Amministrare e monitorare

ASA r2

NetApp
September 26, 2024

Sommario

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.

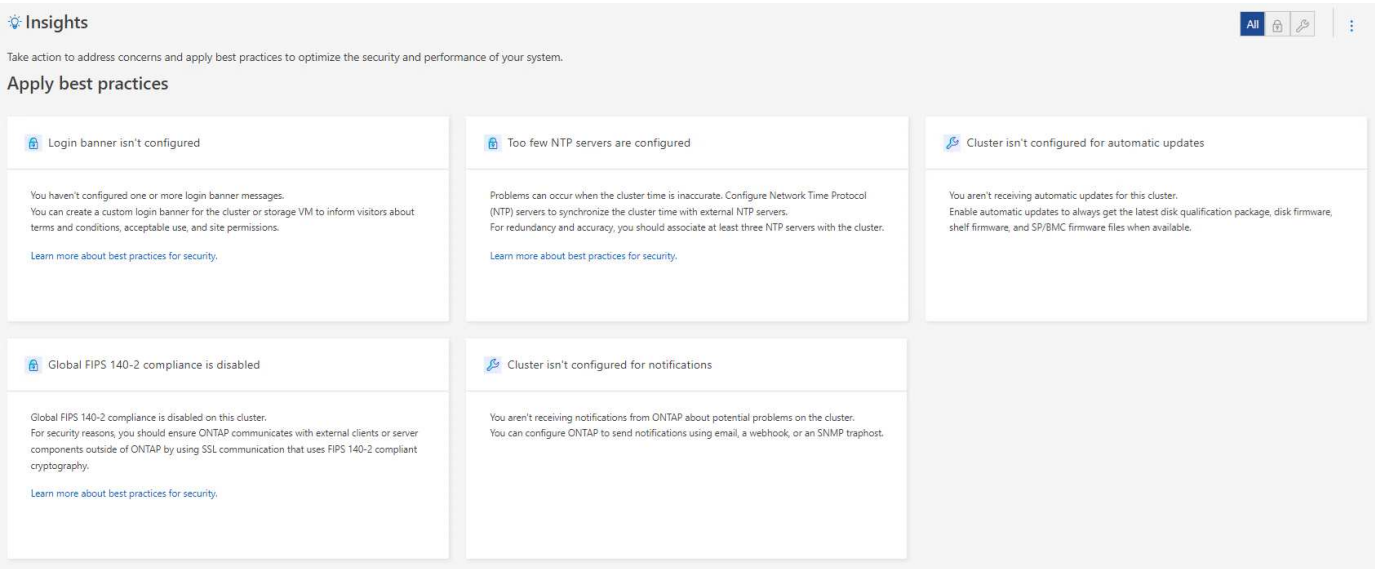
Risultato

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.

Informazioni sul copyright

Informazioni sul marchio commerciale