USA ONTAP per gestire i tuoi dati

ASA r2

NetApp
September 26, 2024

Sommario

USA ONTAP per gestire i tuoi dati

Dimostrazioni video sul sistema storage ASA R2

Guarda brevi video che dimostrano come utilizzare Gestione sistema di ONTAP per eseguire in modo rapido e semplice attività comuni sui tuoi sistemi storage ASA R2.

Configurare i protocolli SAN sul sistema ASA R2

"Trascrizione video"

Provisioning dello storage SAN sul sistema ASA R2

"Trascrizione video"

Replicare i dati su un cluster remoto da un sistema ASA R2

"Trascrizione video"

Gestione dello storage

Eseguire IL provisioning dello storage SAN ONTAP sui sistemi ASA R2

Durante il provisioning dello storage, è possibile consentire agli host SAN di leggere e scrivere dati nei sistemi storage ASA R2. Per il provisioning dello storage, è possibile utilizzare ONTAP System Manager per creare unità di storage, aggiungere initiator degli host e mappare l'host a un'unità di storage. Per attivare le operazioni di lettura/scrittura, è inoltre necessario eseguire le operazioni sull'host.

Creare unità di archiviazione

In un sistema ASA R2, un'unità di storage rende disponibile lo spazio di storage per gli host SAN per le operazioni sui dati. Un'unità di storage si riferisce a un LUN per gli host SCSI o a un namespace NVMe per gli host NVMe. Se il cluster è configurato per supportare gli host SCSI, viene richiesto di creare un LUN. Se il cluster è configurato per supportare gli host NVMe, viene richiesto di creare un namespace NVMe. Un'unità di archiviazione ASA R2 ha una capacità massima di 128TB GB.

Consulta la "NetApp Hardware Universe" per i limiti di storage più attuali per i sistemi ASA R2.

Gli iniziatori host vengono aggiunti e mappati all'unità di archiviazione come parte del processo di creazione dell'unità di archiviazione. È anche possibile "aggiungere iniziatori host"e "mappa"nelle unità di archiviazione dopo la creazione delle unità di archiviazione.

Fasi

1. In System Manager, selezionare **Storage**, quindi selezionare + Add .
2. Immettere un nome per la nuova unità di memorizzazione.
3. Immettere il numero di unità che si desidera creare.

   Se si creano più unità di archiviazione, ciascuna viene creata con la stessa capacità, sistema operativo host e mappatura host.

4. Immettere la capacità dell'unità di archiviazione, quindi selezionare il sistema operativo host.
5. Accettare la **mappatura host** selezionata automaticamente o selezionare un gruppo host diverso per l'unità di archiviazione a cui eseguire la mappatura.

   Host mapping si riferisce al gruppo host a cui verrà mappata la nuova unità di archiviazione. Se esiste un gruppo host preesistente per il tipo di host selezionato per la nuova unità di archiviazione, il gruppo host preesistente viene selezionato automaticamente per la mappatura dell'host. È possibile accettare il gruppo di host selezionato automaticamente per la mappatura host oppure selezionare un gruppo di host diverso.

   Se non esiste un gruppo di host preesistente per gli host in esecuzione sul sistema operativo specificato, ONTAP crea automaticamente un nuovo gruppo di host.

6. Se si desidera eseguire una delle seguenti operazioni, selezionare **altre opzioni** e completare la procedura richiesta.

Opzione	Fasi
Modificare il criterio di qualità del servizio (QoS) predefinito Questa opzione non è disponibile se in precedenza non è stato impostato il criterio QoS predefinito sulla Storage Virtual Machine (VM) su cui viene creata l'unità di storage.	a. In **archiviazione e ottimizzazione**, accanto a **qualità del servizio (QoS)**, selezionare . b. Selezionare un criterio QoS esistente.
Creare una nuova policy QoS	a. In **archiviazione e ottimizzazione**, accanto a **qualità del servizio (QoS)**, selezionare . b. Selezionare **Definisci nuovo criterio**. c. Immettere un nome per il nuovo criterio QoS. d. Impostare un limite per la qualità del servizio, una garanzia di qualità del servizio o entrambi. i. In alternativa, sotto **limite**, specificare un limite massimo di throughput, un limite massimo di IOPS o entrambi. L'impostazione di un throughput massimo e degli IOPS per un'unità di storage ne limita l'impatto sulle risorse di sistema, evitando così la degradazione delle performance dei carichi di lavoro critici. ii. In alternativa, in **garanzia**, immettere un throughput minimo, un IOPS minimo o entrambi. La definizione di un throughput minimo e di IOPS per un'unità di storage garantisce che soddisfi gli obiettivi di performance minimi, indipendentemente dalla richiesta dei carichi di lavoro concorrenti. e. Selezionare **Aggiungi**.

Opzione	Fasi
Aggiungere un nuovo host SCSI	a. In **informazioni host**, selezionare **SCSI** come protocollo di connessione. b. Selezionare il sistema operativo host. c. In **host Mapping**, selezionare **New hosts**. d. Selezionare **FC** o **iSCSI**. e. Selezionare gli iniziatori host esistenti o selezionare **Aggiungi iniziatore** per aggiungere un nuovo iniziatore host. Un esempio di WWPN FC valido è "01:02:03:04:0d:0b:0C:0A". Esempi di nomi di iniziatori iSCSI validi sono "iqn.1995-08.com.example:string" e "eui.0123456789ABCDEF".
Creare un nuovo gruppo host SCSI	a. In **informazioni host**, selezionare **SCSI** come protocollo di connessione. b. Selezionare il sistema operativo host. c. In **host Mapping**, selezionare **nuovo gruppo host**. d. Immettere un nome per il gruppo host, quindi selezionare gli host da aggiungere al gruppo.
Aggiunta di un nuovo sottosistema NVMe	a. In **informazioni host**, selezionare **NVMe** per il protocollo di connessione. b. Selezionare il sistema operativo host. c. In **host Mapping**, selezionare **nuovo sottosistema NVMe**. d. Immettere un nome per il sottosistema o accettare il nome predefinito. e. Immettere un nome per l'iniziatore. f. Se si desidera attivare l'autenticazione in banda o TLS (Transport Layer Security), selezionare ⌄; quindi selezionare le opzioni desiderate. L'autenticazione in-band consente un'autenticazione sicura bidirezionale e unidirezionale tra gli host NVMe e il sistema ASA R2. TLS crittografa tutti i dati inviati in rete tra gli host NVMe/TCP e il sistema ASA R2. g. Selezionare **Aggiungi iniziatore** per aggiungere altri iniziatori. L'NQN host deve essere formattato come <nqn.yyyy-mm> seguito da un nome di dominio completo. L'anno deve essere uguale o successivo al 1970. La lunghezza massima totale deve essere 223. Un esempio di iniziatore NVMe valido è nqn.2014-08.com.example:string

7. Selezionare **Aggiungi**.

Quali sono le prossime novità?

Le unità di storage vengono create e mappate agli host. È ora possibile "creare snapshot"proteggere i dati sul sistema ASA R2.

Per ulteriori informazioni

Ulteriori informazioni su "Modalità di utilizzo delle Storage Virtual Machine dei sistemi ASA R2".

Aggiungere iniziatori host

È possibile aggiungere nuovi iniziatori host al sistema ASA R2 in qualsiasi momento. Gli initiator rendono gli host idonei ad accedere alle unità di storage ed eseguire operazioni sui dati.

Prima di iniziare

Per replicare la configurazione host in un cluster di destinazione durante il processo di aggiunta degli initiator degli host, il cluster deve trovarsi in una relazione di replica. Facoltativamente, è possibile "creare una relazione di replica" dopo l'aggiunta dell'host.

Aggiungere initiator host per host SCSI o NVMe.

Host SCSI

Fasi

1. Selezionare **host**.
2. Selezionare **SCSI**, quindi + Add .
3. Immettere il nome host, selezionare il sistema operativo host e immettere una descrizione host.
4. Se si desidera replicare la configurazione host in un cluster di destinazione, selezionare **Replica configurazione host**, quindi selezionare il cluster di destinazione.

   Il cluster deve trovarsi in una relazione di replica per replicare la configurazione dell'host.

5. Aggiunta di host nuovi o esistenti.

Aggiungere nuovi host	Aggiungere host esistenti
a. Selezionare **nuovi host**. b. Selezionare **FC** o **iSCSI**, quindi selezionare gli iniziatori host. c. In alternativa, selezionare **Configura prossimità host**. La configurazione della prossimità con l'host consente a ONTAP di identificare il controller più vicino all'host per l'ottimizzazione del percorso dei dati e la riduzione della latenza. Ciò è applicabile solo se i dati sono stati replicati in una posizione remota. Se non è stata impostata la replica snapshot, non è necessario selezionare questa opzione. d. Se è necessario aggiungere nuovi iniziatori, selezionare **Aggiungi iniziatori**.	a. Selezionare **host esistenti**. b. Selezionare l'host che si desidera aggiungere. c. Selezionare **Aggiungi**.

6. Selezionare **Aggiungi**.

Quali sono le prossime novità?

Gli host SCSI vengono aggiunti al sistema ASA R2 ed è possibile mappare gli host alle unità di storage.

Host NVMe

Fasi

1. Selezionare **host**.
2. Selezionare **NVMe**, quindi selezionare + Add .
3. Immettere un nome per il sottosistema NVMe, selezionare il sistema operativo host e immettere una descrizione.
4. Selezionare **Aggiungi iniziatore**.

Quali sono le prossime novità?

Gli host NVMe vengono aggiunti al sistema ASA R2 e sarai pronto per mappare gli host alle unità di storage.

Creare gruppi di host

In un sistema ASA R2, un *gruppo host* è il meccanismo utilizzato per fornire agli host l'accesso alle unità di archiviazione. Un gruppo di host si riferisce a un igroup per host SCSI o a un sottosistema NVMe per host NVMe. Un host può vedere solo le unità di archiviazione mappate ai gruppi host a cui appartiene. Quando un gruppo host viene mappato a un'unità di archiviazione, gli host che sono membri del gruppo, sono quindi in grado di montare (creare directory e strutture di file su) l'unità di archiviazione.

I gruppi di host vengono creati automaticamente o manualmente quando si creano le unità di archiviazione. Per creare gruppi host prima o dopo la creazione dell'unità di archiviazione, è possibile utilizzare facoltativamente i seguenti passaggi.

Fasi

1. Da System Manager, selezionare **host**.
2. Selezionare gli host che si desidera aggiungere al gruppo host.

   Dopo aver selezionato il primo host, l'opzione da aggiungere a un gruppo di host viene visualizzata sopra l'elenco degli host.

3. Selezionare **Aggiungi al gruppo host**.
4. Cercare e selezionare il gruppo host a cui si desidera aggiungere l'host.

Quali sono le prossime novità?

È stato creato un gruppo host ed è ora possibile associarlo a un'unità di archiviazione.

Mappare l'unità di archiviazione a un host

Dopo aver creato le unità di storage ASA R2 e aver aggiunto gli initiator degli host, è necessario mappare gli host alle unità di storage per iniziare a fornire i dati. Le unità di archiviazione sono mappate agli host come parte del processo di creazione delle unità di archiviazione. È inoltre possibile mappare le unità di storage esistenti a host nuovi o esistenti in qualsiasi momento.

Fasi

1. Selezionare **archiviazione**.
2. Passare il mouse sul nome dell'unità di archiviazione che si desidera mappare.
3. Selezionare ⋮; quindi selezionare **Map to hosts**.
4. Selezionare gli host che si desidera mappare all'unità di archiviazione, quindi selezionare **Mappa**.

Quali sono le prossime novità?

L'unità di storage viene mappata agli host ed è possibile completare il processo di provisioning sugli host.

Provisioning completo dal lato host

Dopo aver creato le unità di storage, aggiunto gli initiator degli host e mappato le unità di storage, è necessario eseguire sugli host alcuni passaggi prima di poter leggere e scrivere i dati sul sistema ASA R2.

Fasi

1. Per FC e FC/NVMe, zone gli switch FC di WWPN.

   Utilizzare una zona per iniziatore e includere tutte le porte di destinazione in ciascuna zona.

2. Scopri la nuova unità di stoccaggio.
3. Inizializzare l'unità di archiviazione e creare un file system.
4. Verificare che l'host sia in grado di leggere e scrivere i dati sull'unità di archiviazione.

Quali sono le prossime novità?

Il processo di provisioning è stato completato ed è possibile iniziare a fornire i dati. È ora possibile "creare snapshot"proteggere i dati sul sistema ASA R2.

Per ulteriori informazioni

Per ulteriori informazioni sulla configurazione lato host, consultare la "Documentazione dell'host SAN ONTAP" per l'host specifico.

Clonazione dei dati sui sistemi di storage ASA R2

Il cloning dei dati crea copie delle unità di storage e dei gruppi di coerenza nel sistema ASA R2 usando ONTAP System Manager, che può essere utilizzato per lo sviluppo applicativo, il test, i backup, la migrazione dei dati o altre funzioni amministrative.

Clonare le unità di storage

Quando si clona un'unità di storage, si crea una nuova unità di storage sul sistema ASA R2 che è una copia point-in-time e scrivibile dell'unità di storage clonata.

Fasi

1. In System Manager, selezionare **Storage**.
2. Posizionare il puntatore del mouse sul nome dell'unità di archiviazione che si desidera clonare.
3. Selezionare ⋮; quindi selezionare **Clona**.
4. Accettare il nome predefinito per la nuova unità di archiviazione che verrà creata come clone o immetterne una nuova.
5. Selezionare il sistema operativo host.

   Per impostazione predefinita, viene creato un nuovo snapshot per il clone.

6. Se si desidera utilizzare uno snapshot esistente, creare un nuovo gruppo host o aggiungere un nuovo host, selezionare **altre opzioni**.

Opzione	Fasi
Utilizzare un'istantanea esistente	a. In **istantanea da clonare**, selezionare **Usa un snap-hot esistente**. b. Selezionare lo snapshot che si desidera utilizzare per il clone.
Creare un nuovo gruppo host	a. In **mappatura host**, selezionare **nuovo gruppo host**. b. Immettere un nome per il nuovo gruppo host, quindi selezionare gli iniziatori host da includere nel gruppo.

Opzione	Fasi
Aggiungere un nuovo host	a. In **mappatura host**, selezionare **nuovi host**. b. Immettere il nome a per il nuovo host, quindi selezionare **FC** o **iSCSI**. c. Selezionare gli iniziatori host dall'elenco degli iniziatori esistenti o selezionare **Aggiungi** per aggiungere nuovi iniziatori per l'host.

7. Selezionare **Clone**.

Quali sono le prossime novità?

È stata creata una nuova unità di archiviazione identica all'unità di archiviazione clonata. A questo punto, è possibile utilizzare la nuova unità di archiviazione in base alle esigenze.

Clonare i gruppi di coerenza

Quando si clona un gruppo di coerenza, si crea un nuovo gruppo di coerenza identico per struttura, unità di storage e dati al gruppo di coerenza clonato. Utilizza un clone del gruppo di coerenza per eseguire il test delle applicazioni o migrare i dati. Ad esempio, supponiamo che sia necessario migrare un workload di produzione da un gruppo di coerenza. Puoi clonare il gruppo di coerenza per creare una copia del workload di produzione per mantenere come backup fino al completamento della migrazione.

Il clone viene creato a partire da una snapshot del gruppo di coerenza che viene clonato. La snapshot utilizzata per il clone viene acquisita nel momento in cui il processo di cloning viene avviato per impostazione predefinita. È possibile modificare il comportamento predefinito per utilizzare uno snapshot preesistente.

Le mappature delle unità di archiviazione vengono copiate come parte del processo di clonazione. Le policy di Snapshot non vengono copiate come parte del processo di cloning.

Puoi creare cloni da gruppi di coerenza archiviati in locale sul sistema ASA R2 o da gruppi di coerenza replicati in posizioni remote.

Clonare utilizzando lo snapshot locale

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Sposta il mouse sul gruppo di coerenza da clonare.
3. Selezionare ⋮, quindi selezionare **Clona**.
4. Immettere un nome per il clone del gruppo di coerenza o accettare il nome predefinito.
5. Selezionare il sistema operativo host.
6. Se si desidera dissociare il clone dal gruppo di coerenza di origine e allocare spazio su disco, selezionare **Dividi clone**.
7. Se si desidera utilizzare uno snapshot esistente, creare un nuovo gruppo host o aggiungere un nuovo host per il clone, selezionare **altre opzioni**.

Opzione	Fasi
Utilizzare un'istantanea esistente	a. In **istantanea da clonare**, selezionare **Usa uno snapshot esistente**. b. Selezionare lo snapshot che si desidera utilizzare per il clone.
Creare un nuovo gruppo host	a. In **mappatura host**, selezionare **nuovo gruppo host**. b. Immettere un nome per il nuovo gruppo host, quindi selezionare gli iniziatori host da includere nel gruppo.
Aggiungere un nuovo host	a. In **mappatura host**, selezionare **nuovi host**. b. Immettere il nome del nuovo nome host, quindi selezionare **FC** o **iSCSI**. c. Selezionare gli iniziatori host dall'elenco degli iniziatori esistenti o selezionare **Aggiungi iniziatore** per aggiungere nuovi iniziatori per l'host.

8. Selezionare **Clone**.

Clona utilizzando la snapshot remota

Fasi

1. In System Manager, selezionare **protezione > Replica**.
2. Passare il mouse sopra la **sorgente** che si desidera clonare.
3. Selezionare ⋮, quindi selezionare **Clona**.
4. Selezionare il cluster di origine e la VM di storage, quindi immettere un nome per il nuovo gruppo di coerenza o accettare il nome predefinito.
5. Selezionare l'istantanea da clonare, quindi selezionare **Clona**.

Quali sono le prossime novità?

È stato clonato un gruppo di coerenza dalla posizione remota. Il nuovo gruppo di coerenza è disponibile a livello locale sul sistema ASA R2 da utilizzare in base alle necessità.

Quali sono le prossime novità?

Per proteggere i dati è necessario ricorrere "creare snapshot" al gruppo di coerenza clonato.

Modifica delle unità di storage sui sistemi di storage ASA R2

Per ottimizzare le performance sul sistema ASA R2, potrebbe essere necessario modificare le unità di storage per aumentarne la capacità, aggiornare le policy di qualità del servizio o modificare gli host mappati alle unità. Ad esempio, se un nuovo workload dell'applicazione critica viene aggiunto a un'unità di storage esistente, potrebbe essere necessario modificare la policy di qualità del servizio applicata all'unità di storage per supportare il livello di performance necessario per la nuova applicazione.

Aumentare la capacità

Aumentare le dimensioni di un'unità di archiviazione prima che raggiunga la capacità massima per evitare una perdita di accesso ai dati che può verificarsi se l'unità di archiviazione esaurisce lo spazio scrivibile. La capacità di un'unità di archiviazione può essere aumentata a 128 TB, ovvero la dimensione massima consentita da ONTAP.

Modificare le mappature dell'host

Modificare gli host mappati a un'unità di storage per agevolare il bilanciamento dei carichi di lavoro o la riconfigurazione delle risorse di sistema.

Modificare il criterio QoS

Le policy di qualità del servizio garantiscono che le performance dei carichi di lavoro critici non vengano degradate da carichi di lavoro concorrenti. È possibile utilizzare i criteri QoS per impostare un throughput di QoS *Limit* e un throughput di QoS *Guarantee*.

- Limite di throughput della QoS

  Il throughput della QoS *Limit* limita l'impatto di un carico di lavoro sulle risorse di sistema limitando il throughput del carico di lavoro a un numero massimo di IOPS o Mbps o IOPS e Mbps.

- Garanzia di throughput di QoS

  Il throughput della QoS *garanzia* garantisce che i carichi di lavoro critici soddisfino gli obiettivi minimi di throughput, indipendentemente dalla richiesta da parte dei carichi di lavoro concorrenti, garantendo che il throughput per il carico di lavoro critico non scenda al di sotto di un numero minimo di IOPS o Mbps o IOPS e Mbps.

Fasi

1. In System Manager, selezionare **Storage**.
2. Passare il mouse sul nome dell'unità di archiviazione che si desidera modificare.
3. Selezionare ⋮; quindi selezionare **Modifica**.
4. Aggiorna i parametri delle unità di storage in base alle tue esigenze per aumentare la capacità, modificare i criteri di QoS e aggiornare la mappatura degli host.

Quali sono le prossime novità?

Se è stata aumentata la dimensione dell'unità di archiviazione, è necessario eseguire nuovamente la scansione dell'unità di archiviazione sull'host per consentire all'host di riconoscere la modifica delle dimensioni.

Eliminazione delle unità di storage sui sistemi di storage ASA R2

Eliminare un'unità di archiviazione se non è più necessario mantenere i dati contenuti nell'unità. L'eliminazione delle unità di archiviazione non più necessarie può consentire di liberare spazio per altre applicazioni host.

Prima di iniziare

Se l'unità di archiviazione che si desidera eliminare si trova in un gruppo di coerenza che si trova nella relazione di replica, è necessario "rimuovere l'unità di archiviazione dal gruppo di coerenza" prima di eliminarla.

Fasi

1. In System Manager, selezionare **Storage**.
2. Passare il mouse sul nome dell'unità di archiviazione che si desidera eliminare.
3. Selezionare ⋮; quindi selezionare **Elimina**.
4. Confermare che l'eliminazione non può essere annullata.
5. Selezionare **Delete** (Elimina).

Quali sono le prossime novità?

È possibile utilizzare lo spazio liberato dall'unità di archiviazione eliminata alle "aumentare le dimensioni"unità di archiviazione che richiedono capacità aggiuntiva.

Limiti di archiviazione di ASA R2

Per performance, configurazione e supporto ottimali devi conoscere i limiti di storage di ASA R2.

I sistemi ASA R2 supportano quanto segue:

Numero massimo di nodi per cluster	2
Dimensioni massime dell'unità di archiviazione	128 TB

Per ulteriori informazioni

Per un elenco completo dei limiti di archiviazione più recenti di ASA R2, vedere "NetApp Hardware Universe".

Proteggi i tuoi dati

Crea snapshot per eseguire il backup dei dati sui sistemi storage ASA R2

Per eseguire il backup dei dati sul sistema ASA R2, è necessario creare uno snapshot. Puoi utilizzare ONTAP System Manager per creare una snapshot manuale di una singola unità di storage o per creare un gruppo di coerenza e pianificare snapshot automatiche di più unità di storage contemporaneamente.

Passaggio 1: Se si desidera, creare un gruppo di coerenza

Un gruppo di coerenza è un insieme di unità di archiviazione gestite come una singola unità. Crea gruppi di coerenza per semplificare la gestione dello storage e la data Protection per i carichi di lavoro delle applicazioni su più unità di storage. Ad esempio, si supponga di disporre di un database composto da 10 unità di archiviazione in un gruppo di coerenza ed è necessario eseguire il backup dell'intero database. Invece di eseguire il backup di ciascuna unità di storage, è possibile eseguire il backup dell'intero database semplicemente aggiungendo la protezione dei dati snapshot al gruppo di coerenza.

Creare un gruppo di coerenza utilizzando nuove unità di archiviazione o un gruppo di coerenza utilizzando le unità di archiviazione esistenti.

Utilizzare nuove unità di conservazione

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Selezionare + Add ; quindi selezionare **utilizzo di nuove unità di memorizzazione**.
3. Immettere un nome per la nuova unità di archiviazione, il numero di unità e la capacità per unità.

   Se si creano più unità, ciascuna viene creata con la stessa capacità e lo stesso sistema operativo host. Per assegnare una capacità diversa a ciascuna unità, selezionare **altre opzioni**, quindi selezionare **Aggiungi una capacità diversa**.
4. Selezionare il sistema operativo host e la mappatura dell'host.
5. Selezionare **Aggiungi**.

Quali sono le prossime novità?

È stato creato un gruppo di coerenza contenente le unità di archiviazione che si desidera proteggere. A questo punto è possibile creare un'istantanea.

Utilizzare le unità di archiviazione esistenti

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Selezionare + Add ; quindi selezionare **utilizzando le unità di archiviazione esistenti**.
3. Immettere un nome per il gruppo di coerenza, quindi cercare e selezionare le unità di archiviazione che si desidera includere nel gruppo di coerenza.
4. Selezionare **Aggiungi**.

Quali sono le prossime novità?

È stato creato un gruppo di coerenza contenente le unità di archiviazione che si desidera proteggere. A questo punto è possibile creare un'istantanea.

Passaggio 2: Creare un'istantanea

Uno snapshot è una copia locale di sola lettura dei dati che è possibile utilizzare per ripristinare le unità di storage in un momento specifico.

Le istantanee possono essere create su richiesta o automaticamente a intervalli regolari in base a "policy e calendario di snapshot". La policy e la pianificazione degli snapshot specificano quando creare gli snapshot, il numero di copie da conservare, il nome e l'etichetta per la replica. Ad esempio, un sistema potrebbe creare

uno snapshot ogni giorno alle ore 12:10, conservare le due copie più recenti, assegnarle il nome "giornaliero" (allegato con un indicatore data e ora) ed etichettarle "giornalmente" per la replica.

Tipi di snapshot

È possibile creare uno snapshot on-demand di una singola unità di storage o di un gruppo di coerenza. È possibile creare istantanee automatiche di un gruppo di coerenza contenente più unità di archiviazione. Non è possibile creare istantanee automatiche di una singola unità di archiviazione.

- Snapshot on-demand

  È possibile creare un'istantanea su richiesta di un'unità di archiviazione in qualsiasi momento. Non è necessario che l'unità di storage sia membro di un gruppo di coerenza per essere protetta da uno snapshot on-demand. Se si crea uno snapshot on-demand di un'unità di storage che è membro di un gruppo di coerenza, le altre unità di storage nel gruppo di coerenza non vengono incluse nello snapshot on-demand. Se si crea uno snapshot on-demand di un gruppo di coerenza, tutte le unità di storage nel gruppo di coerenza vengono incluse nell'istantanea.

- Snapshot automatizzate

  Le snapshot automatizzate vengono create utilizzando policy di snapshot. Per applicare un criterio snapshot a un'unità di archiviazione per la creazione automatica di snapshot, l'unità di archiviazione deve essere un membro di un gruppo di coerenza. Se si applica un criterio snapshot a un gruppo di coerenza, tutte le unità di archiviazione nel gruppo di coerenza vengono protette con snapshot automatiche.

Creare un'istantanea di un gruppo di coerenza o di un'unità di archiviazione.

Istantanea di un gruppo di coerenza

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Passare il mouse sul nome del gruppo di coerenza che si desidera proteggere.
3. Selezionare ⋮ ; quindi selezionare **Proteggi**.
4. Se si desidera creare un'istantanea immediata su richiesta, in **protezione locale**, selezionare **Aggiungi istantanea adesso**.

   La protezione locale crea lo snapshot sullo stesso cluster contenente l'unità di archiviazione.

   a. Immettere un nome per l'istantanea o accettare il nome predefinito; quindi, facoltativamente, immettere un'etichetta SnapMirror.

      L'etichetta SnapMirror viene utilizzata dalla destinazione remota.

5. Se si desidera creare istantanee automatiche utilizzando un criterio snapshot, selezionare **Pianifica istantanee**.

   a. Selezionare un criterio di snapshot.

      Accettare il criterio snapshot predefinito, selezionare un criterio esistente o creare un nuovo criterio.

Opzione	Fasi
Selezionare un criterio snapshot esistente	Selezionare ⌄ accanto al criterio predefinito, quindi selezionare il criterio esistente che si desidera utilizzare.
Creare una nuova policy per le istantanee	i. Selezionare + Add , quindi immettere i parametri del criterio snapshot. ii. Selezionare **Aggiungi criterio**.

6. Se si desidera replicare le istantanee in un cluster remoto, in **protezione remota** selezionare **Replica in un cluster remoto**.
   a. Seleziona il cluster di origine e la VM di storage, quindi seleziona il criterio di replica.

      Il trasferimento iniziale dei dati per la replica viene avviato immediatamente per impostazione predefinita.

7. Selezionare **Salva**.

Istantanea dell'unità di conservazione

Fasi

1. In System Manager, selezionare **Storage**.
2. Passare il mouse sul nome dell'unità di archiviazione che si desidera proteggere.
3. Selezionare ⋮ ; quindi selezionare **Proteggi**. Se si desidera creare un'istantanea immediata su richiesta, in **protezione locale**, selezionare **Aggiungi istantanea adesso**.

   La protezione locale crea lo snapshot sullo stesso cluster contenente l'unità di archiviazione.

4. Immettere un nome per l'istantanea o accettare il nome predefinito; quindi, facoltativamente, immettere un'etichetta SnapMirror.

   L'etichetta SnapMirror viene utilizzata dalla destinazione remota.

5. Se si desidera creare istantanee automatiche utilizzando un criterio snapshot, selezionare **Pianifica istantanee**.

   a. Selezionare un criterio di snapshot.

      Accettare il criterio snapshot predefinito, selezionare un criterio esistente o creare un nuovo criterio.

Opzione	Fasi
Selezionare un criterio snapshot esistente	Selezionare ⌄ accanto al criterio predefinito, quindi selezionare il criterio esistente che si desidera utilizzare.
Creare una nuova policy per le istantanee	i. Selezionare + Add , quindi immettere i parametri del criterio snapshot. ii. Selezionare **Aggiungi criterio**.

6. Se si desidera replicare le istantanee in un cluster remoto, in **protezione remota** selezionare **Replica in un cluster remoto**.

   a. Seleziona il cluster di origine e la VM di storage, quindi seleziona il criterio di replica.

      Il trasferimento iniziale dei dati per la replica viene avviato immediatamente per impostazione predefinita.

7. Selezionare **Salva**.

Quali sono le prossime novità?

Ora che i tuoi dati sono protetti con snapshot, dovresti "configurare la replica snapshot"copiare i tuoi gruppi di coerenza in una posizione geograficamente remota per il backup e il disaster recovery.

Replica le snapshot su un cluster remoto dai sistemi storage ASA R2

La replica Snapshot è un processo in cui i gruppi di coerenza nel sistema ASA R2 vengono copiati in una posizione remota a livello geografico. Dopo la replica iniziale, le modifiche ai gruppi di coerenza vengono copiate nella posizione remota in base a un criterio di replica. È possibile utilizzare gruppi di coerenza replicati per il disaster recovery o la migrazione dei dati.

La replica Snapshot da un sistema di storage ASA R2 è supportata solo su un altro sistema di storage ASA R2. Non è possibile replicare gli snapshot da un sistema ASA R2 a un sistema ASA, AFF o FAS corrente.

Per impostare la replica Snapshot, è necessario stabilire una relazione di replica tra il sistema ASA R2 e la posizione remota. La relazione di replica è governata da un criterio di replica. Durante la configurazione del cluster viene creato un criterio predefinito per la replica di tutti gli snapshot. È possibile utilizzare il criterio

predefinito o, facoltativamente, crearne uno nuovo.

Passaggio 1: Creare una relazione peer cluster

Prima di poter proteggere i dati replicandoli in un cluster remoto, è necessario creare una relazione di peer cluster tra il cluster locale e quello remoto.

Fasi

1. Nel cluster locale, in System Manager, selezionare **Cluster > Impostazioni**.
2. In **Impostazioni cluster** accanto a **peer cluster** selezionare , quindi selezionare **Aggiungi un peer cluster**.
3. Selezionare **Lauch remote cluster**; in questo modo viene generata una passphrase da utilizzare per l'autenticazione con il cluster remoto.
4. Dopo aver generato la passphrase per il cluster remoto, incollarla sotto **Passphrase** nel cluster locale.
5. Selezionare + Add ; quindi immettere l'indirizzo IP dell'interfaccia di rete intercluster.
6. Selezionare **Initiate cluster peering**.

Quali sono le prossime novità?

Hai effettuato il peering per un cluster ASA R2 locale con un cluster remoto. È ora possibile creare una relazione di replica.

Passaggio 2: Se si desidera, creare un criterio di replica

Questo criterio definisce quando gli aggiornamenti eseguiti nel cluster ASA R2 vengono replicati nel sito remoto.

Fasi

1. In Gestione sistema, selezionare **protezione > Criteri**, quindi selezionare **Criteri di replica**.
2. Selezionare + Add .
3. Immettere un nome per il criterio di replica o accettare il nome predefinito, quindi immettere una descrizione.
4. Selezionare **ambito criterio**.

   Se si desidera applicare il criterio di replica all'intero cluster, selezionare **Cluster**. Se si desidera applicare il criterio di replica solo alle unità di archiviazione in una VM di archiviazione specifica, selezionare **VM di archiviazione**.

5. Selezionare il **tipo di criterio**.

Opzione	Fasi
Copiare i dati nel sito remoto dopo che sono stati scritti nell'origine.	a. Selezionare **asincrono**. b. In **Trasferisci snapshot dall'origine**, accettare la pianificazione di trasferimento predefinita o selezionarne una diversa. c. Selezionare per trasferire tutte le istantanee o per creare regole per determinare quali istantanee trasferire. d. Facoltativamente, attivare la compressione di rete.

Opzione	Fasi
Scrivere i dati contemporaneamente sui siti di origine e remoti.	a. Selezionare **sincrono**.

6. Selezionare **Salva**.

Quali sono le prossime novità?

È stato creato un criterio di replica e ora è possibile creare una relazione di replica tra il sistema ASA R2 e la posizione remota.

Per ulteriori informazioni

Ulteriori informazioni su "Macchine virtuali di storage per l'accesso dei client".

Fase 3: Creare una relazione di replica

Una relazione di replica snapshot stabilisce una connessione tra il sistema ASA R2 e una posizione remota in modo da poter replicare i gruppi di coerenza in un cluster remoto. È possibile utilizzare gruppi di coerenza replicati per il disaster recovery o per la migrazione dei dati.

Per una protezione contro gli attacchi ransomware, quando configuri un rapporto di replica, puoi selezionare di bloccare gli snapshot di destinazione. Gli snapshot bloccati non possono essere eliminati accidentalmente o in modo pericoloso. Puoi utilizzare snapshot bloccate per ripristinare i dati se un'unità di storage viene compromessa da un attacco ransomware.

Prima di iniziare

Se si desidera bloccare gli snapshot di destinazione, è necessario "Inizializzare il clock di conformità snapshot" prima creare la relazione di replica.

Creare una relazione di replica con o senza snapshot di destinazione bloccati.

Con istantanee bloccate

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Selezionare un gruppo di coerenza.
3. Selezionare ⋮; quindi selezionare **Proteggi**.
4. In **protezione remota**, selezionare **Replica in un cluster remoto**.
5. Selezionare **criterio di replica**.

   È necessario selezionare un criterio di replica *vault*.

6. Selezionare **Impostazioni destinazione**.
7. Selezionare **Blocca istantanee di destinazione per impedire l'eliminazione**
8. Immettere il periodo di conservazione dei dati massimo e minimo.
9. Per ritardare l'avvio del trasferimento dati, deselezionare **Avvia trasferimento immediatamente**.

   Il trasferimento iniziale dei dati inizia immediatamente per impostazione predefinita.

10. In alternativa, per ignorare la pianificazione di trasferimento predefinita, selezionare **Impostazioni destinazione**, quindi selezionare **Sovrascrivi pianificazione trasferimento**.

    Il programma di trasferimento deve essere di almeno 30 minuti per essere supportato.

11. Selezionare **Salva**.

Senza istantanee bloccate

Fasi

1. In System Manager, selezionare **protezione > Replica**.
2. Selezionare per creare la relazione di replica con la destinazione locale o l'origine locale.

Opzione	Fasi
Destinazioni locali	a. Selezionare **Destinazioni locali**, quindi selezionare Replicate. b. Cercare e selezionare il gruppo di coerenza di origine. Il gruppo di coerenza *source* fa riferimento al gruppo di coerenza del cluster locale che si desidera replicare.

Opzione	Fasi
Fonti locali	a. Selezionare **origini locali**, quindi selezionare Replicate . b. Cercare e selezionare il gruppo di coerenza di origine. Il gruppo di coerenza *source* fa riferimento al gruppo di coerenza del cluster locale che si desidera replicare. c. In **destinazione di replica**, selezionare il cluster in cui eseguire la replica, quindi selezionare la VM di archiviazione.

3. Selezionare un criterio di replica.
4. Per ritardare l'avvio del trasferimento dati, selezionare **Impostazioni destinazione**, quindi deselezionare **Avvia immediatamente trasferimento**.

   Il trasferimento iniziale dei dati inizia immediatamente per impostazione predefinita.

5. In alternativa, per ignorare la pianificazione di trasferimento predefinita, selezionare **Impostazioni destinazione**, quindi selezionare **Sovrascrivi pianificazione trasferimento**.

   Il programma di trasferimento deve essere di almeno 30 minuti per essere supportato.

6. Selezionare **Salva**.

Quali sono le prossime novità?

Una volta creati un criterio e una relazione di replica, il trasferimento iniziale dei dati inizia come definito nel criterio di replica. Se si desidera, è possibile verificare il failover della replica per verificare se il sistema ASA R2 non è in linea.

Passaggio 4: Verifica del failover della replica

In alternativa, convalida la possibilità di fornire con successo dati da unità di storage replicate su un cluster remoto se il cluster di origine non è in linea.

Fasi

1. In System Manager, selezionare **protezione > Replica**.
2. Passare il mouse sulla relazione di replica che si desidera verificare, quindi selezionare ⋮.
3. Selezionare **Test failover**.
4. Immettere le informazioni di failover, quindi selezionare **Test failover**.

Quali sono le prossime novità?

Ora che i dati sono protetti con la replica snapshot per il disaster recovery, è necessario che "esegui la crittografia dei dati inutilizzati"non possano essere letti se un disco nel sistema ASA R2 viene riutilizzato, restituito, smarrito o rubato.

Proteggi le applicazioni Kubernetes sui sistemi storage ASA R2

Utilizza Astra Control Center per proteggere le applicazioni Kubernetes. Astra Control Center ti consente di migrare applicazioni e dati da un cluster Kubernetes all'altro, replicare le applicazioni in un sistema remoto usando la tecnologia NetApp SnapMirror e clonare le applicazioni dallo staging alla produzione.

Per ulteriori informazioni

"Scopri di più sulla protezione delle applicazioni Kubernetes utilizzando Astra Control".

Ripristina i dati sui sistemi storage ASA R2

I dati di un gruppo di coerenza o di un'unità di archiviazione protetta da snapshot possono essere ripristinati in caso di perdita o danneggiamento.

Ripristinare un gruppo di coerenza

Il ripristino di un gruppo di coerenza sostituisce i dati di tutte le unità di archiviazione del gruppo di coerenza con i dati di uno snapshot. Le modifiche apportate alle unità di archiviazione dopo la creazione dello snapshot non vengono ripristinate.

È possibile ripristinare un gruppo di coerenza da uno snapshot locale o remoto.

Ripristino da uno snapshot locale

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Fare doppio clic sul gruppo di coerenza contenente i dati da ripristinare.

   Viene visualizzata la pagina dei dettagli del gruppo di coerenza.
3. Selezionare **istantanee**.
4. Selezionare l'istantanea che si desidera ripristinare, quindi selezionare ⋮.
5. Selezionare **Ripristina gruppo di coerenza da questa istantanea**, quindi selezionare **Ripristina**.

Ripristino da un'istantanea remota

Fasi

1. In System Manager, selezionare **protezione > Replica**.
2. Selezionare **Destinazioni locali**.
3. Selezionare la **origine** che si desidera ripristinare, quindi selezionare ⋮.
4. Selezionare **Restore** (Ripristina).
5. Seleziona il cluster, la VM di storage e il gruppo di coerenza in cui desideri ripristinare i dati.
6. Selezionare lo snapshot da cui si desidera eseguire il ripristino.
7. Quando richiesto, immettere "Ripristina", quindi selezionare **Ripristina**.

Risultato

Il gruppo di coerenza viene ripristinato al punto temporale dello snapshot utilizzato per il ripristino.

Ripristinare un'unità di archiviazione

Il ripristino di un'unità di archiviazione sostituisce tutti i dati presenti nell'unità di archiviazione con i dati di uno snapshot. Le modifiche apportate all'unità di archiviazione dopo la creazione dell'istantanea non vengono ripristinate.

Fasi

1. In System Manager, selezionare **Storage**.
2. Fare doppio clic sull'unità di archiviazione contenente i dati da ripristinare.

   Viene visualizzata la pagina dei dettagli dell'unità di archiviazione.

3. Selezionare **istantanee**.
4. Selezionare lo snapshot che si desidera ripristinare.
5. Selezionare ⋮; quindi selezionare **Ripristina**.
6. Selezionare **Usa questa istantanea per ripristinare l'unità di archiviazione**, quindi selezionare **Ripristina**.

Risultato

L'unità di archiviazione viene ripristinata al momento dell'istantanea utilizzata per il ripristino.

Gestione dei gruppi di coerenza ONTAP sui sistemi di storage ASA R2

Un gruppo di coerenza è un insieme di unità di archiviazione gestite come una singola unità. Utilizza gruppi di coerenza per una gestione semplificata dello storage. Ad esempio, si supponga di disporre di un database composto da 10 unità di archiviazione in un gruppo di coerenza ed è necessario eseguire il backup dell'intero database. Invece di eseguire il backup di ciascuna unità di storage, è possibile eseguire il backup dell'intero database semplicemente aggiungendo la protezione dei dati snapshot al gruppo di coerenza. Il backup delle unità di storage come gruppo di coerenza anziché singolarmente fornisce anche un backup coerente di tutte le unità, mentre il backup delle singole unità può potenzialmente creare incoerenze.

Aggiungi la data Protection delle snapshot a un gruppo di coerenza

Quando si aggiunge la protezione dei dati di snapshot a un gruppo di coerenza, le snapshot locali del gruppo di coerenza vengono acquisite a intervalli regolari in base a una pianificazione predefinita.

È possibile utilizzare snapshot "ripristinare i dati"persi o danneggiati.

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Passare il mouse sul gruppo di coerenza che si desidera proteggere.
3. Selezionare ⋮; quindi selezionare **Modifica**.
4. In **protezione locale**, selezionare **Pianifica istantanee**.
5. Selezionare un criterio di snapshot.

   Accettare il criterio snapshot predefinito, selezionare un criterio esistente o creare un nuovo criterio.

Opzione	Fasi
Selezionare un criterio snapshot esistente	Selezionare ⌄ accanto al criterio predefinito, quindi selezionare il criterio esistente che si desidera utilizzare.
Creare una nuova policy per le istantanee	a. Selezionare + Add , quindi immettere il nome del nuovo criterio. b. Selezionare l'ambito del criterio. c. In **piani di lavoro** selezionare + Add . d. Selezionare il nome visualizzato in **Nome pianificazione**; quindi selezionare ⌄ . e. Selezionare la pianificazione dei criteri. f. In **numero massimo di snapshot**, immettere il numero massimo di snapshot che si desidera conservare del gruppo di coerenza. g. Facoltativamente, in **SnapMirror label** (etichetta *) immettere un'etichetta SnapMirror. h. Selezionare **Salva**.

6. Selezionare **Modifica**.

Cosa succederà

Ora che i tuoi dati sono protetti con le snapshot, dovresti "configurare la replica snapshot"copiare i tuoi gruppi di coerenza in una posizione geograficamente remota per il backup e il disaster recovery.

Rimozione della data Protection delle snapshot da un gruppo di coerenza

Quando si rimuove la protezione dei dati snapshot da un gruppo di coerenza, gli snapshot vengono disattivati per tutte le unità di archiviazione nel gruppo di coerenza.

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Passare il mouse sul gruppo di coerenza che si desidera interrompere la protezione.
3. Selezionare ⋮; quindi selezionare **Modifica**.
4. In **protezione locale**, deselezionare Pianifica snapshot.
5. Selezionare **Modifica**.

Risultato

Gli snapshot non verranno acquisiti per nessuna delle unità di archiviazione nel gruppo di coerenza.

Aggiungere unità di archiviazione a un gruppo di coerenza

Espandere la quantità di storage gestita da un gruppo di coerenza aggiungendo unità di archiviazione al gruppo di coerenza.

È possibile aggiungere unità di archiviazione esistenti al gruppo di coerenza oppure creare nuove unità di archiviazione da aggiungere al gruppo di coerenza.

Aggiungere unità di archiviazione esistenti

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Passare il mouse sul gruppo di coerenza che si desidera espandere.
3. Selezionare ⋮; quindi selezionare **Espandi**.
4. Selezionare **utilizzando le unità di archiviazione esistenti**.
5. Selezionare le unità di archiviazione da aggiungere al gruppo di coerenza, quindi selezionare **Espandi**.

Aggiungere nuove unità di archiviazione

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Passare il mouse sul gruppo di coerenza che si desidera espandere.
3. Selezionare ⋮; quindi selezionare **Espandi**.
4. Selezionare **utilizzo di nuove unità di archiviazione**.
5. Immettere il numero di unità che si desidera creare e la capacità per unità.

   Se si creano più unità, ciascuna viene creata con la stessa capacità e lo stesso sistema operativo host. Per assegnare una capacità diversa a ciascuna unità, selezionare **Aggiungi una capacità diversa** per assegnare una capacità diversa a ciascuna unità.

6. Selezionare **Espandi**.

Cosa succederà

Dopo aver creato una nuova unità di archiviazione, è necessario "aggiungere iniziatori host" e "mappare l'unità di archiviazione appena creata a un host". L'aggiunta di host initiator rende gli host idonei ad accedere alle unità di storage ed eseguire operazioni sui dati. La mappatura di un'unità di archiviazione a un host consente all'unità di archiviazione di iniziare a fornire i dati all'host a cui viene mappato.

Quali sono le prossime novità?

Gli snapshot esistenti del gruppo di coerenza non includeranno le nuove unità di archiviazione aggiunte. È necessario che "creare uno snapshot immediato"il gruppo di coerenza protegga le nuove unità di archiviazione aggiunte fino a quando non viene creato automaticamente lo snapshot pianificato successivo.

Rimuovere un'unità di archiviazione da un gruppo di coerenza

È necessario rimuovere un'unità di archiviazione da un gruppo di coerenza se si desidera eliminare l'unità di archiviazione, se si desidera gestirla come parte di un gruppo di coerenza diverso o se non è più necessario proteggere i dati in essa contenuti. La rimozione di un'unità di archiviazione da un gruppo di coerenza interrompe la relazione tra l'unità di archiviazione e il gruppo di coerenza, ma non elimina l'unità di archiviazione.

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Fare doppio clic sul gruppo di coerenza da cui si desidera rimuovere un'unità di archiviazione.
3. Nella sezione **Panoramica**, in **unità di archiviazione**, selezionare l'unità di archiviazione che si desidera

rimuovere, quindi selezionare **Rimuovi dal gruppo di coerenza**.

Risultato

L'unità di archiviazione non è più un membro del gruppo di coerenza.

Cosa succederà

Se è necessario continuare la protezione dei dati per l'unità di archiviazione, aggiungere l'unità di archiviazione a un altro gruppo di coerenza.

Eliminare un gruppo di coerenza

Se non è più necessario gestire i membri di un gruppo di coerenza come una singola unità, è possibile eliminare il gruppo di coerenza. Dopo l'eliminazione di un gruppo di coerenza, le unità di storage presenti in precedenza nel gruppo rimangono attive nel cluster.

Prima di iniziare

Se il gruppo di coerenza che si desidera eliminare si trova in una relazione di replica, è necessario interrompere la relazione prima di eliminare il gruppo di coerenza. Dopo aver eliminato un gruppo di coerenza di replica, le unità di storage presenti nel gruppo di coerenza rimangono attive nel cluster e le relative copie replicate rimangono nel cluster remoto.

Fasi

1. In System Manager, selezionare **protezione > gruppi di coerenza**.
2. Passare il mouse sul gruppo di coerenza che si desidera eliminare.
3. Selezionare ⋮; quindi selezionare **Elimina**.
4. Accettare l'avviso, quindi selezionare **Elimina**.

Quali sono le prossime novità?

Dopo aver eliminato un gruppo di coerenza, le unità di archiviazione precedentemente presenti nel gruppo di coerenza non sono più protette dagli snapshot. Considerare l'aggiunta di queste unità di storage a un altro gruppo di coerenza per proteggerle dalla perdita di dati.

Gestire le policy e le pianificazioni di protezione dei dati ONTAP sui sistemi di storage ASA R2

Utilizza policy di Snapshot per proteggere i dati nei gruppi di coerenza in base a una pianificazione automatizzata. Utilizza le pianificazioni di criteri all'interno delle policy di snapshot per determinare la frequenza con cui vengono create le snapshot.

Creare una nuova pianificazione dei criteri di protezione

Una pianificazione dei criteri di protezione definisce la frequenza con cui viene eseguita una policy di snapshot. È possibile creare pianificazioni da eseguire a intervalli regolari in base a un numero di giorni, ore o minuti. Ad esempio, è possibile creare un programma da eseguire ogni ora o solo una volta al giorno. È inoltre possibile creare pianificazioni da eseguire a orari specifici in giorni specifici della settimana o del mese. Ad esempio, è possibile creare una pianificazione da eseguire alle 12:15am:00 il 20th di ogni mese.

La definizione di varie pianificazioni dei criteri di protezione consente di aumentare o diminuire la frequenza di snapshot per diverse applicazioni. Ciò consente di fornire un livello maggiore di protezione e un rischio minore di perdita di dati per i workload critici rispetto a quanto potrebbe essere necessario per i workload meno critici.

Fasi

1. Selezionare **protezione > Criteri**, quindi selezionare **Pianificazione**.
2. Selezionare + Add.
3. Immettere un nome per la pianificazione, quindi selezionare i parametri della pianificazione.
4. Selezionare **Salva**.

Quali sono le prossime novità?

Una volta creata una nuova pianificazione dei criteri, è possibile utilizzare la pianificazione appena creata all'interno delle policy per definire quando vengono creati gli snapshot.

Creare un criterio di snapshot

Una policy di snapshot definisce la frequenza di esecuzione delle snapshot, il numero massimo di snapshot consentite e la durata di conservazione.

Fasi

1. In Gestione sistema, selezionare **protezione > Criteri**, quindi selezionare **Criteri istantanea**.
2. Selezionare + Add.
3. Immettere un nome per il criterio snapshot.
4. Selezionare **Cluster** per applicare il criterio all'intero cluster. Selezionare **Storage VM** per applicare il criterio a una singola VM di storage.
5. Selezionare **Aggiungi pianificazione**, quindi immettere la pianificazione del criterio snapshot.
6. Selezionare **Aggiungi criterio**.

Quali sono le prossime novità?

Una volta creato un criterio snapshot, è possibile applicarlo a un gruppo di coerenza. Gli snapshot verranno acquisiti dal gruppo di coerenza in base ai parametri impostati nella policy di snapshot.

Applicare un criterio snapshot a un gruppo di coerenza

Applicare un criterio snapshot a un gruppo di coerenza per creare, conservare ed etichettare automaticamente gli snapshot del gruppo di coerenza.

Fasi

1. In Gestione sistema, selezionare **protezione > Criteri**, quindi selezionare **Criteri istantanea**.
2. Passare il mouse sul nome della policy di snapshot che si desidera applicare.
3. Selezionare ⋮; quindi selezionare **Applica**.
4. Selezionare i gruppi di coerenza a cui si desidera applicare il criterio snapshot, quindi selezionare **Applica**.

Quali sono le prossime novità?

Ora che i tuoi dati sono protetti con snapshot, dovresti "impostare una relazione di replica"copiare i tuoi gruppi di coerenza in una posizione geograficamente remota per il backup e il disaster recovery.

Modificare, eliminare o disattivare un criterio snapshot

Modificare un criterio snapshot per modificare il nome del criterio, il numero massimo di snapshot o l'etichetta SnapMirror. Eliminare un criterio per rimuoverlo e i relativi dati di backup dal cluster. Disattivare un criterio per interrompere temporaneamente la creazione o il trasferimento degli snapshot specificati dal criterio.

Fasi

1. In Gestione sistema, selezionare **protezione > Criteri**, quindi selezionare **Criteri istantanea**.
2. Passare il mouse sul nome del criterio snapshot che si desidera modificare.
3. Selezionare ⋮; quindi selezionare **Modifica**, **Elimina** o **Disabilita**.

Risultato

Il criterio dello snapshot è stato modificato, eliminato o disabilitato.

Modificare un criterio di replica

Modificare un criterio di replica per modificare la descrizione del criterio, la pianificazione del trasferimento e le regole. È inoltre possibile modificare il criterio per attivare o disattivare la compressione di rete.

Fasi

1. In Gestione sistema, selezionare **protezione > Criteri**.
2. Selezionare **Criteri di replica**.
3. Passare il mouse sul criterio di replica che si desidera modificare, quindi selezionare ⋮.
4. Selezionare **Modifica**.
5. Aggiornare il criterio, quindi selezionare **Salva**.

Risultato

Il criterio di replica è stato modificato.

Metti al sicuro i tuoi dati

Esegui la crittografia dei dati inutilizzati nei sistemi di storage ASA R2

Quando si crittografano i dati a riposo, non è possibile leggerli se un supporto storage viene riutilizzato, restituito, smarrito o rubato. Puoi utilizzare Gestione sistema di ONTAP per crittografare i dati a livello hardware e software per una protezione a doppio livello.

NetApp Storage Encryption (NSE) supporta la crittografia hardware utilizzando dischi con crittografia automatica (SED). I SEDS crittografano i dati durante la scrittura. Ogni SED contiene una chiave di crittografia univoca. I dati crittografati memorizzati sul SED non possono essere letti senza la chiave di crittografia del SED. I nodi che tentano di leggere da un SED devono essere autenticati per accedere alla chiave di crittografia del SED. I nodi vengono autenticati ottenendo una chiave di autenticazione da un gestore di chiavi, quindi presentando la chiave di autenticazione al SED. Se la chiave di autenticazione è valida, il SED fornirà al nodo la propria chiave di crittografia per accedere ai dati in esso contenuti.

Utilizza il gestore delle chiavi integrato in ASA R2 o un gestore delle chiavi esterno per fornire le chiavi di autenticazione ai tuoi nodi.

Oltre a NSE, puoi anche abilitare la crittografia software per aggiungere un altro livello di sicurezza ai dati.

Fasi

1. In Gestione di sistema, selezionare **Cluster > Impostazioni**.
2. Nella sezione **protezione**, in **crittografia**, selezionare **Configura**.
3. Configurare il gestore delle chiavi.

Opzione	Fasi
Configurare il gestore chiavi integrato	a. Selezionare **Onboard Key Manager** per aggiungere i server delle chiavi. b. Inserire una passphrase.
Configurare un gestore di chiavi esterno	a. Selezionare **Gestore chiavi esterno** per aggiungere i server chiavi. b. Selezionare + Add per aggiungere i server chiavi. c. Aggiungere i certificati CA del server KMIP. d. Aggiungere i certificati client KMIP.

4. Selezionare **crittografia a doppio livello** per abilitare la crittografia software.
5. Selezionare **Salva**.

Quali sono le prossime novità?

Ora che hai crittografato i tuoi dati a riposo, se stai utilizzando il protocollo NVMe/TCP, potrai "crittografare tutti i dati inviati in rete" collegare l'host NVMe/TCP e il sistema ASA R2.

Proteggiti dagli attacchi ransomware sui sistemi storage ASA R2

Per una protezione avanzata contro gli attacchi ransomware, replica le snapshot su un cluster remoto, quindi blocca le snapshot di destinazione per renderle a prova di manomissione. Gli snapshot bloccati non possono essere eliminati accidentalmente o in modo pericoloso. Puoi utilizzare snapshot bloccate per ripristinare i dati, se un'unità di storage viene mai compromessa da un attacco ransomware.

Inizializzare l'orologio SnapLock Compliance

Prima di poter creare snapshot a prova di manomissione, è necessario inizializzare il clock SnapLock Compliance sui cluster locali e di destinazione.

Fasi

1. Selezionare **Cluster > Overview** (Cluster > Panoramica).
2. Nella sezione **nodi**, selezionare **Inizializza orologio SnapLock Compliance**.
3. Selezionare **Inizializza**.
4. Verificare che l'orologio di conformità sia inizializzato.
   a. Selezionare **Cluster > Overview** (Cluster > Panoramica).
   b. Nella sezione **nodi**, selezionare ; quindi selezionare **SnapLock Compliance Clock**.

Cosa succederà?

Dopo aver inizializzato l'orologio SnapLock Compliance sui cluster locali e di destinazione, si è pronti per "creare una relazione di replica con gli snapshot bloccati".

Connessioni NVMe sicure sui tuoi sistemi storage ASA R2

Se stai utilizzando il protocollo NVMe, puoi configurare l'autenticazione in-band per migliorare la sicurezza dei tuoi dati. L'autenticazione in-band consente un'autenticazione sicura bidirezionale e unidirezionale tra gli host NVMe e il sistema ASA R2. L'autenticazione in banda è disponibile per tutti gli host NVMe. Se stai utilizzando il protocollo NVMe/TCP, puoi migliorare ulteriormente la sicurezza dei dati configurando TLS (Transport Layer Security) in modo da crittografare tutti i dati inviati in rete tra gli host NVMe/TCP e il sistema ASA R2.

Fasi

1. Selezionare **hosts**, quindi selezionare **NVMe**.
2. Selezionare + Add .
3. Immettere il nome host, quindi selezionare il sistema operativo host.
4. Immettere una descrizione dell'host, quindi selezionare la VM di storage da connettere all'host.
5. Selezionare ⌄ accanto al nome host.
6. Selezionare **autenticazione in banda**.
7. Se si utilizza il protocollo NVMe/TCP, selezionare **Richiedi TLS (Transport Layer Security)**.
8. Selezionare **Aggiungi**.

Risultato

La sicurezza dei dati è migliorata con l'autenticazione in banda e/o TLS.

Informazioni sul copyright

Informazioni sul marchio commerciale