Documentazione di ASA r2

ASA r2

NetApp
September 26, 2024

Sommario

Documentazione di ASA r2

Note di rilascio

Novità di ONTAP 9.16,0 per i sistemi ASA R2

Scopri le nuove funzionalità disponibili in ONTAP 9.16,0 per i sistemi ASA R2.

Piattaforme

Aggiornare	Descrizione
Nuove piattaforme	Sono disponibili i seguenti nuovi sistemi NetApp ASA R2. Queste piattaforme forniscono una soluzione hardware e software unificata che crea un'esperienza semplificata specifica delle esigenze dei clienti SAN. • ASA A1K • ASA A70 • ASA A90

System Manager

Aggiornare	Descrizione
"Supporto ottimizzato per i clienti solo SAN"	System Manager è ottimizzato per offrire supporto per la funzionalità SAN essenziale eliminando al tempo stesso la visibilità di funzionalità e funzioni non supportate negli ambienti SAN.

Gestione dello storage

Aggiornare	Descrizione
"Semplificazione della gestione dello storage"	I sistemi ASA R2 introducono l'utilizzo di unità di storage con gruppi di coerenza per una gestione semplificata dello storage. • Una *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. • *Un gruppo di coerenza* è un insieme di unità di archiviazione gestite come una singola unità.

Sicurezza dei dati

Aggiornare	Descrizione
"Gestore delle chiavi integrato e crittografia dual-layer"	I sistemi ASA R2 supportano un gestore delle chiavi integrato e crittografia dual-layer (hardware e software).

Inizia subito

Informazioni sui sistemi di storage ASA R2

I nuovi sistemi NetApp ASA R2 (ASA A1K, ASA A70 e ASA A90) forniscono una soluzione hardware e software unificata che crea un'esperienza semplificata specifica per le esigenze dei clienti solo SAN.

I sistemi ASA R2 supportano tutti i protocolli SAN (iSCSI, FC, NVMe/FC, NVMe/TCP) su una singola implementazione ha-Pair. I protocolli SCSI (iSCSI ed FC) utilizzano un'architettura Active-Active simmetrica per il multipathing, in modo che tutti i percorsi tra gli host e lo storage siano attivi/ottimizzati. I protocolli NVMe supportano percorsi diretti tra gli host e lo storage.

In un sistema ASA R2, il software ONTAP e System Manager sono ottimizzati per fornire il supporto per le funzionalità SAN essenziali, rimuovendo al contempo funzioni e funzioni non supportate in ambienti SAN.

I sistemi ASA R2 introducono l'utilizzo di unità di storage con gruppi di coerenza:

- Una *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.
- *Un gruppo di coerenza* è un insieme di unità di archiviazione gestite come una singola unità.

I sistemi ASA R2 utilizzano le unità di storage e i gruppi di coerenza per semplificare la gestione dello storage e la protezione dei dati. 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 archiviazione singolarmente, è possibile proteggere l'intero database eseguendo il backup del gruppo di coerenza.

Per contribuire a proteggere i tuoi dati da attacchi dannosi come furto o ransomware, i sistemi ASA R2 supportano un gestore delle chiavi integrato, crittografia a doppio livello, snapshot a prova di manomissione, autenticazione a più fattori e verifica con amministratori multipli.

I sistemi ASA R2 non supportano la combinazione di cluster con gli attuali sistemi ASA, AFF o FAS.

Per ulteriori informazioni

- Per ulteriori informazioni sul supporto e sulle limitazioni dei sistemi ASA R2, consultare "NetApp Hardware Universe".
- Ulteriori informazioni su "I nuovi sistemi ASA R2 rispetto ai sistemi ASA".
- Ulteriori informazioni su "NetApp ASA".

Guida rapida per i sistemi di storage ASA R2

Per iniziare a utilizzare il sistema ASA R2, è necessario installare i componenti hardware, configurare il cluster, impostare l'accesso ai dati dagli host al sistema di storage e eseguire il provisioning dello storage.

1 **Installazione e configurazione dell'hardware**

"Installazione e configurazione" Il tuo sistema ASA R2 e implementalo come coppia ha nel tuo ambiente

ONTAP.

2 **Configurare il cluster**

Utilizzare System Manager per guidare l'utente attraverso un processo rapido e semplice a "Configurazione del cluster ONTAP".

3 **Impostare l'accesso ai dati**

"Collegare il sistema ASA R2 ai client SAN".

4 **Provisioning dello storage**

"Eseguire il provisioning dello storage" Per iniziare a fornire dati ai client SAN.

Quali sono le prossime novità?

È ora possibile utilizzare System Manager per proteggere i dati di "creazione di istantanee".

Installazione del sistema ASA R2

Flusso di lavoro di installazione e setup per i sistemi storage ASA R2

Per installare e configurare il sistema ASA R2, è necessario esaminare i requisiti hardware, preparare il sito, installare e cablare i componenti hardware, accendere il sistema e configurare il cluster ONTAP.

1 **"Esaminare i requisiti di installazione dell'hardware"**

Leggi i requisiti hardware per installare il sistema storage ASA R2.

2 **"Preparazione per l'installazione del sistema di storage ASA R2"**

Per prepararsi all'installazione del sistema ASA R2, è necessario preparare il sito, verificare i requisiti ambientali ed elettrici e assicurarsi che lo spazio rack sia sufficiente. Quindi, disimballare l'apparecchiatura, confrontarne il contenuto con la distinta di imballaggio e registrare l'hardware per accedere ai vantaggi del supporto.

3 **"Installare l'hardware per il sistema di storage ASA R2"**

Per installare l'hardware, installare i kit guide per il sistema di archiviazione e gli scaffali, quindi installare e fissare il sistema di archiviazione nell'armadietto o nel rack per telecomunicazioni. Quindi, far scorrere i ripiani sulle guide. Infine, collegare i dispositivi di gestione dei cavi al retro del sistema di archiviazione per l'instradamento organizzato dei cavi.

4 **"Collegare i controller e gli shelf di storage per il sistema storage ASA R2"**

Per collegare l’hardware, collegare prima gli storage controller alla rete e poi i controller agli shelf di storage.

5 **"Accendere il sistema di archiviazione ASA R2"**

Prima di accendere i controller, accendere ogni shelf NS224 e assegnare un ID shelf univoco per garantire che ogni shelf sia identificato in modo univoco all’interno del setup.

Requisiti di installazione per i sistemi storage ASA R2

Esaminare l’attrezzatura necessaria e le precauzioni di sollevamento per il sistema di storage e i ripiani di stoccaggio ASA R2.

Attrezzatura necessaria per l’installazione

Per installare il sistema di storage ASA R2 sono necessari i seguenti strumenti e attrezzature.

- Accesso a un browser Web per configurare il sistema di archiviazione
- Cinturino da scariche elettrostatiche (ESD)
- Torcia
- Computer portatile o console con connessione USB/seriale
- Graffetta o penna a sfera con punta stretta per l’impostazione di NS224 ID scaffali
- Cacciavite Phillips n. 2

Precauzioni per il sollevamento

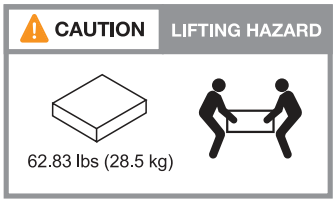
I sistemi storage ASA R2 e gli shelf di storage NS224 sono pesanti. Prestare attenzione durante il sollevamento e lo spostamento di questi elementi.

Pesi del sistema di archiviazione

Prendere le precauzioni necessarie quando si sposta o si solleva il sistema di archiviazione ASA R2.

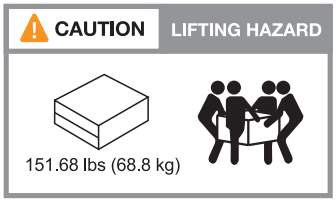
ASA A1K

Un sistema di storage ASA A1K può pesare fino a 28,5 kg (62,83 lb). Per sollevare l'impianto, utilizzare due persone o un sollevatore idraulico.



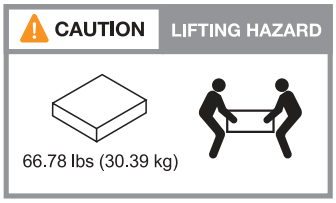
ASA A70 e ASA A90

Un sistema storage ASA A70 o ASA A90 può pesare fino a 68,8 kg (151,68 libbre). Per sollevare l'impianto, utilizzare quattro persone o un sollevatore idraulico.



Peso del ripiano

Un ripiano di stoccaggio NS224 può pesare fino a 30,29 kg (66,78 lb). Per sollevare il ripiano portaoggetti, utilizzare due persone o un sollevatore idraulico. Tenere tutti i componenti nel ripiano portaoggetti (anteriore e posteriore) per evitare di sbilanciare il peso del ripiano.



Informazioni correlate

- "Informazioni sulla sicurezza e avvisi normativi"

Quali sono le prossime novità?

Dopo aver esaminato i requisiti hardware, si "Preparazione dell'installazione del sistema di storage ASA R2".

Preparazione per l'installazione di un sistema di storage ASA R2

Preparare l'installazione del sistema di storage ASA R2 preparando il sito, disimballando le confezioni e confrontando il contenuto delle confezioni con il documento di trasporto e registrando il sistema per accedere ai vantaggi del supporto.

Fase 1: Preparare il sito

Per installare il sistema di storage ASA R2, verificare che il sito e il cabinet o il rack che si intende utilizzare soddisfino le specifiche per la configurazione.

Fasi

1. Utilizzare "NetApp Hardware Universe" per confermare che il sito soddisfi i requisiti ambientali ed elettrici del sistema di storage ASA R2.
2. Assicurarsi di disporre di uno spazio rack adeguato:
   - 4U in una configurazione ha per il sistema storage
   - 2U TB per ogni shelf storage NS224
3. Installare gli switch di rete necessari.

   Per le istruzioni di installazione e per informazioni sulla compatibilità, consultare la "Documentazione dello switch" "NetApp Hardware Universe" .

Fase 2: Disimballare le scatole

Dopo aver verificato che il sito e il cabinet o il rack che si intende utilizzare per il sistema di archiviazione ASA R2 soddisfino le specifiche richieste, disimballare tutte le confezioni e confrontare il contenuto con gli articoli presenti sul documento di trasporto.

Fasi

1. Aprire con attenzione tutte le scatole e disporre il contenuto in modo organizzato.
2. Confrontare il contenuto della confezione con l'elenco riportato sul documento di trasporto.

   È possibile ottenere la distinta di imballaggio eseguendo la scansione del codice QR sul lato del cartone di spedizione.

   I seguenti elementi sono alcuni dei contenuti che potrebbero essere visualizzati nelle caselle.

   Assicurarsi che tutto ciò che è contenuto nelle confezioni corrisponda all'elenco riportato sul documento di trasporto. In caso di discrepanze, annotarle per ulteriori azioni.

Hardware	Cavi	
• Pannello • Dispositivo di gestione dei cavi • Sistema storage • Kit guide con istruzioni (opzionale) • Shelf di storage	• Cavi Ethernet di gestione (cavi RJ-45) • Cavi di rete • Cavi di alimentazione • Cavi di stoccaggio (se è stato ordinato ulteriore spazio di archiviazione) • Cavo della porta seriale USB-C.	

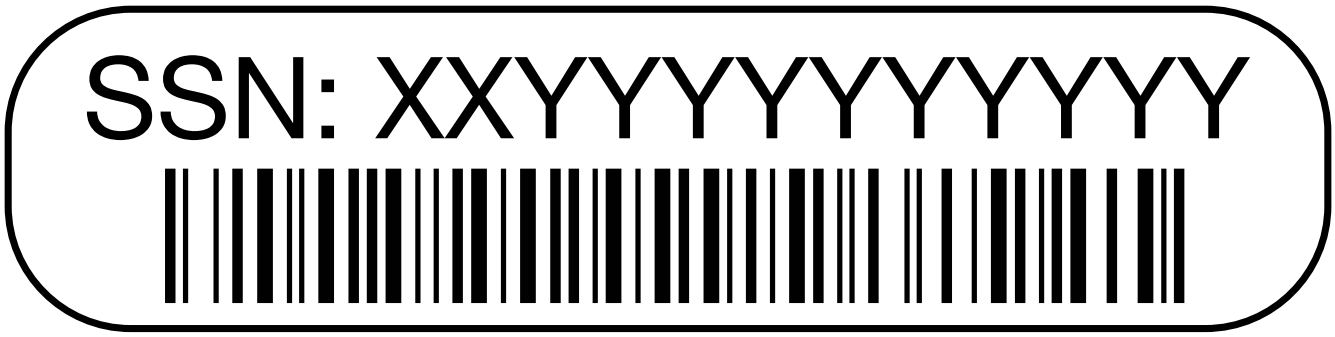
Fase 3: Registrare il sistema di archiviazione

Dopo aver verificato che il sito soddisfa i requisiti delle specifiche del sistema di storage ASA R2 e aver verificato di disporre di tutte le parti ordinate, è necessario registrare il sistema.

Fasi

1. Individua il numero di serie del tuo sistema storage.

Il numero è riportato sul documento di trasporto, nell'e-mail di conferma o sul modulo Gestione sistema del controller dopo averlo disimballato.



2. Andare a "Sito di supporto NetApp".
3. Stabilire se è necessario registrare il sistema storage:

Se sei un…	Attenersi alla procedura descritta di seguito…
Cliente NetApp esistente	a. Accedi con il tuo nome utente e la password. b. Selezionare **sistemi** > **i miei sistemi**. c. Verificare che il nuovo numero di serie sia elencato. d. In caso contrario, seguire le istruzioni per i nuovi clienti NetApp.
Nuovo cliente NetApp	a. Fare clic su **Registrati ora** e creare un account. b. Selezionare **sistemi** > **Registra sistemi**. c. Inserisci il numero di serie del sistema storage e i dettagli richiesti. Una volta approvata la registrazione, è possibile scaricare il software richiesto. Il processo di approvazione potrebbe richiedere fino a 24 ore.

Quali sono le prossime novità?

Dopo aver preparato l'installazione dell'hardware ASA R2, si "Installazione dell'hardware per il sistema di storage ASA R2".

Installare il sistema di storage ASA R2

Dopo aver preparato l'installazione del sistema di archiviazione ASA R2, installare l'hardware per il sistema. Per prima cosa, montare i kit guide. Quindi, installare e proteggere il sistema di archiviazione in un cabinet o in un rack per telecomunicazioni.

Prima di iniziare

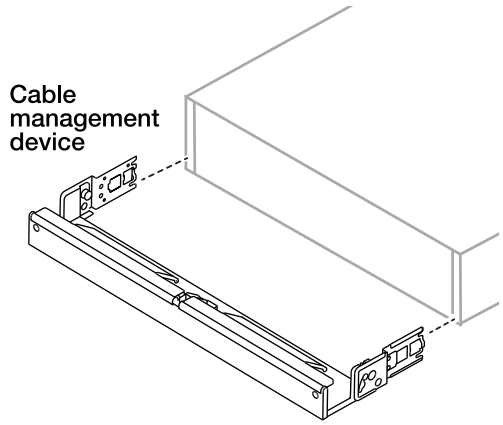
- Assicurarsi di avere le istruzioni fornite con il kit guida.
- Prestare attenzione ai problemi di sicurezza associati al peso del sistema di stoccaggio e del ripiano di stoccaggio.
- Tenere presente che il flusso d'aria attraverso il sistema di storage entra dalla parte anteriore dove sono installati il pannello o i cappucci terminali e fuoriesce dalla parte posteriore dove si trovano le porte.

Fasi

1. Installare i kit guide per il sistema di archiviazione e gli scaffali, secondo necessità, seguendo le istruzioni fornite con i kit.
2. Installare e fissare il sistema di archiviazione nell'armadietto o nel rack per telecomunicazioni:
   a. Posizionare il sistema di stoccaggio sulle guide al centro del cabinet o del rack per telecomunicazioni, quindi sostenere il sistema di archiviazione dal basso e farlo scorrere in posizione.
   b. Fissare il sistema di archiviazione all'armadietto o al rack per telecomunicazioni utilizzando le viti di montaggio incluse.
3. Installazione del ripiano:
   a. Posizionare la parte posteriore del ripiano sulle guide, quindi sostenere il ripiano dal basso e farlo scorrere nell'armadietto o nel rack per telecomunicazioni.

      Se si installano più shelf, posizionare il primo shelf direttamente sopra i controller. Posizionare il secondo shelf direttamente sotto i controller. Ripetere questo modello per tutti gli shelf di storage aggiuntivi.

   b. Fissare il ripiano all'armadietto o al rack per telecomunicazioni utilizzando le viti di montaggio in dotazione.
4. Collegare i dispositivi di gestione dei cavi al retro del sistema di archiviazione.



5. Fissare il frontalino alla parte anteriore del sistema di archiviazione.

Quali sono le prossime novità?

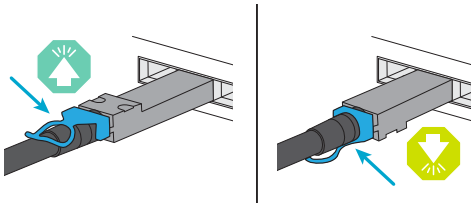
Dopo aver installato l'hardware per il sistema ASA R2, si "Collega i controller e gli shelf di storage del sistema ASA R2".

Collegare l'hardware per il sistema di storage ASA R2

Dopo aver installato l'hardware rack per il sistema di storage ASA R2, installare i cavi di rete per i controller e collegare i cavi tra i controller e gli shelf di storage.

Prima di iniziare

Per l'orientamento corretto della linguetta di estrazione del connettore del cavo, consultare la freccia degli schemi dei cavi.



- Quando si inserisce il connettore, si dovrebbe avvertire uno scatto in posizione; se non si sente uno scatto, rimuoverlo, capovolgere la testa del cavo e riprovare.
- Se si effettua il collegamento a uno switch ottico, inserire il ricetrasmettitore SFP (Small Form-factor pluggable) nella porta del controller prima di collegare il cavo alla porta.

Fase 1: Collegare i controller di archiviazione alla rete

Collegare i controller direttamente l'uno all'altro e alla rete host.

Prima di iniziare

Contattare l'amministratore di rete per informazioni sulla connessione del sistema di archiviazione agli switch di rete host.

A proposito di questa attività

Queste procedure mostrano le configurazioni comuni. Il cablaggio specifico dipende dai componenti ordinati per il sistema di storage in uso. Per informazioni dettagliate sulla configurazione e la priorità degli slot, vedere "NetApp Hardware Universe".

ASA A1K

Connetti gli storage controller per creare connessioni cluster ONTAP e collegare le porte Ethernet di ciascun controller alla rete host.

Fasi

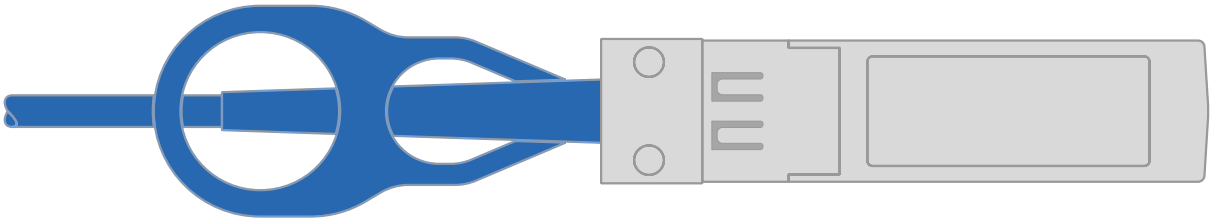
1. Utilizzare il cavo di interconnessione Cluster/ha per collegare le porte da E1a a E1a e le porte da e7a a e7a.

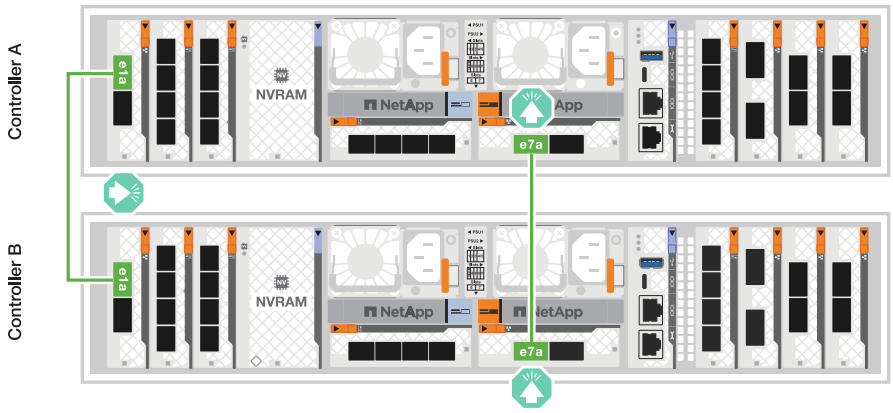
   Il traffico di cluster Interconnect e quello di ha condividono le stesse porte fisiche.

   a. Collegare la porta E1a del controller A alla porta E1a del controller B.

   b. Collegare la porta e7a del controller A alla porta E1a del controller B.

   Cavi di interconnessione cluster/ha

2. Collegare le porte del modulo Ethernet alla rete host.

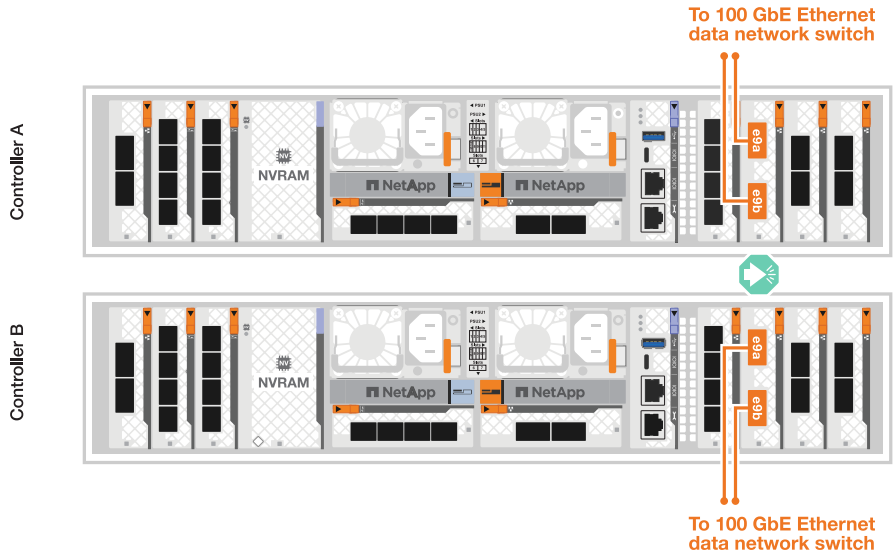
   Di seguito sono riportati alcuni esempi tipici di cablaggio della rete host. Per informazioni sulla configurazione specifica del sistema, vedere "NetApp Hardware Universe" .

   a. Collegare le porte e9a e e9b allo switch di rete dati Ethernet, come illustrato.

   Per ottenere le massime performance di sistema per il traffico cluster e ha, non utilizzare le porte e1b e e7b per le connessioni di rete host. Utilizzare una scheda host separata per ottimizzare le prestazioni.

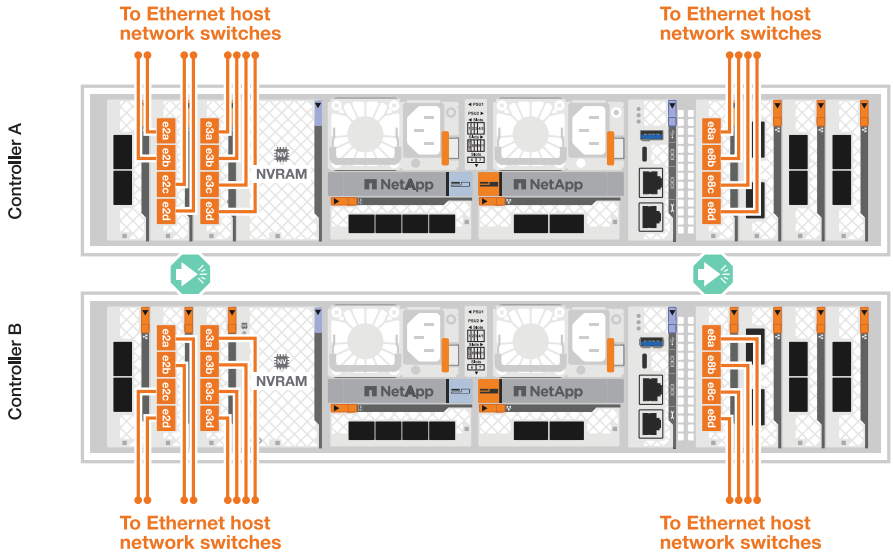
   Cavo 100 GbE



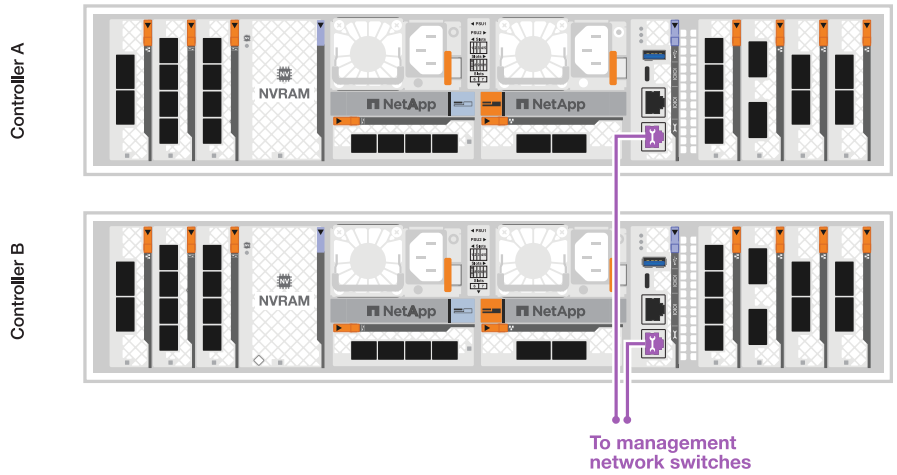
b. Collegare gli switch di rete host 10/25 GbE.

Host 10/25 GbE



3. Utilizzare i cavi RJ-45 1000BASE-T per collegare le porte di gestione del controller (chiave inglese) agli switch della rete di gestione.

*CAVI RJ-45 1000BASE-T.



Non collegare ancora i cavi di alimentazione.

ASA A70 e ASA A90

Connetti gli storage controller per creare connessioni cluster ONTAP e collegare le porte Ethernet di ciascun controller alla rete host.

Fasi

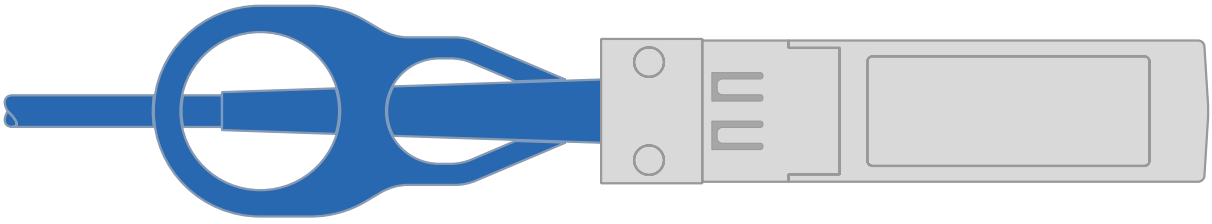
1. Utilizzare il cavo di interconnessione Cluster/ha per collegare le porte da E1a a E1a e le porte da e7a a e7a.

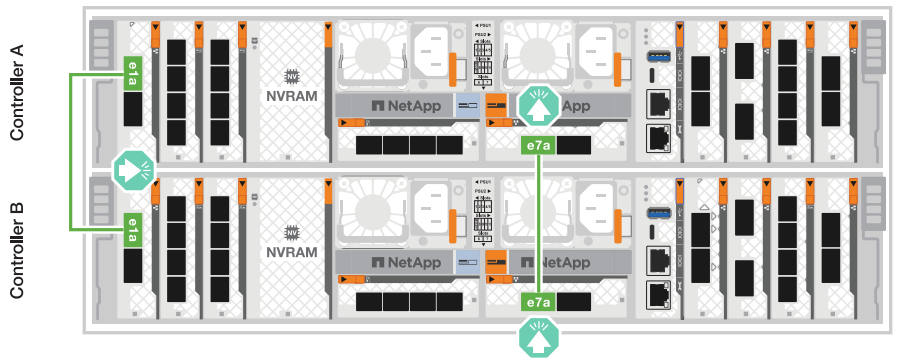
   Il traffico di cluster Interconnect e quello di ha condividono le stesse porte fisiche.

   a. Collegare la porta E1a del controller A alla porta E1a del controller B.

   b. Collegare la porta e7a del controller A alla porta E1a del controller B.

   Cavi di interconnessione cluster/ha





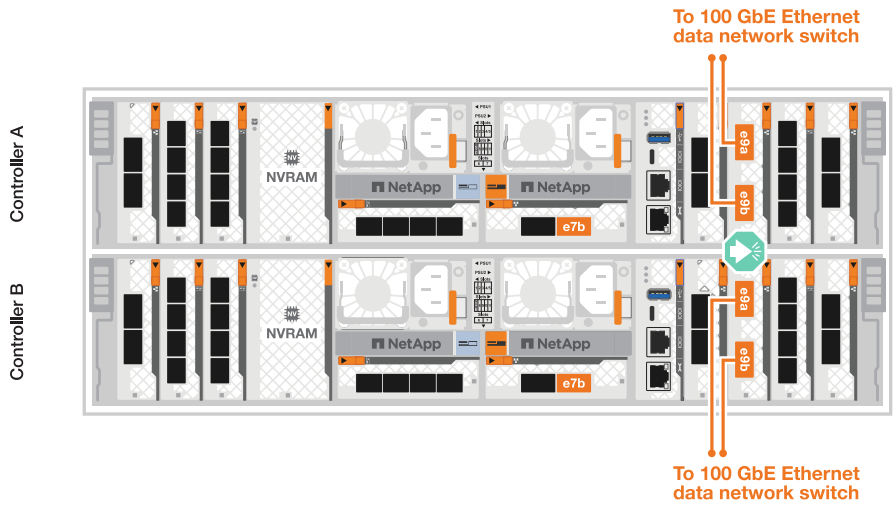
2. Collegare le porte del modulo Ethernet alla rete host.

Di seguito sono riportati alcuni esempi tipici di cablaggio della rete host. Per informazioni sulla configurazione specifica del sistema, vedere "NetApp Hardware Universe" .

a. Collegare le porte e9a e e9b allo switch di rete dati Ethernet, come illustrato.

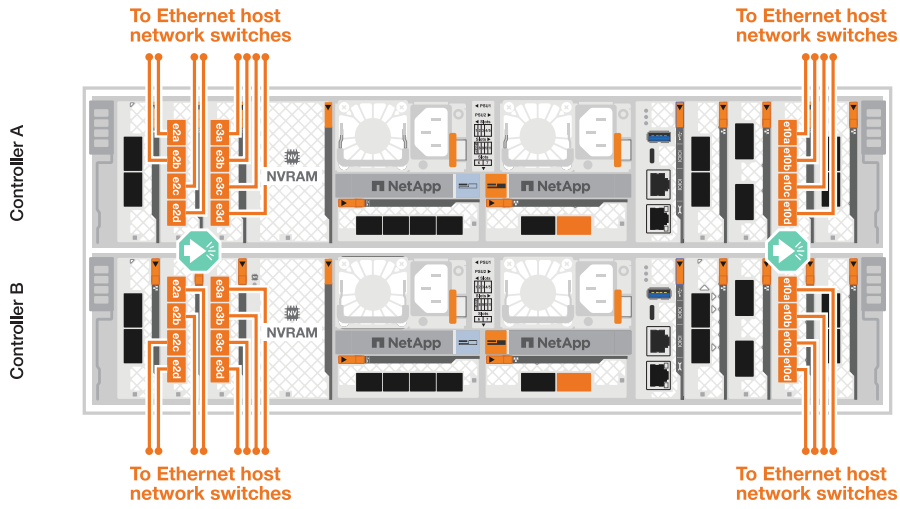
> Per ottenere le massime performance di sistema per il traffico cluster e ha, non utilizzare le porte e1b e e7b per le connessioni di rete host. Utilizzare una scheda host separata per ottimizzare le prestazioni.

Cavo 100 GbE



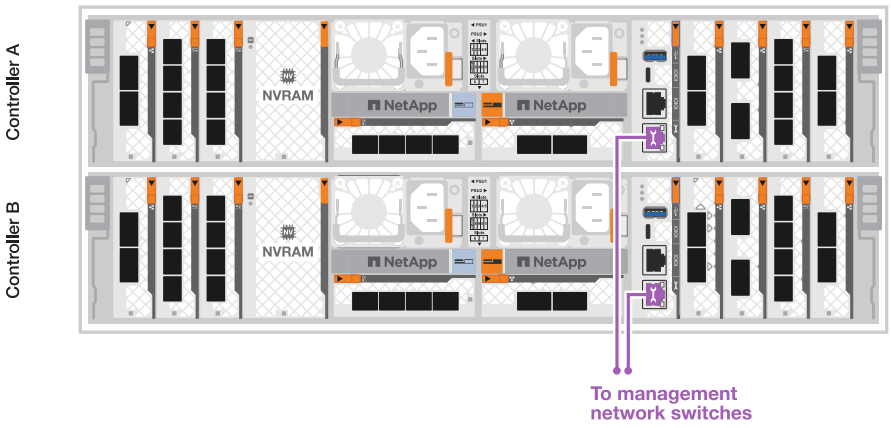
b. Collegare gli switch di rete host 10/25 GbE.

4 porte, 10/25 GbE host



3. Utilizzare i cavi RJ-45 1000BASE-T per collegare le porte di gestione del controller (chiave inglese) agli switch della rete di gestione.

*CAVI RJ-45 1000BASE-T.



Non collegare ancora i cavi di alimentazione.

Fase 2: Connettere gli storage controller agli shelf di storage

Le seguenti procedure di cablaggio mostrano come collegare i controller a uno shelf e a due shelf. Puoi connettere direttamente fino a quattro shelf ai tuoi controller.

ASA A1K

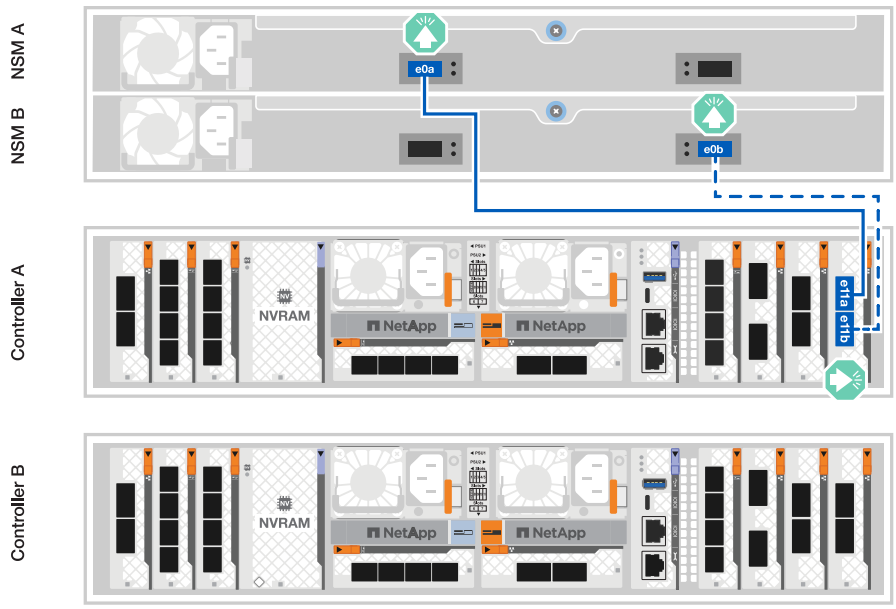
Scegliere una delle seguenti opzioni di cablaggio che corrisponda alla propria configurazione.

Opzione 1: Connettere i controller a uno shelf storage NS224

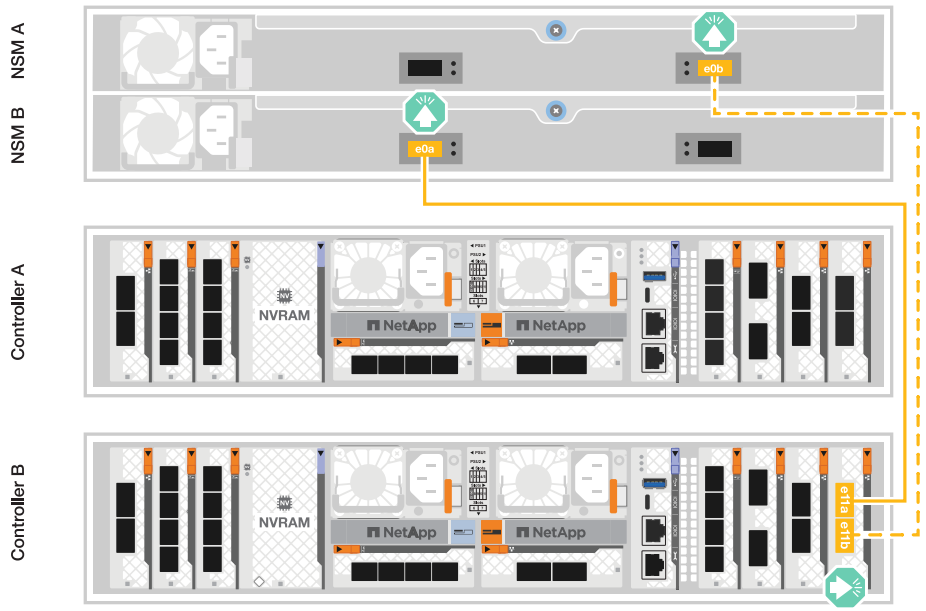
Collegare ciascun controller ai moduli NSM sullo shelf NS224. La grafica mostra il cablaggio di ciascuno dei controller: Il cablaggio del controller A è mostrato in blu e il cablaggio del controller B è mostrato in giallo.

Fasi

1. Sul controller A, collegare le seguenti porte:
   a. Collegare la porta e11a alla porta NSM A e0a.
   b. Collegare la porta e11b alla porta NSM B e0b.



2. Sul controller B, collegare le seguenti porte:
   a. Collegare la porta e11a alla porta NSM B e0a.
   b. Collegare la porta e11b alla porta NSM A e0b.

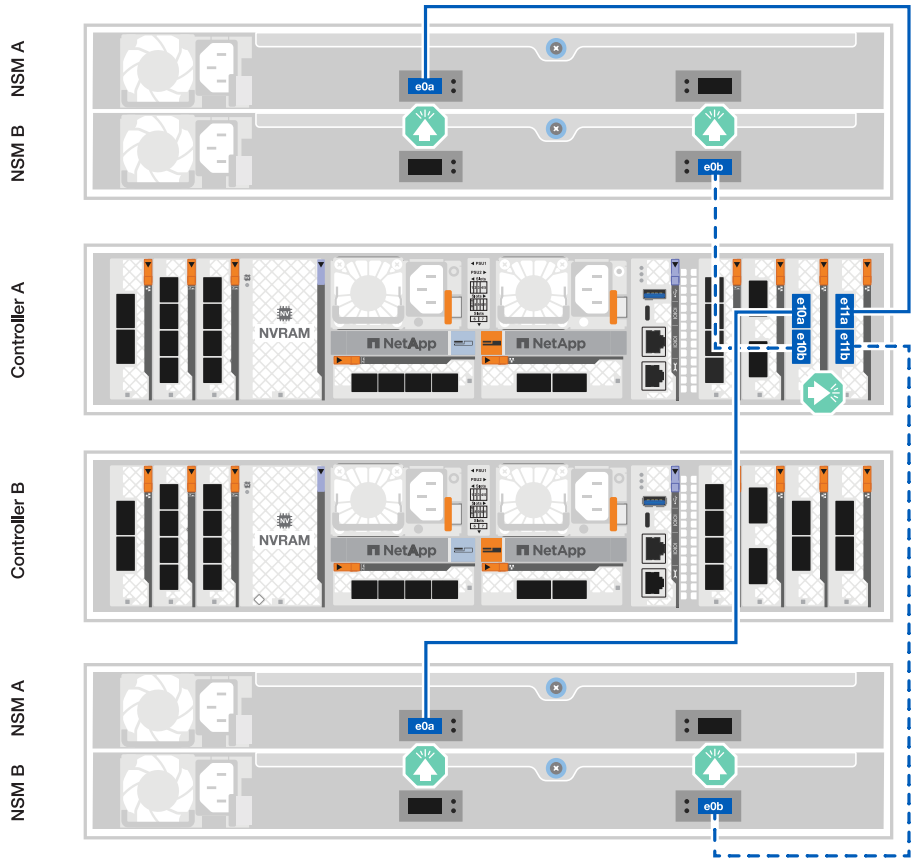


Opzione 2: Connettere i controller a due shelf storage NS224

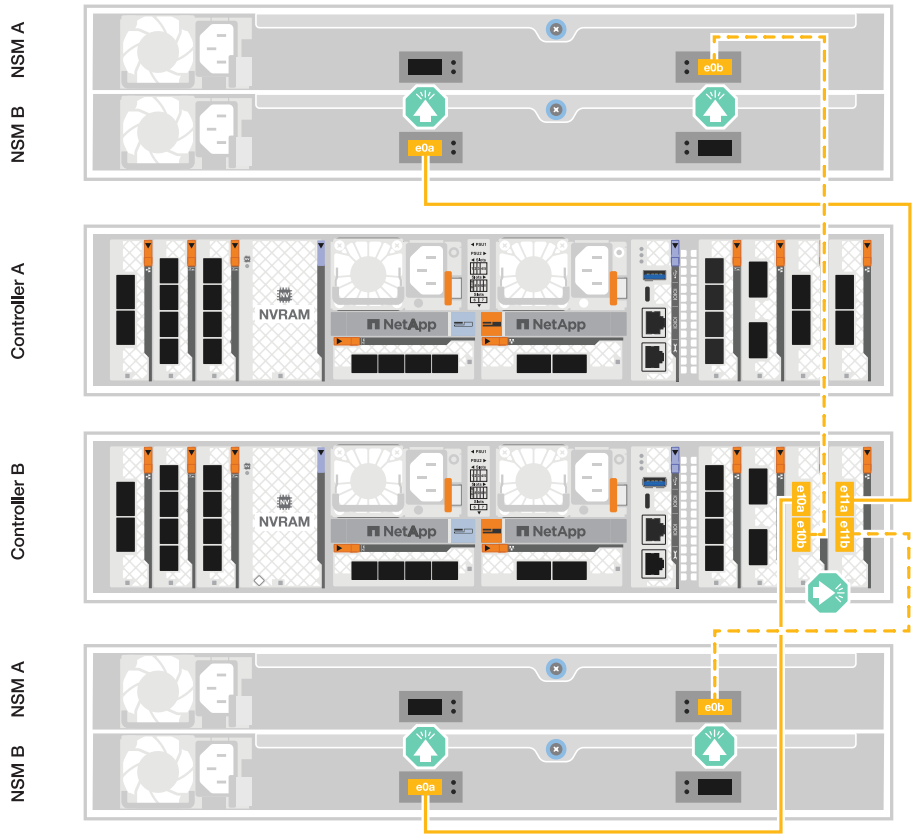
Collegare ciascun controller ai moduli NSM su entrambi gli shelf NS224. La grafica mostra il cablaggio di ciascuno dei controller: Il cablaggio del controller A è mostrato in blu e il cablaggio del controller B è mostrato in giallo.

Fasi

1. Sul controller A, collegare le seguenti porte:
   a. Collegare la porta e11a alla porta e0a NSM A dello shelf 1.
   b. Collegare la porta e11b alla porta NSM B e0b dello shelf 2.
   c. Collegare la porta E10A alla porta e0a NSM A dello shelf 2.
   d. Collegare la porta e10b alla porta e0b NSM A dello shelf 1.



2. Sul controller B, collegare le seguenti porte:
   a. Collegare la porta e11a alla porta NSM B e0a dello shelf 1.
   b. Collegare la porta e11b alla porta e0b NSM A dello shelf 2.
   c. Collegare la porta E10A alla porta NSM B e0a dello shelf 2.
   d. Collegare la porta e10b alla porta e0b NSM A dello shelf 1.



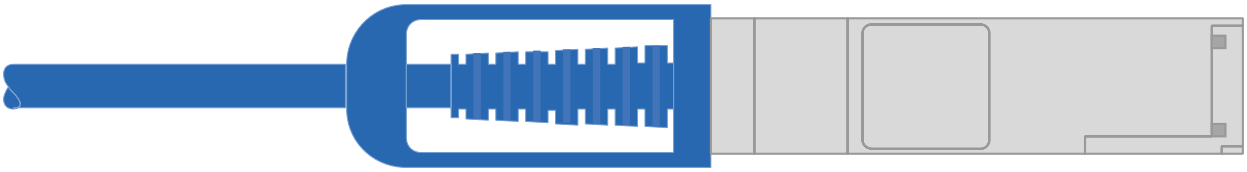
ASA A70 e ASA A90

Scegliere una delle seguenti opzioni di cablaggio che corrisponda alla propria configurazione.

Opzione 1: Connettere i controller a uno shelf storage NS224

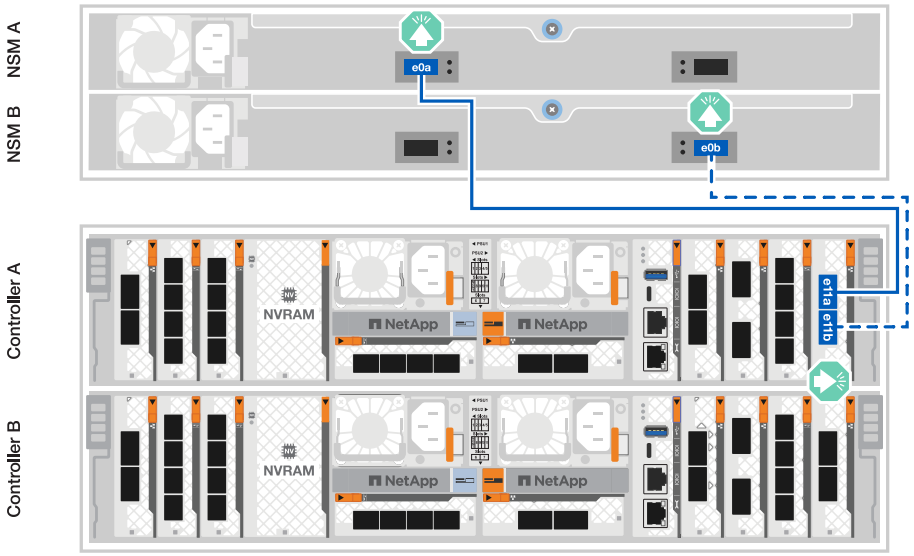
Collegare ciascun controller ai moduli NSM sullo shelf NS224. La grafica mostra il cablaggio di ciascuno dei controller: Il cablaggio del controller A è mostrato in blu e il cablaggio del controller B è mostrato in giallo.

Cavi in rame 100 GbE QSFP28

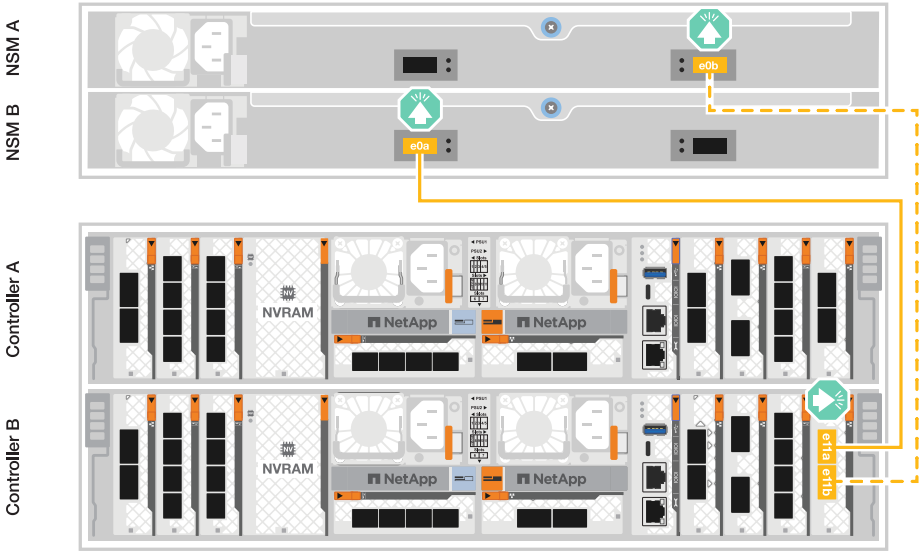


Fasi

1. Collegare la porta e11a del controller A alla porta NSM A e0a.
2. Collegare la porta e11b del controller A alla porta NSM B e0b.



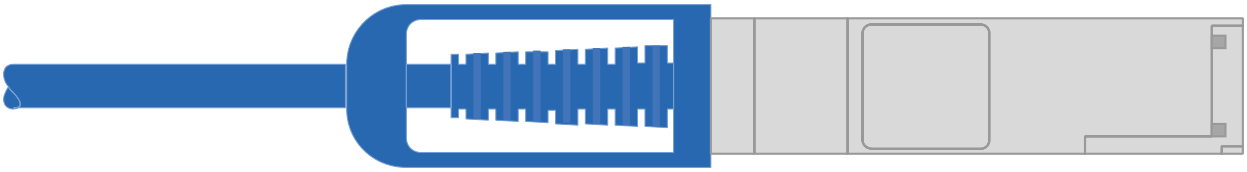
3. Collegare la porta e11a del controller B alla porta NSM B e0a.
4. Collegare la porta e11b del controller B alla porta NSM A e0b.


NSM A
NSM B
Controller A
Controller B
e0b
e0a
NVRAM
NetApp
NetApp
NVRAM
NetApp
NetApp
e11a
e11b

Opzione 2: Connettere i controller a due shelf storage NS224

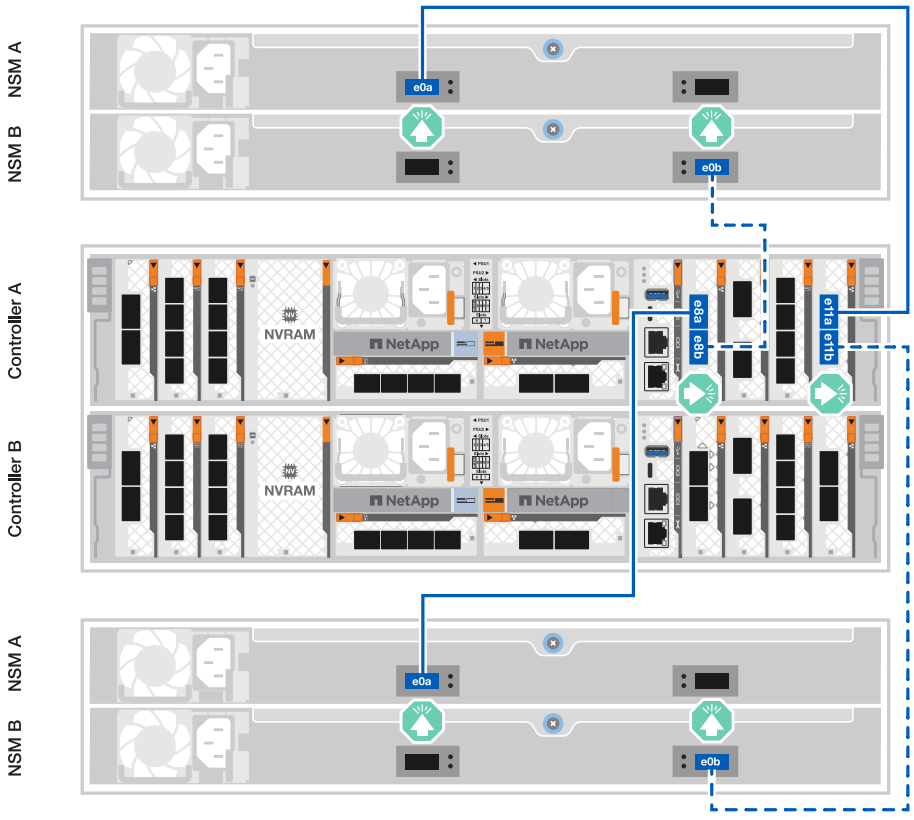
Collegare ciascun controller ai moduli NSM su entrambi gli shelf NS224. La grafica mostra il cablaggio di ciascuno dei controller: Il cablaggio del controller A è mostrato in blu e il cablaggio del controller B è mostrato in giallo.

Cavi in rame 100 GbE QSFP28



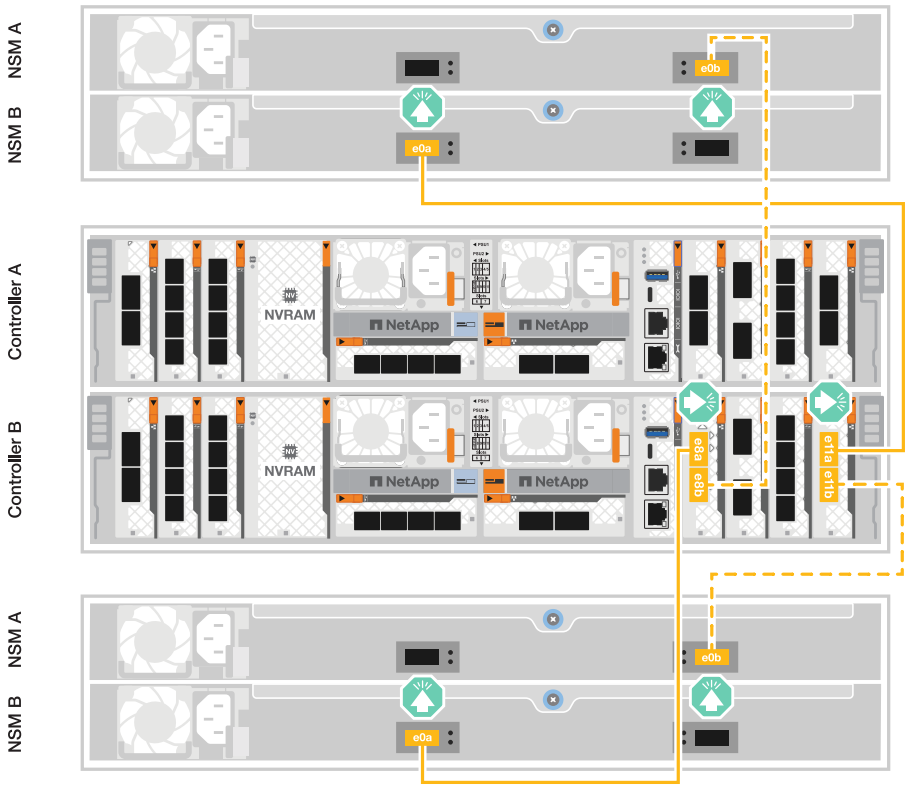
Fasi

1. Sul controller A, collegare le seguenti porte:
   a. Collegare la porta e11a allo shelf 1, la porta NSM A e0a.
   b. Collegare la porta e11b allo shelf 2, la porta NSM B e0b.
   c. Collegare la porta E8a allo shelf 2, la porta NSM A e0a.
   d. Collegare la porta e8b allo shelf 1, la porta NSM B e0b.



2. Sul controller B, collegare le seguenti porte:
   a. Collegare la porta e11a allo shelf 1, la porta NSM B e0a.
   b. Collegare la porta e11b allo shelf 2, la porta NSM A e0b.
   c. Collegare la porta E8a allo shelf 2, la porta NSM B e0a.

d. Collegare la porta e8b allo shelf 1, la porta NSM A e0b.



Quali sono le prossime novità?

Dopo aver collegato i controller di archiviazione alla rete e successivamente i controller agli shelf di archiviazione, è possibile "Accendere il sistema di archiviazione ASA R2".

Accendere il sistema di storage ASA R2

Dopo aver installato l'hardware rack per il sistema di storage ASA R2 e aver installato i cavi per i controller e gli shelf di storage, è necessario accendere gli shelf e i controller di storage.

Passaggio 1: Accendere lo shelf e assegnare l'ID dello shelf

Ogni ripiano NS224 si distingue per un ID ripiano univoco. Grazie a questo ID, lo shelf si distingue all'interno della configurazione del sistema storage. Per impostazione predefinita, gli ID shelf sono assegnati come "00" e "01", tuttavia potrebbe essere necessario regolarli per mantenere l'unicità nel sistema di storage.

A proposito di questa attività

- Un ID shelf valido va da 00 a 99.
- Per rendere effettivo l'ID dello shelf, è necessario spegnere e riaccendere uno shelf (scollegare entrambi i cavi di alimentazione, attendere il tempo necessario e ricollegarlo).

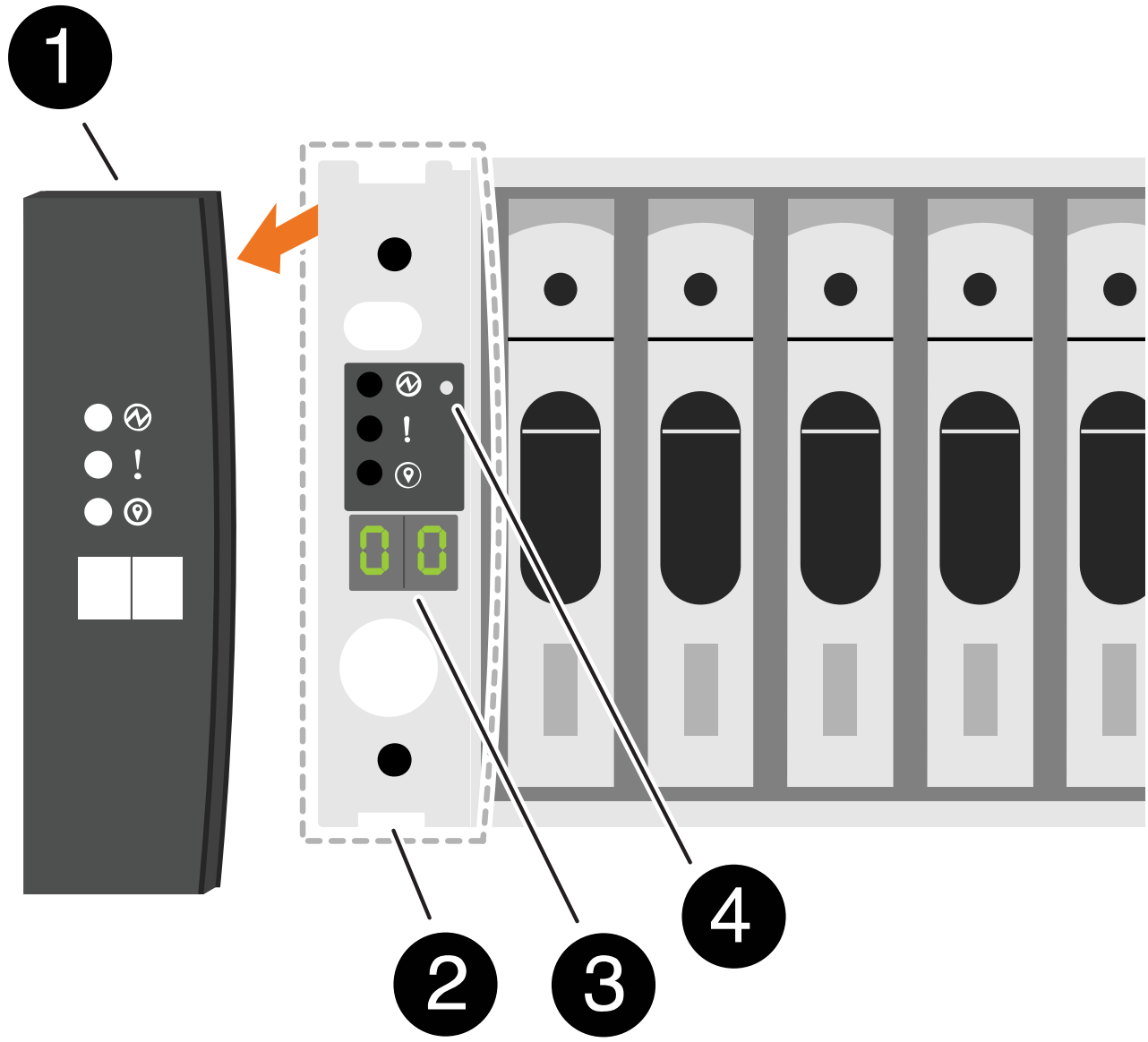
Fasi

1. Accendere lo shelf collegando prima i cavi di alimentazione allo shelf, fissandoli in posizione con il fermo del cavo di alimentazione, quindi collegando i cavi di alimentazione a sorgenti di alimentazione su circuiti

diversi.

Lo shelf si accende e si avvia automaticamente quando viene collegato alla fonte di alimentazione.

2. Rimuovere il cappuccio terminale sinistro per accedere al pulsante ID ripiano dietro la mascherina.



1	Tappo terminale dello scaffale

2	Mascherina dello scaffale
3	Numero ID ripiano
4	Pulsante ID ripiano

3. Modificare il primo numero dell'ID dello shelf:

   a. Inserire l'estremità dritta di una graffetta o una penna a sfera con punta stretta nel foro piccolo per premere il pulsante ID ripiano.

   b. Tenere premuto il pulsante ID ripiano finché il primo numero sul display digitale non lampeggia, quindi rilasciare il pulsante.

      Il lampeggiamento del numero può richiedere fino a 15 secondi. In questo modo viene attivata la modalità di programmazione degli ID dello shelf.

      > Se l'ID richiede più di 15 secondi per lampeggiare, tenere premuto nuovamente il pulsante ID ripiano, assicurandosi di premerlo completamente.

   c. Premere e rilasciare il pulsante ID ripiano per far avanzare il numero fino a raggiungere il numero desiderato da 0 a 9.

      La durata di ogni stampa e rilascio può essere di un solo secondo.

   Il primo numero continua a lampeggiare.

4. Modificare il secondo numero dell'ID dello shelf:

   a. Tenere premuto il pulsante fino a quando il secondo numero sul display digitale non lampeggia.

      Il lampeggiamento del numero può richiedere fino a tre secondi.

   Il primo numero sul display digitale smette di lampeggiare.

a. Premere e rilasciare il pulsante ID ripiano per far avanzare il numero fino a raggiungere il numero desiderato da 0 a 9.

   Il secondo numero continua a lampeggiare.

5. Bloccare il numero desiderato e uscire dalla modalità di programmazione tenendo premuto il pulsante ID ripiano finché il secondo numero non smette di lampeggiare.

   Il numero può richiedere fino a tre secondi per smettere di lampeggiare.

   Entrambi i numeri sul display digitale iniziano a lampeggiare e il LED ambra si illumina dopo circa cinque secondi, avvisando che l'ID ripiano in sospeso non ha ancora avuto effetto.

6. Spegnere e riaccendere lo shelf per almeno 10 secondi per rendere effettivo l'ID dello shelf.
   a. Scollegare il cavo di alimentazione da entrambi gli alimentatori presenti sullo shelf.
   b. Attendere 10 secondi.
   c. Ricollegare i cavi di alimentazione agli alimentatori per completare il ciclo di alimentazione.

      Un alimentatore si accende non appena il cavo di alimentazione viene collegato. Il LED a due colori si illumina di verde.

7. Sostituire il cappuccio terminale sinistro.

Fase 2: Accendere i controller

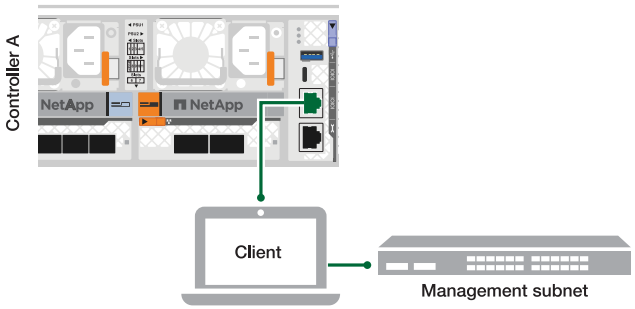
Dopo aver acceso i ripiani di archiviazione e assegnato loro ID univoci, attivare l'alimentazione ai controller di archiviazione.

Fasi

1. Collegare il computer portatile alla porta seriale della console. Ciò consente di monitorare la sequenza di avvio quando i controller sono accesi.
   a. Impostare la porta seriale della console del computer portatile a 115.200 baud con N-8-1.

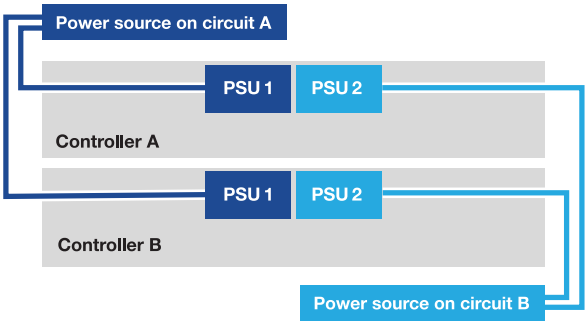
      Per istruzioni su come configurare la porta seriale della console, consultare la guida in linea del laptop.

   b. Collegare il cavo della console al computer portatile e la porta seriale della console sul controller utilizzando il cavo della console fornito con il sistema di archiviazione.
   c. Collegare il computer portatile allo switch sulla subnet di gestione.



   d. Assegnare un indirizzo TCP/IP al computer portatile, utilizzando un indirizzo presente nella subnet di gestione.

2. Collegare i cavi di alimentazione agli alimentatori del controller, quindi collegarli a fonti di alimentazione su diversi circuiti.



   - Il sistema di storage inizia l'avvio. L'avvio iniziale può richiedere fino a otto minuti.
   - I LED lampeggiano e le ventole si avviano, a indicare che i controller si stanno accendendo.
   - Le ventole potrebbero essere molto rumorose al primo avvio. Il rumore della ventola all'avviamento è normale.
3. Fissare i cavi di alimentazione utilizzando il dispositivo di fissaggio su ciascun alimentatore.

Quali sono le prossime novità?

Dopo aver acceso il sistema di archiviazione ASA R2, si "Configurare un cluster ONTAP ASA R2".

Configurare il sistema ASA R2

Configura un cluster ONTAP sul tuo sistema storage ASA R2

System Manager di ONTAP ti guida attraverso un workflow rapido e semplice per la configurazione di un cluster ONTAP ASA R2.

Durante la configurazione del cluster viene creata la macchina virtuale (VM) per lo storage dei dati predefinita. In alternativa, è possibile abilitare il DNS (Domain Name System) per risolvere i nomi host, impostare il cluster in modo che utilizzi il NTP (Network Time Protocol) per la sincronizzazione dell'ora e abilitare la crittografia dei dati inutilizzati.

Prima di iniziare

Raccogliere le seguenti informazioni:

- Indirizzo IP di gestione del cluster

  L'indirizzo IP di gestione del cluster è un indirizzo IPv4 univoco per l'interfaccia di gestione del cluster, utilizzata dall'amministratore del cluster per accedere alla VM di storage di amministrazione e gestire il cluster. È possibile ottenere questo indirizzo IP dall'amministratore responsabile dell'assegnazione degli indirizzi IP all'interno dell'organizzazione.

- Subnet mask di rete

  Durante la configurazione del cluster, ONTAP consiglia una serie di interfacce di rete appropriate per la configurazione in uso. Se necessario, è possibile modificare il suggerimento.

- Indirizzo IP del gateway di rete
- Indirizzo IP del nodo partner

- Nomi di dominio DNS
- Indirizzi IP del server dei nomi DNS
- Indirizzi IP del server NTP
- Data subnet mask (Subnet mask dati)

Fasi

1. Rilevamento della rete cluster
   a. Collegare il computer portatile allo switch di gestione e accedere ai computer e ai dispositivi di rete.
   b. Aprire file Explorer.
   c. Selezionare **rete**, quindi fare clic con il pulsante destro del mouse e selezionare **Aggiorna**.
   d. Selezionare l'icona ONTAP, quindi accettare i certificati visualizzati sullo schermo.

      Viene visualizzato Gestione sistema.

2. In **Password**, creare una password complessa per l'account admin.

   La password deve essere composta da almeno otto caratteri e deve contenere almeno una lettera e un numero.

3. Immettere nuovamente la password per confermare, quindi selezionare **continua**.
4. In **indirizzi di rete**, immettere un nome del sistema di archiviazione o accettare il nome predefinito.

   Se si modifica il nome del sistema di archiviazione predefinito, il nuovo nome deve iniziare con una lettera e deve contenere meno di 44 caratteri. È possibile utilizzare un punto (.), un trattino (-) o un trattino basso (_) nel nome.

5. Immettere l'indirizzo IP della gestione del cluster, la subnet mask, l'indirizzo IP del gateway e l'indirizzo IP del nodo partner, quindi selezionare **continua**.
6. In **servizi di rete**, selezionare le opzioni desiderate per **utilizzare il DNS (Domain Name System) per risolvere i nomi host** e **utilizzare il NTP (Network Time Protocol) per mantenere sincronizzati gli orari**.

   Se si sceglie di utilizzare il DNS, immettere il dominio DNS e i server dei nomi. Se si sceglie di utilizzare NTP, immettere i server NTP, quindi selezionare **continua**.

7. In **Encryption**, immettere una passphrase per Onboard Key Manager (OKM).

   Per impostazione predefinita, è selezionata la crittografia dei dati inutilizzati mediante un gestore di chiavi integrato (OKM). Se si desidera utilizzare un gestore di chiavi esterno, aggiornare le selezioni.

   In alternativa, è possibile configurare il cluster per la crittografia al termine della configurazione.

8. Selezionare **Inizializza**.

   Una volta completata la configurazione, l'utente viene reindirizzato all'indirizzo IP di gestione del cluster.

9. In **rete**, selezionare **Configura protocolli**.

Per configurare IP (iSCSI e NVMe/TCP), procedere come indicato di seguito.	Per configurare FC e NVMe/FC, esegui queste operazioni…
a. Selezionare **IP**, quindi selezionare **Configura interfacce IP**. b. Selezionare **Aggiungi subnet**. c. Immettere un nome per la subnet, quindi immettere gli indirizzi IP della subnet. d. Immettere la subnet mask e, se si desidera, immettere un gateway, quindi selezionare **Aggiungi**. e. Selezionare la subnet appena creata, quindi selezionare **Salva**. f. Selezionare **Salva**.	a. Selezionare **FC**, quindi selezionare **Configura interfacce FC** e/o **Configura interfacce NVMe/FC**. b. Selezionare le porte FC e/o NVMe/FC, quindi selezionare **Salva**.

10. In alternativa, scaricare ed eseguire "ActiveIQ Config Advisor" per confermare la configurazione.

    ActiveIQ Config Advisor è uno strumento per i sistemi NetApp che verifica la presenza di errori di configurazione più comuni.

Quali sono le prossime novità?

Siete pronti a "impostare l'accesso ai dati" partire dai vostri client SAN al vostro sistema ASA R2.

Abilitare l'accesso ai dati dagli host SAN al sistema di storage ASA R2

Per impostare l'accesso ai dati, è necessario verificare che i parametri e le impostazioni specifici sul client SAN fondamentali per il corretto funzionamento con ONTAP siano configurati correttamente. Se utilizzate VMware, dovreste migrare le vostre macchine virtuali.

Configurare l'accesso ai dati dagli host SAN

La configurazione necessaria per impostare l'accesso ai dati dal sistema ASA R2 agli host SAN varia IN base al sistema operativo host e al protocollo. La corretta configurazione è importante per ottenere le migliori performance e il successo del failover.

Consultare la documentazione dell'host SAN ONTAP per "Client SCSI VMware vSphere" "Client VMware vSphere NVMe"e "Altri client SAN" per configurare correttamente gli host per la connessione al sistema ASA R2.

Migrazione di macchine virtuali VMware

Per migrare il carico di lavoro delle macchine virtuali da un sistema storage ASA a un sistema storage ASA R2, NetApp consiglia di utilizzare "VMware vSphere vMotion" per eseguire una migrazione live e senza interruzioni dei dati.

Quali sono le prossime novità?

Puoi "provisioning dello storage"abilitare gli host SAN a leggere e scrivere i dati nelle unità storage.

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.

Amministrare e monitorare

Gestire l’accesso dei client alle macchine virtuali storage sui sistemi storage ASA R2

Le unità storage di un sistema ASA R2 sono contenute in Storage Virtual Machine (VM). Le macchine virtuali storage vengono utilizzate per fornire dati ai client SAN. Utilizza il Gestore di sistema di ONTAP per creare una LIF (interfaccia di rete) che permette ai client SAN di connettersi a una VM storage e di accedere ai dati nelle unità storage. Facoltativamente, è possibile utilizzare le subnet per semplificare la creazione di LIF e gli IPSpace per fornire alle macchine virtuali storage storage risorse storage, amministrazione e routing sicuri.

Creare IPspaces

Un IPSpace è uno spazio di indirizzi IP distinto in cui risiedono le macchine virtuali di storage. Quando si creano IPSpace, è possibile abilitare le VM di storage a disporre di storage, amministrazione e routing propri e sicuri. È inoltre possibile consentire ai client di domini di rete separati amministrativamente di utilizzare indirizzi IP sovrapposti dello stesso intervallo di subnet di indirizzi IP.

È necessario creare un IPSpace prima di poter creare una subnet.

Fasi

1. Selezionare **rete > Panoramica**.
2. In **IPSpace**, selezionare + Add.
3. Immettere un nome per IPSpace o accettare il nome predefinito.

   Un nome IPSpace non può essere "tutto" perché "tutto" è un nome riservato al sistema.

4. Selezionare **Salva**.

Quali sono le prossime novità?

Una volta creato un IPSpace, è possibile utilizzarlo per creare una subnet.

Creare sottoreti

Una subnet consente di allocare blocchi specifici di indirizzi IPv4 o IPv6 da utilizzare quando si crea una LIF (interfaccia di rete) . Una subnet semplifica la creazione della LIF consentendo di specificare il nome della subnet invece di un indirizzo IP e una maschera di rete specifici per ogni LIF.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- "dominio di broadcast"E IPSpace in cui si intende aggiungere la subnet devono già esistere.

Fasi

1. Selezionare **rete > Panoramica**.
2. Selezionare **sottoreti**, quindi selezionare + Add.

3. Inserire il nome della subnet.

   Tutti i nomi di subnet devono essere univoci all'interno di un IPSpace.

4. Immettere l'indirizzo IP della subnet e la subnet mask.
5. Specificare l'intervallo di indirizzi IP per la subnet.

   Quando si specifica l'intervallo di indirizzi IP per la subnet, non sovrapporre gli indirizzi IP alle altre subnet. I problemi di rete possono verificarsi quando gli indirizzi IP della subnet si sovrappongono e sottoreti o host diversi tentano di utilizzare lo stesso indirizzo IP.

6. Selezionare il dominio di broadcast per la subnet.
7. Selezionare **Aggiungi**.

Quali sono le prossime novità?

È stata creata una subnet che può essere utilizzata per semplificare la creazione della LIF.

Creazione di una LIF (interfaccia di rete)

Una LIF (interfaccia di rete) è un indirizzo IP associato a una porta fisica o logica. Creare LIF sulle porte che servono per accedere ai dati. Le macchine virtuali storage servono dati ai client attraverso una o più LIF. In caso di guasto di un componente, una LIF può essere sottoposta a failover o migrata su una porta fisica differente, così che la comunicazione di rete non venga interrotta.

Al momento della creazione di una LIF dati IP, questa può servire sia il traffico iSCSI che NVMe/TCP per impostazione predefinita. Occorre creare LIF dati separate per il traffico FC e NVMe/FC.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- La porta di rete fisica o logica sottostante deve essere stata configurata sullo `up` stato amministrativo.
- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.
- Una LIF che gestisce il traffico intracluster tra i nodi non deve trovarsi sulla stessa subnet di una LIF che gestisce il traffico di gestione o di una LIF che gestisce il traffico di dati.

Fasi

1. Selezionare **rete > Panoramica**.
2. Selezionare **interfacce di rete**, quindi + Add.
3. Seleziona il tipo di interfaccia e il protocollo, quindi seleziona la VM storage.
4. Immettere un nome per la LIF o accettare il nome predefinito.
5. Selezionare il nodo principale dell'interfaccia di rete, quindi inserire l'indirizzo IP e la subnet mask.
6. Selezionare **Salva**.

Risultato

È stata creata una LIF per l'accesso ai dati.

Modifica di una LIF (interfacce di rete)

Le LIF possono essere disattivate o rinominate in base alle esigenze. Puoi anche modificare l'indirizzo IP della LIF e la subnet mask.

Fasi

1. Selezionare **rete > Panoramica**, quindi selezionare **interfacce di rete**.
2. Passare il mouse sull'interfaccia di rete che si desidera modificare, quindi selezionare ⋮.
3. Selezionare **Modifica**.
4. È possibile disattivare l'interfaccia di rete, rinominare l'interfaccia di rete, modificare l'indirizzo IP o modificare la subnet mask.
5. Selezionare **Salva**.

Risultato

La LIF è stata modificata.

Gestisci il networking dei cluster sui sistemi storage ASA R2

Puoi utilizzare Gestione sistema di ONTAP per eseguire un'amministrazione di base della rete di storage sul sistema ASA R2. Ad esempio, è possibile aggiungere un dominio di broadcast o riassegnare le porte a un dominio di broadcast diverso.

Aggiungere un dominio di broadcast

Utilizza i domini di broadcast per semplificare la gestione della rete cluster raggruppando le porte di rete appartenenti alla stessa rete Layer 2. Le Storage Virtual Machine (VM) possono quindi utilizzare le porte nel gruppo per il traffico di dati o di gestione.

Il dominio di broadcast "Default" (predefinito) e il dominio di broadcast "Cluster" (cluster) vengono creati durante la configurazione del cluster. Il dominio di broadcast "Default" contiene le porte che si trovano nello spazio IPSpace "Default". Queste porte vengono utilizzate principalmente per la gestione dei dati. Anche le porte di gestione del cluster e dei nodi si trovano in questo dominio di broadcast. Il dominio di broadcast "Cluster" contiene le porte che si trovano nell'IPSpace "Cluster". Queste porte vengono utilizzate per la comunicazione del cluster e includono tutte le porte del cluster di tutti i nodi del cluster.

Dopo l'inizializzazione del cluster è possibile creare altri domini di broadcast. Quando si crea un dominio di broadcast, viene creato automaticamente un gruppo di failover che contiene le stesse porte.

A proposito di questa attività

L'MTU (Maximum Transmission Unit) delle porte aggiunte a un dominio di broadcast viene aggiornato al valore MTU impostato nel dominio di broadcast.

Fasi

1. In System Manager, selezionare **rete > Panoramica**.
2. In domini **Broadcast**, selezionare + Add.
3. Immettere un nome per il dominio di broadcast o accettare il nome predefinito.

   Tutti i nomi di dominio di trasmissione devono essere univoci all'interno di un IPSpace.

4. Selezionare IPSpace per il dominio di broadcast.

   Se non si specifica un nome IPSpace, il dominio di broadcast viene creato nell'IPSpace "Default".

5. Immettere l'unità massima di trasmissione (MTU).

   MTU è il pacchetto di dati più grande che può essere accettato nel dominio di trasmissione.

6. Selezionare le porte desiderate, quindi selezionare **Salva**.

Risultato

È stato aggiunto un nuovo dominio di trasmissione.

Riassegnare le porte a un dominio di broadcast diverso

Le porte possono appartenere a un solo dominio di trasmissione. Se si desidera modificare il dominio di broadcast a cui appartiene una porta, è necessario riassegnare la porta dal dominio di broadcast esistente a un nuovo dominio di broadcast.

Fasi

1. In System Manager, selezionare **rete > Panoramica**.
2. In **Domini di trasmissione**, selezionare ⋮ accanto al nome del dominio, quindi selezionare **Modifica**.
3. Deselezionare le porte Ethernet che si desidera riassegnare a un altro dominio.
4. Selezionare il dominio di broadcast al quale si desidera riassegnare la porta, quindi selezionare **Riassegna**.
5. Selezionare **Salva**.

Risultato

Le porte sono state riassegnate a un dominio di broadcast diverso.

Creare un VLAN

Una VLAN è costituita da porte switch raggruppate in un dominio di broadcast. Le reti VLAN consentono di aumentare la protezione, isolare i problemi e limitare i percorsi disponibili all'interno dell'infrastruttura di rete IP.

Prima di iniziare

Gli switch implementati nella rete devono essere conformi agli standard IEEE 802.1Q o disporre di un'implementazione delle VLAN specifica del vendor.

A proposito di questa attività

- Non è possibile creare una VLAN su una porta del gruppo di interfacce che non contiene porte membri.
- Quando si configura una VLAN su una porta per la prima volta, la porta potrebbe spegnersi, causando una disconnessione temporanea della rete. Le successive aggiunte di VLAN alla stessa porta non influiscono sullo stato della porta.
- Non creare una VLAN su un'interfaccia di rete con lo stesso identificativo della VLAN nativa dello switch. Ad esempio, se l'interfaccia di rete e0b si trova sulla VLAN nativa 10, non creare una VLAN e0b-10 su tale interfaccia.

Fasi

1. In System Manager, selezionare **rete > porte Ethernet**, quindi selezionare + VLAN.

2. Selezionare il nodo e il dominio di broadcast per la VLAN.
3. Selezionare la porta per la VLAN.

   La VLAN non può essere collegata a una porta che ospita una LIF del cluster o a porte assegnate all'IPSpace del cluster.

4. Immettere un ID VLAN.
5. Selezionare **Salva**.

Risultato

È stata creata una VLAN per aumentare la protezione, isolare i problemi e limitare i percorsi disponibili all'interno dell'infrastruttura di rete IP.

Monitora l'utilizzo e aumenta la capacità

Monitora le performance del cluster e delle unità storage sui sistemi storage ASA R2

Utilizza ONTAP System Manager per monitorare le performance generali del cluster e le performance di specifiche unità di storage e determinare l'impatto di latenza, IOPS e throughput sulle applicazioni business-critical. Le prestazioni possono essere monitorate in vari periodi di tempo, da un'ora a un anno.

Ad esempio, si supponga che un'applicazione critica stia riscontrando un'elevata latenza e un basso throughput. Se non vedi le performance del cluster degli ultimi cinque giorni di lavoro, noterai una diminuzione delle performance alla stessa ora ogni giorno. Queste informazioni vengono utilizzate per determinare se l'applicazione critica è in competizione per le risorse cluster quando inizia l'esecuzione in background di un processo non critico. Potrai quindi modificare la policy di QoS per limitare l'impatto del carico di lavoro non critico sulle risorse di sistema e garantire che il carico di lavoro critico soddisfi gli obiettivi minimi di throughput.

Monitoraggio delle performance del cluster

Utilizza le metriche delle performance del cluster per determinare se è necessario spostare i carichi di lavoro per ridurre al minimo la latenza e massimizzare IOPS e throughput per le tue applicazioni critiche.

Fasi

1. In System Manager, selezionare **Dashboard**.
2. In **Performance**, visualizzare la latenza, gli IOPS e il throughput del cluster in base a ora, giorno, settimana, mese o anno.
3. Selezionare per scaricare i dati sulle prestazioni.

Quali sono le prossime novità?

Utilizza le metriche delle performance del cluster per analizzare se è necessario modificare le policy QoS o apportare altre modifiche ai carichi di lavoro dell'applicazione per massimizzare le performance complessive del cluster.

Monitorare le prestazioni dell'unità di archiviazione

Utilizza le metriche di performance delle unità di storage per determinare l'impatto di applicazioni specifiche su

latenza, IOPS e throughput.

Fasi

1. In System Manager, selezionare **Storage**.
2. Selezionare l'unità di archiviazione che si desidera monitorare, quindi selezionare **Panoramica**.
3. In **Performance**, visualizzare la latenza, gli IOPS e il throughput dell'unità di storage in base a ora, giorno, settimana, mese o anno.
4. Selezionare  per scaricare i dati sulle prestazioni.

Quali sono le prossime novità?

Utilizza le metriche di performance delle tue unità di storage per analizzare se è necessario modificare le policy di QoS assegnate alle tue unità di storage per ridurre la latenza e massimizzare IOPS e throughput.

Monitorare l'utilizzo di cluster e unità storage sui sistemi storage ASA R2

USA Gestione sistema di ONTAP per monitorare il tuo utilizzo dello storage e assicurarti di disporre della capacità di storage necessaria per gestire i carichi di lavoro attuali e futuri.

Monitoraggio dell'utilizzo dei cluster

Monitorare regolarmente la quantità di storage consumata dal cluster per garantire che, se necessario, sia pronta ad espandere la capacità del cluster prima di esaurire lo spazio.

Fasi

1. In System Manager, selezionare **Dashboard**.
2. In **capacità**, visualizzare la quantità di spazio fisico utilizzato e la quantità di spazio disponibile nel cluster.

   Il rapporto di riduzione dei dati rappresenta la quantità di spazio risparmiato grazie all'efficienza dello storage.

Quali sono le prossime novità?

Se lo spazio del cluster sta per esaurirsi o se non ha la capacità necessaria per soddisfare una domanda futura, è necessario pianificare l'"aggiungere nuove unità"utilizzo del sistema ASA R2 per aumentare la capacità di storage.

Monitorare l'utilizzo dell'unità di archiviazione

Monitorare la quantità di storage consumata da un'unità di storage in modo da poter aumentare in maniera proattiva le dimensioni dell'unità di storage in base alle proprie esigenze di business.

Fasi

1. In System Manager, selezionare **Storage**.
2. Selezionare l'unità di archiviazione che si desidera monitorare, quindi selezionare **Panoramica**.
3. In **archiviazione**, visualizzare quanto segue:
   - Dimensioni dell'unità di archiviazione
   - Quantità di spazio utilizzato

- Rapporto di riduzione dei dati

  Il rapporto di riduzione dei dati rappresenta la quantità di spazio risparmiato grazie all'efficienza dello storage

- Istantanea utilizzata

  Lo snapshot utilizzato rappresenta la quantità di storage utilizzata dagli snapshot.

Quali sono le prossime novità?

Se la capacità dell'unità di archiviazione è prossima, è necessario "modificare l'unità di conservazione"aumentarne le dimensioni.

Aumentare la capacità dello storage sui sistemi storage ASA R2

Aggiungi dischi a un nodo o a uno shelf per aumentare la capacità dello storage del tuo sistema ASA R2.

Utilizzare NetApp Hardware Universe per preparare l'installazione di una nuova unità

Prima di installare una nuova unità su un nodo o su uno shelf, utilizzare la NetApp Hardware Universe per verificare che l'unità da aggiungere sia supportata dalla propria piattaforma ASA R2 e per identificare lo slot corretto per la nuova unità. Gli slot corretti per l'aggiunta di dischi variano a seconda del modello di piattaforma e della versione di ONTAP. In alcuni casi, è necessario aggiungere unità a slot specifici in sequenza.

Fasi

1. Consultare la "NetApp Hardware Universe".
2. In **prodotti**, selezionare le configurazioni hardware.
3. Seleziona la piattaforma ASA R2.
4. Selezionare la versione di ONTAP, quindi selezionare **Mostra risultati**.
5. Sotto l'immagine, selezionare **fare clic qui per visualizzare le viste alternative**, quindi scegliere la vista corrispondente alla configurazione.
6. Utilizzare la vista della configurazione per verificare che la nuova unità sia supportata e lo slot corretto per l'installazione.

Risultato

È stato confermato che la nuova unità è supportata e si conosce lo slot appropriato per l'installazione.

Installare una nuova unità sul ASA R2

Il numero minimo di dischi da aggiungere in una singola procedura è sei. L'aggiunta di un singolo disco potrebbe ridurre le prestazioni.

A proposito di questa attività

Ripetere i passi di questa procedura per ciascuna unità.

Fasi

1. Mettere a terra l'utente.
2. Rimuovere delicatamente il pannello frontale dalla parte anteriore della piattaforma.

3. Inserire la nuova unità nello slot corretto.
   a. Con la maniglia della camma in posizione aperta, inserire il nuovo disco con entrambe le mani.
   b. Premere fino all'arresto del disco.
   c. Chiudere la maniglia della camma in modo che l'unità sia completamente inserita nel piano intermedio e la maniglia scatti in posizione.

      Chiudere lentamente la maniglia della camma in modo che sia allineata correttamente con la superficie dell'unità.

4. Verificare che il LED di attività del disco (verde) sia acceso.
   - SE il LED è fisso, l'unità è alimentata.
   - Se il LED lampeggia, l'unità è alimentata e l'i/o è in corso. Il LED lampeggia anche se il firmware dell'unità è in fase di aggiornamento.

     Il firmware del disco viene aggiornato automaticamente (senza interruzioni) sui nuovi dischi che non dispongono delle versioni firmware correnti.

5. Se il nodo è configurato per l'assegnazione automatica delle unità, è possibile attendere che ONTAP assegni automaticamente le nuove unità a un nodo. Se il nodo non è configurato per l'assegnazione automatica delle unità o se lo si preferisce, è possibile assegnare le unità manualmente.

   I nuovi dischi non vengono riconosciuti fino a quando non vengono assegnati a un nodo.

Cosa succederà?

Dopo aver riconosciuto le nuove unità, verificare che siano state aggiunte e che la relativa proprietà sia specificata correttamente.

Aggiornamento del firmware sui sistemi di storage ASA R2

Per impostazione predefinita, ONTAP scarica e aggiorna automaticamente i file del firmware e di sistema sul sistema ASA R2. Se si desidera la flessibilità di visualizzare gli aggiornamenti consigliati prima di scaricarli e installarli, è possibile utilizzare Gestione di sistema di ONTAP per disattivare gli aggiornamenti automatici o modificare i parametri di aggiornamento per visualizzare le notifiche degli aggiornamenti disponibili prima di eseguire qualsiasi azione.

Abilitare gli aggiornamenti automatici

Per impostazione predefinita, gli aggiornamenti consigliati per il firmware dello storage, il firmware SP/BMC e i file di sistema vengono scaricati e installati automaticamente nel sistema ASA R2. Se gli aggiornamenti automatici sono stati disattivati, è possibile attivarli per ripristinare il comportamento predefinito.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Accanto a **aggiornamento automatico** selezionare ⋮, quindi selezionare **Abilita**.
3. Leggere e accettare l'EULA.
4. Accettare le impostazioni predefinite per aggiornare automaticamente il firmware e i file di sistema. In alternativa, selezionare per visualizzare le notifiche o per chiudere automaticamente gli aggiornamenti

consigliati.

5. Selezionare per confermare che le modifiche apportate agli aggiornamenti verranno applicate a tutti gli aggiornamenti correnti e futuri.
6. Selezionare **Salva**.

Risultato

Gli aggiornamenti consigliati vengono scaricati e installati automaticamente nel sistema ASA R2 in base alle selezioni degli aggiornamenti.

Disattivare gli aggiornamenti automatici

Disattivare gli aggiornamenti automatici se si desidera visualizzare gli aggiornamenti consigliati prima di installarli. Se si disattivano gli aggiornamenti automatici, è necessario eseguire manualmente gli aggiornamenti del firmware e dei file di sistema.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Accanto a **aggiornamento automatico** selezionare , quindi selezionare **Disabilita**.

Risultato

Gli aggiornamenti automatici sono disattivati. Controllare regolarmente la presenza di aggiornamenti consigliati e decidere se si desidera eseguire un'installazione manuale.

Visualizzare gli aggiornamenti automatici

Visualizza un elenco di aggiornamenti del firmware e dei file di sistema scaricati nel cluster e pianificati per l'installazione automatica. Consente inoltre di visualizzare gli aggiornamenti precedentemente installati automaticamente.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Accanto a **aggiornamento automatico** selezionare , quindi selezionare **Visualizza tutti gli aggiornamenti automatici**.

Modificare gli aggiornamenti automatici

È possibile scegliere di scaricare e installare automaticamente gli aggiornamenti consigliati per il firmware dello storage, il firmware SP/BMC e i file di sistema nel cluster, oppure scegliere di chiudere automaticamente gli aggiornamenti consigliati. Se si desidera controllare manualmente l'installazione o l'eliminazione degli aggiornamenti, selezionare per ricevere una notifica quando è disponibile un aggiornamento consigliato; quindi, è possibile selezionare manualmente l'installazione o l'eliminazione.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Accanto a **aggiornamento automatico** selezionare , quindi selezionare **Modifica aggiornamenti automatici**.
3. Aggiorna le selezioni per gli aggiornamenti automatici.
4. Selezionare **Salva**.

Risultato

Gli aggiornamenti automatici vengono modificati in base alle selezioni effettuate.

Aggiornare il firmware manualmente

Se si desidera la flessibilità di visualizzare gli aggiornamenti consigliati prima che vengano scaricati e installati, è possibile disattivare gli aggiornamenti automatici e aggiornare il firmware manualmente.

Fasi

1. Scaricare il file di aggiornamento del firmware su un server o un client locale.
2. In System Manager, selezionare **Cluster > Overview**, quindi selezionare **Update**.
3. Selezionare **aggiornamento firmware**; quindi selezionare + Update firmware.

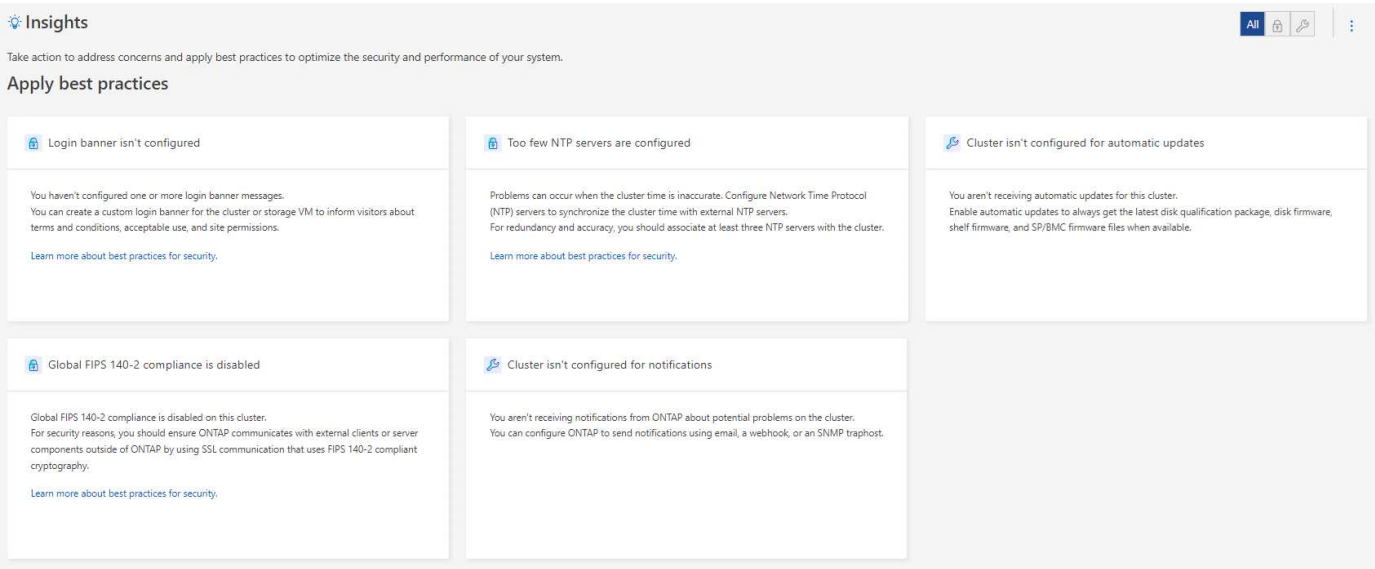
Risultato

Il firmware è stato aggiornato.

Ottimizza la sicurezza e le performance del cluster con informazioni dettagliate sul sistema storage ASA R2

Visualizza *Insights* in Gestione di sistema di ONTAP per identificare le Best practice e le modifiche alla configurazione che puoi implementare sul tuo sistema ASA R2 per ottimizzare la sicurezza e le performance del cluster.

Ad esempio, si supponga che per il cluster siano configurati server NTP (Network Time Protocol). Tuttavia, non si sa che il numero di server NTP consigliati per la gestione ottimale del tempo del cluster è inferiore a quello consigliato. Per evitare problemi che possono verificarsi quando il tempo del cluster è impreciso, Insights ti informerà che sono stati configurati troppi pochi server NTP e ti darà la possibilità di scoprire di più su questo problema, risolverlo o eliminarlo.



Fasi

1. In System Manager, selezionare **Insights**.
2. Rivedere i consigli.

Cosa succederà

Eseguire le azioni necessarie per implementare le Best practice e ottimizzare la sicurezza e le performance del cluster.

Visualizza eventi e processi del cluster sui sistemi di storage ASA R2

Utilizzare Gestione di sistema di ONTAP per visualizzare un elenco di errori o avvisi che si sono verificati nel sistema insieme alle azioni correttive consigliate. È inoltre possibile visualizzare i registri di controllo del sistema e un elenco dei processi attivi, completati o non riusciti.

Fasi

1. In System Manager, selezionare **Eventi e processi**.
2. Visualizzare eventi e processi del cluster.

Per visualizzare questo…	Eseguire questa operazione…
Eventi del cluster	Selezionare **Eventi**, quindi selezionare **Registro eventi**.
Suggerimenti Active IQ	Selezionare **Eventi**, quindi selezionare **Suggerimenti Active IQ**.
Avvisi di sistema	a. Selezionare **Avvisi di sistema**. b. Selezionare l'avviso di sistema per il quale si desidera eseguire l'azione. c. Riconoscere o sopprimere l'avviso.
Processi cluster	Selezionare **processi**.
Registri di audit	Selezionare **registri di controllo**.

Invia notifiche e-mail per eventi cluster e registri di controllo

Configurare il sistema in modo che invii una notifica a indirizzi e-mail specifici in caso di evento cluster o voce del registro di controllo.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Accanto a **Gestione notifiche** selezionare ⋮.
3. Per configurare una destinazione eventi, selezionare **Visualizza destinazioni eventi**, quindi selezionare **Destinazioni eventi**. Per configurare una destinazione del registro di controllo, selezionare **Visualizza destinazioni di controllo**, quindi selezionare **Destinazioni del registro di controllo**.
4. Selezionare + Add.
5. Immettere le informazioni sulla destinazione, quindi selezionare **Aggiungi**.

Risultato

L’indirizzo e-mail aggiunto riceverà le notifiche e-mail specificate per gli eventi del cluster e i registri di controllo.

Gestire i nodi

Riavviare un nodo su un sistema storage ASA R2

Potrebbe essere necessario riavviare un nodo per la manutenzione, la risoluzione dei problemi, gli aggiornamenti software o altri motivi amministrativi. Al riavvio di un nodo, il partner ha esegue automaticamente un takeover. Il nodo partner esegue quindi un giveback automatico dopo che il nodo riavviato torna online.

Fasi

1. In System Manager, selezionare **Cluster > Panoramica**.
2. Selezionare ⋮ accanto al nodo che si desidera riavviare, quindi selezionare **Reboot** (Riavvia).
3. Immettere il motivo per cui si sta riavviando il nodo, quindi selezionare **Reboot** (Riavvia).

   Il motivo del riavvio viene registrato nel registro di controllo del sistema.

Quali sono le prossime novità?

Durante il riavvio del nodo, il partner ha esegue un takeover in modo da evitare interruzioni del servizio dati. Una volta completato il reboot, il partner ha esegue un giveback.

Ridenominazione di un nodo in un sistema storage ASA R2

Puoi utilizzare Gestione sistema di ONTAP per rinominare un nodo sul sistema ASA R2. Potrebbe essere necessario rinominare un nodo per allinearlo alle convenzioni di denominazione dell’organizzazione o per altri motivi amministrativi.

Fasi

1. In System Manager, selezionare **Cluster > Panoramica**.
2. Selezionare ⋮ accanto al nodo che si desidera rinominare, quindi selezionare **Rinomina**.
3. Immettere il nuovo nome per il nodo, quindi selezionare **Rinomina**.

Risultato

Il nuovo nome viene applicato al nodo.

Gestire gli account e i ruoli degli utenti sui sistemi di storage ASA R2

Utilizzare System Manager per configurare l’accesso al controller di dominio Active Directory, l’autenticazione LDAP e SAML per gli account utente. Creare ruoli di account utente per definire funzioni specifiche che gli utenti assegnati ai ruoli possono eseguire nel cluster.

Configurare l’accesso al controller di dominio Active Directory

Configurare l’accesso al controller di dominio Active Directory (ad) al cluster o alla VM di storage in modo da abilitare l’accesso all’account ad.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Nella sezione **protezione**, in **Active Directory**, selezionare **Configura**.

Quali sono le prossime novità?

È ora possibile attivare l’accesso all’account ad sul sistema ASA R2.

Configure LDAP (Configura SNMP)

Configurare un server LDAP (Lightweight Directory Access Protocol) per gestire centralmente le informazioni degli utenti per l’autenticazione.

Prima di iniziare

È necessario aver generato una richiesta di firma del certificato e aggiunto un certificato digitale del server con firma CA.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Nella sezione **protezione**, accanto a **LDAP**, selezionare .
3. Immettere il server LDAP e le informazioni di associazione necessarie, quindi selezionare **Salva**.

Quali sono le prossime novità?

È ora possibile utilizzare LDAP per le informazioni utente e l’autenticazione.

Configurare l’autenticazione SAML

L’autenticazione SAML (Security Assertion Markup Language) consente agli utenti di essere autenticati da un provider di identità sicuro (IdP) invece che da fornitori di servizi diretti quali Active Directory e LDAP.

Prima di iniziare

- È necessario configurare l’IdP che si intende utilizzare per l’autenticazione remota.

  Vedere la documentazione IdP per la configurazione.

- È necessario disporre dell’URI dell’IdP.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. In **sicurezza**, accanto a **autenticazione SAML**, selezionare .
3. Selezionare **attiva autenticazione SAML**.
4. Immettere l’URL IdP e l’indirizzo IP del sistema host, quindi selezionare **Salva**.

   Una finestra di conferma visualizza le informazioni sui metadati, che sono state copiate automaticamente negli Appunti.

5. Vai al sistema IdP specificato, quindi copia i metadati dagli Appunti per aggiornare i metadati del sistema.
6. Tornare alla finestra di conferma in System Manager, quindi selezionare **ho configurato l'IdP con l'URI host o i metadati**.
7. Selezionare **Logout** per abilitare l'autenticazione basata su SAML.

   Il sistema IdP visualizza una schermata di autenticazione.

Quali sono le prossime novità?

È ora possibile utilizzare l'autenticazione SAML per gli account utente.

Creare ruoli account utente

I ruoli per gli amministratori del cluster e gli amministratori delle macchine virtuali storage vengono creati automaticamente al momento dell'inizializzazione del cluster. Creare ulteriori ruoli di account utente per definire funzioni specifiche che gli utenti assegnati ai ruoli possono eseguire nel cluster.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Nella sezione **protezione**, accanto a **utenti e ruoli**, selezionare →.
3. In **ruoli**, selezionare + Add .
4. Selezionare gli attributi del ruolo.

   Per aggiungere più attributi, selezionare + Add .
5. Selezionare **Salva**.

Risultato

Viene creato un nuovo account utente che può essere utilizzato sul sistema ASA R2.

Creare un account amministratore

Creare un account utente amministratore per consentire all'utente dell'account di eseguire azioni specifiche sul cluster in base al ruolo assegnato all'account. Per migliorare la protezione dell'account, impostare l'autenticazione a più fattori (MFA) quando si crea l'account.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Nella sezione **protezione**, accanto a **utenti e ruoli**, selezionare →.
3. In **utenti**, selezionare + Add .
4. Immettere un nome utente, quindi selezionare un ruolo da assegnare all'utente.
5. Selezionare il metodo di accesso utente e il metodo di autenticazione.
6. Per attivare MFA, selezionare + Add ; quindi un metodo di accesso secondario e un metodo di autenticazione
7. Immettere una password per l'utente.
8. Selezionare **Salva**.

Risultato

Viene creato un nuovo account amministratore che può essere utilizzato nel cluster ASA R2.

Gestione dei certificati di sicurezza sui sistemi di storage ASA R2

Utilizzare i certificati di sicurezza digitali per verificare l'identità dei server remoti.

Il protocollo OCSP (Online Certificate Status Protocol) convalida lo stato delle richieste di certificati digitali dai servizi ONTAP utilizzando connessioni SSL e TLS (Transport Layer Security).

Generare una richiesta di firma del certificato

Generare una richiesta di firma del certificato (CSR) per creare una chiave privata che può essere utilizzata per generare un certificato pubblico.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. In **sicurezza**, accanto a **certificati**, selezionare →; quindi selezionare + Generate CSR.
3. Immettere il nome comune dell'oggetto, quindi selezionare il paese.
4. Se si desidera modificare le impostazioni predefinite GSR, selezionare uso esteso dei tasti o aggiungere nomi alternativi dell'oggetto, selezionare ↙↗ More options; quindi effettuare gli aggiornamenti desiderati.
5. Selezionare **generate**.

Risultato

È stata generata una CSR che può essere utilizzata per generare un certificato pubblico.

Aggiungere un'autorità di certificazione attendibile

ONTAP fornisce un set predefinito di certificati root attendibili per le applicazioni che utilizzano TLS (Transport Layer Security). È possibile aggiungere ulteriori autorità di certificazione attendibili in base alle esigenze.

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. In **sicurezza**, accanto a **certificati**, selezionare →.
3. Selezionare **autorità di certificazione attendibili**.
4. Immettere o importare i dettagli del certificato, quindi selezionare + Add.

Risultato

È stata aggiunta una nuova autorità di certificazione attendibile al sistema ASA R2.

Rinnovare o eliminare un'autorità di certificazione attendibile

Le autorità di certificazione attendibili devono essere rinnovate annualmente. Se non si desidera rinnovare un certificato scaduto, è necessario eliminarlo.

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. In **sicurezza**, accanto a **certificati**, selezionare →.

3. Selezionare **autorità di certificazione attendibili**.
4. Selezionare l'autorità di certificazione attendibile che si desidera rinnovare o eliminare.
5. Rinnovare o eliminare l'autorità di certificazione.

Per rinnovare l'autorità di certificazione, procedere come indicato di seguito.	Per eliminare l'autorità di certificazione, procedere come indicato di seguito.
a. Selezionare ⋮; quindi selezionare **Rinnova**. b. Immettere o importare le informazioni sul certificato, quindi selezionare **Rinnova**.	a. Selezionare ⋮; quindi selezionare **Elimina**. b. Confermare che si desidera eliminare, quindi selezionare **Elimina**.

Risultato

È stata rinnovata o eliminata un'autorità di certificazione attendibile esistente nel sistema ASA R2.

Aggiungere un certificato client/server o le autorità di certificazione locali

Aggiungere un certificato client/server o le autorità di certificazione locali per abilitare i servizi Web protetti.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. In **sicurezza**, accanto a **certificati**, selezionare →.
3. Selezionare **certificati client/server** o **autorità di certificazione locali**.
4. Aggiungere le informazioni sul certificato, quindi selezionare + Add.

Risultato

È stato aggiunto un nuovo certificato client/server o autorità locali al sistema ASA R2.

Rinnovare o eliminare un certificato client/server o le autorità di certificazione locali

I certificati client/server e le autorità di certificazione locali devono essere rinnovati annualmente. Se non si desidera rinnovare un certificato scaduto o le autorità di certificazione locali, è necessario eliminarlo.

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. In **sicurezza**, accanto a certificati, selezionare →.
3. Selezionare **certificati client/server** o **autorità di certificazione locali**.
4. Selezionare il certificato che si desidera rinnovare o eliminare.
5. Rinnovare o eliminare l'autorità di certificazione.

Per rinnovare l'autorità di certificazione, procedere come indicato di seguito.	Per eliminare l'autorità di certificazione, procedere come indicato di seguito.
a. Selezionare ⋮; quindi selezionare **Rinnova**. b. Immettere o importare le informazioni sul certificato, quindi selezionare **Rinnova**.	Selezionare ⋮; quindi selezionare **Elimina**.

Risultato

È stato rinnovato o eliminato un certificato client/server esistente o un'autorità di certificazione locale sul sistema ASA R2.

Verifica della connettività host sul sistema di storage ASA R2

In caso di problemi con le operazioni dei dati host, è possibile utilizzare Gestione sistema di ONTAP per verificare che la connessione dall'host al sistema di storage ASA R2 sia attiva.

Fasi

1. In System Manager, selezionare **host**.

   Lo stato della connettività host viene indicato accanto al nome del gruppo di host come segue:

   - **OK**: Indica che tutti gli iniziatori sono collegati a entrambi i nodi.
   - **Partially Connected**: Indica che alcuni iniziatori non sono connessi a entrambi i nodi.
   - **Nessuno collegato**: Indica che non sono collegati iniziatori.

Quali sono le prossime novità?

Aggiorna l'host per correggere i problemi di connettività. Il ONTAP verificherà nuovamente lo stato della connessione ogni quindici minuti.

Esegui la manutenzione del tuo sistema storage ASA R2

```
https://docs.netapp.com/us-en/ontap-systems/asa-r2-landing-
maintain/index.html["Documentazione di manutenzione di ASA R2"^]Per
informazioni su come eseguire le procedure di manutenzione sui componenti
del sistema ASA R2, consultare la sezione.
```

Scopri di più

ASA R2 per power user della ONTAP

Confrontare i sistemi ASA R2 con gli altri sistemi ONTAP

I sistemi ASA R2 offrono una soluzione hardware e software unificata per ambienti solo SAN basati su piattaforme all-flash. I sistemi ASA R2 variano rispetto ad altri sistemi ONTAP (ASA, AFF e FAS) per quanto riguarda l'implementazione del layer di storage, dei protocolli supportati e della personalità ONTAP.

In un sistema ASA R2, il software ONTAP è ottimizzato per fornire il supporto per le funzionalità SAN essenziali, limitando al contempo la visibilità e la disponibilità di funzioni e funzioni non legate a SAN. Ad esempio, Gestione sistema in esecuzione su un sistema ASA R2 non visualizza le opzioni per la creazione di home directory per i client NAS. Questa versione semplificata di ONTAP è identificata come *personalità ASA R2*. ONTAP in esecuzione su tutti gli altri sistemi ONTAP (ASA, AFF, FAS) è identificato come *Unified ONTAP personality*. Le differenze tra le personalità ONTAP sono indicate nel riferimento comandi ONTAP (pagine man), nella specifica REST API e nei messaggi EMS, dove applicabile.

Puoi verificare la personalità dello storage ONTAP da System Manager o dall'interfaccia a riga di comando di ONTAP.

- Dal menu di System Manager, selezionare **Cluster > Overview**.
- Dalla CLI, immettere: `san config show`

La personalità del tuo sistema storage ONTAP non può essere modificata.

Il layer di storage per i sistemi ONTAP dotati di personalità ONTAP unificata utilizza gli aggregati come unità di base dello storage. Un aggregato possiede un set specifico di dischi disponibili in un sistema storage. L'aggregato alloca spazio sui dischi di cui è proprietario nei volumi per LUN e namespace. Un utente ONTAP unificato può utilizzare l'interfaccia a riga di comando (CLI) per creare e modificare aggregati, volumi, LUN e namespace.

Il layer di storage dei sistemi ASA R2 utilizza una zona di disponibilità dello storage invece degli aggregati. Una zona di disponibilità dello storage è un pool comune di storage che ha accesso a tutti i dischi disponibili nel sistema di archiviazione. La zona di disponibilità dello storage è visibile a entrambi i nodi in una coppia ha ASA R2. Al momento della creazione di un'unità di storage (basata su un namespace LUN o NVMe), ONTAP crea automaticamente un volume contenente una Storage Virtual Machine (VM) nella zona di disponibilità dello storage per alloggiare l'unità storage. Grazie a questo approccio semplificato e automatizzato alla gestione dello storage, alcune opzioni di System Manager, i comandi di ONTAP e gli endpoint delle API REST non sono disponibili o hanno un utilizzo limitato in un sistema ASA R2. Ad esempio, poiché la creazione e la gestione dei volumi sono automatizzate per i sistemi ASA R2, il menu **volumi** non viene visualizzato in Gestione sistema e il `volume create` comando non è supportato.

Lo storage ASA R2 si confronta con altri sistemi storage ONTAP nei seguenti modi:

	ASA r2	ASA	AFF	FAS
ONTAP Personality	ASA r2	ASA	Unificato	Unificato
Supporto del protocollo SAN	Sì	Sì	Sì	Sì
Supporto protocollo NAS	No	No	Sì	Sì
Supporto livello di archiviazione	Zona di disponibilità dello storage	Aggregati	Aggregati	Aggregati

Le seguenti piattaforme ASA sono classificate come sistemi ASA R2:

- ASA A1K
- ASA A70
- ASA A90

Per ulteriori informazioni

- Ulteriori informazioni su "Sistemi hardware ONTAP".
- Vedere il supporto completo della configurazione e le limitazioni per i sistemi ASA e ASA R2 in "NetApp Hardware Universe".
- Ulteriori informazioni su "NetApp ASA".

Riepilogo delle differenze del sistema ASA R2

Di seguito sono descritte le principali differenze tra i sistemi ASA R2 e i sistemi FAS, AFF e ASA relativi all'interfaccia a riga di comando (CLI) e all'API REST di ONTAP.

Creazione di SVM predefinita con servizi di protocollo

I nuovi cluster contengono automaticamente una SVM dati predefinita con i protocolli SAN abilitati. Le interfacce LIF dati IP supportano i protocolli iSCSI e NVMe/TCP e utilizzano `default-data-blocks` la policy di servizio per impostazione predefinita.

Creazione automatica di un volume

La creazione di un'unità di storage (LUN o namespace) crea automaticamente un volume dalla zona di disponibilità dello storage. Ciò si traduce in uno spazio dei nomi comune e semplificato. L'eliminazione di un'unità di memorizzazione elimina automaticamente il volume associato.

Modifiche a thin provisioning e thick provisioning

Le unità di storage per vengono sempre fornite in thin provisioning sui sistemi di storage ASA R2. Il thick provisioning non è supportato.

Supporto e limitazioni del software ONTAP per i sistemi di storage ASA R2

Sebbene i sistemi ASA R2 offrano un'ampia gamma di supporto per le soluzioni SAN, alcune funzionalità del software ONTAP non sono supportate.

I sistemi ASA R2 non supportano quanto segue:

- Failover LIF iSCSI
- FabricPool
- Thick provisioning LUN
- MetroCluster
- Protocolli a oggetti
- API ONTAP S3 SnapMirror e S3
- Da SnapMirror al cloud
- Da SnapMirror a sistemi non ASA R2
- Mappa LUN selettiva (SLM)

I sistemi ASA R2 supportano quanto segue:

- SnapLock
- Crittografia a doppio layer

Per ulteriori informazioni

- Per "NetApp Hardware Universe"ulteriori informazioni sul supporto hardware e sulle limitazioni di ASA R2, consultare la.
- "Informazioni su come bloccare le istantanee" Sul sistema ASA R2.
- "Scopri come applicare la crittografia a doppio livello" Ai dati sul sistema ASA R2.

Supporto dell'interfaccia CLI ONTAP per i sistemi storage ASA R2

Invece degli aggregati tradizionali, che gestiscono un set specifico di dischi disponibili in un sistema storage, i sistemi ASA R2 utilizzano *una zona di disponibilità dello storage*. Una zona di disponibilità dello storage è un pool comune di storage che ha accesso a tutti i dischi disponibili nel sistema di archiviazione. La zona di disponibilità dello storage è visibile a entrambi i nodi in una coppia ha ASA R2. Quando viene creata un'unità di storage (namespace LUN o NVMe), ONTAP crea automaticamente un volume contenente una Storage Virtual Machine (VM) nella zona di disponibilità dello storage per alloggiare l'unità di storage.

Grazie a questo approccio semplificato alla gestione dello storage, `storage aggregate` i comandi non sono supportati sui sistemi ASA R2. `lun` `volume`Anche il supporto di determinati comandi e parametri è limitato.

I seguenti comandi e set di comandi non sono supportati in ASA su R2:

Comandi <code> DENGINE </code> non supportati

- `lun copy`
- `lun geometry`
- `lun import`
- `lun mapping add-reportng-nodes`
- `lun mapping-remove-reporting-nodes`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

  Questo comando viene sostituito con la ridenominazione del namespace nvme lun Rename/vserver.

- `lun transition`

I comandi e i parametri </code> non supportati per <code>

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

  Questo comando non è disponibile se utilizzato insieme ai seguenti parametri:

  - `-anti-ransomware-state`
  - `-autosize`
  - `-autosize-mode`
  - `-autosize-shrik-threshold-percent`
  - `-autosize-reset`
  - `-group`
  - `-is-cloud-write-enabled`
  - `-is-space-enforcement-logical`
  - `-max-autosize`
  - `-min-autosize`
  - `-offline`
  - `-online`
  - `-percent-snapshot-space`
  - `-qos*`
  - `-size`
  - `-snapshot-policy`
  - `-space-guarantee`
  - `-space-mgmt-try-first`
  - `-state`
  - `-tiering-policy`
  - `-tiering-minimum-cooling-days`
  - `-user`
  - `-unix-permisions`
  - `-vserver-dr-protection`
- `volume make-vsroot`
- `volume mount`

- `volume move`
- `volume offline`
- `volume rehost`
- `volume rename`
- `volume restrict`
- `volume transition-prepare-to-downgrade`
- `volume unmount`

Comandi </code> di <code> hdebcloesk non supportati

- `volume clone create`
- `volume clone split`

Comandi <code> DENGINE SnapLock </code> non supportati

- `volume snaplock modify`

Comandi <code> </code> non supportati

- `volume snapshot`
- `volume snapshot autodelete modify`
- `volume snapshot policy modify`

Set di comandi </code> <code> non supportati

- `volume activity-tracking`
- `volume analytics`
- `volume conversion`
- `volume file`
- `volume flexcache`
- `volume flexgroup`
- `volume inode-upgrade`
- `volume object-store`
- `volume qtree`
- `volume quota`
- `volume reallocation`
- `volume rebalance`
- `volume recovery-queue`
- `volume schedule-style`

Comandi </code> non supportati per <code>

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

Per ulteriori informazioni

Per "Riferimento comando ONTAP"un elenco completo dei comandi supportati, consultare la

Configurare un cluster ONTAP ASA R2 utilizzando la CLI

Si consiglia di "Utilizza System Manager per configurare il cluster ONTAP ASA R2". System Manager offre un workflow guidato rapido e semplice per rendere operativo il cluster. Tuttavia, se sei abituato a lavorare con i comandi di ONTAP, l'interfaccia a riga di comando (CLI) di ONTAP può essere utilizzata facoltativamente per il setup del cluster. Il cluster configurato con l'utilizzo della CLI non offre opzioni o vantaggi aggiuntivi rispetto al cluster configurato con System Manager.

Durante il setup del cluster viene creata la tua macchina virtuale per lo storage dei dati predefinita, viene creata un'unità storage iniziale e vengono rilevate automaticamente le LIF dati. In alternativa, è possibile abilitare il DNS (Domain Name System) per risolvere i nomi host, impostare il cluster in modo che utilizzi il NTS (Network Time Protocol) per la sincronizzazione dell'ora e abilitare la crittografia dei dati a riposo.

Prima di iniziare

Raccogliere le seguenti informazioni:

- Indirizzo IP di gestione del cluster

  L'indirizzo IP di gestione del cluster è un indirizzo IPv4 univoco per l'interfaccia di gestione del cluster, utilizzata dall'amministratore del cluster per accedere alla VM di storage di amministrazione e gestire il cluster. È possibile ottenere questo indirizzo IP dall'amministratore responsabile dell'assegnazione degli indirizzi IP all'interno dell'organizzazione.

- Subnet mask di rete

  Durante la configurazione del cluster, ONTAP consiglia una serie di interfacce di rete appropriate per la configurazione in uso. Se necessario, è possibile modificare il suggerimento.

- Indirizzo IP del gateway di rete
- Indirizzo IP del nodo partner
- Nomi di dominio DNS
- Indirizzi IP del server dei nomi DNS
- Indirizzi IP del server NTP
- Data subnet mask (Subnet mask dati)

Fasi

1. Accendere entrambi i nodi della coppia ha.
2. Mostra i nodi rilevati sulla rete locale:

   ```
   system node show-discovered -is-in-cluster false
   ```

3. Avviare la procedura guidata di configurazione del cluster:

   ```
   cluster setup
   ```

4. Riconoscere l'istruzione AutoSupport.
5. Inserire i valori per la porta dell'interfaccia di gestione dei nodi, l'indirizzo IP, la maschera di rete e il gateway predefinito.
6. Premere **Invio** per continuare l'installazione utilizzando l'interfaccia della riga di comando, quindi immettere **create** per creare un nuovo cluster.
7. Accettare le impostazioni predefinite del sistema o inserire i propri valori.
8. Una volta completata la configurazione sul primo nodo, accedere al cluster.
9. Verificare che il cluster sia attivo e che il primo nodo sia integro:

   ```
   system node show-discovered
   ```

10. Aggiungere il secondo nodo al cluster:

```
cluster add-node -cluster-ip <partner_node_ip_address>
```

11. In alternativa, è possibile sincronizzare l'ora del sistema nel cluster

Sincronizza senza autenticazione simmetrica	`cluster time-service ntp server create -server <server_name>`
Sincronizza con autenticazione simmetrica	`cluster time-service ntp server create -server <server_ip_address> -key-id <key_id>`

a. Verificare che il cluster sia associato a un server NTP:

```
Cluster time-service ntp show
```

12. In alternativa, scaricare ed eseguire "ActiveIQ Config Advisor" per confermare la configurazione.

Quali sono le prossime novità?

Sei pronto per "impostare l'accesso ai dati"passare dai client SAN al tuo sistema.

Supporto delle API REST per ASA R2

L'API REST di ASA R2 si basa sull'API REST fornita con la personalità ONTAP unificata, con una serie di modifiche adattate alle caratteristiche e alle capacità uniche della personalità ASA R2.

Tipi di modifiche alle API

Esistono diversi tipi di differenze tra l'API REST del sistema ASA R2 e l'API REST ONTAP unificata disponibile con i sistemi FAS, AFF e ASA. La comprensione dei tipi di modifiche consente di utilizzare al meglio la documentazione di riferimento API online.

I nuovi endpoint ASA R2 non sono supportati in Unified ONTAP

Sono stati aggiunti diversi endpoint all'API REST di ASA R2 che non sono disponibili con Unified ONTAP.

Ad esempio, un nuovo endpoint block-volume è stato aggiunto all'API REST per i sistemi ASA R2. L'endpoint del volume a blocchi offre l'accesso agli oggetti del namespace LUN e NVMe, consentendo una vista aggregata delle risorse. Questa opzione è disponibile solo tramite l'API REST.

Come altro esempio, gli endpoint **storage-unit** offrono una vista aggregata di LUN e namespace NVMe. Ci sono diversi endpoint e sono tutti basati su o derivati da `/api/storage/storage-units`. È inoltre necessario rivedere `/api/storage/luns` e `/api/storage/namespaces`.

Restrizioni sui metodi HTTP utilizzati per alcuni endpoint

Diversi endpoint disponibili con ASA R2 hanno restrizioni su quali metodi HTTP possono essere utilizzati rispetto a Unified ONTAP. Ad esempio, POST ed ELIMINAZIONE non sono consentiti quando si utilizza l'endpoint `/api/protocols/nvme/services` con i sistemi ASA R2.

Modifiche alle proprietà per un endpoint e un metodo HTTP

Alcune combinazioni di endpoint e metodo del sistema ASA R2 non supportano tutte le proprietà definite disponibili nel linguaggio ONTAP unificato. Ad esempio, quando si utilizza la PATCH con l'endpoint `/api/storage/volumes/{uuid}`, diverse proprietà non sono supportate con ASA R2, tra cui:

- `autosize.maximum`
- `autosize.minimum`
- `autosize.mode`

Modifiche all'elaborazione interna

Sono state apportate diverse modifiche al modo in cui ASA R2 elabora determinate richieste di API REST. Ad esempio, una richiesta di ELIMINAZIONE con l'endpoint `/api/storage/luns/{uuid}` viene elaborata in modo asincrono.

Maggiore sicurezza con OAuth 2,0

OAuth 2,0 è il quadro di autorizzazione standard del settore. Viene utilizzato per limitare e controllare l'accesso alle risorse protette in base ai token di accesso firmati. È possibile configurare OAuth 2,0 utilizzando Gestione sistema per proteggere le risorse di sistema di ASA R2.

Dopo aver configurato OAuth 2,0 con System Manager, è possibile controllare l'accesso da parte dei client dell'API REST. È necessario innanzitutto ottenere un token di accesso da un server di autorizzazione. Il client REST passa quindi il token al cluster ASA R2 come token bearer utilizzando l'intestazione della richiesta di autorizzazione HTTP. Per ulteriori informazioni, vedere "Autenticazione e autorizzazione utilizzando OAuth 2,0" .

Accedere alla documentazione di riferimento dell'API di ASA R2 tramite l'interfaccia utente Swagger

È possibile accedere alla documentazione di riferimento delle API REST tramite l'interfaccia utente Swagger nel sistema ASA R2.

A proposito di questa attività

Per informazioni dettagliate sull'API REST, accedere alla pagina della documentazione di riferimento di ASA R2. Come parte di questo, è possibile cercare la stringa **specifiche della piattaforma** per trovare dettagli sul supporto del sistema ASA R2 per le chiamate e le proprietà API.

Prima di iniziare

È necessario disporre di quanto segue:

- Indirizzo IP o nome host della LIF di gestione cluster del sistema ASA R2
- Nome utente e password di un account con autorizzazione ad accedere all'API REST

Fasi

1. Digitare l'URL nel browser e premere **Invio**:
   `https://<ip_address>/docs/api`

2. Accedere utilizzando l’account amministratore.

   Viene visualizzata la pagina di documentazione dell’API di ASA R2 con le chiamate API organizzate nelle principali categorie di risorse.

3. Per visualizzare un esempio di chiamata API applicabile solo ai sistemi ASA R2, scorrere fino alla categoria **SAN** e fare clic su **GET /storage/storage-units**.

Richiedi assistenza

Gestisci AutoSupport sui sistemi storage ASA R2

AutoSupport è un meccanismo che monitora in modo proattivo lo stato di salute del sistema e invia automaticamente messaggi al supporto tecnico NetApp, all'organizzazione di supporto interna e a un partner di supporto.

I messaggi AutoSupport al supporto tecnico sono abilitati per impostazione predefinita quando si configura il cluster. È necessario impostare le opzioni corrette e disporre di un host di posta valido per l'invio dei messaggi all'organizzazione di supporto interna. ONTAP inizia a inviare messaggi AutoSupport 24 ore dopo l'attivazione.

Prima di iniziare

Per gestire AutoSupport è necessario essere un amministratore del cluster.

Verificare la connettività AutoSupport

Dopo aver configurato il cluster, è necessario verificare la connettività AutoSupport per verificare che il supporto tecnico riceva i messaggi generati da AutoSupport.

Fasi

1. In Gestione di sistema, selezionare **Cluster >Settings**.
2. Accanto a **AutoSupport** selezionare ⋮; quindi selezionare **verifica connettività**.
3. Immettere un oggetto per il messaggio AutoSupport, quindi selezionare **Invia messaggio AutoSupport di prova**.

Quali sono le prossime novità?

Il supporto tecnico è in grado di ricevere messaggi AutoSupport dal sistema ASA R2 e dispone dei dati necessari per assisterti in caso di problemi.

Aggiungi destinatari AutoSupport

Aggiungere i membri dell'organizzazione di assistenza interna all'elenco degli indirizzi e-mail che ricevono i messaggi AutoSupport.

Fasi

1. In Gestione di sistema, selezionare **Cluster >Settings**.
2. Accanto a **AutoSupport** selezionare ⋮; quindi selezionare **altre opzioni**.
3. Accanto a **e-mail**, selezionare ✎; quindi selezionare + Add .
4. Immettere l'indirizzo e-mail del destinatario, quindi la categoria del destinatario.

   Per i partner, selezionare **Partner** per la categoria destinatario. Selezionare **Generale** per i membri dell'organizzazione di supporto interna.

5. Selezionare Salva.

Quali sono le prossime novità?

Gli indirizzi e-mail aggiunti riceveranno nuovi messaggi AutoSupport per la categoria di destinatari specifica.

Invia dati AutoSupport

In caso di problemi del sistema ASA R2, i dati di AutoSupport possono ridurre significativamente il tempo necessario per identificare e risolvere i problemi.

Fasi

1. In Gestione di sistema, selezionare **Cluster >Settings**.
2. Accanto a **AutoSupport** selezionare ⋮; quindi selezionare **generate and send** (genera e invia*).
3. Immettere un oggetto per il messaggio AutoSupport, quindi selezionare **Invia**.

Quali sono le prossime novità?

I dati AutoSupport vengono inviati all'assistenza tecnica.

Elimina la generazione dei casi di supporto

Se si sta eseguendo un aggiornamento o una manutenzione sul sistema ASA R2, potrebbe essere utile sospendere la generazione di casi di supporto AutoSupport fino al completamento dell'aggiornamento o della manutenzione.

Fasi

1. In Gestione di sistema, selezionare **Cluster >Settings**.
2. Accanto a **AutoSupport** selezionare ⋮; quindi selezionare **Sospendi generazione casi di supporto**.
3. Specificare il numero di ore per sospendere la generazione di casi di supporto, quindi selezionare i nodi per i quali non si desidera generare casi.
4. Selezionare **Invia**.

Quali sono le prossime novità?

I casi AutoSupport non verranno generati durante il tempo specificato. Se l'upgrade o la manutenzione vengono completati prima della scadenza del tempo specificato, dovresti riprendere immediatamente la generazione del caso di supporto.

Riprendere la generazione dei casi di supporto

Se la generazione di casi di supporto è stata sospesa durante una finestra di aggiornamento o manutenzione, riprendere la generazione di casi di supporto subito dopo il completamento dell'aggiornamento o della manutenzione.

Fasi

1. In Gestione di sistema, selezionare **Cluster >Settings**.
2. Accanto a **AutoSupport** selezionare ⋮; quindi selezionare **Riprendi generazione caso supporto**.
3. Selezionare i nodi per i quali si desidera riprendere i casi AutoSupport generati.
4. Selezionare **Invia**.

Risultato

I casi AutoSupport vengono generati automaticamente per il sistema ASA R2, in base alle esigenze.

Invio e visualizzazione dei casi di supporto per i sistemi storage ASA R2

Se hai un problema che richiede assistenza, puoi utilizzare ONTAP System Manager per inviare un caso al supporto tecnico. È inoltre possibile utilizzare Gestione di sistema di ONTAP per visualizzare i casi chiusi o in corso.

Devi "Registrato con Active IQ"visualizzare i casi di supporto per il tuo sistema ASA R2.

Fasi

1. Per inviare un caso di supporto, in Gestione sistema, selezionare **cluster >supporto**, quindi selezionare **Vai al supporto NetApp**.
2. Per visualizzare un caso inviato in precedenza, in System Manager selezionare **Cluster >Support**, quindi selezionare **View my cases**.

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

Informazioni sul copyright

Informazioni sul marchio commerciale