spostati senza interrompere il servizio dati, sia che tu stia eseguendo aggiornamenti hardware, aggiungendo nodi, bilanciando le performance o ottimizzando la capacità tra gli aggregati.

La stessa SVM può avere una LIF per il traffico NAS e una LIF per il traffico SAN. Per accedere a SVM, i client e gli host necessitano solo dell'indirizzo LIF (indirizzo IP per NFS, SMB o iSCSI; WWPN per FC). I LIF mantengono i propri indirizzi mentre si spostano. Le porte possono ospitare più LIF. Ogni SVM dispone di sicurezza, amministrazione e spazio dei nomi propri.

Oltre alle SVM dei dati, ONTAP implementa speciali SVM per l'amministrazione:

- Una *SVM amministrativa* viene creata quando il cluster viene configurato.
- Un *nodo SVM* viene creato quando un nodo si unisce a un cluster nuovo o esistente.
- Viene creata automaticamente una *SVM di sistema* per le comunicazioni a livello di cluster in un IPSpace.

Non è possibile utilizzare queste SVM per la distribuzione dei dati. Esistono inoltre LIF speciali per il traffico all'interno e tra i cluster e per la gestione di cluster e nodi.



Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.

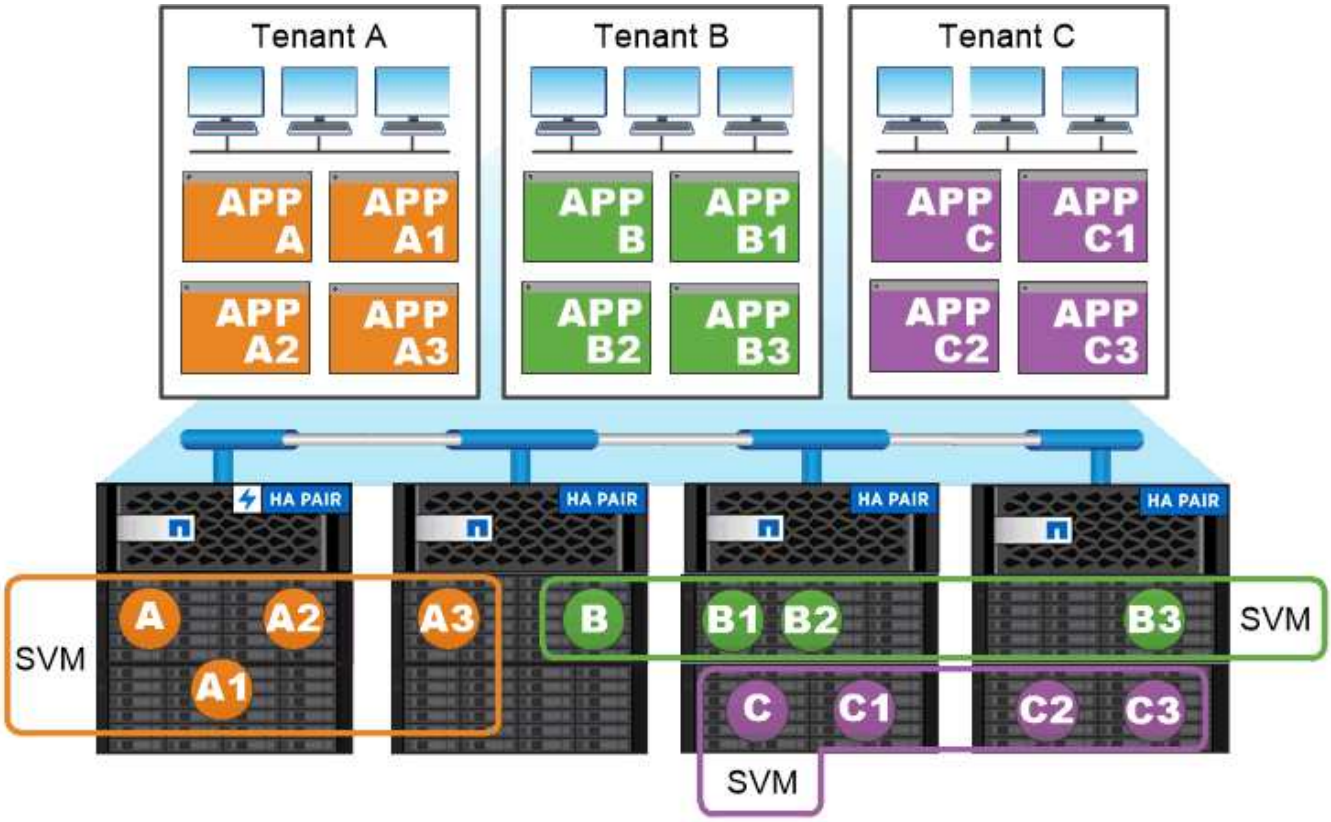
Perché ONTAP è come il middleware

Gli oggetti logici utilizzati da ONTAP per le attività di gestione dello storage soddisfano gli obiettivi familiari di un pacchetto middleware ben progettato: Proteggere l'amministratore dai dettagli di implementazione di basso livello e isolare la configurazione dalle modifiche delle caratteristiche fisiche come nodi e porte. L'idea di base è che l'amministratore dovrebbe essere in grado di spostare facilmente volumi e LIF, riconfigurando alcuni campi piuttosto che l'intera infrastruttura di storage.

Casi di utilizzo di SVM

I service provider utilizzano le SVM in accordi di multi-tenancy sicuri per isolare i dati di ciascun tenant, fornire a ciascun tenant la propria autenticazione e amministrazione e semplificare il chargeback. È possibile assegnare più LIF alla stessa SVM per soddisfare le diverse esigenze dei clienti e utilizzare la QoS per proteggere dai carichi di lavoro dei tenant "bullismo" dei carichi di lavoro degli altri tenant.

Gli amministratori utilizzano le SVM per scopi simili all'interno dell'azienda. È possibile separare i dati da diversi reparti o mantenere i volumi di storage a cui accedono gli host in una SVM e i volumi di condivisione utente in un'altra. Alcuni amministratori mettono LUN iSCSI/FC e datastore NFS in una condivisione SVM e SMB in un'altra.



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

Amministrazione di cluster e SVM

Un *amministratore del cluster* accede alla SVM amministrativa per il cluster. La SVM amministrativa e un amministratore del cluster con il nome riservato `admin` vengono creati automaticamente quando viene configurato il cluster.

Un amministratore del cluster con l'impostazione predefinita `admin` il ruolo può amministrare l'intero cluster e le relative risorse. L'amministratore del cluster può creare ulteriori amministratori del cluster con ruoli diversi in base alle esigenze.

Un *amministratore SVM* accede a una SVM di dati. L'amministratore del cluster crea gli amministratori SVM e SVM dei dati in base alle necessità.

Agli amministratori di SVM viene assegnato il `vsadmin` ruolo per impostazione predefinita. L'amministratore del cluster può assegnare ruoli diversi agli amministratori SVM in base alle esigenze.

RBAC (role-based Access Control)

Il *ruolo* assegnato a un amministratore determina i comandi a cui l'amministratore ha accesso. Il ruolo viene assegnato quando si crea l'account per l'amministratore. È possibile assegnare un ruolo diverso o definire ruoli personalizzati in base alle esigenze.

Spazi dei nomi e punti di giunzione

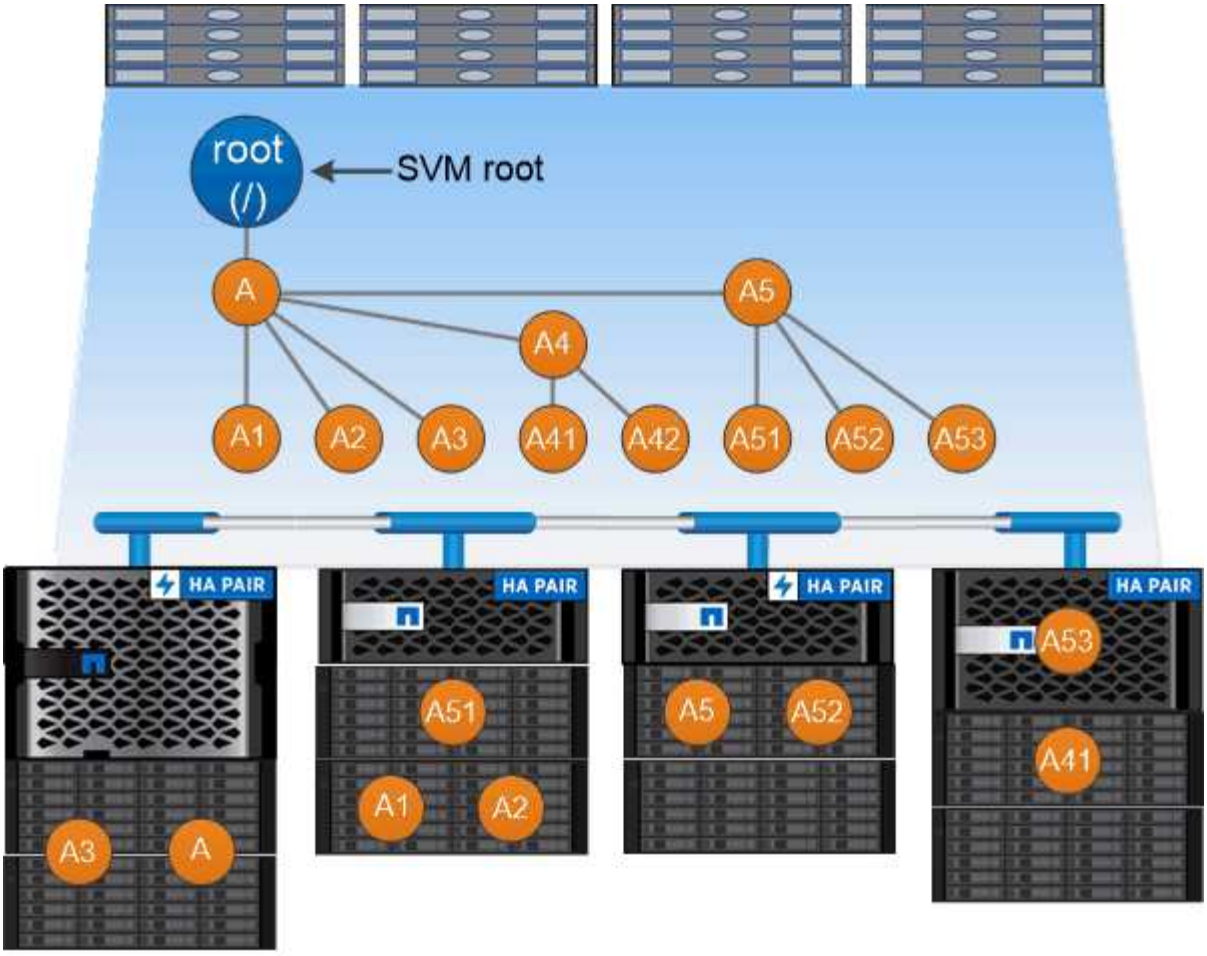
Un *namespace* NAS è un raggruppamento logico di volumi Uniti in *punti di giunzione* per creare una singola gerarchia di file system. Un client con autorizzazioni sufficienti può accedere ai file nello spazio dei nomi senza specificare la posizione dei file nello storage. I volumi Junctioned possono risiedere in qualsiasi punto del cluster.

Invece di montare ogni volume contenente un file di interesse, i client NAS montano un NFS *export* o accedono a una *share.* SMB. L'esportazione o la condivisione rappresenta l'intero namespace o una posizione intermedia all'interno dello spazio dei nomi. Il client accede solo ai volumi montati sotto il proprio access point.

È possibile aggiungere volumi allo spazio dei nomi in base alle esigenze. È possibile creare punti di giunzione direttamente sotto una giunzione di un volume padre o in una directory all'interno di un volume. Il percorso di una giunzione di volume per un volume denominato "vol3" potrebbe essere `/vol1/vol2/vol3`, o. `/vol1/dir2/vol3`, o persino `/dir1/dir2/vol3`. Il percorso è chiamato *percorso di giunzione.*

Ogni SVM dispone di uno spazio dei nomi univoco. Il volume root SVM è il punto di ingresso della gerarchia dello spazio dei nomi.

Per garantire che i dati rimangano disponibili in caso di interruzione o failover di un nodo, è necessario creare una copia *mirror per la condivisione del carico* per il volume root SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Esempio

Nell'esempio riportato di seguito viene creato un volume denominato "home4" situato su SVM vs1 con un percorso di giunzione `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Failover del percorso

Panoramica del failover del percorso

Esistono importanti differenze nel modo in cui ONTAP gestisce il failover del percorso nelle topologie NAS e SAN. Una LIF NAS esegue automaticamente la migrazione a una porta di rete diversa dopo un errore di collegamento. Un LIF SAN non esegue la migrazione (a meno che non venga spostato manualmente dopo l'errore). Invece, la tecnologia multipathing sull'host devia il traffico verso una LIF diversa, sulla stessa SVM,

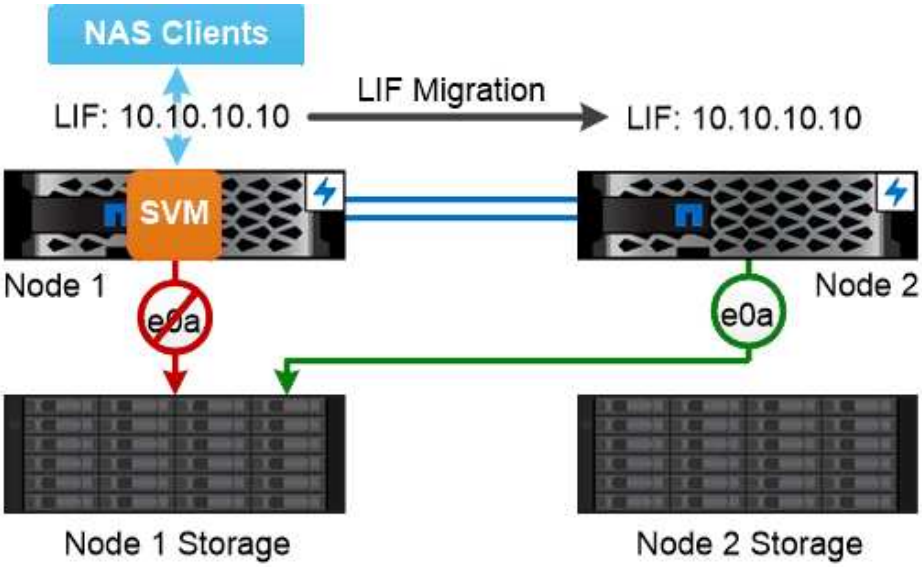
ma accede a una porta di rete diversa.

Failover del percorso NAS

Un LIF NAS esegue automaticamente la migrazione a una porta di rete esistente dopo un errore di collegamento sulla porta corrente. La porta alla quale LIF migra deve essere membro del *gruppo di failover* per LIF. La *policy di gruppo di failover* restringe le destinazioni di failover per un LIF di dati alle porte sul nodo che possiede i dati e il suo partner ha.

Per comodità amministrativa, ONTAP crea un gruppo di failover per ogni *dominio di trasmissione* nell'architettura di rete. I domini di broadcast raggruppano le porte appartenenti alla stessa rete Layer 2. Se, ad esempio, si utilizzano VLAN per separare il traffico in base al reparto (Engineering, Marketing, Finance e così via), ogni VLAN definisce un dominio di trasmissione separato. Il gruppo di failover associato al dominio di trasmissione viene aggiornato automaticamente ogni volta che si aggiunge o rimuove una porta del dominio di trasmissione.

È quasi sempre consigliabile utilizzare un dominio di broadcast per definire un gruppo di failover per garantire che il gruppo di failover rimanga aggiornato. Talvolta, tuttavia, è possibile definire un gruppo di failover non associato a un dominio di broadcast. Ad esempio, è possibile che si desideri eseguire il failover delle LIF solo sulle porte di un sottoinsieme delle porte definite nel dominio di trasmissione.



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

subnet

Una *subnet* riserva un blocco di indirizzi IP in un dominio di trasmissione. Questi indirizzi appartengono alla stessa rete Layer 3 e vengono allocati alle porte nel dominio di trasmissione quando si crea una LIF. In genere, quando si definisce un indirizzo LIF, è più semplice e meno soggetto a errori specificare un nome di subnet che specificare un indirizzo IP e una maschera di rete.

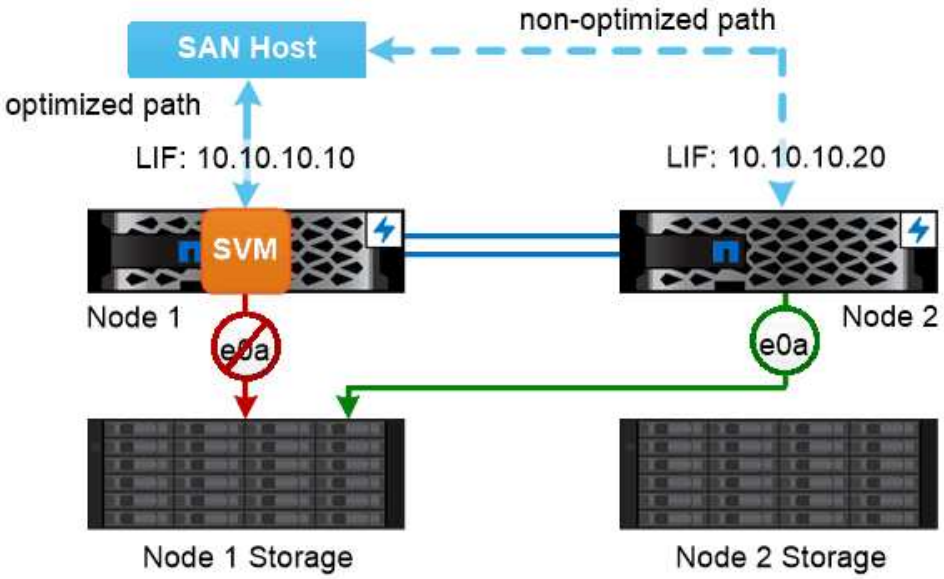
Failover del percorso SAN

Un host SAN utilizza ALUA (Asymmetric Logical Unit Access) e MPIO (Multipath i/o) per reindirizzare il traffico a una LIF sopravvissuta dopo un errore di collegamento. I percorsi predefiniti determinano i possibili percorsi verso il LUN serviti da SVM.

In un ambiente SAN, gli host sono considerati *iniziatori* di richieste a LUN *targets.* MPIO consente percorsi multipli dagli iniziatori alle destinazioni. ALUA identifica i percorsi più diretti, denominati *percorsi ottimizzati.*

In genere, si configurano più percorsi ottimizzati per le LIF sul nodo proprietario del LUN e più percorsi non ottimizzati per le LIF sul partner ha. In caso di guasto di una porta sul nodo proprietario, l'host instrada il traffico verso le porte sopravvissute. Se tutte le porte si guastano, l'host instrada il traffico sui percorsi non ottimizzati.

Per impostazione predefinita, la mappa LUN selettiva (SLM) di ONTAP limita il numero di percorsi dall'host a un LUN. Un LUN appena creato è accessibile solo attraverso i percorsi verso il nodo proprietario del LUN o del suo partner ha. È inoltre possibile limitare l'accesso a un LUN configurando i LIF in un *set di porte* per l'iniziatore.



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

spostamento di volumi in ambienti SAN

Per impostazione predefinita, ONTAP *Selective LUN Map (SLM)* limita il numero di percorsi a un LUN da un host SAN. Un LUN appena creato è accessibile solo attraverso i percorsi al nodo proprietario del LUN o del suo partner ha, i *nodi di reporting* per il LUN.

Ciò significa che quando si sposta un volume in un nodo di un'altra coppia ha, è necessario aggiungere nodi di reporting per la coppia ha di destinazione alla mappatura LUN. È quindi possibile specificare i nuovi percorsi nella configurazione di MPIO. Una volta completato lo spostamento del volume, è possibile eliminare i nodi di reporting per la coppia ha di origine dalla mappatura.

Bilanciamento del carico

Le performance dei carichi di lavoro iniziano ad essere influenzate dalla latenza quando la quantità di lavoro su un nodo supera le risorse disponibili. È possibile gestire un nodo sovraccarico aumentando le risorse disponibili (aggiornamento di dischi o CPU) o riducendo il carico (spostamento di volumi o LUN in nodi diversi in base alle necessità).

È inoltre possibile utilizzare ONTAP *qualità del servizio (QoS) dello storage* per garantire che le performance dei carichi di lavoro critici non vengano degradate da carichi di lavoro concorrenti:

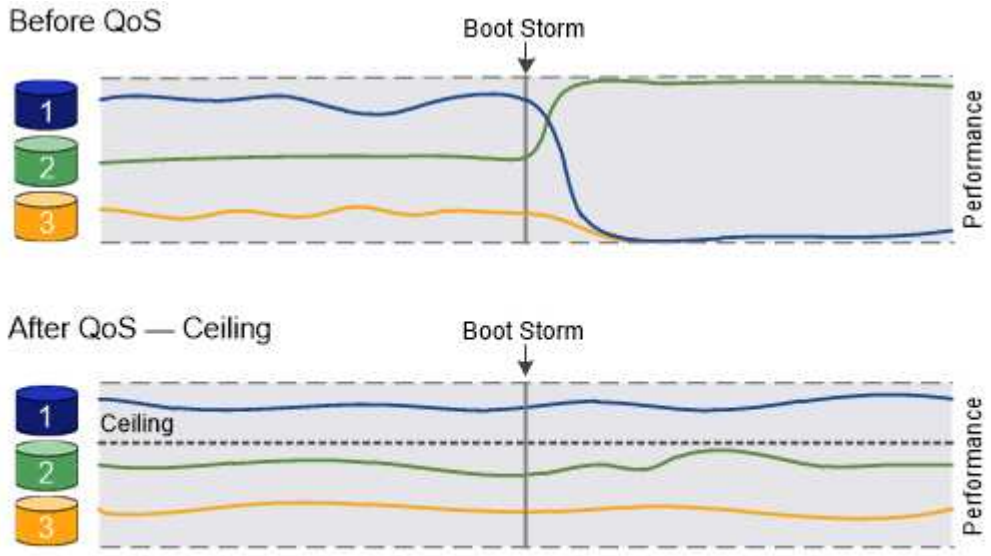
- È possibile impostare un *soffitto* di throughput QoS su un carico di lavoro concorrente per limitarne l'impatto sulle risorse di sistema (QoS Max).
- È possibile impostare un *floor* di throughput QoS per un carico di lavoro critico, garantendo che soddisfi gli obiettivi di throughput minimi indipendentemente dalla domanda mediante carichi di lavoro concorrenti (QoS min).
- È possibile impostare un tetto e un piano QoS per lo stesso carico di lavoro.

Limiti di throughput

Un limite massimo di throughput limita il throughput per un carico di lavoro a un numero massimo di IOPS o MB/s. Nella figura seguente, il limite massimo di throughput per il carico di lavoro 2 garantisce che non vengano utilizzati i carichi di lavoro 1 e 3 "bully".

Un *gruppo di policy* definisce il limite massimo di throughput per uno o più carichi di lavoro. Un carico di lavoro rappresenta le operazioni di i/o per un *oggetto storage:* volume, file o LUN o tutti i volumi, file o LUN di una SVM. È possibile specificare il limite massimo quando si crea il gruppo di criteri oppure attendere che i carichi di lavoro vengano monitorati per specificarlo.

> Il throughput per i carichi di lavoro potrebbe superare il limite massimo specificato fino al 10%, soprattutto se un carico di lavoro subisce rapidi cambiamenti nel throughput. Il limite massimo potrebbe essere superato fino al 50% per gestire i burst.



The throughput ceiling for workload 2 ensures that it does not "bully" workloads 1 and 3.

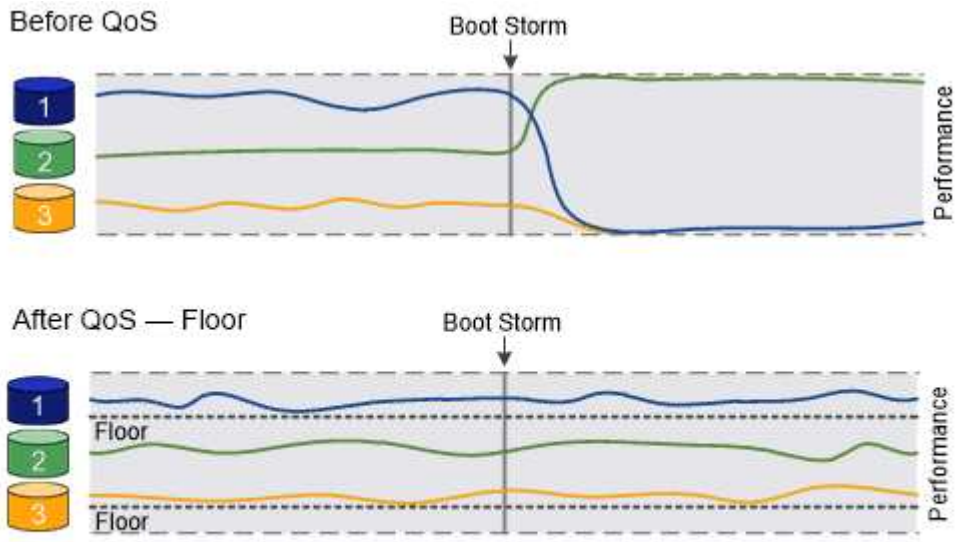
Piani di throughput

Un piano di throughput garantisce che il throughput per un carico di lavoro non scenda al di sotto di un numero minimo di IOPS. Nella figura riportata di seguito, i livelli di throughput per il carico di lavoro 1 e il carico di lavoro 3 garantiscono il raggiungimento degli obiettivi di throughput minimi, indipendentemente dalla domanda per carico di lavoro 2.

> Come suggeriscono gli esempi, un limite di throughput rallenta direttamente il throughput. Un piano di throughput rallenta indirettamente il throughput, dando priorità ai carichi di lavoro per i quali è stato impostato il piano.

Un carico di lavoro rappresenta le operazioni di i/o di un volume, LUN o, a partire da ONTAP 9.3, file. Un gruppo di criteri che definisce un piano di throughput non può essere applicato a una SVM. È possibile specificare il piano di lavoro quando si crea il gruppo di policy oppure attendere fino a quando non si monitorano i carichi di lavoro per specificarlo.

> Il throughput di un carico di lavoro potrebbe scendere al di sotto del piano specificato se la capacità delle performance (spazio di crescita) sul nodo o sull'aggregato è insufficiente o durante operazioni critiche come `volume move trigger-cutover`. Anche quando è disponibile una capacità sufficiente e non si svolgono operazioni critiche, il throughput di un workload potrebbe scendere al di sotto del piano specificato fino al 5%.



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

QoS adattiva

Normalmente, il valore del gruppo di criteri assegnato a un oggetto di storage è fisso. È necessario modificare il valore manualmente quando la dimensione dell'oggetto di storage cambia. Un aumento della quantità di spazio utilizzata su un volume, ad esempio, richiede solitamente un aumento corrispondente del limite di throughput specificato per il volume.

QoS adattiva scala automaticamente il valore del gruppo di policy in base alle dimensioni del carico di lavoro, mantenendo il rapporto tra IOPS e TB|GB in base alle dimensioni del carico di lavoro. Si tratta di un vantaggio significativo quando si gestiscono centinaia o migliaia di carichi di lavoro in un'implementazione di grandi dimensioni.

In genere, si utilizza la QoS adattiva per regolare i limiti di throughput, ma è anche possibile utilizzarla per gestire i piani di throughput (quando le dimensioni del carico di lavoro aumentano). La dimensione del carico di lavoro viene espressa come spazio allocato per l'oggetto di storage o come spazio utilizzato dall'oggetto di storage.

> Lo spazio utilizzato è disponibile per i piani di throughput in ONTAP 9.5 e versioni successive. Non è supportato per i piani di throughput in ONTAP 9.4 e versioni precedenti.

A partire da ONTAP 9.13.1, è possibile utilizzare la QoS adattiva per impostare i livelli e i limiti di throughput a livello di SVM.

- Una policy di *spazio allocato* mantiene il rapporto IOPS/TB|GB in base alle dimensioni nominali dell'oggetto di storage. Se il rapporto è di 100 IOPS/GB, un volume da 150 GB avrà un limite di throughput di 15,000 IOPS, a condizione che il volume rimanga tale. Se il volume viene ridimensionato a 300 GB, la QoS adattiva regola il limite di throughput a 30,000 IOPS.
- Una policy *used space* (predefinita) mantiene il rapporto IOPS/TB|GB in base alla quantità di dati effettivi memorizzati prima dell'efficienza dello storage. Se il rapporto è di 100 IOPS/GB, un volume da 150 GB con 100 GB di dati memorizzati avrebbe un limite massimo di throughput di 10,000 IOPS. Man mano che la quantità di spazio utilizzato cambia, la QoS adattiva regola il limite di throughput in base al rapporto.

Replica

Copie Snapshot

Tradizionalmente, le tecnologie di replica di ONTAP servivano per il disaster recovery (DR) e l'archiviazione dei dati. Con l'avvento dei servizi cloud, la replica di ONTAP è stata adattata al trasferimento dei dati tra endpoint nel data fabric NetApp. La base per tutti questi utilizzi è la tecnologia Snapshot di ONTAP.

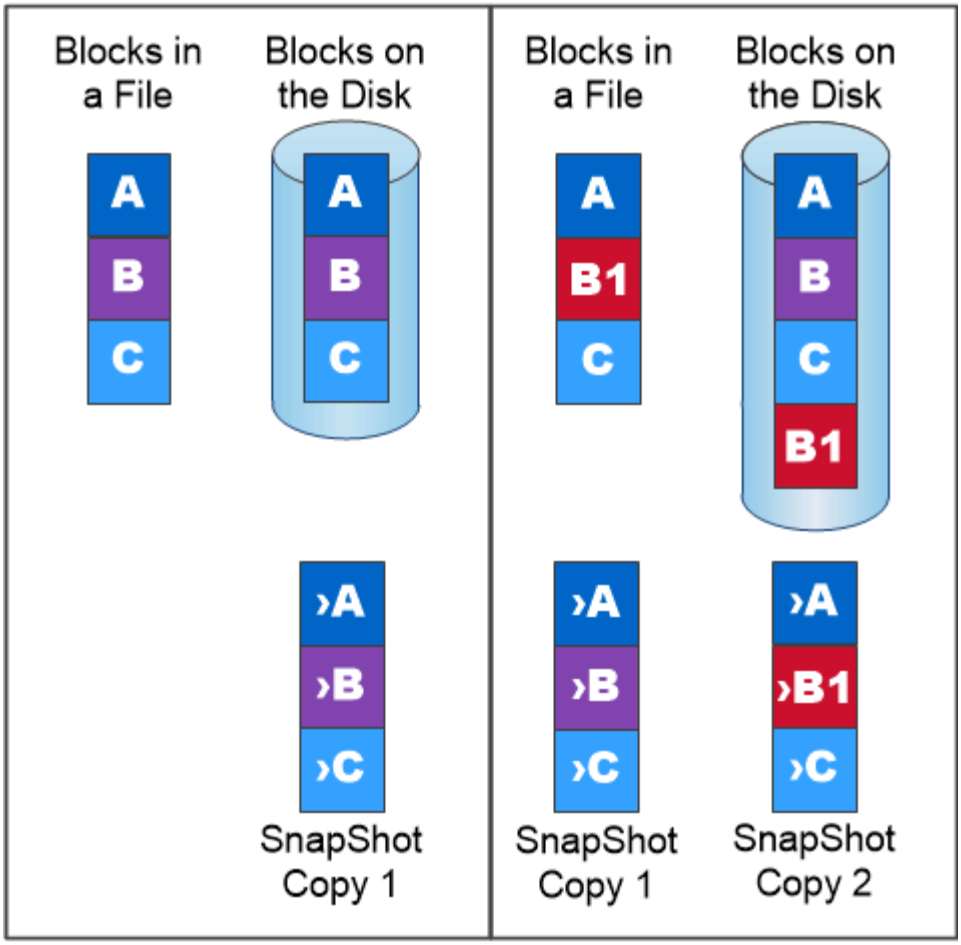
Una *copia Snapshot* è un'immagine point-in-time di sola lettura di un volume. Dopo aver creato una copia Snapshot, il file system attivo e la copia Snapshot puntano agli stessi blocchi di disco; pertanto, la copia Snapshot non utilizza spazio su disco aggiuntivo. Con il passare del tempo, l'immagine consuma uno spazio di storage minimo e subisce un overhead delle performance trascurabile in quanto registra solo le modifiche ai file dall'ultima copia Snapshot.

Le copie Snapshot devono la loro efficienza alla tecnologia di virtualizzazione dello storage di base di ONTAP, il suo *Write Anywhere file Layout (WAFL).* come un database, WAFL utilizza i metadati per puntare ai blocchi di dati effettivi sul disco. Tuttavia, a differenza di un database, WAFL non sovrascrive i blocchi esistenti. Scrive i dati aggiornati in un nuovo blocco e cambia i metadati.

Le copie Snapshot sono efficienti perché, al contrario, vengono utilizzati blocchi di dati di copia, mentre ONTAP fa riferimento ai metadati durante la creazione di una copia Snapshot. In questo modo si eliminano sia il tempo di ricerca che altri sistemi incorrono nell'individuazione dei blocchi da copiare, sia il costo della copia stessa.

È possibile utilizzare una copia Snapshot per ripristinare singoli file o LUN o per ripristinare l'intero contenuto di un volume. ONTAP confronta le informazioni del puntatore nella copia Snapshot con i dati su disco per ricostruire l'oggetto mancante o danneggiato, senza downtime o costi di performance significativi.

Una *policy Snapshot* definisce il modo in cui il sistema crea le copie Snapshot dei volumi. Il criterio specifica quando creare le copie Snapshot, quante copie conservare, come assegnarle un nome e come etichettarle per la replica. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti, chiamarle "daily" (con data e ora) ed etichettarle "daily" per la replica.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

Disaster recovery e trasferimento dei dati SnapMirror

SnapMirror è una tecnologia di disaster recovery progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. Come suggerisce il nome, SnapMirror crea una replica, o *mirror*, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di disastro nel sito primario.

I dati vengono mirrorati a livello di volume. La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene chiamata *relazione di protezione dei dati.* i cluster in cui risiedono i volumi e le SVM che servono i dati dei volumi devono essere *peering.* Una relazione peer consente lo scambio di cluster e SVM dati in modo sicuro.

È inoltre possibile creare una relazione di protezione dei dati tra le SVM. In questo tipo di relazione, viene replicata tutta o parte della configurazione di SVM, dalle esportazioni NFS e dalle condivisioni SMB a RBAC, nonché i dati nei volumi di proprietà di SVM.

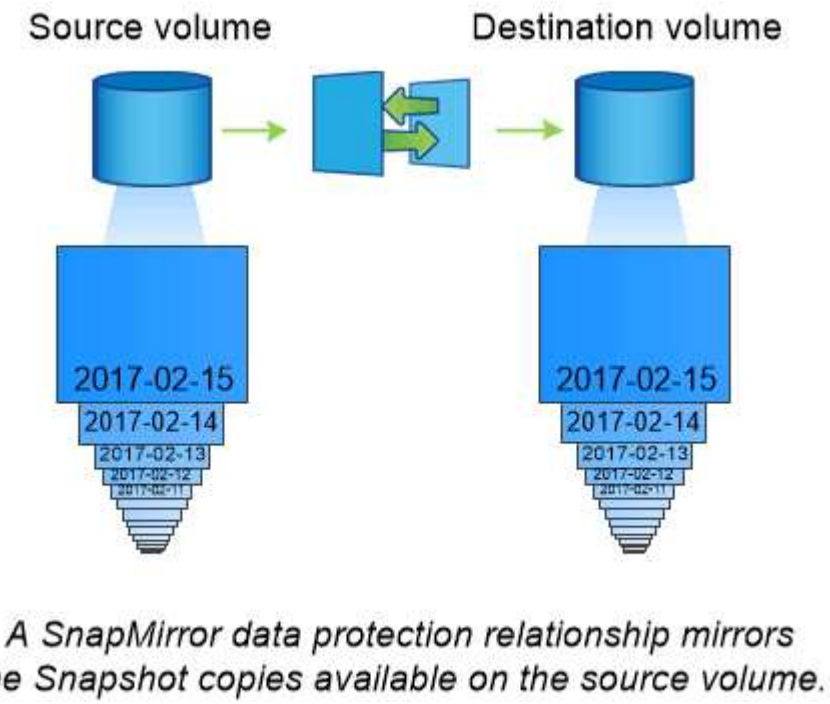
A partire da ONTAP 9.10.1, è possibile creare relazioni di protezione dei dati tra i bucket S3 utilizzando S3 SnapMirror. I bucket di destinazione possono essere su sistemi ONTAP locali o remoti o su sistemi non ONTAP come StorageGRID e AWS.

La prima volta che si richiama SnapMirror, esegue un *trasferimento baseline* dal volume di origine al volume di destinazione. Il trasferimento della linea di base in genere prevede i seguenti passaggi:

- Creare una copia Snapshot del volume di origine.
- Trasferire la copia Snapshot e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.
- Trasferire le copie Snapshot rimanenti, meno recenti, sul volume di origine al volume di destinazione per l'utilizzo in caso di danneggiamento del mirror "Active".

Una volta completato il trasferimento di riferimento, SnapMirror trasferisce solo le nuove copie Snapshot nel mirror. Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. La conservazione rispecchia la policy Snapshot sull'origine. È possibile attivare il volume di destinazione con interruzioni minime in caso di disastro nel sito primario e riattivare il volume di origine quando il servizio viene ripristinato.

Poiché SnapMirror trasferisce solo le copie Snapshot dopo la creazione della linea di base, la replica è rapida e senza interruzioni. Come implica il caso di utilizzo del failover, i controller sul sistema secondario devono essere equivalenti o quasi equivalenti ai controller sul sistema primario per fornire i dati in modo efficiente dallo storage mirrorato.



utilizzo di SnapMirror per il trasferimento dei dati

È inoltre possibile utilizzare SnapMirror per replicare i dati tra endpoint nel data fabric NetApp. Quando si crea il criterio SnapMirror, è possibile scegliere tra replica singola o ricorrente.

Backup di SnapMirror Cloud nello storage a oggetti

SnapMirror Cloud è una tecnologia di backup e recovery progettata per gli utenti ONTAP che desiderano trasferire i propri flussi di lavoro di data Protection nel cloud. Le organizzazioni che si allontanano dalle architetture di backup su nastro legacy possono utilizzare lo storage a oggetti come repository alternativo per la conservazione e l'archiviazione dei dati a lungo termine. SnapMirror Cloud offre la replica dello storage

ONTAP-to-object come parte di una strategia di backup incrementale per sempre.

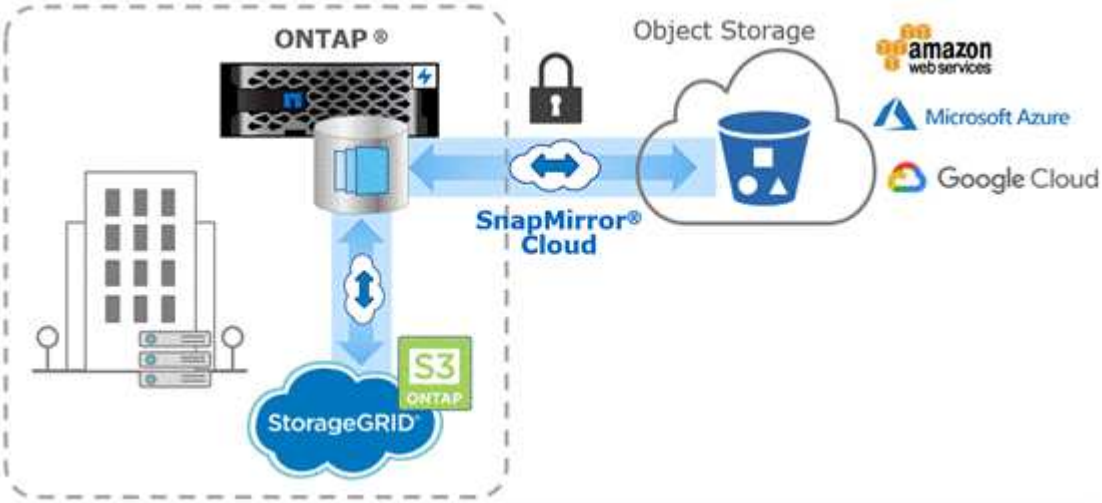
SnapMirror Cloud è stato introdotto in ONTAP 9.8 come estensione della famiglia di tecnologie di replica SnapMirror. Mentre SnapMirror viene spesso utilizzato per i backup da ONTAP a ONTAP, SnapMirror Cloud utilizza lo stesso motore di replica per trasferire le copie Snapshot per ONTAP ai backup dello storage a oggetti compatibili con S3.

Destinato ai casi di utilizzo del backup, SnapMirror Cloud supporta sia la conservazione a lungo termine che i flussi di lavoro di archiviazione. Come per SnapMirror, il backup iniziale di SnapMirror Cloud esegue un trasferimento di riferimento di un volume. Per i backup successivi, SnapMirror Cloud genera una copia snapshot del volume di origine e trasferisce la copia snapshot con solo i blocchi di dati modificati a una destinazione di storage a oggetti.

Le relazioni cloud di SnapMirror possono essere configurate tra sistemi ONTAP e destinazioni di storage a oggetti on-premise e cloud pubblico selezionate, tra cui Amazon S3, Google Cloud Storage e Microsoft Azure Blob Storage. Ulteriori destinazioni di storage a oggetti on-premise includono StorageGRID e ONTAP S3.

La replica cloud di SnapMirror è una funzionalità ONTAP concessa in licenza e richiede un'applicazione approvata per orchestrare i flussi di lavoro di protezione dei dati. Sono disponibili diverse opzioni di orchestrazione per la gestione dei backup di SnapMirror Cloud:

- Diversi partner di backup di terze parti che offrono supporto per la replica di SnapMirror Cloud. I vendor partecipanti sono disponibili su "Blog di NetApp".
- Backup e ripristino BlueXP per una soluzione nativa NetApp per ambienti ONTAP
- API per lo sviluppo di software personalizzato per i flussi di lavoro di data Protection o l'utilizzo di strumenti di automazione



Archiviazione SnapVault

La licenza SnapMirror viene utilizzata per supportare le relazioni SnapVault per il backup e le relazioni SnapMirror per il disaster recovery. A partire da ONTAP 9,3, le licenze SnapVault sono obsolete e le licenze SnapMirror possono essere utilizzate per configurare relazioni di vault, mirror e mirror-and-vault. La replica di SnapMirror viene utilizzata per la replica da ONTAP a ONTAP delle copie Snapshot, supportando i casi di utilizzo di backup e disaster recovery.

SnapVault è una tecnologia di archiviazione, progettata per la replica delle copie Snapshot disk-to-disk per la

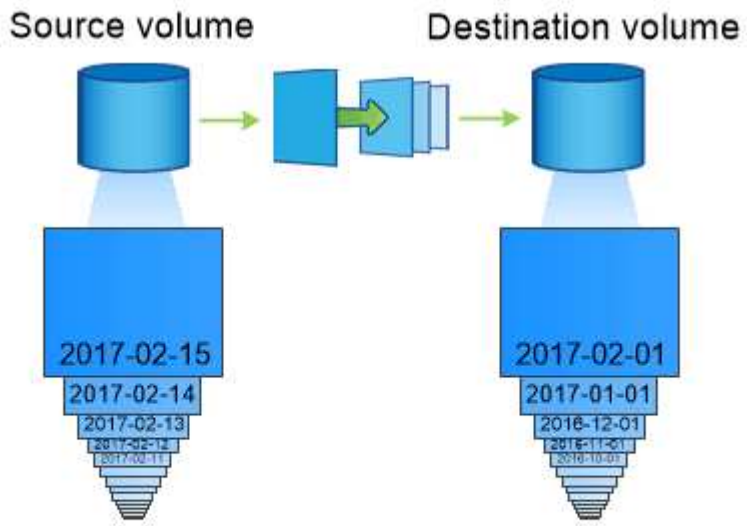
conformità agli standard e altri scopi correlati alla governance. A differenza di una relazione SnapMirror, in cui la destinazione contiene di solito solo le copie Snapshot attualmente nel volume di origine, una destinazione SnapVault conserva in genere le copie Snapshot point-in-time create in un periodo molto più lungo.

È possibile conservare copie Snapshot mensili dei dati per un periodo di 20 anni, ad esempio per rispettare le normative contabili governative per la propria azienda. Poiché non è necessario fornire dati dallo storage del vault, è possibile utilizzare dischi più lenti e meno costosi sul sistema di destinazione.

Come con SnapMirror, SnapVault esegue un trasferimento di riferimento la prima volta che lo si richiama. Esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e i blocchi di dati a cui fa riferimento al volume di destinazione. A differenza di SnapMirror, SnapVault non include copie Snapshot precedenti nella linea di base.

Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. Le regole definite nella policy per la relazione identificano quali nuove copie Snapshot includere negli aggiornamenti e quante copie conservare. Le etichette definite nella policy (“monhly,” ad esempio) devono corrispondere a una o più etichette definite nella policy Snapshot sull’origine. In caso contrario, la replica non riesce.

> SnapMirror e SnapVault condividono la stessa infrastruttura di comando. Specificare il metodo da utilizzare per la creazione di un criterio. Entrambi i metodi richiedono cluster peered e SVM peered.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Backup nel cloud e supporto per backup tradizionali

Oltre alle relazioni di protezione dei dati SnapMirror e SnapVault, che erano disk-to-disk solo per ONTAP 9,7 e versioni precedenti, oggi esistono diverse soluzioni di backup che offrono un’alternativa meno costosa per la conservazione dei dati a lungo termine.

Numerose applicazioni di protezione dei dati di terze parti offrono il backup tradizionale per i dati gestiti da ONTAP. Veeam, Veritas e CommVault, tra gli altri, offrono backup integrato per i sistemi ONTAP.

A partire da ONTAP 9.8, SnapMirror Cloud offre la replica asincrona delle copie Snapshot dalle istanze di

ONTAP agli endpoint dello storage a oggetti. La replica di SnapMirror Cloud richiede un'applicazione con licenza per l'orchestrazione e la gestione dei flussi di lavoro per la protezione dei dati. Le relazioni cloud di SnapMirror sono supportate dai sistemi ONTAP per selezionare obiettivi di storage a oggetti per il cloud pubblico e on-premise, tra cui AWS S3, la piattaforma di storage cloud di Google o lo storage Blob di Microsoft Azure, che offrono una maggiore efficienza con il software di backup del vendor. Contatta il tuo rappresentante NetApp per un elenco delle applicazioni certificate supportate e dei vendor di storage a oggetti.

Se sei interessato alla protezione dei dati nativa del cloud, BlueXP può essere utilizzato per configurare le relazioni di SnapMirror o SnapVault tra volumi on-premise e istanze di Cloud Volumes ONTAP nel cloud pubblico.

BlueXP fornisce inoltre backup delle istanze di Cloud Volumes ONTAP utilizzando un modello SaaS (Software as a Service). Gli utenti possono eseguire il backup delle istanze di Cloud Volumes ONTAP su storage a oggetti cloud pubblico compatibile con S3 e S3 utilizzando il backup cloud disponibile su NetApp Cloud Central.

"Risorse per la documentazione di Cloud Volumes ONTAP e BlueXP"

"NetApp Cloud Central"

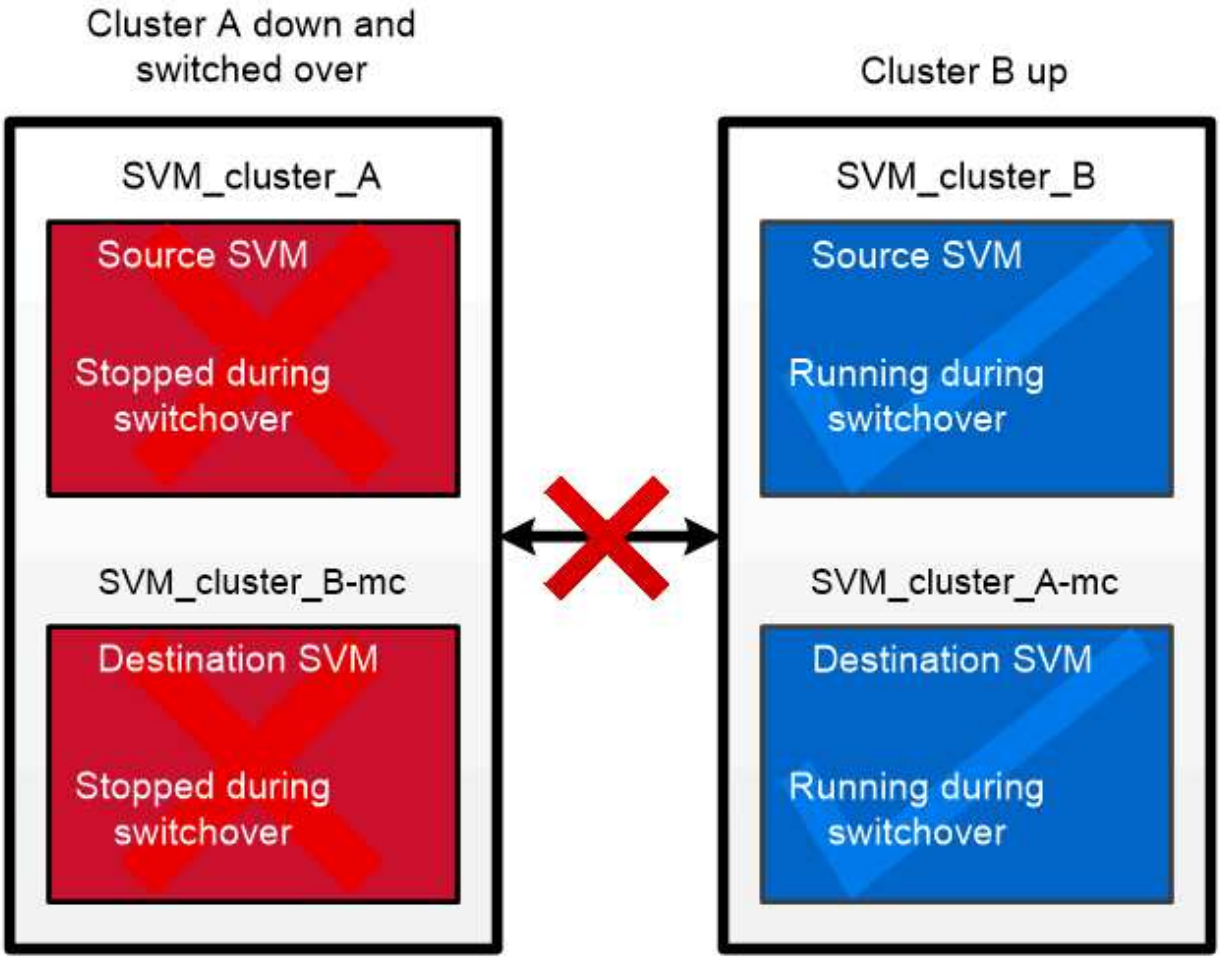
Disponibilità continua di MetroCluster

Le configurazioni MetroCluster proteggono i dati implementando due cluster fisicamente separati con mirroring. Ciascun cluster replica in modo sincrono i dati e la configurazione SVM dell'altro. In caso di disastro in un sito, un amministratore può attivare la SVM mirrorata e iniziare a fornire i dati dal sito sopravvissuto.

- Le configurazioni *Fabric-attached MetroCluster* supportano cluster a livello metropolitano.
- Le configurazioni *stretch MetroCluster* supportano cluster a livello di campus.

In entrambi i casi, i cluster devono essere peering.

MetroCluster utilizza una funzionalità di ONTAP denominata *SyncMirror* per eseguire il mirroring sincrono dei dati aggregati per ciascun cluster nelle copie, o *plex*, nello storage dell'altro cluster. Se si verifica uno switchover, il plex remoto sul cluster in uso viene online e la SVM secondaria inizia a fornire i dati.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

utilizzo di SyncMirror in implementazioni non MetroCluster è possibile utilizzare SyncMirror in un'implementazione non MetroCluster per proteggere dalla perdita di dati in caso di guasti di più dischi rispetto a quelli protetti dal tipo RAID o in caso di perdita di connettività ai dischi del gruppo RAID. La funzione è disponibile solo per le coppie ha.

I dati aggregati vengono mirrorati in plessi memorizzati su diversi shelf di dischi. Se uno degli shelf non è disponibile, il plesso non interessato continua a fornire dati mentre si corregge la causa del guasto.

Tenere presente che un aggregato mirrorato utilizzando SyncMirror richiede il doppio dello storage rispetto a un aggregato senza mirror. Ogni plex richiede un numero di dischi pari a quello del plex che esegue il mirroring. Per eseguire il mirroring di un aggregato da 1,440 GB, ad esempio 1,440 GB per ciascun plex, sono necessari 2,880 GB di spazio su disco.

Con SyncMirror, si consiglia di mantenere almeno il 20% di spazio libero per gli aggregati con mirroring, per ottenere performance e disponibilità dello storage ottimali. Sebbene il suggerimento sia del 10% per gli aggregati non speculari, il 10% di spazio aggiuntivo può essere utilizzato dal filesystem per assorbire le modifiche incrementali. I cambiamenti incrementali aumentano l'utilizzo dello spazio per gli aggregati con mirroring grazie all'architettura copy-on-write basata su Snapshot di ONTAP. Il mancato rispetto di queste Best practice può avere un impatto negativo sulle performance di risincronizzazione del SyncMirror, che influisce indirettamente sui flussi di lavoro operativi come NDU per le implementazioni di cloud non condivisi e lo switchback per le implementazioni di MetroCluster.

SyncMirror è disponibile anche per le implementazioni della virtualizzazione FlexArray.

Efficienza dello storage

Panoramica dell'efficienza dello storage di ONTAP

L'efficienza dello storage misura la efficacia con cui un sistema storage utilizza lo spazio disponibile ottimizzando le risorse di storage, riducendo lo spazio sprecato e riducendo l'impatto fisico dei dati scritti. Una maggiore efficienza dello storage consente di memorizzare la quantità massima di dati nel minor spazio possibile al minor costo possibile. Ad esempio, utilizzando tecnologie per l'efficienza dello storage che rilevano ed eliminano blocchi di dati duplicati e blocchi di dati pieni di zero, si riduce la quantità complessiva di storage fisico necessario e si riduce il costo complessivo.

ONTAP offre una vasta gamma di tecnologie per l'efficienza dello storage che riducono la quantità di hardware fisico o di cloud storage consumato dai dati e che forniscono anche miglioramenti significativi alle performance di sistema, tra cui letture dei dati più rapide, copie dei set di dati più rapide e un provisioning più rapido delle macchine virtuali.

Le tecnologie per l'efficienza dello storage di ONTAP includono:

- **Thin provisioning**

  Thin provisioning Consente di allocare lo storage in un volume o LUN in base alle necessità, anziché riservarlo in anticipo. Questo riduce la quantità di storage fisico necessario consentendo di allocare in eccesso i volumi o le LUN in base a un potenziale utilizzo, senza riservare spazio non attualmente in uso.

- **Deduplica**

Deduplica riduce la quantità di storage fisico necessaria per un volume in tre modi distinti.

- **Deduplicazione a blocchi zero**

  La deduplica zero block rileva ed elimina i blocchi di dati riempiti con tutti gli zero e aggiorna solo i metadati. viene quindi salvato il 100% dello spazio tipicamente utilizzato dai blocchi zero. La deduplica zero block è abilitata per impostazione predefinita su tutti i volumi deduplicati.

- **Deduplicazione inline**

  La deduplica inline rileva i blocchi di dati duplicati e li sostituisce con dei riferimenti a un blocco condiviso univoco prima che i dati vengano scritti sul disco. La deduplica inline accelera il provisioning delle macchine virtuali del 20-30%. A seconda della versione di ONTAP in uso e della piattaforma in uso, la deduplica inline è disponibile a livello di volume o aggregato. È abilitato per impostazione predefinita nei sistemi AFF e ASA. È necessario abilitare manualmente la deduplica inline su sistemi FAS.

- **Deduplicazione in background**

  La deduplica in background rileva anche i blocchi di dati duplicati e li sostituisce con dei riferimenti a un blocco condiviso unico, ma migliora ulteriormente l'efficienza dello storage dopo che i dati sono stati scritti sul disco. È possibile impostare la deduplica in background in modo che venga eseguita quando vengono soddisfatti determinati criteri sul sistema di storage. Ad esempio, è possibile abilitare la deduplica in background quando il volume raggiunge un utilizzo del 10%. È inoltre possibile attivare manualmente la deduplica in background o impostarla per l'esecuzione su una pianificazione specifica. È abilitato per impostazione predefinita nei sistemi AFF e ASA. È necessario abilitare manualmente la deduplica in background sui sistemi FAS.

La deduplica è supportata sia all'interno dei volumi che tra i volumi di un aggregato. Le letture dei dati deduplicati non comportano in genere alcun costo per le prestazioni.

- **Compressione**

  Compressione riduce la quantità di storage fisico necessaria per un volume combinando blocchi di dati in gruppi di compressione, ciascuno dei quali viene memorizzato come un singolo blocco. Quando viene ricevuta una richiesta di lettura o sovrascrittura, viene letto solo un piccolo gruppo di blocchi, non l'intero file. Questo processo ottimizza le prestazioni di lettura e sovrascrittura e consente una maggiore scalabilità nelle dimensioni dei file compressi.

  La compressione può essere eseguita inline o post-process. La compressione inline genera risparmi di spazio immediati grazie alla compressione dei dati in memoria prima che vengano scritti sul disco. La compressione post-elaborazione scrive prima i blocchi su disco come non compressi, quindi, in un momento pianificato, comprime i dati. È necessario attivare manualmente la compressione.

- **Compattazione**

  La tecnologia di compaction riduce la quantità di storage fisico richiesta per un volume prelevando porzioni di dati memorizzate in blocchi da 4 KB, ma di dimensioni inferiori a 4 KB e combinandole in un singolo blocco. La tecnologia di compaction avviene mentre i dati sono ancora in memoria, in modo da non consumare spazio non necessario sui dischi. È abilitato per impostazione predefinita nei sistemi AFF e ASA. Devi attivare manualmente la compaction sui sistemi FAS.

- **Volumi, file e LUN di FlexClone**

  Tecnologia FlexClone Sfrutta i metadati Snapshot per creare copie scrivibili point-in-time di un volume, file o LUN. Le copie condividono i blocchi di dati con i genitori, senza consumare storage tranne ciò che è

necessario per i metadati fino a quando le modifiche non vengono scritte in una copia o nella relativa copia padre. Quando viene scritta una modifica, viene memorizzato solo il delta.

Se le copie tradizionali dei set di dati richiedono pochi minuti o anche ore per la creazione, la tecnologia FlexClone consente di copiare quasi istantaneamente anche i set di dati più estesi.

- **Efficienza di stoccaggio sensibile alla temperatura**

  ONTAP offre "efficienza dello storage sensibile alla temperatura" i vantaggi, valutando la frequenza di accesso ai dati del volume ed eseguendo la mappatura di tale frequenza al grado di compressione applicato a tali dati. Per i dati cold a cui si accede raramente, i blocchi di dati più grandi vengono compressi, mentre per i dati hot, a cui si accede frequentemente e che vengono sovrascritti più spesso, i blocchi di dati più piccoli vengono compressi, rendendo il processo più efficiente.

  L'efficienza dello storage sensibile alla temperatura (TSSE) viene introdotta in ONTAP 9.8 e attivata automaticamente sui volumi AFF appena creati con thin provisioning.

Puoi realizzare il vantaggio di queste tecnologie nelle tue operazioni quotidiane con il minimo sforzo. Ad esempio, si supponga di dover fornire a 5.000 utenti lo spazio di archiviazione per le home directory e si stimi che lo spazio massimo necessario a qualsiasi utente sia di 1 GB. È possibile riservare in anticipo un aggregato da 5 TB per soddisfare la potenziale esigenza di storage totale. Tuttavia, è anche noto che i requisiti di capacità delle home directory variano notevolmente a seconda dell'organizzazione. Invece di riservare 5 TB di spazio totale all'organizzazione, è possibile creare un aggregato da 2 TB. Quindi è possibile utilizzare il thin provisioning per assegnare nominalmente 1 GB di storage a ciascun utente, ma allocare lo storage solo in base alle necessità. È possibile monitorare attivamente l'aggregato nel tempo e aumentare le dimensioni fisiche effettive in base alle necessità.

Un altro esempio potrebbe essere l'utilizzo di una VDI (Virtual Desktop Infrastructure) con una grande quantità di dati duplicati tra i virtual desktop. La deduplica riduce l'utilizzo dello storage eliminando automaticamente i blocchi di informazioni duplicati nell'infrastruttura di desktop virtuale, sostituendoli con un puntatore al blocco originale. Altre tecnologie per l'efficienza dello storage di ONTAP, come la compressione, possono essere eseguite in background senza alcun intervento da parte dell'utente.

La tecnologia di partizione dei dischi di ONTAP offre anche una maggiore efficienza dello storage. La tecnologia RAID DP protegge da guasti a due unità disco senza sacrificare le prestazioni o aggiungere overhead del mirroring del disco. La partizione avanzata dei dischi a stato solido con ONTAP 9 aumenta la capacità utilizzabile di quasi il 20%.

NetApp offre le stesse funzionalità di efficienza dello storage disponibili con ONTAP on-premise nel cloud. Durante la migrazione dei dati da ONTAP on-premise al cloud, l'efficienza dello storage esistente viene preservata. Ad esempio, supponiamo di disporre di un database SQL contenente dati business-critical da spostare da un sistema on-premise nel cloud. Puoi utilizzare la replica dei dati in BlueXP per migrare i tuoi dati e, come parte del processo di migrazione, puoi abilitare la tua policy on-premise più recente per le copie Snapshot nel cloud.

Thin provisioning

ONTAP offre un'ampia gamma di tecnologie per l'efficienza dello storage oltre alle copie Snapshot. Le tecnologie chiave includono thin provisioning, deduplica, compressione e volumi FlexClone, file, E LUN. Come le copie Snapshot, tutte sono basate sul layout di file Write Anywhere (WAFL) di ONTAP.

Un volume o LUN *con thin provisioning* è un volume per il quale lo storage non è riservato in anticipo. Invece, lo storage viene allocato in modo dinamico, in base alle esigenze. Lo spazio libero viene nuovamente rilasciato

nel sistema di storage quando i dati nel volume o nel LUN vengono cancellati.

Supponiamo che la tua organizzazione debba fornire a 5,000 utenti lo storage per le home directory. Si stima che le home directory più grandi consumeranno 1 GB di spazio.

In questa situazione, è possibile acquistare 5 TB di storage fisico. Per ogni volume che memorizza una home directory, si dovrebbe riservare spazio sufficiente per soddisfare le esigenze dei consumatori più grandi.

Tuttavia, come aspetto pratico, sai anche che i requisiti di capacità della home directory variano notevolmente in tutta la community. Per ogni grande utente dello storage, sono dieci i clienti che consumano poco o niente spazio.

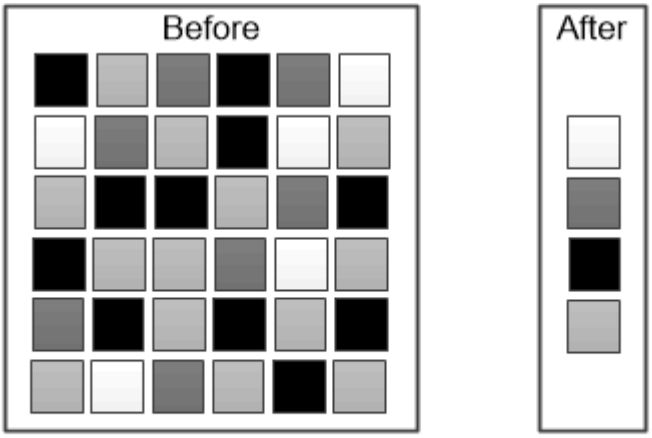
Il thin provisioning ti consente di soddisfare le esigenze dei grandi consumatori di storage senza dover acquistare storage che potresti non utilizzare mai. Poiché lo spazio di storage non viene allocato fino a quando non viene consumato, è possibile “assegnare in eccesso” un aggregato di 2 TB assegnando nominalmente una dimensione di 1 GB a ciascuno dei 5,000 volumi contenuti nell’aggregato.

Se hai ragione, il rapporto tra utenti leggeri e utenti pesanti è di 10:1 e se assumi un ruolo attivo nel monitoraggio dello spazio libero sull’aggregato, puoi essere sicuro che le scritture dei volumi non falliscono a causa della mancanza di spazio.

Deduplica

Deduplica riduce la quantità di storage fisico richiesta per un volume (o per tutti i volumi in un aggregato AFF) eliminando i blocchi duplicati e sostituendoli con riferimenti a un singolo blocco condiviso. Le letture dei dati deduplicati non comportano in genere alcun costo per le prestazioni. Le scritture comportano un costo trascurabile, tranne che per i nodi sovraccarichi.

Quando i dati vengono scritti durante il normale utilizzo, WAFL utilizza un processo batch per creare un catalogo di *firme a blocchi.* dopo l’avvio della deduplica, ONTAP confronta le firme nel catalogo per identificare i blocchi duplicati. Se esiste una corrispondenza, viene eseguito un confronto byte per byte per verificare che i blocchi candidati non siano stati modificati dalla creazione del catalogo. Solo se tutti i byte corrispondono, il blocco duplicato viene scartato e il relativo spazio su disco viene recuperato.



Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.

Compressione

Compressione riduce la quantità di storage fisico richiesta per un volume combinando i blocchi di dati in *gruppi di compressione*, ciascuno dei quali viene memorizzato come un singolo blocco. Le letture dei dati compressi sono più veloci rispetto ai metodi di compressione tradizionali, poiché ONTAP decomprime solo i gruppi di compressione che contengono i dati richiesti, non un intero file o LUN.

È possibile eseguire la compressione inline o post-processo, separatamente o in combinazione:

- *Compressione inline* comprime i dati in memoria prima che vengano scritti su disco, riducendo significativamente la quantità di i/o di scrittura su un volume, ma potenzialmente degradando le prestazioni di scrittura. Le operazioni che richiedono prestazioni elevate vengono posticipate fino alla successiva operazione di compressione post-processo, se presente.
- *Compressione post-processo* comprime i dati dopo la scrittura su disco, secondo la stessa pianificazione della deduplica.

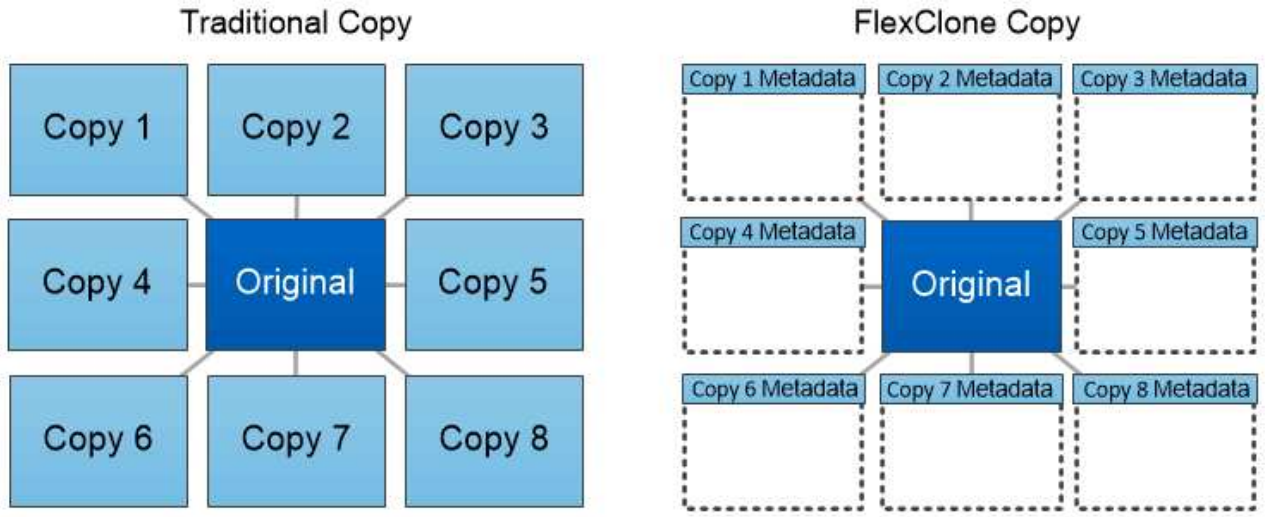
Inline data compaction i file di piccole dimensioni o i/o con zeri vengono memorizzati in un blocco di 4 KB, indipendentemente dal fatto che richiedano o meno 4 KB di storage fisico. *Inline data compaction* combina blocchi di dati che normalmente consumerebbero più blocchi da 4 KB in un singolo blocco da 4 KB su disco. La compattazione avviene quando i dati sono ancora in memoria, quindi è più adatta ai controller più veloci.

Volumi, file e LUN FlexClone

La tecnologia *FlexClone* fa riferimento ai metadati Snapshot per creare copie scrivibili point-in-time di un volume. Le copie condividono i blocchi di dati con i genitori, senza consumare storage, ad eccezione di quanto richiesto per i metadati fino a quando le modifiche non vengono scritte nella copia. I file FlexClone e le LUN FlexClone utilizzano una tecnologia identica, tranne per il fatto che non è necessaria una copia Snapshot di backup.

Il software FlexClone consente di copiare quasi istantaneamente anche i set di dati più grandi, anche se le copie tradizionali richiedono pochi minuti o persino ore. Ciò lo rende ideale per le situazioni in cui sono necessarie più copie di set di dati identici (ad esempio, un'implementazione di desktop virtuale) o copie temporanee di un set di dati (test di un'applicazione rispetto a un set di dati di produzione).

È possibile clonare un volume FlexClone esistente, clonare un volume contenente cloni LUN o clonare dati di mirroring e vault. È possibile *separare* un volume FlexClone dal relativo volume padre, nel qual caso la copia viene allocata al proprio storage.



FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

Misurazioni della capacità in System Manager

La capacità del sistema può essere misurata come spazio fisico o spazio logico. A partire da ONTAP 9.7, System Manager fornisce misurazioni della capacità fisica e logica.

Le differenze tra le due misurazioni sono spiegate nelle seguenti descrizioni:

- **Capacità fisica**: Lo spazio fisico si riferisce ai blocchi fisici di storage utilizzati nel volume o nel Tier locale. Il valore della capacità fisica utilizzata è in genere inferiore al valore della capacità logica utilizzata a causa della riduzione dei dati dalle funzionalità di efficienza dello storage (come deduplica e compressione).
- **Capacità logica**: Lo spazio logico si riferisce allo spazio utilizzabile (i blocchi logici) in un volume o in un Tier locale. Lo spazio logico si riferisce al modo in cui lo spazio teorico può essere utilizzato, senza tenere conto dei risultati della deduplica o della compressione. Il valore dello spazio logico utilizzato deriva dalla quantità di spazio fisico utilizzato e dai risparmi derivanti dalle funzionalità di efficienza dello storage (come deduplica e compressione) configurate. Questa misurazione appare spesso più grande della capacità fisica utilizzata perché include copie Snapshot, cloni e altri componenti e non riflette la compressione dei dati e altre riduzioni dello spazio fisico. Pertanto, la capacità logica totale potrebbe essere superiore allo spazio fornito.

> In System Manager, le rappresentazioni della capacità non tengono conto delle capacità del Tier storage root (aggregato).

Misurazioni della capacità utilizzata

Le misurazioni della capacità utilizzata vengono visualizzate in modo diverso a seconda della versione di System Manager in uso, come illustrato nella seguente tabella:

Versione di System Manager	Termine utilizzato per la capacità	Tipo di capacità a cui si fa riferimento

9.9.1 e versioni successive	Logica utilizzata	Spazio logico utilizzato se sono state attivate le impostazioni di efficienza dello storage)
9.7 e 9.8	Utilizzato	Spazio logico utilizzato (se sono state attivate le impostazioni di efficienza dello storage)
9.5 e 9.6 (visualizzazione classica)	Utilizzato	Spazio fisico utilizzato

Termini di misurazione della capacità

Quando si descrive la capacità, vengono utilizzati i seguenti termini:

- **Capacità allocata**: Quantità di spazio allocato per i volumi in una VM di storage.
- **Available**: La quantità di spazio fisico disponibile per memorizzare i dati o per eseguire il provisioning dei volumi in una VM di storage o su un Tier locale.
- **Capacità tra volumi**: La somma dello storage utilizzato e dello storage disponibile di tutti i volumi su una VM di storage.
- **Dati del client**: Quantità di spazio utilizzata dai dati del client (fisici o logici).
  - A partire da ONTAP 9.13.1, la capacità utilizzata dai dati del client viene definita **uso logico** e la capacità utilizzata dalle copie Snapshot viene visualizzata separatamente.
  - In ONTAP 9.12.1 e versioni precedenti, la capacità utilizzata dai dati del client aggiunta alla capacità utilizzata dalle copie Snapshot viene definita **logica utilizzata**.
- **Impegnato**: Quantità di capacità impegnata per un Tier locale.
- **Riduzione dei dati**:
  - A partire da ONTAP 9.13.1, i rapporti di riduzione dei dati vengono visualizzati come segue:
    - Il valore di riduzione dei dati visualizzato sul pannello **Capacity** è il rapporto tra lo spazio logico utilizzato e lo spazio fisico utilizzato senza considerare le riduzioni significative ottenute utilizzando le funzionalità di efficienza dello storage, come le copie Snapshot.
    - Quando si visualizza il pannello dei dettagli, vengono visualizzati sia il rapporto visualizzato nel pannello di panoramica che il rapporto complessivo di tutto lo spazio logico utilizzato rispetto allo spazio fisico utilizzato. Definito **con copie Snapshot**, questo valore include i benefici derivanti dall'utilizzo di copie Snapshot e altre funzionalità di efficienza dello storage.
  - In ONTAP 9.12.1 e versioni precedenti, i rapporti di riduzione dei dati vengono visualizzati come segue:
    - Il valore di riduzione dei dati visualizzato sul pannello **Capacity** è il rapporto complessivo di tutto lo spazio logico utilizzato rispetto allo spazio fisico utilizzato e include i benefici derivanti dall'utilizzo di copie Snapshot e altre funzionalità di efficienza dello storage.
    - Quando si visualizza il pannello dei dettagli, vengono visualizzati il rapporto **complessivo** visualizzato nel pannello di panoramica e il rapporto dello spazio logico utilizzato solo dai dati del client rispetto allo spazio fisico utilizzato solo dai dati del client, denominato **senza copie Snapshot e cloni**.
- **Logica utilizzata**:
  - A partire da ONTAP 9.13.1, la capacità utilizzata dai dati del client viene definita **uso logico** e la

capacità utilizzata dalle copie Snapshot viene visualizzata separatamente.

  - In ONTAP 9.12.1 e versioni precedenti, la capacità utilizzata dai dati client aggiunti alla capacità utilizzata dalle copie Snapshot viene definita **logica utilizzata**.

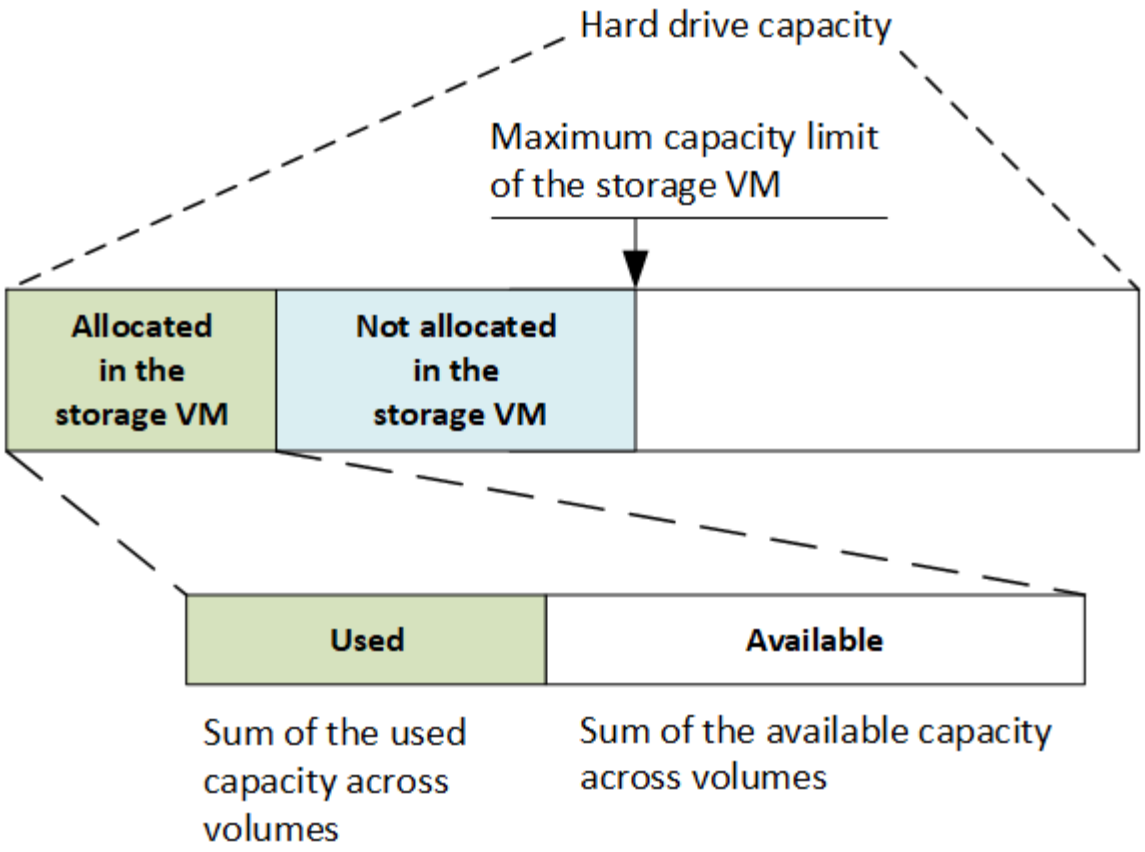
- **Logical used %**: Percentuale della capacità logica utilizzata corrente rispetto alle dimensioni fornite, escluse le riserve Snapshot. Questo valore può essere superiore al 100%, perché include risparmi di efficienza nel volume.
- **Capacità massima**: Quantità massima di spazio allocato per i volumi su una VM di storage.
- **Fisico utilizzato**: La quantità di capacità utilizzata nei blocchi fisici di un volume o di un Tier locale.
- **Physical used %**: Percentuale di capacità utilizzata nei blocchi fisici di un volume rispetto alle dimensioni del provisioning.
- **Capacità di provisioning**: Un file system (volume) allocato da un sistema Cloud Volumes ONTAP ed pronto per l'archiviazione dei dati dell'utente o dell'applicazione.
- **Reserved**: Quantità di spazio riservato ai volumi già sottoposti a provisioning in un Tier locale.
- **Used**: Quantità di spazio che contiene dati.
- **Utilizzato e riservato**: La somma dello spazio fisico utilizzato e riservato.

Capacità di una VM storage

La capacità massima di una VM di storage è determinata dallo spazio allocato totale per i volumi più lo spazio non allocato rimanente.

- Lo spazio allocato per i volumi è la somma della capacità utilizzata e della capacità disponibile di volumi FlexVol, FlexGroup e FlexCache.
- La capacità dei volumi viene inclusa nelle somme, anche quando sono limitate, offline o nella coda di ripristino dopo l'eliminazione.
- Se i volumi sono configurati con la crescita automatica, il valore massimo di dimensionamento automatico del volume viene utilizzato nelle somme. Senza la crescita automatica, la capacità effettiva del volume viene utilizzata nelle somme.

Il grafico seguente spiega come la misurazione della capacità tra i volumi si riferisce al limite massimo di capacità.



A partire da ONTAP 9.13.1, gli amministratori del cluster possono farlo "Abilitare un limite massimo di capacità per una VM di storage". Tuttavia, non è possibile impostare limiti di storage per una VM di storage che contiene volumi per la protezione dei dati, in una relazione SnapMirror o in una configurazione MetroCluster. Inoltre, le quote non possono essere configurate in modo da superare la capacità massima di una VM di storage.

Una volta impostato il limite massimo di capacità, non è possibile modificarlo in una dimensione inferiore alla capacità attualmente allocata.

Quando una VM di storage raggiunge il limite massimo di capacità, alcune operazioni non possono essere eseguite. System Manager fornisce suggerimenti per le fasi successive di **"Insights"**.

Unità di misura della capacità

System Manager calcola la capacità dello storage in base a unità binarie di 1024 (2^{10}) byte.

- A partire da ONTAP 9.10.1, le unità di capacità dello storage vengono visualizzate in Gestione sistemi come KiB, MiB, GiB, TIB e PIB.
- In ONTAP 9.10.0 e versioni precedenti, queste unità vengono visualizzate in Gestione sistema come KB, MB, GB, TB e PB.

> Le unità utilizzate in Gestione sistema per il throughput continuano a essere KB/s, MB/s, GB/s, TB/s e PB/s per tutte le release di ONTAP.

Unità di capacità visualizzata in Gestore di sistema per ONTAP 9.10.0 e versioni precedenti	Unità di capacità visualizzata in Gestore di sistema per ONTAP 9.10.1 e versioni successive	Calcolo	Valore in byte
KB	KiB	1024	1024 byte
MB	MIB	1024 * 1024	1,048,576 byte
GB	Gib	1024 * 1024 * 1024	1,073,741,824 byte
TB	TIB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 byte
PB	PIB	1024 * 1024 * 1024 * 1024 * 1024	1,125,899,906,842,624 byte

Informazioni correlate

"Monitorare la capacità in System Manager"

"Creazione di report e applicazione dello spazio logico per i volumi"

Panoramica dell'efficienza dello storage sensibile alla temperatura

ONTAP offre vantaggi in termini di efficienza dello storage sensibili alla temperatura, valutando la frequenza di accesso ai dati del volume e mappando tale frequenza al grado di compressione applicato a tali dati. Per i dati cold a cui si accede raramente, i blocchi di dati più grandi vengono compressi, mentre per i dati hot, a cui si accede frequentemente e che vengono sovrascritti più spesso, i blocchi di dati più piccoli vengono compressi, rendendo il processo più efficiente.

L'efficienza dello storage sensibile alla temperatura (TSSE) viene introdotta in ONTAP 9.8 e attivata automaticamente sui volumi AFF appena creati con thin provisioning. È possibile abilitare l'efficienza dello storage sensibile alla temperatura sui volumi AFF esistenti e sui volumi DP non AFF con thin provisioning.

Introduzione delle modalità "predefinite" ed "efficienti"

A partire da ONTAP 9.10.1, sono state introdotte due modalità di efficienza dello storage a livello di volume solo per i sistemi AFF, *default* e *Efficient*. Le due modalità consentono di scegliere tra la compressione file (predefinita), che è la modalità predefinita per la creazione di nuovi volumi AFF, o l'efficienza dello storage sensibile alla temperatura (efficiente), che consente l'efficienza dello storage sensibile alla temperatura. Con ONTAP 9.10.1, "l'efficienza dello storage sensibile alla temperatura deve essere impostata in modo esplicito" per attivare la compressione adattativa automatica. Tuttavia, altre funzionalità di efficienza dello storage, come la compattazione dei dati, la pianificazione della deduplica automatica, la deduplica inline, la deduplica inline tra volumi e la deduplica in background tra volumi, sono attivate per impostazione predefinita sulle piattaforme AFF sia per le modalità predefinite che per quelle efficienti.

Entrambe le modalità di efficienza dello storage (predefinite ed efficienti) sono supportate negli aggregati abilitati per FabricPool e con tutti i tipi di policy di tiering.

Efficienza dello storage sensibile alla temperatura abilitata sulle piattaforme C-Series

L'efficienza dello storage sensibile alla temperatura è attivata per impostazione predefinita sulle piattaforme AFF C-Series e durante la migrazione dei volumi da una piattaforma non TSSE a una piattaforma C-Series abilitata a TSSE utilizzando lo spostamento del volume o SnapMirror con le seguenti release installate sulla destinazione:

- ONTAP 9.12.1P4 e versioni successive
- ONTAP 9.13.1 e versioni successive

Per ulteriori informazioni, vedere "Comportamento in termini di efficienza dello storage con lo spostamento dei volumi e le operazioni SnapMirror".

Tuttavia, per i volumi esistenti, l'efficienza dello storage sensibile alla temperatura non viene attivata automaticamente "modificare la modalità di efficienza dello storage" manualmente per passare alla modalità efficiente.

> Una volta impostata la modalità di efficienza dello storage su efficiente, non sarà più possibile modificarla.

Efficienza dello storage migliorata grazie al confezionamento sequenziale di blocchi fisici contigui

A partire da ONTAP 9.13.1, l'efficienza dello storage sensibile alla temperatura aggiunge un impacchettamento sequenziale di blocchi fisici contigui per migliorare ulteriormente l'efficienza dello storage. I volumi con efficienza dello storage sensibile alla temperatura attivata dispongono automaticamente del packing sequenziale attivato quando si aggiornano i sistemi a ONTAP 9.13.1. Una volta attivato il packing sequenziale, è necessario "reimballare manualmente i dati esistenti".

Considerazioni sull'upgrade

Quando si esegue l'aggiornamento a ONTAP 9.10.1 e versioni successive, ai volumi esistenti viene assegnata una modalità di efficienza dello storage basata sul tipo di compressione attualmente attivata sui volumi. Durante un aggiornamento, ai volumi con compressione attivata viene assegnata la modalità predefinita e ai volumi con efficienza dello storage sensibile alla temperatura attivata viene assegnata la modalità efficiente. Se la compressione non è attivata, la modalità di efficienza dello storage rimane vuota.

Sicurezza

Autenticazione e autorizzazione del client

ONTAP utilizza metodi standard per proteggere l'accesso client e amministratore allo storage e per proteggerlo dai virus. Sono disponibili tecnologie avanzate per la crittografia dei dati a riposo e per lo storage WORM.

ONTAP autentica un computer client e un utente verificando la propria identità con un'origine attendibile. ONTAP autorizza un utente ad accedere a un file o a una directory confrontando le credenziali dell'utente con le autorizzazioni configurate nel file o nella directory.

Autenticazione

È possibile creare account utente locali o remoti:

- Un account locale è un account in cui le informazioni dell'account risiedono nel sistema di storage.
- Un account remoto è un account in cui le informazioni sull'account vengono memorizzate in un controller di dominio Active Directory, in un server LDAP o in un server NIS.

ONTAP utilizza i servizi dei nomi locali o esterni per cercare informazioni relative a nome host, utente, gruppo, netgroup e mappatura dei nomi. ONTAP supporta i seguenti servizi per i nomi:

- Utenti locali
- DNS
- Domini NIS esterni
- Domini LDAP esterni

Una *name service switch table* specifica le fonti per la ricerca delle informazioni di rete e l'ordine in cui ricercarle (fornendo la funzionalità equivalente del file /etc/nsswitch.conf sui sistemi UNIX). Quando un client NAS si connette a SVM, ONTAP verifica i servizi dei nomi specificati per ottenere le informazioni richieste.

supporto Kerberos Kerberos è un protocollo di autenticazione di rete che fornisce "sautenticazione trong" crittografando le password utente nelle implementazioni client-server. ONTAP supporta l'autenticazione Kerberos 5 con controllo dell'integrità (krb5i) e l'autenticazione Kerberos 5 con controllo della privacy (krb5p).

Autorizzazione

ONTAP valuta tre livelli di sicurezza per determinare se un'entità è autorizzata a eseguire un'azione richiesta su file e directory che risiedono su una SVM. L'accesso è determinato dalle autorizzazioni effettive dopo la valutazione dei livelli di sicurezza:

- Sicurezza di esportazione (NFS) e condivisione (SMB)

  La sicurezza di esportazione e condivisione si applica all'accesso client a una data esportazione NFS o condivisione SMB. Gli utenti con privilegi amministrativi possono gestire la sicurezza a livello di esportazione e condivisione dai client SMB e NFS.

- Protezione di file e directory di Access Guard a livello di storage

  La sicurezza di Access Guard a livello di storage si applica all'accesso dei client SMB e NFS ai volumi SVM. Sono supportate solo le autorizzazioni di accesso NTFS. Affinché ONTAP esegua controlli di sicurezza sugli utenti UNIX per l'accesso ai dati sui volumi per i quali è stato applicato Storage-Level Access Guard, l'utente UNIX deve eseguire il mapping a un utente Windows sulla SVM proprietaria del volume.

- Sicurezza nativa a livello di file in NTFS, UNIX e NFSv4

  La protezione nativa a livello di file esiste nel file o nella directory che rappresenta l'oggetto di storage. È possibile impostare la sicurezza a livello di file da un client. Le autorizzazioni dei file sono efficaci indipendentemente dal fatto che SMB o NFS vengano utilizzati per accedere ai dati.

Autenticazione con SAML

ONTAP supporta il linguaggio SAML (Security Assertion Markup Language) per l'autenticazione degli utenti remoti. Sono supportati diversi provider di identità (IDP). Per ulteriori informazioni sugli IDP supportati e istruzioni per l'attivazione dell'autenticazione SAML, fare riferimento a. "Configurare l'autenticazione SAML".

OAuth 2,0 con client API REST ONTAP

Il supporto per il framework Open Authorization (OAuth 2,0) è disponibile a partire da ONTAP 9,14. È possibile utilizzare OAuth 2,0 solo per prendere decisioni di autorizzazione e controllo degli accessi quando il client

utilizza l'API REST per accedere a ONTAP. Tuttavia, puoi configurare e abilitare la funzionalità con qualsiasi interfaccia amministrativa di ONTAP, inclusi CLI, System Manager e API REST.

Le funzionalità standard di OAuth 2,0 sono supportate insieme a diversi server di autorizzazione più diffusi. È possibile migliorare ulteriormente la protezione di ONTAP utilizzando token di accesso con vincoli di mittente basati su TLS comuni. Inoltre, è disponibile una vasta gamma di opzioni di autorizzazione, tra cui ambiti indipendenti, oltre all'integrazione con i ruoli REST di ONTAP e le definizioni degli utenti locali. Vedere "Panoramica dell'implementazione di ONTAP OAuth 2,0" per ulteriori informazioni.

Autenticazione amministratore e RBAC

Gli amministratori utilizzano account di accesso locali o remoti per autenticarsi al cluster e alla SVM. RBAC (Role-Based Access Control) determina i comandi a cui un amministratore ha accesso.

Autenticazione

È possibile creare account di amministratore SVM e cluster locali o remoti:

- Un account locale è un account in cui le informazioni sull'account, la chiave pubblica o il certificato di protezione risiedono nel sistema di storage.
- Un account remoto è un account in cui le informazioni sull'account vengono memorizzate in un controller di dominio Active Directory, in un server LDAP o in un server NIS.

Ad eccezione del DNS, ONTAP utilizza gli stessi servizi di nome per autenticare gli account amministratore utilizzati per autenticare i client.

RBAC

Il *ruolo* assegnato a un amministratore determina i comandi a cui l'amministratore ha accesso. Il ruolo viene assegnato quando si crea l'account per l'amministratore. È possibile assegnare un ruolo diverso o definire ruoli personalizzati in base alle esigenze.

Scansione virus

È possibile utilizzare la funzionalità antivirus integrata nel sistema di storage per proteggere i dati da virus o altri codici dannosi. La scansione antivirus di ONTAP, denominata *Vscan*, combina il software antivirus di terze parti più all'avanguardia con le funzionalità di ONTAP che offrono la flessibilità necessaria per controllare quali file vengono sottoposti a scansione e quando.

I sistemi storage trasferiscono le operazioni di scansione a server esterni che ospitano software antivirus di terze parti. Il *connettore antivirus ONTAP*, fornito da NetApp e installato sul server esterno, gestisce le comunicazioni tra il sistema di storage e il software antivirus.

- È possibile utilizzare *on-access scanning* per verificare la presenza di virus quando i client aprono, leggono, rinominano o chiudono i file su SMB. L'operazione sul file viene sospesa fino a quando il server esterno non riporta lo stato di scansione del file. Se il file è già stato sottoposto a scansione, ONTAP consente l'operazione. In caso contrario, richiede una scansione dal server.

  La scansione on-access non è supportata per NFS.

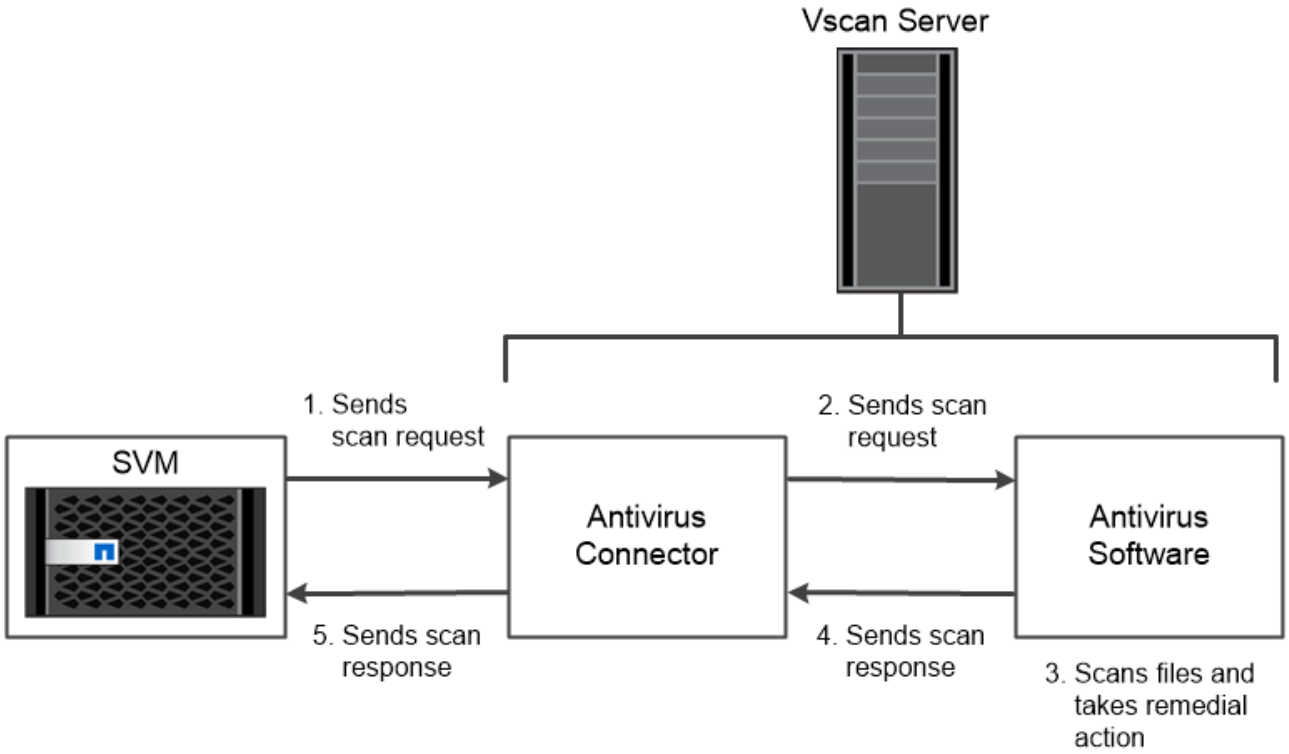
- È possibile utilizzare la *scansione on-demand* per controllare i file alla ricerca di virus immediatamente o in base a una pianificazione. Ad esempio, è possibile eseguire scansioni solo in ore non di punta. Il server esterno aggiorna lo stato di scansione dei file selezionati, in modo che la latenza di accesso ai file (presupponendo che non siano stati modificati) sia in genere ridotta al successivo accesso tramite SMB.

  È possibile utilizzare la scansione on-demand per qualsiasi percorso nello spazio dei nomi SVM, anche per i volumi esportati solo tramite NFS.

In genere, si abilitano entrambe le modalità di scansione su una SVM. In entrambe le modalità, il software antivirus esegue un'azione correttiva sui file infetti in base alle impostazioni del software.

scansione virus in disaster recovery e configurazioni MetroCluster

Per le configurazioni di disaster recovery e MetroCluster, è necessario configurare server Vscan separati per i cluster locali e partner.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

Crittografia

ONTAP offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

ONTAP è conforme agli standard federali sull'elaborazione delle informazioni (FIPS) 140-2 per tutte le connessioni SSL. È possibile utilizzare le seguenti soluzioni di crittografia:

- Soluzioni hardware:
  - NetApp Storage Encryption (NSE)

    NSE è una soluzione hardware che utilizza dischi con crittografia automatica (SED).

  - SED NVMe

    ONTAP offre la crittografia completa del disco per i SED NVMe che non dispongono della certificazione FIPS 140-2.

- Soluzioni software:
  - NetApp aggregate Encryption (NAE)

    NAE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con chiavi univoche per ciascun aggregato.

  - NetApp Volume Encryption (NVE)

    NVE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con una chiave univoca per ciascun volume.

Utilizzare soluzioni di crittografia sia software (NAE o NVE) che hardware (NSE o NVMe SED) per ottenere una doppia crittografia a riposo. L'efficienza dello storage non è influenzata dalla crittografia NAE o NVE.

Crittografia dello storage NetApp

NetApp Storage Encryption (NSE) supporta i SED che crittografano i dati durante la scrittura. I dati non possono essere letti senza una chiave di crittografia memorizzata sul disco. La chiave di crittografia, a sua volta, è accessibile solo a un nodo autenticato.

In caso di richiesta i/o, un nodo esegue l'autenticazione in un SED utilizzando una chiave di autenticazione recuperata da un server di gestione delle chiavi esterno o da Onboard Key Manager:

- Il server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi di autenticazione ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).
- Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati.

NSE supporta HDD e SSD con crittografia automatica. È possibile utilizzare NetApp Volume Encryption con NSE per la doppia crittografia dei dati sui dischi NSE.

> Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSe non crittografa i dati che risiedono nel modulo Flash cache.

Dischi con crittografia automatica NVMe

I dischi SED NVMe non dispongono della certificazione FIPS 140-2, tuttavia, utilizzano la crittografia trasparente dei dischi AES a 256 bit per proteggere i dati inattivi.

Le operazioni di crittografia dei dati, come la generazione di una chiave di autenticazione, vengono eseguite internamente. La chiave di autenticazione viene generata la prima volta che il sistema di storage accede al disco. In seguito, i dischi proteggono i dati inattivi richiedendo l'autenticazione del sistema di storage ogni volta che vengono richieste operazioni sui dati.

Crittografia aggregata NetApp

NetApp aggregate Encryption (NAE) è una tecnologia software per la crittografia di tutti i dati su un aggregato. Un vantaggio di NAE è che i volumi sono inclusi nella deduplica a livello di aggregato, mentre i volumi NVE sono esclusi.

Con NAE attivato, i volumi all'interno dell'aggregato possono essere crittografati con chiavi aggregate.

A partire da ONTAP 9,7, gli aggregati e i volumi appena creati sono crittografati per impostazione predefinita, quando si dispone di "Licenza NVE" e gestione della chiave integrata o esterna.

Crittografia dei volumi NetApp

NetApp Volume Encryption (NVE) è una tecnologia software per la crittografia dei dati inattivi di un volume alla volta. Una chiave di crittografia accessibile solo al sistema di storage garantisce che i dati del volume non possano essere letti se il dispositivo sottostante è separato dal sistema.

Entrambi i dati, incluse le copie Snapshot, e i metadati sono crittografati. L'accesso ai dati viene fornito da una chiave XTS-AES-256 univoca, una per volume. Un Onboard Key Manager integrato protegge le chiavi dello stesso sistema con i dati.

È possibile utilizzare NVE su qualsiasi tipo di aggregato (HDD, SSD, ibrido, LUN array), con qualsiasi tipo di RAID e in qualsiasi implementazione ONTAP supportata, incluso ONTAP Select. È inoltre possibile utilizzare NVE con NetApp Storage Encryption (NSE) per eseguire la doppia crittografia dei dati sui dischi NSE.

quando utilizzare i server KMIP sebbene sia meno costoso e generalmente più conveniente utilizzare Onboard Key Manager, è necessario configurare i server KMIP se si verifica una delle seguenti condizioni:

- La soluzione di gestione delle chiavi di crittografia deve essere conforme agli standard FIPS (Federal Information Processing Standards) 140-2 o ALLO standard OASIS KMIP.
- Hai bisogno di una soluzione multi-cluster. I server KMIP supportano più cluster con gestione centralizzata delle chiavi di crittografia.

  I server KMIP supportano più cluster con gestione centralizzata delle chiavi di crittografia.

- La tua azienda richiede una maggiore sicurezza nell'archiviazione delle chiavi di autenticazione su un sistema o in una posizione diversa dai dati.

  I server KMIP memorizzano le chiavi di autenticazione separatamente dai dati.

Informazioni correlate

"FAQ - NetApp Volume Encryption e NetApp aggregate Encryption"

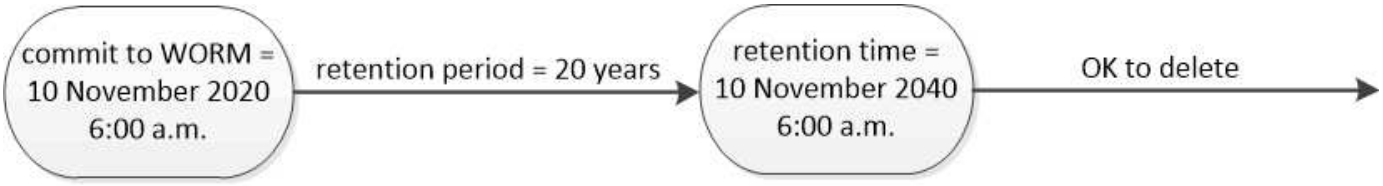
Storage WORM

SnapLock è una soluzione per la compliance dalle performance elevate per le organizzazioni che utilizzano lo storage *write once, Read Many (WORM)* per conservare i file critici in forma non modificata per scopi normativi e di governance.

Una singola licenza consente di utilizzare SnapLock in una *modalità di conformità* rigorosa, per soddisfare mandati esterni come la norma SEC 17a-4, e una *modalità aziendale* più allentata, per soddisfare le normative interne per la protezione delle risorse digitali. SnapLock utilizza un *ComplianceClock* a prova di manomissione

per determinare quando è trascorso il periodo di conservazione di un file WORM.

È possibile utilizzare *SnapLock for SnapVault* per proteggere WORM le copie Snapshot sullo storage secondario. È possibile utilizzare SnapMirror per replicare i file WORM in un'altra posizione geografica per il disaster recovery e altri scopi.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

Gestione dei dati consapevole dell'applicazione

La gestione dei dati consapevole delle applicazioni consente di descrivere l'applicazione che si desidera implementare su ONTAP in termini di applicazione, piuttosto che in termini di storage. L'applicazione può essere configurata e pronta per la distribuzione rapida dei dati con input minimi utilizzando System Manager e le API REST.

La funzione di gestione dei dati basata sulle applicazioni consente di configurare, gestire e monitorare lo storage a livello di singole applicazioni. Questa funzionalità incorpora le Best practice ONTAP pertinenti per il provisioning ottimale delle applicazioni, con posizionamento bilanciato degli oggetti storage in base ai livelli di servizio delle performance desiderati e alle risorse di sistema disponibili.

La funzionalità di gestione dei dati consapevole dell'applicazione include un set di modelli di applicazione, con ciascun modello costituito da un set di parametri che descrivono collettivamente la configurazione di un'applicazione. Questi parametri, spesso preimpostati con valori predefiniti, definiscono le caratteristiche che un amministratore dell'applicazione può specificare per il provisioning dello storage su un sistema ONTAP, come dimensioni del database, livelli di servizio, elementi di accesso al protocollo come LIF, criteri di protezione locale e criteri di protezione remota. In base ai parametri specificati, ONTAP configura entità di storage come LUN e volumi con dimensioni e livelli di servizio appropriati per l'applicazione.

È possibile eseguire le seguenti attività per le applicazioni:

- Creare applicazioni utilizzando i modelli di applicazione
- Gestire lo storage associato alle applicazioni
- Modificare o eliminare le applicazioni
- Visualizzare le applicazioni
- Gestire le copie Snapshot delle applicazioni
- Creare gruppi di coerenza Fornire funzionalità di protezione dei dati selezionando più LUN nello stesso volume o in volumi diversi

FabricPool

Molti clienti NetApp dispongono di quantità significative di dati memorizzati a cui si accede raramente. Chiamiamo i dati *cold*. I clienti hanno anche dati ai quali si accede

frequentemente, che chiamiamo *hot* data. Idealmente, si desidera conservare i dati più caldi sullo storage più veloce per ottenere le migliori performance. I dati cold possono passare a uno storage più lento, purché sia immediatamente disponibile, se necessario. Ma come fai a sapere quali parti dei tuoi dati sono calde e quali sono fredde?

FabricPool è una funzionalità di ONTAP che sposta automaticamente i dati tra un Tier locale ad alte performance (aggregato) e un Tier cloud in base ai modelli di accesso. Il tiering libera lo storage locale costoso per i dati hot mantenendo i dati cold prontamente disponibili dallo storage a oggetti a basso costo nel cloud. FabricPool monitora costantemente l'accesso ai dati e sposta i dati tra i Tier per ottenere le migliori performance e il massimo risparmio.

L'utilizzo di FabricPool per il Tier dei dati cold nel cloud è uno dei modi più semplici per ottenere l'efficienza del cloud e creare una configurazione del cloud ibrido. FabricPool funziona a livello di blocchi di storage, quindi funziona sia con i dati di file che con i dati LUN.

Ma FabricPool non è solo per il tiering dei dati on-premise nel cloud. Molti clienti utilizzano FabricPool in Cloud Volumes ONTAP per eseguire il tiering dei dati cold da uno storage cloud più costoso a uno storage a oggetti a basso costo all'interno del cloud provider. A partire da ONTAP 9.8, puoi acquisire analytics su volumi abilitati FabricPool con "Analisi del file system" oppure "efficienza dello storage sensibile alla temperatura".

Le applicazioni che utilizzano i dati non sono consapevoli del fatto che i dati sono a livelli, pertanto non sono necessarie modifiche alle applicazioni. Il tiering è completamente automatico, quindi non è necessaria alcuna amministrazione in corso.

È possibile memorizzare i dati cold nello storage a oggetti di uno dei principali provider di cloud. Oppure scegli NetApp StorageGRID per conservare i tuoi dati nel tuo cloud privato, per ottenere le massime performance e il controllo completo sui tuoi dati.

Informazioni correlate

"Documento Gestore di sistema di FabricPool"

"Tiering BlueXP"

"Elenco di riproduzione FabricPool su NetApp TechComm TV"