Administration und Überwachung

ASA r2

NetApp
September 26, 2024

Inhalt

Administration und Überwachung

Management des Client-Zugriffs auf Storage-VMs auf ASA r2 Storage-Systemen

Storage-Einheiten eines ASA r2-Systems befinden sich in Storage Virtual Machines (VMs). Storage-VMs dienen der Bereitstellung von Daten für Ihre SAN-Clients. Erstellen Sie mit ONTAP System Manager eine LIF (Netzwerkschnittstelle) für Ihre SAN-Clients, um eine Storage-VM anzuschließen und auf Daten in den Storage-Einheiten zuzugreifen. Optional können Sie Subnetze zur Vereinfachung der LIF-Erstellung und IPspaces verwenden, um Ihren Storage VMs ihren eigenen sicheren Storage, die Administration und das Routing bereitzustellen.

Erstellen von IPspaces

Ein IPspace ist ein eindeuiger IP-Adressbereich, in dem sich Storage-VMs befinden. Wenn Sie IPspaces erstellen, ermöglichen Sie Ihren Storage-VMs ihren eigenen sicheren Storage, ihre Administration und ihr eigenes sicheres Routing. Außerdem können Clients in administrativ getrennten Netzwerkdomänen überlappende IP-Adressen aus demselben IP-Adressensubnetz verwenden.

Sie müssen einen IPspace erstellen, bevor Sie ein Subnetz erstellen können.

Schritte

1. Wählen Sie **Netzwerk > Übersicht**.
2. Wählen Sie unter **IPspaces** die Option + Add .
3. Geben Sie einen Namen für die IP-Adresse ein, oder übernehmen Sie den Standardnamen.

   Der IPspace-Name kann nicht „all“ sein, da „all“ ein systemreservierter Name ist.

4. Wählen Sie **Speichern**.

Was kommt als Nächstes?

Nachdem Sie nun einen IPspace erstellt haben, können Sie ihn zum Erstellen eines Subnetzes verwenden.

Subnetze erstellen

Ein Subnetz ermöglicht es Ihnen, bestimmte Blöcke von IPv4- oder IPv6-Adressen zuzuweisen, die beim Erstellen einer LIF (Netzwerkschnittstelle) verwendet werden sollen. Ein Subnetz vereinfacht die LIF-Erstellung, da Sie in der Lage sind, den Subnetznamen anstelle einer bestimmten IP-Adresse und Netzwerkmaske für jede LIF anzugeben.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Der "Broadcast-Domäne" und IP-Bereich, in dem Sie das Subnetz hinzufügen möchten, muss bereits vorhanden sein.

Schritte

1. Wählen Sie **Netzwerk > Übersicht**.

2. Wählen Sie **Subnetze** aus, und wählen Sie dann + Add .
3. Geben Sie den Subnetznamen ein.

   Alle Subnetznamen müssen innerhalb eines IPspaces eindeutig sein.

4. Geben Sie die Subnetz-IP-Adresse und die Subnetzmaske ein.
5. Geben Sie den IP-Adressbereich für das Subnetz an.

   Wenn Sie den IP-Adressbereich für das Subnetz angeben, überlappen Sie IP-Adressen nicht mit anderen Subnetzen. Netzwerkprobleme können auftreten, wenn sich Subnetz-IP-Adressen überlappen und unterschiedliche Subnetze oder Hosts versuchen, dieselbe IP-Adresse zu verwenden.

6. Wählen Sie die Broadcast-Domäne für das Subnetz aus.
7. Wählen Sie **Hinzufügen**.

Was kommt als Nächstes?

Sie haben ein Subnetz erstellt, mit dem Sie nun die Erstellung Ihrer LIFs vereinfachen können.

LIF erstellen (Netzwerkschnittstelle)

Eine LIF (Netzwerkschnittstelle) ist eine IP-Adresse, die einem physischen oder logischen Port zugeordnet ist. Erstellen Sie LIFs an den Ports, die Sie für den Datenzugriff verwenden möchten. Storage-VMs stellen Daten über ein oder mehrere LIFs für Clients bereit. Bei einem Komponentenausfall kann eine LIF ein Failover durchführen oder zu einem anderen physischen Port migriert werden, sodass die Netzwerkkommunikation nicht unterbrochen wird.

Wenn eine IP-Daten-LIF erstellt wird, kann sie standardmäßig sowohl iSCSI- als auch NVMe/TCP-Datenverkehr verarbeiten. Für den FC- und NVMe/FC-Datenverkehr müssen getrennte Daten-LIFs erstellt werden.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Der zugrunde liegende physische oder logische Netzwerkport muss im Administratorstatus konfiguriert worden `up` sein.
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.
- Ein LIF, die Intracluster-Datenverkehr zwischen Nodes verarbeiten, sollte sich nicht im selben Subnetz wie ein LIF-Handling-Datenverkehr oder eine LIF mit Datenverkehr befinden.

Schritte

1. Wählen Sie **Netzwerk > Übersicht**.
2. Wählen Sie **Netzwerkschnittstellen** aus, und wählen Sie dann + Add .
3. Wählen Sie den Schnittstellentyp und das Protokoll aus und anschließend die Storage-VM aus.
4. Geben Sie einen Namen für das LIF ein, oder übernehmen Sie den Standardnamen.
5. Wählen Sie den Startknoten für die Netzwerkschnittstelle aus, und geben Sie dann die IP-Adresse und die Subnetzmaske ein.
6. Wählen Sie **Speichern**.

Ergebnis

Sie haben eine LIF für den Datenzugriff erstellt.

Ändern einer LIF (Netzwerkschnittstellen)

LIFs können bei Bedarf deaktiviert oder umbenannt werden. Sie können auch die LIF-IP-Adresse und die Subnetzmaske ändern.

Schritte

1. Wählen Sie **Netzwerk > Übersicht** und dann **Netzwerkschnittstellen**.
2. Bewegen Sie den Mauszeiger über die Netzwerkschnittstelle, die Sie bearbeiten möchten, und wählen Sie dann ⋮.
3. Wählen Sie **Bearbeiten**.
4. Sie können die Netzwerkschnittstelle deaktivieren, die Netzwerkschnittstelle umbenennen, die IP-Adresse ändern oder die Subnetzmaske ändern.
5. Wählen Sie **Speichern**.

Ergebnis

Ihr LIF wurde geändert.

Managen Sie Cluster-Netzwerke auf ASA r2 Storage-Systemen

Mit ONTAP System Manager können Sie eine grundlegende Storage-Netzwerkadministration auf Ihrem ASA r2 System durchführen. Sie können beispielsweise eine Broadcast-Domäne hinzufügen oder Ports einer anderen Broadcast-Domäne neu zuweisen.

Fügen Sie eine Broadcast-Domäne hinzu

Verwenden Sie Broadcast-Domänen, um das Management Ihres Cluster-Netzwerks zu vereinfachen, indem Sie Netzwerkports gruppieren, die zum gleichen Layer-2-Netzwerk gehören. Storage Virtual Machines (VMs) können dann die Ports in der Gruppe für Daten- oder Managementdatenverkehr verwenden.

Während des Cluster-Setups werden die „Standard“-Broadcast-Domäne und die „Cluster“ Broadcast-Domäne erstellt. Die „Standard“-Broadcast-Domäne enthält Ports, die sich im „Standard“-IPspace befinden. Diese Ports werden hauptsächlich zum Bereitstellen von Daten genutzt. Auch Cluster-Management- und Node-Management-Ports befinden sich in dieser Broadcast-Domäne. Die Broadcast-Domain „Cluster“ enthält Ports die sich im „Cluster“ IPspace befinden. Diese Ports werden für die Cluster-Kommunikation verwendet und umfassen alle Cluster-Ports aus allen Nodes im Cluster.

Sie können zusätzliche Broadcast-Domänen erstellen, nachdem das Cluster initialisiert wurde. Wenn Sie eine Broadcast-Domäne erstellen, wird automatisch eine Failover-Gruppe erstellt, die dieselben Ports enthält.

Über diese Aufgabe

Die maximale Übertragungseinheit (MTU) der Ports, die einer Broadcast-Domäne hinzugefügt wurden, wird auf den in der Broadcast-Domäne eingestellten MTU-Wert aktualisiert.

Schritte

1. Wählen Sie im System Manager **Netzwerk > Übersicht** aus.

2. Wählen Sie unter **Broadcast** Domains die Option + Add.
3. Geben Sie einen Namen für die Broadcast-Domäne ein, oder akzeptieren Sie den Standardnamen.

   Alle Broadcast-Domain-Namen müssen innerhalb eines IPspaces eindeutig sein.

4. Wählen Sie den IPspace für die Broadcast-Domäne aus.

   Wenn Sie keinen IPspace-Namen angeben, wird die Broadcast-Domain im „Standard“-IPspace erstellt.

5. Geben Sie die maximale Übertragungseinheit (MTU) ein.

   MTU ist das größte Datenpaket, das in Ihrer Broadcast-Domäne akzeptiert werden kann.

6. Wählen Sie die gewünschten Ports aus, und wählen Sie dann **Speichern**.

Ergebnis

Sie haben eine neue Broadcast-Domäne hinzugefügt.

Weisen Sie Ports einer anderen Broadcast-Domäne neu zu

Ports können nur zu einer Broadcast-Domäne gehören. Wenn Sie die Broadcast-Domäne ändern möchten, zu der ein Port gehört, müssen Sie den Port seiner vorhandenen Broadcast-Domäne einer neuen Broadcast-Domäne zuweisen.

Schritte

1. Wählen Sie im System Manager **Netzwerk > Übersicht** aus.
2. Wählen Sie unter **Broadcast Domains** ⋮ neben dem Domainnamen aus, und wählen Sie dann **Bearbeiten**.
3. Heben Sie die Auswahl der Ethernet-Ports auf, die Sie einer anderen Domäne neu zuweisen möchten.
4. Wählen Sie die Broadcast-Domain aus, der Sie den Port neu zuweisen möchten, und wählen Sie dann **Neu zuweisen** aus.
5. Wählen Sie **Speichern**.

Ergebnis

Sie haben Ports einer anderen Broadcast-Domäne neu zugewiesen.

Erstellen Sie eine VLAN

Ein VLAN besteht aus Switch-Ports, die zu einer Broadcast-Domäne zusammengefasst sind. Mithilfe von VLANs können Sie die Sicherheit erhöhen, Probleme isolieren und verfügbare Pfade innerhalb Ihrer IP-Netzwerkinfrastruktur einschränken.

Bevor Sie beginnen

Die im Netzwerk implementierten Switches müssen entweder den IEEE 802.1Q Standards entsprechen oder über eine anbieterspezifische Implementierung von VLANs verfügen.

Über diese Aufgabe

- Ein VLAN kann nicht auf einem Port der Schnittstellengruppe erstellt werden, der keine Mitgliedsports enthält.
- Wenn Sie ein VLAN zum ersten Mal über einen Port konfigurieren, könnte der Port ausfallen, was zu einer vorübergehenden Trennung des Netzwerks führt. Nachfolgende VLAN-Erweiterungen zum selben Port

wirken sich nicht auf den Portstatus aus.

- Sie sollten kein VLAN auf einer Netzwerkschnittstelle mit derselben Kennung wie das native VLAN des Switches erstellen. Wenn beispielsweise die Netzwerkschnittstelle e0b auf nativem VLAN 10 ist, sollten Sie keine VLAN e0b-10 auf dieser Schnittstelle erstellen.

Schritte

1. Wählen Sie im System Manager **Netzwerk > Ethernet-Ports** aus, und wählen Sie dann + VLAN.
2. Wählen Sie den Knoten und die Broadcast-Domäne für das VLAN aus.
3. Wählen Sie den Port für das VLAN aus.

   Das VLAN kann nicht mit einem Port verbunden werden, der eine Cluster-LIF hostet, oder mit den dem Cluster-IPspace zugewiesenen Ports.

4. Geben Sie eine VLAN-ID ein.
5. Wählen Sie **Speichern**.

Ergebnis

Sie haben ein VLAN erstellt, um die Sicherheit zu erhöhen, Probleme zu isolieren und die verfügbaren Pfade innerhalb Ihrer IP-Netzwerkinfrastruktur einzuschränken.

Überwachung der Nutzung und Erhöhung der Kapazität

Überwachung der Performance von Clustern und Speichereinheiten auf ASA r2-Storage-Systemen

Überwachen Sie mit ONTAP System Manager die Gesamt-Performance Ihres Clusters und die Performance bestimmter Storage-Einheiten, um zu bestimmen, wie Latenz, IOPS und Durchsatz sich auf Ihre geschäftskritischen Applikationen auswirken. Die Performance kann über verschiedene Zeiträume von einer Stunde bis zu einem Jahr überwacht werden.

Nehmen wir zum Beispiel an, eine geschäftskritische Applikation hat eine hohe Latenz und einen niedrigen Durchsatz. Wenn Sie die Cluster-Performance der letzten fünf Arbeitstage anzeigen, bemerken Sie jeden Tag einen Performance-Abfall zur gleichen Zeit. Anhand dieser Informationen können Sie ermitteln, ob die kritische Anwendung im Wettbewerb um Clusterressourcen steht, wenn im Hintergrund ein nicht kritischer Prozess ausgeführt wird. Anschließend können Sie Ihre QoS-Richtlinie ändern, um die Auswirkungen des nicht kritischen Workloads auf Systemressourcen zu begrenzen und sicherzustellen, dass Ihre kritische Workload die minimalen Durchsatzziele erfüllt.

Überwachen Sie die Cluster-Performance

Mithilfe von Cluster-Performance-Kennzahlen können Sie bestimmen, ob Sie Workloads verlagern müssen, um die Latenz zu minimieren sowie die IOPS und den Durchsatz Ihrer kritischen Applikationen zu maximieren.

Schritte

1. Wählen Sie in System Manager **Dashboard** aus.
2. Unter **Performance** sehen Sie die Latenz, IOPS und den Durchsatz für den Cluster nach Stunde, Tag, Woche, Monat oder Jahr.
3.

Wählen Sie  diese Option, um die Leistungsdaten herunterzuladen.

Was kommt als Nächstes?

Analysieren Sie mithilfe Ihrer Cluster-Performance-Kennzahlen, ob Sie Ihre QoS-Richtlinien ändern oder andere Anpassungen an den Applikations-Workloads vornehmen müssen, um die Cluster-Performance insgesamt zu maximieren.

Überwachung der Leistung der Speichereinheit

Verwenden Sie Performance-Kennzahlen der Storage-Einheit, um den Einfluss spezifischer Applikationen auf Latenz, IOPS und Durchsatz zu bestimmen.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die zu überwachende Speichereinheit aus, und wählen Sie dann **Übersicht**.
3. Unter **Performance** sehen Sie die Latenz, IOPS und den Durchsatz für die Speichereinheit nach Stunde, Tag, Woche, Monat oder Jahr.
4. Wählen Sie  diese Option, um die Leistungsdaten herunterzuladen.

Was kommt als Nächstes?

Analysieren Sie mithilfe Ihrer Performance-Kennzahlen der Storage-Einheiten, ob Sie die QoS-Richtlinien, die Ihren Storage-Einheiten zugewiesen sind, ändern müssen, um die Latenz zu verringern und die IOPS und den Durchsatz zu maximieren.

Überwachung der Auslastung von Clustern und Speichereinheiten auf ASA r2-Storage-Systemen

Mit ONTAP System Manager überwachen Sie Ihre Storage-Auslastung, um sicherzustellen, dass Sie die Storage-Kapazität haben, die Sie für aktuelle und zukünftige Workloads benötigen.

Überwachen der Cluster-Auslastung

Überwachen Sie regelmäßig den von Ihrem Cluster verbrauchten Storage, um sicherzustellen, dass Sie bei Bedarf bereit sind, die Cluster-Kapazität zu erweitern, bevor der Speicherplatz knapp wird.

Schritte

1. Wählen Sie in System Manager **Dashboard** aus.
2. Unter **Capacity** sehen Sie die Menge des physisch belegten Speicherplatzes und die Menge des verfügbaren Speicherplatzes auf Ihrem Cluster.

   Die Datenreduzierungsration gibt den durch Storage-Effizienz eingesparten Speicherplatz an.

Was kommt als Nächstes?

Wenn der Speicherplatz des Clusters knapp "Fügen Sie neue Laufwerke hinzu"ist oder nicht über die Kapazität verfügt, um zukünftigen Anforderungen gerecht zu werden, sollten Sie Ihr ASA r2 System einplanen, um Ihre Storage-Kapazität zu erhöhen.

Überwachung der Auslastung der Speichereinheiten

Überwachen Sie den Storage-Verbrauch einer Storage-Einheit, um proaktiv die Größe der Storage-Einheit ganz nach Ihren Bedürfnissen zu erweitern.

Schritte

1. Wählen Sie im System Manager **Storage** aus.
2. Wählen Sie die zu überwachende Speichereinheit aus, und wählen Sie dann **Übersicht**.
3. Sehen Sie sich unter **Speicher** Folgendes an:
   - Größe der Speichereinheit
   - Menge des belegten Speicherplatzes
   - Datenreduzierungsquote

     Das Datenreduzierungsverhältnis stellt den durch Storage-Effizienz eingesparten Speicherplatz dar
   - Verwendeter Snapshot

     Der von Snapshots verwendete Snapshot stellt die Größe des von Snapshots verwendeten Speichers dar.

Was kommt als Nächstes?

Wenn sich die Speicherkapazität Ihrer Speichereinheit nähert, sollten Sie "Ändern Sie die Speichereinheit"sie vergrößern.

Erhöhen Sie die Storage-Kapazität auf ASA r2 Storage-Systemen

Fügen Sie zu einem Node oder Shelf Laufwerke hinzu, um die Storage-Kapazität Ihres ASA r2 Systems zu erhöhen.

Verwenden Sie NetApp Hardware Universe, um die Installation eines neuen Laufwerks vorzubereiten

Bevor Sie ein neues Laufwerk an einem Node oder Shelf installieren, verwenden Sie den NetApp Hardware Universe, um sicherzustellen, dass das hinzuzufügende Laufwerk von Ihrer ASA r2-Plattform unterstützt wird, und um den richtigen Steckplatz für das neue Laufwerk zu ermitteln. Die richtigen Steckplätze zum Hinzufügen von Laufwerken variieren je nach Plattformmodell und ONTAP-Version. In einigen Fällen müssen Sie in der Folge Laufwerke zu bestimmten Steckplätzen hinzufügen.

Schritte

1. Gehen Sie zum "NetApp Hardware Universe".
2. Wählen Sie unter **Produkte** Ihre Hardwarekonfigurationen aus.
3. Wählen Sie Ihre ASA r2-Plattform aus.
4. Wählen Sie Ihre ONTAP-Version aus, und wählen Sie dann **Ergebnisse anzeigen**.
5. Wählen Sie unter der Grafik **Klicken Sie hier, um alternative Ansichten zu sehen**; wählen Sie dann die Ansicht, die Ihrer Konfiguration entspricht.
6. Überprüfen Sie anhand der Konfigurationsansicht, ob das neue Laufwerk unterstützt wird und ob der richtige Steckplatz für die Installation vorhanden ist.

Ergebnis

Sie haben bestätigt, dass Ihr neues Laufwerk unterstützt wird, und Sie kennen den passenden Steckplatz für die Installation.

Installieren Sie ein neues Laufwerk auf dem ASA r2

Die Mindestanzahl der Laufwerke, die Sie in einem einzigen Verfahren hinzufügen sollten, beträgt sechs. Das Hinzufügen eines einzigen Laufwerks kann zu einer Performance-Verringerung führen.

Über diese Aufgabe

Wiederholen Sie die Schritte in diesem Verfahren für jedes Laufwerk.

Schritte

1. Richtig gemahlen.
2. Entfernen Sie vorsichtig die Blende von der Vorderseite der Plattform.
3. Setzen Sie das neue Laufwerk in den richtigen Steckplatz ein.
   a. Setzen Sie den neuen Antrieb mit beiden Händen ein, indem Sie den Nockengriff in die offene Position bringen.
   b. Drücken Sie, bis das Laufwerk stoppt.
   c. Schließen Sie den Nockengriff, so dass der Antrieb fest in der Mittelebene sitzt und der Griff einrastet.

      Schließen Sie den Nockengriff langsam, damit er korrekt an der Antriebsfläche ausgerichtet ist.
4. Vergewissern Sie sich, dass die Aktivitäts-LED (grün) des Laufwerks leuchtet.
   - WENN die LED konstant leuchtet, wird das Laufwerk mit Strom versorgt.
   - Wenn die LED blinkt, wird das Laufwerk mit Strom versorgt und E/A wird ausgeführt. Die LED blinkt auch, wenn die Laufwerksfirmware aktualisiert wird.

     Die Laufwerk-Firmware wird automatisch (unterbrechungsfrei) auf neuen Laufwerken aktualisiert, die keine aktuellen Firmware-Versionen aufweisen.
5. Wenn der Node für die automatische Laufwerkszuweisung konfiguriert ist, können Sie warten, bis ONTAP die neuen Laufwerke einem Node automatisch zuweist. Ist der Node nicht für die automatische Laufwerkszuweisung konfiguriert oder ist er vorzuziehen, können Sie die Laufwerke manuell zuweisen.

   Die neuen Laufwerke werden erst erkannt, wenn sie einem Node zugewiesen sind.

Was kommt als Nächstes?

Nachdem die neuen Laufwerke erkannt wurden, überprüfen Sie, ob sie hinzugefügt wurden und ihre Eigentumsrechte korrekt angegeben wurden.

Aktualisieren der Firmware auf ASA r2-Speichersystemen

ONTAP lädt automatisch Firmware- und Systemdateien auf Ihrem ASA r2-System herunter und aktualisiert diese standardmäßig. Wenn Sie die Möglichkeit haben möchten, empfohlene Updates vor dem Herunterladen und Installieren anzuzeigen, können Sie ONTAP System Manager verwenden, um automatisierte Updates zu deaktivieren oder Aktualisierungsparameter zu bearbeiten, um Ihnen Benachrichtigungen über verfügbare Updates anzuzeigen, bevor eine Aktion durchgeführt wird.

Aktivieren Sie automatische Updates

Empfohlene Updates für Speicher-Firmware, SP/BMC-Firmware und Systemdateien werden automatisch heruntergeladen und standardmäßig auf Ihrem ASA r2-System installiert. Wenn automatische Updates deaktiviert wurden, können Sie sie aktivieren, um das Standardverhalten wiederherzustellen.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie neben **Automatic Update** ⋮, und wählen Sie dann **enable**.
3. Lesen und akzeptieren Sie die EULA.
4. Akzeptieren Sie die Standardeinstellungen, um Ihre Firmware und Systemdateien automatisch zu aktualisieren. Wählen Sie optional aus, um Benachrichtigungen anzuzeigen oder empfohlene Updates automatisch zu verwerfen.
5. Wählen Sie diese Option, um zu bestätigen, dass Ihre Aktualisierungsänderungen auf alle aktuellen und zukünftigen Aktualisierungen angewendet werden.
6. Wählen Sie **Speichern**.

Ergebnis

Empfohlene Aktualisierungen werden automatisch heruntergeladen und auf Ihrem ASA r2-System installiert, basierend auf Ihrer Auswahl für das Update.

Deaktivieren Sie automatische Updates

Deaktivieren Sie automatische Updates, wenn Sie die Möglichkeit haben möchten, empfohlene Updates vor der Installation anzuzeigen. Wenn Sie automatische Updates deaktivieren, müssen Sie Firmware- und Systemdateiaktualisierungen manuell durchführen.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie neben **Automatic Update** ⋮, und wählen Sie dann **Disable**.

Ergebnis

Automatische Updates sind deaktiviert. Sie sollten regelmäßig nach empfohlenen Updates suchen und entscheiden, ob Sie eine manuelle Installation durchführen möchten.

Automatische Updates anzeigen

Zeigen Sie eine Liste der Firmware- und Systemdatei-Updates an, die auf das Cluster heruntergeladen wurden und für die automatische Installation geplant sind. Zeigen Sie auch Updates an, die zuvor automatisch installiert wurden.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie neben **Automatisches Update** ⋮, und wählen Sie dann **Alle automatischen Updates anzeigen**.

Automatische Aktualisierungen bearbeiten

Sie können festlegen, dass empfohlene Updates für Storage-Firmware, SP/BMC Firmware und Ihre Systemdateien automatisch heruntergeladen und auf dem Cluster installiert werden. Alternativ können Sie

festlegen, dass empfohlene Updates automatisch verworfen werden. Wenn Sie die Installation oder das Entlassen von Updates manuell steuern möchten, wählen Sie die Option, um benachrichtigt zu werden, wenn eine empfohlene Aktualisierung verfügbar ist. Sie können dann manuell auswählen, um sie zu installieren oder zu schließen.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie neben **Automatisches Update** ⋮, und wählen Sie dann **Automatische Updates bearbeiten**.
3. Aktualisieren Sie die Auswahl für automatische Aktualisierungen.
4. Wählen Sie **Speichern**.

Ergebnis

Automatische Aktualisierungen werden basierend auf Ihrer Auswahl geändert.

Aktualisieren Sie die Firmware manuell

Wenn Sie die Möglichkeit haben möchten, empfohlene Updates vor dem Herunterladen und Installieren anzuzeigen, können Sie automatische Updates deaktivieren und Ihre Firmware manuell aktualisieren.

Schritte

1. Laden Sie die Firmware-Aktualisierungsdatei auf einen Server oder lokalen Client herunter.
2. Wählen Sie im System Manager **Cluster > Übersicht**, und wählen Sie dann **Update**.
3. Wählen Sie **Firmware-Update**; die Option + Update firmware.

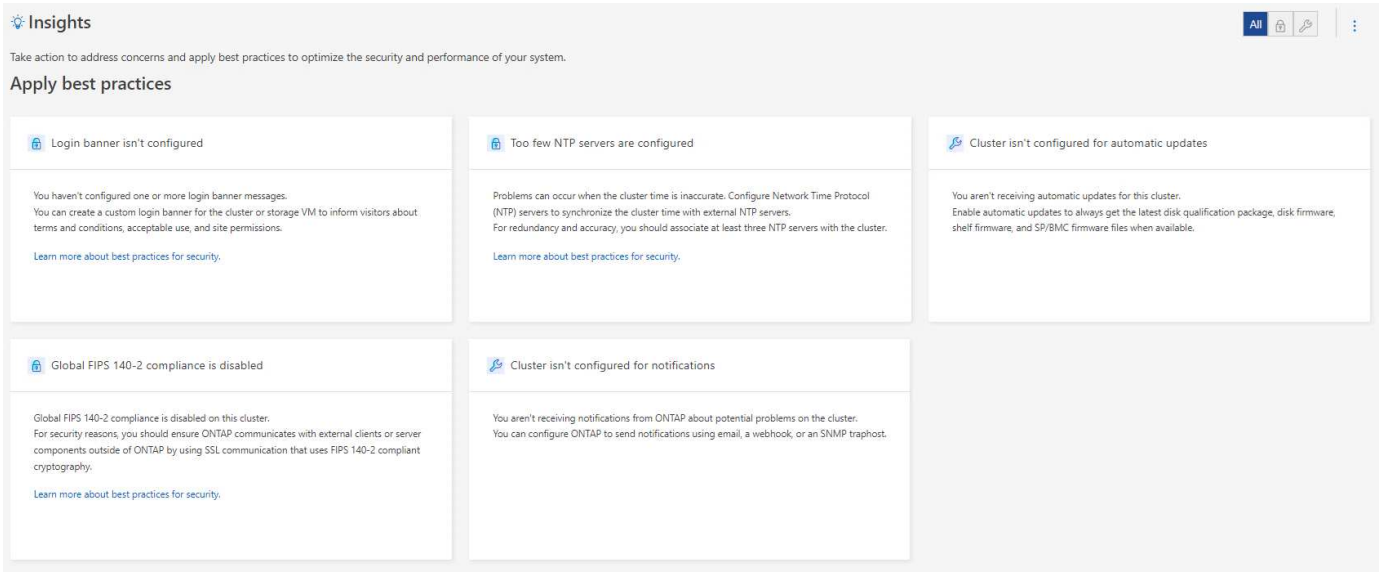
Ergebnis

Ihre Firmware wird aktualisiert.

ASA r2 Storage-System bietet Einblick in Cluster-Sicherheit und -Performance

Zeigen Sie *Insights* im ONTAP-System-Manager an, um Best Practices und Konfigurationsänderungen zu ermitteln, die Sie auf Ihrem ASA r2-System implementieren können, um Clustersicherheit und -Leistung zu optimieren.

Angenommen, Sie haben für das Cluster NTP-Server (Network Time Protocol) konfiguriert. Sie wissen jedoch nicht, dass für ein optimales Cluster-Zeitmanagement weniger als die empfohlene Anzahl von NTP-Servern erforderlich ist. Damit Sie Probleme vermeiden können, die bei ungenauer Cluster-Zeit auftreten können, werden Sie von Insights benachrichtigt, dass zu wenige NTP-Server konfiguriert sind, und Sie haben die Möglichkeit, mehr über dieses Problem zu erfahren, das Problem zu beheben oder es zu schließen.



Schritte

1. Wählen Sie im System Manager **Insights** aus.
2. Besprechen Sie die Empfehlungen.

Wie es weiter geht

Führen Sie alle erforderlichen Aktionen durch, um Best Practices zu implementieren und die Sicherheit und Performance des Clusters zu optimieren.

Anzeigen von Clusterereignissen und -Jobs auf ASA r2-Speichersystemen

Verwenden Sie ONTAP System Manager, um eine Liste der Fehler oder Warnmeldungen anzuzeigen, die in Ihrem System aufgetreten sind, sowie empfohlene Korrekturmaßnahmen. Sie können auch Systemauditprotokolle und eine Liste von Jobs anzeigen, die aktiv, abgeschlossen oder fehlgeschlagen sind.

Schritte

1. Wählen Sie im System Manager **Ereignisse & Jobs** aus.
2. Anzeigen von Clusterereignissen und -Jobs

Um dies anzuzeigen…	Tun Sie das…
Cluster-Ereignisse	Wählen Sie **Events**, und wählen Sie dann **Event Log**.
Vorschläge von Active IQ	Wählen Sie **Ereignisse** und dann **Active IQ Suggestions**.
Systemmeldungen	a. Wählen Sie **System Alerts**. b. Wählen Sie die Systemwarnung aus, für die Sie Maßnahmen ergreifen möchten. c. Bestätigen oder unterdrücken Sie die Warnmeldung.

Um dies anzuzeigen…	Tun Sie das…
Cluster-Jobs	Wählen Sie **Jobs**.
Prüfprotokolle	Wählen Sie **Audit-Protokolle**.

Senden von E-Mail-Benachrichtigungen für Cluster-Ereignisse und Prüfprotokolle

Konfigurieren Sie das System so, dass eine Benachrichtigung an bestimmte E-Mail-Adressen gesendet wird, wenn ein Clusterereignis- oder Überwachungsprotokolleintrag vorhanden ist.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie neben **Benachrichtigungsverwaltung** ⋮.
3. Um ein Ereignisziel zu konfigurieren, wählen Sie **Ereignisziele anzeigen** und dann **Ereignisziele**. Wählen Sie zum Konfigurieren eines Überwachungsprotokollziels **Überwachungsziele anzeigen** aus, und wählen Sie dann **Überwachungsziele** aus.
4. Wählen Sie + Add.
5. Geben Sie die Zielinformationen ein, und wählen Sie dann **Hinzufügen**.

Ergebnis

Die von Ihnen hinzugefügte E-Mail-Adresse erhält nun die angegebenen E-Mail-Benachrichtigungen für Clusterereignisse und Prüfprotokolle.

Managen von Nodes

Starten Sie einen Node auf einem ASA r2-Speichersystem neu

Möglicherweise müssen Sie einen Node aus Wartungsgründen, zur Fehlerbehebung, zu Softwareupdates oder aus anderen administrativen Gründen neu booten. Beim Neustart eines Node führt der HA-Partner automatisch eine Übernahme aus. Der Partner-Node führt dann ein automatisches Giveback durch, nachdem der neu gebootete Node wieder online geschaltet wurde.

Schritte

1. Wählen Sie im System Manager **Cluster > Übersicht** aus.
2. Wählen Sie ⋮ neben dem Knoten, den Sie neu starten möchten, und wählen Sie dann **Neustart**.
3. Geben Sie den Grund für das Neustarten des Knotens ein, und wählen Sie dann **Neustart** aus.

   Der von Ihnen eingegebene Grund für das Neubooten wird im Systemauditprotokoll aufgezeichnet.

Was kommt als Nächstes?

Während des Neubootens des Node führt der HA-Partner einen Takeover aus, sodass der Datenservice nicht unterbrochen wird. Nach Abschluss des Neubootens führt der HA-Partner ein Giveback durch.

Benennen Sie einen Knoten in einem ASA r2-Speichersystem um

Sie können ONTAP System Manager verwenden, um einen Knoten auf dem ASA r2-System umzubenennen. Möglicherweise müssen Sie einen Node umbenennen, um ihn an die Namenskonventionen Ihres Unternehmens oder aus anderen administrativen Gründen anzupassen.

Schritte

1. Wählen Sie im System Manager **Cluster > Übersicht** aus.
2. Wählen Sie ⋮ neben dem Knoten, den Sie umbenennen möchten, und wählen Sie dann **Umbenennen**.
3. Geben Sie den neuen Namen für den Knoten ein, und wählen Sie dann **Umbenennen**.

Ergebnis

Der neue Name wird auf den Node angewendet.

Managen von Benutzerkonten und Rollen auf ASA r2 Storage-Systemen

Mit System Manager können Sie den Active Directory-Domänencontroller-Zugriff sowie die LDAP- und SAML-Authentifizierung für Ihre Benutzerkonten konfigurieren. Erstellen Sie Benutzerkontorollen, um bestimmte Funktionen zu definieren, die Benutzer, die den Rollen zugewiesen sind, auf dem Cluster ausführen können.

Konfigurieren Sie den Zugriff auf den Active Directory-Domänencontroller

Konfigurieren Sie den Active Directory (AD) Domain Controller-Zugriff auf das Cluster oder die Storage-VM, damit Sie den Zugriff auf das AD-Konto aktivieren können.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** unter **Active Directory Konfigurieren** aus.

Was kommt als Nächstes?

Sie können nun den AD-Kontozugriff auf Ihrem ASA r2-System aktivieren.

LDAP konfigurieren

Konfigurieren Sie einen LDAP-Server (Lightweight Directory Access Protocol) zur zentralen Verwaltung von Benutzerinformationen für die Authentifizierung.

Bevor Sie beginnen

Sie müssen eine Zertifikatsignierungsanforderung erstellt und ein digitales Zertifikat für einen CA-signierten Server hinzugefügt haben.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** neben **LDAP** die Option ⚙.

3. Geben Sie den erforderlichen LDAP-Server und die Verbindungsinformationen ein, und wählen Sie dann **Speichern**.

Was kommt als Nächstes?

Sie können jetzt LDAP für Benutzerinformationen und Authentifizierung verwenden.

Konfigurieren Sie die SAML-Authentifizierung

Die SAML-Authentifizierung (Security Assertion Markup Language) ermöglicht die Authentifizierung von Benutzern durch einen sicheren Identitätsanbieter (Secure Identity Provider, IdP) anstelle von direkten Dienstanbietern wie Active Directory und LDAP.

Bevor Sie beginnen

- Der IdP, den Sie für die Remote-Authentifizierung verwenden möchten, muss konfiguriert werden.

  Informationen zur Konfiguration finden Sie in der IdP-Dokumentation.

- Sie müssen die URI des IdP haben.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie unter **Sicherheit** neben **SAML-Authentifizierung** die Option ⚙ .
3. Wählen Sie **SAML-Authentifizierung aktivieren**.
4. Geben Sie die IdP-URL und die IP-Adresse des Hostsystems ein, und wählen Sie dann **Speichern**.

   In einem Bestätigungsfenster werden die Metadateninformationen angezeigt, die automatisch in die Zwischenablage kopiert wurden.

5. Wechseln Sie zum angegebenen IdP-System, und kopieren Sie dann die Metadaten aus der Zwischenablage, um die Systemmetadaten zu aktualisieren.
6. Kehren Sie zum Bestätigungsfenster im System Manager zurück; wählen Sie dann **I have configured the IdP with the Host URI or metadata** aus.
7. Wählen Sie **Abmelden**, um die SAML-basierte Authentifizierung zu aktivieren.

   Das IdP-System zeigt einen Authentifizierungsbildschirm an.

Was kommt als Nächstes?

Sie können jetzt die SAML-Authentifizierung für Ihre Benutzerkonten verwenden.

Erstellen von Benutzerkontorollen

Rollen für Cluster-Administratoren und Storage-VM-Administratoren werden automatisch erstellt, wenn das Cluster initialisiert wird. Erstellen Sie zusätzliche Benutzerkontorollen, um bestimmte Funktionen zu definieren, die Benutzer, die den Rollen zugewiesen sind, auf Ihrem Cluster ausführen können.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** neben **Benutzer und Rollen** die Option →.
3. Wählen Sie unter **Rollen** die Option + Add .

4. Wählen Sie die Rollenattribute aus.

   Um mehrere Attribute hinzuzufügen, wählen Sie + Add .

5. Wählen Sie **Speichern**.

Ergebnis

Ein neues Benutzerkonto wird erstellt und steht für die Verwendung auf Ihrem ASA r2-System zur Verfügung.

Erstellen Sie ein Administratorkonto

Erstellen Sie ein Administrator-Benutzerkonto, mit dem der Account-Benutzer basierend auf der dem Konto zugewiesenen Rolle bestimmte Aktionen für den Cluster ausführen kann. Um die Kontosicherheit zu verbessern, richten Sie bei der Erstellung des Kontos eine Multi-Faktor-Authentifizierung (MFA) ein.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie im Abschnitt **Sicherheit** neben **Benutzer und Rollen** die Option →.
3. Wählen Sie unter **Benutzer** die Option + Add .
4. Geben Sie einen Benutzernamen ein, und wählen Sie dann eine Rolle aus, die dem Benutzer zugewiesen werden soll.
5. Wählen Sie die Benutzeranmeldemethode und die Authentifizierungsmethode aus.
6. Um MFA zu aktivieren, wählen Sie + Add ; und wählen Sie dann eine sekundäre Anmeldemethode und Authentifizierungsmethode aus
7. Geben Sie ein Kennwort für den Benutzer ein.
8. Wählen Sie **Speichern**.

Ergebnis

Ein neues Administratorkonto wird erstellt und steht für den ASA r2-Cluster zur Verfügung.

Managen von Sicherheitszertifikaten auf ASA r2-Speichersystemen

Verwenden Sie digitale Sicherheitszertifikate, um die Identität von Remote-Servern zu überprüfen.

Online Certificate Status Protocol (OCSP) validiert den Status von digitalen Zertifikatsanforderungen von ONTAP-Diensten mithilfe von SSL- und TLS-Verbindungen (Transport Layer Security).

Generieren Sie eine Anforderung zum Signieren eines Zertifikats

Erstellen Sie eine Zertifikatsignierungsanforderung (CSR), um einen privaten Schlüssel zu erstellen, mit dem ein öffentliches Zertifikat erstellt werden kann.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie unter **Security** neben **Certificates** die Option →; und wählen Sie dann + Generate CSR.

3. Geben Sie den allgemeinen Namen des Studienteilnehmers ein, und wählen Sie dann das Land aus.
4. Wenn Sie die GSR-Standardwerte ändern möchten, wählen Sie Erweiterte Tastenverwendung oder fügen Sie alternative Namen für 

das Thema hinzu, wählen Sie ; und dann die gewünschten Aktualisierungen vornehmen.
5. Wählen Sie **Erzeugen**.

Ergebnis

Sie haben eine CSR erstellt, mit der Sie ein öffentliches Zertifikat erstellen können.

Fügen Sie eine vertrauenswürdige Zertifizierungsstelle hinzu

ONTAP bietet einen Standardsatz vertrauenswürdiger Stammzertifikate für Anwendungen, die TLS (Transport Layer Security) verwenden. Sie können bei Bedarf weitere vertrauenswürdige Zertifizierungsstellen hinzufügen.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie unter **Sicherheit** neben **Zertifikate** die Option →.
3. Wählen Sie **Vertrauenswürdige Zertifizierungsstellen**.
4. Geben Sie die Zertifikatdetails ein oder importieren Sie 

sie, und wählen Sie dann .

Ergebnis

Sie haben Ihrem ASA r2-System eine neue vertrauenswürdige Zertifizierungsstelle hinzugefügt.

Erneuern oder Löschen einer vertrauenswürdigen Zertifizierungsstelle

Vertrauenswürdige Zertifizierungsstellen müssen jährlich erneuert werden. Wenn Sie ein abgelaufenes Zertifikat nicht erneuern möchten, sollten Sie es löschen.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie unter **Sicherheit** neben **Zertifikate** die Option →.
3. Wählen Sie **Vertrauenswürdige Zertifizierungsstellen**.
4. Wählen Sie die Zertifizierungsstelle aus, die Sie erneuern oder löschen möchten.
5. Erneuern oder löschen Sie die Zertifizierungsstelle.

Um die Zertifizierungsstelle zu erneuern, gehen Sie folgendermaßen vor:	Gehen Sie folgendermaßen vor, um die Zertifizierungsstelle zu löschen:
a. Wählen Sie ⋮; und dann **erneuern**. b. Geben Sie die Zertifikatinformationen ein oder importieren Sie sie, und wählen Sie dann **Renew** aus.	a. Wählen Sie ⋮; und dann **Löschen**. b. Bestätigen Sie, dass Sie löschen möchten, und wählen Sie dann **Löschen**.

Ergebnis

Sie haben eine vorhandene vertrauenswürdige Zertifizierungsstelle auf Ihrem ASA r2-System erneuert oder gelöscht.

Fügen Sie ein Client/Server-Zertifikat oder lokale Zertifizierungsstellen hinzu

Fügen Sie ein Client/Server-Zertifikat oder lokale Zertifizierungsstellen hinzu, um sichere Webdienste zu ermöglichen.

Schritte

1. Wählen Sie in System Manager **Cluster > Einstellungen** aus.
2. Wählen Sie unter **Sicherheit** neben **Zertifikate** die Option →.
3. Wählen Sie **Client/Server-Zertifikate** oder **Local Certificate Authorities** aus.
4. Fügen Sie die Zertifikatinformationen hinzu, und wählen Sie dann + Add.

Ergebnis

Sie haben Ihrem ASA r2-System ein neues Client/Server-Zertifikat oder lokale Behörden hinzugefügt.

Erneuern oder löschen Sie ein Client/Server-Zertifikat oder lokale Zertifizierungsstellen

Client/Server-Zertifikate und lokale Zertifizierungsstellen müssen jährlich erneuert werden. Wenn Sie ein abgelaufenes Zertifikat oder eine lokale Zertifizierungsstelle nicht erneuern möchten, sollten Sie diese löschen.

Schritte

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie unter **Sicherheit** neben Zertifikate die Option →.
3. Wählen Sie **Client/Server-Zertifikate** oder **Lokale Zertifizierungsstellen** aus.
4. Wählen Sie das Zertifikat aus, das Sie erneuern oder löschen möchten.
5. Erneuern oder löschen Sie die Zertifizierungsstelle.

Um die Zertifizierungsstelle zu erneuern, gehen Sie folgendermaßen vor:	Gehen Sie folgendermaßen vor, um die Zertifizierungsstelle zu löschen:
a. Wählen Sie ⋮; und dann **erneuern**. b. Geben Sie die Zertifikatinformationen ein oder importieren Sie sie, und wählen Sie dann **Renew** aus.	Wählen Sie ⋮; und dann **Löschen**.

Ergebnis

Sie haben ein vorhandenes Client/Server-Zertifikat oder eine lokale Zertifizierungsstelle auf Ihrem ASA r2-System erneuert oder gelöscht.

Überprüfen Sie die Hostkonnektivität auf Ihrem ASA r2-Speichersystem

Wenn bei den Host-Datenvorgängen ein Problem auftritt, können Sie mithilfe von ONTAP System Manager überprüfen, ob die Verbindung zwischen dem Host und dem ASA r2 Storage-System aktiv ist.

Schritte

1. Wählen Sie im System Manager **Host** aus.

   Der Host-Konnektivitätsstatus wird neben dem Namen der Host-Gruppe wie folgt angezeigt:

   - **OK**: Zeigt an, dass alle Initiatoren mit beiden Knoten verbunden sind.
   - **Teilweise verbunden**: Zeigt an, dass einige der Initiatoren nicht mit beiden Knoten verbunden sind.
   - **Keine Verbindung**: Zeigt an, dass keine Initiatoren verbunden sind.

Was kommt als Nächstes?

Aktualisieren Sie Ihren Host, um Verbindungsprobleme zu beheben. ONTAP überprüft den Verbindungsstatus alle 15 Minuten erneut.