Proteggi i tuoi dati

Amazon FSx for NetApp ONTAP

NetApp
February 17, 2026

Sommario

Proteggi i tuoi dati

Tipi di protezione dei dati in NetApp Workload Factory

FSx per ONTAP supporta snapshot, NetApp Autonomous Ransomware Protection con intelligenza artificiale, replica e backup per la protezione dei dati. Ti consigliamo di utilizzare una combinazione di diverse tipologie di protezione dei dati per prepararti all'inevitabile e salvaguardare i tuoi dati.

Tipi di protezione dei dati

La data Protection per i tuoi carichi di lavoro ti aiuta a garantire un ripristino da qualsiasi perdita di dati in qualsiasi momento. Informatevi sui tipi di protezione dei dati prima di selezionare le funzioni da utilizzare.

Snapshot

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

Protezione autonoma dal ransomware NetApp con intelligenza artificiale

NetApp Autonomous Ransomware Protection with AI (ARP/AI) utilizza l'analisi del carico di lavoro negli ambienti NAS (NFS/SMB) per rilevare e segnalare attività anomale che potrebbero essere un attacco ransomware. Quando si sospetta un attacco, ARP/AI crea anche nuovi snapshot immutabili, oltre alla protezione esistente fornita dagli snapshot pianificati.

Replica

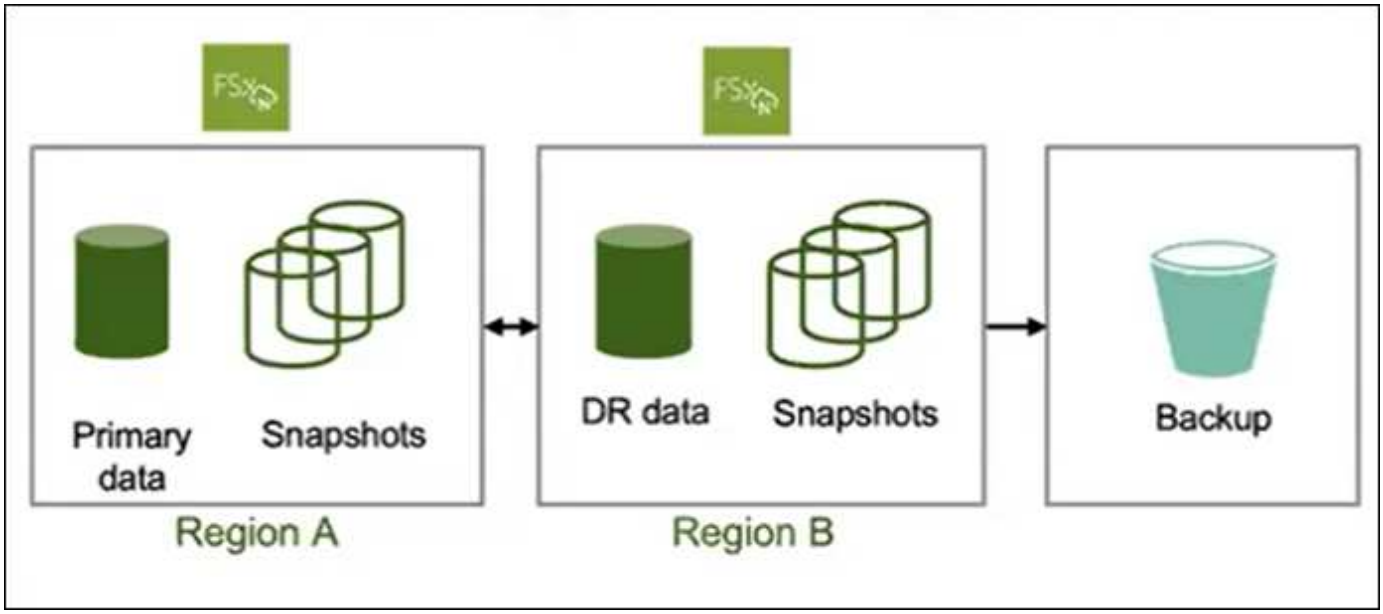
La replica crea una copia secondaria dei dati su un altro file system FSX per ONTAP e aggiorna continuamente i dati secondari. I dati restano aggiornati e disponibili in qualsiasi momento, ad esempio per il disaster recovery.

Puoi scegliere di creare sia volumi replicati in un altro file system FSX per ONTAP e file di backup nel cloud. In alternativa, puoi scegliere di creare volumi replicati o file di backup.

Backup

Puoi creare backup dei tuoi dati nel cloud per la protezione e la conservazione a lungo termine. Se necessario, è possibile ripristinare un volume, una cartella o singoli file dal backup nello stesso file system di lavoro o in un altro file system.

Il diagramma seguente mostra una rappresentazione visiva della data Protection per lo storage FSX per ONTAP utilizzando snapshot, replica tra aree e backup in storage a oggetti.



Best practice per la protezione dei dati dei carichi di lavoro

FSX per ONTAP offre diverse opzioni di protezione dei dati, che possono essere combinate insieme per raggiungere i recovery point objective e time objective selezionati. Per una protezione ottimale, si consiglia di utilizzare sia gli snapshot dei volumi che i backup dei volumi.

Un recovery point objective (RPO) descrive la frequenza di esecuzione delle copie dei dati più recenti, che dipende dalla frequenza di esecuzione delle copie. Un recovery time objective (RTO) definisce il tempo necessario per il ripristino dei dati.

Proteggi i dati dei carichi di lavoro con le snapshot

Gli Snapshot sono versioni virtuali point-in-time di un volume acquisite su base pianificata. È possibile accedere alle snapshot utilizzando 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. Le snapshot consentono inoltre agli utenti di ripristinare specifici file e directory, diminuendo ulteriormente l'RTO. Le copie Snapshot consumano ulteriore spazio per i volumi solo in caso di modifiche apportate.

Proteggi i dati del tuo carico di lavoro con la protezione autonoma dai ransomware NetApp con intelligenza artificiale

NetApp Autonomous Ransomware Protection with AI (ARP/AI) funge da importante ulteriore livello di difesa se il software antivirus non riesce a rilevare un'intrusione. L'impostazione di una policy ARP/AI la abilita per tutte le VM di archiviazione e per tutti i volumi esistenti e di nuova creazione. Una volta abilitato, ARP/AI rileva e protegge tutti i volumi e le VM di archiviazione. Se un'estensione di file viene contrassegnata come anomala, è necessario valutare l'avviso.

Proteggi i dati dei tuoi carichi di lavoro con la replica dei volumi

La replica di un volume crea una copia dei dati più recenti di un volume, inclusi tutti i relativi snapshot in un'area diversa. Se non puoi permetterti RTO di più ore di un'operazione di ripristino di un volume completo da un backup di un volume, prendi in considerazione l'esecuzione di una replica di un volume. Mentre la replica del volume garantisce che i dati recenti siano disponibili in un'area diversa, è necessario regolare i client per utilizzare il volume nell'altra area.

Proteggi i dati dei tuoi carichi di lavoro con i backup

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

Consigli per la protezione dei dati dei carichi di lavoro

Prendi in considerazione i seguenti consigli per proteggere i dati del tuo carico di lavoro.

- Utilizzare la replica del volume per il disaster recovery: se l'applicazione richiede un RTO basso, valutare l'utilizzo della replica del volume per replicare i dati in un'altra regione.
- Utilizzare i backup di volume insieme alle istantanee: L'utilizzo congiunto delle due funzioni garantisce la possibilità di ripristinare i file dalle istantanee ed eseguire ripristini completi in caso di perdita di volume utilizzando i backup.
- Definire una policy di backup dei volumi: Accertarsi che la policy di backup soddisfi i requisiti aziendali in termini di durata e frequenza dei backup. Si consiglia di conservare un minimo di due backup giornalieri per ogni volume.
- Definire una pianificazione snapshot: È meno probabile che vengano utilizzate le snapshot meno recenti per ripristinare i dati. Consigliamo di definire una pianificazione delle snapshot che tenga conto dei rendimenti in diminuzione dovuti al mantenimento delle snapshot più vecchie rispetto al costo di capacità delle snapshot aggiuntiva.
- Abilita una policy ARP/AI per il tuo file system o per singoli volumi per aggiungere un ulteriore livello di protezione e proteggere i tuoi dati dagli attacchi ransomware.

Utilizzare gli snapshot

Crea una snapshot manuale di un volume FSX per ONTAP

Creare uno snapshot manuale di un volume FSx for ONTAP in NetApp Workload Factory. Gli snapshot sono versioni puntuali del contenuto del volume.

Gli snapshot sono risorse di volumi e offrono acquisizioni istantanee dei dati che occupano spazio solo per i dati modificati. A causa del cambiamento dei dati nel tempo, le snapshot solitamente occupano più spazio man mano che diventano più datate.

FSX per ONTAP Volumes usa il copy-on-write just-in-time in modo che i file non modificati nelle snapshot non consumino la capacità del volume.

> Le snapshot non sono copie dei tuoi dati. Se vuoi creare copie dei tuoi dati, prendi in considerazione l'utilizzo di FSX per ONTAP o delle funzionalità di replica dei volumi.

Prima di iniziare

Per creare uno snapshot manuale di un volume è necessario associare un collegamento. "Scopri come associare un collegamento esistente o come creare e associare un nuovo collegamento". Dopo l'associazione del collegamento, tornare a questa operazione.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, seleziona il menu azioni del file system che contiene il volume per cui creare uno snapshot, quindi seleziona **Gestisci**.
5. Nella panoramica del file system, selezionare la scheda **volumi**.
6. Dalla scheda **Volumi**, seleziona il menu delle azioni per il volume da proteggere con gli snapshot.
7. Selezionare **Azioni di protezione dei dati** e quindi **Gestisci snapshot**.
8. Dalla pagina Gestisci snapshot, seleziona **Crea snapshot**.
9. Nella finestra di dialogo Crea uno snapshot, procedi come segue:
   a. Immettere un nome per lo snapshot nel campo **Nome snapshot**.
   b. Facoltativamente, seleziona un'etichetta o creane una nuova.
   c. Impostare **periodo di conservazione** come numero di ore, giorni, mesi o anni.
   d. Facoltativo: **Rendi questo snapshot immutabile** per evitare che venga eliminato durante il periodo di conservazione.

      Accettare la dichiarazione relativa agli snapshot immutabili.
10. Selezionare **Crea**.

Creare un criterio di snapshot per le VM di archiviazione in Workload Factory

Crea un criterio di snapshot personalizzato per le VM di archiviazione in Workload Factory per gestire la creazione e la conservazione degli snapshot. Un criterio di snapshot definisce il modo in cui il sistema crea snapshot per una VM di archiviazione. È possibile creare un criterio di snapshot per una VM di archiviazione in un file system FSx for ONTAP . È anche possibile condividere la policy su più VM di archiviazione.

A proposito di questa attività

È possibile creare un criterio di snapshot personalizzato diverso da quello delle tre policy integrate per FSX for ONTAP:

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

Per impostazione predefinita, ogni volume è associato al criterio di snapshot del file system `default` . Consigliamo di utilizzare questa policy per la maggior parte dei carichi di lavoro.

La personalizzazione di un criterio consente di specificare quando creare le snapshot, il numero di copie da conservare e il nome delle stesse.

Prima di iniziare

- Una volta creato un criterio snapshot, la sua associazione con le VM di storage non può essere modificata, ma è sempre possibile aggiungere o rimuovere il criterio dai volumi.

- Prima di utilizzare le snapshot, occorre valutare quanto segue:
  - Per la maggior parte dei set di dati, è sufficiente una capacità aggiuntiva del 20% per conservare le snapshot per un massimo di quattro settimane. Man mano che i dati diventano più datati, il loro utilizzo per i ripristini diventa meno probabile.
  - La sovrascrittura di tutti i dati di uno snapshot consuma una notevole capacità del volume, fattore che influisce sul provisioning della capacità del volume.
- Per creare un criterio di snapshot personalizzato, è necessario associare un collegamento. "Scopri come associare un collegamento esistente o come creare e associare un nuovo collegamento". Dopo l'associazione del collegamento, tornare a questa operazione.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, selezionare il menu azioni del file system con il volume e quindi selezionare **Gestisci**.
5. Nella panoramica del file system, selezionare la scheda **Storage VM**.
6. Dalla scheda **VM di archiviazione**, seleziona il menu delle azioni per il volume da proteggere con snapshot pianificati, quindi **Azioni avanzate** e infine **Gestisci criteri snapshot**.
7. Nella pagina di gestione dei criteri di snapshot, selezionare **Crea criterio di snapshot**.
8. Nel campo **Snapshot policy name** (Nome criterio istantanea), immettere un nome per il criterio snapshot.
9. Facoltativamente, immettere una descrizione per il criterio snapshot.
10. In **Policy Schedule and Copies**, selezionare quando creare snapshot. Ad esempio, ogni minuto o ogni ora.

    È possibile selezionare più di una frequenza.
11. In **numero di copie**, immettere il numero di copie da conservare.

    Il numero massimo di copie è 1.023.
12. Facoltativo: In **convenzione di denominazione**, immettere un **prefisso** per la policy.
13. **Etichetta di conservazione** viene compilata automaticamente.

    Questa etichetta si riferisce all'etichetta SnapMirror o di replica utilizzata per selezionare solo gli snapshot specificati per la replica dal file system di origine a quello di destinazione.
14. Facoltativo: Abilitare **istantanee immutabili** per qualsiasi pianificazione necessaria, impostare il **periodo di conservazione** per ogni pianificazione e accettare l'istruzione per continuare.

    L'attivazione degli snapshot immutabili blocca tutti gli snapshot in questa policy per impedire l'eliminazione degli snapshot durante il periodo di conservazione.
15. **Condivisione tra VM di archiviazione**: Abilitata per impostazione predefinita. Quando abilitata, la policy di snapshot viene condivisa tra tutte le macchine virtuali storage nel file system. Disattiva per creare una policy di snapshot per una singola macchina virtuale di storage.
16. Selezionare **Crea**.

Ripristina un volume da uno snapshot in Workload Factory

In Workload Factory è possibile ripristinare i dati da uno snapshot a un volume esistente o a un nuovo volume. L'operazione di ripristino consente il recupero in un determinato momento quando un volume contiene file eliminati o danneggiati.

A proposito di questa attività

È possibile ripristinare i dati da uno snapshot su un volume esistente o su un nuovo volume.

La creazione di un nuovo volume da uno snapshot crea una copia di un intero volume in pochi secondi, indipendentemente dalle dimensioni del volume. La copia appena creata rappresenta un nuovo volume.

Prima di iniziare

Prima di creare un volume da uno snapshot, prendere in considerazione le seguenti limitazioni:

- È possibile ripristinare un volume da uno snapshot solo se si dispone già di una copia snapshot del volume.
- Modifiche ai modelli di autorizzazione: Se si utilizza questa operazione per cambiare il tipo di protocollo NAS (Network-Attached Storage), è possibile che cambi anche il modello di autorizzazione fornito dallo stile di protezione. Potrebbero verificarsi problemi di autorizzazione all'accesso ai file, che è possibile risolvere solo manualmente con l'accesso dell'amministratore utilizzando gli strumenti client NAS per l'impostazione delle autorizzazioni.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, selezionare il menu azioni del file system con il volume e quindi selezionare **Gestisci**.
5. Nella panoramica del file system, selezionare la scheda **volumi**.
6. Dalla scheda **Volumi**, selezionare il menu delle azioni per il volume da ripristinare da uno snapshot.
7. Selezionare **Azioni di protezione dei dati** e quindi **Gestisci snapshot**.
8. Dalla pagina Gestisci snapshot, seleziona il menu delle azioni per lo snapshot da ripristinare, quindi seleziona **Ripristina**.
9. Nella finestra di dialogo Ripristina volume da uno snapshot, seleziona una delle seguenti opzioni:
   - Attiva/disattiva per selezionare **Ripristina come nuovo volume**.

     Nel campo **nome volume ripristinato**, immettere un nome univoco per il volume da ripristinare.

   - Ripristina i dati da uno snapshot a un volume esistente. Questa operazione elimina definitivamente tutti i dati modificati dopo la creazione dello snapshot.

     Accettare la dichiarazione per procedere.
10. Selezionare **Restore** (Ripristina).

Utilizzare i backup per l'archiviazione degli oggetti

Creare un backup manuale di un volume in NetApp Workload Factory

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

A proposito di questa attività

I backup di FSX per ONTAP vengono eseguiti per volume, pertanto ogni backup contiene solo i dati di un volume specifico.

I backup di FSX per ONTAP sono incrementali e questo significa che solo i dati sul volume modificati dopo il salvataggio dell'ultimo backup. In questo modo si riduce al minimo il tempo necessario per creare il backup e lo storage necessario per il backup, risparmiando sui costi di storage senza duplicare i dati.

Prima di iniziare

Per eseguire il backup dei volumi, sia il volume che il file system devono disporre di una capacità di storage SSD sufficiente per archiviare lo snapshot di backup. Quando si crea una snapshot di backup, la capacità di storage aggiuntiva consumata dalla snapshot non può far sì che il volume superi il 98% di utilizzo dello storage SSD. In questo caso, il backup non viene eseguito correttamente.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, selezionare il menu azioni del file system con il volume e quindi selezionare **Gestisci**.
5. Nella panoramica del file system, selezionare la scheda **volumi**.
6. Dalla scheda **Volumi**, selezionare l'azione relativa al volume di cui eseguire il backup.
7. Selezionare **azioni protezione dati**, **FSX per il backup ONTAP**, quindi **Backup manuale**.
8. Nella finestra di dialogo Backup manuale, immettere un nome per il backup.
9. Selezionare **Backup**.

Ripristina un volume da un backup in NetApp Workload Factory

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

Workload Factory determina se si dispone di capacità sufficiente per il ripristino e, in caso contrario, può aggiungere automaticamente capacità del Tier di storage SSD.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, selezionare il menu azioni del file system con il volume e quindi selezionare **Gestisci**.

5. Nella panoramica del file system, selezionare la scheda **volumi**.
6. Dalla scheda **Volumi**, selezionare il menu delle azioni per il volume da ripristinare da un backup.
7. Selezionare **azioni protezione dati**, **FSX per il backup ONTAP**, quindi **Ripristina da un backup**.
8. Nella finestra di dialogo Ripristina da un backup, specificare quanto segue:
   a. **File system di destinazione**: Selezionare il file system di destinazione dal menu a discesa.
   b. **VM di archiviazione di destinazione**: Selezionare la VM di archiviazione di destinazione dal menu a discesa.
   c. **Nome backup**: Selezionare il nome del backup dal menu a discesa.
   d. **Nome volume ripristinato**: Immettere il nome del volume ripristinato.
9. Verificare la capacità del file system per l'operazione di ripristino.

   Quando la capacità del file system è limitata, si possono verificare le seguenti condizioni:

   - Il ripristino può spingere la capacità utilizzata oltre la soglia specificata. È possibile completare l'operazione di ripristino. Considerare"Aggiunta manuale della capacità del Tier di storage SSD" oppure selezionando Workload Factory per aggiungere automaticamente la capacità del livello di archiviazione SSD.
   - Il ripristino richiede capacità SSD aggiuntiva. Per procedere, è necessario selezionare Workload Factory per aggiungere automaticamente la capacità del livello di archiviazione SSD.
10. Selezionare **Restore** (Ripristina).

Utilizzare la replicazione

Replica i dati su FSx per ONTAP in NetApp Workload Factory

Crea una relazione di replica per un file system FSx for ONTAP in NetApp Workload Factory per evitare la perdita di dati in caso di un disastro imprevisto. Puoi replicare i dati tra due file system FSx for ONTAP o tra un sistema ONTAP on-premises e un file system FSx for ONTAP.

Per la migrazione della storage VM, è necessario completare l'operazione di cutover subito dopo aver creato una relazione di replica.

A proposito di questa attività

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

I volumi replicati nel file system di destinazione sono volumi di protezione dei 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.

- La replica non è supportata per i volumi a blocchi che utilizzano i protocolli iSCSI o NVMe.
- Puoi replicare un volume di origine (lettura/scrittura) o un volume di data Protection (DP). La replica a cascata è supportata, ma non è un terzo hop. Ulteriori informazioni su "replica a cascata".

Casi d'uso della migrazione

Quando si seleziona il caso d'uso di migrazione, è possibile scegliere facoltativamente di replicare i dati e le impostazioni di configurazione della storage VM per una singola storage VM. Quando si migrano dati e impostazioni di configurazione simultaneamente, assicurati che l'ultima replica per il volume sia stata completata nelle ultime 24 ore. Tutti i volumi nella stessa VM di storage devono essere selezionati per utilizzare questa funzionalità. La policy di tiering per tutti i volumi predefinita è quella del volume di origine, che è consigliata per i casi d'uso di migrazione.

Workload Factory supporta la replica della migrazione tra i seguenti sistemi 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
  - Dalla prima alla seconda generazione
  - Seconda alla seconda generazione

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

1. Creare una relazione di replica, seleziona **Migration** come caso d'uso e seleziona **Replicate storage VM configuration**.
2. 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.

Creare una relazione di replica

Replica i dati tra due file system FSx for ONTAP o tra un sistema ONTAP on-premises e un file system FSx for ONTAP.

Prima di iniziare

Rivedi questi requisiti prima di iniziare.

- È necessario disporre di un FSx for ONTAP file system da utilizzare per il volume di destinazione nella replica dei dati.
- Il file system FSx for ONTAP utilizzato per la relazione di replica deve avere un collegamento associato. "Scopri come associare un collegamento esistente o come creare e associare un nuovo collegamento". Dopo aver associato il collegamento, tornare 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.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, seleziona il file system che contiene il volume o i volumi da replicare.
5. Replicare tutti i volumi in un file system o volumi selezionati.
   - Per replicare tutti i volumi in un file system: Dalla panoramica del file system, selezionare **Replica dati**.
   - Per replicare volumi selezionati: Dalla panoramica del file system, selezionare la scheda **volumi**.

     Nella tabella volumi, selezionare uno o più volumi, quindi selezionare **Replica dati**.
6. Nella pagina Replica dati, in destinazione replica, fornire quanto segue:

   a. **Caso d'uso**: selezionare 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. È possibile accettare i valori consigliati o apportare modifiche durante la compilazione del modulo.
      - Migrazione: Trasferimento dei dati nel file system FSX per ONTAP di destinazione

        Replica configurazione VM di storage: facoltativamente, seleziona per replicare i dati e le impostazioni di configurazione della VM di storage per una singola VM di storage. Quando si migrano dati e impostazioni di configurazione simultaneamente, assicurati che l'ultima replica per il volume sia stata completata nelle ultime 24 ore. Tutti i volumi nella stessa VM di storage devono essere selezionati per utilizzare questa funzionalità. La policy di tiering per tutti i volumi predefinita è quella del volume di origine, che è consigliata per i casi d'uso di migrazione.

      - Disaster recovery "hot": Garantisce alta disponibilità e rapido disaster recovery per i carichi di lavoro critici
      - Disaster recovery a freddo o di archivio:
        - Disaster recovery a freddo: Utilizza RTO (recovery time objective) e RPO (recovery point objects) più lunghi per ridurre i costi
        - Archiviazione: Replica i dati per storage e conformità a lungo termine
      - Altro

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

        - Per la migrazione e altre, il criterio di replica è denominato *MirrorAllSnapshots*. *MirrorAllSnapshots* è un criterio asincrono per il mirroring di tutti gli snapshot e del file system attivo più recente.
        - Per il disaster recovery hot, cold o di archivio, il criterio di replica si chiama *MirrorAndVault*. *MirrorAndVault* è un criterio asincrono e vault per il mirroring del file system attivo più recente e degli snapshot giornalieri e settimanali.

          Per tutti i casi di utilizzo, se si abilitano gli snapshot per la conservazione a lungo termine, il

criterio di replica predefinito è *MirrorAndVault*.

b. **FSX per il file system ONTAP**: Selezionare credenziali, area e FSX per il nome del file system ONTAP per il file system FSX per ONTAP di destinazione.

c. **Nome VM di archiviazione**: Selezionare la VM di archiviazione dal menu a discesa. La VM di archiviazione selezionata è la destinazione per tutti i volumi selezionati in questa relazione di replica.

d. **Volume name**: Il nome del volume di destinazione viene generato automaticamente con il seguente formato `{OriginalVolumeName}_copy`. È possibile utilizzare il nome del volume generato automaticamente o immettere un altro nome di volume.

e. **Criterio di tiering**: Selezionare il criterio di tiering per i dati memorizzati nel volume di destinazione. Il criterio di tiering predefinito corrisponde alla policy di tiering consigliata per il caso d'utilizzo selezionato.

Bilanciato (Automatico) è il criterio di suddivisione in livelli predefinito quando si crea un volume utilizzando la console Workload Factory. Per ulteriori informazioni sulle politiche di suddivisione in livelli del volume, fare riferimento a"Capacità di storage dei volumi" nella documentazione di AWS FSx per NetApp ONTAP . Si noti che Workload Factory utilizza nomi basati sui casi d'uso nella console Workload Factory per i criteri di suddivisione in livelli e include i nomi dei criteri di suddivisione in livelli FSx for ONTAP tra parentesi.

Se hai selezionato il caso d'uso di migrazione, Workload Factory sceglie automaticamente di copiare la policy di suddivisione in livelli del volume di origine nel volume di destinazione. È possibile deselezionare la copia del criterio di suddivisione in livelli e selezionare un criterio di suddivisione in livelli che si applichi al volume selezionato per la replica.

a. **Velocità di trasferimento massima**: Selezionare **limitata** e immettere il limite massimo di trasferimento in MB/s. In alternativa, selezionare **illimitato**.

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

7. In Impostazioni di replica, specificare quanto segue:

a. **Intervallo di replica**: Consente di selezionare la frequenza di trasferimento degli snapshot dal volume di origine al volume di destinazione.

b. **Conservazione a lungo termine**: Facoltativamente, abilitare gli snapshot per la conservazione a lungo termine. La conservazione a lungo termine permette ai servizi di business di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria.

Le repliche senza conservazione a lungo termine utilizzano la policy *MirrorAllSnapshots*. Abilitando la conservazione a lungo termine, alla replica viene assegnata la policy *MirrorAndVault*.

Se si attiva la conservazione a lungo termine, selezionare un criterio esistente o creare un nuovo criterio per definire gli snapshot da replicare e il numero da conservare.

Per la conservazione a lungo termine sono necessarie etichette di origine e destinazione corrispondenti. Se lo si desidera, workload Factory può creare etichette mancanti.

- **Scegliere un criterio esistente**: Selezionare un criterio esistente dal menu a discesa.
- **Crea una nuova policy**: inserisci un **nome policy**.

c. **Snapshot immutabili**: Facoltativo. Selezionare **attiva istantanee immutabili** per impedire l'eliminazione degli snapshot creati in questo criterio durante il periodo di conservazione.
   - Impostare **periodo di conservazione** in numero di ore, giorni, mesi o anni.
   - **Snapshot policies**: Nella tabella, selezionare la frequenza del criterio di snapshot e il numero di copie da conservare. È possibile selezionare più criteri di snapshot.

d. **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. Fornendo i seguenti dettagli:
   - **Nome punto di accesso S3**: immettere il nome del punto di accesso S3.
   - **Utente**: seleziona un utente esistente con accesso al volume oppure crea un nuovo utente.
   - **Tipo di utente**: selezionare **UNIX** o **Windows** come tipo di utente.
   - **Configurazione di rete**: seleziona **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 VPC specifica.
   - **Abilita metadati**: l'abilitazione dei metadati crea una tabella S3 contenente tutti gli oggetti accessibili dal punto di accesso S3, che puoi utilizzare per auditing, governance, analisi automatica e ottimizzazione. L'abilitazione dei metadati comporta costi AWS aggiuntivi. Consulta "Documentazione sui prezzi di Amazon S3" per ulteriori informazioni.

e. **Tag del punto di accesso S3**: Facoltativamente, puoi aggiungere fino a 50 tag.

8. Selezionare **Crea**.

Risultato

La relazione di replica viene visualizzata 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.

Cut over replication per casi d'uso di migrazione

Dopo aver creato una 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 VM di storage al file system FSx for ONTAP di destinazione. La replica cutover migra in modo permanente i dati e le impostazioni di configurazione della VM di storage dal file system di origine al file system FSx for ONTAP di destinazione. Durante il cutover, i dati vengono replicati per l'ultima volta. Il sistema elimina il volume o i volumi di origine dopo il completamento del cutover. Questa azione non può essere annullata.

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 come creare e associare un nuovo collegamento". Dopo aver associato il collegamento, tornare a questa operazione.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, seleziona il file system che contiene il volume o i volumi da replicare.
5. Seleziona la scheda **Replication relationships**.
6. Nella tabella Relazioni di replicazione, seleziona la relazione di replicazione su cui eseguire il cutover, quindi seleziona **Cut over replication**.
7. Rivedere le informazioni nella finestra di dialogo Cut over replication e quindi digitare *cut over* per confermare.
8. Seleziona **cutover**.

Risultato

Dopo cutover, i volumi di origine vengono eliminati e i volumi di destinazione diventano di lettura/scrittura. È possibile "modificare la tiering policy" per i volumi di destinazione dopo cutover.

Inizializzare una relazione di replica in NetApp Workload Factory

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.

A proposito di questa attività

L'inizializzazione esegue un trasferimento *baseline*: Crea uno snapshot del volume di origine, quindi trasferisce lo snapshot e tutti i blocchi di dati che fa riferimento al volume di destinazione.

Prima di iniziare

Considerare quando si sceglie di completare questa operazione. L'inizializzazione può richiedere molto tempo. Si consiglia di eseguire il trasferimento di riferimento in ore non di punta.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, seleziona il menu delle azioni del file system da aggiornare, quindi seleziona **Gestisci**.
5. Nella panoramica del file system, selezionare la scheda **Relazioni di replica**.
6. Nella scheda Relazioni di replica, selezionare il menu delle azioni della relazione di replica da inizializzare.
7. Selezionare **Inizializza**.
8. Nella finestra di dialogo Inizializza relazione, selezionare **Inizializza**.

Proteggi i tuoi dati con la protezione autonoma dai ransomware NetApp con intelligenza artificiale

Proteggi i tuoi dati con NetApp Autonomous Ransomware Protection con AI (ARP/AI), una funzionalità che utilizza l'analisi del carico di lavoro negli ambienti NAS (NFS/SMB) per rilevare e avvisare in caso di attività anomale che potrebbero essere un attacco ransomware. Quando si sospetta un attacco, ARP/AI crea anche nuovi snapshot immutabili dai quali è possibile ripristinare i dati.

A proposito di questa attività

Utilizzare ARP/AI per proteggersi dagli attacchi denial-of-service, in cui l'aggressore trattiene i dati finché non viene pagato un riscatto. ARP/AI offre il rilevamento ransomware in tempo reale basato su:

- Identificazione dei dati in entrata come crittografati o non crittografati.
- Analisi che rilevano:
  - **Entropia**: Una valutazione della casualità dei dati in un file
  - **Tipi di estensione del file**: Un'estensione non conforme al normale tipo di estensione
  - **IOPS dei file**: Un picco nell'attività anomala dei volumi con crittografia dei dati

ARP/AI è in grado di rilevare la diffusione della maggior parte degli attacchi ransomware dopo che è stato crittografato solo un numero limitato di file, di intervenire automaticamente per proteggere i dati e di avvisare l'utente che si sta verificando un sospetto attacco.

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

Modalità di apprendimento e attive

ARP/AI opera prima in *modalità di apprendimento* e poi passa automaticamente in *modalità attiva*.

- **Modalità di apprendimento**: quando si abilita ARP/AI, viene eseguito in *modalità di apprendimento*. In modalità di apprendimento, il file system FSx for ONTAP sviluppa un profilo di avviso basato sulle aree analitiche: entropia, tipi di estensione file e IOPS file. Dopo che il file system ha eseguito ARP/AI in modalità di apprendimento per un tempo sufficiente a valutare le caratteristiche del carico di lavoro, Workload Factory passa automaticamente ad ARP/AI in *modalità attiva* e inizia a proteggere i dati.
- **Modalità attiva**: dopo che ARP/AI passa alla *modalità attiva*, FSx for ONTAP crea snapshot ARP/AI per proteggere i dati se viene rilevata una minaccia.

  In modalità attiva, se un'estensione del file è contrassegnata come anomala, è necessario valutare l'avviso. Puoi agire sull'avviso per proteggere i tuoi dati o contrassegnarlo come falso positivo. Se si contrassegna un avviso come falso positivo, il profilo di avviso viene aggiornato. Ad esempio, se l'avviso viene attivato da una nuova estensione di file e l'utente contrassegna l'avviso come falso positivo, non verrà visualizzato alcun avviso alla successiva visualizzazione dell'estensione del file.

  I volumi FlexVol contenenti un dispositivo a blocchi avviano ARP/AI in modalità attiva.

Configurazioni non supportate

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

- Volumi iSCSI

- Volumi NVMe

Abilita ARP/AI per un file system o un volume

L'abilitazione di ARP/AI per un file system aggiunge automaticamente la protezione a tutti i volumi NAS esistenti e ai volumi NAS (NFS/SMB) appena creati. È anche possibile abilitare ARP/AI per singoli volumi.

Dopo aver abilitato ARP/AI, se si verifica un attacco e si identifica che è reale, Workload Factory imposta automaticamente una policy di snapshot che esegue fino a sei snapshot ogni quattro ore. Ogni snapshot viene bloccato per 2-5 giorni.

Prima di iniziare

Per abilitare ARP/AI per un file system o un volume, è necessario associare un collegamento. "Scopri come associare un collegamento esistente o come creare e associare un nuovo collegamento" . Dopo aver associato il collegamento, tornare a questa operazione.

Abilita ARP/AI per un file system

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx per ONTAP**, selezionare il menu azioni del file system per abilitare ARP/AI, quindi selezionare **Gestisci**.
5. In Informazioni, seleziona l'icona della matita accanto a **Protezione autonoma da ransomware**. L'icona della matita appare accanto alla freccia quando il mouse passa sopra la riga **Protezione autonoma dal ransomware**.
6. Dalla pagina NetApp Autonomous Ransomware Protection with AI (ARP/AI), procedere come segue:
   a. Abilita o disabilita la funzionalità.
   b. **Creazione automatica di snapshot**: seleziona il numero massimo di snapshot da conservare e l'intervallo di tempo tra un'acquisizione e l'altra. L'impostazione predefinita è 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. Abilitare 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 automaticamente la scansione e rilevare le anomalie.
7. Accettare la dichiarazione per procedere.
8. Selezionare **Applica** per salvare le modifiche.

Abilita ARP/AI per un volume

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx per ONTAP**, selezionare il menu azioni del file system per abilitare ARP/AI, quindi selezionare **Gestisci**.
5. Dalla scheda Volumi, seleziona il menu azioni del volume per abilitare ARP/AI, quindi **Azioni di protezione dati** e infine **Gestisci ARP/AI**.
6. Nella finestra di dialogo Gestisci ARP/AI, procedere come segue:
   a. Abilita o disabilita la funzionalità.
   b. **Rilevamento**: facoltativamente, seleziona uno qualsiasi dei seguenti parametri per eseguire automaticamente la scansione e rilevare le anomalie.
7. Accettare la dichiarazione per procedere.
8. Selezionare **Applica** per salvare le modifiche.

Convalida degli attacchi ransomware

Determinare se un attacco è un falso allarme o un incidente ransomware autentico.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, seleziona il file system per cui convalidare gli attacchi ransomware.
5. Nella panoramica del file system, selezionare la scheda **volumi**.
6. Seleziona **analizza attacchi** dal riquadro Autonomous ransomware Protection.
7. Scarica il report sugli eventi di attacco per verificare se alcuni file o cartelle sono stati compromessi e decidere se si è verificato un attacco.
8. Se non si è verificato alcun attacco, selezionare **Falso allarme** per il volume nella tabella, quindi selezionare **Chiudi**
9. Se si è verificato un attacco, selezionare **attacco reale** per il volume nella tabella. Viene visualizzata la finestra di dialogo Ripristina dati volume compromessi. È possibile procedere immediatamente a oppure selezionare **Chiudi** e tornare a ripristina i tuoi daticompletare il processo di ripristino in un secondo momento.

Recuperare i dati dopo un attacco ransomware

Quando si sospetta un attacco, il sistema esegue un'istantanea del volume in quel momento e blocca tale copia. Se l'attacco viene confermato in un secondo momento, i file interessati o l'intero volume possono essere ripristinati utilizzando lo snapshot ARP/AI.

Gli snapshot bloccati non possono essere eliminati fino al termine del periodo di conservazione. Tuttavia, se in seguito decidi di contrassegnare l'attacco come falso positivo, la copia bloccata verrà eliminata.

Conoscendo i file interessati e il momento dell'attacco, è possibile recuperare in modo selettivo i file interessati da vari snapshot, anziché semplicemente riportare l'intero volume in uno degli snapshot.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, seleziona il file system per cui recuperare i dati.
5. Nella panoramica del file system, selezionare la scheda **volumi**.
6. Seleziona **analizza attacchi** dal riquadro Autonomous ransomware Protection.
7. Se si è verificato un attacco, selezionare **attacco reale** per il volume nella tabella.
8. Nella finestra di dialogo Ripristina dati volume compromessi, seguire le istruzioni per eseguire il ripristino a livello di file o a livello di volume. Nella maggior parte dei casi, i file vengono ripristinati piuttosto che in un intero volume.
9. Dopo aver completato il ripristino, selezionare **Chiudi**.

Risultato

I dati compromessi sono stati ripristinati.

Clonare un volume in NetApp Workload Factory

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

Il clone riflette lo stato corrente dei dati point-in-time. È inoltre possibile utilizzare i cloni per fornire agli utenti aggiuntivi l'accesso ai dati senza fornire loro l'accesso ai dati di produzione.

A proposito di questa attività

Il cloning dei volumi è supportato solo per i volumi FlexClone.

Quando viene clonato un volume, viene creato un volume scrivibile con riferimenti agli snapshot dal volume principale. La creazione dei cloni avviene in pochi secondi. I dati clonati non risiedono nel clone del volume, ma risiedono invece nel volume principale. Tutti i nuovi dati scritti sul volume dopo la creazione del clone risiedono sul clone.

Perché un volume clonato contenga tutti i dati del volume principale ed eventuali nuovi dati aggiunti al clone dopo la creazione, sarà necessario "dividere il clone" farlo dal volume principale. Inoltre, non puoi eliminare un volume principale se ha un clone. Prima di eliminare un volume principale, è necessario dividere un clone.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare **FSx per ONTAP**.
4. Da **FSx for ONTAP**, seleziona il menu azioni del file system FSx for ONTAP che contiene il volume da clonare, quindi seleziona **Gestisci**.
5. Dalla scheda Panoramica del file system, selezionare la scheda **volumi**.
6. Nella scheda Volumi, seleziona il menu delle azioni del volume da clonare.
7. Selezionare **azioni protezione dati**, quindi **Clona volume**.
8. Nella finestra di dialogo Clone volume (Clona volume), immettere un nome per il clone del volume.
9. Selezionare **Clone**.

Utilizzare i dati del cluster ONTAP locale in NetApp Workload Factory

Scopri e replica i dati ONTAP on-premise in NetApp Workload Factory in modo che possano essere utilizzati per arricchire le basi di conoscenza dell'intelligenza artificiale.

A proposito di questa attività

Per utilizzare i dati da un cluster ONTAP on-premise, dovrai prima rilevare il cluster ONTAP on-premise. Dopo aver scoperto un cluster ONTAP on-premise, puoi utilizzare i dati per uno dei seguenti casi di utilizzo.

Casi di utilizzo

Si noti che il caso di utilizzo principale per il carico di lavoro GenAI è al centro di questa serie di attività.

- **Workload Genai**: Replica dei dati dei volumi ONTAP on-premise in un file system FSX per ONTAP in modo che i dati possano essere utilizzati in "Arricchire le knowledge base dell'ai".
- **Backup e migrazione nel cloud**: I dati dei volumi ONTAP on-premise replicati in un file system FSX per ONTAP possono essere utilizzati come backup nel cloud.
- **Tiering dei dati**: Dopo la replica, è possibile eseguire il tiering dei dati del volume ONTAP on-premise con accesso meno frequente dal Tier di storage SSD al Tier di storage del pool di capacità.

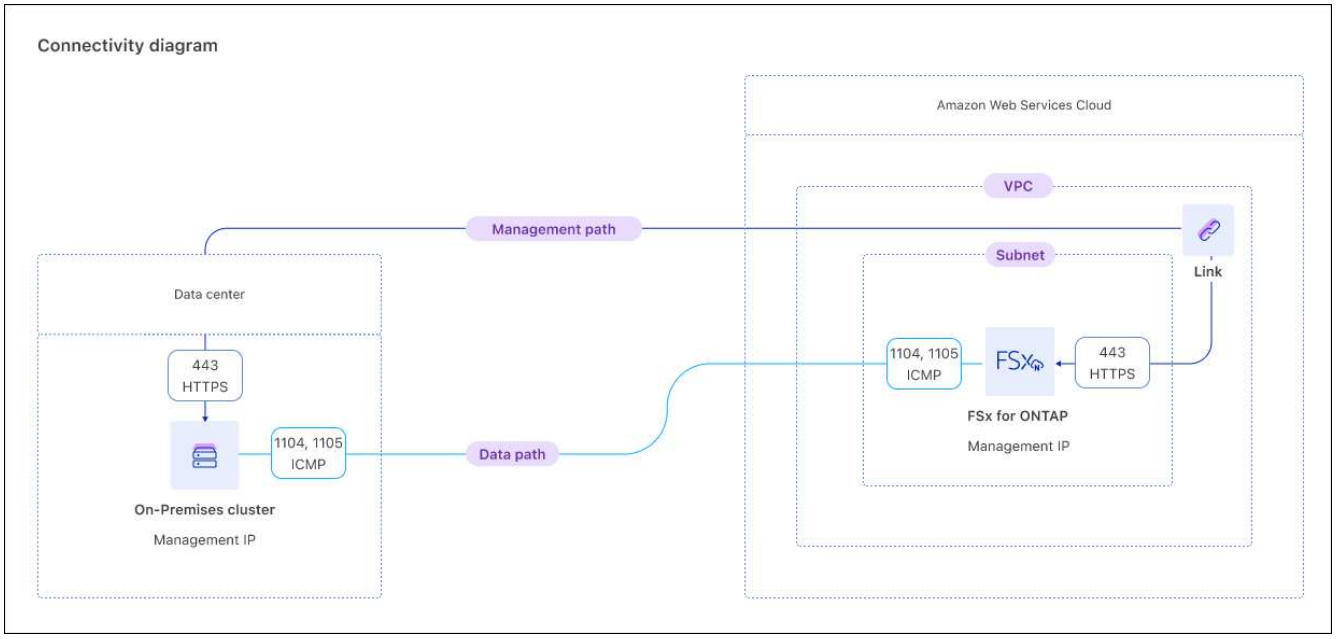
Scopri un cluster ONTAP on-premise

Scopri un cluster ONTAP locale in NetApp Workload Factory in modo da poter replicare i dati su un file system Amazon FSx for NetApp ONTAP .

Prima di iniziare

Prima di iniziare, assicurarsi di disporre dei seguenti elementi:

- Un file system FSX per ONTAP per la replica.
- Un link connesso da associare al cluster on-premise rilevato. Se non si dispone di un collegamento, è necessario "creane uno".
- Credenziali utente ONTAP con autorizzazioni richieste.
- ONTAP on-premise versione 9,8 e successive.
- Connettività come mostrato nello schema seguente.



Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu e quindi seleziona **Archiviazione**.
3. Selezionare la scheda **ONTAP on-premise**.

4. Selezionare **Discover**.
5. Esaminare i prerequisiti e selezionare **Avanti**.
6. Nella pagina Scopri ONTAP on-premise, fornire quanto segue in **Configurazione cluster**:
    a. **Link**: Seleziona un link. Il collegamento verrà associato al cluster locale per creare connettività tra il cluster e Workload Factory.

        Se non è stato creato un collegamento, seguire le istruzioni, quindi tornare a questa operazione e selezionare il collegamento.

    b. **Indirizzo IP del cluster**: Fornire l'indirizzo IP per il cluster ONTAP locale da replicare.
    c. **Credenziali ONTAP**: Inserisci le credenziali ONTAP per il cluster ONTAP on-premise. Assicurarsi che l'utente disponga delle autorizzazioni necessarie.
7. Selezionare **rilevamento** per avviare il processo di rilevamento.

Risultato

Il cluster ONTAP on-premise viene rilevato e ora viene visualizzato nella scheda **ONTAP on-premise**.

Ora puoi visualizzare i dati nel tuo cluster ONTAP on-premise e Replicare i dati in un file system FSX per ONTAP.

Replica dei dati dei volumi da un cluster ONTAP on-premise

Replica dei dati del volume da un cluster ONTAP on-premise in un file system FSX per ONTAP. Dopo la replica, i dati possono essere utilizzati per arricchire le knowledge base ai.

Prima di iniziare

- Devi rilevare un cluster ONTAP on-premise per replicare i dati dei suoi volumi.
- È necessario disporre di un file system FSX disponibile per ONTAP come destinazione della replica.
- Sia il cluster ONTAP on-premise che il file system FSX per ONTAP utilizzati per la relazione di replica devono avere un link associato. "Scopri come associare un collegamento esistente o come creare e associare un nuovo collegamento". Dopo l'associazione del collegamento, tornare a questa operazione.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu  e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare * ONTAP locale*.
4. Per trovare i volumi per VM di archiviazione, è possibile **selezionare VM di archiviazione** dal menu a discesa.
5. Selezionare uno o più volumi da replicare, quindi selezionare **Replica**.
6. Nella pagina Crea replica, in destinazione replica, specificare quanto segue:
    a. **FSX per il file system ONTAP**: Selezionare credenziali, area e FSX per il nome del file system ONTAP per il file system FSX per ONTAP di destinazione.
    b. **Nome VM di archiviazione**: Selezionare la VM di archiviazione dal menu a discesa.
    c. **Volume name**: Il nome del volume di destinazione viene generato automaticamente con il seguente formato `{OriginalVolumeName}_copy`. È possibile utilizzare il nome del volume generato

automaticamente o immettere un altro nome di volume.

d. **Dati di tiering**: Selezionare il criterio di tiering per i dati memorizzati nel volume di destinazione.
   - **Auto**: criterio di suddivisione in livelli predefinito quando si crea un volume utilizzando l'interfaccia utente Workload Factory FSx for ONTAP . Suddivide tutti i dati inattivi, inclusi i dati utente e gli snapshot, nel livello di archiviazione del pool di capacità per un periodo di tempo specifico.
   - **Solo Snapshot**: Esegue il tiering solo dei dati snapshot nel Tier di storage del pool di capacità.
   - **Nessuno**: Mantiene tutti i dati del volume nel Tier di storage primario.
   - **All**: Contrassegna tutti i dati utente e i dati snapshot come cold e li memorizza nel Tier di storage del pool di capacità.

     Tenere presente che alcune policy di tiering dispongono di un periodo di raffreddamento minimo associato che imposta il tempo, o *giorni di raffreddamento*, che i dati dell'utente in un volume devono rimanere inattivi per essere considerati "cold" e spostati nel Tier di storage del pool di capacità. Il periodo di raffreddamento inizia quando i dati vengono scritti sul disco.

Per ulteriori informazioni sulle policy di tiering dei volumi, fare riferimento a "Capacità di storage dei volumi"nella documentazione di AWS FSX per NetApp ONTAP.

a. **Velocità di trasferimento massima**: Selezionare **limitata** e immettere il limite massimo di trasferimento in MIB/s. In alternativa, selezionare **illimitato**.

   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 per ONTAP per i carichi di lavoro critici, ad esempio quelli utilizzati principalmente per il disaster recovery.

7. In Impostazioni di replica, specificare quanto segue:
   a. **Intervallo di replica**: Consente di selezionare la frequenza di trasferimento degli snapshot dal volume di origine al volume di destinazione.
   b. **Conservazione a lungo termine**: Facoltativamente, abilitare gli snapshot per la conservazione a lungo termine.

      Se si attiva la conservazione a lungo termine, selezionare un criterio esistente o creare un nuovo criterio per definire gli snapshot da replicare e il numero da conservare.

      - Per un criterio esistente, selezionare **Scegli un criterio esistente**, quindi selezionare il criterio esistente dal menu a discesa.
      - Per un nuovo criterio, selezionare **Crea un nuovo criterio** e fornire quanto segue:
        - **Policy name**: Inserire un nome di policy.
        - **Snapshot policies**: Nella tabella, selezionare la frequenza del criterio di snapshot e il numero di copie da conservare. È possibile selezionare più criteri di snapshot.
8. Selezionare **Crea**.

Risultato

La relazione di replica viene visualizzata nella scheda **Relazioni di replica** nel file system FSX for ONTAP di destinazione.

Rimuovere un cluster ONTAP locale da NetApp Workload Factory

Rimuovere un cluster ONTAP locale da NetApp Workload Factory quando necessario.

Prima di iniziare

Prima di rimuovere il cluster, occorre "eliminare tutte le relazioni di replica esistenti"utilizzare tutti i volumi del cluster ONTAP on-premise, in modo che non rimangano relazioni interrotte.

Fasi

1. Accedere utilizzando uno dei "esperienze di console".
2. Seleziona il menu e quindi seleziona **Archiviazione**.
3. Dal menu Archiviazione, selezionare * ONTAP locale*.
4. Seleziona il cluster ONTAP on-premise da rimuovere.
5. Selezionare il menu azioni e selezionare **Rimuovi da Workload Factory**.

Risultato

Il cluster ONTAP locale viene rimosso da NetApp Workload Factory.

Proteggi i tuoi dati con un cyber vault

Un volume di cyber vault è un luogo di archiviazione isolato e sicuro utilizzato per archiviare copie di backup dei dati, proteggendoli da attacchi ransomware e altre minacce informatiche. Come parte della creazione del vault, creerai un volume del cyber vault, disabiliterai tutti i protocolli client e configurerai una relazione di replica tra il volume di origine e il volume del cyber vault, quindi creerai snapshot immutabili sul volume del cyber vault.

Cos'è un cyber vault?

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

Il cyber vault è un archivio dati "air-gapped", immutabile e indelebile, immune alle minacce che colpiscono la rete principale, come malware, ransomware o persino minacce interne. È possibile realizzare un caveau informatico con snapshot immutabili e indelebili.

I backup air-gapping che utilizzano metodi tradizionali comportano la creazione di spazio e la separazione fisica del supporto primario e secondario. Spostando i media fuori sede e/o interrompendo la connettività, i malintenzionati non hanno accesso ai dati. Ciò protegge i dati ma può comportare tempi di ripristino più lenti.

FSx per i cyber vault ONTAP

Amazon FSx for NetApp ONTAP è supportato come origine e destinazione del cyber vault.

Implementazione

Workload Factory fornisce assistenza nella creazione di un'architettura di cyber vault. Dopo aver contattato NetApp per esprimere il tuo interesse nell'implementazione di un cyber vault, uno specialista NetApp ti contatterà per discutere le tue esigenze.

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

Informazioni correlate

Per ulteriori informazioni sui cyber vault e su come impostare questa architettura, fare riferimento a "Documentazione del cyber vault ONTAP".