



Proteggi i tuoi dati

Workload Factory for NetApp Console

NetApp

October 07, 2026

This PDF was generated from <https://docs.netapp.com/it-it/data-services-workloads/fsx-storage/data-protection-overview.html> on October 07, 2026. Always check docs.netapp.com for the latest.

Sommario

Proteggi i tuoi dati	1
Tipi di protezione dei dati in NetApp Workload Factory	1
Tipi di protezione dei dati	1
Best practice per proteggere i dati del tuo workload	2
Proteggi i dati del tuo workload con gli snapshot	2
Proteggi i dati del tuo workload con NetApp Autonomous Ransomware Protection with AI	2
Proteggi i dati del tuo workload con la replica dei volumi	2
Proteggi i dati del tuo carico di lavoro con i backup	3
Raccomandazioni per proteggere i dati del tuo workload	3
Usa le snapshot per proteggere i dati	3
Utilizza gli snapshot per proteggere i dati in NetApp Workload Factory	3
Gestisci le policy di snapshot per i volumi in NetApp Workload Factory	6
Gestisci le Snapshot di un volume FSx for ONTAP	10
Utilizza i backup per proteggere i dati in NetApp Workload Factory	12
Crea un backup su richiesta di un volume	12
Gestire la pianificazione dei backup per un file system FSx for ONTAP	13
Ripristinare un volume da un backup in NetApp Workload Factory	13
Usa la replica per proteggere i dati	14
Replica i dati su FSx per ONTAP in NetApp Workload Factory	14
Replica i dati del cluster ONTAP on-premises in NetApp Workload Factory	24
Replica una VM di storage in un altro file system FSx for ONTAP	28
Monitora i ritardi di replica in NetApp Workload Factory	29
Gestisci le relazioni di replica in NetApp Workload Factory	30
Proteggi i tuoi dati FSx for ONTAP con NetApp Autonomous Ransomware Protection con AI	34
Abilitare ARP/AI per un file system o un volume	35
Convalida gli attacchi ransomware	36
Recupera i dati dopo un attacco ransomware	37
Clona un volume in NetApp Workload Factory	37
Proteggi i tuoi dati FSx for ONTAP con un cyber vault	38

Proteggi i tuoi dati

Tipi di protezione dei dati in NetApp Workload Factory

FSx for ONTAP supporta snapshot, NetApp Autonomous Ransomware Protection with AI, replica e backup per la protezione dei dati. Ti consigliamo di utilizzare una combinazione di tipi di protezione dei dati per prepararti all'inevitabile e salvaguardare i tuoi dati.

Tipi di protezione dei dati

La protezione dei dati per i tuoi carichi di lavoro ti aiuta a garantire il ripristino in qualsiasi momento in caso di perdita di dati. Scopri i diversi tipi di protezione dei dati prima di selezionare le funzionalità che desideri utilizzare.

Istantanee

Uno snapshot crea un'immagine point-in-time di sola lettura di un volume all'interno del volume di origine come copia snapshot. Puoi utilizzare la copia snapshot per recuperare singoli file o per ripristinare l'intero contenuto di un volume. Gli snapshot sono alla base di tutti i metodi di backup. La copia snapshot creata sul tuo volume viene utilizzata per mantenere sincronizzati il volume replicato e il file di backup con le modifiche apportate al volume di origine.

NetApp Protezione autonoma dal ransomware con AI

NetApp Autonomous Ransomware Protection with AI (ARP/AI) utilizza l'analisi dei carichi di lavoro negli ambienti NAS (NFS/SMB) per rilevare e avvisare in caso di attività anomale che potrebbero indicare un attacco ransomware. Quando sospetta un attacco, ARP/AI crea anche nuove snapshot immutabili, oltre alla protezione esistente fornita dalle snapshot pianificate.

Replica

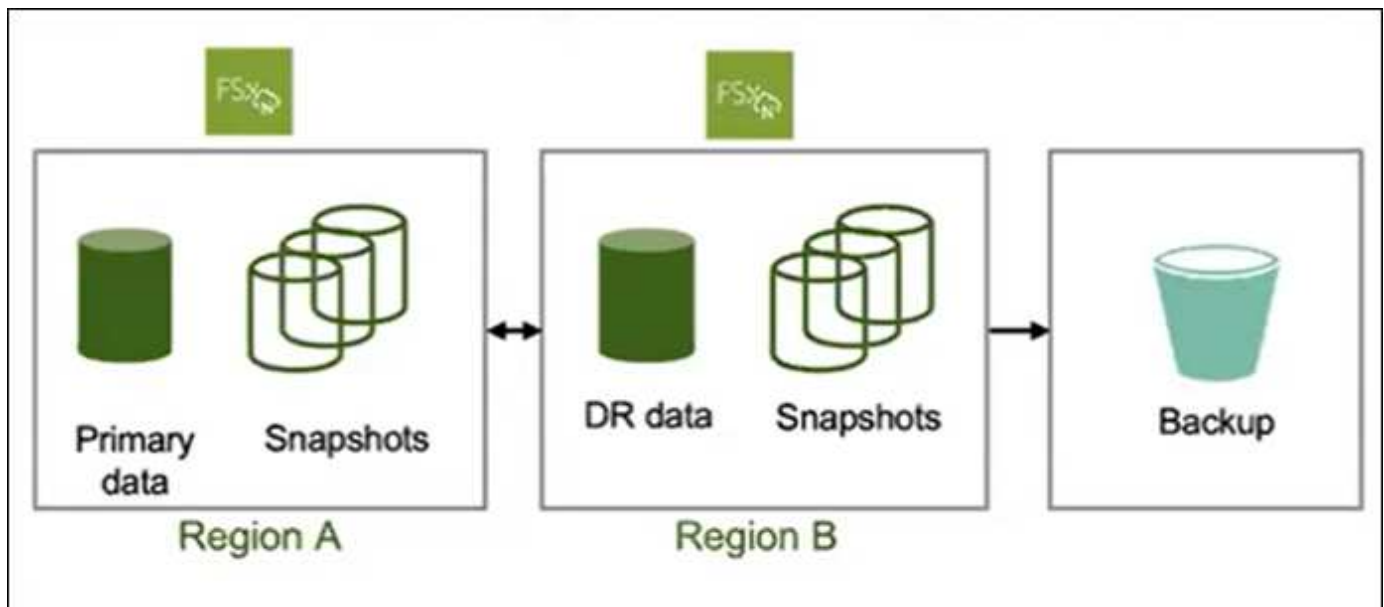
La replica crea una copia secondaria dei tuoi dati su un altro file system FSx for ONTAP e aggiorna continuamente i dati secondari. I tuoi dati restano aggiornati e disponibili ogni volta che ti servono, ad esempio per il disaster recovery.

Puoi scegliere di creare sia volumi replicati su un altro file system FSx for ONTAP sia file di backup nel cloud. Oppure puoi scegliere di creare solo volumi replicati o solo file di backup: la scelta è tua.

Backup

Puoi creare backup dei tuoi dati nel cloud per proteggerli e conservarli a lungo termine. Se necessario, puoi ripristinare un volume, una cartella o singoli file dal backup nello stesso file system di lavoro o in uno diverso.

Il diagramma seguente mostra una rappresentazione visiva della protezione dei dati per lo storage FSx per ONTAP tramite snapshot, replica tra regioni e backup su storage a oggetti.



Best practice per proteggere i dati del tuo workload

FSx for ONTAP offre diverse opzioni di protezione dei dati che possono essere combinate per raggiungere gli obiettivi selezionati in termini di punto di ripristino e tempo di ripristino. Per la migliore protezione possibile, ti consigliamo di utilizzare sia gli snapshot del volume sia i backup del volume.

Un recovery point objective (RPO) descrive quanto è recente l'ultima copia garantita dei tuoi dati, che dipende dalla frequenza con cui vengono effettuate le copie. Un recovery time objective (RTO) definisce quanto tempo serve per ripristinare i tuoi dati.

Proteggi i dati del tuo workload con gli snapshot

Gli snapshot sono versioni virtuali point-in-time di un volume che vengono create a intervalli programmati. Puoi accedere agli snapshot utilizzando i comandi standard del file system. Gli snapshot offrono un RPO di appena un'ora. L'RTO dipende dalla quantità di dati da ripristinare ed è limitato principalmente dal limite di throughput del volume. Gli snapshot ti consentono inoltre di ripristinare file e directory specifici, riducendo ulteriormente l'RTO. Gli snapshot consumano spazio aggiuntivo sul volume solo per le modifiche apportate al volume.

Proteggi i dati del tuo workload con NetApp Autonomous Ransomware Protection with AI

NetApp Autonomous Ransomware Protection with AI (ARP/AI) rappresenta un importante ulteriore livello di difesa se il software antivirus non è riuscito a rilevare un'intrusione. L'impostazione di una policy ARP/AI la abilita per tutte le VM di storage e per tutti i volumi esistenti e appena creati. Una volta abilitata, ARP/AI rileva e protegge tutti i volumi e le VM di storage. Se un'estensione di file viene segnalata come anomala, dovresti valutare l'avviso.

Proteggi i dati del tuo workload con la replica dei volumi

La replica del volume crea una copia dei dati più recenti di un volume, inclusi tutti i relativi snapshot, in una regione diversa. Se non puoi permetterti RTO di diverse ore per un'operazione di ripristino completo del volume da un backup del volume, prendi in considerazione l'esecuzione di una replica del volume. Anche se la replica del volume garantisce la disponibilità di dati recenti in una regione diversa da usare, devi configurare i client in modo che utilizzino il volume nell'altra regione.

Proteggi i dati del tuo carico di lavoro con i backup

I backup di volume forniscono copie point-in-time indipendenti del tuo volume. Possono essere utilizzati per archiviare backup precedenti e fornire la necessaria seconda copia dei tuoi dati. Le pianificazioni di backup giornaliere, settimanali e mensili consentono RPO a partire da un giorno. I backup di volume possono essere ripristinati solo nella loro interezza. La creazione di un volume da un backup (RTO) può richiedere da poche ore a molti giorni, a seconda delle dimensioni del backup.

Raccomandazioni per proteggere i dati del tuo workload

Considera le seguenti raccomandazioni per proteggere i dati del tuo workload.

- Usa la replica dei volumi per il disaster recovery: se la tua applicazione richiede un RTO basso, valuta l'utilizzo della replica dei volumi per replicare i dati in un'altra regione.
- Utilizza i backup del volume insieme agli snapshot: usare insieme queste due funzionalità ti garantisce di poter ripristinare i file dagli snapshot ed eseguire ripristini completi in caso di perdita del volume usando i backup.
- Definisci una policy di backup: assicurati che la policy di backup soddisfi i requisiti aziendali in termini di anzianità e frequenza dei backup. Consigliamo di mantenere un minimo di due backup giornalieri per ogni volume.
- Definisci una pianificazione degli snapshot: è meno probabile che gli snapshot meno recenti vengano utilizzati per ripristinare i dati. Ti consigliamo di definire una pianificazione degli snapshot che tenga conto del rendimento decrescente del mantenimento degli snapshot meno recenti rispetto al costo di una capacità snapshot aggiuntiva.
- Abilita una policy ARP/AI per il tuo file system o per singoli volumi per aggiungere un ulteriore livello di protezione e salvaguardare i tuoi dati dagli attacchi ransomware.

Usa le snapshot per proteggere i dati

Utilizza gli snapshot per proteggere i dati in NetApp Workload Factory

Proteggi i dati dei volumi da cancellazioni o danneggiamenti accidentali creando e gestendo snapshot in NetApp Workload Factory. Puoi creare uno snapshot on-demand di un volume, definire una snapshot policy per automatizzare la creazione e la conservazione degli snapshot per le VM di storage e ripristinare un volume da uno snapshot esistente per recuperare i dati in un punto specifico nel tempo.

Crea un'istantanea su richiesta di un volume

Crea uno snapshot manuale di un volume FSx for ONTAP in NetApp Workload Factory. Gli snapshot sono versioni point-in-time del contenuto del tuo volume.

Gli Snapshot sono risorse dei volumi e rappresentano istantanee dei tuoi dati che occupano spazio solo per i dati modificati. Poiché i dati cambiano nel tempo, gli Snapshot in genere occupano più spazio man mano che invecchiano.

I volumi FSx for ONTAP utilizzano il copy-on-write just-in-time, in modo che i file non modificati nelle Snapshot non consumino alcuna capacità del volume.



Gli snapshot non sono copie dei tuoi dati. Se desideri creare copie dei tuoi dati, valuta l'utilizzo

delle funzionalità di backup del volume o di replica del volume.

Prima di iniziare

Devi associare un collegamento per creare un'istantanea manuale di un volume. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il collegamento, torna a questa procedura.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx for ONTAP**, seleziona il menu delle azioni del file system che contiene il volume per cui vuoi creare uno Snapshot, quindi seleziona **Manage**.
4. Nella panoramica del file system, seleziona la scheda **Volumi**.
5. Dalla scheda **Volumi**, seleziona il menu Azioni per il volume da proteggere con Snapshot.
6. Seleziona **Azioni di protezione dei dati** e poi **Gestisci snapshot**.
7. Dalla pagina Gestisci snapshot, seleziona **Crea snapshot**.
8. Nella finestra di dialogo Crea uno Snapshot, procedi come segue:
 - a. Inserisci un nome per la snapshot nel campo **Nome snapshot**.
 - b. Se vuoi, seleziona un'etichetta o creane una nuova.
 - c. Imposta il **periodo di conservazione** come numero di ore, giorni, mesi o anni.
 - d. Opzionale: **Rendi immutabile questa snapshot** per impedire che venga eliminata durante il periodo di conservazione.

Accetta l'affermazione relativa alle snapshot immutabili.
9. Seleziona **Crea**.

Crea una policy di snapshot per le macchine virtuali di archiviazione

Crea una policy di Snapshot personalizzata per le VM di storage in Workload Factory per gestire la creazione e il periodo di conservazione degli Snapshot. Una policy di Snapshot definisce come il sistema crea gli Snapshot per una VM di storage. Puoi creare una policy di Snapshot per una VM di storage in un file system FSx for ONTAP. Puoi anche condividere la policy tra più VM di storage.

Puoi creare una policy di Snapshot personalizzata diversa dalle tre policy di Snapshot integrate per FSx for ONTAP:

- `default`
- `default-1weekly`
- `none`

Per impostazione predefinita, ogni volume è associato alla policy di Snapshot `default` del file system. Ti consigliamo di utilizzare questa policy per la maggior parte dei carichi di lavoro.

Personalizzando una policy, puoi specificare quando creare Snapshot, quante copie conservare e come denominarle.

Prima di iniziare

- Una volta creata una policy di Snapshot, non puoi modificarne l'associazione con le VM di storage, ma puoi sempre aggiungere o rimuovere la policy dai volumi.
- Prima di utilizzare gli snapshot, considera quanto segue sulla capacità degli snapshot:
 - Per la maggior parte dei set di dati, una capacità aggiuntiva del 20% è sufficiente per conservare le snapshot fino a quattro settimane. Man mano che i dati invecchiano, è meno probabile che vengano usati per i ripristini.
 - La sovrascrittura di tutti i dati in uno Snapshot consuma una notevole capacità del volume, fattore che incide sul provisioning della capacità del volume.
- Per creare una policy di snapshot personalizzata, devi associare un collegamento. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il collegamento, torna a questa procedura.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx for ONTAP**, seleziona il menu Azioni del file system con il volume, quindi seleziona **Gestisci**.
4. Nella panoramica del file system, seleziona la scheda **Storage VMs**.
5. Dalla scheda **Storage VMs**, seleziona il menu delle azioni per il volume da proteggere con Snapshot pianificate, quindi **Advanced actions** e infine **Manage snapshot policies**.
6. Nella pagina di gestione delle policy di Snapshot, seleziona **Crea policy di Snapshot**.
7. Nel campo **Nome policy di Snapshot**, inserisci un nome per la policy di Snapshot.
8. Facoltativamente, inserisci una descrizione per la policy di Snapshot.
9. Nella sezione **Pianificazione e copie dei criteri**, seleziona quando creare gli Snapshot. Ad esempio, ogni minuto o ogni ora.

Puoi selezionare più di una frequenza.

10. In **Numero di copie**, inserisci il numero di copie da conservare.

Il numero massimo di copie è 1,023.

11. Facoltativo: nella sezione **Convenzione di denominazione**, inserisci un **prefisso** per la policy.
12. L'etichetta di conservazione viene popolata automaticamente.

Questa etichetta si riferisce all'etichetta SnapMirror, ovvero all'etichetta di replica utilizzata per selezionare solo le Snapshot specificate per la replica dal file system di origine al file system di destinazione.

13. Opzionale: abilita gli **Snapshot immutabili** per le pianificazioni necessarie, imposta il **periodo di conservazione** per ciascuna pianificazione e accetta l'affermazione per continuare.

L'attivazione degli Snapshot immutabili blocca tutti gli Snapshot in questa policy di Snapshot per impedirne l'eliminazione durante il periodo di conservazione.

14. **Condivisione tra VM di storage**: Abilitato per impostazione predefinita. Quando è abilitato, la policy di Snapshot viene condivisa tra tutte le VM di storage nel file system. Disabilitalo per creare una policy di Snapshot per una singola VM di storage.

15. Seleziona **Crea**.

Ripristinare un volume da uno Snapshot

Puoi ripristinare i dati da uno snapshot su un volume esistente o su un nuovo volume. L'operazione di ripristino consente il recupero point-in-time quando un volume contiene file eliminati o danneggiati.

La creazione di un nuovo volume da una Snapshot consente di ottenere una copia dell'intero volume in pochi secondi, indipendentemente dalle dimensioni del volume. La copia appena creata rappresenta un nuovo volume.

Prima di iniziare

Considera le seguenti limitazioni prima di creare un volume da uno snapshot:

- Puoi ripristinare un volume da uno snapshot solo se disponi di una copia snapshot esistente del volume.
- Modifiche ai modelli di autorizzazione: se usi questa operazione per cambiare il tipo di protocollo network-attached storage (NAS), potrebbe cambiare anche il modello di autorizzazione fornito dallo stile di sicurezza. Potresti riscontrare problemi di autorizzazione per l'accesso ai file, che puoi risolvere solo manualmente con accesso come amministratore utilizzando gli strumenti del client NAS per l'impostazione delle autorizzazioni.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx for ONTAP**, seleziona il menu Azioni del file system con il volume, quindi seleziona **Gestisci**.
4. Nella panoramica del file system, seleziona la scheda **Volumi**.
5. Dalla scheda **Volumi**, seleziona il menu Azioni per il volume da ripristinare da uno Snapshot.
6. Seleziona **Azioni di protezione dei dati** e poi **Gestisci snapshot**.
7. Dalla pagina Gestisci snapshot, seleziona il menu delle azioni per lo snapshot da ripristinare, quindi seleziona **Ripristina**.
8. Nella finestra di dialogo Ripristina volume da snapshot, seleziona una delle seguenti opzioni:
 - Attiva l'opzione **Ripristina come nuovo volume**.

Nel campo **Nome del volume ripristinato**, immetti un nome univoco per il volume da ripristinare.

- Ripristina i dati da una Snapshot in un volume esistente. Questa operazione elimina definitivamente tutti i dati modificati dopo la creazione della Snapshot.

Accetta la dichiarazione per procedere.

9. Seleziona **Restore**.

Gestisci le policy di snapshot per i volumi in NetApp Workload Factory

Gestisci le policy di Snapshot per i volumi FSx for ONTAP in Workload Factory. Una policy di Snapshot definisce come il sistema crea gli Snapshot per un volume.

Le operazioni di gestione degli Snapshot, come l'assegnazione, la modifica e l'eliminazione delle policy di Snapshot per i volumi in un file system FSx for ONTAP, sono gestite a livello di storage VM. Le policy di

Snapshot possono essere condivise con una singola storage VM o con tutte le storage VM.

Alcune attività di gestione richiedono di associare un collegamento al file system FSx for ONTAP. ["Scopri i collegamenti di Workload Factory"](#).

Per impostazione predefinita, ogni volume è associato alla policy di Snapshot `default` del file system. Ti consigliamo di utilizzare questa policy per la maggior parte dei carichi di lavoro.

Assegna una policy di Snapshot a un volume

Puoi assegnare una policy di Snapshot a un singolo volume per creare Snapshot pianificati per tale volume.

Prima di iniziare

Devi associare un collegamento per assegnare una policy di snapshot. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il collegamento, torna a questa procedura.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. Seleziona il menu delle azioni del file system che contiene il volume a cui vuoi assegnare una policy di Snapshot, quindi seleziona **Manage**.
5. Nella panoramica del file system, seleziona la scheda **Storage VMs**.
6. Dalla scheda **Storage VMs**, seleziona il menu delle azioni per la VM di storage che contiene il volume da proteggere con Snapshot pianificate, quindi **Advanced actions** e infine **Manage snapshot policies**.
7. Nella pagina di gestione delle policy di Snapshot, seleziona il menu delle azioni della policy di Snapshot e quindi seleziona **Assign policy to volume**.
8. Nella finestra di dialogo Assegna policy di Snapshot, seleziona una policy di Snapshot da assegnare al volume e controlla la pianificazione della policy.

Se la policy contiene Snapshot immutabili e vuoi usarla, accetta la dichiarazione.

9. Seleziona **Assegna**.

Risultato

La policy di Snapshot è assegnata al volume.

Modificare una policy di Snapshot

Puoi modificare il nome della policy di Snapshot, la pianificazione e il numero di copie da conservare, nonché abilitare o disabilitare gli Snapshot immutabili. Non puoi abilitare o disabilitare la condivisione della policy tra le VM di storage. Questa opzione è disponibile solo durante la creazione della policy di Snapshot.

Prima di iniziare

Per visualizzare i criteri snapshot esistenti, devi associare un collegamento. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il collegamento, torna a questa procedura.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. Seleziona il menu Azioni del file system e quindi seleziona **Gestisci**.
5. Nella panoramica del file system, seleziona la scheda **Storage VMs**.
6. Dalla scheda **Storage VMs**, seleziona il menu delle azioni per la VM di storage che contiene il volume da proteggere con Snapshot pianificate, quindi **Advanced actions** e infine **Manage snapshot policies**.
7. Nella pagina di gestione delle policy di Snapshot, seleziona il menu delle azioni per la policy di Snapshot da modificare e poi seleziona **Modifica**.
8. Nella finestra di dialogo Modifica policy di Snapshot, apporta le modifiche necessarie alla policy di Snapshot.
9. Seleziona **Applica**.

Risultato

La policy di Snapshot è stata aggiornata.

Abilita snapshot immutabili

Blocca le Snapshot per impedirne l'eliminazione durante il periodo di conservazione.

Prima di iniziare

Devi associare un collegamento per abilitare gli snapshot immutabili. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il collegamento, torna a questa procedura.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Volumes explorer**.
3. Seleziona il menu Azioni del volume per cui vuoi bloccare gli Snapshot.
4. Seleziona **Azioni di protezione dei dati, Snapshot**, quindi **Rendi uno Snapshot immutabile**.
5. Nella finestra di dialogo Rendi immutabile una Snapshot, procedi come segue:
 - a. **Nome Snapshot**: Seleziona la Snapshot da bloccare.
 - b. Imposta il **periodo di conservazione** nel numero di ore, giorni, mesi o anni.
 - c. Accetta l'affermazione.
6. Seleziona **Applica**.

Risultato

La Snapshot del volume è ora bloccata.

Abilita la conservazione a lungo termine degli snapshot in NetApp Workload Factory

In NetApp Workload Factory, puoi abilitare gli snapshot per la conservazione a lungo termine, che ti consente di replicare snapshot specifici per il disaster recovery a lungo termine.

La conservazione a lungo termine consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover trasparente delle applicazioni tramite una copia secondaria.

Gli stessi passaggi si applicano per abilitare e modificare gli Snapshot destinati alla conservazione a lungo termine.

Quando un cluster ONTAP on-premises è la destinazione della relazione di replica, la modifica delle Snapshot per la conservazione a lungo termine non è supportata.



La modifica della conservazione a lungo termine non è disponibile quando si replicano i dati e le impostazioni di configurazione dello storage VM.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Dal menu **FSx for ONTAP**, seleziona **Inventory**, quindi seleziona il menu delle azioni del file system da aggiornare e infine seleziona **Manage**.
4. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
5. Nella scheda Relazioni di replica, seleziona il menu Azioni della pianificazione della relazione di replica da modificare.
6. Seleziona **Modifica conservazione a lungo termine**.
7. Nella finestra di dialogo Modifica conservazione a lungo termine, puoi attivare o disattivare le Snapshot per la conservazione a lungo termine.
8. Se scegli di disabilitare gli snapshot per la conservazione a lungo termine, seleziona **Applica** per completare questa operazione.
9. Se scegli di abilitare gli Snapshot per la conservazione a lungo termine, scegli se selezionare una policy esistente o crearne una nuova.
 - a. Per utilizzare una policy esistente, selezionala dal menu a tendina.
 - b. Per creare una nuova policy, inserisci quanto segue:
 - i. **Nome della policy**: Inserisci un nome per la policy.
 - ii. **policy di Snapshot**: Seleziona una o più policy di Snapshot.
 - iii. **Copie da conservare**: Inserisci il numero di copie Snapshot da conservare sul file system di destinazione.
10. Seleziona **Applica**.

Rimuovere una policy di Snapshot da un volume

Rimuovi una policy di Snapshot da un volume perché non vuoi più Snapshot del volume o perché vuoi eliminare una policy di Snapshot assegnata a più volumi. Per [eliminare una policy di Snapshot](#) assegnata a più di un volume, devi rimuoverla manualmente da tutti i volumi.

Prima di iniziare

Devi associare un collegamento per rimuovere una policy snapshot. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il collegamento, torna a questa procedura.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Dal menu **FSx for ONTAP**, seleziona **Inventory**, quindi seleziona il menu delle azioni del file system da aggiornare e infine seleziona **Manage**.
4. Nella panoramica del file system, seleziona la scheda **Storage VMs**.
5. Dalla scheda **Storage VMs**, seleziona il menu delle azioni per la VM di storage che contiene il volume da proteggere con Snapshot pianificate, quindi **Advanced actions** e infine **Manage snapshot policies**.
6. Nella pagina di gestione delle policy di Snapshot, seleziona il menu delle azioni della policy di Snapshot e quindi seleziona **Assign policy to volume**.
7. Nella finestra di dialogo Assegna policy di Snapshot, seleziona **None** per rimuovere la policy di Snapshot.
8. Seleziona **Assegna**.

Risultato

La policy di Snapshot viene rimossa dal volume.

Elimina una policy di Snapshot

Elimina una policy di Snapshot quando non ti serve più.

Quando una policy di Snapshot è assegnata a più di un volume, devi [rimuoverlo](#) manualmente da tutti i volumi per eliminare la policy di Snapshot. In alternativa, puoi [assegnare una diversa policy di Snapshot](#) ai volumi.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Dal menu **FSx for ONTAP**, seleziona **Inventory**, quindi seleziona il menu delle azioni del file system da aggiornare e infine seleziona **Manage**.
4. Nella panoramica del file system, seleziona la scheda **Storage VMs**.
5. Dalla scheda **VM di archiviazione**, seleziona il menu delle azioni della VM di archiviazione con la policy di Snapshot da eliminare, quindi **Azioni avanzate** e infine **Gestisci policy di Snapshot**.
6. Nella pagina di gestione delle policy di Snapshot, seleziona il menu delle azioni per la policy di Snapshot da eliminare e quindi seleziona **Elimina**.
7. Nella finestra di dialogo Delete, seleziona **Delete** per eliminare il criterio.

Gestisci le Snapshot di un volume FSx for ONTAP

Modifica le impostazioni degli Snapshot, abilita l'accesso alle directory ed elimina gli Snapshot per gestire gli Snapshot e la protezione dei dati in Workload Factory.

Modifica uno Snapshot

Modifica il nome, l'etichetta e il periodo di conservazione di uno snapshot. Se lo snapshot non è già immutabile, puoi renderlo immutabile.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Volumes explorer**.
3. Seleziona il menu Azioni per il volume con l'istantanea da modificare.
4. Seleziona **Azioni di protezione dei dati** e poi **Gestisci snapshot**.
5. Dalla pagina Gestisci snapshot, seleziona il menu delle azioni per lo snapshot da modificare, quindi seleziona **Modifica**.
6. Nella finestra di dialogo Modifica snapshot, puoi modificare quanto segue:
 - a. Cambia il nome.
 - b. Cambia l'etichetta.
 - c. Modifica il periodo di conservazione.
 - d. Opzionale: **Rendi immutabile questa snapshot** per impedire che venga eliminata durante il periodo di conservazione.

Se l'istantanea è già immutabile, non puoi modificare questa impostazione.

Accetta l'affermazione relativa alle snapshot immutabili.

7. Seleziona **Applica**.

Accedi a uno Snapshot

Abilita l'accesso alla directory degli snapshot per consentire agli utenti di accedere agli snapshot in autonomia.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Volumes explorer**.
3. Seleziona il menu Azioni per il volume con lo snapshot a cui accedere.
4. Seleziona **Azioni di protezione dei dati** e poi **Gestisci snapshot**.
5. Dalla pagina Gestisci snapshot, seleziona il menu delle azioni per lo snapshot a cui vuoi accedere, quindi seleziona **Accedi**.
6. Nella finestra di dialogo Access snapshot, seleziona **Abilita accesso alla directory snapshot** per accedere a questo snapshot del volume e a tutti gli snapshot del volume.
 - Per i volumi NFS: seleziona **Percorso di accesso NFS** per visualizzare il percorso NFS per lo snapshot.
 - Per i volumi SMB/CIFS: seleziona **Percorso di accesso SMB** per visualizzare il percorso SMB per lo Snapshot.
7. Copia il percorso di accesso.
8. Seleziona **Applica**.

Ripristina i dati da una Snapshot

Hai la possibilità di ripristinare i dati da uno Snapshot su un volume esistente o su un nuovo volume.

"Ripristinare un volume da uno Snapshot"

Elimina una snapshot

Elimina uno Snapshot per liberare spazio.

Le Snapshot immutabili non possono essere eliminate finché il periodo di conservazione non termina.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu  **Workloads > Volumes explorer**.
3. Seleziona il menu Azioni per il volume con lo snapshot da eliminare.
4. Seleziona **Azioni di protezione dei dati** e poi **Gestisci snapshot**.
5. Dalla pagina Gestisci snapshot, seleziona il menu delle azioni relativo allo snapshot da eliminare, quindi seleziona **Elimina**.
6. Nella finestra di dialogo Elimina snapshot, digita "delete".
7. Seleziona **Delete** per confermare l'eliminazione.

Informazioni correlate

- ["Crea uno snapshot"](#)
- ["Creare una policy di Snapshot"](#)
- ["Ripristinare un volume da uno Snapshot"](#)

Utilizza i backup per proteggere i dati in NetApp Workload Factory

Proteggi i dati dei tuoi volumi da cancellazioni accidentali, danneggiamenti e altri eventi di perdita di dati creando e ripristinando backup in NetApp Workload Factory. Puoi impostare una pianificazione dei backup, creare un backup su richiesta di un volume al di fuori dei backup programmati regolarmente e ripristinare un volume da un backup esistente su qualsiasi file system FSx for ONTAP nel tuo account AWS.

Crea un backup su richiesta di un volume

Crea un backup manuale di un volume al di fuori dei backup pianificati regolarmente in NetApp Workload Factory.

Informazioni su questa attività

I backup dei volumi vengono eseguiti per singolo volume, quindi ogni backup contiene solo i dati in un particolare volume.

I backup del volume sono incrementali, il che significa che vengono salvati solo i dati sul volume che sono stati modificati dopo il backup più recente. Questo riduce al minimo il tempo necessario per creare il backup e lo spazio di archiviazione richiesto per il backup, con conseguente risparmio sui costi di archiviazione grazie all'assenza di duplicazione dei dati.

Prima di iniziare

Per eseguire il backup dei volumi, sia il volume che il file system devono disporre di una capacità disponibile del tier di storage SSD sufficiente per memorizzare la Snapshot di backup. Quando esegui una Snapshot di backup, la capacità di storage aggiuntiva utilizzata dalla Snapshot non può far superare al volume il 98% di utilizzo dello storage SSD. Se succede, il backup non andrà a buon fine.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Volumes explorer**.
3. Seleziona il menu Azioni per il volume di cui eseguire il backup.
4. Seleziona **Data protection actions**, **Volume backups** e quindi **Manual backup**.
5. Nella finestra di dialogo di backup manuale, inserisci un nome per il backup.
6. Seleziona **Back up**.

Gestire la pianificazione dei backup per un file system FSx for ONTAP

Gestisci la pianificazione dei backup per un file system FSx for ONTAP in NetApp Workload Factory.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx for ONTAP**, seleziona il menu delle azioni del file system per cui vuoi aggiornare la pianificazione del backup, quindi seleziona **Manage**.
4. Nella sezione Informazioni, seleziona l'icona a forma di matita accanto a **Volume backups**. L'icona a forma di matita appare accanto alla freccia a discesa quando il puntatore del mouse si posiziona sulla riga **Volume backups**.
5. Nella finestra di dialogo **Volume backups**, fornire le seguenti informazioni:
 - a. **Backup automatici giornalieri**: Attiva o disattiva la funzione. Se disattivi la funzione, seleziona **Applica**. Se attivi la funzione, segui i passaggi successivi.
 - b. **Periodo di conservazione dei backup automatici**: Inserisci il numero di giorni per cui conservare i backup automatici.
 - c. **Finestra di backup automatico giornaliera**: Seleziona **Nessuna preferenza** (viene selezionato automaticamente per te un orario di inizio giornaliero del backup) oppure **Seleziona l'orario di inizio per i backup giornalieri** e specifica un orario di inizio.
 - d. **Finestra di manutenzione settimanale**: Seleziona **Nessuna preferenza** (verrà selezionato automaticamente un orario di inizio per la finestra di manutenzione settimanale) oppure **Seleziona l'orario di inizio per la finestra di manutenzione settimanale di 30 minuti** e specifica un orario di inizio.
6. Seleziona **Applica**.

Ripristinare un volume da un backup in NetApp Workload Factory

In NetApp Workload Factory, puoi ripristinare un volume da un backup in qualsiasi FSx for ONTAP file system nel tuo account AWS.

Workload Factory determina se hai abbastanza capacità per il ripristino e può aggiungere automaticamente

capacità al tier di storage SSD se non ne hai a sufficienza.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Volumes explorer**.
3. Seleziona il menu Azioni per il volume da ripristinare da un backup.
4. Seleziona **Data protection actions**, **Volume backups** e quindi **Restore from a backup**.
5. Nella finestra di dialogo Ripristina da un backup, inserisci quanto segue:
 - a. **File system di destinazione**: Seleziona il file system di destinazione dal menu a tendina.
 - b. **Storage VM di destinazione**: Seleziona la storage VM di destinazione dal menu a discesa.
 - c. **Nome del backup**: Seleziona il nome del backup dal menu a tendina.
 - d. **Nome del volume ripristinato**: Inserisci il nome del volume ripristinato.
6. Verifica la capacità del file system per l'operazione di ripristino.

Quando la capacità del file system è limitata, potrebbero verificarsi i seguenti problemi:

- Il ripristino può portare la capacità utilizzata oltre la soglia che hai specificato. Puoi completare l'operazione di ripristino. Considera ["aggiunta manuale della capacità del tier di storage SSD"](#) o seleziona per Workload Factory l'aggiunta automatica della capacità del tier di storage SSD.
- Il ripristino richiede capacità SSD aggiuntiva. Per procedere, devi selezionare l'opzione affinché Workload Factory aggiunga automaticamente capacità del tier di storage SSD.

7. Seleziona **Restore**.

Usa la replica per proteggere i dati

Replica i dati su FSx per ONTAP in NetApp Workload Factory

Replica i dati in NetApp Workload Factory per proteggerti dalla perdita di dati se la regione in cui risiedono i tuoi dati subisce un disastro. La replica dei dati è supportata tra i file system FSx for ONTAP e i sistemi ONTAP on-premises o Cloud Volumes ONTAP. Workload Factory supporta anche la replica a cascata per estendere la protezione dei dati ai sistemi terziari o per migrare i tuoi dati.

Quando si replicano i dati e le impostazioni di configurazione di una storage VM, è necessario prima creare e inizializzare la relazione di replica e quindi attendere che i dati vengano sincronizzati almeno una volta prima di completare l'operazione di cutover.

Replica standard

La replica protegge i tuoi dati se un disastro colpisce la tua regione; può anche essere utilizzata per scopi di migrazione.

La replica include la creazione e l'inizializzazione di una relazione di replica. Per configurare la replica, è necessario creare la relazione di replica. Per trasferire i dati tra i sistemi storage di origine e di destinazione, è necessario inizializzare la relazione di replica. Durante la migrazione dei dati e delle impostazioni di configurazione delle VM di storage, è inoltre necessario completare l'operazione di cutover.

I volumi replicati nel file system di destinazione sono volumi di protezione dati (DP) e seguono il formato di denominazione: {OriginalVolumeName}_copy.

Se si replica un volume sorgente con file immutabili, il volume di destinazione e il file system rimangono bloccati fino al termine del periodo di conservazione del volume sorgente. La funzionalità dei file immutabili è disponibile quando si ["creare un volume"](#) per un file system FSx for ONTAP.



È possibile replicare un volume sorgente (read/write) o un volume di protezione dati (DP). La replica a cascata è supportata, ma un terzo hop non lo è. Scopri di più su ["replicazione a cascata"](#).

Casi d'uso della migrazione

Per la migrazione, è possibile scegliere di replicare i dati e le impostazioni di configurazione di una singola storage VM. Se si migrano dati e impostazioni di configurazione insieme, assicurarsi che l'ultima replica del volume sia stata completata nelle ultime 24 ore. È necessario selezionare tutti i volumi nella stessa storage VM per utilizzare questa funzionalità. La policy di tiering per tutti i volumi viene impostata di default sulla policy di tiering del volume di origine, che è consigliata per i casi d'uso di migrazione.

Workload Factory supporta la replica della migrazione per le VM di storage tra i seguenti sistemi di storage.

- Sistemi ONTAP on-premises e file system FSx for ONTAP
- Cloud Volumes ONTAP e FSx per ONTAP file system
- FSx per ONTAP e FSx per ONTAP file system
 - Prima alla prima generazione
 - Seconda alla seconda generazione

Per migrare i dati e le impostazioni di configurazione delle storage VM, è necessario completare tre operazioni.

1. [Creare la relazione di replica](#), seleziona **Migration** come caso d'uso e seleziona **Replicate storage VM configuration**.
2. [Inizializza la relazione di replica](#) per trasferire i dati dal sistema di origine al sistema storage di destinazione.
3. [Cut over replication per casi d'uso di migrazione](#) per migrare in modo permanente dati e impostazioni di configurazione dal file system di origine al file system FSx for ONTAP di destinazione.

Passaggio 1: Creare la relazione di replica

Replica i dati tra due file system FSx for ONTAP, tra un sistema ONTAP on-premises e un file system FSx for ONTAP, oppure tra Cloud Volumes ONTAP e un file system FSx for ONTAP.

Prima di iniziare

Rivedi questi requisiti prima di iniziare.

- Assicurarsi che sia disponibile un file system FSx for ONTAP da utilizzare come destinazione nella relazione di replica.
- Aprire le porte TCP 11104 e 11105 per il trasferimento e la gestione sicura dei dati tra i sistemi di archiviazione. ICMP è facoltativo, ma può aiutare con i controlli di rete e la risoluzione dei problemi.
- Il file system FSx for ONTAP utilizzato per la relazione di replica deve avere un collegamento associato. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo

aver associato il link, torna a questa operazione.

- Per la replica da un sistema ONTAP on-premises a un file system FSx for ONTAP, assicurati di aver individuato il sistema ONTAP on-premises.
- La replica non è supportata per i volumi in uno stato diverso da disponibile, creato o configurato in modo errato e quando la versione di ONTAP non è compatibile.
- Per i casi d'uso di migrazione, assicurati che l'ultima replica per il volume sia stata completata nelle ultime 24 ore prima di creare una relazione di replica con dati e impostazioni di configurazione della storage VM.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Dalla pagina FSx for ONTAP, seleziona il file system che contiene i volumi da replicare.
4. Replica tutti i volumi di un file system oppure solo i volumi selezionati.
 - Per replicare tutti i volumi in un file system: dalla panoramica del file system, seleziona **Replicate data**.
 - Per replicare volumi selezionati: dalla panoramica del file system, seleziona la scheda **Volumi**.

Nella tabella Volumes, seleziona uno o più volumi, quindi seleziona **Replicate data**.

5. Nella pagina Replica dati, in Destinazione della replica, fornisci le seguenti informazioni:
 - a. **Caso d'uso:** Seleziona uno dei seguenti casi d'uso per la replica. A seconda del caso d'uso selezionato, Workload Factory compila il modulo con i valori consigliati in conformità con le best practice. Puoi accettare i valori consigliati o apportare modifiche durante la compilazione del modulo.
 - Intelligenza artificiale (AI) e machine learning (ML): replica i tuoi dati ONTAP on-premises su Amazon FSx for NetApp ONTAP e crea punti di accesso S3 per supportare l'addestramento di AI e ML nel cloud
 - Migrazione: trasferisce i tuoi dati al file system FSx for ONTAP di destinazione

Replica la configurazione della VM di archiviazione: Facoltativamente, seleziona per replicare i dati e le impostazioni di configurazione di una singola VM di archiviazione. Quando migri dati e impostazioni, tutti i volumi devono completare la replica nelle ultime 24 ore e poi effettuare il cutover contemporaneamente.

La policy di tiering per tutti i volumi viene impostata di default sulla policy di tiering del volume di origine, che è consigliata per i casi d'uso di migrazione.

Durante la migrazione, i client accedono ai dati dal file system ONTAP. Dopo il cutover, i volumi sono disponibili tramite gli indirizzi IP del file system FSx for ONTAP di destinazione. Aggiorna tutti i client o le risorse che utilizzano ancora il vecchio indirizzo IP.

- Disaster recovery a caldo: garantisce elevata disponibilità e un rapido disaster recovery per i carichi di lavoro critici
- Ripristino di emergenza a freddo o da archivio:
 - Disaster recovery a freddo: utilizza obiettivi di tempo di ripristino (RTO) e obiettivi del punto di ripristino (RPO) più lunghi per ridurre i costi
 - Archivio: replica i dati per storage a lungo termine e conformità
- Altro

Inoltre, la selezione del caso d'uso determina il criterio di replica, o il criterio SnapMirror (ONTAP). I termini utilizzati per descrivere i criteri di replica provengono da ["Documentazione ONTAP 9"](#).

- Per la migrazione e altre operazioni, la policy di replica si chiama *MirrorAllSnapshots*. *MirrorAllSnapshots* è una policy asincrona per il mirroring di tutte le Snapshot e del file system attivo più recente.
- Per il ripristino di emergenza a caldo, a freddo o tramite archivio, la policy di replica si chiama *MirrorAndVault*. *MirrorAndVault* è una policy asincrona e di vault per il mirroring del file system attivo più recente e degli snapshot giornalieri e settimanali.

Per tutti i casi d'uso, se abiliti i Snapshot per la conservazione a lungo termine, la policy di replica predefinita è *MirrorAndVault*.

- b. **FSx for ONTAP file system:** seleziona credenziali, regione e nome del FSx for ONTAP file system per il file system di destinazione FSx for ONTAP.
- c. **Nome della VM di archiviazione:** Seleziona la VM di archiviazione. La VM di archiviazione che selezioni è la destinazione per tutti i volumi selezionati in questa relazione di replica.

Quando i nomi delle storage VM di origine e di destinazione sono identici, creiamo un alias del file system per i nomi delle storage VM di destinazione per evitare conflitti di peering.

- d. **Nome del volume:** Il nome del volume di destinazione viene generato automaticamente con il seguente formato {OriginalVolumeName}_copy. Puoi usare il nome del volume generato automaticamente o inserire un altro nome per il volume.
- e. **Politica di tiering:** Seleziona la politica di tiering per i dati archiviati nel volume di destinazione. Per impostazione predefinita, la politica di tiering è quella consigliata per il caso d'uso che hai selezionato.

Bilanciato (Automatico) è il criterio di tiering predefinito quando crei un volume usando la console di Workload Factory. Per ulteriori informazioni sui criteri di tiering dei volumi, consulta ["Capacità di archiviazione del volume"](#) nella documentazione di AWS FSx for NetApp ONTAP. Nota che Workload Factory usa nomi basati sui casi d'uso nella console di Workload Factory per i criteri di tiering e include i nomi dei criteri di tiering di FSx for ONTAP tra parentesi.

Se hai selezionato il caso d'uso di migrazione, Workload Factory seleziona automaticamente l'opzione per copiare il criterio di tiering del volume di origine nel volume di destinazione. Puoi deselectare l'opzione per copiare il criterio di tiering e selezionare un criterio di tiering applicabile al volume selezionato per la replica.

- a. **Velocità di trasferimento massima:** seleziona **Limitata** e inserisci il limite massimo di trasferimento in MB/s. In alternativa, seleziona **Illimitata**.

Senza un limite, le prestazioni della rete e delle applicazioni potrebbero diminuire. In alternativa, consigliamo una velocità di trasferimento illimitata per i file system FSx for ONTAP per i carichi di lavoro critici, ad esempio quelli utilizzati principalmente per il disaster recovery.

6. Nella sezione Impostazioni di replica, inserisci le seguenti informazioni:

- a. **Inizializza la relazione di replica:** scegli se inizializzare la relazione di replica immediatamente dopo averla creata o in un secondo momento. Tieni presente che l'inizializzazione può richiedere tempo e potresti voler eseguire il trasferimento baseline durante le ore di minore affluenza.

Per inizializzare in seguito manualmente, fai riferimento alle istruzioni in [Passaggio 2: Inizializzare la relazione di replica](#).

- b. **Intervallo di replica:** Seleziona la frequenza con cui le Snapshot vengono trasferite dal volume di origine al volume di destinazione.
- c. **Conservazione a lungo termine:** Facoltativamente, abilita gli Snapshot per la conservazione a lungo termine. La conservazione a lungo termine consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover trasparente delle applicazioni tramite una copia secondaria.

Le repliche senza conservazione a lungo termine utilizzano la policy *MirrorAllSnapshots*. L'abilitazione della conservazione a lungo termine assegna alla replica la policy *MirrorAndVault*.

Se abiliti la conservazione a lungo termine, seleziona un criterio esistente o creane uno nuovo per definire gli Snapshot da replicare e il numero da conservare.



Per la conservazione a lungo termine sono necessarie etichette corrispondenti tra origine e destinazione. Se vuoi, Workload Factory può creare per te le etichette mancanti.

- **Scegli una policy esistente:** seleziona una policy esistente.
 - **Crea una nuova policy:** inserisci un **nome della policy**.
- d. **Snapshot immutabili:** Opzionale. Seleziona **Abilita snapshot immutabili** per impedire che gli snapshot creati in base a questa policy vengano eliminati durante il periodo di conservazione.
- Imposta il **periodo di conservazione** nel numero di ore, giorni, mesi o anni.
 - **Criteri Snapshot:** Nella tabella, seleziona la frequenza del criterio Snapshot e il numero di copie da conservare. Puoi selezionare più di un criterio Snapshot.
- e. **Punto di accesso S3:** facoltativamente, collega un punto di accesso S3 per accedere ai dati del file system FSx for ONTAP residenti su volumi NFS o SMB/CIFS tramite le API AWS S3. È supportato solo il tipo di accesso ai file. Fornire i seguenti dettagli:
- **Nome punto di accesso S3:** Inserisci il nome del punto di accesso S3.
 - **Utente:** Seleziona un utente esistente con accesso al volume o crea un nuovo utente.
 - **Tipo di utente:** seleziona **UNIX** o **Windows** come tipo di utente.
 - **Configurazione di rete:** Selezionare **Internet** o **Virtual private cloud (VPC)**. Il tipo di rete scelto determina se il punto di accesso è accessibile da Internet o limitato a una specifica VPC.
 - **Abilita tabella inventario:** quando si abilita la tabella inventario sul volume, il sistema genera metadati per tutti gli oggetti accessibili al punto di accesso S3 e comporta costi di richiesta AWS S3. Per ulteriori informazioni, consulta "[Documentazione sui prezzi di Amazon S3](#)".
- f. **Tag del punto di accesso S3:** Facoltativamente, puoi aggiungere fino a 50 tag.

7. Seleziona **Crea**.

Risultato

La relazione di replica appare nella scheda **Relazioni di replica** nel file system FSx for ONTAP di destinazione.

Se hai creato una relazione di replica per scopi di migrazione, devi eseguire il cutover di tutti i volumi e della relativa storage VM associata per completare la migrazione dei dati e delle impostazioni di configurazione della storage VM nel file system FSx for ONTAP di destinazione.

Passaggio 2: Inizializzare la relazione di replica

Inizializza una relazione di replica tra i volumi di origine e di destinazione per trasferire lo snapshot e tutti i blocchi di dati in NetApp Workload Factory.

L'inizializzazione esegue un trasferimento baseline: crea un'istantanea del volume di origine, quindi trasferisce l'istantanea e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.

Prima di iniziare

Valuta attentamente il momento migliore per completare questa operazione. L'inizializzazione può richiedere molto tempo. Potresti preferire eseguire il trasferimento baseline nelle ore di minor traffico.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx per ONTAP**, selezionare il menu delle azioni del file system da aggiornare e quindi selezionare **Gestisci**.
4. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
5. Nella scheda Relazioni di replica, selezionare il menu Azioni della relazione di replica da inizializzare.
6. Seleziona **Inizializza**.
7. Nella finestra di dialogo Inizializza relazione, selezionare **Inizializza**.

Quando lo stato della replica mostra **Idle**, il trasferimento dei dati è completato.

Fase 3: Cutover della replica per i casi d'uso di migrazione

Dopo aver creato la relazione di replica per un caso d'uso di migrazione, è necessario eseguire il cutover della replica per completare la migrazione dei dati e delle impostazioni di configurazione della storage VM al file system FSx for ONTAP di destinazione. Il cutover della replica migra in modo permanente i dati e le impostazioni di configurazione della storage VM dal file system di origine al file system FSx for ONTAP di destinazione. Durante il cutover, i dati vengono replicati per l'ultima volta. La storage VM di origine va offline quando inizia il cutover.

Pianifica l'operazione di cutover

Considerare quanto segue quando si pianifica l'operazione di cutover per i casi d'uso di migrazione.

- **Supporto della versione di replica:** i sistemi storage di origine e di destinazione devono avere la stessa versione principale di ONTAP. Ad esempio, se il sistema di origine esegue la versione di ONTAP 9.18.1, anche il sistema di destinazione deve eseguire una versione di 9.18.1.
- **Impostazioni di configurazione della VM di archiviazione:**
 - L'operazione di cutover non migra tutte le impostazioni di configurazione della VM di storage alla VM di storage di destinazione. Ad esempio, le impostazioni iSCSI, MTU del dominio broadcast e DNS non vengono migrate. Aggiorna queste impostazioni manualmente sulla VM di storage di destinazione dopo il cutover. Per ulteriori dettagli, fare riferimento alla sezione [Aggiornare le impostazioni di configurazione dopo cutover](#).
 - Se la VM di archiviazione utilizza l'autenticazione tramite tunnel di dominio, configura e abilita un tunnel di dominio sul file system prima di avviare la migrazione.
- **Cloni:** I cloni vengono migrati come volumi individuali e, pertanto, occuperanno più spazio sul file system

FSx for ONTAP di destinazione. Si consiglia di eliminare i cloni prima del cutover per evitare un aumento della capacità sul sistema di destinazione.

- **Volumi cache:** Per ONTAP FlexCache 9.17.x o versioni precedenti. Le VM di storage di origine che contengono volumi cache non sono supportate per cutover. Rimuovere la relazione ONTAP FlexCache prima del cutover per evitare errori di migrazione.
- **Punti di accesso AWS S3:** la replica di cutover per i casi d'uso di migrazione non è supportata per i volumi con punti di accesso S3. Eliminare i punti di accesso S3 dal volume di origine per evitare errori di migrazione.
- **ONTAP S3 configurations:** La replica di cutover per i casi d'uso di migrazione non è supportata per i vserver con configurazioni ONTAP S3. Rimuovere le configurazioni ONTAP S3, inclusi object-store-server, bucket, utenti, gruppi o policy sul vserver, per evitare errori di migrazione.
- **Numeri di serie LUN e iSCSI target IQN:** I numeri di serie LUN e l'iSCSI target IQN cambiano durante cutover.

Prima di iniziare

Rivedi questi requisiti prima di iniziare.

- Interrompere l'accesso dei client alla storage VM prima di eseguire il cutover della replica.
- Assicurarsi che tutti i volumi di origine non stiano servendo alcun dato prima di eseguire il cutover della replica.
- Assicurarsi che i dati siano sincronizzati tra i volumi di origine e di destinazione prima di eseguire il cutover della replica.
- Il file system FSx for ONTAP utilizzato per la relazione di replica deve avere un collegamento associato. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il link, torna a questa operazione.
 - Nel gruppo di sicurezza associato al file system FSx for ONTAP, per la connettività del collegamento, devono essere aperte le seguenti porte: porta 443 (HTTPS) e porta 22 (SSH).

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx for ONTAP**, seleziona il file system che contiene il volume o i volumi da replicare.
4. Seleziona la scheda **Replication relationships**.
5. Nella tabella Relazioni di replicazione, seleziona la relazione di replicazione su cui eseguire il cutover, quindi seleziona **Cut over replication**.
6. Rivedere le informazioni nella finestra di dialogo Cut over replication e quindi digitare *cut over* per confermare.
7. Seleziona **cutover**.

Risultato

Dopo aver avviato cutover, la macchina virtuale di archiviazione di origine va offline.

Aggiornare le impostazioni di configurazione dopo cutover

Dopo aver eseguito il cutover della replica per i casi d'uso di migrazione, aggiornare le seguenti impostazioni di configurazione della storage VM sulla storage VM di destinazione.

- Per iSCSI:
 - Ricrea l'igroup
 - Aggiorna la mappatura LUN
 - Accedere a ciascun client SAN e aggiornare le impostazioni iSCSI/MPIO per il nuovo target e rimuovere i vecchi indirizzi IP del target vserver
- Verificare che le impostazioni MTU del dominio broadcast siano conformi alle aspettative
- Verificare che le impostazioni DNS siano conformi alle aspettative
- Ricrea le relazioni della cache (relazioni ONTAP FlexCache) se erano presenti volumi di cache nella VM di archiviazione di origine.

Se necessario, ["modificare la tiering policy"](#) per il/i volume/i di destinazione dopo cutover.

Replica a cascata per volumi di protezione dati

NetApp Workload Factory supporta la replica dei volumi di protezione dei dati, chiamati anche *deployment a cascata*. Un *deployment a cascata* consiste in una catena di relazioni in cui un volume di origine viene replicato su un volume secondario (primo passaggio) e il volume secondario viene replicato su un volume terziario (secondo passaggio). Se il volume secondario non è disponibile, puoi sincronizzare la relazione tra i volumi primario e terziario senza eseguire un nuovo trasferimento baseline.

Questa funzionalità è supportata per i file system FSx for ONTAP con versione di ONTAP 9.6 e successive. Fai riferimento a ["Documentazione ONTAP per le versioni di ONTAP compatibili"](#).

Scopri di più su ["come funzionano le implementazioni a cascata"](#).

Prima di iniziare

Prima di iniziare, tieni presente quanto segue:

- Tieni presente che i volumi che fanno parte di una configurazione a cascata potrebbero impiegare più tempo per risincronizzarsi.
- Se il volume di origine della relazione è un volume di protezione dei dati ed è la destinazione di un'altra relazione, l'inversione della relazione di replica non è supportata.
- È supportata una sola replica di un volume di protezione dei dati (o un secondo hop). Non è considerata best practice creare una seconda replica di un volume di protezione dei dati (o un terzo hop).
- Aprire le porte TCP 11104 e 11105 per il trasferimento e la gestione sicura dei dati tra i sistemi di archiviazione. ICMP è facoltativo, ma può aiutare con i controlli di rete e la risoluzione dei problemi.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx for ONTAP**, seleziona il menu Azioni del file system che contiene i volumi da replicare, quindi seleziona **Gestisci**.
4. Dalla panoramica del file system, seleziona la scheda **Volumi**.
5. Nella tabella Volumi, seleziona uno o più volumi di protezione dei dati (volumi DP/replicati), quindi seleziona **Replica dati**.
6. Nella pagina Replica dati, in Destinazione della replica, fornisci le seguenti informazioni:

a. **Caso d'uso:** Seleziona uno dei seguenti casi d'uso per la replica. A seconda del caso d'uso selezionato, Workload Factory compila il modulo con i valori consigliati in conformità con le best practice. Puoi accettare i valori consigliati o apportare modifiche durante la compilazione del modulo.

- **Intelligenza artificiale (AI) e machine learning (ML):** replica i tuoi dati ONTAP on-premises su Amazon FSx for NetApp ONTAP e crea punti di accesso S3 per supportare l'addestramento di AI e ML nel cloud
- **Migrazione:** trasferisce i tuoi dati al file system FSx for ONTAP di destinazione

Replica la configurazione della VM di archiviazione: Facoltativamente, seleziona per replicare i dati e le impostazioni di configurazione di una singola VM di archiviazione. Quando migri dati e impostazioni, tutti i volumi devono completare la replica nelle ultime 24 ore e poi effettuare il cutover contemporaneamente.

La policy di tiering per tutti i volumi viene impostata di default sulla policy di tiering del volume di origine, che è consigliata per i casi d'uso di migrazione.

Durante la migrazione, i client accedono ai dati dal file system ONTAP. Dopo il cutover, i volumi sono disponibili tramite gli indirizzi IP del file system FSx for ONTAP di destinazione. Aggiorna tutti i client o le risorse che utilizzano ancora il vecchio indirizzo IP.

- **Disaster recovery a caldo:** garantisce elevata disponibilità e un rapido disaster recovery per i carichi di lavoro critici
- **Ripristino di emergenza a freddo o da archivio:**
 - **Disaster recovery a freddo:** utilizza obiettivi di tempo di ripristino (RTO) e obiettivi del punto di ripristino (RPO) più lunghi per ridurre i costi
 - **Archivio:** replica i dati per storage a lungo termine e conformità
- **Altro**

Inoltre, la selezione del caso d'uso determina il criterio di replica, o il criterio SnapMirror (ONTAP). I termini utilizzati per descrivere i criteri di replica provengono da "[Documentazione ONTAP 9](#)".

- Per la migrazione e altre operazioni, la policy di replica si chiama *MirrorAllSnapshots*. *MirrorAllSnapshots* è una policy asincrona per il mirroring di tutte le Snapshot e del file system attivo più recente.
- Per il ripristino di emergenza a caldo, a freddo o tramite archivio, la policy di replica si chiama *MirrorAndVault*. *MirrorAndVault* è una policy asincrona e di vault per il mirroring del file system attivo più recente e degli snapshot giornalieri e settimanali.

Per tutti i casi d'uso, se abiliti i Snapshot per la conservazione a lungo termine, la policy di replica predefinita è *MirrorAndVault*.

b. **FSx for ONTAP file system:** seleziona credenziali, regione e nome del FSx for ONTAP file system per il file system di destinazione FSx for ONTAP.

c. **Nome della VM di archiviazione:** Seleziona la VM di archiviazione. La VM di archiviazione che selezioni è la destinazione per tutti i volumi selezionati in questa relazione di replica.

Quando i nomi delle storage VM di origine e di destinazione sono identici, creiamo un alias del file system per i nomi delle storage VM di destinazione per evitare conflitti di peering.

d. **Nome del volume:** Il nome del volume di destinazione viene generato automaticamente con il seguente formato {OriginalVolumeName}_copy. Puoi usare il nome del volume generato

automaticamente o inserire un altro nome per il volume.

- e. **Politica di tiering:** Seleziona la politica di tiering per i dati archiviati nel volume di destinazione. Per impostazione predefinita, la politica di tiering è quella consigliata per il caso d'uso che hai selezionato.

Bilanciato (Automatico) è il criterio di tiering predefinito quando crei un volume usando la console di Workload Factory. Per ulteriori informazioni sui criteri di tiering dei volumi, consulta ["Capacità di archiviazione del volume"](#) nella documentazione di AWS FSx for NetApp ONTAP. Nota che Workload Factory usa nomi basati sui casi d'uso nella console di Workload Factory per i criteri di tiering e include i nomi dei criteri di tiering di FSx for ONTAP tra parentesi.

Se hai selezionato il caso d'uso di migrazione, Workload Factory seleziona automaticamente l'opzione per copiare il criterio di tiering del volume di origine nel volume di destinazione. Puoi deselectare l'opzione per copiare il criterio di tiering e selezionare un criterio di tiering applicabile al volume selezionato per la replica.

- a. **Velocità di trasferimento massima:** seleziona **Limitata** e inserisci il limite massimo di trasferimento in MB/s. In alternativa, seleziona **Illimitata**.

Senza un limite, le prestazioni della rete e delle applicazioni potrebbero diminuire. In alternativa, consigliamo una velocità di trasferimento illimitata per i file system FSx for ONTAP per i carichi di lavoro critici, ad esempio quelli utilizzati principalmente per il disaster recovery.

7. Nella sezione Impostazioni di replica, inserisci le seguenti informazioni:

- a. **Inizializza la relazione di replica:** scegli se inizializzare la relazione di replica immediatamente dopo averla creata o in un secondo momento. Tieni presente che l'inizializzazione può richiedere tempo e potresti voler eseguire il trasferimento baseline durante le ore di minore affluenza.

Per inizializzare in seguito manualmente, fai riferimento alle istruzioni in [Passaggio 2: Inizializzare la relazione di replica](#).

- b. **Intervallo di replica:** Seleziona la frequenza con cui le Snapshot vengono trasferite dal volume di origine al volume di destinazione.
- c. **Conservazione a lungo termine:** Facoltativamente, abilita gli Snapshot per la conservazione a lungo termine. La conservazione a lungo termine consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover trasparente delle applicazioni tramite una copia secondaria.

Le repliche senza conservazione a lungo termine utilizzano la policy *MirrorAllSnapshots*. L'abilitazione della conservazione a lungo termine assegna alla replica la policy *MirrorAndVault*.

Se abiliti la conservazione a lungo termine, seleziona un criterio esistente o creane uno nuovo per definire gli Snapshot da replicare e il numero da conservare.



Per la conservazione a lungo termine sono necessarie etichette corrispondenti tra origine e destinazione. Se vuoi, Workload Factory può creare per te le etichette mancanti.

- **Scegli una policy esistente:** seleziona una policy esistente.
 - **Crea una nuova policy:** inserisci un **nome della policy**.
- d. **Snapshot immutabili:** Opzionale. Seleziona **Abilita snapshot immutabili** per impedire che gli snapshot creati in base a questa policy vengano eliminati durante il periodo di conservazione.

- Imposta il **periodo di conservazione** nel numero di ore, giorni, mesi o anni.
 - **Criteri Snapshot:** Nella tabella, seleziona la frequenza del criterio Snapshot e il numero di copie da conservare. Puoi selezionare più di un criterio Snapshot.
- e. **Punto di accesso S3:** facoltativamente, collega un punto di accesso S3 per accedere ai dati del file system FSx for ONTAP residenti su volumi NFS o SMB/CIFS tramite le API AWS S3. È supportato solo il tipo di accesso ai file. Fornire i seguenti dettagli:
- **Nome punto di accesso S3:** Inserisci il nome del punto di accesso S3.
 - **Utente:** Seleziona un utente esistente con accesso al volume o crea un nuovo utente.
 - **Tipo di utente:** seleziona **UNIX** o **Windows** come tipo di utente.
 - **Configurazione di rete:** Selezionare **Internet** o **Virtual private cloud (VPC)**. Il tipo di rete scelto determina se il punto di accesso è accessibile da Internet o limitato a una specifica VPC.
 - **Abilita tabella inventario:** quando si abilita la tabella inventario sul volume, il sistema genera metadati per tutti gli oggetti accessibili al punto di accesso S3 e comporta costi di richiesta AWS S3. Per ulteriori informazioni, consulta ["Documentazione sui prezzi di Amazon S3"](#).
- f. **Tag del punto di accesso S3:** Facoltativamente, puoi aggiungere fino a 50 tag.

8. Seleziona **Crea**.

Risultato

Il volume o i volumi replicati vengono replicati e vengono visualizzati nella scheda **Relazioni di replica** del file system FSx for ONTAP di destinazione.

Informazioni correlate

["Modificare la policy di tiering"](#) per il/i volume di destinazione dopo cutover.

Replica i dati del cluster ONTAP on-premises in NetApp Workload Factory

Individua e replica i dati ONTAP locali in NetApp Workload Factory così puoi usarli come backup nel cloud.

Informazioni su questa attività

Per utilizzare i dati di un cluster ONTAP on-premises, devi innanzitutto individuare il cluster ONTAP on-premises. Dopo aver individuato un cluster ONTAP on-premises, puoi utilizzare i dati per uno dei seguenti casi d'uso.

Casi d'uso

- **Backup e migrazione al cloud:** i dati di un volume ONTAP on-premises replicati in un FSx for ONTAP file system possono essere usati come backup nel cloud.
- **Tiering dei dati:** Dopo la replica, i dati dei volumi ONTAP on-premises a cui accedi raramente possono essere spostati dal tier di storage SSD al tier di storage capacity pool.

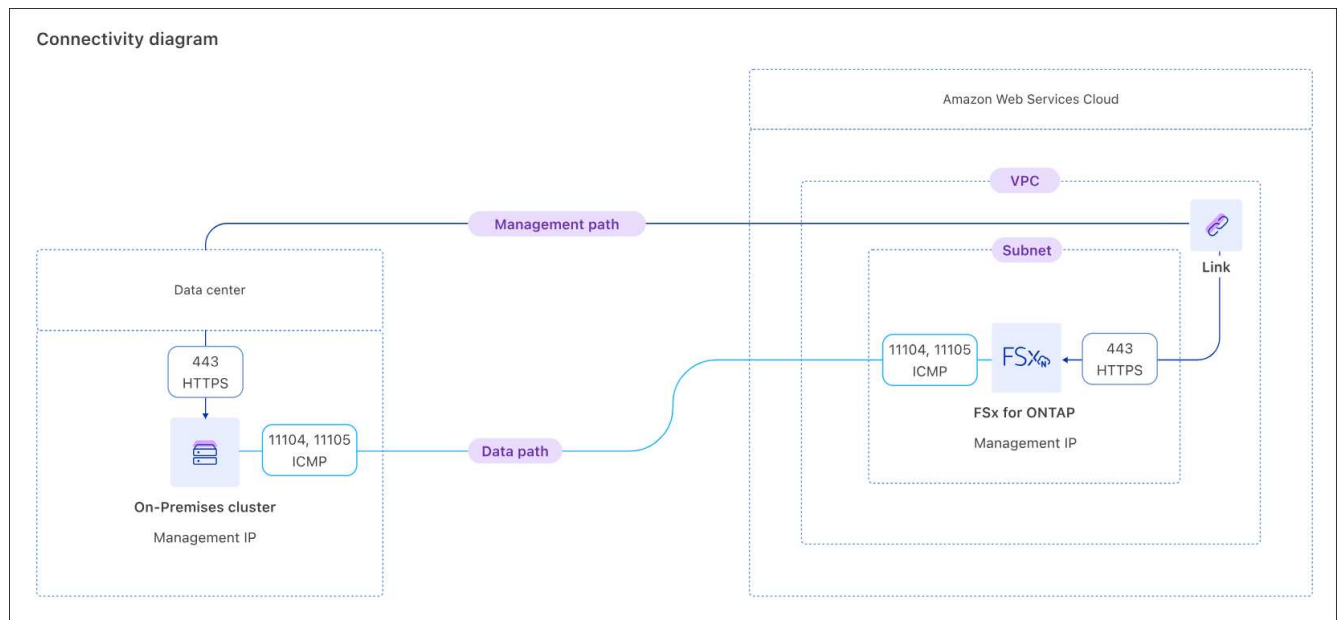
Scopri un cluster ONTAP on-premises

Individua un cluster ONTAP on-premises in NetApp Workload Factory così puoi replicare i dati in un file system Amazon FSx for NetApp ONTAP.

Prima di iniziare

Assicurati di avere a disposizione quanto segue prima di iniziare:

- Un file system FSx for ONTAP per la replica.
- Un collegamento connesso da associare al cluster on-premises rilevato. Se non hai un collegamento, dovrai ["creare uno"](#).
- Credenziali utente ONTAP con le autorizzazioni richieste.
- Versione di ONTAP on-premises 9.8 e successive.
- Connettività come mostrato nel diagramma seguente.



Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu  **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Dal menu **FSx for ONTAP**, seleziona **On-premises ONTAP**.
4. Seleziona **Discover**.
5. Esamina i prerequisiti e seleziona **Avanti**.
6. Nella pagina Discover ONTAP on-premises, inserisci quanto segue in **Configurazione cluster**:
 - a. **Collegamento**: Seleziona un collegamento. Il collegamento verrà associato al cluster on-premises per creare la connettività tra il cluster e Workload Factory.

Se non hai ancora creato un collegamento, segui le istruzioni e poi torna a questa operazione e seleziona il collegamento.

 - b. **Indirizzo IP del cluster**: Fornisci l'indirizzo IP del cluster ONTAP on-premises da replicare.
 - c. **Credenziali ONTAP**: Fornisci quanto segue:
 - GovCloud account: Inserisci l'ARN con le credenziali ONTAP.
 - Tutti gli altri account: Inserisci le credenziali ONTAP per il cluster ONTAP on-premises. Assicurati che l'utente abbia le autorizzazioni necessarie.
7. Seleziona **Discover** per avviare il processo di individuazione.

Risultato

Il cluster ONTAP on-premises è stato rilevato e ora viene visualizzato nella scheda **On-Premises ONTAP**.

Ora puoi visualizzare i dati nel tuo cluster ONTAP on-premise e [replicare i dati in un file system FSx for ONTAP](#).

Replica i dati del volume da un cluster ONTAP on-premises

Replica i dati dei volumi da un cluster ONTAP on-premises a un file system FSx for ONTAP. Dopo la replica, i dati possono essere utilizzati per arricchire le basi di conoscenza dell'IA.

Prima di iniziare

- Devi rilevare un cluster ONTAP on-premises per replicarne i dati del volume.
- Devi disporre di un file system FSx for ONTAP disponibile che funga da destinazione per la replica.
- Sia il cluster ONTAP on-premises che il file system FSx for ONTAP che usi per la relazione di replica devono avere un collegamento associato. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il collegamento, torna a questa procedura.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Dal menu **FSx for ONTAP**, seleziona **On-premises ONTAP**.
4. Per trovare i volumi in base alla VM di storage, puoi **selezionare la VM di storage** dal menu a discesa.
5. Seleziona uno o più volumi da replicare e poi seleziona **Replica**.
6. Nella pagina Crea replica, in Destinazione replica, inserisci quanto segue:
 - a. **FSx for ONTAP file system**: seleziona credenziali, regione e nome del FSx for ONTAP file system per il file system di destinazione FSx for ONTAP.
 - b. **Nome della VM di storage**: seleziona la VM di storage dal menu a discesa.
 - c. **Nome del volume**: Il nome del volume di destinazione viene generato automaticamente con il seguente formato {OriginalVolumeName}_copy. Puoi usare il nome del volume generato automaticamente o inserire un altro nome per il volume.
 - d. **Tiering dei dati**: Seleziona la policy di tiering per i dati archiviati nel volume di destinazione.
 - **Auto**: il criterio di tiering predefinito quando crei un volume utilizzando l'interfaccia utente di Workload Factory FSx for ONTAP. Esegue il tiering di tutti i dati cold, inclusi i dati utente e gli Snapshot, nel tier di storage capacity pool per un periodo di tempo specifico.
 - **Solo Snapshot**: i tier eseguono il tiering solo dei dati Snapshot nel tier di storage del capacity pool.
 - **Nessuno**: Mantiene tutti i dati del volume sul tier di storage primario.
 - **Tutti**: contrassegna tutti i dati utente e i dati Snapshot come freddi e li memorizza nel tier di storage del pool di capacità.

Tieni presente che alcune policy di tiering prevedono un periodo di raffreddamento minimo associato che definisce il tempo, o *giorni di raffreddamento*, durante il quale i dati utente in un volume devono rimanere inattivi perché i dati siano considerati "freddi" e spostati nel tier di storage del capacity pool. Il periodo di raffreddamento inizia quando i dati vengono scritti sul disco.

Per ulteriori informazioni sulle policy di tiering dei volumi, consulta ["Capacità di archiviazione del volume"](#) la documentazione di AWS FSx for NetApp ONTAP.

- a. **Velocità di trasferimento:** seleziona **Limitata** e inserisci il limite massimo di trasferimento in MiB/s. In alternativa, seleziona **Illimitata**.

Senza un limite, le prestazioni della rete e delle applicazioni potrebbero diminuire. In alternativa, per i file system FSx for ONTAP per carichi di lavoro critici, ad esempio quelli utilizzati principalmente per il disaster recovery, consigliamo una velocità di trasferimento illimitata.

7. Nella sezione Impostazioni di replica, inserisci le seguenti informazioni:

- a. **Intervallo di replica:** Seleziona la frequenza con cui le Snapshot vengono trasferite dal volume di origine al volume di destinazione.
- b. **Conservazione a lungo termine:** Facoltativamente, abilita gli snapshot per la conservazione a lungo termine.

Se abiliti la conservazione a lungo termine, seleziona un criterio esistente o creane uno nuovo per definire gli Snapshot da replicare e il numero da conservare.

- Per un criterio esistente, seleziona **Scegli un criterio esistente** e poi seleziona il criterio esistente dal menu a discesa.
- Per una nuova policy, seleziona **Crea una nuova policy** e fornisci quanto segue:
 - **Nome della policy:** Inserisci un nome per la policy.
 - **Criteri Snapshot:** Nella tabella, seleziona la frequenza del criterio Snapshot e il numero di copie da conservare. Puoi selezionare più di un criterio Snapshot.

8. Seleziona **Crea**.

Risultato

La relazione di replica appare nella scheda **Relazioni di replica** nel file system FSx for ONTAP di destinazione.

Rimuovi un cluster ONTAP da NetApp Workload Factory

Rimuovi un cluster ONTAP on-premises da NetApp Workload Factory quando necessario.

Prima di iniziare

Devi ["eliminare tutte le relazioni di replica esistenti"](#) per tutti i volumi nel cluster ONTAP on-premises prima di rimuovere il cluster, in modo che non rimangano relazioni interrotte.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Dal menu **FSx for ONTAP**, seleziona **On-premises ONTAP**.
4. Seleziona il cluster ONTAP on-premises da rimuovere.
5. Seleziona il menu Azioni e seleziona **Rimuovi da Workload Factory**.

Risultato

Il cluster ONTAP viene rimosso da NetApp Workload Factory.

Replica una VM di storage in un altro file system FSx for ONTAP

La replica di una VM di storage in un altro FSx for ONTAP file system in NetApp Workload Factory fornisce un livello di protezione per l'accesso ai dati in caso di perdita di dati. Questa operazione replica tutti i volumi di una VM di storage in un altro FSx for ONTAP file system.

Prima di iniziare

Per replicare una storage VM su un altro file system FSx for ONTAP, devi associare un collegamento. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il collegamento, torna a questa procedura.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx for ONTAP**, seleziona il menu Azioni del file system con la VM di storage da replicare e quindi seleziona **Manage**.
4. Nella panoramica del file system, in Storage VMs, seleziona **Manage**.
5. Nella schermata Gestisci VM di storage, seleziona il menu delle azioni della VM di storage per la quale desideri replicare una SVM, quindi seleziona **Azioni avanzate > Replica VM di storage**.
6. Nella pagina Replica dati, in Destinazione della replica, fornisci le seguenti informazioni:
 - a. **FSx for ONTAP file system**: seleziona credenziali, regione e nome del FSx for ONTAP file system per il file system di destinazione FSx for ONTAP.
 - b. **Nome della VM di storage**: seleziona la VM di storage dal menu a discesa.
 - c. **Nome del volume**: Il nome del volume di destinazione viene generato automaticamente con il seguente formato {OriginalVolumeName}_copy.
 - d. **Politica di tiering**: Seleziona la politica di tiering per i dati archiviati nel volume di destinazione.

Auto è la policy di tiering predefinita quando crei un volume utilizzando l'interfaccia utente di Workload Factory FSx for ONTAP. Per ulteriori informazioni sulle policy di tiering dei volumi, consulta ["Capacità di archiviazione del volume"](#) la documentazione di AWS FSx for NetApp ONTAP.
 - e. **Velocità di trasferimento massima**: seleziona **Limitata** e inserisci il limite massimo di trasferimento in MB/s. In alternativa, seleziona **Illimitata**.

Senza un limite, le prestazioni della rete e delle applicazioni potrebbero diminuire. In alternativa, per i file system FSx for ONTAP per carichi di lavoro critici, ad esempio quelli utilizzati principalmente per il disaster recovery, consigliamo una velocità di trasferimento illimitata.
7. Nella sezione Impostazioni di replica, inserisci le seguenti informazioni:
 - a. **Intervallo di replica**: Seleziona la frequenza con cui le Snapshot vengono trasferite dal volume di origine al volume di destinazione.
 - b. **Conservazione a lungo termine**: Facoltativamente, abilita gli snapshot per la conservazione a lungo termine.

Se abiliti la conservazione a lungo termine, seleziona un criterio esistente o creane uno nuovo per definire gli Snapshot da replicare e il numero da conservare.

- i. Per **Scegli una policy esistente**, seleziona una policy esistente dal menu a discesa.
 - ii. Per **Creare una nuova policy**, inserisci quanto segue:
 - A. **Nome della policy**: Inserisci un nome per la policy.
 - B. **Criteri Snapshot**: Nella tabella, seleziona la frequenza del criterio Snapshot e il numero di copie da conservare. Puoi selezionare più di un criterio Snapshot.
8. Seleziona **Crea**.

Risultato

Tutti i volumi all'interno della macchina virtuale di archiviazione vengono replicati nel file system di destinazione.

Monitora i ritardi di replica in NetApp Workload Factory

Attiva il monitoraggio per tenere sotto controllo i ritardi di replica nel tuo account. Workload Factory ti avvisa quando i ritardi superano una determinata soglia. Per impostazione predefinita, la soglia è pari al 150% dell'intervallo di replica per consentire tempi di trasferimento normali e ridurre i falsi allarmi. Puoi regolare la soglia in base al tuo RPO e ricevere notifiche quando i ritardi la superano. Puoi anche esportare i dati in un file CSV per ulteriori analisi.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Da **FSx per ONTAP**, selezionare il menu delle azioni del file system da aggiornare e quindi selezionare **Gestisci**.
4. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
5. Seleziona **Abilita il tracking**.
6. Nella finestra di dialogo Abilita cronologia ritardo replica, seleziona **Abilita**.
7. Tornando al riquadro Cronologia ritardo replica, seleziona **Personalizza soglia** per impostare la soglia che preferisci.
8. Nella finestra di dialogo Personalizza la soglia del tempo di ritardo, inserisci la soglia in ore e minuti.
9. Facoltativamente, seleziona **Abilita notifiche di ritardo** per ricevere notifiche quando la replica supera la soglia di ritardo.

Le notifiche arrivano tramite email e includono:

- File system di origine
- Volume sorgente
- File system di destinazione
- Volume di destinazione
- Soglia del tempo di ritardo superata
- Collegamento alla relazione di replica

10. Seleziona **Applica**.

Informazioni correlate

["Gestisci le relazioni di replica"](#)

Gestisci le relazioni di replica in NetApp Workload Factory

Gestisci le tue relazioni di replica in NetApp Workload Factory. Puoi sospendere, riprendere, invertire, arrestare ed eliminare le relazioni di replica tra volumi di origine e di destinazione. Puoi anche modificare la pianificazione della replica del volume di origine e limitare la velocità di trasferimento per le tue relazioni di replica.

Modifica la pianificazione della replica di un volume di origine

Modifica la pianificazione della replica del volume di origine in una relazione di replica in NetApp Workload Factory.

Scegli con quale frequenza le Snapshot dal volume di origine vengono trasferite al volume replicato in base agli obiettivi del punto di ripristino (RPO) richiesti.

Quando un cluster ONTAP on-premises è il target della relazione di replica, non puoi modificare la pianificazione della replica.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. In **Inventory**, seleziona il menu delle azioni del file system da aggiornare e quindi seleziona **Manage**.
5. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
6. Nella scheda Relazioni di replica, seleziona il menu Azioni della pianificazione della relazione di replica da modificare.
7. Seleziona **Modifica intervallo di replica**.
8. Nella finestra di dialogo Modifica intervallo di replica, seleziona la frequenza di trasferimento degli Snapshot dal volume di origine. Puoi scegliere tra le seguenti frequenze:
 - Ogni 5 minuti
 - Ogni ora
 - Ogni 8 ore
 - Quotidiano
 - Settimanale
9. Seleziona **Applica**.

Limita la velocità di trasferimento massima di una relazione di replica

Limitare la velocità di trasferimento massima è facoltativo, ma consigliato. Senza un limite, le prestazioni della rete e delle applicazioni potrebbero diminuire.

In alternativa, consigliamo una velocità di trasferimento illimitata per i file system FSx for ONTAP per i carichi di lavoro critici, ad esempio quelli utilizzati principalmente per il disaster recovery.

Prima di iniziare

Valuta quanta larghezza di banda allocare per la replica.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. In **Inventory**, seleziona il menu delle azioni del file system da aggiornare e quindi seleziona **Manage**.
5. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
6. Nella scheda Relazioni di replica, seleziona il menu Azioni della relazione di replica per cui vuoi limitare la velocità di trasferimento massima.
7. Seleziona **Modifica velocità di trasferimento massima**.
8. Nella finestra di dialogo Modifica velocità di trasferimento massima, seleziona **Limitata** e immetti il limite massimo di trasferimento in MB/s.

In alternativa, seleziona **Illimitato**.

9. Seleziona **Applica**.

Aggiorna manualmente i dati snapshot in una relazione di replica

Una relazione di replica ha una pianificazione di replica impostata, ma puoi aggiornare manualmente i dati Snapshot trasferiti tra i volumi di origine e di destinazione in NetApp Workload Factory in qualsiasi momento.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. In **Inventory**, seleziona il menu delle azioni del file system da aggiornare e quindi seleziona **Manage**.
5. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
6. Nella scheda Relazioni di replica, seleziona il menu Azioni della relazione di replica da aggiornare.
7. Seleziona **Aggiorna**.
8. Nella finestra di dialogo Aggiorna, seleziona **Aggiorna**.

Metti in pausa una relazione di replica

Metti in pausa una relazione di replica per interrompere gli aggiornamenti di replica pianificati dal volume di origine al volume di destinazione. Il volume di destinazione passa da sola lettura a lettura/scrittura. Entrambi i volumi continuano a condividere l'ultima Snapshot di replica come nuova base di riferimento per la successiva risincronizzazione.

Prima di iniziare

Se metti in pausa un trasferimento in corso, il trasferimento non viene influenzato e la relazione passa a "Quiescing" finché il trasferimento non viene completato. Se il trasferimento corrente si interrompe, verrà considerato un trasferimento futuro e non verrà riavviato.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. In **Inventory**, seleziona il menu delle azioni del file system da aggiornare e quindi seleziona **Manage**.
5. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
6. Nella scheda Relazioni di replica, seleziona il menu Azioni della relazione di replica da mettere in pausa.
7. Seleziona **Pausa (Quiescenza)**.
8. Nella finestra di dialogo **Disattiva relazione**, seleziona **Disattiva**.

Risultato

La relazione si mette in pausa e il suo stato viene visualizzato come "In pausa".

Riprendi una relazione di replica sospesa

Quando riprendi una relazione di replica, tutte le modifiche apportate al volume di destinazione mentre la replica era interrotta vengono eliminate. Il volume di destinazione passa da lettura/scrittura a sola lettura e riceve di nuovo gli aggiornamenti dal volume di origine all'intervallo di replica pianificato.



I dati scritti sul volume sorgente originale tra l'ultima replica dei dati e il momento in cui il volume sorgente viene disabilitato non vengono conservati.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. In **Inventory**, seleziona il menu delle azioni del file system da aggiornare e quindi seleziona **Manage**.
5. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
6. Nella scheda Relazioni di replica, seleziona il menu Azioni della relazione di replica da riprendere.
7. Seleziona **Resume**.
8. Nella finestra di dialogo Riprendi relazione, seleziona **Riprendi**.

Risultato

La relazione riprende e il suo stato è visualizzato come "Replicated".

Invertire una relazione di replica

Inverti una relazione di replica in modo che il volume di destinazione diventi il volume di origine.

Le operazioni inverse sono supportate per quanto segue:

- Due file system FSx for ONTAP
- Un file system FSx for ONTAP e un sistema ONTAP locale

Dopo aver interrotto la replica e apportato modifiche al volume di destinazione, puoi replicare tali modifiche nel volume di origine. Questa procedura è comune negli scenari di disaster recovery, in cui lavori sul volume di destinazione per un certo periodo di tempo e vuoi invertire i ruoli dei volumi.

Quando inverti e riprendi una replica, i ruoli di origine e destinazione dei volumi si scambiano: il volume di destinazione diventa il nuovo volume di origine e il volume di origine diventa il nuovo volume di destinazione. L'operazione di inversione sovrascrive anche il contenuto del nuovo volume di destinazione con il contenuto del nuovo volume di origine. Se inverti una replica due volte, viene ristabilita la direzione di replica originale.

NOTA:

- I dati scritti sul volume sorgente originale tra l'ultima replica dei dati e il momento in cui il volume sorgente viene disabilitato non vengono conservati.
- La replica inversa non è disponibile quando si replicano i dati e le impostazioni di configurazione della storage VM.

Prima di iniziare

Assicurati di conoscere i ruoli attuali e futuri dei volumi di origine e di destinazione, perché le modifiche apportate al nuovo volume di destinazione vengono sovrascritte da quelle del nuovo volume di origine. Se lo usi in modo errato, potresti causare una perdita di dati indesiderata.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. In **Inventory**, seleziona il menu delle azioni del file system da aggiornare e quindi seleziona **Manage**.
5. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
6. Nella scheda Relazioni di replica, seleziona il menu Azioni della relazione di replica da invertire.
7. Seleziona **Relazione inversa**.
8. Nella finestra di dialogo Relazione inversa, seleziona **Inverti**.

Interrompi una relazione di replica

Interrompi una relazione di replica in NetApp Workload Factory. Quando interrompi una relazione di replica, gli aggiornamenti di replica pianificati dal volume di origine al volume di destinazione vengono sospesi. Il volume di destinazione passa dalla modalità di sola lettura alla modalità di lettura/scrittura.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. In **Inventory**, seleziona il menu delle azioni del file system da aggiornare e quindi seleziona **Manage**.
5. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
6. Nella scheda Relazioni di replica, seleziona il menu delle azioni della relazione di replica da interrompere.

7. Seleziona **Break**.
8. Nella finestra di dialogo Interrompi replica, seleziona **Interrompi**.

Risultato

Lo stato della replica del volume cambia in **Broken**. Il volume di destinazione diventa scrivibile.

Eliminare una relazione di replica

Elimina una relazione di replica in NetApp Workload Factory. Quando elimini una relazione di replica, viene rimossa la relazione di replica tra il volume di origine e il volume di destinazione. Dopo l'eliminazione della relazione di replica, entrambi i volumi continuano a esistere indipendentemente con i dati correnti che contengono.

Quando elimini una relazione di replica, FSx for ONTAP elimina anche gli Snapshot di replica comuni dei volumi di origine e di destinazione.

Passaggi

1. Accedi al "NetApp Console".
2. Seleziona il menu , **Workloads > Storage**.
3. Dal menu Storage, seleziona **Inventory**.
4. In **Inventory**, seleziona il menu delle azioni del file system da aggiornare e quindi seleziona **Manage**.
5. Dalla panoramica del file system, selezionare la scheda **Relazioni di replica**.
6. Nella scheda Relazioni di replica, seleziona il menu Azioni della relazione di replica da eliminare.
7. Seleziona **Delete**.
8. Nella finestra di dialogo Elimina relazione, seleziona **Elimina**.

Proteggi i tuoi dati FSx for ONTAP con NetApp Autonomous Ransomware Protection con AI

Proteggi i tuoi dati con NetApp Autonomous Ransomware Protection with AI (ARP/AI). Monitora l'attività negli ambienti NAS (NFS/SMB) e SAN per rilevare comportamenti anomali che potrebbero indicare un attacco ransomware. Se viene rilevata una minaccia, ARP/AI crea automaticamente nuove snapshot immutabili così puoi ripristinare i tuoi dati.

Informazioni su questa attività

Utilizza ARP/AI per proteggerti dagli attacchi di denial-of-service, in cui l'attaccante trattiene i dati finché non viene pagato un riscatto. ARP/AI offre il rilevamento del ransomware in real-time basato su:

- Identificazione dei dati in entrata come crittografati o in chiaro.
- Analisi che rilevano:
 - **Entropia**: una valutazione della casualità dei dati in un file (utilizzata sia in ambienti NAS che SAN)
 - **Tipi di estensione file**: un'estensione che non si conforma al tipo di estensione normale (usata solo in ambienti NAS)
 - **IOPS dei file**: un picco di attività anomala del volume con crittografia dei dati (usato solo in ambienti NAS)

ARP/AI può rilevare la diffusione della maggior parte degli attacchi ransomware dopo che è stato crittografato solo un piccolo numero di file, intervenire automaticamente per proteggere i dati e avisarti che è in corso un sospetto attacco.

La funzionalità ARP/AI si aggiorna automaticamente in base alla versione di ONTAP eseguita da Amazon FSx for NetApp ONTAP, così non devi effettuare aggiornamenti manuali.

Modalità di apprendimento e modalità attiva

Il comportamento di ARP/AI dipende dal protocollo e dal tipo di volume:

- **Volumi NAS (NFS/SMB):** ARP/AI inizia a funzionare non appena lo abiliti. Utilizza un modello di intelligenza artificiale pre-addestrato per rilevare immediatamente le minacce ransomware.
- **Volumi SAN (a partire da ONTAP 9.17.1):** ARP/AI offre una protezione immediata, anche durante il primo periodo di valutazione. Durante questo periodo di 2-4 settimane, il sistema apprende le normali attività di crittografia e imposta le soglie di avviso. Allo stesso tempo, continua a monitorare i tuoi dati, rilevare le minacce e inviare avvisi.
- **Modalità attiva:** Quando la modalità attiva è attiva, FSx per ONTAP crea snapshot ARP/AI per aiutarti a proteggere i tuoi dati quando rileva una possibile minaccia.

Se il sistema segnala un'estensione di file come insolita, esamina l'avviso. Puoi rispondere all'avviso per proteggere i tuoi dati oppure contrassegnarlo come falso positivo se l'attività è prevista.

Quando contrassegni un avviso come falso positivo, il sistema aggiorna le sue impostazioni di avviso. Ad esempio, se una nuova estensione di file attiva un avviso e la contrassegni come falso positivo, non riceverai un avviso la prossima volta che il sistema rileva quella estensione di file.

Configurazioni non supportate

Le seguenti configurazioni non supportano l'utilizzo di ARP/AI.

- volumi NVMe
- Volumi iSCSI con versioni di ONTAP precedenti alla 9.17.1

Abilitare ARP/AI per un file system o un volume

Attivando ARP/AI per un file system, proteggi automaticamente tutti i volumi NAS attuali e nuovi (NFS/SMB). A partire da ONTAP 9.17.1, supporta anche i volumi SAN (iSCSI). Puoi anche attivare ARP/AI per volumi specifici.

Se ARP/AI rileva un attacco reale dopo la sua attivazione, Workload Factory crea automaticamente una snapshot policy. Questa policy può creare fino a sei snapshot ogni quattro ore. Ogni snapshot è bloccato per 2-5 giorni.

Prima di iniziare

Per abilitare ARP/AI per un file system o un volume, devi associare un collegamento. ["Scopri come associare un collegamento esistente o creare e associare un nuovo collegamento"](#). Dopo aver associato il collegamento, torna a questa procedura.

Abilita ARP/AI per un file system

Passaggi

1. Accedi al ["NetApp Console"](#).
- 2.

Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.

3. Dal menu **FSx for ONTAP**, seleziona **Inventory**, quindi seleziona il menu delle azioni del file system per abilitare ARP/AI e infine seleziona **Manage**.
4. In Informazioni, seleziona l'icona della matita accanto a **Autonomous Ransomware Protection**. L'icona della matita appare accanto alla freccia quando passi con il mouse sulla riga **Autonomous Ransomware Protection**.
5. Dalla pagina Protezione autonoma contro i ransomware con intelligenza artificiale (ARP/AI) di NetApp, procedi come segue:
 - a. Attiva o disattiva la funzione.
 - b. **Creazione automatica di snapshot**: Seleziona il numero massimo di snapshot da conservare e l'intervallo di tempo tra l'acquisizione di uno snapshot e l'altro. L'impostazione predefinita è di 6 snapshot ogni 4 ore.
 - c. **Snapshot immutabili**: Seleziona il periodo di conservazione predefinito in ore e il numero massimo di giorni per conservare gli snapshot immutabili. Abilita questa opzione per garantire che gli snapshot non possano essere eliminati o modificati fino al termine del periodo di conservazione specificato.
 - d. **Rilevamento**: Facoltativamente, seleziona uno qualsiasi dei seguenti parametri per eseguire la scansione e rilevare automaticamente le anomalie.
6. Accetta la dichiarazione per procedere.
7. Seleziona **Applica** per salvare le modifiche.

Abilita ARP/AI per un volume

Passaggi

1. Accedi al "[NetApp Console](#)".
2. Seleziona il menu , **Workloads > Volumes explorer**.
3. Seleziona il menu Azioni del volume per abilitare ARP/AI, poi **Azioni di protezione dei dati** e quindi **Gestisci ARP/AI**.
4. Nella finestra di dialogo Gestisci ARP/AI, esegui queste operazioni:
 - a. Attiva o disattiva la funzione.
 - b. **Rilevamento**: Facoltativamente, seleziona uno qualsiasi dei seguenti parametri per eseguire la scansione e rilevare automaticamente le anomalie.
5. Accetta la dichiarazione per procedere.
6. Seleziona **Applica** per salvare le modifiche.

Convalida gli attacchi ransomware

Determina se un attacco è un falso allarme o un vero e proprio incidente ransomware.

Passaggi

1. Accedi al "[NetApp Console](#)".
2. Seleziona il menu , **Carichi di lavoro > Archiviazione > FSx for ONTAP**.

3. Dal menu **FSx for ONTAP**, seleziona **Inventory** e poi seleziona il file system per cui vuoi convalidare gli attacchi ransomware.
4. Dalla panoramica del file system, seleziona la scheda **Volumi**.
5. Seleziona **Analizza gli attacchi** dal riquadro Protezione autonoma dal ransomware.
6. Scarica il report degli eventi di attacco per verificare se file o cartelle sono stati compromessi e poi decidere se si è verificato un attacco.
7. Se non si è verificato alcun attacco, seleziona **Falso allarme** per il volume nella tabella e quindi seleziona **Chiudi**.
8. Se si è verificato un attacco, seleziona **Attacco reale** per il volume nella tabella. Si apre la finestra di dialogo Ripristina dati del volume compromesso. Puoi procedere [recupera i tuoi dati](#) immediatamente oppure selezionare **Chiudi** e tornare più tardi per completare il processo di ripristino.

Recupera i dati dopo un attacco ransomware

Quando il sistema rileva un possibile attacco, crea e blocca un'istantanea del volume in quel preciso istante.

Se l'attacco viene successivamente confermato, puoi ripristinare i file interessati o l'intero volume dallo snapshot.

Gli snapshot bloccati non possono essere eliminati fino alla scadenza del periodo di conservazione. Se in seguito l'attacco viene identificato come un falso allarme, lo snapshot bloccato viene eliminato.

Poiché il sistema identifica i file interessati e l'ora dell'attacco, puoi recuperare solo i file interessati dagli snapshot disponibili invece di ripristinare l'intero volume.

Passaggi

1. Accedi al ["NetApp Console"](#).
2. Seleziona il menu  **Carichi di lavoro > Archiviazione > FSx for ONTAP**.
3. Dal menu **FSx for ONTAP**, seleziona **Inventory** e poi seleziona il file system da cui recuperare i dati.
4. Dalla panoramica del file system, seleziona la scheda **Volumi**.
5. Seleziona **Analizza gli attacchi** dal riquadro Protezione autonoma dal ransomware.
6. Se si è verificato un attacco, seleziona **Attacco reale** per il volume nella tabella.
7. Nella finestra di dialogo Restore compromised volume data, segui le istruzioni per eseguire il ripristino a livello di file o di volume. Nella maggior parte dei casi, ripristinerai i file anziché un intero volume.
8. Dopo aver completato il ripristino, seleziona **Chiudi**.

Risultato

I dati compromessi sono stati ripristinati.

Clona un volume in NetApp Workload Factory

Clona un volume in NetApp Workload Factory per creare un volume di lettura/scrittura del volume originale per i test.

Il clone riflette lo stato attuale, point-in-time, dei dati. Puoi anche utilizzare i cloni per consentire ad altri utenti di accedere ai dati senza dare loro accesso ai dati di produzione.

Informazioni su questa attività

La clonazione dei volumi è supportata solo per i volumi FlexClone.

Quando cloni un volume, viene creato un volume scrivibile con riferimenti agli Snapshot del volume d'origine. La creazione del clone avviene in secondi. I dati clonati non risiedono sul volume clone, ma sul volume d'origine. Tutti i nuovi dati scritti sul volume dopo la creazione del clone risiedono sul clone.

Affinché un volume clonato contenga tutti i dati del volume d'origine e tutti i nuovi dati aggiunti al clone dopo la creazione, devi **"dividi il clone"** dal volume d'origine. Inoltre, non puoi eliminare un volume d'origine se contiene un clone. Un clone deve essere suddiviso prima di poter eliminare un volume d'origine.

Passaggi

1. Accedi al **"NetApp Console"**.
2. Seleziona il menu , **Workloads > Volumes explorer**.
3. Seleziona il menu delle azioni del volume da clonare.
4. Seleziona **Azioni di protezione dei dati**, quindi **Clona volume**.
5. Nella finestra di dialogo Clone volume, immetti un nome per il clone del volume.
6. Seleziona **Clone**.

Proteggi i tuoi dati FSx for ONTAP con un cyber vault

Un volume del cyber vault è una posizione di archiviazione isolata e sicura utilizzata per memorizzare copie di backup dei tuoi dati, proteggendoli da attacchi ransomware e altre minacce informatiche. Nell'ambito della creazione del vault, creerai un volume del cyber vault, disabiliterai tutti i protocolli client, imposterai una relazione di replica tra il volume di origine e il volume del cyber vault e creerai snapshot immutabili sul volume del cyber vault.

Che cos'è un cyber vault?

Un cyber vault è una specifica tecnica di protezione dei dati che prevede l'archiviazione di dati critici in un ambiente isolato, separato dall'infrastruttura IT principale.

Il cyber vault è un repository di dati "air-gapped", immutabile e indelebile, immune alle minacce che colpiscono la rete principale, come malware, ransomware o persino minacce interne. Un cyber vault può essere realizzato tramite Snapshot immutabili e indelebili.

I backup con isolamento fisico (air-gapping) che utilizzano metodi tradizionali prevedono la creazione di spazio e la separazione fisica dei supporti primario e secondario. Spostando i supporti in una sede esterna e/o interrompendo la connettività, i malintenzionati non hanno accesso ai dati. Questo protegge i dati, ma può comportare tempi di ripristino più lunghi.

vault informatici di FSx for ONTAP

Amazon FSx for NetApp ONTAP è supportato sia come origine sia come destinazione di un cyber vault.

Implementazione

Workload Factory ti assiste nella creazione di un'architettura di cyber vault. Dopo che contatti NetApp per esprimere il tuo interesse a implementare un cyber vault, uno specialista di NetApp ti contatta per discutere i tuoi requisiti.

Per iniziare, invia un'e-mail a ng-FSx-CyberVault@netapp.com.

Informazioni correlate

Per ulteriori informazioni sui cyber vault e su come configurare questa architettura, consulta "[Documentazione di ONTAP cyber vault](#)".

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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