Sicherheit und Datenverschlüsselung

ONTAP 9

NetApp
April 24, 2024

Inhalt

Sicherheit und Datenverschlüsselung

Überblick über das Sicherheitsmanagement mit System Manager

Ab ONTAP 9.7 managen Sie die Cluster-Sicherheit mit System Manager.

Mit System Manager können Kunden anhand von Standardmethoden von ONTAP den Storage-Zugriff von Clients und Administratoren sichern und sich gegen Viren schützen. Fortschrittliche Technologien stehen zur Verschlüsselung von Daten im Ruhezustand und ALS WORM Storage zur Verfügung.

Wenn Sie den klassischen System-Manager verwenden (nur in ONTAP 9.7 und früher verfügbar), lesen Sie "System Manager Classic (ONTAP 9.0 bis 9.7)"

Virus-Scan

Sie können die integrierte Virenschutzfunktionalität des Storage-Systems verwenden, um Daten vor Viren oder anderen schädlichen Angriffen zu schützen. ONTAP Virus Scanning, genannt *Vscan*, kombiniert erstklassige Antivirensoftware von Drittanbietern mit ONTAP-Funktionen, die Ihnen die Flexibilität geben, die Sie benötigen, um zu kontrollieren, welche Dateien gescannt werden und wann.

Verschlüsselung

ONTAP bietet sowohl Software- als auch hardwarebasierte Verschlüsselungstechnologien, um sicherzustellen, dass Daten im Ruhezustand nicht gelesen werden können, wenn das Storage-Medium neu verwendet, zurückgegeben, verloren gegangen oder gestohlen wird.

WORM-Storage

SnapLock ist eine hochperformante Compliance-Lösung für Unternehmen, die WORM_-Storage (Write Once_, _Read Many) verwenden, um kritische Dateien zu regulatorischen und Governance-Zwecken in unveränderter Form aufzubewahren.

Schutz vor Ransomware

Autonome Ransomware-Schutz – Übersicht

Seit ONTAP 9.10.1 nutzt die Funktion Autonomous Ransomware Protection (ARP) Workload-Analysen in NAS-Umgebungen (NFS und SMB), um ungewöhnliche Aktivitäten, die auf einen Ransomware-Angriff hinweisen, proaktiv zu erkennen und zu warnen.

Wenn ein Angriff vermutet wird, erstellt ARP zusätzlich zu dem bestehenden Schutz vor geplanten Snapshot-Kopien auch neue Snapshot-Kopien.

Lizenzen und Enablement

ARP erfordert eine Lizenz. ARP ist mit dem verfügbar "ONTAP ONE Lizenz". Wenn Sie nicht über die ONTAP One-Lizenz verfügen, stehen andere Lizenzen zur Verfügung, um ARP zu verwenden. Diese unterscheiden sich je nach Ihrer ONTAP-Version.

ONTAP-Versionen	Lizenz
ONTAP 9.11.1 und höher	Anti_Ransomware
ONTAP 9.10.1	MT_EK_MGMT (mandantenfähiger Schlüsselmanagement)

- Wenn Sie ein Upgrade auf ONTAP 9.11.1 oder höher durchführen und ARP bereits auf Ihrem System konfiguriert ist, müssen Sie die neue Anti-Ransomware-Lizenz nicht erwerben. Für neue ARP-Konfigurationen ist die neue Lizenz erforderlich.
- Wenn Sie von ONTAP 9.11.1 oder höher auf ONTAP 9.10.1 zurücksetzen und ARP mit der Anti-Ransomware-Lizenz aktiviert haben, wird eine Warnmeldung angezeigt und muss unter Umständen ARP neu konfigurieren. "Erfahren Sie mehr über das Zurücksetzen von ARP".

Sie können ARP entweder mit System Manager oder mit der ONTAP CLI für einzelne Volumes konfigurieren.

ONTAP Strategie zum Schutz der Ransomware

Eine effektive Strategie zur Erkennung von Ransomware sollte mehr als nur eine einzige Sicherungsebene umfassen.

Eine Analogie wäre die Sicherheit eines Fahrzeugs. Sie verlassen sich nicht auf eine einzelne Funktion, wie einen Sicherheitsgurt, um Sie bei einem Unfall komplett zu schützen. Airbags, Anti-Lock-Bremsen und Vorkollisionswarnung sind weitere Sicherheitsmerkmale, die zu einem viel besseren Ergebnis führen. Ransomware-Schutz sollte in der gleichen Weise betrachtet werden.

Während ONTAP Funktionen wie FPolicy, Snapshot-Kopien, SnapLock und Active IQ Digital Advisor zum Schutz vor Ransomware umfasst, konzentriert sich die folgenden Informationen auf die ARP-integrierte Funktion mit Machine-Learning-Funktionen.

Weitere Informationen zu den weiteren Anti-Ransomware-Funktionen von ONTAP finden Sie unter "TR-4572: NetApp Lösung gegen Ransomware"

Was ARP erkennt

ARP wurde zum Schutz vor Denial-of-Service-Angriffen entwickelt, bei denen der Angreifer Daten zurückhält, bis ein Lösegeld bezahlt wird. ARP bietet die Erkennung von Ransomware auf der Basis von:

- Identifizierung der eingehenden Daten als verschlüsselt oder als Klartext.
- Analytics, die erkennt
  - **Entropie**: Eine Auswertung der Zufälligkeit der Daten in einer Datei
  - **Dateierweiterungstypen**: Eine Erweiterung, die nicht dem normalen Erweiterungstyp entspricht
  - **Datei-IOPS**: Ein Anstieg der anormalen Volume-Aktivität mit Datenverschlüsselung (ab ONTAP 9.11.1)

ARP erkennt die Ausbreitung der meisten Ransomware-Angriffe, nachdem nur wenige Dateien verschlüsselt sind, automatisch Maßnahmen zur Datensicherung ergreifen und Sie darauf aufmerksam machen, dass im Verdacht stehende Angriffe auf einen Angriff stattfindet.

> Kein Ransomware-Erkennungs- oder Präventionssystem kann die Sicherheit bei einem Ransomware-Angriff vollständig gewährleisten. Obwohl es möglich ist, dass ein Angriff unentdeckt bleibt, fungiert ARP als wichtige zusätzliche Verteidigungsschicht, wenn Antivirensoftware einen Angriff nicht erkennt.

Lernen und aktive Modi

ARP verfügt über zwei Modi:

- **Learning** (oder „Dry Run"-Modus)
- **Aktiv** (oder „aktiviert"-Modus)

Wenn Sie ARP aktivieren, wird es im *Learning Mode* ausgeführt. Im Lernmodus entwickelt das ONTAP System ein Warnmeldungsprofil auf der Grundlage der Analysebereiche Entropie, Dateierweiterungstypen und Datei-IOPS. Nachdem Sie ARP im Learning-Modus ausreichend Zeit ausgeführt haben, um Workload-Merkmale zu bewerten, können Sie in den aktiven Modus wechseln und mit dem Schutz Ihrer Daten beginnen. Sobald ARP in den aktiven Modus gewechselt ist, erstellt ONTAP ARP Snapshot Kopien, um die Daten zu schützen, wenn eine Bedrohung erkannt wird.

Es wird empfohlen, ARP 30 Tage lang im Lernmodus zu belassen. Ab ONTAP 9.13.1 bestimmt ARP automatisch das optimale Lernintervall und automatisiert den Switch, der vor 30 Tagen auftreten kann.

Wenn im aktiven Modus eine Dateierweiterung als anormal gekennzeichnet ist, sollten Sie die Warnmeldung auswerten. Sie können auf die Warnung reagieren, um Ihre Daten zu schützen, oder Sie können die Warnung als falsch positiv markieren. Wenn Sie eine Warnung als falsch positiv markieren, wird das Warnungsprofil aktualisiert. Wenn die Warnmeldung beispielsweise durch eine neue Dateierweiterung ausgelöst wird und Sie die Warnmeldung als falsch positiv markieren, erhalten Sie beim nächsten Mal keine Warnmeldung, wenn diese Dateierweiterung beobachtet wird. Der Befehl `security anti-ransomware volume workload-behavior show` Zeigt Dateierweiterungen an, die im Volume erkannt wurden. (Wenn Sie diesen Befehl zu Beginn des Lernmodus ausführen und er eine genaue Darstellung der Dateitypen anzeigt, sollten Sie diese Daten nicht als Grundlage für den Wechsel in den aktiven Modus verwenden, da ONTAP weiterhin andere Metriken sammelt.)

Ab ONTAP 9.11.1 können Sie die Erkennungsparameter für ARP anpassen. Weitere Informationen finden Sie unter Verwalten von ARP-Angriffserkennungsparametern.

Bedrohungsbewertung und ARP Snapshot Kopien

Im aktiven Modus bewertet ARP die Bedrohungswahrscheinlichkeit anhand eingehender Daten, die mit gelernten Analysen gemessen werden. Eine Messung wird zugewiesen, wenn ARP eine Bedrohung erkennt:

- **Low**: Früheste Erkennung einer Anomalie im Volume (z.B. wird eine neue Dateierweiterung im Volume beobachtet).
- **Mittel**: Es werden mehrere Dateien mit derselben nie zuvor gesehenen Dateierweiterung beobachtet.
  - In ONTAP 9.10.1 liegt der Schwellenwert für die Eskalation auf moderat bei 100 oder mehr Dateien. Ab ONTAP 9.11.1 kann die Dateimenge geändert werden; der Standardwert ist 20.

In einer Situation mit geringen Bedrohungen erkennt ONTAP eine Auffälligkeit und erstellt eine Snapshot Kopie des Volumes, um den bestmöglichen Recovery-Punkt zu erreichen. ONTAP übergibt den Namen der ARP Snapshot Kopie mit `Anti-ransomware-backup` Um es leicht zu identifizieren, zum Beispiel `Anti_ransomware_backup.2022-12-20_1248`.

Die Bedrohung wird eskaliert und mäßig, nachdem ONTAP einen Analysebericht ausgeführt hat und

festgestellt hat, ob die Anomalie mit einem Ransomware-Profil übereinstimmt. Bedrohungen, die auf der niedrigen Ebene bleiben, werden protokolliert und im Abschnitt **Ereignisse** von System Manager sichtbar. Wenn die Angriffswahrscheinlichkeit mäßig ist, generiert ONTAP eine EMS-Benachrichtigung, in der Sie aufgefordert werden, die Bedrohung zu bewerten. ONTAP sendet keine Warnungen über geringe Bedrohungen, aber ab ONTAP 9.14.1 können Sie Ändern Sie die Einstellungen für Warnmeldungen. Weitere Informationen finden Sie unter Reagieren Sie auf ungewöhnliche Aktivitäten.

Sie können Informationen zu einer Bedrohung, unabhängig von der Ebene, im System Manager **Ereignisse** Abschnitt oder mit dem anzeigen `security anti-ransomware volume show` Befehl.

ARP Snapshot Kopien werden mindestens zwei Tage aufbewahrt. Ab ONTAP 9.11.1 können Sie die Aufbewahrungseinstellungen ändern. Weitere Informationen finden Sie unter Ändern Sie Optionen für Snapshot Kopien.

Wiederherstellung von Daten im ONTAP nach einem Ransomware-Angriff

Wenn ein Angriff vermutet wird, erstellt das System zu diesem Zeitpunkt eine Volume Snapshot Kopie und sperrt die Kopie. Wenn der Angriff später bestätigt wird, kann das Volume mithilfe der ARP Snapshot Kopie wiederhergestellt werden.

Gesperrte Snapshot Kopien können nicht auf normale Weise gelöscht werden. Wenn Sie sich jedoch später entscheiden, den Angriff als falsch positiv zu markieren, wird die gesperrte Kopie gelöscht.

Durch das Wissen über die betroffenen Dateien und den Zeitpunkt eines Angriffs können betroffene Dateien selektiv von verschiedenen Snapshot Kopien wiederhergestellt werden, anstatt das gesamte Volume einfach auf eine der Snapshot Kopien zurückzugreifen.

ARP baut auf bewährte ONTAP-Technologie zur Datensicherung und Disaster Recovery auf, um auf Ransomware-Angriffe zu reagieren. Weitere Informationen zur Wiederherstellung von Daten finden Sie in den folgenden Themen.

- "Wiederherstellen von Snapshot-Kopien (System Manager)"
- "Wiederherstellen von Dateien aus Snapshot-Kopien (CLI)"
- "Intelligente Ransomware-Recovery"

Anwendungsfälle und Überlegungen zum autonomen Ransomware-Schutz

Autonomous Ransomware Protection (ARP) ist ab ONTAP 9.10.1 für NAS-Workloads verfügbar. Vor der Bereitstellung von ARP sollten Sie die empfohlenen Verwendungszwecke und unterstützten Konfigurationen sowie die Auswirkungen auf die Performance kennen.

Unterstützte und nicht unterstützte Konfigurationen

Bei der Entscheidung, ARP zu verwenden, ist es wichtig sicherzustellen, dass die Arbeitslast Ihres Volumes für ARP geeignet ist und dass sie die erforderlichen Systemkonfigurationen erfüllt.

Geeignete Workloads

ARP eignet sich für:

- Datenbanken auf NFS-Storage

- Home Directorys für Windows oder Linux

  Da Benutzer Dateien mit Erweiterungen erstellen können, die während des Lernzeitraums nicht erkannt wurden, besteht eine größere Möglichkeit von False-positive-Meldungen in diesem Workload.

- Bilder und Video

  Beispielsweise Gesundheitsdaten und EDA-Daten (Electronic Design Automation)

Ungeeignete Workloads

ARP ist nicht geeignet für:

- Workloads mit hoher Frequenz, die Dateien erstellen oder löschen (Hunderttausende Dateien in wenigen Sekunden, z. B. Test-/Entwicklungs-Workloads).
- Die Erkennung von ARP-Bedrohungen hängt von der Fähigkeit ab, einen ungewöhnlichen Anstieg bei der Erstellung, Umbenennung oder Löschung von Dateien zu erkennen. Wenn die Anwendung selbst die Quelle der Dateiaktivität ist, kann sie nicht effektiv von Ransomware-Aktivitäten unterschieden werden.
- Workloads, bei denen die Anwendung oder der Host Daten verschlüsselt.
  ARP hängt davon ab, dass eingehende Daten als verschlüsselt oder unverschlüsselt unterschieden werden. Wenn die Applikation selbst die Daten verschlüsselt, wird die Effektivität der Funktion verringert. Die Funktion kann jedoch immer noch basierend auf den Dateiaktivitäten (Löschen, Überschreiben, Erstellen, Erstellen oder Erstellen von Dateien oder Erstellen oder Umbenennen mit einer neuen Dateierweiterung) und dem Dateityp funktionieren.

Unterstützte Konfigurationen

ARP ist ab ONTAP 9.10.1 für NFS und SMB Volumes in lokalen ONTAP Systemen verfügbar.

Andere Konfigurationen und Volume-Typen werden in den folgenden ONTAP-Versionen unterstützt:

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumes sind mit asynchronem SnapMirror geschützt	✓	✓	✓		
SVMs gesichert mit asynchronem SnapMirror (SVM Disaster Recovery)	✓	✓	✓		
SVM-Datenmobilität (`vserver migrate`)	✓	✓	✓		
FlexGroup Volumes	✓	✓			
Überprüfung durch mehrere Administratoren	✓	✓			

SnapMirror und ARP-Interoperabilität

Ab ONTAP 9.12.1 wird ARP auf asynchronen SnapMirror Ziel-Volumes unterstützt. ARP ist **nicht** mit SnapMirror Synchronous unterstützt.

Wenn ein SnapMirror Quell-Volume ARP-aktiviert ist, übernimmt das SnapMirror Ziel-Volume automatisch den ARP-Konfigurationsstatus (Learning, Enabled usw.), ARP-Trainingsdaten und ARP-erstellte Snapshots des Quell-Volume. Es ist keine explizite Aktivierung erforderlich.

Während das Zielvolume aus schreibgeschützten (RO) Snapshot Kopien besteht, wird auf seinen Daten keine ARP Verarbeitung durchgeführt. Wenn das SnapMirror Ziel-Volume jedoch in Read-Write (RW) konvertiert wird, wird ARP automatisch auf dem RW-konvertierten Zielvolume aktiviert. Das Zielvolumen erfordert neben dem, was bereits auf dem Quellvolumen aufgezeichnet wurde, keine zusätzlichen Lernverfahren.

In ONTAP 9.10.1 und 9.11.1 überträgt SnapMirror nicht den ARP-Konfigurationsstatus, die Trainingsdaten und Snapshot-Kopien von den Quell- auf Ziel-Volumes. Wenn also das SnapMirror Ziel-Volume in RW konvertiert wird, muss ARP auf dem Ziel-Volume nach der Konvertierung explizit in den Learning Mode aktiviert werden.

ARP und Virtual Machines

ARP wird mit Virtual Machines (VMs) unterstützt. Die ARP-Erkennung verhält sich bei Änderungen innerhalb und außerhalb der VM unterschiedlich. ARP wird nicht für Workloads mit entropischen Dateien innerhalb der VM empfohlen.

Änderungen außerhalb der VM

ARP kann Änderungen an Dateierweiterungen auf einem NFS-Volume außerhalb der VM erkennen, wenn eine neue Erweiterung verschlüsselt in das Volume eintritt oder sich eine Dateierweiterung ändert. Nachweisbare Änderungen an Dateierweiterungen:

- .Vmx
- .vmxf
- .Vmdk
- -Flat.vmdk
- .nvram
- .Vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .Log
- -\#.log

Änderungen innerhalb der VM

Wenn der Ransomware-Angriff auf die VM zielt und Dateien innerhalb der VM geändert werden, ohne Änderungen außerhalb der VM vorzunehmen, erkennt ARP die Bedrohung, wenn die Standard-Entropie der VM gering ist (z. B. .txt-, .docx- oder .mp4-Dateien). Obwohl ARP in diesem Szenario einen Schutz-Snapshot erstellt, generiert es keine Bedrohungswarnung, da die Dateierweiterungen außerhalb der VM nicht manipuliert wurden.

Wenn es sich bei den Dateien standardmäßig um Dateien mit hoher Entropie handelt (z. B. .gzip- oder passwortgeschützte Dateien), sind die Erkennungsfunktionen von ARP begrenzt. ARP kann in dieser Instanz immer noch proaktive Snapshots machen, es werden jedoch keine Warnmeldungen ausgelöst, wenn die Dateierweiterungen nicht extern manipuliert wurden.

Nicht unterstützte Konfigurationen

ARP wird in den folgenden Systemkonfigurationen nicht unterstützt:

- ONTAP S3-Umgebungen
- SAN-Umgebungen

ARP unterstützt die folgenden Volume-Konfigurationen nicht:

- FlexGroup Volumes (in ONTAP 9.10.1 bis 9.12.1) Ab ONTAP 9.13.1 werden FlexGroup Volumes unterstützt)
- FlexCache Volumes (ARP wird auf Ursprungs-FlexVol Volumes unterstützt, jedoch nicht auf Cache Volumes)
- Offline-Volumes
- REINE SAN-Volumes
- SnapLock Volumes
- SnapMirror Synchronous
- Asynchronous SnapMirror (nur in ONTAP 9.10.1 und 9.11.1 unterstützt Asynchrones SnapMirror wird ab ONTAP 9.12.1 unterstützt. Weitere Informationen finden Sie unter [snapmirror].)
- Eingeschränkte Volumes
- Root-Volumes von Storage-VMs
- Volumes von angestoppten Storage VMs

ARP-Performance- und Frequenzüberlegungen

ARP kann die System-Performance im Hinblick auf den Durchsatz und die IOPS-Spitzenwerte minimal beeinträchtigen. Die Auswirkungen der ARP-Funktion hängen von den spezifischen Volume Workloads ab. Für gängige Workloads werden die folgenden Konfigurationsgrenzwerte empfohlen:

Workload-Merkmale	Empfohlene Volume-Beschränkung pro Node	Performance-Verschlechterung bei Überschreitung der Grenze des Volume pro Node:[*]
Leseintensiv oder die Daten komprimiert werden können.	150	4 % der maximalen IOPS
Schreibintensiv und die Daten können nicht komprimiert werden.	60	10 % der maximalen IOPS

Pass:[*] die Systemleistung wird unabhängig von der Anzahl der hinzugefügten Volumes, die über den empfohlenen Grenzwerten liegen, nicht über diesen Prozentwerten hinaus beeinträchtigt.

Da ARP-Analysen in einer priorisierten Reihenfolge ausgeführt werden und die Anzahl der geschützten Volumes zunimmt, werden die Analysen auf jedem Volume weniger häufig ausgeführt.

Verifizierung mehrerer Administratoren mit Volumes, die mit ARP gesichert sind

Ab ONTAP 9.13.1 können Sie die Multi-Admin-Verifizierung (MAV) aktivieren, um zusätzliche Sicherheit mit ARP zu gewährleisten. MAV stellt sicher, dass mindestens zwei oder mehr authentifizierte Administratoren erforderlich sind, um ARP zu deaktivieren, ARP zu unterbrechen oder einen vermuteten Angriff als falsch positiv auf einem geschützten Volume zu markieren. Erfahren Sie, wie Sie "Aktivieren Sie MAV für ARP-geschützte Volumes".

Sie müssen Administratoren für eine MAV-Gruppe definieren und MAV-Regeln für das erstellen `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, und `security anti-ransomware volume attack clear-suspect` ARP-Befehle, die Sie schützen möchten. Jeder Administrator in der MAV-Gruppe muss jede neue Regelanforderung und genehmigen "Fügen Sie die MAV-Regel erneut hinzu" Innerhalb der MAV-Einstellungen.

Ab ONTAP 9.14.1 bietet ARP Warnungen für die Erstellung eines ARP-Snapshot und für die Beobachtung einer neuen Dateierweiterung an. Warnmeldungen für diese Ereignisse sind standardmäßig deaktiviert. Alarme können auf Volume- oder SVM-Ebene festgelegt werden. Mit können Sie MAV-Regeln auf SVM-Ebene erstellen `security anti-ransomware vserver event-log modify` Oder auf Lautstärkeregelung mit `security anti-ransomware volume event-log modify`.

Nächste Schritte

- "Autonomer Schutz Vor Ransomware"
- "Aktivieren Sie MAV für ARP-geschützte Volumes"

Autonomer Schutz Vor Ransomware

Ab ONTAP 9.10.1 kann der autonome Ransomware-Schutz (ARP) auf neuen oder bestehenden Volumes aktiviert werden. Sie aktivieren ARP zunächst im Lernmodus, in dem das System die Arbeitslast analysiert, um das normale Verhalten zu charakterisieren. Sie können ARP auf einem vorhandenen Volume aktivieren, oder Sie können ein neues Volume erstellen und ARP von Anfang an aktivieren.

Über diese Aufgabe

Sie sollten ARP zunächst immer im Lern- (oder Dry-Run-) Modus aktivieren. Wenn Sie im aktiven Modus beginnen, kann dies zu überhöhten falsch-positiven Berichten führen.

Es wird empfohlen, ARP mindestens 30 Tage im Lernmodus laufen zu lassen. Ab ONTAP 9.13.1 bestimmt ARP automatisch das optimale Lernintervall und automatisiert den Switch, der vor 30 Tagen auftreten kann. Weitere Informationen finden Sie unter "Lernen und aktive Modi".

> In bestehenden Volumes gelten der Lern- und der aktiv-Modus nur für neu geschriebene Daten, nicht für bereits vorhandene Daten im Volume. Die vorhandenen Daten werden nicht gescannt und analysiert, da die Merkmale eines früheren normalen Datenverkehrs auf der Grundlage der neuen Daten angenommen werden, nachdem das Volume für ARP aktiviert wurde.

Bevor Sie beginnen

- Sie müssen eine Storage-VM (SVM) für NFS oder SMB (oder beides) aktivieren.
- Der Korrekte Lizenz Muss für Ihre ONTAP-Version installiert sein.
- Sie müssen NAS-Workloads und Clients konfiguriert haben.
- Das Volumen, auf dem Sie ARP setzen möchten, muss geschützt sein und über einen aktiven verfügen

"Verbindungspfad".

- Das Volumen muss zu weniger als 100 % voll sein.
- Es wird empfohlen, das EMS-System so zu konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden, die Hinweise auf ARP-Aktivitäten enthalten. Weitere Informationen finden Sie unter "Konfigurieren Sie EMS-Ereignisse zum Senden von E-Mail-Benachrichtigungen".
- Ab ONTAP 9.13.1 wird empfohlen, die Multi-Admin-Verifizierung (MAV) zu aktivieren, sodass für die ARP-Konfiguration (Autonomous Ransomware Protection) mindestens zwei authentifizierte Benutzeradministratoren erforderlich sind. Weitere Informationen finden Sie unter "Aktivieren Sie die Verifizierung durch mehrere Administratoren".

Aktivieren Sie ARP

Sie können ARP mit System Manager oder der ONTAP CLI aktivieren.

System Manager

Schritte

1. Wählen Sie **Storage > Volumes** und dann das zu schützende Volume aus.
2. Wählen Sie im Register **Sicherheit** der **Volumes**-Übersicht **Status** aus, um im Lernmodus im Feld **Anti-Ransomware** von deaktiviert zu aktiviert zu wechseln.
3. Wenn der Lernzeitraum vorbei ist, schalten Sie ARP in den aktiven Modus um.

   > Ab ONTAP 9.13.1 bestimmt ARP automatisch das optimale Lernintervall und automatisiert den Switch. Das können Sie "Deaktivieren Sie diese Einstellung auf der zugehörigen Speicher-VM" Wenn Sie den Lernmodus manuell auf den aktiven Modus umschalten möchten.

   a. Wählen Sie **Storage > Volumes** und dann das Volume aus, das für den aktiven Modus bereit ist.
   b. Wählen Sie im Register **Sicherheit** der Übersicht **Volumes** im Feld Anti-Ransomware **Switch** in den aktiven Modus.
4. Sie können den ARP-Status des Volumes im Feld **Anti-Ransomware** überprüfen.

   Um den ARP-Status für alle Volumes anzuzeigen, wählen Sie im Bereich **Volumes ein/Ausblenden** aus, und stellen Sie dann sicher, dass der Status **Anti-Ransomware** aktiviert ist.

CLI

Der Prozess der Aktivierung von ARP mit der CLI unterscheidet sich, wenn sie es auf einem vorhandenen Volume und nicht auf einem neuen Volume aktivieren.

Aktivieren Sie ARP auf einem vorhandenen Volume

1. Ändern Sie ein vorhandenes Volume, um Ransomware-Schutz im Learning-Modus zu ermöglichen:

   ```
   security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
   ```

   Wenn Sie ONTAP 9.13.1 oder höher ausführen, ist das adaptive Lernen aktiviert, sodass die Änderung des aktiven Status automatisch erfolgt. Wenn Sie nicht möchten, dass dieses Verhalten automatisch aktiviert wird, ändern Sie die Einstellung auf SVM-Ebene für alle zugehörigen Volumes:

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

2. Wenn der Lernzeitraum vorbei ist, ändern Sie das geschützte Volume, um in den aktiven Modus zu wechseln, falls nicht bereits automatisch ausgeführt:

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   Sie können auch mit dem Befehl „Volume ändern“ in den aktiven Modus wechseln:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Überprüfen Sie den ARP-Status des Volumes.

   ```
   security anti-ransomware volume show
   ```

Aktivieren Sie ARP auf einem neuen Volume

1. Erstellen Sie ein neues Volume mit aktiviertem Ransomware-Schutz, bevor Sie Daten bereitstellen.

   ```
   volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size
   nn -anti-ransomware-state dry-run -junction-path /path_name
   ```

   Wenn Sie ONTAP 9.13.1 oder höher ausführen, ist das adaptive Lernen aktiviert, sodass die Änderung des aktiven Status automatisch erfolgt. Wenn Sie nicht möchten, dass dieses Verhalten automatisch aktiviert wird, ändern Sie die Einstellung auf SVM-Ebene für alle zugehörigen Volumes:

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

2. Wenn der Lernzeitraum vorbei ist, ändern Sie das geschützte Volume, um in den aktiven Modus zu wechseln, falls nicht bereits automatisch ausgeführt:

   ```
   security anti-ransomware volume enable -volume vol_name -vserver svm_name
   ```

   Sie können auch mit dem Befehl „Volume ändern“ in den aktiven Modus wechseln:

   ```
   volume modify -volume vol_name -vserver svm_name -anti-ransomware-state
   active
   ```

3. Überprüfen Sie den ARP-Status des Volumes.

   ```
   security anti-ransomware volume show
   ```

Autonome Ransomware-Sicherung in neuen Volumes standardmäßig aktiviert

Ab ONTAP 9.10.1 können Sie Storage-VMs (SVMs) so konfigurieren, dass neue Volumes im Learning-Modus standardmäßig für Autonomous Ransomware Protection (ARP) aktiviert sind.

Über diese Aufgabe

Standardmäßig werden neue Volumes mit ARP im deaktivierten Modus erstellt. Sie können diese Einstellung in System Manager und mit der CLI ändern. Standardmäßig aktivierte Volumes sind im Lern- (oder Dry-Run-) Modus auf ARP eingestellt.

ARP wird nur auf Volumes aktiviert, die in der SVM erstellt wurden, nachdem Sie die Einstellung geändert haben. ARP wird auf vorhandenen Volumes nicht aktiviert. Erfahren Sie, wie Sie "Aktivieren Sie ARP in einem vorhandenen Volume".

Ab ONTAP 9.13.1 wurde das adaptive Lernen zu ARP-Analysen hinzugefügt und der Wechsel vom Lernmodus zum aktiven Modus erfolgt automatisch. Weitere Informationen finden Sie unter "Lernen und aktive Modi".

Bevor Sie beginnen

- Der Korrekte Lizenz Muss für Ihre ONTAP-Version installiert sein.
- Das Volumen muss zu weniger als 100 % voll sein.
- Verbindungspfade müssen aktiv sein.
- Ab ONTAP 9.13.1 wird empfohlen, die Multi-Admin-Verifizierung (MAV) zu aktivieren, sodass für

Ransomware-Vorgänge mindestens zwei authentifizierte Benutzeradministratoren erforderlich sind. "Weitere Informationen .".

Schalten Sie ARP vom Lernen in den aktiven Modus

Ab ONTAP 9.13.1 wurde das adaptive Lernen zu ARP-Analysen hinzugefügt. Der Wechsel vom Lernmodus in den aktiven Modus erfolgt automatisch. Die autonome Entscheidung von ARP, automatisch vom Lernmodus in den aktiven Modus zu wechseln, basiert auf den Konfigurationseinstellungen der folgenden Optionen:

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

Nach 30 Lerntagen wird ein Volumen automatisch in den aktiven Modus geschaltet, auch wenn eine oder mehrere dieser Bedingungen nicht erfüllt sind. Das heißt, wenn die automatische Umschaltung aktiviert ist, wechselt die Lautstärke nach maximal 30 Tagen in den aktiven Modus. Der Maximalwert von 30 Tagen ist festgelegt und kann nicht geändert werden.

Weitere Informationen zu ARP-Konfigurationsoptionen, einschließlich Standardwerten, finden Sie im "Befehlsreferenz für ONTAP".

Schritte

Sie können System Manager oder die ONTAP-CLI verwenden, um ARP standardmäßig zu aktivieren.

System Manager

1. Wählen Sie **Speicher > Speicher-VMs** und wählen Sie dann die Speicher-VM aus, die Volumes enthält, die Sie mit ARP schützen möchten.
2. Navigieren Sie zur Registerkarte **Einstellungen**. Suchen Sie unter **Sicherheit** die **Anti-Ransomware** -Kachel und wählen Sie aus
3. Aktivieren Sie das Kontrollkästchen, um ARP für NAS-Volumes zu aktivieren. Aktivieren Sie das Zusatzfeld, um ARP auf allen in Frage kommenden NAS-Volumes in der Speicher-VM zu aktivieren.

> Wenn Sie ein Upgrade auf ONTAP 9.13.1 durchgeführt haben, wird die Einstellung **nach ausreichend Lernen automatisch vom Lernmodus zum aktiven Modus wechseln** automatisch aktiviert. Auf diese Weise kann ARP das optimale Lernintervall bestimmen und den Wechsel zum aktiven Modus automatisieren. Deaktivieren Sie die Einstellung, wenn Sie manuell in den aktiven Modus wechseln möchten.

CLI

1. Ändern Sie eine vorhandene SVM, um ARP standardmäßig in neuen Volumes zu aktivieren:
   `vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

   Über die CLI können Sie auch eine neue SVM erstellen, wobei ARP standardmäßig für neue Volumes aktiviert ist.
   `vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]`

   Wenn Sie ein Upgrade auf ONTAP 9.13.1 oder höher durchgeführt haben, ist das adaptive Lernen aktiviert, sodass die Änderung des aktiven Status automatisch erfolgt. Wenn dieses Verhalten nicht automatisch aktiviert werden soll, verwenden Sie den folgenden Befehl:

   ```
   vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to
   -enabled false
   ```

Unterbrechen Sie den autonomen Ransomware-Schutz, um Workload-Ereignisse aus der Analyse auszuschließen

Wenn Sie ungewöhnliche Workload-Ereignisse erwarten, können Sie die ARP-Analyse (Autonomous Ransomware Protection, Autonomous Ransomware Protection) jederzeit unterbrechen und wieder aufnehmen.

Ab ONTAP 9.13.1 können Sie die Multi-Admin-Verifizierung (MAV) aktivieren, sodass mindestens zwei authentifizierte Benutzeradministratoren zum Anhalten des ARP erforderlich sind. "Weitere Informationen .".

Über diese Aufgabe

Während einer ARP-Pause werden keine Ereignisse protokolliert oder sind Maßnahmen bei neuen Schreibvorgängen. Die Analyse wird jedoch für frühere Protokolle im Hintergrund fortgesetzt.

> Verwenden Sie die ARP-Deaktivierungsfunktion nicht, um die Analyse anzuhalten. Dadurch wird ARP auf dem Volume deaktiviert, und alle vorhandenen Informationen rund um das gelernte Workload-Verhalten sind verloren. Dies würde einen Neustart des Lernzeitraums erfordern.

Schritte

Sie können System Manager oder die ONTAP-CLI verwenden, um ARP anzuhalten.

System Manager

1. Wählen Sie **Speicher > Volumes** und wählen Sie dann das Volume aus, auf dem Sie ARP anhalten möchten.
2. Wählen Sie auf der Registerkarte **Sicherheit** der Volumes-Übersicht **Anti-Ransomware anhalten** im Feld **Anti-Ransomware** aus.

> Wenn Sie ab ONTAP 9.13.1 MAV zum Schutz Ihrer ARP-Einstellungen verwenden, werden Sie durch den Pause-Vorgang aufgefordert, die Genehmigung eines oder mehrerer zusätzlicher Administratoren einzuholen. "Die Genehmigung muss von allen Administratoren eingeholt werden" Der MAV-Genehmigungsgruppe zugeordnet oder der Vorgang schlägt fehl.

CLI

1. ARP auf einem Volume anhalten:

   ```
   security anti-ransomware volume pause -vserver svm_name -volume vol_name
   ```

2. Um die Verarbeitung fortzusetzen, verwenden Sie den `resume` Parameter.

   ```
   security anti-ransomware volume resume -vserver svm_name -volume vol_name
   ```

3. **Wenn Sie MAV (verfügbar mit ARP ab ONTAP 9.13.1) zum Schutz Ihrer ARP-Einstellungen verwenden,** fordert Sie der Pausenvorgang auf, die Genehmigung eines oder mehrerer zusätzlicher Administratoren einzuholen. Die Genehmigung muss von allen Administratoren, die mit der MAV-Genehmigungsgruppe verknüpft sind, eingeholt werden. Andernfalls schlägt der Vorgang fehl.

   Wenn Sie MAV verwenden und für einen erwarteten Pausenbetrieb zusätzliche Genehmigungen erforderlich sind, führt jeder Genehmiger der MAV-Gruppe Folgendes durch:

   a. Anfrage anzeigen:

      ```
      security multi-admin-verify request show
      ```

   b. Genehmigen Sie die Anforderung:

      ```
      security multi-admin-verify request approve -index[number returned from show request]
      ```

      Die Antwort für den letzten Gruppengenehmiger zeigt an, dass das Volume geändert wurde und der Status von ARP angehalten wurde.

      Wenn Sie MAV verwenden und ein Genehmiger der MAV-Gruppe sind, können Sie eine Anforderung für einen Pause-Vorgang ablehnen:

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

Managen Sie die Parameter für die Erkennung von Angriffen gegen autonomen Ransomware-Schutz

Ab ONTAP 9.11.1 können Sie die Parameter für die Ransomware-Erkennung auf einem bestimmten Volume mit aktiviertem Autonomem Ransomware-Schutz ändern und einen bekannten Anstieg als normale Dateiaktivität melden. Durch die Anpassung der Erkennungsparameter wird die Genauigkeit der Berichterstellung auf der Grundlage Ihrer spezifischen Volumenbelastung verbessert.

Wie die Angriffserkennung funktioniert

Wenn sich der Autonomous Ransomware Protection (ARP) im Lernmodus befindet, werden Grundwerte für das Volume-Verhalten entwickelt. Es handelt sich um Entropie, Dateiendungen und – seit ONTAP 9.11.1 – IOPS. Diese Baselines dienen zur Bewertung von Ransomware-Bedrohungen. Weitere Informationen zu diesen Kriterien finden Sie unter Was ARP erkennt.

In ONTAP 9.10.1 gibt ARP eine Warnung aus, wenn beide der folgenden Bedingungen erkannt werden:

- Mehr als 20 Dateien mit Dateierweiterungen, die bisher nicht im Volume beobachtet wurden
- Hohe Entropie-Daten

Ab ONTAP 9.11.1 gibt ARP eine Bedrohungswarnung aus, wenn *only* eine Bedingung erfüllt ist. Wenn beispielsweise mehr als 20 Dateien mit Dateierweiterungen, die zuvor nicht im Volume beobachtet wurden, innerhalb eines Zeitraums von 24 Stunden beobachtet werden, kategorisiert ARP diese Datei als Bedrohung *unabhängig* der beobachteten Entropie. (Die Dateiwerte 24 Stunden und 20 Stunden sind Standardwerte, die geändert werden können.)

Ab ONTAP 9.14.1 können Sie Alarme konfigurieren, wenn ARP eine neue Dateierweiterung beobachtet, und wenn ARP einen Snapshot erstellt. Weitere Informationen finden Sie unter [modify-alerts]

Bestimmte Volumes und Workloads erfordern unterschiedliche Erkennungsparameter. Zum Beispiel kann Ihr ARP-fähiges Volume zahlreiche Arten von Dateierweiterungen hosten. In diesem Fall möchten Sie die Schwellenwertanzahl für nie zuvor gesehene Dateierweiterungen auf eine Zahl ändern, die größer ist als die Standardeinstellung von 20 oder Warnungen deaktivieren, die auf nie zuvor gesehenen Dateierweiterungen basieren. Ab ONTAP 9.11.1 können Sie die Parameter zur Angriffserkennung anpassen, um sie besser auf Ihre spezifischen Workloads anzupassen.

Parameter für die Angriffserkennung ändern

Je nach erwartetem Verhalten des ARP-aktivierten Volumens können Sie die Angriffserkennungsparameter ändern.

Schritte

1. Anzeigen der vorhandenen Angriffserkennungsparameter:

   ```
   security anti-ransomware volume attack-detection-parameters show -vserver
   svm_name -volume volume_name
   ```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                                Vserver Name : vs1
                                                 Volume Name : vol1
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                  Is Detection Based on File Create Rate? : true
                  Is Detection Based on File Rename Rate? : true
                  Is Detection Based on File Delete Rate? : true
           Is Detection Relaxing Popular File Extensions? : true
                High Entropy Data Surge Notify Percentage : 100
                 File Create Rate Surge Notify Percentage : 100
                 File Rename Rate Surge Notify Percentage : 100
                 File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 20
       Never Seen before File Extensions Duration in Hour : 24
```

2. Alle angezeigten Felder können mit booleschen oder ganzzahligen Werten geändert werden. Um ein Feld zu ändern, verwenden Sie die `security anti-ransomware volume attack-detection-parameters modify` Befehl.

   Eine vollständige Liste der Parameter finden Sie unter "Befehlsreferenz für ONTAP".

Bekannte Überspannungen melden

ARP ändert auch im aktiven Modus weiterhin Basiswerte für Erkennungsparameter. Wenn Sie von Überspannungen in Ihrer Volumenaktivität wissen - entweder einmal Überspannungen oder eine Überspannung, die für eine neue Normalität charakteristisch ist - sollten Sie sie als sicher melden. Die manuelle Meldung dieser Überspannungen als sicher hilft, die Genauigkeit der ARP-Bedrohungsbewertungen zu verbessern.

Melden Sie eine einmalige Überspannung

1. Wenn ein einmaliger Anstieg unter bekannten Umständen auftritt und Sie möchten, dass ARP in Zukunft einen ähnlichen Anstieg meldet, beheben Sie den Anstieg des Workload-Verhaltens:

   ```
   security anti-ransomware volume workload-behavior clear-surge -vserver
   svm_name -volume volume_name
   ```

Änderung des Basisliniensprunges

1. Wenn eine gemeldete Überspannung als normales Anwendungsverhalten betrachtet werden sollte, melden Sie den Überspannungswert als solche, um den Überspannungswert der Basislinie zu ändern.

   ```
   security anti-ransomware volume workload-behavior update-baseline-from-surge
   -vserver svm_name -volume volume_name
   ```

Konfigurieren von ARP-Warnungen

Ab ONTAP 9.14.1 ermöglicht ARP die Angabe von Warnungen für zwei ARP-Ereignisse:

- Beobachtung der neuen Dateierweiterung auf einem Volume
- Erstellung eines ARP-Snapshots

Warnmeldungen für diese beiden Ereignisse können für einzelne Volumes oder für die gesamte SVM festgelegt werden. Wenn Sie Alarme für die SVM aktivieren, werden die Meldungseinstellungen nur von Volumes übernommen, die nach dem Aktivieren der Warnmeldung erstellt wurden. Standardmäßig sind Warnmeldungen auf keinem Volume aktiviert.

Ereigniswarnungen können durch Verifizierung durch mehrere Administratoren gesteuert werden. Weitere Informationen finden Sie unter Verifizierung mehrerer Administratoren mit Volumes, die mit ARP gesichert sind.

System Manager

Festlegen von Warnmeldungen für ein Volume

1. Navigieren Sie zu **Volumen**. Wählen Sie das einzelne Volume aus, für das Sie die Einstellungen ändern möchten.
2. Wählen Sie die Registerkarte **Sicherheit** und dann **Ereignissicherheitseinstellungen**.
3. Um Warnungen für **Neue Dateierweiterung entdeckt** und **Ransomware Snapshot erstellt** zu erhalten, wählen Sie das Dropdown-Menü unter der Überschrift **Schweregrad**. Ändern Sie die Einstellung von **Ereignis nicht generieren** in **Hinweis**.
4. Wählen Sie **Speichern**.

Festlegen von Warnmeldungen für eine SVM

1. Navigieren Sie zu **Storage VM**, und wählen Sie dann die SVM aus, für die Sie Einstellungen aktivieren möchten.
2. Suchen Sie unter der Überschrift **Sicherheit** die **Anti-Ransomware**-Karte. Wählen Sie ⋮ Dann **Ransomware-Ereignis-Schweregrad bearbeiten**.
3. Um Warnungen für **Neue Dateierweiterung entdeckt** und **Ransomware Snapshot erstellt** zu erhalten, wählen Sie das Dropdown-Menü unter der Überschrift **Schweregrad**. Ändern Sie die Einstellung von **Ereignis nicht generieren** in **Hinweis**.
4. Wählen Sie **Speichern**.

CLI

Festlegen von Warnmeldungen für ein Volume

- So legen Sie Warnungen für eine neue Dateierweiterung fest:

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- So legen Sie Warnungen für die Erstellung eines ARP-Snapshots fest:

  ```
  security anti-ransomware volume event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- Bestätigen Sie Ihre Einstellungen mit dem `anti-ransomware volume event-log show` Befehl.

Festlegen von Warnmeldungen für eine SVM

- So legen Sie Warnungen für eine neue Dateierweiterung fest:

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-new-file-extension-seen true
  ```

- So legen Sie Warnungen für die Erstellung eines ARP-Snapshots fest:

  ```
  security anti-ransomware vserver event-log modify -vserver svm_name -is
  -enabled-on-snapshot-copy-creation true
  ```

- Bestätigen Sie Ihre Einstellungen mit dem `security anti-ransomware vserver event-log show` Befehl.

Weitere Informationen

- "Autonome Ransomware-Schutzangriffe und den Überblick über den autonomen Ransomware-Schutz"

Reagieren Sie auf ungewöhnliche Aktivitäten

Wenn Autonomous Ransomware Protection (ARP) abnormale Aktivitäten in einem geschützten Volume erkennt, wird eine Warnung ausgegeben. Sie sollten die Benachrichtigung bewerten, um festzustellen, ob die Aktivität akzeptabel ist (falsch positiv) oder ob ein Angriff schädlich erscheint.

Über diese Aufgabe

ARP zeigt eine Liste der verdächtigen Dateien an, wenn sie eine beliebige Kombination von hoher Datenentropie, abnormaler Volume-Aktivität mit Datenverschlüsselung und ungewöhnlichen Dateierweiterungen erkennt.

Wenn die Warnung ausgegeben wird, können Sie darauf reagieren, indem Sie die Dateiaktivität auf zwei Arten markieren:

- **Falsch positiv**

  Der identifizierte Dateityp wird für Ihren Workload erwartet und kann ignoriert werden.

- **Potenzieller Ransomware-Angriff**

  Der identifizierte Dateityp ist bei Ihrer Workload unerwartet und sollte als potenzieller Angriff behandelt werden.

In beiden Fällen wird die normale Überwachung nach der Aktualisierung und dem Löschen der Benachrichtigungen fortgesetzt. ARP zeichnet Ihre Bewertung im Bedrohungsprofil auf und verwendet Ihre Wahl zur Überwachung der nachfolgenden Dateiaktivitäten.

Im Falle eines vermuteten Angriffs müssen Sie feststellen, ob es sich um einen Angriff handelt, darauf reagieren, wenn er der Fall ist, und geschützte Daten wiederherstellen, bevor Sie die Benachrichtigungen löschen. "Erfahren Sie mehr darüber, wie Sie nach einem Ransomware-Angriff wiederherstellen können".

> Wenn Sie ein gesamtes Volume wiederherstellen, müssen keine Hinweise gelöscht werden.

Bevor Sie beginnen

ARP muss im aktiven Modus ausgeführt werden.

Schritte

Sie können System Manager oder die ONTAP CLI verwenden, um auf eine anormale Aufgabe zu reagieren.

System Manager

1. Wenn Sie eine Benachrichtigung über „anormale Aktivität“ erhalten, folgen Sie dem Link oder navigieren Sie zur Registerkarte **Sicherheit** in der Übersicht **Volumes**.

   Warnungen werden im Fenster **Übersicht** des Menüs **Ereignisse** angezeigt.

2. Wenn eine Meldung „erkannte anormale Volumenaktivität“ angezeigt wird, zeigen Sie die verdächtigen Dateien an.

   Wählen Sie auf der Registerkarte **Sicherheit** die Option **vermutete Dateitypen anzeigen** aus.

3. Prüfen Sie im Dialogfeld * Verdachtsed File Types* jeden Dateityp und markieren Sie ihn entweder als „False positive“ oder „Potential Ransomware Attack“.

Wenn Sie diesen Wert ausgewählt haben…	Führen Sie diese Aktion durch…
Falsch Positiv	Wählen Sie **Update** und **Suspect File Types löschen**, um Ihre Entscheidung zu erfassen und die normale ARP-Überwachung fortzusetzen. Wenn Sie ab ONTAP 9.13.1 MAV zum Schutz Ihrer ARP-Einstellungen verwenden, werden Sie durch den Clear-Suspect-Vorgang aufgefordert, die Genehmigung eines oder mehrerer zusätzlicher Administratoren einzuholen. "Die Genehmigung muss von allen Administratoren eingeholt werden" Der MAV-Genehmigungsgruppe zugeordnet oder der Vorgang schlägt fehl.
Möglicher Angriff Durch Ransomware	Reagieren Sie auf den Angriff und stellen Sie geschützte Daten wieder her. Wählen Sie dann **Update** und **Suspect File Types löschen**, um Ihre Entscheidung aufzuzeichnen und die normale ARP-Überwachung fortzusetzen. Es gibt keine verdächtigen Dateitypen, die gelöscht werden müssen, wenn Sie ein ganzes Volume wiederhergestellt haben.

CLI

1. Wenn Sie eine Benachrichtigung über einen vermuteten Ransomware-Angriff erhalten, überprüfen Sie die Zeit und den Schweregrad des Angriffs:

   ```
   security anti-ransomware volume show -vserver svm_name -volume vol_name
   ```

   Probenausgabe:

   ```
   Vserver Name: vs0
   Volume Name: vol1
   State: enabled
   Attack Probability: moderate
   Attack Timeline: 9/14/2021 01:03:23
   Number of Attacks: 1
   ```

Sie können auch EMS-Nachrichten überprüfen:

```
event log show -message-name callhome.arw.activity.seen
```

2. Erstellen Sie einen Angriffsbericht, und notieren Sie den Ausgabeland:

   ```
   security anti-ransomware volume attack generate-report -volume vol_name
   -dest-path file_location/
   ```

   Probenausgabe:

   ```
   Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
   "vs0:vol1/"
   ```

3. Zeigt den Bericht auf einem Administrator-Client-System an. Beispiel:

   ```
   [root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08

   19  "9/14/2021 01:03:23"   test_dir_1/test_file_1.jpg.lckd
   20  "9/14/2021 01:03:46"   test_dir_2/test_file_2.jpg.lckd
   21  "9/14/2021 01:03:46"   test_dir_3/test_file_3.png.lckd`
   ```

4. Nehmen Sie eine der folgenden Aktionen auf Grundlage Ihrer Bewertung der Dateiendungen:

   - Falsch positiv

     Geben Sie den folgenden Befehl ein, um Ihre Entscheidung aufzuzeichnen, die neue Erweiterung zur Liste der zulässigen hinzuzufügen und die normale Anti-Ransomware-Überwachung fortzusetzen:
     `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`

     Verwenden Sie einen der folgenden Parameter, um die Erweiterungen zu identifizieren:
     `[-seq-no integer]` Sequenznummer der Datei in der Liste der Verdächtigen.
     `[-extension text, … ]` Dateierweiterungen
     `[-start-time date_time -end-time date_time]` Start- und Endzeiten für den zu löhenden Bereich im Format „MM/TT/JJJJ HH:MM:SS“.

   - Möglicher Ransomware-Angriff

     Reagieren Sie auf den Angriff und "Wiederherstellen von Daten aus dem ARP-erstellten Backup-Snapshot". Nachdem die Daten wiederhergestellt wurden, geben Sie den folgenden Befehl ein, um Ihre Entscheidung zu notieren und die normale ARP-Überwachung fortzusetzen:

     ```
     anti-ransomware volume attack clear-suspect -vserver svm_name -volume
     vol_name [extension identifiers] -false-positive false
     ```

     Verwenden Sie einen der folgenden Parameter, um die Erweiterungen zu identifizieren:
     `[-seq-no integer]` Sequenznummer der Datei in der Liste der Verdächtigen
     `[-extension text, … ]` Dateierweiterung
     `[-start-time date_time -end-time date_time]` Start- und Endzeiten für den zu löhenden Bereich im Format „MM/TT/JJJJ HH:MM:SS“.

Es gibt keine verdächtigen Dateitypen, die gelöscht werden müssen, wenn Sie ein ganzes Volume wiederhergestellt haben. Der von ARP erstellte Backup-Snapshot wird entfernt und der Angriffsbericht wird gelöscht.

5. Wenn Sie MAV und ein erwartetes verwenden `clear-suspect` Für den Betrieb sind zusätzliche Genehmigungen erforderlich. Jeder Genehmiger der MAV-Gruppe führt die folgenden Schritte aus:

   a. Anfrage anzeigen:

   ```
   security multi-admin-verify request show
   ```

   b. Genehmigen Sie die Anforderung, das normale Anti-Ransomware-Monitoring fortzusetzen:

   ```
   security multi-admin-verify request approve -index[number returned from show request]
   ```

   Die Antwort für den letzten Gruppengenehmiger zeigt an, dass das Volume geändert und ein false positive aufgezeichnet wurde.

6. Wenn Sie MAV verwenden und ein Genehmiger der MAV-Gruppe sind, können Sie auch eine eindeutige Anforderung ablehnen:

   ```
   security multi-admin-verify request veto -index[number returned from show request]
   ```

Weitere Informationen

- "KB: Snapshots zum autonomen Ransomware-Schutz – Informationen zu Angriffen und dem autonomen Ransomware-Schutz".

Wiederherstellung von Daten nach einem Ransomware-Angriff

Autonomous Ransomware Protection (ARP) erstellt Snapshot-Kopien mit dem Namen `Anti_ransomware_backup` Potenzielle Ransomware-Bedrohungen werden erkannt. Sie können eine dieser ARP Snapshot Kopien oder eine andere Snapshot Kopie Ihres Volumes zum Wiederherstellen von Daten verwenden.

Über diese Aufgabe

Wenn das Volume über SnapMirror Beziehungen verfügt, replizieren Sie alle gespiegelten Kopien des Volumes unmittelbar nach der Wiederherstellung aus einer Snapshot Kopie manuell. Dadurch können nicht nutzbare Spiegelkopien erstellt werden, die gelöscht und neu erstellt werden müssen.

Zum Wiederherstellen aus einem anderen Snapshot als dem `Anti_ransomware_backup` Snapshot Nachdem ein Systemangriff erkannt wurde, müssen Sie den ARP-Snapshot zuerst freigeben.

Wenn kein Systemangriff gemeldet wurde, müssen Sie zuerst vom wiederherstellen `Anti_ransomware_backup` Snapshot-Kopie dann eine nachfolgende Wiederherstellung des Volume von der Snapshot-Kopie Ihrer Wahl abschließen.

Schritte

Die Wiederherstellung von Daten kann mit System Manager oder der ONTAP CLI erfolgen.

System Manager

Wiederherstellung nach einem Systemangriff

1. fahren Sie mit Schritt 2 fort, um die Wiederherstellung aus dem ARP-Snapshot durchzuführen. Um Restores aus einer früheren Snapshot Kopie durchzuführen, müssen Sie zuerst die Sperre des ARP Snapshot freigeben.
   a. Wählen Sie **Storage > Volumes**.
   b. Wählen Sie **Sicherheit** und dann **vermutete Dateitypen anzeigen**
   c. Markieren Sie die Dateien als "falsch positiv" .
   d. Wählen Sie **Update** und **Verdächtige Dateitypen löschen**
2. Anzeige der Snapshot Kopien in Volumes:

   Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies** aus.

3. Wählen Sie ⋮ Neben der Snapshot Kopie, die Sie wiederherstellen möchten, dann **Wiederherstellen**.

Wiederherstellung, wenn ein Systemangriff nicht erkannt wurde

1. Anzeige der Snapshot Kopien in Volumes:

   Wählen Sie **Storage > Volumes**, dann das Volume und **Snapshot Copies** aus.

2. Wählen Sie ⋮ Sie wählen die aus `Anti_ransomware_backup` Snapshot:
3. Wählen Sie **Wiederherstellen**.
4. Kehren Sie zum Menü **Snapshot Kopien** zurück und wählen Sie dann die Snapshot Kopie aus, die Sie verwenden möchten. Wählen Sie **Wiederherstellen**.

CLI

Wiederherstellung nach einem Systemangriff

1. fahren Sie mit Schritt zwei fort, um die Wiederherstellung aus der ARP Snapshot Kopie durchzuführen. Um Daten aus früheren Snapshot Kopien wiederherzustellen, müssen Sie die Sperre des ARP Snapshot freigeben.

   > Die Anti-Ransomware-SnapLock muss nur freigegeben werden, wenn Sie die verwenden, bevor die Daten aus früheren Snapshot Kopien wiederhergestellt werden `volume snap restore` Wie unten beschrieben. Wenn Sie Daten mit Flex Clone, Single File Snap Restore oder anderen Methoden wiederherstellen, ist dies nicht erforderlich.

   Markieren Sie den Angriff als „falsch positiv“ und „eindeutig verdächtig“:
   `anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true`
   Verwenden Sie einen der folgenden Parameter, um die Erweiterungen zu identifizieren:
   `[-seq-no integer]` Sequenznummer der Datei in der Liste der Verdächtigen.
   `[-extension text, … ]` Dateierweiterungen
   `[-start-time date_time -end-time date_time]` Start- und Endzeiten für den zu löhenden Bereich im Format „MM/TT/JJJJ HH:MM:SS“.

2. Listen Sie die Snapshot Kopien in einem Volume auf:

```
volume snapshot show -vserver SVM -volume volume
```

Im folgenden Beispiel werden die Snapshot Kopien in angezeigt `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. Stellen Sie den Inhalt eines Volumes aus einer Snapshot Kopie wieder her:

   ```
   volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
   ```

   Im folgenden Beispiel wird der Inhalt von wiederhergestellt `vol1`:

   ```
   cluster1::> volume snapshot restore -vserver vs0 -volume vol1
   -snapshot daily.2013-01-25_0010
   ```

Wiederherstellung, wenn ein Systemangriff nicht erkannt wurde

1. Listen Sie die Snapshot Kopien in einem Volume auf:

   ```
   volume snapshot show -vserver SVM -volume volume
   ```

   Im folgenden Beispiel werden die Snapshot Kopien in angezeigt `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                 State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Stellen Sie den Inhalt eines Volumes aus einer Snapshot Kopie wieder her:

   `volume snapshot restore -vserver SVM -volume volume -snapshot snapshot`

   Im folgenden Beispiel wird der Inhalt von wiederhergestellt `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

3. Wiederholen Sie die Schritte 1 und 2, um das Volume mithilfe der Desire Snapshot-Kopie wiederherzustellen.

Weitere Informationen

- "KB: Schutz vor Ransomware und Recovery in ONTAP"

Optionen für automatische Snapshot-Kopien ändern

Ab ONTAP 9.11.1 können Sie die CLI verwenden, um die Aufbewahrungseinstellungen für ARP-Snapshot Kopien (Autonomous Ransomware Protection) zu steuern, die als Reaktion auf vermutete Ransomware-Angriffe automatisch generiert werden.

Bevor Sie beginnen

Sie können nur ARP-Snapshot-Optionen auf einer Node-SVM ändern.

Schritte

1. Um alle aktuellen Einstellungen von ARP Snapshot Kopien anzuzeigen, geben Sie Folgendes ein: `vserver options -vserver svm_name arw*`

   Der `vserver options` Befehl ist ein verborgener Befehl. Um die man-Page anzuzeigen, geben Sie ein `man vserver options` Über die ONTAP CLI.

2. Um die ausgewählten aktuellen Einstellungen von ARP Snapshot Kopien anzuzeigen, geben Sie Folgendes ein:
   `vserver options -vserver svm_name -option-name arw_setting_name`
3. Geben Sie zum Ändern der Einstellungen für ARP Snapshot Kopien Folgendes ein:
   `vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value`

   Die folgenden Einstellungen können geändert werden:

ARW-Einstellung	Beschreibung
arw.Snap.max.count	Gibt die maximale Anzahl von ARP Snapshot-Kopien an, die jederzeit in einem Volume vorhanden sein können. Ältere Kopien werden gelöscht, um sicherzustellen, dass die Gesamtzahl der ARP Snapshot Kopien innerhalb dieses festgelegten Limits liegt.
arw.snap.create.interval.hours	Gibt das Intervall *in Stunden* zwischen ARP Snapshot Kopien an. Bei Verdacht eines Angriffs wird eine neue Snapshot Kopie erstellt, und die zuvor erstellte Kopie ist älter als dieses angegebene Intervall.
arw.snap.normal.retain.interval.hours	Gibt die Dauer *in Stunden* an, für die eine ARP Snapshot Kopie aufbewahrt wird. Wenn eine ARP Snapshot-Kopie diese alt wird, werden alle anderen ARP Snapshot-Kopien, die erstellt wurden, bevor die neueste Kopie, auf die dieses Alter zu erreichen, gelöscht. Keine ARP Snapshot Kopie kann älter als diese Dauer sein.
arw.snap.max.retain.interval.days	Gibt die maximale Dauer *in Tagen* an, für die eine ARP Snapshot Kopie aufbewahrt werden kann. Alle ARP-Snapshot-Kopien, die älter als diese Dauer sind, werden gelöscht, wenn auf dem Volume kein Angriff gemeldet wird. + Das maximale Aufbewahrungsintervall für ARP Snapshot Kopien wird ignoriert, wenn eine mäßige Bedrohung erkannt wird. Die als Antwort auf die Bedrohung erstellte ARP Snapshot-Kopie wird beibehalten, bis Sie auf die Bedrohung reagiert haben. Wenn eine Bedrohung als falsch positiv markiert wird, löschen Sie die ARP Snapshot Kopien auf dem Volume.
arw.snap.create.interval.hours.post.max.count	Gibt das Intervall *in Stunden* zwischen ARP Snapshot Kopien an, wenn das Volume bereits die maximale Anzahl an ARP Snapshot Kopien enthält. Wenn die Höchstzahl erreicht wird, wird eine ARP Snapshot-Kopie gelöscht, um Platz für eine neue Kopie zu schaffen. Die neue Erstellungsgeschwindigkeit von ARP Snapshot Kopien kann mit dieser Option die ältere Kopie beibehalten werden. Wenn das Volume bereits die maximale Anzahl von ARP Snapshot-Kopien enthält, wird dieses in dieser Option angegebene Intervall anstelle von arw.snap.create.interval.hours für die Erstellung der nächsten ARP Snapshot-Kopie verwendet.
arw.surge.snap.interval.days	Gibt das Intervall *in Tagen* zwischen ARP-Überspannungs-Snapshot-Kopien an. ONTAP erzeugt eine ARP Snapshot Überspannungskopie, wenn ein Anstieg des IO-Verkehrs auftritt, und die letzte erstellte ARP Snapshot-Kopie ist älter als dieses angegebene Intervall. Mit dieser Option wird auch die Aufbewahrungsfrist *in Tag* für einen ARP-Überspannungsabgleich festgelegt.

Schützen Sie sich vor Viren

Übersicht über die Virenschutzkonfiguration

Vscan ist eine von NetApp entwickelte Virenschutzlösung, mit der Kunden ihre Daten vor Angriffen durch Viren oder anderen Schadcode schützen können.

Vscan führt Virenprüfungen durch, wenn Clients über SMB auf Dateien zugreifen. Sie können Vscan so konfigurieren, dass er nach Bedarf oder nach einem Zeitplan scannt. Sie können mit Vscan über die ONTAP-Befehlszeilenschnittstelle (CLI) oder ONTAP-APIs (Application Programming Interfaces) interagieren.

Verwandte Informationen

"Partnerlösungen von Vscan"

Über den Virenschutz von NetApp

Informationen zur Virenprüfung von NetApp

Vscan ist eine von NetApp entwickelte Virenschutzlösung, mit der Kunden ihre Daten vor Angriffen durch Viren oder anderen Schadcode schützen können. Es kombiniert von Partnern bereitgestellte Antivirensoftware mit ONTAP-Funktionen, um Kunden die Flexibilität zu geben, die sie für die Verwaltung der Dateiprüfung benötigen.

So funktioniert die Virenprüfung

Storage-Systeme verlagern Scanvorgänge auf externe Server, auf denen Virenschutz-Software von Drittanbietern gehostet wird.

Basierend auf dem aktiven Scanmodus sendet ONTAP Scananforderungen, wenn Clients über SMB (On-Access) auf Dateien zugreifen oder an bestimmten Orten auf Dateien zugreifen, nach Zeitplan oder sofort (On-Demand).

- Sie können *On-Access Scanning* verwenden, um nach Viren zu suchen, wenn Clients Dateien über SMB öffnen, lesen, umbenennen oder schließen. Dateivorgänge werden angehalten, bis der externe Server den Scanstatus der Datei meldet. Wenn die Datei bereits gescannt wurde, ermöglicht ONTAP den Dateivorgang. Andernfalls fordert er einen Scan vom Server an.

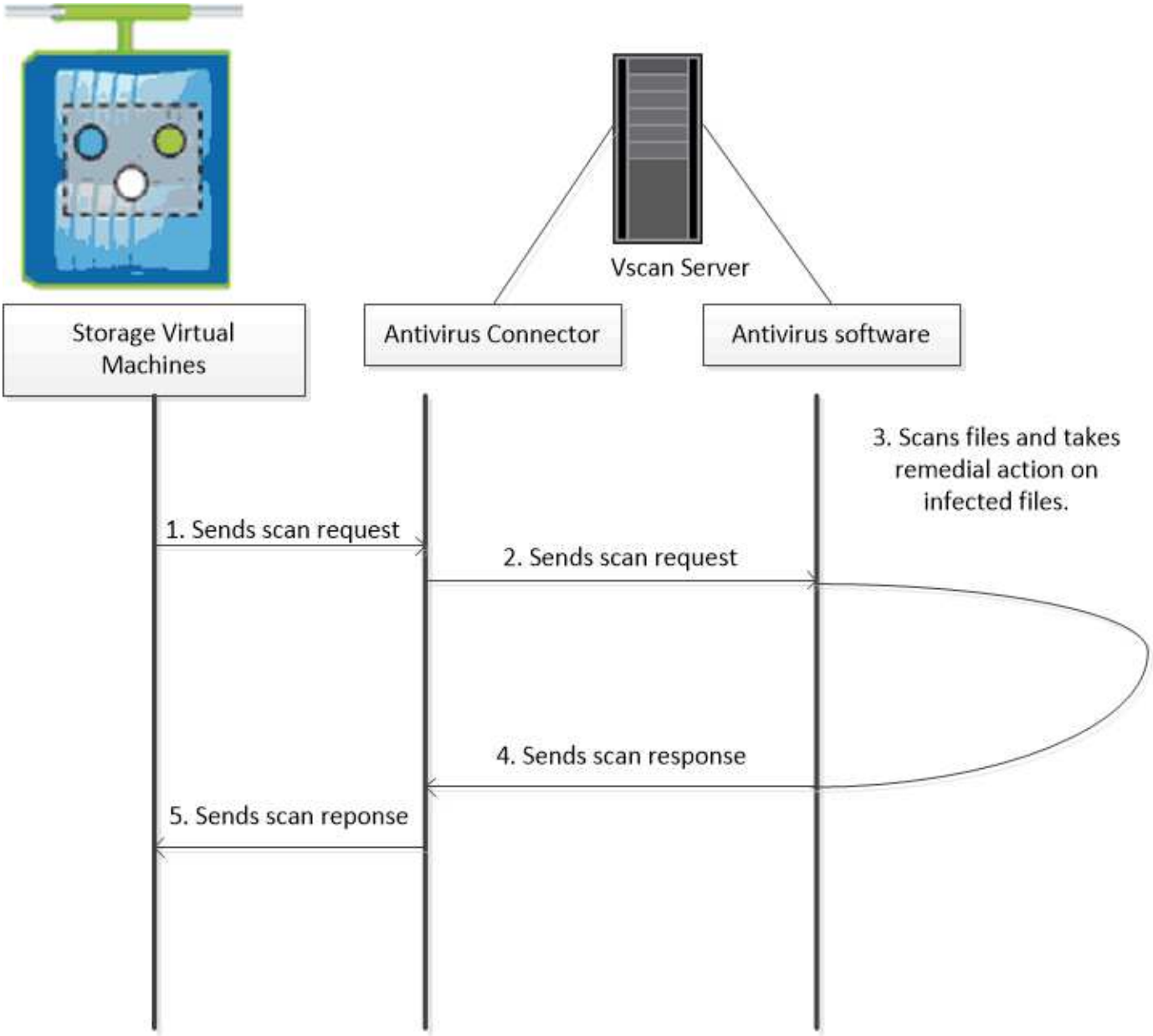
  Das Scannen beim Zugriff wird für NFS nicht unterstützt.

- Sie können *On-Demand Scan* verwenden, um Dateien sofort oder nach Zeitplan auf Viren zu überprüfen. Wir empfehlen die Ausführung von On-Demand-Scans nur in Zeiten geringerer Auslastung, um eine Überlastung der vorhandenen AV-Infrastruktur zu vermeiden, die normalerweise für Scans bei Zugriff verwendet wird. Der externe Server aktualisiert den Scanstatus der geprüften Dateien, sodass die Latenz beim Dateizugriff über SMB reduziert wird. Wenn Dateiänderungen oder Softwareupdates vorgenommen wurden, wird eine neue Dateiprüfung vom externen Server angefordert.

  Der bedarfsorientierte Scan eignet sich für jeden Pfad im SVM Namespace. Dies gilt auch für Volumes, die nur über NFS exportiert werden.

In der Regel können Sie auf einer SVM sowohl den Scan-Modus für den Zugriff als auch den On-Demand-Modus aktivieren. In beiden Modi führt die Antivirensoftware anhand Ihrer Softwareeinstellungen Abhilfemaßnahmen für infizierte Dateien durch.

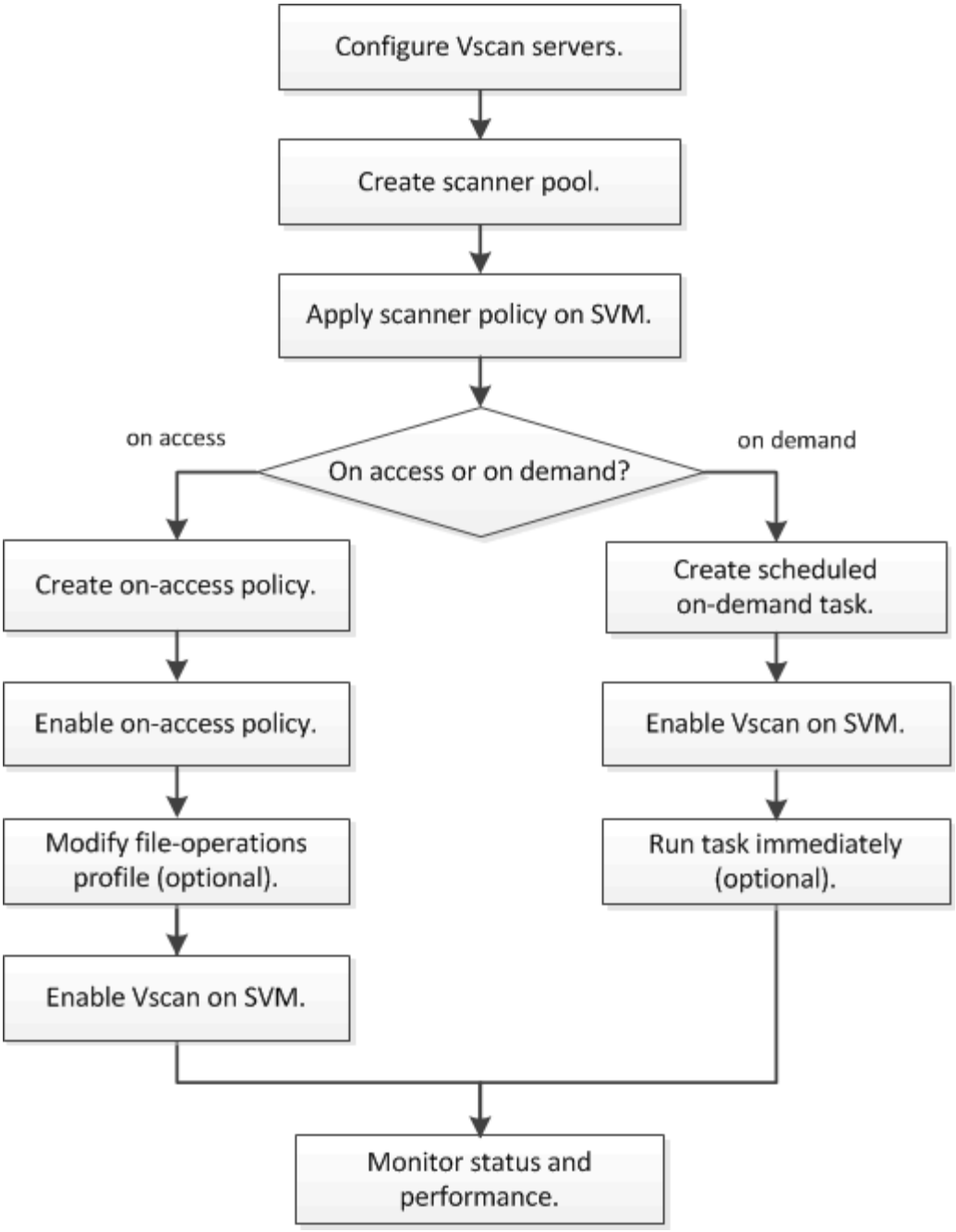
Der von NetApp bereitgestellte und auf dem externen Server installierte ONTAP Antivirus Connector übernimmt die Kommunikation zwischen dem Storage-System und der Antivirensoftware.



Workflow für Virenprüfung

Sie müssen einen Scannerpool erstellen und eine Scannerrichtlinie anwenden, bevor Sie das Scannen aktivieren können. In der Regel können Sie auf einer SVM sowohl den Scan-Modus für den Zugriff als auch den On-Demand-Modus aktivieren.

Sie müssen die CIFS-Konfiguration abgeschlossen haben.



Nächste Schritte

- Erstellen Sie einen Scanner-Pool auf einem einzelnen Cluster
- Wenden Sie eine Scannerrichtlinie auf einem einzelnen Cluster an
- Erstellen einer Zugriffsrichtlinie

Virenschutz-Architektur

Die NetApp Virenschutzarchitektur besteht aus der Vscan-Serversoftware und den zugehörigen Einstellungen.

Vscan Server-Software

Sie müssen diese Software auf dem Vscan-Server installieren.

- **ONTAP Antivirus Connector**

  Hierbei handelt es sich um die von NetApp bereitgestellte Software, die die Kommunikation von Scananforderungen und -antworten zwischen SVMs und Virenschutz-Software übernimmt. Er kann auf einer virtuellen Maschine ausgeführt werden, um die bestmögliche Leistung zu erzielen, verwenden Sie jedoch eine physische Maschine. Sie können diese Software von der NetApp Support-Website herunterladen (Anmeldung erforderlich).

- **Antivirus-Software**

  Dies ist eine vom Partner bereitgestellte Software, die Dateien auf Viren oder anderen schädlichen Code scannt. Sie geben die Abhilfemaßnahmen für infizierte Dateien an, wenn Sie die Software konfigurieren.

Vscan-Softwareeinstellungen

Sie müssen diese Softwareeinstellungen auf dem Vscan-Server konfigurieren.

- **Scanner-Pool**

  Diese Einstellung definiert die Vscan-Server und privilegierten Benutzer, die eine Verbindung zu SVMs herstellen können. Es definiert auch eine Zeitdauer für die Scan-Anforderung, nach der die Scan-Anforderung an einen alternativen Vscan-Server gesendet wird, wenn eine verfügbar ist.

  > Sie sollten in der Antivirensoftware auf dem Vscan-Server die Zeitdauer für die Zeitüberschreitung bei Scan-Request-Anforderung des Scanners auf fünf Sekunden einstellen. Dadurch werden Situationen vermieden, in denen der Dateizugriff verzögert oder ganz verweigert wird, da die Zeitüberschreitung auf der Software größer ist als die Zeitdauer für die Scananforderung.

- **Privilegierter Benutzer**

  Diese Einstellung ist ein Domänenbenutzerkonto, das ein Vscan-Server verwendet, um eine Verbindung mit der SVM herzustellen. Das Konto muss in der Liste der privilegierten Benutzer im Scanner-Pool vorhanden sein.

- **Scanner-Richtlinie**

  Diese Einstellung bestimmt, ob ein Scannerpool aktiv ist. Scannerrichtlinien sind systemdefiniert, sodass Sie keine benutzerdefinierten Scannerrichtlinien erstellen können. Nur diese drei Richtlinien sind verfügbar:

  - `Primary` Gibt an, dass der Scannerpool aktiv ist.
  - `Secondary` Gibt an, dass der Scanner-Pool nur aktiv ist, wenn keiner der Vscan-Server im primären Scanner-Pool verbunden ist.
  - `Idle` Gibt an, dass der Scannerpool inaktiv ist.

- **Zugangsrichtlinie**

  Diese Einstellung definiert den Umfang eines Scans bei Zugriff. Sie können die maximale Dateigröße für den Scan, Dateierweiterungen und Pfade für den Scan sowie Dateierweiterungen und -Pfade für den Scan angeben.

  Standardmäßig werden nur Lese- und Schreib-Volumes gescannt. Sie können Filter festlegen, die das Scannen von schreibgeschützten Volumes ermöglichen oder das Scannen auf Dateien beschränken, die mit dem Zugriff ausführen geöffnet wurden:

- `scan-ro-volume` Ermöglicht das Scannen schreibgeschützter Volumes.
- `scan-execute-access` Schränkt das Scannen auf Dateien ein, die durch Ausführen des Zugriffs geöffnet wurden.

> „`Zugriff ausführen`“ unterscheidet sich von „`Berechtigung ausführen`“. Ein bestimmter Client hat nur dann “Execute Access” auf eine ausführbare Datei, wenn die Datei mit “Execute Intent” geöffnet wurde.

Sie können die einstellen `scan-mandatory` Option „aus“, um festzulegen, dass der Dateizugriff zulässig ist, wenn keine Vscan-Server für Virenprüfungen verfügbar sind. Im On-Access-Modus können Sie aus den folgenden beiden Optionen wählen, die sich gegenseitig ausschließen:

- Obligatorisch: Mit dieser Option versucht Vscan, die Scananforderung an den Server zu senden, bis die Timeout-Zeit abläuft. Wenn die Scananforderung vom Server nicht akzeptiert wird, wird die Clientzugriffsanforderung abgelehnt.
- Nicht obligatorisch: Mit dieser Option erlaubt Vscan immer den Client-Zugriff, unabhängig davon, ob ein Vscan-Server für den Virenscanner verfügbar war oder nicht.

- **On-Demand Task**

  Diese Einstellung definiert den Umfang eines On-Demand-Scans. Sie können die maximale Dateigröße für den Scan, Dateierweiterungen und Pfade für den Scan sowie Dateierweiterungen und -Pfade für den Scan angeben. Dateien in Unterverzeichnissen werden standardmäßig gescannt.

  Sie verwenden einen Cron-Zeitplan, um festzulegen, wann die Aufgabe ausgeführt wird. Sie können das verwenden `vserver vscan on-demand-task run` Befehl zum sofortigen Ausführen der Aufgabe.

- **Vscan-Dateioperationen-Profil (nur beim Scannen beim Zugriff)**

  Der `vscan-fileop-profile` Parameter für das `vserver cifs share create` Befehl definiert, welche SMB-Dateioperationen einen Virus-Scan auslösen. Standardmäßig ist der Parameter auf festgelegt `standard`, Das ist NetApp Best Practice. Sie können diesen Parameter bei Bedarf anpassen, wenn Sie eine SMB-Freigabe erstellen oder ändern:

  - `no-scan` Gibt an, dass Virenscans nie für die Freigabe ausgelöst werden.
  - `standard` Gibt an, dass Virenscans durch Öffnen, Schließen und Umbenennen ausgelöst werden.
  - `strict` Gibt an, dass Virenscans durch Öffnen, Lesen, Schließen und Umbenennen ausgelöst werden.

    Der `strict` Profil bietet erhöhte Sicherheit für Situationen, in denen mehrere Clients gleichzeitig auf eine Datei zugreifen. Wenn ein Client eine Datei schließt, nachdem ein Virus darauf geschrieben wurde, und die gleiche Datei weiterhin auf einem zweiten Client geöffnet bleibt, `strict` Stellt sicher, dass ein Lesevorgang auf dem zweiten Client einen Scan auslöst, bevor die Datei geschlossen wird.

    Sie sollten vorsichtig sein, die zu beschränken `strict` Profil für Freigaben, die Dateien enthalten, auf die Sie erwarten, wird gleichzeitig zugegriffen. Da dieses Profil mehr Scananforderungen generiert, kann dies die Performance beeinträchtigen.

  - `writes-only` Gibt an, dass Virenscans nur ausgelöst werden, wenn geänderte Dateien geschlossen werden.

    Seit `writes-only` Weniger Scananforderungen werden generiert, in der Regel wird die Performance

verbessert.

Wenn Sie dieses Profil verwenden, muss der Scanner so konfiguriert sein, dass nicht reparierbare infizierte Dateien gelöscht oder isoliert werden können, sodass kein Zugriff darauf möglich ist. Wenn beispielsweise ein Client eine Datei nach dem Schreiben eines Virus schließt und die Datei nicht repariert, gelöscht oder isoliert wird, kann jeder Client, der auf die Datei zugreift, eine Datei schließen `without` Das Schreiben wird infiziert sein.

> Wenn eine Client-Anwendung einen Umbenennung durchführt, wird die Datei mit dem neuen Namen geschlossen und nicht gescannt. Wenn ein solcher Betrieb in Ihrer Umgebung Sicherheitsaspekte mit sich bringt, sollten Sie den verwenden `standard` Oder `strict` Profil:

Partnerlösungen von Vscan

NetApp arbeitet mit Trellix, Symantec, Trend Micro und Sentinel One zusammen, um branchenführende Anti-Malware- und Antiviren-Lösungen bereitzustellen, die auf der ONTAP Vscan-Technologie aufbauen. Diese Lösungen helfen Ihnen, Dateien auf Malware zu scannen und alle betroffenen Dateien zu beheben.

Wie in der folgenden Tabelle dargestellt, werden die Details zur Interoperabilität von Trellix, Symantec und Trend Micro in der Interoperabilitätsmatrix von NetApp beibehalten. Interoperabilitätsdetails für Trellix und Symantec finden Sie auch auf den Partner-Websites. Informationen zur Interoperabilität von Sentinel One und anderen neuen Partnern werden vom Partner auf seinen Websites gepflegt.

Partner	Lösungsdokumentation	Details zur Interoperabilität
Trellix (ehemals McAfee)	"Trellix Produktdokumentation"	• "NetApp Interoperabilitäts-Matrix-Tool" • "Unterstützte Plattformen für Endpoint Security Storage Protection (trellix.com)"
Symantec	"Symantec Protection Engine 9.0.0"	• "NetApp Interoperabilitäts-Matrix-Tool" • "Support Matrix für Partnergeräte, die mit Symantec Protection Engine (SPE) für Network Attached Storage (NAS) zertifiziert sind 9.x.x" • "Support Matrix für Partnergeräte, die mit Symantec Protection Engine (SPE) für Network Attached Storage (NAS) zertifiziert sind 8.x (broadcom.com)"
Trend Micro	"Trend Micro ServerProtect for Storage 6.0 – Leitfaden für die ersten Schritte"	"NetApp Interoperabilitäts-Matrix-Tool"

Partner	Lösungsdokumentation	Details zur Interoperabilität
Sentinel One	• "SentinelOne Singularity Cloud Data Security" • "SentinelOne-Unterstützung" Für diesen Link ist eine Benutzeranmeldung erforderlich. Sie können den Zugriff über Sentinel One anfordern.	Tiefes Instinkt

Installation und Konfiguration des Vscan-Servers

Installation und Konfiguration des Vscan-Servers

Richten Sie einen oder mehrere Vscan-Server ein, um sicherzustellen, dass Dateien auf Ihrem System auf Viren gescannt werden. Befolgen Sie die Anweisungen Ihres Anbieters, um die Antivirensoftware auf dem Server zu installieren und zu konfigurieren.

Befolgen Sie die Anweisungen in der von NetApp bereitgestellten README-Datei, um den ONTAP Antivirus Connector zu installieren und zu konfigurieren. Befolgen Sie alternativ die Anweisungen auf der "Installieren Sie die Seite ONTAP Antivirus Connector".

> Für Disaster Recovery- und MetroCluster-Konfigurationen müssen Sie separate Vscan-Server für die primären/lokalen und sekundären/Partner-ONTAP-Cluster einrichten und konfigurieren.

Anforderungen an die Virenschutz-Software

- Informationen zu den Anforderungen an Antivirensoftware finden Sie in der Dokumentation des Anbieters.
- Informationen zu den von Vscan unterstützten Herstellern, Software und Versionen finden Sie im "Partnerlösungen von Vscan" Seite.

Anforderungen für den Antivirus Connector von ONTAP

- Sie können den ONTAP Antivirus Connector von der Seite **Software-Download** auf der NetApp Support-Website herunterladen. "NetApp Downloads: Software"
- Informationen zu den Windows-Versionen, die vom ONTAP-VirenschutzConnector unterstützt werden, und zu den Interoperabilitätsanforderungen finden Sie unter "Partnerlösungen von Vscan".

> Sie können verschiedene Versionen von Windows-Servern für verschiedene Vscan-Server in einem Cluster installieren.

- .NET 3.0 oder höher muss auf dem Windows-Server installiert sein.
- SMB 2.0 muss auf dem Windows Server aktiviert sein.

Installieren Sie den ONTAP Antivirus Connector

Installieren Sie den ONTAP-Virenschutzanschluss auf dem Vscan-Server, um die

Kommunikation zwischen dem System, auf dem ONTAP ausgeführt wird, und dem Vscan-Server zu ermöglichen. Bei der Installation des ONTAP Antivirus Connectors kann die Virenschutzsoftware mit einer oder mehreren Storage Virtual Machines (SVMs) kommunizieren.

Über diese Aufgabe

- Siehe "Partnerlösungen von Vscan" Auf dieser Seite finden Sie Informationen zu unterstützten Protokollen, Softwareversionen von Antivirenanbietern, ONTAP-Versionen, Interoperabilitätsanforderungen und Windows-Servern.
- .NET 4.5.1 oder höher muss installiert sein.
- Der ONTAP Antivirus Connector kann auf einer virtuellen Maschine ausgeführt werden. Um die beste Performance zu erzielen, empfiehlt NetApp jedoch die Verwendung einer dedizierten Virtual Machine für Virenschutzprüfungen.
- SMB 2.0 muss auf dem Windows-Server aktiviert sein, auf dem Sie den ONTAP-Antivirus-Connector installieren und ausführen.

Bevor Sie beginnen

- Laden Sie die Installationsdatei für den ONTAP Antivirus Connector von der Support-Website herunter und speichern Sie sie in einem Verzeichnis auf Ihrer Festplatte.
- Stellen Sie sicher, dass Sie die Anforderungen für die Installation des ONTAP-Virenschutzanschlusses erfüllen.
- Überprüfen Sie, ob Sie über Administratorrechte für die Installation des Antivirus Connectors verfügen.

Schritte

1. Starten Sie den Antivirus Connector-Installationsassistenten, indem Sie die entsprechende Setup-Datei ausführen.
2. Wählen Sie *Next*. Das Dialogfeld Zielordner wird geöffnet.
3. Wählen Sie *Next*, um den Antivirus Connector in dem Ordner zu installieren, der aufgelistet ist, oder wählen Sie *Change*, um ihn in einem anderen Ordner zu installieren.
4. Das Dialogfeld ONTAP AV-Connector Windows-Dienstanmeldeinformationen wird geöffnet.
5. Geben Sie Ihre Windows-Dienstanmeldeinformationen ein, oder wählen Sie **Hinzufügen**, um einen Benutzer auszuwählen. Bei einem ONTAP-System muss dieser Benutzer ein gültiger Domänenbenutzer sein und in der Scannerpoolkonfiguration für die SVM vorhanden sein.
6. Wählen Sie **Weiter**. Das Dialogfeld bereit zur Installation des Programms wird geöffnet.
7. Wählen Sie **Installieren**, um mit der Installation zu beginnen, oder wählen Sie **Zurück**, wenn Sie Änderungen an den Einstellungen vornehmen möchten.
   Ein Statusfeld wird geöffnet und zeigt den Fortschritt der Installation an, gefolgt vom Dialogfeld InstallShield Wizard abgeschlossen.
8. Aktivieren Sie das Kontrollkästchen ONTAP LIFs konfigurieren, wenn Sie mit der Konfiguration von ONTAP Management oder Daten-LIFs fortfahren möchten.
   Sie müssen mindestens eine ONTAP Management- oder Daten-LIF konfigurieren, bevor dieser Vscan-Server verwendet werden kann.
9. Aktivieren Sie das Kontrollkästchen Windows Installer-Protokoll anzeigen*, wenn Sie die Installationsprotokolle anzeigen möchten.
10. Wählen Sie **Fertig stellen**, um die Installation zu beenden und den InstallShield-Assistenten zu schließen. Das Symbol **Configure ONTAP LIFs** wird auf dem Desktop gespeichert, um die ONTAP LIFs zu

konfigurieren.

11. Fügen Sie dem Antivirus Connector eine SVM hinzu.
Sie können dem VirenschutzConnector eine SVM hinzufügen, indem Sie entweder eine ONTAP-Management-LIF hinzufügen, die zum Abrufen der Liste der Daten-LIFs abgefragt wird, oder die Daten-LIF oder LIFs direkt konfigurieren.
Wenn die ONTAP Management LIF konfiguriert ist, müssen Sie außerdem die Abfrageinformationen und die Anmeldeinformationen des ONTAP Administratorkontos angeben.
    - Vergewissern Sie sich, dass die Management-LIF oder die IP-Adresse der SVM für aktiviert ist `management-https`. Dies ist nicht erforderlich, wenn Sie nur die Daten-LIFs konfigurieren.
    - Vergewissern Sie sich, dass Sie ein Benutzerkonto für die HTTP-Anwendung erstellt und eine Rolle zugewiesen haben, die (mindestens schreibgeschützt) Zugriff auf das hat `/api/network/ip/interfaces` REST-API:
    Weitere Informationen zum Erstellen eines Benutzers finden Sie im "Rolle für Sicherheits-Login erstellen" Und "Sicherheits-Login erstellen" ONTAP-man-Pages.

> Sie können den Domänenbenutzer auch als Konto verwenden, indem Sie eine SVM für einen Authentifizierungstunnel für eine administrative SVM hinzufügen. Weitere Informationen finden Sie im "Sicherheit Login Domain-Tunnel erstellen" ONTAP-man-Page verwenden oder `/api/security/acccounts` Und `/api/security/roles` REST-APIs zum Konfigurieren des Administratorkontos und der Rolle.

Schritte

1. Klicken Sie mit der rechten Maustaste auf das Symbol **ONTAP-LIFs konfigurieren**, das nach Abschluss der Installation des Virenschutzanschlusses auf Ihrem Desktop gespeichert wurde, und wählen Sie dann **als Administrator ausführen** aus.
2. Wählen Sie im Dialogfeld ONTAP LIFs konfigurieren den bevorzugten Konfigurationstyp aus und führen Sie dann die folgenden Aktionen durch:

Um diesen Typ von LIF zu erstellen…	Führen Sie diese Schritte aus…
Daten-LIF	a. „Rolle“ auf „Daten“ setzen b. Stellen Sie das „Datenprotokoll“ auf „cifs“ ein. c. Firewall-Richtlinie auf „Daten“ setzen d. Setzen Sie „Service Policy“ auf „default-Data-files“
Management-LIF	a. „Rolle* auf „Daten“ setzen b. Stellen Sie „Datenprotokoll“ auf „keine“ ein. c. Firewall-Richtlinie auf „Management“ setzen d. Service-Richtlinie auf Standardmanagement setzen

Weitere Informationen "Erstellen einer LIF".

Nachdem Sie eine LIF erstellt haben, geben Sie die Daten- oder Management-LIF- oder IP-Adresse der hinzuzufügenden SVM ein. Sie können auch die Cluster-Management-LIF eingeben. Wenn Sie die Cluster-Management-LIF angeben, können alle SVMs innerhalb des Clusters, die SMB verwenden, den Vscan-Server verwenden.

> Wenn Kerberos-Authentifizierung für Vscan-Server erforderlich ist, muss jede SVM-Daten-LIF über einen eindeutigen DNS-Namen verfügen. Sie müssen diesen Namen als Server-Principal-Name (SPN) im Windows Active Directory registrieren. Wenn für jede Daten-LIF kein eindeutiger DNS-Name verfügbar oder als SPN registriert ist, verwendet der Vscan-Server den NT LAN Manager-Mechanismus zur Authentifizierung. Wenn Sie die DNS-Namen und SPNs nach der Verbindung mit dem Vscan-Server hinzufügen oder ändern, müssen Sie den Antivirus Connector-Dienst auf dem Vscan-Server neu starten, um die Änderungen anzuwenden.

3. Geben Sie zum Konfigurieren einer Management-LIF die Abfragedauer in Sekunden ein. Die Abfragedauer ist die Häufigkeit, mit der der Antivirus Connector auf Änderungen an den SVMs oder der LIF-Konfiguration des Clusters prüft. Das standardmäßige Abfrageintervall beträgt 60 Sekunden.
4. Geben Sie den Namen und das Passwort des ONTAP Administratorkontos ein, um eine Management-LIF zu konfigurieren.
5. Klicken Sie auf **Test**, um die Verbindung zu überprüfen und die Authentifizierung zu überprüfen. Die Authentifizierung wird nur für eine Management-LIF-Konfiguration verifiziert.
6. Klicken Sie auf **Update**, um die LIF zur Liste der LIFs hinzuzufügen, zu denen Sie die Abfrage durchführen oder eine Verbindung herstellen möchten.
7. Klicken Sie auf **Speichern**, um die Verbindung zur Registrierung zu speichern.
8. Klicken Sie auf **Export**, wenn Sie die Liste der Verbindungen in eine Registry-Import- oder Registry-Export-Datei exportieren möchten. Dies ist nützlich, wenn mehrere Vscan-Server denselben Satz an Management- oder Daten-LIFs verwenden.

Siehe "Konfigurieren Sie die Seite ONTAP Antivirus Connector" Für Konfigurationsoptionen.

Konfigurieren Sie den ONTAP-Virenschutzanschluss

Konfigurieren Sie den ONTAP Antivirus Connector so, dass eine oder mehrere Storage Virtual Machines (SVMs) angegeben werden, zu denen Sie eine Verbindung herstellen möchten, indem Sie entweder die ONTAP Management-LIF eingeben, Abfrageinformationen und die Anmeldedaten des ONTAP Administratorkontos oder nur die Daten-LIF eingeben. Sie können auch die Details einer SVM-Verbindung ändern oder eine SVM-Verbindung entfernen. Standardmäßig verwendet der ONTAP Antivirus Connector REST-APIs, um die Liste der Daten-LIFs abzurufen, wenn die ONTAP Management-LIF konfiguriert ist.

Ändern Sie die Details einer SVM-Verbindung

Sie können die Details einer SVM-Verbindung (Storage Virtual Machine) aktualisieren, die dem VirenschutzConnector hinzugefügt wurde, indem Sie die ONTAP-Verwaltungs-LIF und die Abfrageinformationen ändern. Sie können die Daten-LIFs nicht aktualisieren, nachdem sie hinzugefügt wurden. Zum Aktualisieren der Daten-LIFs müssen Sie sie zunächst entfernen und sie dann erneut mit der neuen LIF oder IP-Adresse hinzufügen.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie ein Benutzerkonto für die HTTP-Anwendung erstellt und eine Rolle zugewiesen haben, die (mindestens schreibgeschützt) Zugriff auf das hat `/api/network/ip/interfaces` REST-API:
Weitere Informationen zum Erstellen eines Benutzers finden Sie im "Rolle für Sicherheits-Login erstellen" Und das "Sicherheits-Login erstellen" Befehle.

Sie können den Domänenbenutzer auch als Konto verwenden, indem Sie eine SVM für einen Authentifizierungstunnel für eine administrative SVM hinzufügen.
Weitere Informationen finden Sie im "Sicherheit Login Domain-Tunnel erstellen" ONTAP-Hauptseite.

Schritte

1. Klicken Sie mit der rechten Maustaste auf das Symbol **ONTAP-LIFs konfigurieren**, das nach Abschluss der Installation des Virenschutzanschlusses auf Ihrem Desktop gespeichert wurde, und wählen Sie dann **als Administrator ausführen** aus. Das Dialogfeld ONTAP LIFs konfigurieren wird geöffnet.
2. Wählen Sie die SVM-IP-Adresse aus, und klicken Sie dann auf **Update**.
3. Aktualisieren Sie die Informationen nach Bedarf.
4. Klicken Sie auf **Speichern**, um die Verbindungsdetails in der Registrierung zu aktualisieren.
5. Klicken Sie auf **Export**, wenn Sie die Liste der Verbindungen in einen Registry-Import oder eine Registry-Exportdatei exportieren möchten.
   Dies ist nützlich, wenn mehrere Vscan-Server denselben Satz an Management- oder Daten-LIFs verwenden.

Entfernen Sie eine SVM-Verbindung aus dem Antivirus Connector

Wenn Sie keine SVM-Verbindung mehr benötigen, können Sie sie entfernen.

Schritte

1. Klicken Sie mit der rechten Maustaste auf das Symbol **ONTAP-LIFs konfigurieren**, das nach Abschluss der Installation des Virenschutzanschlusses auf Ihrem Desktop gespeichert wurde, und wählen Sie dann **als Administrator ausführen** aus. Das Dialogfeld ONTAP LIFs konfigurieren wird geöffnet.
2. Wählen Sie eine oder mehrere SVM-IP-Adressen aus, und klicken Sie dann auf **Entfernen**.
3. Klicken Sie auf **Speichern**, um die Verbindungsdetails in der Registrierung zu aktualisieren.
4. Klicken Sie auf **Export**, wenn Sie die Liste der Verbindungen in eine Registry-Import- oder Registry-Export-Datei exportieren möchten.
   Dies ist nützlich, wenn mehrere Vscan-Server denselben Satz an Management- oder Daten-LIFs verwenden.

Fehlerbehebung

Bevor Sie beginnen

Wenn Sie in diesem Verfahren Registrierungswerte erstellen, verwenden Sie den rechten Fensterbereich.

Sie können Antivirus Connector-Protokolle für Diagnosezwecke aktivieren oder deaktivieren. Diese Protokolle sind standardmäßig deaktiviert. Um die Leistung zu verbessern, sollten Sie die Antivirus Connector-Protokolle deaktiviert halten und nur für kritische Ereignisse aktivieren.

Schritte

1. Wählen Sie **Start**, geben Sie "regedit" in das Suchfeld ein, und wählen Sie dann `regedit.exe` In der Liste Programme.
2. Suchen Sie in **Registrierungs-Editor** den folgenden Unterschlüssel für den ONTAP Antivirus Connector:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Erstellen Sie Registrierungswerte, indem Sie den Typ, den Namen und die Werte angeben, die in der folgenden Tabelle aufgeführt sind:

Typ	Name	Werte
Zeichenfolge	Tracepath	c:\avshim.log

Dieser Registrierungswert kann jeder andere gültige Pfad sein.

4. Erstellen Sie einen weiteren Registrierungswert, indem Sie den Typ, den Namen, die Werte und die Protokollinformationen in der folgenden Tabelle angeben:

Typ	Name	Kritische Protokollierung	Zwischenprotokollierung	Ausführliche Protokollierung
DWORD	Tracelevel	1	2 oder 3	4

Dadurch werden die Protokolle des Antivirus Connector aktiviert, die unter dem im TracePath in Schritt 3 angegebenen Pfadwert gespeichert werden.

5. Deaktivieren Sie Antivirus Connector-Protokolle, indem Sie die in Schritt 3 und 4 erstellten Registrierungswerte löschen.
6. Erstellen Sie einen weiteren Registrierungswert vom Typ "MULTI_SZ" mit dem Namen "LogRotation" (ohne Anführungszeichen). In „LogRotation“
Geben Sie „logFileSize:1“ als Eintrag für die Rotationsgröße an (wobei 1 für 1MB steht) und geben Sie in der nächsten Zeile „logFileCount:5“ als an an an
Eingabe für Rotationsgrenze (5 ist die Grenze).

> Diese Werte sind optional. Wenn sie nicht angegeben werden, werden für die Rotationsgröße bzw. die Rotationsgrenze Standardwerte von 20MB und 10 Dateien verwendet. Die angegebenen Ganzzahlwerte enthalten keine Dezimalwerte oder Bruchwerte. Wenn Sie Werte angeben, die höher als die Standardwerte sind, werden stattdessen die Standardwerte verwendet.

7. Um die benutzerdefinierte Protokollrotation zu deaktivieren, löschen Sie die Registrierungswerte, die Sie in Schritt 6 erstellt haben.

Anpassbares Banner

Ein benutzerdefiniertes Banner ermöglicht es Ihnen, eine rechtsverbindliche Aussage und einen Haftungsausschluss für den Systemzugriff im Fenster *Configure ONTAP LIF API* zu platzieren.

Schritt

1. Ändern Sie das Standard-Banner, indem Sie den Inhalt im aktualisieren `banner.txt` Datei im Installationsverzeichnis speichern und dann die Änderungen speichern.
Sie müssen das Fenster ONTAP LIF-API konfigurieren erneut öffnen, um die Änderungen im Banner anzuzeigen.

Aktivieren Sie den Modus Erweiterte Verordnung (EO)

Sie können den EO-Modus (Extended Ordinance) für einen sicheren Betrieb aktivieren und deaktivieren.

Schritte

1. Wählen Sie **Start**, geben Sie "regedit" in das Suchfeld ein, und wählen Sie dann aus `regedit.exe` In der

Liste Programme.

2. Suchen Sie in **Registrierungs-Editor** den folgenden Unterschlüssel für den ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Erstellen Sie im rechten Fensterbereich einen neuen Registrierungswert vom Typ "DWORD" mit dem Namen "EO_Mode" (ohne Anführungszeichen) und dem Wert "1" (ohne Anführungszeichen), um den EO-Modus zu aktivieren oder den Wert "0" (ohne Anführungszeichen), um den EO-Modus zu deaktivieren.

> Standardmäßig, wenn die `EO_Mode` Registrierungseintrag fehlt, EO-Modus ist deaktiviert. Wenn Sie den EO-Modus aktivieren, müssen Sie sowohl den externen Syslog-Server als auch die gegenseitige Zertifikatauthentifizierung konfigurieren.

Konfigurieren Sie den externen Syslog-Server

Bevor Sie beginnen

Beachten Sie, dass Sie beim Erstellen von Registrierungswerten in diesem Verfahren den rechten Fensterbereich verwenden.

Schritte

1. Wählen Sie **Start**, geben Sie "regedit" in das Suchfeld ein, und wählen Sie dann aus `regedit.exe` In der Liste Programme.
2. Erstellen Sie in **Registrierungs-Editor** den folgenden Unterschlüssel für den ONTAP Antivirus Connector für die Syslog-Konfiguration: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Erstellen Sie einen Registrierungswert, indem Sie den Typ, den Namen und den Wert wie in der folgenden Tabelle dargestellt angeben:

Typ	Name	Wert
DWORD	Syslog_aktiviert	1 oder 0

   Bitte beachten Sie, dass ein Wert „1“ das Syslog aktiviert und mit einem Wert „0“ deaktiviert.

4. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name
REG_SZ	Syslog_Host

   Geben Sie die IP-Adresse oder den Domänennamen des Syslog-Hosts für das Wertfeld an.

5. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name
REG_SZ	Syslog_Port

Geben Sie im Feld Wert die Portnummer an, auf der der Syslog-Server ausgeführt wird.

6. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name
REG_SZ	Syslog_Protocol

Geben Sie das Protokoll, das auf dem Syslog-Server verwendet wird, entweder „tcp“ oder „udp“ in das Wertfeld ein.

7. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_Level	2	5	6	7

8. Erstellen Sie einen anderen Registrierungswert, indem Sie die in der folgenden Tabelle aufgeführten Informationen bereitstellen:

Typ	Name	Wert
DWORD	Syslog_tls	1 oder 0

Bitte beachten Sie, dass ein Wert von „1“ Syslog mit Transport Layer Security (TLS) aktiviert und ein Wert von „0“ das Syslog mit TLS deaktiviert.

Stellen Sie sicher, dass ein konfigurierter externer Syslog-Server reibungslos ausgeführt wird

- Wenn der Schlüssel fehlt oder einen Nullwert hat:
  - Das Protokoll ist standardmäßig auf „tcp“ eingestellt.
  - Der Port ist standardmäßig auf "514" für einfaches "tcp/udp" und standardmäßig auf "6514" für TLS.
  - Die Syslog-Ebene ist standardmäßig auf 5 (LOG_NOTICE) eingestellt.
- Sie können bestätigen, dass Syslog aktiviert ist, indem Sie überprüfen, ob das aktiviert ist `syslog_enabled` Wert ist „1“. Wenn der `syslog_enabled` Der Wert ist „1“, Sie sollten sich beim konfigurierten Remote-Server anmelden können, unabhängig davon, ob der EO-Modus aktiviert ist.
- Wenn der EO-Modus auf „1“ eingestellt ist und Sie den ändern `syslog_enabled` Wert von „1“ bis „0“, gilt:
  - Sie können den Service nicht starten, wenn syslog im EO-Modus nicht aktiviert ist.
  - Wenn das System in einem stabilen Zustand ausgeführt wird, erscheint eine Warnung, die besagt, dass Syslog im EO-Modus nicht deaktiviert werden kann und syslog zwangsweise auf „1“ gesetzt ist, was Sie in der Registrierung sehen können. In diesem Fall sollten Sie zuerst den EO-Modus deaktivieren und dann syslog deaktivieren.
- Wenn der Syslog-Server bei Aktivierung von EO-Modus und Syslog nicht erfolgreich ausgeführt werden kann, wird der Dienst nicht mehr ausgeführt. Dies kann aus einem der folgenden Gründe auftreten:
  - Ein ungültiger oder kein syslog_Host ist konfiguriert.

    - Ein ungültiges Protokoll außer UDP oder TCP ist konfiguriert.
    - Eine Portnummer ist ungültig.
- Bei einer TCP- oder TLS-über-TCP-Konfiguration schlägt die Verbindung fehl, wenn der Server den IP-Port nicht abhört, und der Dienst wird heruntergefahren.

Konfigurieren Sie die Authentifizierung des gegenseitigen X.509-Zertifikats

X.509-zertifikatbasierte gegenseitige Authentifizierung ist für die SSL-Kommunikation (Secure Sockets Layer) zwischen dem Antivirus Connector und ONTAP im Verwaltungspfad möglich. Wenn der EO-Modus aktiviert ist und das Zertifikat nicht gefunden wird, wird der AV-Connector beendet. Führen Sie die folgenden Schritte auf dem Antivirus Connector durch:

Schritte

1. Der Antivirus Connector sucht nach dem Clientzertifikat des Virenschutzanschlusses und dem Zertifikat der Zertifizierungsstelle (CA) für den NetApp-Server im Verzeichnispfad, von dem aus der Virenschutzanschlussanschluss das Installationsverzeichnis ausführt. Kopieren Sie die Zertifikate in diesen festen Verzeichnispfad.
2. Betten Sie das Clientzertifikat und seinen privaten Schlüssel in das PKCS12-Format ein und benennen Sie es mit „AV_Client.P12“.
3. Stellen Sie sicher, dass das zum Signieren des Zertifikats für den NetApp-Server verwendete Zertifizierungsstellenzertifikat (zusammen mit jeder Zwischenzertifizierungsstelle bis zur Stammzertifizierungsstelle) im PEM-Format (Privacy Enhanced Mail) mit dem Namen „ONTAP_CA.pem“ vorliegt. Platzieren Sie es im Installationsverzeichnis des Antivirus Connectors. Installieren Sie auf dem NetApp ONTAP-System das CA-Zertifikat (zusammen mit einer Zwischenzertifikationsberechtigung bis zur Stammzertifizierungsstelle), mit dem das Clientzertifikat für den Antivirus-Connector unter „ONTAP“ als Zertifikat vom Typ „Client-CA“ signiert wird.

Konfigurieren von Scannerpools

Konfigurieren Sie die Übersicht über Scannerpools

Ein Scanner-Pool definiert die Vscan-Server und privilegierten Benutzer, die eine Verbindung zu SVMs herstellen können. Eine Scannerrichtlinie bestimmt, ob ein Scannerpool aktiv ist.

> Wenn Sie eine Exportrichtlinie auf einem SMB-Server verwenden, müssen Sie jeden Vscan-Server zur Exportrichtlinie hinzufügen.

Erstellen Sie einen Scanner-Pool auf einem einzelnen Cluster

Ein Scanner-Pool definiert die Vscan-Server und privilegierten Benutzer, die eine Verbindung zu SVMs herstellen können. Sie können einen Scanner-Pool für eine einzelne SVM oder für alle SVMs eines Clusters erstellen.

Was Sie benötigen

- SVMs und Vscan-Server müssen sich in derselben Domäne oder in vertrauenswürdigen Domänen befinden.
- Für Scanner-Pools, die für eine einzelne SVM definiert sind, müssen Sie den ONTAP Antivirus Connector mit der logischen Schnittstelle für das SVM-Management oder SVM-Daten konfiguriert haben.

- Für Scanner-Pools, die für alle SVMs in einem Cluster definiert sind, müssen Sie den ONTAP Antivirus Connector mit der Cluster-Management-LIF konfiguriert haben.
- Die Liste der privilegierten Benutzer muss das Domain-Benutzerkonto enthalten, das der Vscan-Server zur Verbindung mit der SVM verwendet.
- Sobald der Scanner-Pool konfiguriert ist, überprüfen Sie den Verbindungsstatus zu den Servern.

Schritte

1. Erstellen eines Scannerpools:

   `vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users`

   - Legen Sie eine Daten-SVM für einen Pool fest, der für eine einzelne SVM definiert ist, und geben Sie eine Cluster-Admin-SVM für einen Pool an, der für alle SVMs in einem Cluster definiert ist.
   - Geben Sie für jeden Host-Namen des Vscan-Servers eine IP-Adresse oder einen FQDN an.
   - Geben Sie die Domäne und den Benutzernamen für jeden privilegierten Benutzer an. Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

     Mit dem folgenden Befehl wird ein Scannerpool mit dem Namen erstellt `SP` Auf dem `vs1` SVM:

   ```
   cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
   SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
   cifs\u1,cifs\u2
   ```

2. Überprüfen Sie, ob der Scannerpool erstellt wurde:

   `vserver vscan scanner-pool show -vserver *data_SVM|cluster_admin_SVM* -scanner -pool *scanner_pool*`

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die Details für das angezeigt `SP` Scanner-Pool:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

Sie können auch die verwenden `vserver vscan scanner-pool show` Befehl zum Anzeigen aller Scannerpools auf einer SVM. Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

Erstellen von Scannerpools in MetroCluster-Konfigurationen

Sie müssen primäre und sekundäre Scannerpools auf jedem Cluster einer MetroCluster Konfiguration erstellen, die den primären und sekundären SVMs im Cluster entsprechen.

Was Sie benötigen

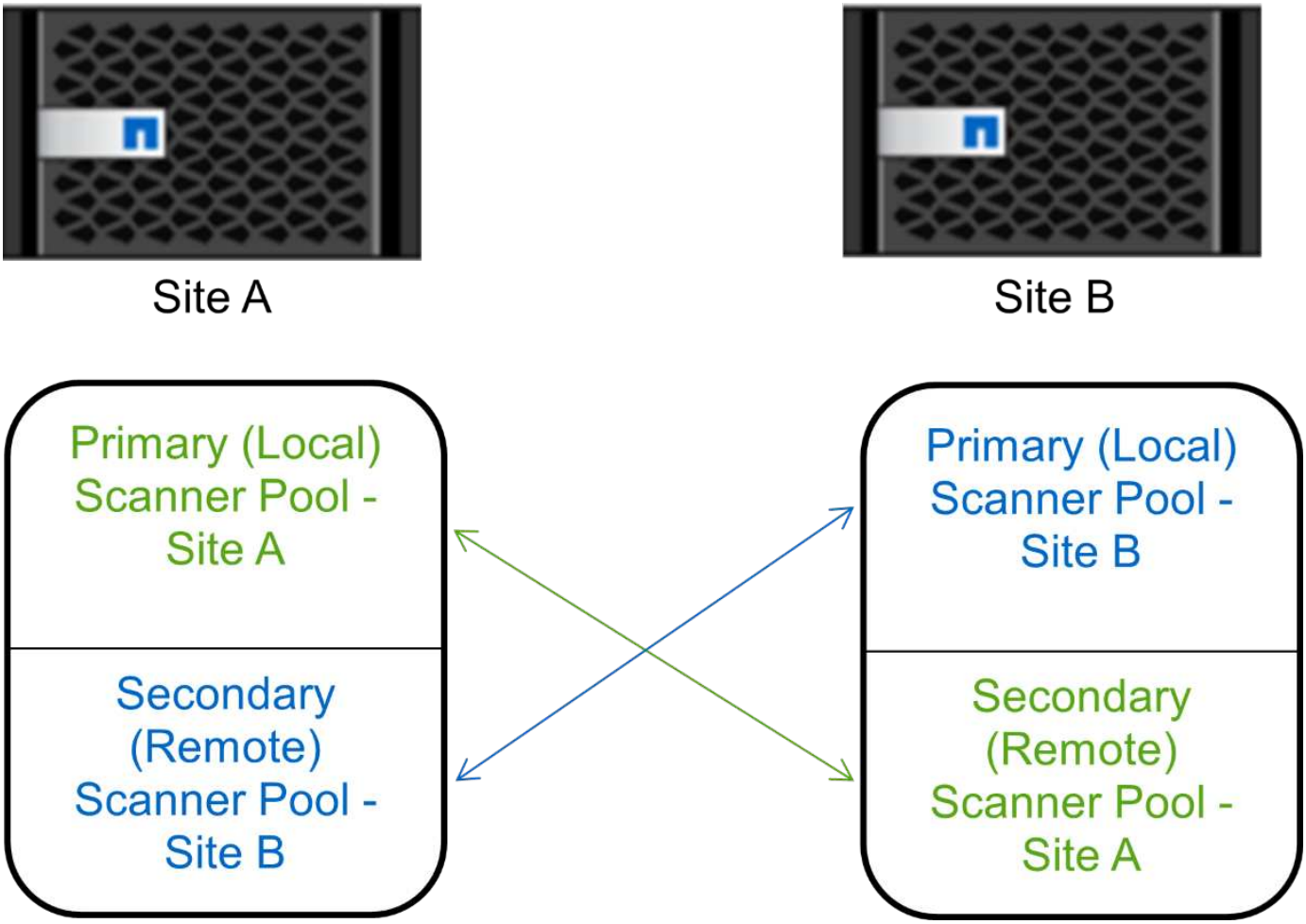
- SVMs und Vscan-Server müssen sich in derselben Domäne oder in vertrauenswürdigen Domänen befinden.
- Für Scanner-Pools, die für eine einzelne SVM definiert sind, müssen Sie den ONTAP Antivirus Connector mit der logischen Schnittstelle für das SVM-Management oder SVM-Daten konfiguriert haben.
- Für Scanner-Pools, die für alle SVMs in einem Cluster definiert sind, müssen Sie den ONTAP Antivirus Connector mit der Cluster-Management-LIF konfiguriert haben.
- Die Liste der privilegierten Benutzer muss das Domain-Benutzerkonto enthalten, das der Vscan-Server zur Verbindung mit der SVM verwendet.
- Sobald der Scanner-Pool konfiguriert ist, überprüfen Sie den Verbindungsstatus zu den Servern.

Über diese Aufgabe

MetroCluster Konfigurationen sichern Daten, indem zwei physisch getrennte gespiegelte Cluster implementiert werden. Jedes Cluster repliziert die Daten synchron zur SVM-Konfiguration des anderen. Eine primäre SVM auf dem lokalen Cluster stellt Daten bereit, wenn das Cluster online ist. Eine sekundäre SVM auf dem lokalen Cluster stellt Daten bereit, wenn das Remote-Cluster offline ist.

Das heißt, Sie müssen auf jedem Cluster in einer MetroCluster-Konfiguration primäre und sekundäre Scanner-Pools erstellen. Der sekundäre Pool wird dann aktiv, wenn das Cluster damit beginnt, Daten von der sekundären SVM bereitzustellen. Für Disaster Recovery (DR) ist die Konfiguration ähnlich wie MetroCluster.

Diese Abbildung zeigt eine typische MetroCluster/DR-Konfiguration.



Schritte

1. Erstellen eines Scannerpools:

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - Legen Sie eine Daten-SVM für einen Pool fest, der für eine einzelne SVM definiert ist, und geben Sie eine Cluster-Admin-SVM für einen Pool an, der für alle SVMs in einem Cluster definiert ist.
   - Geben Sie für jeden Host-Namen des Vscan-Servers eine IP-Adresse oder einen FQDN an.
   - Geben Sie die Domäne und den Benutzernamen für jeden privilegierten Benutzer an.

     Sie müssen alle Scannerpools aus dem Cluster erstellen, das die primäre SVM enthält.

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit den folgenden Befehlen werden primäre und sekundäre Scannerpools auf jedem Cluster in einer MetroCluster-Konfiguration erstellt:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Überprüfen Sie, ob die Scannerpools erstellt wurden:

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die Details für den Scannerpool angezeigt `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                   Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: idle
                            Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   Sie können auch die verwenden `vserver vscan scanner-pool show` Befehl zum Anzeigen aller Scannerpools auf einer SVM. Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

Wenden Sie eine Scannerrichtlinie auf einem einzelnen Cluster an

Eine Scannerrichtlinie bestimmt, ob ein Scannerpool aktiv ist. Sie müssen einen Scanner-Pool aktivieren, bevor die von ihm definierten Vscan-Server eine Verbindung zu einer

SVM herstellen können.

Über diese Aufgabe

- Sie können nur eine Scannerrichtlinie auf einen Scannerpool anwenden.
- Wenn Sie einen Scanner-Pool für alle SVMs eines Clusters erstellt haben, müssen Sie für jede SVM einzeln eine Scannerrichtlinie anwenden.

Schritte

1. Anwendung einer Scannerrichtlinie:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Eine Scannerrichtlinie kann einen der folgenden Werte aufweisen:

   - `Primary` Gibt an, dass der Scannerpool aktiv ist.
   - `Secondary` Gibt an, dass der Scannerpool nur aktiv ist, wenn keiner der Vscan-Server im primären Scannerpool angeschlossen ist.
   - `Idle` Gibt an, dass der Scannerpool inaktiv ist.

     Das folgende Beispiel zeigt, dass der Scanner-Pool mit dem Namen `SP` Auf dem `vs1` SVM ist aktiv:

   ```
   cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
   -scanner-pool SP  -scanner-policy primary
   ```

2. Vergewissern Sie sich, dass der Scanner-Pool aktiv ist:

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die Details für das angezeigt `SP` Scanner-Pool:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                              Scanner Pool: SP
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

Sie können das verwenden `vserver vscan scanner-pool show-active` Befehl zum Anzeigen der aktiven Scannerpools auf einer SVM. Die vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

Wenden Sie die Scannerrichtlinien in MetroCluster-Konfigurationen an

Eine Scannerrichtlinie bestimmt, ob ein Scannerpool aktiv ist. Sie müssen eine Scannerrichtlinie auf die primären und sekundären Scannerpools in jedem Cluster einer MetroCluster-Konfiguration anwenden.

Über diese Aufgabe

- Sie können nur eine Scannerrichtlinie auf einen Scannerpool anwenden.
- Wenn Sie einen Scanner-Pool für alle SVMs eines Clusters erstellt haben, müssen Sie für jede SVM einzeln eine Scannerrichtlinie anwenden.
- Für Disaster Recovery- und MetroCluster-Konfigurationen müssen Sie eine Scannerrichtlinie auf jeden Scanner-Pool im lokalen Cluster und Remote-Cluster anwenden.
- In der Richtlinie, die Sie für das lokale Cluster erstellen, müssen Sie das lokale Cluster in angeben `cluster` Parameter. In der Richtlinie, die Sie für den Remote-Cluster erstellen, müssen Sie den Remote-Cluster in angeben `cluster` Parameter. Der Remote-Cluster kann dann im Katastrophenfall Virenscans übernehmen.

Schritte

1. Anwendung einer Scannerrichtlinie:

   `vserver vscan scanner-pool apply-policy -vserver` *`data_SVM`* `-scanner-pool` *`scanner_pool`* `-scanner-policy primary|secondary|idle -cluster` *`cluster_to_apply_policy_on`*

   Eine Scannerrichtlinie kann einen der folgenden Werte aufweisen:

   - `Primary` Gibt an, dass der Scannerpool aktiv ist.
   - `Secondary` Gibt an, dass der Scannerpool nur aktiv ist, wenn keiner der Vscan-Server im primären Scannerpool angeschlossen ist.

- `Idle` Gibt an, dass der Scannerpool inaktiv ist.

> Sie müssen alle Scannerrichtlinien auf dem Cluster anwenden, das die primäre SVM enthält.

Mit den folgenden Befehlen werden die Scannerrichtlinien auf die primären und sekundären Scannerpools in jedem Cluster in einer MetroCluster-Konfiguration angewendet:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Vergewissern Sie sich, dass der Scanner-Pool aktiv ist:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die Details für den Scannerpool angezeigt `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: primary
                            Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   Sie können das verwenden `vserver vscan scanner-pool show-active` Befehl zum Anzeigen der aktiven Scannerpools auf einer SVM. Eine vollständige Befehlssyntax finden Sie in der man-Page für den

Befehl.

Befehle zum Verwalten von Scannerpools

Sie können Scannerpools ändern und löschen und privilegierte Benutzer und Vscan-Server für einen Scannerpool verwalten. Sie können auch zusammenfassende Informationen zum Scanner-Pool anzeigen.

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Ändern eines Scannerpools	`vserver vscan scanner-pool modify`
Löschen eines Scannerpools	`vserver vscan scanner-pool delete`
Fügen Sie privilegierte Benutzer zu einem Scanner-Pool hinzu	`vserver vscan scanner-pool privileged-users add`
Löschen Sie privilegierte Benutzer aus einem Scannerpool	`vserver vscan scanner-pool privileged-users remove`
Fügen Sie Vscan-Server einem Scanner-Pool hinzu	`vserver vscan scanner-pool servers add`
Löschen Sie Vscan-Server aus einem Scannerpool	`vserver vscan scanner-pool servers remove`
Zeigen Sie die Zusammenfassung und Details für einen Scannerpool an	`vserver vscan scanner-pool show`
Zeigen Sie privilegierte Benutzer für einen Scannerpool an	`vserver vscan scanner-pool privileged-users show`
Zeigen Sie Vscan-Server für alle Scannerpools an	`vserver vscan scanner-pool servers show`

Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages.

Konfigurieren Sie das Scannen beim Zugriff

Erstellen einer Zugriffsrichtlinie

Eine Zugriffsrichtlinie definiert den Umfang eines Scans beim Zugriff. Sie können eine On-Access-Richtlinie für eine einzelne SVM oder für alle SVMs in einem Cluster erstellen. Falls Sie eine Zugriffsrichtlinie für alle SVMs in einem Cluster erstellt haben, müssen Sie die Richtlinie für jede SVM einzeln aktivieren.

Über diese Aufgabe

- Sie können die maximale Dateigröße für den Scan, Dateierweiterungen und Pfade für den Scan sowie

Dateierweiterungen und -Pfade für den Scan angeben.

- Sie können die einstellen `scan-mandatory` Option „aus“, um festzulegen, dass der Dateizugriff zulässig ist, wenn keine Vscan-Server für Virenprüfungen verfügbar sind.
- Standardmäßig erstellt ONTAP eine Zugriffsrichtlinie mit dem Namen „Default_CIFS“ und ermöglicht sie für alle SVMs in einem Cluster.
- Jede Datei, die auf der Grundlage des für den Scanausschluss qualifiziert ist `paths-to-exclude`, `file-ext-to-exclude`, Oder `max-file-size` Parameter werden für das Scannen nicht berücksichtigt, auch wenn der `scan-mandatory` Die Option ist auf ein eingestellt. (Prüfen Sie dies "Fehlerbehebung" Abschnitt für Konnektivitätsprobleme im Zusammenhang mit `scan-mandatory` Option.)
- Standardmäßig werden nur Lese- und Schreib-Volumes gescannt. Sie können Filter festlegen, die das Scannen von schreibgeschützten Volumes ermöglichen oder das Scannen auf Dateien beschränken, die mit dem Zugriff ausführen geöffnet wurden.
- Ein Virus-Scan wird nicht auf einer SMB-Freigabe durchgeführt, für die der kontinuierlich verfügbare Parameter auf Ja gesetzt ist.
- Siehe "Virenschutz-Architektur" Abschnitt für Details zum *Vscan file-Operations Profil*.
- Sie können maximal zehn (10) Zugriffsrichtlinien pro SVM erstellen. Sie können jedoch jeweils nur eine Richtlinie für den Zugriff aktivieren.
  - Sie können in einer Richtlinie für den Zugriff maximal hundert (100) Pfade und Dateierweiterungen von der Virenüberprüfung ausschließen.
- Einige Empfehlungen zum Dateiausschluss:
  - Ziehen Sie es in Erwägung, große Dateien (Dateigröße kann angegeben werden) von Virus-Scans auszuschließen, da sie zu einer langsamen Antwortzeit oder Scan-Anfrage-Timeouts für CIFS-Benutzer führen können. Die Standarddateigröße für Ausschluss beträgt 2 GB.
  - Es empfiehlt sich, Dateierweiterungen wie z. B. auszuschließen `.vhd` Und `.tmp` Weil Dateien mit diesen Erweiterungen möglicherweise nicht zum Scannen geeignet sind.
  - Es empfiehlt sich, Dateipfade wie das Quarantäneverzeichnis oder Pfade auszuschließen, in denen nur virtuelle Festplatten oder Datenbanken gespeichert sind.
  - Vergewissern Sie sich, dass alle Ausschlüsse in derselben Richtlinie angegeben sind, da jeweils nur eine Richtlinie aktiviert werden kann. NetApp empfiehlt dringend, die gleichen Ausschlüsse zu verwenden, die in der Antiviren-Engine angegeben sind.
- Für einen ist eine Zugangsrichtlinie erforderlich On-Demand-Scan. Um das Scannen beim Zugriff auf zu vermeiden, sollten Sie die Einstellung festlegen `-scan-files-with-no-ext` Zu false und `-file-ext-to-exclude` Um * auszuschließen, um alle Nebenstellen auszuschließen.

Schritte

1. Erstellen einer Richtlinie für den Zugriff:

   ```
   vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
   -policy-name policy_name -protocol CIFS -max-file-size
   max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
   -file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
   extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
   -exclude paths_of_files_to_exclude -scan-mandatory on|off
   ```

   - Legen Sie eine Daten-SVM für eine Richtlinie fest, die für eine einzelne SVM, einen Cluster-Admin-SVM für eine Richtlinie festgelegt ist, die für alle SVMs in einem Cluster definiert ist.

- Der `-file-ext-to-exclude` Die Einstellung überschreibt den `-file-ext-to-include` Einstellung.
- Einstellen `-scan-files-with-no-ext` Um Dateien ohne Erweiterungen zu scannen.
  Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen für den Zugriff erstellt `Policy1` Auf dem `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include “mp*”,"tx*" -file-ext-to-exclude "mp3","txt" -scan
-files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
```

2. Überprüfen Sie, ob die Richtlinie für den Zugriff auf den Zugriff erstellt wurde: `vserver vscan on-access-policy show -instance` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`name`*

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die Details für das angezeigt `Policy1` Richtlinie:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Aktivieren einer Zugriffsrichtlinie

Eine Zugriffsrichtlinie definiert den Umfang eines Scans beim Zugriff. Sie müssen eine Zugriffsrichtlinie auf einer SVM aktivieren, bevor deren Dateien gescannt werden können.

Falls Sie eine Zugriffsrichtlinie für alle SVMs in einem Cluster erstellt haben, müssen Sie die Richtlinie für jede SVM einzeln aktivieren. Sie können jeweils nur eine Zugriffsrichtlinie für eine SVM aktivieren.

Schritte

1. Aktivieren einer Zugriffsrichtlinie:

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name
```

`policy_name`

Mit dem folgenden Befehl wird eine Richtlinie für den Zugriff mit dem Namen aktiviert `Policy1` Auf dem `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. Vergewissern Sie sich, dass die Zugriffsrichtlinie aktiviert ist:

   `vserver vscan on-access-policy show -instance` *`data_SVM`* `-policy-name` *`policy_name`*

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die Details für das angezeigt `Policy1` Richtlinie für den Zugriff:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: on
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Ändern Sie das Vscan-Dateibetriebsprofil für eine SMB-Freigabe

Das Profil *Vscan file-Operations* für eine SMB-Freigabe definiert die Vorgänge auf der Freigabe, die einen Scan auslösen können. Standardmäßig ist der Parameter auf festgelegt `standard`. Sie können den Parameter beim Erstellen oder Ändern einer SMB-Freigabe nach Bedarf anpassen.

Siehe "Virenschutz-Architektur" Abschnitt für Details zum *Vscan file-Operations Profil*.

> Der Virus-Scan wird nicht auf einer SMB-Freigabe durchgeführt, die über den verfügt `continuously-available` Parameter auf gesetzt `Yes`.

Schritt

1. Ändern Sie den Wert des Vscan-Dateioperationsprofils für eine SMB-Freigabe:

   `vserver cifs share modify -vserver` *`data_SVM`* `-share-name` *`share`* `-path` *`share_path`* `-vscan-fileop-profile no-scan|standard|strict|writes-only`

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl wird das Profil der Vscan-Dateivorgänge für eine SMB-Freigabe in geändert `strict`:

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

Befehle zum Managen von Zugriffsrichtlinien

Sie können eine Richtlinie für den Zugriff ändern, deaktivieren oder löschen. Sie können sich eine Zusammenfassung und Details der Richtlinie anzeigen lassen.

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Erstellen einer Zugriffsrichtlinie	`vserver vscan on-access-policy create`
Ändern Sie eine Zugriffsrichtlinie	`vserver vscan on-access-policy modify`
Aktivieren einer Zugriffsrichtlinie	`vserver vscan on-access-policy enable`
Deaktivieren einer Zugriffsrichtlinie	`vserver vscan on-access-policy disable`
Löschen Sie eine Zugriffsrichtlinie	`vserver vscan on-access-policy delete`
Zusammenfassung und Details zu einer Zugriffsrichtlinie anzeigen	`vserver vscan on-access-policy show`
Fügen Sie zur Liste der auszuschließenden Pfade hinzu	`vserver vscan on-access-policy paths-to-exclude add`
Löschen Sie die Liste der auszuschließenden Pfade	`vserver vscan on-access-policy paths-to-exclude remove`
Zeigen Sie die Liste der auszuschließenden Pfade an	`vserver vscan on-access-policy paths-to-exclude show`
Fügen Sie zur Liste der auszuschließenden Dateierweiterungen hinzu	`vserver vscan on-access-policy file-ext-to-exclude add`

Löschen Sie aus der Liste der auszuschließenden Dateierweiterungen	`vserver vscan on-access-policy file-ext-to-exclude remove`
Zeigen Sie die Liste der auszuschließenden Dateierweiterungen an	`vserver vscan on-access-policy file-ext-to-exclude show`
Fügen Sie zur Liste der einzuschließen von Dateierweiterungen hinzu	`vserver vscan on-access-policy file-ext-to-include add`
Löschen Sie aus der Liste der einzuschließen Dateiendungen	`vserver vscan on-access-policy file-ext-to-include remove`
Die Liste der einzuschließen von Dateierweiterungen anzeigen	`vserver vscan on-access-policy file-ext-to-include show`

Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages.

Konfigurieren Sie das Scannen nach Bedarf

Konfigurieren Sie die Übersicht über das Scannen nach Bedarf

Mithilfe des On-Demand-Scans können Sie Dateien sofort oder nach einem Zeitplan auf Viren überprüfen.

Möglicherweise möchten Sie Scans beispielsweise außerhalb der Stoßzeiten durchführen oder sehr große Dateien scannen, die von einem Scan beim Zugriff ausgeschlossen wurden. Sie können einen Cron-Zeitplan verwenden, um anzugeben, wann die Aufgabe ausgeführt wird.

Zu diesem Thema behandelt wird

- Sie können beim Erstellen einer Aufgabe einen Zeitplan zuweisen.
- Es kann jeweils nur eine Aufgabe gleichzeitig für eine SVM geplant werden.
- Das Scannen nach Bedarf unterstützt keine Suche nach symbolischen Links oder Stream-Dateien.

> Das Scannen nach Bedarf unterstützt keine Suche nach symbolischen Links oder Stream-Dateien.

> Um eine On-Demand-Aufgabe zu erstellen, muss mindestens eine On-Access-Richtlinie aktiviert sein. Dabei kann es sich um eine Standardrichtlinie oder eine beim Zugriff erstellte Richtlinie handeln.

Erstellen Sie eine On-Demand-Aufgabe

Eine On-Demand-Aufgabe definiert den Umfang des On-Demand-Virus-Scans. Sie können die maximale Größe der zu scannenden Dateien, die Erweiterungen und Pfade der Dateien angeben, die in den Scan aufgenommen werden sollen, sowie die Erweiterungen und Pfade der Dateien, die vom Scan ausgeschlossen werden sollen.

Dateien in Unterverzeichnissen werden standardmäßig gescannt.

Über diese Aufgabe

- Für jede SVM können maximal zehn (10) On-Demand-Aufgaben vorhanden sein, aber nur eine kann aktiv sein.
- Eine On-Demand-Aufgabe erstellt einen Bericht, der Informationen zu den Statistiken zu den Scans enthält. Auf diesen Bericht kann mit einem Befehl oder durch Herunterladen der Berichtsdatei zugegriffen werden, die von der Aufgabe an dem definierten Speicherort erstellt wurde.

Bevor Sie beginnen

- Dieser muss unbedingt vorhanden sein Richtlinie beim Zugriff erstellt. Dabei kann es sich um eine Standard- oder eine vom Benutzer erstellte Richtlinie handeln. Ohne die Richtlinie für den Zugriff können Sie den Scan nicht aktivieren.

Schritte

1. On-Demand-Aufgabe erstellen:

   `vserver vscan on-demand-task create -vserver` *`data_SVM`* `-task-name` *`task_name`* `-scan-paths` *`paths_of_files_to_scan`* `-report-directory` *`report_directory_path`* `-report-expiry-time` *`expiration_time_for_report`* `-schedule cron_schedule -max -file-size` *`max_size_of_files_to_scan`* `-paths-to-exclude` *`paths`* `-file-ext-to -exclude` *`file_extensions`* `-file-ext-to-include` *`file_extensions`* `-scan-files-with -no-ext true|false -directory-recursion true|false`

   - Der `-file-ext-to-exclude` Die Einstellung überschreibt den `-file-ext-to-include` Einstellung.
   - Einstellen `-scan-files-with-no-ext` Um Dateien ohne Erweiterungen zu scannen.

     Eine vollständige Liste der Optionen finden Sie im "Befehlsreferenz".

     Mit dem folgenden Befehl wird eine On-Demand-Aufgabe mit dem Namen erstellt `Task1` Auf der `vs1`SVM:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

   +

   > Sie können das verwenden `job show` Befehl zum Anzeigen des Status des Jobs. Sie können das verwenden `job pause` Und `job resume` Befehle zum Anhalten und Neustarten des Jobs oder `job stop` Befehl zum Beenden des Jobs.

2. Überprüfen Sie, ob die Aufgabe On-Demand erstellt wurde:

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

Mit dem folgenden Befehl werden die Details für das angezeigt `Task1` Aufgabe:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                           Vserver: vs1
                         Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

Nachdem Sie fertig sind

Sie müssen den Scan auf der SVM aktivieren, bevor die Aufgabe geplant werden soll.

On-Demand-Aufgabe planen

Sie können eine Aufgabe erstellen, ohne einen Zeitplan zuzuweisen, und die verwenden `vserver vscan on-demand-task schedule` Befehl zum Zuweisen eines Zeitplans oder Hinzufügen eines Zeitplans beim Erstellen der Aufgabe.

Über diese Aufgabe

Der mit dem zugewiesene Zeitplan `vserver vscan on-demand-task schedule` Der Befehl überschreibt einen Zeitplan, der bereits dem zugewiesen ist `vserver vscan on-demand-task create` Befehl.

Schritte

1. Planung einer On-Demand-Aufgabe:

   ```
   vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name
   -schedule cron_schedule
   ```

   Der folgende Befehl plant eine Aufgabe mit dem Namen „On Access“ `Task2` Auf dem `vs2` SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

Um den Status des Jobs anzuzeigen, verwenden Sie die `job show` Befehl. Der `job pause` Und `job resume` Befehle bzw. den Job anhalten und neu starten; der `job stop` Befehl beendet den Job.

2. Vergewissern Sie sich, dass die On-Demand-Aufgabe geplant ist:

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die Details für das angezeigt `Task 2` Aufgabe:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                           Vserver: vs2
                         Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                  Report Log Level: info
```

Nachdem Sie fertig sind

Sie müssen den Scan auf der SVM aktivieren, bevor die Aufgabe geplant werden soll.

Führen Sie eine On-Demand-Aufgabe sofort aus

Sie können eine On-Demand-Aufgabe sofort ausführen, unabhängig davon, ob Sie einen Zeitplan zugewiesen haben.

Bevor Sie beginnen

Sie müssen das Scannen auf der SVM aktiviert haben.

Schritt

1. Führen Sie eine On-Demand-Aufgabe sofort aus:

   `vserver vscan on-demand-task run -vserver` *`data_SVM`* `-task-name` *`task_name`*

   Mit dem folgenden Befehl wird eine Aufgabe mit dem Namen für den Zugriff ausgeführt `Task1` Auf dem `vs1` SVM:

   ```
   cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
   Task1
   [Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
   command to view the status.
   ```

   Sie können das verwenden `job show` Befehl zum Anzeigen des Status des Jobs. Sie können das verwenden `job pause` Und `job resume` Befehle zum Anhalten und Neustarten des Jobs oder `job stop` Befehl zum Beenden des Jobs.

Befehle für das Managen von On-Demand-Aufgaben

Sie können eine On-Demand-Aufgabe ändern, löschen oder aufheben. Sie können eine Zusammenfassung und Details für die Aufgabe anzeigen und Berichte für die Aufgabe verwalten.

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Erstellen Sie eine On-Demand-Aufgabe	`vserver vscan on-demand-task create`
Ändern Sie eine Aufgabe nach Bedarf	`vserver vscan on-demand-task modify`
Löschen Sie eine On-Demand-Aufgabe	`vserver vscan on-demand-task delete`
Führen Sie eine On-Demand-Aufgabe aus	`vserver vscan on-demand-task run`
On-Demand-Aufgabe planen	`vserver vscan on-demand-task schedule`
Aufheben der Planung einer On-Demand-Aufgabe	`vserver vscan on-demand-task unschedule`
Zusammenfassung und Details für eine On-Demand-Aufgabe anzeigen	`vserver vscan on-demand-task show`
On-Demand-Berichte anzeigen	`vserver vscan on-demand-task report show`

On-Demand-Berichte löschen	`vserver vscan on-demand-task report delete`

Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages.

Best Practices zur Konfiguration der Off-Box-Antivirus-Funktion in ONTAP

Beachten Sie die folgenden Empfehlungen zur Konfiguration der Off-Box-Funktion in ONTAP.

- Beschränken Sie privilegierte Benutzer auf Virenprüfungen. Normale Benutzer sollten von der Verwendung privilegierter Benutzeranmeldeinformationen abschrecken. Diese Einschränkung kann erreicht werden, indem die Anmelderechte für privilegierte Benutzer in Active Directory deaktiviert werden.
- Privilegierte Benutzer müssen nicht Teil einer Benutzergruppe sein, die über eine große Anzahl von Rechten in der Domäne verfügt, z. B. der Administratorengruppe oder der Gruppe der Backup-Operatoren. Privilegierte Benutzer dürfen nur durch das Storage-System validiert werden, damit sie Vscan-Serververbindungen herstellen und auf Dateien für Virenprüfungen zugreifen können.
- Verwenden Sie die Computer, auf denen Vscan-Server ausgeführt werden, nur für Virenscans. Um die allgemeine Nutzung zu verhindern, deaktivieren Sie die Windows-Terminaldienste und andere Remote-Zugriffsbestimmungen auf diesen Computern und gewähren das Recht, neue Software nur Administratoren auf diesen Computern zu installieren.
- Widmen Sie die Vscan-Server Virenprüfungen und verwenden Sie sie nicht für andere Vorgänge, z. B. Backups. Sie können den Vscan-Server als virtuelle Maschine (VM) ausführen. Wenn Sie den Vscan-Server als VM ausführen, stellen Sie sicher, dass die der VM zugewiesenen Ressourcen nicht gemeinsam genutzt werden und zum Durchführen eines Virus-Scans ausreichen.
- Bereitstellen einer ausreichenden CPU-, Arbeitsspeicher- und Festplattenkapazität für den Vscan-Server, um eine übermäßige Zuweisung von Ressourcen zu vermeiden. Die meisten Vscan-Server sind für die Verwendung mehrerer CPU-Core-Server und die Verteilung der Last über die CPUs konzipiert.
- NetApp empfiehlt für die Verbindung von SVM zu dem Vscan-Server die Verwendung eines dedizierten Netzwerks mit einem privaten VLAN, damit der Scan-Verkehr nicht durch anderen Client-Netzwerk-Traffic beeinträchtigt wird. Erstellen Sie eine separate Netzwerkkarte (NIC), die speziell für das Virenschutz-VLAN auf dem Vscan-Server und die logische Datenschnittstelle auf der SVM eingerichtet ist. Dieser Schritt vereinfacht die Administration und die Fehlerbehebung bei Netzwerkproblemen. Der Antivirus-Verkehr sollte über ein privates Netzwerk getrennt werden. Der Virenschutz-Server sollte so konfiguriert werden, dass er mit dem Domänencontroller (DC) und ONTAP auf eine der folgenden Arten kommuniziert:
    - Das DC sollte über das private Netzwerk, das zur Trennung des Datenverkehrs verwendet wird, mit den Antivirenservern kommunizieren.
    - Der DC- und Antivirus-Server sollten über ein anderes Netzwerk (nicht das zuvor erwähnte private Netzwerk) kommunizieren, das nicht mit dem CIFS-Client-Netzwerk identisch ist.
    - Um die Kerberos-Authentifizierung für die Virenkommunikation zu aktivieren, erstellen Sie einen DNS-Eintrag für die privaten LIFs und einen Dienstprinzipalnamen auf dem DC, der dem für die private LIF erstellten DNS-Eintrag entspricht. Verwenden Sie diesen Namen, wenn Sie eine LIF zum Antivirus Connector hinzufügen. Der DNS sollte in der Lage sein, einen eindeutigen Namen für jede private LIF zurückzugeben, die mit dem Antivirus Connector verbunden ist.

Wenn die LIF für Vscan-Datenverkehr für Client-Datenverkehr auf einem anderen Port als der LIF konfiguriert ist, kann die Vscan LIF ein Failover auf einen anderen Node durchführen, wenn ein Port-Ausfall auftritt. Die Änderung bewirkt, dass der Vscan-Server vom neuen Knoten nicht erreichbar ist und die Scanbenachrichtigungen für Dateivorgänge auf dem Knoten fehlschlagen. Vergewissern Sie sich, dass der Vscan-Server über mindestens eine LIF auf einem Node erreichbar ist, damit er Scananforderungen für Dateivorgänge verarbeiten kann, die auf diesem Node ausgeführt werden.

- Verbinden Sie das NetApp Storage-System und den Vscan-Server über mindestens ein 1-GbE-Netzwerk.
- Verbinden Sie in einer Umgebung mit mehreren Vscan-Servern alle Server mit ähnlichen leistungsstarken Netzwerkverbindungen. Die Verbindung der Vscan-Server verbessert die Leistung durch die Möglichkeit der Lastverteilung.
- Für Remote-Standorte und Zweigstellen empfiehlt NetApp die Verwendung eines lokalen Vscan-Servers statt eines externen Vscan-Servers, da ersterer sich ideal für eine hohe Latenz eignet. Wenn die Kosten ein Faktor sind, verwenden Sie einen Laptop oder PC für einen moderaten Virenschutz. Sie können regelmäßige vollständige Filesystem-Scans planen, indem Sie die Volumes oder qtrees gemeinsam nutzen und von jedem System am Remote-Standort aus scannen.
- Verwenden Sie mehrere Vscan-Server, um die Daten auf der SVM für Lastverteilung und Redundanz zu scannen. Die Menge der CIFS-Workloads und der daraus resultierende Virenschutzdatenverkehr variieren je SVM. Überwachen Sie CIFS und die Latenz beim Virenscannen auf dem Storage Controller. Überwachen Sie den Trend der Ergebnisse im Laufe der Zeit. Wenn die CIFS-Latenz und die Latenz von Virenscans aufgrund von CPU- oder Anwendungswarteschlangen auf den Vscan-Servern über die Trendschwellenwerte hinaus zunimmt, kann es bei CIFS-Clients zu langen Wartezeiten kommen. Fügen Sie zusätzliche Vscan-Server hinzu
  Um die Last zu verteilen.
- Installieren Sie die neueste Version des ONTAP-Virenschutzanschlusses.
- Halten Sie Virenschutz-Engines und Definitionen auf dem neuesten Stand. Wenden Sie sich an Partner, um Empfehlungen zu erhalten, wie oft Sie Updates durchführen sollten.
- In einer mandantenfähigen Umgebung kann ein Scanner-Pool (Pool von Vscan Servern) mit mehreren SVMs genutzt werden, vorausgesetzt die Vscan Server und SVMs sind Teil derselben Domäne oder derselben vertrauenswürdigen Domäne.
- Die Virenschutzrichtlinie für infizierte Dateien sollte auf „löschen“ oder „Quarantäne“ gesetzt werden, was der von den meisten Antivirenanbietern festgelegte Standardwert ist. Wenn das "vscan-fileop-Profil" auf "write_only" gesetzt ist und eine infizierte Datei gefunden wird, bleibt die Datei in der Freigabe und kann geöffnet werden, da das Öffnen einer Datei keinen Scan auslöst. Die Virenprüfung wird erst ausgelöst, nachdem die Datei geschlossen wurde.
- Der `scan-engine timeout` Der Wert muss kleiner sein als der `scanner-pool request-timeout` Wert:
  Wenn sie auf einen höheren Wert eingestellt ist, kann der Zugriff auf Dateien verzögert werden und möglicherweise eine Zeitverzögerung erreichen.
  Um dies zu vermeiden, konfigurieren Sie das `scan-engine timeout` Bis 5 Sekunden weniger als der `scanner-pool request-timeout` Wert: Anweisungen zum Ändern des finden Sie in der Dokumentation des Scannerherstellers `scan-engine timeout` Einstellungen. Der `scanner-pool timeout` Kann mit dem folgenden Befehl im erweiterten Modus und durch Angabe des entsprechenden Werts für geändert werden `request-timeout` Parameter:
  `vserver vscan scanner-pool modify`.
- Bei einer Umgebung, die auf Scan-Workloads beim Zugriff ausgelegt ist und On-Demand-Scans erfordert, empfiehlt NetApp, den On-Demand-Scan-Job außerhalb der Spitzenzeiten zu planen, um zusätzliche Belastungen der vorhandenen Virenschutz-Infrastruktur zu vermeiden.

Weitere Informationen zu Best Practices für Partner finden Sie unter "Partnerlösungen von Vscan".

Aktivieren Sie das Virensuchen auf einer SVM

Sie müssen den Virenscan auf einer SVM aktivieren, bevor ein Zugriff oder On-Demand-Scan ausgeführt werden kann.

Schritte

1. Virenprüfung auf einer SVM aktivieren:

   ```
   vserver vscan enable -vserver data_SVM
   ```

   > Sie können das verwenden `vserver vscan disable` Befehl zum Deaktivieren des Virenscans, falls erforderlich.

   Mit dem folgenden Befehl wird das Scannen von Viren auf der aktiviert `vs1` SVM:

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. Vergewissern Sie sich, dass der Virus-Scan auf der SVM aktiviert ist:

   ```
   vserver vscan show -vserver data_SVM
   ```

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl wird der Vscan-Status des angezeigt `vs1` SVM:

   ```
   cluster1::> vserver vscan show -vserver vs1

                              Vserver: vs1
                         Vscan Status: on
   ```

Setzen Sie den Status der gescannten Dateien zurück

Gelegentlich möchten Sie den Scanstatus erfolgreich gescannter Dateien auf einer SVM mithilfe von zurücksetzen `vserver vscan reset` Befehl zum Verwerfen der zwischengespeicherten Informationen für die Dateien. Mit diesem Befehl können Sie beispielsweise die Virenüberprüfung neu starten, wenn ein falsch konfigurierter Scan durchgeführt wird.

Über diese Aufgabe

Nachdem Sie den ausgeführt haben `vserver vscan reset` Befehl: Alle geeigneten Dateien werden beim nächsten Zugriff gescannt.

> Dieser Befehl kann sich nachteilig auf die Performance auswirken, abhängig von der Anzahl und Größe der neu zu speicherenden Dateien.

Was Sie benötigen

Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Status der gescannten Dateien zurücksetzen:

   ```
   vserver vscan reset -vserver data_SVM
   ```

   Mit dem folgenden Befehl wird der Status der gescannten Dateien auf dem zurückgesetzt `vs1` SVM:

   ```
   cluster1::> vserver vscan reset -vserver vs1
   ```

Zeigen Sie Vscan-Ereignisprotokollinformationen an

Sie können das verwenden `vserver vscan show-events` Befehl zum Anzeigen von Ereignisprotokollinformationen zu infizierten Dateien, Aktualisierungen auf Vscan-Servern und dergleichen. Sie können Ereignisinformationen für das Cluster oder bestimmte Nodes, SVMs oder Vscan-Server anzeigen.

Bevor Sie beginnen

Zum Anzeigen des Vscan-Ereignisprotokolls sind erweiterte Berechtigungen erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Anzeigen von Vscan-Ereignisprotokollinformationen:

   ```
   vserver vscan show-events
   ```

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden Ereignisprotokollinformationen für das Cluster angezeigt `cluster1`:

```
cluster1::*> vserver vscan show-events

Vserver     Node            Server          Event Type        Event Time
----------- --------------- --------------- -----------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

Überwachung und Fehlerbehebung von Konnektivitätsproblemen

Mögliche Verbindungsprobleme bei der Option „Scannen erforderlich“

Sie können das verwenden `vserver vscan connection-status show` Befehle zum Anzeigen von Informationen über Vscan-Serververbindungen, die bei der Behebung von Verbindungsproblemen hilfreich sein könnten.

Standardmäßig wird der verwendet `scan-mandatory` Option für das Scannen beim Zugriff verweigert den Dateizugriff, wenn keine Vscan-Serververbindung zum Scannen verfügbar ist. Obwohl diese Option wichtige Sicherheitsfunktionen bietet, kann sie in einigen Situationen zu Problemen führen.

- Bevor Sie den Client-Zugriff aktivieren, müssen Sie sicherstellen, dass mindestens ein Vscan-Server mit einer SVM auf jedem Node mit einer LIF verbunden ist. Wenn Sie nach Aktivierung des Client-Zugriffs Server mit SVMs verbinden müssen, müssen Sie den deaktivieren `scan-mandatory` Option auf der SVM, um sicherzustellen, dass der Dateizugriff nicht verweigert wird, da keine Vscan-Serververbindung verfügbar ist. Sie können die Option wieder einschalten, nachdem der Server verbunden ist.
- Wenn ein Ziel-LIF alle Vscan-Serververbindungen für eine SVM hostet, geht die Verbindung zwischen dem Server und der SVM verloren, wenn die LIF migriert wird. Um sicherzustellen, dass der Dateizugriff nicht verweigert wird, weil keine Vscan-Serververbindung verfügbar ist, müssen Sie das deaktivieren `scan-mandatory` Vor der Migration des LIF Option. Sie können die Option wieder einschalten, nachdem das LIF migriert wurde.

Jeder SVM sollten mindestens zwei Vscan-Server zugewiesen sein. Als Best Practice wird empfohlen, Vscan-Server über ein anderes Netzwerk als den für Client-Zugriffe verwendeten Vscan-Servern mit dem Speichersystem zu verbinden.

Befehle zum Anzeigen des Verbindungsstatus des Vscan-Servers

Sie können das verwenden `vserver vscan connection-status show` Befehle zum Anzeigen der Zusammenfassung und detaillierter Informationen zum Verbindungsstatus des Vscan-Servers.

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Zeigen Sie eine Zusammenfassung der Vscan-Serververbindungen an	`vserver vscan connection-status show`
Details zu Vscan-Serververbindungen anzeigen	`vserver vscan connection-status show-all`
Details für verbundene Vscan-Server anzeigen	`vserver vscan connection-status show-connected`
Details zu verfügbaren Vscan-Servern anzeigen, die nicht verbunden sind	`vserver vscan connection-status show-not-connected`

Weitere Informationen zu diesen Befehlen finden Sie im "ONTAP-man-Pages".

Fehlerbehebung beim Virenscan

Bei häufigen Problemen mit der Virenprüfung gibt es mögliche Ursachen und Möglichkeiten, diese zu lösen. Virus-Scan wird auch als Vscan bezeichnet.

Problem	Wie man es löst
Die Vscan-Server können keine Verbindung herstellen Dem Storage-System Clustered ONTAP	Prüfen Sie, ob die Scannerpoolkonfiguration die IP-Adresse des Vscan-Servers angibt. Überprüfen Sie auch, ob die zulässigen privilegierten Benutzer in der Scannerpoolliste aktiv sind. Führen Sie zum Überprüfen des Scannerpools den aus `vserver vscan scanner-pool show` In der Eingabeaufforderung des Storage-Systems. Wenn die Vscan-Server immer noch keine Verbindung herstellen können, liegt möglicherweise ein Problem mit dem Netzwerk vor.
Bei Clients beobachten wir eine hohe Latenz.	Es ist wahrscheinlich an der Zeit, dem Scanner-Pool weitere Vscan-Server hinzuzufügen.
Es werden zu viele Scans ausgelöst.	Ändern Sie den Wert des `vscan-fileop-profile` Parameter, um die Anzahl der für Virenprüfungen überwachten Dateioperationen zu beschränken.
Einige Dateien werden nicht gescannt.	Überprüfen Sie die Zugangsrichtlinie. Es ist möglich, dass der Pfad für diese Dateien zur Pfadausschlussliste hinzugefügt wurde oder dass ihre Größe den konfigurierten Wert für Ausschlüsse überschreitet. Führen Sie zum Überprüfen der Zugriffsrichtlinie den aus `vserver vscan on-access-policy show` In der Eingabeaufforderung des Storage-Systems.

Dateizugriff wurde verweigert.	Prüfen Sie, ob die Einstellung „*Scan-mandatory*“ in der Richtlinienkonfiguration angegeben ist. Diese Einstellung verweigert den Datenzugriff, wenn keine Vscan-Server verbunden sind. Ändern Sie die Einstellung nach Bedarf.

Überwachen Sie den Status und die Performance-Aktivitäten

Sie können die kritischen Aspekte des Vscan-Moduls überwachen, z. B. den Verbindungsstatus des Vscan-Servers,
Der Zustand der Vscan-Server und die Anzahl der gescannten Dateien. Diese Informationen helfen
Sie diagnostizieren Probleme im Zusammenhang mit dem Vscan-Server.

Anzeigen von Vscan-Serververbindungsinformationen

Sie können den Verbindungsstatus von Vscan-Servern anzeigen, um die bereits verwendeten Verbindungen zu verwalten
Und die verfügbaren Verbindungen. Verschiedene Befehle zeigen Informationen an
Informationen zum Verbindungsstatus von Vscan-Servern.

Befehl…	Angezeigte Informationen…
`vserver vscan connection-status show`	Zusammenfassung des Verbindungsstatus
`vserver vscan connection-status show-all`	Detaillierte Informationen zum Verbindungsstatus
`vserver vscan connection-status show-not-connected`	Status der verfügbaren, aber nicht verbundenen Verbindungen
`vserver vscan connection-status show-connected`	Informationen zum angeschlossenen Vscan-Server

Weitere Informationen zu diesen Befehlen finden Sie im "Man-Pages".

Vscan-Server-Statistiken anzeigen

Sie können Vscan-Server-spezifische Statistiken anzeigen, um die Leistung zu überwachen und Probleme im Zusammenhang mit zu diagnostizieren
Virus-Scan. Sie müssen eine Datenprobe erfassen, bevor Sie den verwenden können `statistics show` Befehl an
Zeigt die Vscan-Server-Statistiken an.
Um eine Datenprobe auszufüllen, gehen Sie wie folgt vor:

Schritt

1. Führen Sie die aus `statistics start` Befehl und das `optional statistics` Befehl stoppen.

Anzeigen von Statistiken für Vscan-Serveranfragen und -Latenzen

Sie können ONTAP verwenden `offbox_vscan` Zähler pro SVM zur Überwachung der Vscan-Rate Serveranfragen, die pro Sekunde versendet und empfangen werden, und die Server-Latenzen über alle Vscan hinweg
Server: Führen Sie zum Anzeigen dieser Statistiken den folgenden Schritt aus:

Schritt

1. Führen Sie die Statistikshow aus `object offbox_vscan -instance SVM` Befehl mit dem Folgende Zähler:

Zähler…	Angezeigte Informationen…
`scan_request_dispatched_rate`	Anzahl der von ONTAP an die Vscan-Server gesendeten Virenscanner pro Sekunde
`scan_noti_received_rate`	Anzahl der von ONTAP von den Vscan-Servern zurückempfangenen Virenscans pro Sekunde
`dispatch_latency`	Latenz innerhalb von ONTAP, um einen verfügbaren Vscan-Server zu identifizieren und die Anforderung an diesen Vscan-Server zu senden
`scan_latency`	Round-Trip-Latenz von ONTAP auf den Vscan-Server, einschließlich der Zeit für die Ausführung des Scans

Beispiel für Statistiken, die von einem ONTAP Offbox vscan-Zähler generiert wurden

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
--------------------------------------------------------------------
```

Anzeigen von Statistiken zu einzelnen Vscan-Serveranfragen und -Latenzen

Sie können ONTAP verwenden `offbox_vscan_server` Zähler auf einem pro SVM, pro Box-Vscan-Server, Und auf Node-Basis, um die Rate der versendeten Vscan-Serveranfragen und die Serverlatenz zu überwachen

Jeder Vscan-Server einzeln. Um diese Informationen zu erfassen, führen Sie den folgenden Schritt aus:

Schritt

1. Führen Sie die aus `statistics show -object offbox_vscan -instance SVM:servername:nodename` Befehl mit den folgenden Zählern:

Zähler…	Angezeigte Informationen…
`scan_request_dispatched_rate`	Anzahl der von ONTAP gesendeten Virenscanner
`scan_latency`	Round-Trip-Latenz von ONTAP auf den Vscan-Server, einschließlich der Zeit für die Ausführung des Scans Zu den Vscan-Servern pro Sekunde

Beispiel für Statistiken, die von einem ONTAP offbox_vscan_Server-Zähler generiert wurden

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-----------------------------------------------------------------
```

Anzeigen von Statistiken für die Vscan-Serverauslastung

Sie können auch ONTAP verwenden `offbox_vscan_server` Zähler zur Erfassung der serverseitigen Vscan-Nutzung
Statistiken. Diese Statistiken werden auf SVM-, Off-Box- und Vscan-Server- und Node-Basis verfolgt. Sie Einbeziehen der CPU-Auslastung auf dem Vscan-Server, Warteschlangentiefe für Scanvorgänge auf dem Vscan-Server
(Aktuell und maximal), verwendeter Speicher und verwendetes Netzwerk.
Diese Statistiken werden vom Antivirus Connector an die Statistikzähler in ONTAP weitergeleitet. Sie
Auf Daten basieren, die alle 20 Sekunden abgefragt werden und zur Genauigkeit mehrfach erfasst werden müssen;
Andernfalls spiegeln die Werte in den Statistiken nur die letzte Abfrage wider. CPU-Auslastung und Warteschlangen
Dies ist besonders wichtig für die Überwachung und Analyse. Ein hoher Wert für eine durchschnittliche Warteschlange kann darauf hinweisen, dass der
Vscan Server hat einen Engpass.
Erfassen von Auslastungsstatistiken für den Vscan-Server auf einem pro SVM, pro-Off-Box-Vscan-Server und pro Node
Gehen Sie wie folgt vor:

Schritt

1. Sammeln von Auslastungsstatistiken für den Vscan-Server

   Führen Sie die aus `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` Mit dem folgenden Befehl `offbox_vscan_server` Zähler:

Zähler…	Angezeigte Informationen…
`scanner_stats_pct_cpu_used`	CPU-Auslastung auf dem Vscan-Server
`scanner_stats_pct_input_queue_avg`	Durchschnittliche Warteschlange von Scananforderungen auf dem Vscan-Server
`scanner_stats_pct_input_queue_hiwatermark`	Spitzenwarteschlange von Scananforderungen auf dem Vscan-Server
`scanner_stats_pct_mem_used`	Auf dem Vscan-Server verwendeter Speicher
`scanner_stats_pct_network_used`	Auf dem Vscan-Server verwendetes Netzwerk

Beispiel für Auslastungsstatistiken für den Vscan-Server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

Prüfung von NAS-Ereignissen auf SVMs

SMB- und NFS-Auditing und Sicherheits-Tracing

Zudem können die mit ONTAP verfügbaren Auditing-Funktionen für Dateizugriffe über SMB und NFS verwendet werden, beispielsweise von nativen Audits und Dateirichtlinien-

Management über FPolicy.

Unter den folgenden Umständen sollten Audits für SMB- und NFS-Dateizugriffe entworfen und implementiert werden:

- Der grundlegende Dateizugriff über SMB und NFS wurde konfiguriert.
- Sie möchten eine Überwachungskonfiguration mit einer der folgenden Methoden erstellen und verwalten:
  - Native ONTAP Funktionalität
  - Externe FPolicy Server

Prüfung von NAS-Ereignissen auf SVMs

Das Auditing von NAS-Ereignissen ist eine Sicherheitsmaßnahme, mit der Sie bestimmte SMB- und NFS-Ereignisse auf Storage Virtual Machines (SVMs) nachverfolgen und protokollieren können. So können Sie potenzielle Sicherheitsprobleme verfolgen und Sicherheitsverletzungen nachweisen. Außerdem können Sie zentrale Active Directory-Zugriffsrichtlinien erstellen und prüfen, um zu sehen, welche Ergebnisse diese implementieren würden.

SMB-Ereignisse

Sie können die folgenden Ereignisse prüfen:

- SMB-Datei- und Ordnerzugriff

  SMB-Datei- und Ordnerzugriffe auf Objekte prüfen, die in FlexVol Volumes gespeichert sind, die zu prüfenden SVMs gehören.

- SMB-Anmeldung und -Abmeldung

  Sie können SMB-Anmeldeereignisse und Abmeldeereignisse für SMB-Server auf SVMs prüfen.

- Staging von zentralen Zugriffsrichtlinien

  Sie können den effektiven Zugriff auf Objekte auf SMB-Servern anhand von Berechtigungen überprüfen, die anhand vorgeschlagener, zentraler Zugriffsrichtlinien angewendet werden. Das Auditing durch die Durchführung von zentralen Zugriffsrichtlinien ermöglicht es Ihnen, die Auswirkungen zentraler Zugriffsrichtlinien zu sehen, bevor sie bereitgestellt werden.

  Das Auditing von zentralen Zugriffsrichtlinien-Staging wird über Active Directory GPOs eingerichtet. Die SVM-Auditing-Konfiguration muss jedoch für das Auditing von Staging von zentralen Zugriffsrichtlinien konfiguriert werden.

  Obwohl Sie die zentrale Zugriffsrichtlinien-Staging in der Überwachungskonfiguration aktivieren können, ohne die dynamische Zugriffskontrolle auf dem SMB-Server zu aktivieren, werden zentrale Zugriffsrichtlinien-Staging-Ereignisse nur erzeugt, wenn Dynamic Access Control aktiviert ist. Die dynamische Zugriffskontrolle wird über eine SMB-Serveroption aktiviert. Sie ist standardmäßig nicht aktiviert.

NFS-Ereignisse

Sie können Datei- und Verzeichnisereignisse prüfen, indem Sie die NFSv4-ACL auf Objekten verwenden, die auf SVMs gespeichert sind.

Funktionsweise des Audits

Grundlegende Prüfungskonzepte

Um das Auditing in ONTAP zu verstehen, sollten Sie einige grundlegende Prüfungskonzepte kennen.

- **Staging-Dateien**

  Die zwischenliegenden Binärdateien auf einzelnen Knoten, in denen Audit-Datensätze vor der Konsolidierung und Konvertierung gespeichert werden. Staging-Dateien sind in Staging-Volumes enthalten.

- **Staging Volumen**

  Ein von ONTAP erstelltes dediziertes Volume zum Speichern von Staging-Dateien. Es gibt ein Staging-Volume pro Aggregat. Staging Volumes werden von allen revisionssichere Storage Virtual Machines (SVMs) gemeinsam genutzt, um Audit-Datensätze des Datenzugriffs für Daten-Volumes im jeweiligen Aggregat zu speichern. Die Audit-Datensätze jeder SVM werden in einem separaten Verzeichnis innerhalb des Staging-Volume gespeichert.

  Cluster-Administratoren können Informationen über Staging Volumes anzeigen, die meisten anderen Volume-Vorgänge sind jedoch nicht zulässig. Nur ONTAP kann Staging-Volumes erstellen. ONTAP weist Staging-Volumes automatisch einen Namen zu. Alle Staging-Volume-Namen beginnen mit `MDV_aud_` Anschließend die UUID des Aggregats, welches das Staging-Volume enthält (z. B.: `MDV_aud_1d0131843d4811e296fc123478563412`.)

- **System-Volumes**

  Ein FlexVol Volume mit speziellen Metadaten, wie z. B. Metadaten für Audit-Protokolle für Fileservices. Die Admin-SVM ist Eigentümer von System-Volumes, die im Cluster sichtbar sind. Staging Volumes sind eine Art System-Volume.

- * Konsolidierungsaufgabe*

  Eine Aufgabe, die bei aktivierter Prüfung erstellt wird. Diese langwierige Aufgabe auf jeder SVM nimmt die Audit-Datensätze aus Staging-Dateien über die Mitglied-Nodes der SVM auf. Mit dieser Aufgabe werden die Audit-Datensätze in einer sortierten chronologischen Reihenfolge zusammengeführt und dann in ein benutzerlesbares Ereignisprotokollformat konvertiert, das in der Überwachungskonfiguration angegeben ist – entweder das EVTX- oder das XML-Dateiformat. Die umgerechneten Ereignisprotokolle werden im Verzeichnis für Revisionsereignisse gespeichert, das in der SVM-Audit-Konfiguration angegeben ist.

Funktionsweise des ONTAP-Prüfprozesses

Der ONTAP-Audit-Prozess unterscheidet sich vom Microsoft-Audit-Prozess. Bevor Sie die Prüfung konfigurieren, sollten Sie verstehen, wie der ONTAP-Audit-Prozess funktioniert.

Auditdatensätze werden zunächst in binären Staging-Dateien auf einzelnen Knoten gespeichert. Wenn das Auditing auf einer SVM aktiviert ist, behält jeder Member-Node Staging-Dateien für diese SVM bei. Sie werden in regelmäßigen Abständen konsolidiert und in benutzerlesbare Ereignisprotokolle umgewandelt, die im Verzeichnis der Auditereignisse für die SVM gespeichert sind.

Prozess, bei dem die Prüfung auf einer SVM aktiviert ist

Auditing kann nur auf SVMs aktiviert werden. Wenn der Storage-Administrator das Auditing für die SVM ermöglicht, überprüft das Auditing-Subsystem, ob Staging-Volumes vorhanden sind. Für jedes Aggregat, das Daten-Volumes der SVM enthält, muss ein Staging-Volume vorhanden sein. Das Audit-Subsystem erstellt alle erforderlichen Staging-Volumes, wenn sie nicht vorhanden sind.

Das Revisions-Subsystem schließt auch andere erforderliche Aufgaben ab, bevor die Prüfung aktiviert wird:

- Das Audit-Subsystem überprüft, ob der Protokollverzeichnis-Pfad verfügbar ist und keine Symlinks enthält.

  Das Logverzeichnis muss bereits als Pfad innerhalb des Namespace der SVM vorhanden sein. Es wird empfohlen, ein neues Volume oder einen neuen qtree zu erstellen, um die Audit-Log-Dateien zu speichern. Das Audit-Subsystem weist keinen Standardspeicherort für Protokolldateien zu. Wenn der in der Überwachungskonfiguration angegebene Protokollverzeichnis-Pfad kein gültiger Pfad ist, schlägt die Erstellung der Überwachungskonfiguration mit dem fehl `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` Fehler.

  Die Konfigurationserstellung schlägt fehl, wenn das Verzeichnis existiert, aber Symlinks enthält.

- Auditing plant die Konsolidierungsaufgabe.

  Nach der Planung dieser Aufgabe wird die Prüfung aktiviert. Die SVM-Überwachungskonfiguration und die Protokolldateien bleiben bei einem Neustart erhalten oder wenn die NFS- oder SMB-Server angehalten oder neu gestartet werden.

Konsolidierung von Ereignisprotokolls

Die Protokollkonsolidierung ist eine geplante Aufgabe, die auf routinemäßiger Basis ausgeführt wird, bis die Prüfung deaktiviert ist. Bei deaktiviertem Auditing überprüft der Konsolidierungsauftrag, ob alle übrigen Protokolle konsolidiert werden.

Garantierte Audits

Standardmäßig ist Auditing garantiert. ONTAP garantiert, dass alle prüffähigen Dateizugriffsereignisse (wie durch konfigurierte Audit-Policy-ACLs festgelegt) aufgezeichnet werden, selbst wenn ein Knoten nicht verfügbar ist. Ein angeforderter Dateivorgang kann erst abgeschlossen werden, wenn der Prüfdatensatz für diesen Vorgang im Staging-Volume auf einem persistenten Speicher gespeichert wird. Wenn Audit-Datensätze nicht auf der Festplatte in den Staging-Dateien gespeichert werden können, entweder aufgrund von mangelhaftdem Speicherplatz oder aufgrund anderer Probleme, werden Client-Vorgänge verweigert.

> Ein Administrator oder Account-Benutzer mit Zugriff auf die Berechtigungsebene kann die Dateiauditprotokollierung mithilfe des NetApp Manageability SDK oder REST-APIs umgehen. Sie können ermitteln, ob Dateiaktionen mit NetApp Manageability SDK oder REST-APIs ausgeführt wurden, indem Sie die in den gespeicherten Befehlsprotokollen überprüfen `audit.log` Datei:
>
> Weitere Informationen zu Audit-Protokollen zum Befehlsprotokoll finden Sie im Abschnitt „Managen der Audit-Protokollierung für Verwaltungsaktivitäten“ in "Systemadministration".

Konsolidierungsprozess, wenn ein Node nicht verfügbar ist

Wenn ein Node mit Volumes, die zu einer SVM mit aktivierter Prüfung gehören, nicht verfügbar ist, hängt das Verhalten der Überwachungskonsolidierungsaufgabe davon ab, ob der Storage Failover (SFO)-Partner (oder

der HA-Partner im Fall eines Clusters mit zwei Nodes) verfügbar ist:

- Wenn das Staging-Volume über den SFO-Partner verfügbar ist, werden die zuletzt vom Node gemeldeten Staging-Volumes gescannt und die Konsolidierung wird normal durchgeführt.
- Wenn der SFO-Partner nicht verfügbar ist, erstellt die Aufgabe eine partielle Protokolldatei.

  Wenn ein Knoten nicht erreichbar ist, konsolidiert der Konsolidierungsauftrag die Audit-Datensätze von den anderen verfügbaren Nodes dieser SVM. Um festzustellen, dass er nicht vollständig ist, fügt die Aufgabe das Suffix hinzu `.partial` Zum konsolidierten Dateinamen.

- Nachdem der nicht verfügbare Knoten verfügbar ist, werden die Audit-Datensätze in diesem Knoten zu diesem Zeitpunkt mit den Audit-Datensätzen der anderen Knoten konsolidiert.
- Alle Audit-Datensätze werden erhalten bleiben.

Drehung des Ereignisprotokolls

Audit-Ereignisprotokolldateien werden gedreht, wenn sie eine konfigurierte Größe des Schwellenwertprotokolls oder einen konfigurierten Zeitplan erreichen. Wenn eine Ereignis-Log-Datei gedreht wird, benennt der geplante Konsolidierungsvorgang zunächst die in eine zeitgestempelte Archivdatei konvertierte aktive Datei und erstellt dann eine neue aktive, konvertierte Ereignis-Log-Datei.

Prozess bei deaktiviertem Auditing auf der SVM

Wenn die Prüfung auf der SVM deaktiviert ist, wird die Konsolidierungsaufgabe ein letztes Mal ausgelöst. Alle ausstehenden, aufgezeichneten Audit-Datensätze werden in einem vom Benutzer lesbaren Format protokolliert. Vorhandene Ereignisprotokolle, die im Verzeichnis für das Ereignisprotokoll gespeichert sind, werden nicht gelöscht, wenn die Prüfung auf der SVM deaktiviert ist und zur Anzeige zur Verfügung stehen.

Nachdem alle bestehenden Staging-Dateien für diese SVM konsolidiert wurden, wird die Aufgabe der Konsolidierung aus dem Zeitplan entfernt. Durch Deaktivieren der Überwachungskonfiguration für die SVM wird die Überwachungskonfiguration nicht entfernt. Ein Storage-Administrator kann das Auditing jederzeit neu aktivieren.

Der beim Auditing erstellte Konsolidierungsauftrag überwacht die Konsolidierungsaufgabe und erstellt sie neu, wenn die Konsolidierungsaufgabe aufgrund eines Fehlers beendet wird. Benutzer können den Überwachungskonsolidierungsauftrag nicht löschen.

Anforderungen und Überlegungen des Audits

Bevor Sie das Auditing über eine Storage Virtual Machine (SVM) konfigurieren und aktivieren, müssen Sie bestimmte Anforderungen und Überlegungen beachten.

- Die maximale Anzahl der unterstützten SVMs mit Auditing-Aktivierung hängt von Ihrer Version von ONTAP ab:

ONTAP-Version	Maximal
9.8 und früher	50
9.9.1 und höher	400

- Das Auditing ist nicht an SMB- oder NFS-Lizenzen gebunden.

  Auch wenn SMB- und NFS-Lizenzen nicht auf dem Cluster installiert sind, können Sie das Auditing

konfigurieren und aktivieren.

- NFS-Prüfung unterstützt Sicherheitsvorkehrungen (Typ U).
- Für NFS-Prüfung gibt es keine Zuordnung zwischen Modus-Bits und Audit-Aces.

  Beim Konvertieren von ACLs in Mode-Bits werden die Auditierung von Aces übersprungen. Beim Konvertieren von Modusbits zu ACLs werden keine Auditierungsaces generiert.

- Das in der Überwachungskonfiguration angegebene Verzeichnis muss vorhanden sein.

  Wenn sie nicht vorhanden ist, schlägt der Befehl zum Erstellen der Überwachungskonfiguration fehl.

- Das in der Überwachungskonfiguration angegebene Verzeichnis muss die folgenden Anforderungen erfüllen:
  - Das Verzeichnis darf keine symbolischen Links enthalten.

    Wenn das in der Überwachungskonfiguration angegebene Verzeichnis symbolische Links enthält, schlägt der Befehl zum Erstellen der Überwachungskonfiguration fehl.

  - Sie müssen das Verzeichnis über einen absoluten Pfad angeben.

    Sie sollten keinen relativen Pfad angeben, z. B. `/vs1/../`.

- Die Prüfung hängt davon ab, dass in den Staging-Volumes Platz zur Verfügung steht.

  Sie müssen einen Plan kennen und sicherstellen, dass ausreichend Platz für die Staging-Volumes in Aggregaten mit auditierten Volumes vorhanden ist.

- Die Prüfung hängt davon ab, dass im Volume genügend Speicherplatz verfügbar ist, der das Verzeichnis enthält, in dem konvertierte Ereignisprotokolle gespeichert werden.

  Sie müssen sich bewusst sein und einen Plan erstellen, um sicherzustellen, dass in den Volumes ausreichend Speicherplatz für die Speicherung von Ereignisprotokollen vorhanden ist. Sie können die Anzahl der Ereignisprotokolle angeben, die im Überwachungsverzeichnis aufbewahrt werden sollen, indem Sie die verwenden `-rotate-limit` Parameter beim Erstellen einer Überwachungskonfiguration, der dabei helfen kann, sicherzustellen, dass genügend Speicherplatz für die Ereignisprotokolle im Volume vorhanden ist.

- Obwohl Sie die zentrale Zugriffsrichtlinien-Staging in der Überwachungskonfiguration aktivieren können, ohne Dynamic Access Control auf dem SMB-Server zu aktivieren, muss Dynamic Access Control aktiviert sein, um zentrale Zugriffs-Policy-Staging-Ereignisse zu generieren.

  Die dynamische Zugriffskontrolle ist standardmäßig nicht aktiviert.

Überlegungen zu Aggregatspeicherplatz bei Aktivierung von Auditing

Wenn eine Audit-Konfiguration erstellt und Auditing auf mindestens einer Storage Virtual Machine (SVM) im Cluster aktiviert wird, erstellt das Audit-Subsystem Staging-Volumes auf allen bestehenden Aggregaten und auf allen neu erstellten Aggregaten. Wenn Sie das Auditing auf dem Cluster aktivieren, müssen Sie bestimmte Überlegungen zu Aggregatspeicherplatz beachten.

Die Erstellung von Staging-Volumes kann aufgrund der nicht verfügbaren Speicherkapazität in einem Aggregat fehlschlagen. Dies kann passieren, wenn Sie eine Audit-Konfiguration erstellen und vorhandene Aggregate nicht über genügend Platz verfügen, um das Staging-Volume zu enthalten.

Sie sollten sicherstellen, dass auf vorhandenen Aggregaten für die Staging-Volumes genügend Speicherplatz vorhanden ist, bevor das Auditing auf einer SVM aktiviert wird.

Einschränkungen für die Größe von Prüfdatensätzen für Staging-Dateien

Die Größe eines Audit-Datensatzes für eine Staging-Datei darf nicht größer als 32 KB sein.

Wenn große Audit-Datensätze auftreten können

Bei der Prüfung der Verwaltung können große Audit-Datensätze in einem der folgenden Szenarien auftreten:

- Benutzer zu oder aus Gruppen mit einer großen Anzahl von Benutzern hinzufügen oder löschen.
- Hinzufügen oder Löschen einer Zugriffssteuerungsliste für Dateifreigabe (File-share Access Control List, ACL) auf einer Dateifreigabe mit einer großen Anzahl von Benutzern für die Dateifreigabe
- Andere Szenarien.

Deaktivieren Sie die Managementprüfung, um dieses Problem zu vermeiden. Ändern Sie dazu die Audit-Konfiguration, und entfernen Sie Folgendes aus der Liste der Audit-Ereignistypen:

- Dateifreigabe
- Benutzerkonto
- Sicherheitsgruppe
- Änderung der Autorisierungsrichtlinie

  Nach dem Entfernen werden diese vom Audit-Subsystem für Fileservices nicht geprüft.

Die Auswirkungen von zu großen Audit-Datensätzen

- Wenn die Größe eines Audit-Datensatzes zu groß ist (über 32 KB), wird der Audit-Datensatz nicht erstellt und das Audit-Subsystem erzeugt eine EMS-Meldung (Event Management System), die der folgenden ähnelt:

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  Wenn die Prüfung gewährleistet ist, schlägt der Dateivorgang fehl, da sein Audit-Datensatz nicht erstellt werden kann.

- Wenn die Größe des Audit-Datensatzes mehr als 9,999 Byte beträgt, wird die gleiche EMS-Meldung wie oben angezeigt. Ein partieller Prüfdatensatz wird erstellt, wobei der größere Schlüsselwert fehlt.
- Wenn der Prüfdatensatz 2,000 Zeichen überschreitet, wird anstelle des tatsächlichen Werts die folgende Fehlermeldung angezeigt:

  ```
  The value of this field was too long to display.
  ```

Die unterstützten Audit-Ereignisprotokollformate

Unterstützte Dateiformate für die umgerechneten Audit-Ereignisprotokolle sind `EVTX` Und `XML` Dateiformate.

Sie können den Dateityp angeben, wenn Sie die Überwachungskonfiguration erstellen. Standardmäßig konvertiert ONTAP die Binärprotokolle in das `EVTX` Dateiformat.

Anzeigen von Audit-Ereignisprotokollen

Mithilfe von Audit-Ereignisprotokollen können Sie feststellen, ob Sie über eine ausreichende Dateisicherheit verfügen und ob es keine falschen Datei- und Ordnerzugriffsversuche gab. Sie können die in gespeicherten Audit-Ereignisprotokolle anzeigen und verarbeiten `EVTX` Oder `XML` Dateiformate.

- `EVTX` Dateiformat

  Sie können die konvertierte öffnen `EVTX` Ereignisprotokolle als gespeicherte Dateien mit Microsoft Event Viewer prüfen.

  Es gibt zwei Optionen, die Sie für die Anzeige von Ereignisprotokollen mit der Ereignisanzeige verwenden können:

  - Allgemeine Ansicht

    Für den Ereignisdatensatz werden Informationen angezeigt, die für alle Ereignisse gemeinsam sind. In dieser ONTAP-Version werden die ereignisspezifischen Daten für den Ereignisdatensatz nicht angezeigt. Mithilfe der detaillierten Ansicht können ereignisspezifische Daten angezeigt werden.

  - Detailansicht

    Eine freundliche Aussicht und eine XML-Ansicht stehen zur Verfügung. Die freundliche Ansicht und die XML-Ansicht zeigen sowohl die Informationen, die für alle Ereignisse gemeinsam sind, als auch die ereignisspezifischen Daten für den Ereignisdatensatz.

- `XML` Dateiformat

  Sie können anzeigen und verarbeiten `XML` Prüfung von Ereignisprotokollen für Anwendungen von Drittanbietern, die den unterstützen `XML` Dateiformat. XML-Anzeigewerkzeuge können verwendet werden, um die Überwachungsprotokolle anzuzeigen, vorausgesetzt, Sie haben das XML-Schema und Informationen zu Definitionen für die XML-Felder. Weitere Informationen zum XML-Schema und zu Definitionen finden Sie im "ONTAP-Überwachungsschema – Referenz".

Wie aktive Prüfprotokolle mit der Ereignisanzeige angezeigt werden

Wenn der Audit-Konsolidierungsprozess auf dem Cluster ausgeführt wird, fügt der Konsolidierungsprozess neue Datensätze an die aktive Audit-Log-Datei für revisionssichere Storage Virtual Machines (SVMs) an. Auf dieses aktive Prüfprotokoll kann über eine SMB-Freigabe in Microsoft Event Viewer zugegriffen und geöffnet werden.

Neben der Anzeige vorhandener Überwachungsdatensätze verfügt die Ereignisanzeige über eine Aktualisierungsoption, mit der Sie den Inhalt im Konsolenfenster aktualisieren können. Ob die neu angefügten

Protokolle in der Ereignisanzeige angezeigt werden, hängt davon ab, ob Oplocks auf der Freigabe aktiviert sind, die zum Zugriff auf das aktive Audit-Protokoll verwendet wird.

Oplocks-Einstellung auf dem Share	Verhalten
Aktiviert	Event Viewer öffnet das Protokoll, das Ereignisse enthält, die bis zu diesem Zeitpunkt geschrieben wurden. Beim Aktualisierungsvorgang wird das Protokoll nicht mit neuen Ereignissen aktualisiert, die durch den Konsolidierungsvorgang angehängt sind.
Deaktiviert	Event Viewer öffnet das Protokoll, das Ereignisse enthält, die bis zu diesem Zeitpunkt geschrieben wurden. Beim Aktualisierungsvorgang wird das Protokoll mit neuen Ereignissen aktualisiert, die durch den Konsolidierungsprozess angefügt werden.

Diese Informationen gelten nur für `EVTX` Ereignisprotokolle `XML` Ereignisprotokolle können über SMB in einem Browser oder über NFS mit einem beliebigen XML-Editor oder Viewer angezeigt werden.

SMB-Ereignisse, die geprüft werden können

SMB-Ereignisse, die geprüft werden können, Übersicht

ONTAP kann bestimmte SMB-Ereignisse überprüfen, einschließlich bestimmter Datei- und Ordnerzugriffsereignisse, bestimmter Anmelde- und Abmeldungsereignisse sowie zentrale Staging von Zugriffsrichtlinien. Das Wissen, welche Zugriffsereignisse auditiert werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den Ereignisprotokollen.

Die folgenden zusätzlichen SMB Ereignisse können im ONTAP 9.2 und höher geprüft werden:

EREIGNIS-ID (EVT/EVTX)	Ereignis	Beschreibung	Kategorie
4670	Objektberechtigungen wurden geändert	OBJEKTZUGRIFF: Berechtigungen geändert.	Dateizugriff
4907	Objektaudits-Einstellungen wurden geändert	OBJEKTZUGRIFF: Audit-Einstellungen geändert.	Dateizugriff
4913	Objektzugriffsrichtlinie wurde geändert	OBJEKTZUGRIFF: KAPPE GEÄNDERT.	Dateizugriff

Die folgenden SMB Ereignisse können im ONTAP 9.0 und höher geprüft werden:

EREIGNIS-ID (EVT/EVTX)	Ereignis	Beschreibung	Kategorie

540/4624	Ein Konto wurde erfolgreich angemeldet	ANMELDUNG/ABMELDUNG: Netzwerk (SMB)-Anmeldung	Anmeldung und Anmeldung
529/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Unbekannter Benutzername oder schlechtes Passwort.	Anmeldung und Anmeldung
530/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Einschränkung der Anmeldezeit des Kontos.	Anmeldung und Anmeldung
531/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Konto derzeit deaktiviert.	Anmeldung und Anmeldung
532/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDEN: Benutzerkonto abgelaufen.	Anmeldung und Anmeldung
533/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Benutzer kann sich nicht bei diesem Computer anmelden.	Anmeldung und Anmeldung
534/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Der Benutzer hat hier keinen Logon-Typ erhalten.	Anmeldung und Anmeldung
535/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Das Kennwort des Benutzers ist abgelaufen.	Anmeldung und Anmeldung
537/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Anmeldung aus anderen als den oben genannten Gründen fehlgeschlagen.	Anmeldung und Anmeldung
539/4625	Ein Konto konnte sich nicht anmelden	ANMELDUNG/ABMELDUNG: Konto gesperrt.	Anmeldung und Anmeldung
538/4634	Ein Konto wurde abgemeldet	ANMELDUNG/ABMELDUNG: Lokale oder Netzwerk-Benutzer abmelden.	Anmeldung und Anmeldung
560/4656	Objekt Öffnen/Objekt Erstellen	OBJEKTZUGRIFF: Objekt (Datei oder Verzeichnis) geöffnet.	Dateizugriff
563/4659	Objekt öffnen mit dem zu löschenden Ziel	OBJEKTZUGRIFF: Ein Handle zu einem Objekt (Datei oder Verzeichnis) wurde mit dem Ziel zum Löschen angefordert.	Dateizugriff

564/4660	Objekt Löschen	OBJEKTZUGRIFF: Objekt löschen (Datei oder Verzeichnis). ONTAP generiert dieses Ereignis, wenn ein Windows-Client versucht, das Objekt (Datei oder Verzeichnis) zu löschen.	Dateizugriff
567/4663	Objekt Lesen/Objekt Schreiben/Objekt-Attribute Abrufen/Objekt-Attribute Festlegen	OBJEKTZUGRIFF: Objektzugriffsversuch (Lesen, Schreiben, get attribut, set attribut). **Hinweis:** bei diesem Event prüft ONTAP nur den ersten SMB-Lesevorgang und den ersten SMB-Schreibvorgang (Erfolg oder Fehler) auf einem Objekt. Dadurch wird verhindert, dass ONTAP übermäßige Protokolleinträge erstellt, wenn ein einzelner Client ein Objekt öffnet und viele aufeinanderfolgende Lese- oder Schreibvorgänge an demselben Objekt durchführt.	Dateizugriff
NA/4664	Harter Link	OBJEKTZUGRIFF: Es wurde versucht, eine harte Verbindung zu erstellen.	Dateizugriff
NA/4818	Die vorgeschlagene zentrale Zugangsrichtlinie gewährt nicht dieselben Zugriffsberechtigungen wie die aktuelle zentrale Zugriffsrichtlinie	OBJEKTZUGRIFF: Zentrale Zugriffsrichtlinien-Staging.	Dateizugriff
NA/NA Data ONTAP Ereignis-ID 9999	Objekt Umbenennen	OBJEKTZUGRIFF: Objekt umbenannt. Dies ist ein ONTAP-Event. Derzeit wird es von Windows nicht als einzelnes Ereignis unterstützt.	Dateizugriff
NA/NA Data ONTAP Ereignis-ID 9998	Verknüpfung Des Objekts Aufheben	OBJEKTZUGRIFF: Objekt wird nicht verknüpft. Dies ist ein ONTAP-Event. Derzeit wird es von Windows nicht als einzelnes Ereignis unterstützt.	Dateizugriff

Weitere Informationen zu Event 4656

Der `HandleID` Kennzeichnung im Audit `XML` Event enthält den Handle des Objekts (Datei oder Verzeichnis), auf das zugegriffen wird. Der `HandleID` Das Tag für das Ereignis EVTX 4656 enthält unterschiedliche Informationen, je nachdem, ob das offene Ereignis zum Erstellen eines neuen Objekts oder zum Öffnen eines vorhandenen Objekts ist:

- Wenn das offene Ereignis eine offene Anforderung ist, ein neues Objekt (Datei oder Verzeichnis) zu erstellen, wird das angezeigt `HandleID` Das Tag im XML-Ereignis „Audit“ ist leer `HandleID` (Beispiel: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  Der `HandleID` Ist leer, weil die OFFENE (zum Erstellen eines neuen Objekts) Anforderung geprüft wird, bevor die tatsächliche Objekterstellung stattfindet und bevor ein Handle vorhanden ist. Nachfolgende geprüfte Ereignisse für dasselbe Objekt haben den richtigen Objektgriff im `HandleID` Tag:

- Wenn das offene Ereignis eine offene Anfrage zum Öffnen eines vorhandenen Objekts ist, wird dem Audit-Ereignis das zugewiesene Handle dieses Objekts im zugewiesen `HandleID` Tag (zum Beispiel: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Legen Sie fest, welcher Pfad zum geprüften Objekt vollständig ist

Der im gedruckte Objektpfad `<ObjectName>` Das Tag für einen Prüfdatensatz enthält den Namen des Volumens (in Klammern) und den relativen Pfad aus der Root des enthaltenden Volumens. Wenn Sie den vollständigen Pfad des geprüften Objekts einschließlich des Verbindungspfades bestimmen möchten, müssen Sie bestimmte Schritte durchführen.

Schritte

1. Ermitteln Sie den Volume-Namen und den relativen Pfad zum geprüften Objekt, indem Sie sich das ansehen `<ObjectName>` Kennzeichnung im Audit-Ereignis.

   In diesem Beispiel lautet der Volume-Name „`data1`“ und der relative Pfad zur Datei `/dir1/file.txt`:

   ```
   <Data Name="ObjectName">(data1);/dir1/file.txt</Data>
   ```

2. Anhand des im vorherigen Schritt festgelegten Volume-Namens bestimmen Sie, was der Verbindungspfad für das Volume ist, das das geprüfte Objekt enthält:

   In diesem Beispiel lautet der Volume-Name „`data1`“ und der Verbindungspfad für das Volume mit dem geprüften Objekt lautet `/data/data1`:

   ```
   volume show -junction -volume data1
   ```

   ```
                                   Junction                      Junction
   Vserver   Volume       Language Active    Junction Path     Path Source
   --------- ------------ -------- --------  ----------------- -----------
   vs1       data1        en_US.UTF-8
                                   true      /data/data1       RW_volume
   ```

3. Bestimmen Sie den vollständigen Pfad zum geprüften Objekt, indem Sie den im gefundenen relativen Pfad anhängen `<ObjectName>` Markieren Sie den Verbindungspfad für das Volume.

   In diesem Beispiel ist der Verbindungspfad für das Volume:

   ```
   /data/data1/dir1/file.text
   ```

Überlegungen beim Auditing von Symlinks und Hard Links

Es gibt bestimmte Überlegungen, die Sie bei der Prüfung von Symlinks und harten Links beachten müssen.

Ein Audit-Datensatz enthält Informationen über das zu prüfenden Objekt einschließlich des Pfads zum geprüften Objekt, das im identifiziert wird `ObjectName` Tag: Sie sollten sich bewusst sein, wie Pfade für Symlinks und harte Links in aufgezeichnet werden `ObjectName` Tag:

Symlinks

Ein Symlink ist eine Datei mit einer separaten Inode, die einen Zeiger auf den Speicherort eines Zielobjekts enthält, das als Ziel bezeichnet wird. Beim Zugriff auf ein Objekt über einen Symlink interpretiert ONTAP automatisch den Symlink und folgt dem tatsächlichen kanonischen protokollunabhängigen Pfad zum Zielobjekt im Volume.

In der folgenden Beispielausgabe gibt es zwei Symlinks, die beide auf eine Datei mit dem Namen verweisen `target.txt`. Einer der Symlinks ist ein relativer Symlink und einer ist ein absolutes Symlink. Wenn eines der Symlinks geprüft wird, wird das angezeigt `ObjectName` Das Tag im Überwachungsereignis enthält den Pfad zur Datei `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Feste Verbindungen

Eine harte Verbindung ist ein Verzeichniseintrag, der einen Namen mit einer vorhandenen Datei auf einem Dateisystem verknüpft. Die harte Verbindung verweist auf den Inode-Speicherort der Originaldatei. Ähnlich wie ONTAP Symlinks interpretiert, interpretiert ONTAP die harte Verbindung und folgt dem eigentlichen kanonischen Pfad zum Zielobjekt im Volume. Wenn der Zugriff auf ein Objekt mit harter Verbindung geprüft wird, zeichnet das Ereignis Audit diesen absoluten kanonischen Pfad im auf `ObjectName` Markieren Sie anstelle des Pfads der harten Verbindung.

Überlegungen beim Prüfen alternativer NTFS-Datenströme

Beim Auditing von Dateien mit alternativen NTFS-Datenströmen müssen Sie bestimmte Überlegungen beachten.

Der Speicherort eines zu auditiditierenden Objekts wird in einem Ereignisdatensatz mit zwei Tags, dem, aufgezeichnet `ObjectName` Tag (der Pfad) und der `HandleID` Kennzeichnen (Griff). Um die zu protokollierenden Stream-Anforderungen richtig zu ermitteln, müssen Sie sich bewusst sein, welche ONTAP-Datensätze in diesen Feldern für NTFS-alternative Datenströme enthalten sind:

- EVTX-ID: 4656 Ereignisse (Öffnen und Erstellen von Audit-Ereignissen)
  - Der Pfad des alternativen Datenstroms wird im aufgezeichnet `ObjectName` Tag:
  - Das Handle des alternativen Datenstroms wird im aufgezeichnet `HandleID` Tag:

- EVTX-ID: 4663 Ereignisse (alle anderen Audit-Ereignisse, wie Lesen, Schreiben, getattr usw.)
  - Der Pfad der Basisdatei, nicht der alternative Datenstrom, wird im aufgezeichnet `ObjectName` Tag:
  - Das Handle des alternativen Datenstroms wird im aufgezeichnet `HandleID` Tag:

Beispiel

Das folgende Beispiel zeigt, wie die EVTX-ID identifiziert werden kann: 4663 Ereignisse für alternative Datenströme mit dem `HandleID` Tag: Obwohl das `ObjectName` Das Tag (Pfad), das im Ereignis „Audit lesen“ aufgezeichnet wurde, befindet sich in dem Pfad der Basisdatei, dem `HandleID` Mit dem Tag kann das Ereignis als Prüfdatensatz für den alternativen Datenstrom identifiziert werden.

Stream-Dateinamen nehmen das Formular ein `base_file_name:stream_name`. In diesem Beispiel ist der `dir1` Das Verzeichnis enthält eine Basisdatei mit einem alternativen Datenstrom mit folgenden Pfaden:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

> Die Ausgabe im folgenden Ereignisbeispiel wird wie angegeben abgeschnitten; in der Ausgabe werden nicht alle verfügbaren Ausgabetags für die Ereignisse angezeigt.

Bei einer EVTX-ID 4656 (Open Audit Event) zeichnet der Audit-Datensatz-Ausgang für den alternativen Datenstrom den alternativen Namen des Datenstroms in auf `ObjectName` Tag:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

Bei einer EVTX-ID 4663 (Ereignis „Audit lesen“) zeichnet die Ausgabe des Prüfdatensätzen für denselben alternativen Datenstrom den Namen der Basisdatei in der auf `ObjectName` Markieren Sie jedoch den Griff im `HandleID` Das Tag ist der Griff des alternativen Datenstroms und kann verwendet werden, um dieses Ereignis mit dem alternativen Datenstrom zu korrelieren:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

Es können NFS-Datei- und Verzeichniszugriffe geprüft werden

ONTAP kann bestimmte NFS-Datei- und Verzeichniszugriffe prüfen. Das Wissen, welche Zugriffsereignisse auditiert werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den umgerechneten Audit-Ereignisprotokollen.

Sie können die folgenden NFS-Datei- und Verzeichniszugriffsereignisse prüfen:

- LESEN
- OFFEN
- SCHLIESSEN
- LESDIR
- SCHREIBEN
- SETATTR
- ERSTELLEN
- VERLINKEN
- OPENATTR
- ENTFERNEN
- GETATTR
- VERIFIZIEREN
- NVERIFY
- UMBENENNEN

Um NFS-UMBENENNUNGSEREIGNISSE zuverlässig zu prüfen, sollten Sie Überwachungsaces auf Verzeichnissen statt auf Dateien festlegen, da Dateiberechtigungen nicht auf EINEN UMBENENNUNGSVORGANG überprüft werden, wenn die Verzeichnisberechtigungen ausreichen.

Planen der Überwachungskonfiguration

Bevor Sie das Auditing auf Storage Virtual Machines (SVMs) konfigurieren, müssen Sie wissen, welche Konfigurationsoptionen verfügbar sind, und die Werte planen, die Sie für die einzelnen Optionen festlegen möchten. Diese Informationen können Ihnen dabei helfen, die Prüfungskonfiguration zu konfigurieren, die Ihren geschäftlichen Anforderungen entspricht.

Es gibt bestimmte Konfigurationsparameter, die allen Überwachungskonfigurationen gemeinsam sind.

Darüber hinaus gibt es bestimmte Parameter, mit denen Sie angeben können, welche Methoden beim Drehen der konsolidierten und konvertierten Prüfprotokolle verwendet werden. Sie können eine der drei folgenden Methoden angeben, wenn Sie die Prüfung konfigurieren:

- Drehen Sie Protokolle basierend auf der Protokollgröße

  Dies ist die Standardmethode, mit der Protokolle gedreht werden.

- Protokolle nach einem Zeitplan drehen
- Protokolle nach Protokollgröße und Zeitplan rotieren (je nachdem, welches Ereignis zuerst eintritt)
  F

> Mindestens eine der Methoden für die Protokollrotation sollte immer eingestellt werden.

Gemeinsame Parameter für alle Überwachungskonfigurationen

Es gibt zwei erforderliche Parameter, die Sie beim Erstellen der Überwachungskonfiguration angeben müssen. Sie können außerdem drei optionale Parameter angeben:

Informationstyp	Option	Erforderlich	Einschließlich	Ihre Werte
SVM Name Name der SVM, auf der die Audit-Konfiguration erstellt werden soll. Die SVM muss bereits vorhanden sein.	`-vserver vserver_name`	Ja.	Ja.	

Zielpfad protokollieren Gibt das Verzeichnis an, in dem umgerechnete Audit-Protokolle gespeichert werden, in der Regel ein dediziertes Volume oder qtree. Der Pfad muss im SVM-Namespace bereits vorhanden sein. Der Pfad kann bis zu 864 Zeichen lang sein und muss über Lese-/Schreibberechtigungen verfügen. Wenn der Pfad nicht gültig ist, schlägt der Befehl für die Prüfungskonfiguration fehl. Wenn die SVM eine Disaster-Recovery-Quelle für SVM ist, kann sich der Protokollzielpfad nicht auf dem Root-Volume befinden. Das liegt daran, dass der Root-Volume-Inhalt nicht zum Disaster-Recovery-Ziel repliziert wird. Sie können ein FlexCache-Volume nicht als Protokollziel verwenden (ONTAP 9.7 und höher).	`-destination text`	Ja.	Ja.	

Kategorien von Ereignissen zur Prüfung Gibt die Kategorien von zu prüfenden Ereignissen an. Folgende Ereigniskategorien können geprüft werden: • Dateizugriff (SMB und NFSv4) • SMB-Anmeldung und -Abmeldung • Staging von zentralen Zugriffsrichtlinien Die Staging-Ereignisse für zentrale Zugriffsrichtlinien sind ab Windows 2012 Active Directory-Domänen verfügbar. • Ereignisse in der Kategorie Dateifreigabe • Änderungsereignisse für die Überwachungsrichtlinien • Lokale Benutzerkontenverwaltungsereignisse • Ereignisse für das Management von Sicherheitsgruppen • Änderungsereignisse für die Autorisierungsrichtlinie Der Standardwert ist der Dateizugriff sowie das SMB-Anmelde- und -Abmeldungs -Ereignis. **Hinweis:** bevor Sie angeben können `cap-staging` Als Ereigniskategorie muss auf der SVM ein SMB-Server vorhanden sein. Obwohl Sie die zentrale Zugriffsrichtlinien-Staging in der Überwachungskonfiguration aktivieren können, ohne die dynamische Zugriffskontrolle auf dem SMB-Server zu aktivieren, werden zentrale Zugriffsrichtlinien-Staging-Ereignisse nur erzeugt, wenn Dynamic Access Control aktiviert ist. Die dynamische Zugriffskontrolle wird über eine SMB-Serveroption aktiviert. Sie ist standardmäßig nicht aktiviert.	`-events` {`file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`
`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change`}	Nein

		Ausgabeformat *Log-Datei* Legt das Ausgabeformat der Prüfprotokolle fest. Das Ausgabeformat kann entweder ONTAP-spezifisch sein `XML` Oder Microsoft Windows `EVTX` Protokollformat: Standardmäßig lautet das Ausgabeformat `EVTX`.	`-format` {`xml`	`evtx`}

Nein			*Log-Dateien Rotationsgrenze* Legt fest, wie viele Audit-Log-Dateien gespeichert werden sollen, bevor die älteste Protokolldatei ausgedreht wird. Wenn Sie beispielsweise einen Wert von eingeben `5`, Die letzten fünf Log-Dateien werden beibehalten. Der Wert von `0` Zeigt an, dass alle Protokolldateien aufbewahrt werden. Der Standardwert ist 0.	`-rotate-limit integer`

Parameter, die zur Bestimmung des Drehungswhres von Audit-Ereignisprotokollen verwendet werden

Protokolle auf Basis der Protokollgröße drehen

Standardmäßig werden Auditprotokolle auf der Grundlage der Größe gedreht.

- Die Standard-Protokollgröße beträgt 100 MB
- Wenn Sie die Standard-Protokollrotation-Methode und die Standard-Protokollgröße verwenden möchten, müssen Sie keine spezifischen Parameter für die Protokollrotation konfigurieren.
- Wenn Sie die Prüfprotokolle allein auf Grundlage einer Protokollgröße drehen möchten, können Sie mit dem folgenden Befehl die Einstellung aufheben `-rotate-schedule-minute` Parameter: `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

Wenn Sie die Standardprotokollgröße nicht verwenden möchten, können Sie das konfigurieren `-rotate -size` Parameter zur Angabe einer benutzerdefinierten Protokollgröße:

Informationstyp	Option	Erforderlich	Einschließlich	Ihre Werte
Größe der Protokolldatei Bestimmt die Größenbeschränkung der Prüfprotokoll-Datei.	`-rotate-size` {`integer`[KB MB/GB/TB/PB]}	Nein		

Protokolle nach Zeitplan drehen

Wenn Sie die Prüfprotokolle nach einem Zeitplan drehen möchten, können Sie die Protokollrotation mithilfe der zeitbasierten Rotationsparameter in beliebiger Kombination planen.

- Wenn Sie zeitbasierte Rotation verwenden, wird das angezeigt `-rotate-schedule-minute` Parameter muss angegeben werden.
- Alle anderen zeitbasierten Rotationsparameter sind optional.
- Der Rotationsplan wird unter Verwendung aller zeitbezogenen Werte berechnet.

  Wenn Sie beispielsweise nur die angeben `-rotate-schedule-minute` Parameter, die Audit-Log-Dateien werden auf der Grundlage der Minuten gedreht, die an allen Wochentagen, während aller Stunden an allen Monaten des Jahres angegeben sind.

- Wenn Sie nur einen oder zwei zeitbasierte Rotationsparameter angeben (z. B. `-rotate-schedule -month` Und `-rotate-schedule-minutes`), die Log-Dateien werden basierend auf den Minutenwerten, die Sie an allen Wochentagen, während aller Stunden, aber nur während der angegebenen Monate angegeben.

  Sie können z. B. angeben, dass das Audit-Protokoll in den Monaten Januar, März und August alle Montag, Mittwoch und Samstag um 10:30 Uhr gedreht werden soll

- Wenn Sie Werte für beide angeben `-rotate-schedule-dayofweek` Und `-rotate-schedule-day`, Sie werden unabhängig betrachtet.

  Beispiel: Wenn Sie angeben `-rotate-schedule-dayofweek` Als Freitag und `-rotate-schedule -day` Als 13, dann werden die Audit-Protokolle an jedem Freitag und am 13. Tag des angegebenen Monats gedreht werden, nicht nur an jedem Freitag der 13…

- Wenn Sie die Prüfprotokolle nur nach einem Zeitplan drehen möchten, können Sie mit dem folgenden Befehl die Einstellung aufheben `-rotate-size` Parameter: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

Anhand der folgenden Liste verfügbarer Überwachungsparameter können Sie bestimmen, welche Werte für die Konfiguration eines Zeitplans für die Rotation des Ereignisprotokolls verwendet werden sollen:

Informationstyp	Option	Erforderlich	Einschließlich	Ihre Werte
Drehplan Log: Monat Legt den monatlichen Zeitplan für rotierende Prüfprotokolle fest. Gültige Werte sind `January` Bis `December`, und `all`. Sie können z. B. angeben, dass das Prüfprotokoll in den Monaten Januar, März und August gedreht werden soll.	`-rotate-schedule-month chron_month`	Nein		
Drehplan Log: Wochentag Legt den täglichen Zeitplan (Wochentag) für rotierende Prüfprotokolle fest. Gültige Werte sind `Sunday` Bis `Saturday`, und `all`. Sie können z. B. angeben, dass das Audit-Protokoll dienstags und freitags oder an allen Wochentagen gedreht werden soll.	`-rotate-schedule -dayofweek chron_dayofweek`	Nein		
Drehplan Log: Tag Bestimmt den Tag des Monatsplans für das Drehen des Prüfprotokolls. Gültige Werte reichen von `1` Bis `31`. Sie können z. B. angeben, dass das Audit-Protokoll an den 10. Und 20. Tagen eines Monats oder an allen Tagen eines Monats gedreht werden soll.	`-rotate-schedule-day chron_dayofmonth`	Nein		
Drehplan Log: Stunde Legt den Stundenplan für das Drehen des Prüfprotokolls fest. Gültige Werte reichen von `0` (Mitternacht) bis `23` (11:00 Uhr). Angeben `all` Dreht die Prüfprotokolle jede Stunde. Sie können beispielsweise angeben, dass das Prüfprotokoll um 6 (6 Uhr) und 18 (6 Uhr) gedreht werden soll.	`-rotate-schedule-hour chron_hour`	Nein		

Drehplan Log: Minute Legt den Minutenplan für das Drehen des Prüfprotokolls fest. Gültige Werte reichen von `0` Bis `59`. Sie können z. B. angeben, dass das Prüfprotokoll in der 30. Minute gedreht werden soll.	`-rotate-schedule-minute chron_minute`	Ja, wenn Sie eine planbasierte Protokollrotation konfigurieren, andernfalls Nein		

Rundprotokolle basierend auf Loggröße und Zeitplan drehen

Sie können wählen, ob Sie die Protokolldateien basierend auf der Protokollgröße und einem Zeitplan drehen möchten, indem Sie die beiden festlegen `-rotate-size` Parameter und die zeitbasierten Rotationsparameter in beliebiger Kombination. Beispiel: Wenn `-rotate-size` Ist auf 10 MB und eingestellt `-rotate-schedule -minute` Ist auf 15 gesetzt, drehen sich die Protokolldateien, wenn die Protokolldateigröße 10 MB oder in der 15. Minute jeder Stunde (je nachdem, welches Ereignis zuerst eintritt) erreicht.

Erstellen einer Datei- und Verzeichnisüberprüfung auf SVMs

Erstellen Sie die Überwachungskonfiguration

Das Erstellen einer Datei- und Verzeichnisüberwachung auf Ihrer Storage Virtual Machine (SVM) umfasst die Analyse der verfügbaren Konfigurationsoptionen, die Planung der Konfiguration und die Konfiguration sowie die Aktivierung der Konfiguration. Sie können dann Informationen zur Überwachungskonfiguration anzeigen, um zu bestätigen, dass die resultierende Konfiguration die gewünschte Konfiguration ist.

Bevor Sie mit dem Auditing von Datei- und Verzeichnisereignissen beginnen können, müssen Sie eine Auditing-Konfiguration auf der Storage Virtual Machine (SVM) erstellen.

Bevor Sie beginnen

Wenn Sie eine Auditing-Konfiguration für zentrale Zugriffsrichtlinien-Staging erstellen möchten, muss auf der SVM ein SMB-Server vorhanden sein.

- Obwohl Sie die zentrale Zugriffsrichtlinien-Staging in der Überwachungskonfiguration aktivieren können, ohne die dynamische Zugriffskontrolle auf dem SMB-Server zu aktivieren, werden zentrale Zugriffsrichtlinien-Staging-Ereignisse nur erzeugt, wenn Dynamic Access Control aktiviert ist.

  Die dynamische Zugriffskontrolle wird über eine SMB-Serveroption aktiviert. Sie ist standardmäßig nicht aktiviert.

- Wenn die Argumente eines Feldes in einem Befehl ungültig sind, z. B. ungültige Einträge für Felder, doppelte Einträge und nicht vorhandene Einträge, dann schlägt der Befehl vor der Audit-Phase fehl.

  Solche Fehler erzeugen keinen Audit-Datensatz.

Über diese Aufgabe

Wenn die SVM eine SVM Disaster-Recovery-Quelle ist, kann sich der Zielpfad nicht auf dem Root-Volume befinden.

Schritt

1. Erstellen Sie mithilfe der Informationen im Planungsarbeitsblatt die Überwachungskonfiguration, um Prüfprotokolle auf der Grundlage der Protokollgröße oder eines Zeitplans zu drehen:

Wenn Sie die Prüfprotokolle drehen möchten, um…	Eingeben…
Protokollgröße	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
Einen Zeitplan	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

Beispiele

Im folgenden Beispiel wird eine Überwachungskonfiguration erstellt, die Dateivorgänge und SMB-Anmelde- und -Abmeldungsereignisse (Standard) anhand der größenbasierten Rotation prüft. Das Protokollformat lautet `EVTX` (Standardeinstellung). Die Protokolle werden im gespeichert `/audit_log` Verzeichnis. Die maximale Größe der Protokolldatei ist `200 MB`. Die Protokolle werden gedreht, wenn sie eine Größe von 200 MB erreichen:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

Im folgenden Beispiel wird eine Überwachungskonfiguration erstellt, die Dateivorgänge und SMB-Anmelde- und -Abmeldungsereignisse (Standard) anhand der größenbasierten Rotation prüft. Das Protokollformat lautet `EVTX` (Standardeinstellung). Die Protokolle werden im gespeichert `/cifs_event_logs` Verzeichnis. Die maximale Größe der Protokolldatei ist `100 MB` (Die Standardeinstellung), und die Protokollrotationsgrenze ist `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

Im folgenden Beispiel wird eine Audit-Konfiguration erstellt, die Dateivorgänge, CIFS-Anmelde- und

-Abmeldungsereignisse und zentrale Zugriffs- und Staging-Ereignisse anhand zeitbasierter Rotation prüft. Das Protokollformat lautet `EVTX` (Standardeinstellung). Die Prüfprotokolle werden monatlich um 12:30 Uhr gedreht An allen Wochentagen. Die Protokollrotationsgrenze ist `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Prüfung auf SVM aktivieren

Nachdem Sie die Auditing-Konfiguration abgeschlossen haben, müssen Sie das Auditing auf der Storage Virtual Machine (SVM) aktivieren.

Was Sie benötigen

Die SVM-Audit-Konfiguration muss bereits vorhanden sein.

Über diese Aufgabe

Wenn die SVM-Konfiguration für Disaster-Recovery-ID-verwerfen (nach Abschluss der SnapMirror-Initialisierung) und eine Audit-Konfiguration vorhanden ist, deaktiviert ONTAP die Prüfungskonfiguration automatisch. Die Prüfung wird auf der schreibgeschützten SVM deaktiviert, um zu verhindern, dass die Staging-Volumes gefüllt werden. Sie können das Auditing nur aktivieren, wenn die SnapMirror Beziehung beschädigt ist und die SVM Lese-/Schreibzugriff ist.

Schritt

1. Prüfung auf der SVM aktivieren:

   ```
   vserver audit enable -vserver vserver_name
   ```

   ```
   vserver audit enable -vserver vs1
   ```

Überprüfen Sie die Überwachungskonfiguration

Nach Abschluss der Überwachungskonfiguration sollten Sie überprüfen, ob die Prüfung ordnungsgemäß konfiguriert und aktiviert ist.

Schritte

1. Überprüfen Sie die Überwachungskonfiguration:

   ```
   vserver audit show -instance -vserver vserver_name
   ```

   Mit dem folgenden Befehl werden alle Audit-Konfigurationsinformationen für Storage Virtual Machine (SVM) vs1 in Listenform angezeigt:

   ```
   vserver audit show -instance -vserver vs1
   ```

```
                            Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops
                         Log Format: evtx
                 Log File Size Limit: 200MB
       Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
```

Audit-Richtlinien für Dateien und Ordner konfigurieren

Audit-Richtlinien für Dateien und Ordner konfigurieren

Die Implementierung der Prüfung von Datei- und Ordnerzugriffsereignissen ist ein zweistufiger Prozess. Zunächst müssen Sie eine Audit-Konfiguration auf Storage Virtual Machines (SVMs) erstellen und aktivieren. Zweitens müssen Sie die Audit-Richtlinien für die Dateien und Ordner konfigurieren, die Sie überwachen möchten. Sie können Audit-Richtlinien konfigurieren, um sowohl erfolgreiche als auch fehlgeschlagene Zugriffsversuche zu überwachen.

Sie können sowohl SMB- als auch NFS-Audit-Richtlinien konfigurieren. Audit-Richtlinien für SMB und NFS gelten für unterschiedliche Konfigurationsanforderungen und Audit-Funktionen.

Wenn die entsprechenden Audit-Richtlinien konfiguriert sind, überwacht ONTAP die SMB- und NFS-Zugriffsereignisse wie in den Audit-Richtlinien festgelegt, nur wenn SMB- oder NFS-Server ausgeführt werden.

Konfigurieren Sie die Audit-Richtlinien für Dateien und Verzeichnisse im NTFS-Sicherheitsstil

Bevor Sie Vorgänge in Dateien und Verzeichnissen prüfen können, müssen Sie die Überwachungsrichtlinien für die Dateien und Verzeichnisse konfigurieren, für die Sie Audit-Informationen erfassen möchten. Dies ist zusätzlich zur Einrichtung und Aktivierung der Audit-Konfiguration. Sie können NTFS-Audit-Richtlinien über die Registerkarte Windows-Sicherheit oder über die ONTAP-CLI konfigurieren.

Konfigurieren von NTFS-Audit-Richtlinien über die Registerkarte Windows-Sicherheit

Sie können NTFS-Audit-Richtlinien für Dateien und Verzeichnisse über die Registerkarte **Windows Security** im Fenster Windows-Eigenschaften konfigurieren. Dies ist die gleiche Methode, die bei der Konfiguration von Audit-Richtlinien für Daten auf einem Windows-Client verwendet wird. Auf diese Weise können Sie die gleiche GUI-Schnittstelle verwenden, die Sie gewohnt sind.

Was Sie benötigen

Das Auditing muss auf der Storage Virtual Machine (SVM) konfiguriert werden, die die Daten enthält, auf die Sie Systemzugriffssteuerungslisten (SACLs) anwenden.

Über diese Aufgabe

Das Konfigurieren von NTFS-Audit-Richtlinien erfolgt durch Hinzufügen von Einträgen zu NTFS-SACLs, die mit einem NTFS-Sicherheitsdeskriptor verknüpft sind. Der Sicherheitsdeskriptor wird dann auf NTFS-Dateien und -Verzeichnisse angewendet. Diese Aufgaben werden automatisch von der Windows GUI übernommen. Der Sicherheitsdeskriptor kann Discretionary Access Control Lists (DACLs) zum Anwenden von Datei- und Ordnerzugriffsberechtigungen, SACLs für Datei- und Ordnerprüfung oder SACLs und DACLs enthalten.

Führen Sie die folgenden Schritte auf einem Windows-Host aus, um NTFS-Audit-Richtlinien über die Registerkarte Windows-Sicherheit festzulegen:

Schritte

1. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
2. Füllen Sie die Box * Map Network Drive* aus:

   a. Wählen Sie einen **Drive**-Buchstaben aus.

   b. Geben Sie im Feld **Ordner** den SMB-Servernamen ein, der die Freigabe enthält und die zu prüfenden Daten sowie den Namen der Freigabe enthält.

      Sie können anstelle des SMB-Servernamens die IP-Adresse der Datenschnittstelle für den SMB-Server angeben.

      Wenn der Name Ihres SMB-Servers „`SMB_SERVER`“ lautet und Ihre Freigabe den Namen „`share1`“ hat, sollten Sie eingeben `\\SMB_SERVER\share1`.

   c. Klicken Sie Auf **Fertig Stellen**.

   Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

3. Wählen Sie die Datei oder das Verzeichnis aus, für die Sie den Audit-Zugriff aktivieren möchten.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis, und wählen Sie dann **Eigenschaften** aus.
5. Wählen Sie die Registerkarte **Sicherheit**.
6. Klicken Sie Auf **Erweitert**.
7. Wählen Sie die Registerkarte **Revision** aus.
8. Führen Sie die gewünschten Aktionen aus:

Wenn Sie… wollen	Gehen Sie wie folgt vor
Einrichten der Prüfung für einen neuen Benutzer oder eine neue Gruppe	a. Klicken Sie Auf **Hinzufügen**. b. Geben Sie in das Feld Objektnamen eingeben, um auszuwählen, den Namen des Benutzers oder der Gruppe ein, den Sie hinzufügen möchten. c. Klicken Sie auf **OK**.

Audit von einem Benutzer oder einer Gruppe entfernen	a. Wählen Sie im Feld Objektnamen eingeben den Benutzer oder die Gruppe aus, die Sie entfernen möchten. b. Klicken Sie Auf **Entfernen**. c. Klicken Sie auf **OK**. d. Überspringen Sie den Rest dieses Verfahrens.
Ändern Sie die Prüfung für einen Benutzer oder eine Gruppe	a. Wählen Sie im Feld Objektnamen eingeben den Benutzer oder die Gruppe aus, die Sie ändern möchten. b. Klicken Sie Auf **Bearbeiten**. c. Klicken Sie auf **OK**.

Wenn Sie eine Prüfung für einen Benutzer oder eine Gruppe einrichten oder die Prüfung für einen vorhandenen Benutzer oder eine vorhandene Gruppe ändern, wird das Feld Überwachungseintrag für <Object> geöffnet.

9. Wählen Sie im Feld **Apply to** aus, wie Sie diesen Prüfungseintrag anwenden möchten.

   Sie können eine der folgenden Optionen auswählen:

   - **Dieser Ordner, Unterordner und Dateien**
   - **Dieser Ordner und Unterordner**
   - **Nur dieser Ordner**
   - **Dieser Ordner und die Dateien**
   - **Nur Unterordner und Dateien**
   - **Nur Unterordner**
   - **Nur Dateien** Wenn Sie eine Prüfung auf eine einzelne Datei einrichten, ist die Box **Apply to** nicht aktiv. Die Einstellung **auf** anwenden ist standardmäßig auf **nur dieses Objekt** eingestellt.

   > Da durch das Auditing SVM-Ressourcen belegt werden, wählen Sie nur die minimale Stufe aus, die die Auditing-Ereignisse erfüllt, die Ihre Sicherheitsanforderungen erfüllen.

10. Wählen Sie im Feld **Zugriff** aus, was geprüft werden soll und ob erfolgreiche Ereignisse, Fehlereignisse oder beides geprüft werden sollen.
    - Wenn erfolgreiche Ereignisse geprüft werden sollen, wählen Sie das Feld Erfolg aus.
    - Um Fehlerereignisse zu überwachen, wählen Sie das Feld Fehler aus.

      Wählen Sie nur die Aktionen aus, die Sie überwachen müssen, um Ihre Sicherheitsanforderungen zu erfüllen. Weitere Informationen zu diesen prüffähigen Ereignissen finden Sie in Ihrer Windows-Dokumentation. Sie können die folgenden Ereignisse prüfen:

    - **Volle Kontrolle**
    - **Traverse Ordner / Datei ausführen**
    - **Ordner auflisten / Daten lesen**
    - **Attribute lesen**
    - **Erweiterte Attribute lesen**

- **Dateien erstellen / Daten schreiben**
- **Ordner erstellen / Daten anhängen**
- **Attribute schreiben**
- **Erweiterte Attribute schreiben**
- **Löschen von Unterordnern und Dateien**
- **Löschen**
- **Berechtigungen lesen**
- **Berechtigungen ändern**
- **Besitzrechte übernehmen**

11. Wenn Sie nicht möchten, dass sich die Überwachungseinstellung auf nachfolgende Dateien und Ordner des ursprünglichen Containers verbreitet, wählen Sie die Option **Diese Überwachungseinträge auf Objekte und/oder Container innerhalb dieses Containers only** anwenden aus.
12. Klicken Sie Auf **Anwenden**.
13. Klicken Sie nach dem Hinzufügen, Entfernen oder Bearbeiten von Prüfungseinträgen auf **OK**.

    Das Feld Überwachungseintrag für <Object> wird geschlossen.

14. Wählen Sie im Feld **Revision** die Vererbungseinstellungen für diesen Ordner aus.

    Wählen Sie nur die minimale Stufe aus, die die Überwachungsereignisse enthält, die Ihren Sicherheitsanforderungen entsprechen. Sie können eine der folgenden Optionen auswählen:

    - Wählen Sie aus dem übergeordneten Feld dieses Objekts die Option vererbbare Überwachungseinträge einschließen aus.
    - Wählen Sie das Kontrollkästchen Alle bestehenden vererbbaren Überwachungseinträge für alle abhängigen Elemente durch vererbbare Prüfeinträge aus diesem Objekt ersetzen aus.
    - Wählen Sie beide Felder aus.
    - Wählen Sie keine der Kontrollkästchen aus. Wenn Sie SACLs auf eine einzelne Datei setzen, ist das Ersetzen aller vorhandenen vererbbaren Überwachungseinträge auf allen Nachkommen durch vererbbare Prüfeinträge aus diesem Objektfeld nicht im Feld Auditing vorhanden.

15. Klicken Sie auf **OK**.

    Das Feld Auditing wird geschlossen.

Konfigurieren Sie die NTFS-Audit-Richtlinien mithilfe der ONTAP-CLI

Über die ONTAP-Befehlszeilenschnittstelle können Sie die Audit-Richtlinien für Dateien und Ordner konfigurieren. So können Sie NTFS-Audit-Richtlinien konfigurieren, ohne dass eine Verbindung zu den Daten über eine SMB-Freigabe auf einem Windows-Client hergestellt werden muss.

Sie können NTFS-Audit-Richtlinien mit konfigurieren `vserver security file-directory` Befehlsfamilie.

Sie können NTFS SACLs nur mit der CLI konfigurieren. Das Konfigurieren von NFSv4 SACLs wird von dieser ONTAP-Befehlfamilie nicht unterstützt. Weitere Informationen über die Verwendung dieser Befehle zum Konfigurieren und Hinzufügen von NTFS-SACLs zu Dateien und Ordnern finden Sie auf den man-Pages.

Konfigurieren Sie Auditing für Dateien und Verzeichnisse im UNIX-Sicherheitsstil

Sie konfigurieren Audit für Dateien und Verzeichnisse im UNIX-Sicherheitsstil durch Hinzufügen von Audit ACLs zu NFSv4.x ACLs. So können Sie bestimmte NFS-Datei- und Verzeichniszugriffe zu Sicherheitszwecken überwachen.

Über diese Aufgabe

Für NFSv4.x sind Ermessenswert- und SystemAsse in derselben ACL gespeichert. Sie werden nicht in separaten DACLs und SACLs gespeichert. Daher müssen Sie beim Hinzufügen von Audit Aces zu einer vorhandenen ACL Vorsicht walten lassen, um zu vermeiden, dass eine vorhandene ACL überschrieben und verloren geht. Die Reihenfolge, in der Sie die Audit Aces zu einer bestehenden ACL hinzufügen, ist nicht von Bedeutung.

Schritte

1. Rufen Sie die vorhandene ACL für die Datei oder das Verzeichnis mithilfe von ab `nfs4_getfacl` Oder gleichwertiger Befehl.

   Weitere Informationen zum Bearbeiten von ACLs finden Sie in den man-Pages des NFS-Clients.

2. Fügen Sie die gewünschten Audit Aces hinzu.
3. Wenden Sie die aktualisierte ACL mithilfe des auf die Datei oder das Verzeichnis an `nfs4_setfacl` Oder gleichwertiger Befehl.

Informationen über auf Dateien und Verzeichnisse angewandte Audit-Richtlinien anzeigen

Zeigen Sie Informationen über Überwachungsrichtlinien mithilfe der Registerkarte Windows-Sicherheit an

Sie können Informationen zu Audit-Richtlinien anzeigen, die auf Dateien und Verzeichnisse angewendet wurden, indem Sie die Registerkarte Sicherheit im Fenster Windows-Eigenschaften verwenden. Das ist dieselbe Methode für Daten auf einem Windows Server, mit der Kunden dieselbe Benutzeroberfläche nutzen können, die sie bereits kennen.

Über diese Aufgabe

Durch das Anzeigen von Informationen über Überwachungsrichtlinien, die auf Dateien und Verzeichnisse angewendet werden, können Sie überprüfen, ob die entsprechenden SACLs (System Access Control Lists) für bestimmte Dateien und Ordner festgelegt sind.

Führen Sie die folgenden Schritte auf einem Windows-Host aus, um Informationen über SACLs anzuzeigen, die auf NTFS-Dateien und -Ordner angewendet wurden.

Schritte

1. Wählen Sie im Menü **Tools** im Windows Explorer die Option **Netzwerklaufwerk zuordnen** aus.
2. Füllen Sie das Dialogfeld **Map Network Drive** aus:

   a. Wählen Sie einen **Drive**-Buchstaben aus.

   b. Geben Sie im Feld **Ordner** die IP-Adresse oder den Namen des SMB-Servers der virtuellen Speichermaschine (SVM) ein, die den Share enthält, der sowohl die zu prüfenden Daten als auch den

Namen der Freigabe enthält.

Wenn der Name Ihres SMB-Servers „`SMB_SERVER`“ lautet und Ihre Freigabe den Namen „`share1`“ hat, sollten Sie eingeben `\\SMB_SERVER\share1`.

> Sie können anstelle des SMB-Servernamens die IP-Adresse der Datenschnittstelle für den SMB-Server angeben.

c. Klicken Sie Auf **Fertig Stellen**.

Das ausgewählte Laufwerk ist mit dem Windows Explorer-Fenster verbunden und bereit, in dem die Dateien und Ordner in der Freigabe angezeigt werden.

3. Wählen Sie die Datei oder das Verzeichnis aus, für das Sie Audit-Informationen anzeigen.
4. Klicken Sie mit der rechten Maustaste auf die Datei oder das Verzeichnis, und wählen Sie **Eigenschaften**.
5. Wählen Sie die Registerkarte **Sicherheit**.
6. Klicken Sie Auf **Erweitert**.
7. Wählen Sie die Registerkarte **Revision** aus.
8. Klicken Sie Auf **Weiter**.

   Das Feld Auditing wird geöffnet. Das Feld * Revisionseinträge* zeigt eine Zusammenfassung von Benutzern und Gruppen an, deren SACLs auf sie angewendet wurden.

9. Wählen Sie im Feld * Überwachungseinträge* den Benutzer oder die Gruppe aus, deren SACL-Einträge angezeigt werden sollen.
10. Klicken Sie Auf **Bearbeiten**.

    Der Überwachungseintrag für <object> wird geöffnet.

11. Zeigen Sie im Feld **Zugriff** die aktuellen SACLs an, die auf das ausgewählte Objekt angewendet werden.
12. Klicken Sie auf **Abbrechen**, um das Feld **Prüfeintrag für <Object>** zu schließen.
13. Klicken Sie auf **Abbrechen**, um das Feld **Revision** zu schließen.

Zeigt Informationen zu NTFS-Audit-Richtlinien auf FlexVol-Volumes mithilfe der CLI an

Sie können Informationen zu NTFS-Audit-Richtlinien auf FlexVol Volumes anzeigen, einschließlich der Sicherheitsstile und effektiven Sicherheitsstile, der angewandten Berechtigungen und Informationen zu Zugriffssteuerungslisten des Systems. Sie können die Informationen zur Überprüfung der Sicherheitskonfiguration oder zur Fehlerbehebung bei Audit-Problemen verwenden.

Über diese Aufgabe

Durch das Anzeigen von Informationen über Überwachungsrichtlinien, die auf Dateien und Verzeichnisse angewendet werden, können Sie überprüfen, ob die entsprechenden SACLs (System Access Control Lists) für bestimmte Dateien und Ordner festgelegt sind.

Sie müssen den Namen der Storage Virtual Machine (SVM) und den Pfad zu den Dateien oder Ordnern angeben, deren Audit-Informationen angezeigt werden sollen. Sie können die Ausgabe als Übersichtsformular oder als detaillierte Liste anzeigen.

- Bei NTFS-Volumes und qtrees werden für Audit-Richtlinien nur NTFS-Systemzugriffssteuerungslisten (SACLs) verwendet.
- Dateien und Ordner in einem gemischten Security-Stil-Volume mit NTFS effektive Sicherheit können NTFS-Audit-Richtlinien auf sie angewendet werden.

  Gemischte sicherheitsrelevante Volumes und qtrees können einige Dateien und Verzeichnisse enthalten, die UNIX-Dateiberechtigungen verwenden, entweder Modus-Bits oder NFSv4-ACLs und einige Dateien und Verzeichnisse, die NTFS-Dateiberechtigungen verwenden.

- Die oberste Ebene eines gemischten Security-Volumes kann entweder UNIX oder NTFS effektive Sicherheit haben und möglicherweise NTFS SACLs enthalten.
- Da die Sicherheit des Storage-Level Access Guard auf einem Volume oder qtree mit gemischtem Sicherheitsstil konfiguriert werden kann, selbst wenn der effektive Sicherheitsstil des Volume Root oder qtree UNIX ist, Die Ausgabe für einen Volume- oder qtree-Pfad, wo Storage-Level Access Guard konfiguriert ist, zeigt möglicherweise sowohl normale Datei als auch Ordner NFSv4 SACLs und Storage-Level Access Guard NTFS SACLs an.
- Wenn der im Befehl eingegebene Pfad zu Daten mit NTFS-effektiver Sicherheit besteht, zeigt die Ausgabe auch Informationen über Dynamic Access Control Aces an, wenn Dynamic Access Control für den angegebenen Datei- oder Verzeichnispfad konfiguriert ist.
- Wenn Sicherheitsinformationen über Dateien und Ordner mit NTFS-effektiver Sicherheit angezeigt werden, enthalten UNIX-bezogene Ausgabefelder nur Informationen über die Berechtigung von UNIX-Dateien.

  NTFS-Dateien und -Ordner verwenden bei der Ermittlung der Zugriffsrechte auf Dateien nur NTFS-Dateiberechtigungen und Windows-Benutzer und -Gruppen.

- Die ACL-Ausgabe wird nur für Dateien und Ordner mit NTFS- oder NFSv4-Sicherheit angezeigt.

  Dieses Feld ist leer für Dateien und Ordner, die UNIX-Sicherheit verwenden, die nur Modus-Bit-Berechtigungen angewendet haben (keine NFSv4 ACLs).

- Die Felder „Eigentümer“ und „Gruppenausgabe“ in der ACL-Ausgabe gelten nur bei NTFS-Sicherheitsdeskriptoren.

Schritt

1. Anzeige von Datei- und Verzeichnisaudits-Einstellungen mit der gewünschten Detailebene:

Informationen anzeigen…	Geben Sie den folgenden Befehl ein…
In zusammengefassener Form	`vserver security file-directory show -vserver vserver_name -path path`
Als detaillierte Liste	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Beispiele

Im folgenden Beispiel werden die Informationen zu den Überwachungsrichtlinien für den Pfad angezeigt `/corp` In SVM vs1. Der Pfad verfügt über NTFS effektive Sicherheit. Der NTFS-Sicherheitsdeskriptor enthält sowohl einen ERFOLG als auch einen SACL-Eintrag FÜR ERFOLG/FEHLER.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Im folgenden Beispiel werden die Informationen zu den Überwachungsrichtlinien für den Pfad angezeigt `/datavol1` In SVM vs1. Der Pfad enthält sowohl normale Datei- als auch Ordner-SACLs und Speicher-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Möglichkeiten zum Anzeigen von Informationen über Dateisicherheitsrichtlinien und Audit-Richtlinien

Mithilfe des Platzhalterzeichens (*) können Sie Informationen über Dateisicherheit und Audit-Richtlinien aller Dateien und Verzeichnisse unter einem bestimmten Pfad oder

einem Root-Volume anzeigen.

Das Platzhalterzeichen (*) kann als letzte Unterkomponente eines bestimmten Verzeichnispfades verwendet werden, unter dem Sie Informationen zu allen Dateien und Verzeichnissen anzeigen möchten.

Wenn Sie Informationen zu einer bestimmten Datei oder einem Verzeichnis mit dem Namen „*“ anzeigen möchten, müssen Sie den vollständigen Pfad innerhalb doppelter Anführungszeichen („ “) angeben.

Beispiel

Mit dem folgenden Befehl mit dem Platzhalterzeichen werden die Informationen über alle Dateien und Verzeichnisse unter dem Pfad angezeigt `/1/` Von SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                   Vserver: vs1
                 File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                   Vserver: vs1
                 File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

Mit dem folgenden Befehl werden Informationen zu einer Datei mit dem Namen „*“ unter dem Pfad angezeigt `/vol1/a` Von SVM vs1. Der Pfad ist in doppelte Anführungszeichen eingeschlossen (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: “/vol1/a/*”
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Änderungsereignisse in der CLI, die geprüft werden können

Änderungsereignisse in der CLI, die geprüft werden können, Übersicht

ONTAP kann bestimmte CLI-Änderungsereignisse prüfen, darunter bestimmte SMB-Share-Ereignisse, bestimmte Audit-Richtlinienereignisse, bestimmte lokale Ereignisse von Sicherheitsgruppen, Ereignisse lokaler Benutzergruppen und Autorisierungsrichtlinien. Das Verständnis, welche Änderungsereignisse überprüft werden können, ist hilfreich bei der Interpretation der Ergebnisse aus den Ereignisprotokollen.

Sie können die Ereignisse, die auf einer Storage Virtual Machine (SVM) stattfinden, verwalten, indem Sie die Überwachungsprotokolle manuell drehen, die Prüfung aktivieren oder deaktivieren, Informationen über das Auditing von Änderungsereignissen anzeigen, Änderungsereignisse für das Auditing ändern und Änderungsereignisse für das Auditing löschen.

Wenn Sie als Administrator einen beliebigen Befehl zum Ändern der Konfiguration in Bezug auf SMB-Share, lokale Benutzergruppe, lokale Sicherheitsgruppe, Autorisierungsrichtlinie und Ereignis für Prüfrichtlinien ausführen, Ein Datensatz erzeugt und das entsprechende Ereignis wird auditiert:

Kategorie „Audits“	Veranstaltungen	Ereignis-IDs	Führen Sie diesen Befehl aus…

Mhost Auditing	Richtlinienänderung	[4719] Audit-Konfiguration geändert	`vserver audit disable
enable	modify`	Dateifreigabe	[5142] Netzwerkfreigabe wurde hinzugefügt
`vserver cifs share create`	[5143] Netzwerkfreigabe wurde geändert	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] Netzwerkfreigabe gelöscht	`vserver cifs share delete`
Prüfung	Benutzerkonto	[4720] lokaler Benutzer erstellt	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] lokaler Benutzer aktiviert	`vserver cifs users-and-groups local-user create	modify`	[4724] Zurücksetzen des lokalen Benutzerpassworts
`vserver cifs users-and-groups local-user set-password`	[4725] lokaler Benutzer deaktiviert	`vserver cifs users-and-groups local-user create	modify`
[4726] lokaler Benutzer gelöscht	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] Lokale Benutzeränderung	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] lokaler Benutzer umbenennen	`vserver cifs users-and-groups local-user rename`	Sicherheitsgruppe	[4731] Lokale Sicherheitsgruppe erstellt
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] Lokale Sicherheitsgruppe gelöscht	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] Lokale Sicherheitsgruppe Geändert

`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] Benutzer zur lokalen Gruppe hinzugefügt	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`
[4733] Benutzer aus der lokalen Gruppe entfernt	`vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser`	Änderung der Autorisierungsrichtlinie	[4704] Benutzerrechte Zugewiesen
`vserver cifs users-and-groups privilege add-privilege`	[4705] Benutzerrechte Entfernt	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

Dateifreigabe-Ereignisse verwalten

Wenn ein Dateifreigabe-Ereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert. Die Dateifreigabe-Ereignisse werden generiert, wenn die SMB-Netzwerkfreigabe mit geändert wird `vserver cifs share` Ähnliche Befehle.

Die Dateifreigabe-Ereignisse mit den Ereignis-ids 5142, 5143 und 5144 werden generiert, wenn eine SMB-Netzwerkfreigabe für die SVM hinzugefügt, geändert oder gelöscht wird. Die Konfiguration der SMB-Netzwerkfreigabe wird mithilfe des geändert `cifs share access control create|modify|delete` Befehle.

Im folgenden Beispiel wird ein Dateifreigabe-Ereignis mit der ID 5143 erzeugt, wenn ein Freigabetobjekt namens 'Audit_dest' erstellt wird:

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

Management von Änderungs- und Audit-Richtlinien

Wenn ein Ereignis für die Änderung von Audit-Richtlinien für eine Storage Virtual Machine (SVM) konfiguriert und ein Audit aktiviert ist, werden Audit-Ereignisse generiert. Die Ereignisse der Revisionspolitik-Änderung werden generiert, wenn eine Audit-Richtlinie mit geändert wird `vserver audit` Ähnliche Befehle.

Das Ereignis „Audit-Policy-change“ mit der Ereignis Event-id 4719 wird immer dann generiert, wenn eine Audit-Richtlinie deaktiviert, aktiviert oder geändert wird. Außerdem wird festgestellt, wann ein Benutzer versucht, die Prüfung für die Tracks zu deaktivieren. Er ist standardmäßig konfiguriert und erfordert zum Deaktivieren Diagnoseberechtigung.

Im folgenden Beispiel wird ein Änderungsereignis für die Audit-Richtlinie mit der generierten ID 4719 angezeigt, wenn ein Audit deaktiviert ist:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

Verwalten von Benutzerkontenereignis

Wenn ein Benutzerkontenereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert.

Ereignisse des Benutzerkontos mit Event-ids 4720, 4722, 4724, 4725, 4726 4738 und 4781 werden generiert, wenn ein lokaler SMB- oder NFS-Benutzer aus dem System erstellt oder gelöscht wird, ein lokales Benutzerkonto ist aktiviert, deaktiviert oder geändert und das lokale SMB-Benutzerpasswort wird zurückgesetzt oder geändert. Die Benutzerkontoereignisse werden generiert, wenn ein Benutzerkonto mit geändert wird `vserver cifs users-and-groups <local user>` Und `vserver services name-service <unix user>` Befehle.

Im folgenden Beispiel wird ein Benutzerkontoereignis mit der ID 4720 angezeigt, das beim Erstellen eines lokalen SMB-Benutzers generiert wurde:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

Im folgenden Beispiel wird ein Benutzerkontoereignis mit der anhand der ID 4781 erstellten ID angezeigt, wenn der im vorhergehenden Beispiel erstellte lokale SMB-Benutzer umbenannt wird:

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

Verwalten von Sicherheitsereignisereignis

Wenn ein Sicherheitsereignis für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert.

Die Ereignisse der Sicherheitsgruppe mit Ereignis-ids 4731, 4732, 4733, 4734 und 4735 werden generiert, wenn eine lokale SMB- oder NFS-Gruppe aus dem System erstellt oder gelöscht wird und der lokale Benutzer aus der Gruppe hinzugefügt oder entfernt wird. Die Ereignisse der Sicherheitsgruppe werden generiert, wenn ein Benutzerkonto mit geändert wird `vserver cifs users-and-groups <local-group>` Und `vserver services name-service <unix-group>` Befehle.

Im folgenden Beispiel wird ein Ereignis der Sicherheitsgruppe mit der generierten ID 4731 angezeigt, wenn eine lokale UNIX-Sicherheitsgruppe erstellt wird:

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

Management von Berechtigungs- und Richtlinienänderungen

Wenn ein Ereignis zur Änderung von Autorisierungsrichtlinien für eine Storage Virtual Machine (SVM) konfiguriert ist und ein Audit aktiviert ist, werden Audit-Ereignisse generiert.

Die Ereignisse mit den Ereignis-ids 4704 und 4705 werden generiert, sobald die Autorisierungsrechte für einen SMB-Benutzer und eine SMB-Gruppe erteilt oder widerrufen werden. Die Ereignisse zur Änderung der Autorisierungsrichtlinie werden generiert, wenn die Autorisierungsrechte mit zugewiesen oder widerrufen werden `vserver cifs users-and-groups privilege` Ähnliche Befehle.

Im folgenden Beispiel wird ein Ereignis für die Autorisierungsrichtlinie mit der generierten ID 4704 angezeigt, wenn die Autorisierungsrechte für eine SMB-Benutzergruppe zugewiesen sind:

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

Management von Audit-Konfigurationen

Drehen Sie die Überwachungsprotokolle manuell

Bevor Sie die Protokolle der Audit-Ereignisse anzeigen können, müssen die Protokolle in benutzerlesbare Formate konvertiert werden. Wenn Sie die Ereignisprotokolle für eine bestimmte Storage Virtual Machine (SVM) anzeigen möchten, bevor ONTAP das Protokoll automatisch rotiert, können Sie die Überwachungsprotokolle auf einer SVM manuell drehen.

Schritt

1. Drehen Sie die Überwachungsprotokolle mit dem `vserver audit rotate-log` Befehl.

   ```
   vserver audit rotate-log -vserver vs1
   ```

   Das Revisionsprotokoll wird im SVM-Audit-Ereignisprotokoll mit dem von der Audit-Konfiguration angegebenen Format gespeichert (`XML` Oder `EVTX`), und kann mit der entsprechenden Anwendung angezeigt werden.

Aktivieren und Deaktivieren der Prüfung auf SVMs

Sie können die Überprüfung auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Möglicherweise möchten Sie die Datei- und Verzeichnisüberprüfung vorübergehend beenden, indem Sie die Prüfung deaktivieren. Sie können die Prüfung jederzeit aktivieren (falls eine Überwachungskonfiguration vorhanden ist).

Was Sie benötigen

Bevor Sie Auditing auf der SVM aktivieren können, muss die Auditing-Konfiguration der SVM bereits

vorhanden sein.

"Erstellen Sie die Überwachungskonfiguration"

Über diese Aufgabe

Durch Deaktivieren der Prüfung wird die Konfiguration der Prüfung nicht gelöscht.

Schritte

1. Führen Sie den entsprechenden Befehl aus:

Wenn Prüfung ausgeführt werden soll…	Geben Sie den Befehl ein…
Aktiviert	`vserver audit enable -vserver vserver_name`
Deaktiviert	`vserver audit disable -vserver vserver_name`

2. Überprüfen Sie, ob die Prüfung den gewünschten Status hat:

   ```
   vserver audit show -vserver vserver_name
   ```

Beispiele

Das folgende Beispiel ermöglicht das Auditing von SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

Im folgenden Beispiel wird das Auditing von SVM vs1 deaktiviert:

```
cluster1::> vserver audit disable -vserver vs1

                              Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                   Rotation Schedules: -
            Log Files Rotation Limit: 10
```

Zeigt Informationen zu Überwachungskonfigurationen an

Sie können Informationen zu Überwachungskonfigurationen anzeigen. Diese Informationen unterstützen Sie bei der Ermittlung der gewünschten Konfiguration für die jeweilige SVM. Mit den angezeigten Informationen können Sie auch überprüfen, ob eine Überwachungskonfiguration aktiviert ist.

Über diese Aufgabe

Sie können ausführliche Informationen zum Auditing von Konfigurationen auf allen SVMs anzeigen oder Sie können durch Angabe optionaler Parameter anpassen, welche Informationen in der Ausgabe angezeigt werden. Wenn Sie keinen der optionalen Parameter angeben, wird Folgendes angezeigt:

- SVM-Name, auf den die Audit-Konfiguration zutrifft
- Der Prüfstatus, der sein kann `true` Oder `false`

  Wenn der Prüfstatus lautet `true`, Prüfung ist aktiviert. Wenn der Prüfstatus lautet `false`, Prüfung ist deaktiviert.

- Die Kategorien der zu prüfenden Ereignisse
- Das Format des Prüfprotokolls
- Das Zielverzeichnis, in dem das Audit-Subsystem konsolidierte und konvertierte Audit-Protokolle speichert

Schritt

1. Zeigen Sie Informationen über die Überwachungskonfiguration mithilfe des an `vserver audit show` Befehl.

   Weitere Informationen zur Verwendung des Befehls finden Sie in den man-Pages.

Beispiele

Im folgenden Beispiel wird eine Zusammenfassung der Audit-Konfiguration für alle SVMs angezeigt:

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

Im folgenden Beispiel werden alle Audit-Konfigurationsinformationen für alle SVMs in Listenform angezeigt:

```
cluster1::> vserver audit show -instance

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                           Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
```

Befehle zum Ändern von Überwachungskonfigurationen

Wenn Sie eine Überwachungseinstellung ändern möchten, können Sie die aktuelle Konfiguration jederzeit ändern, einschließlich der Änderung des Protokollpfadziels und des Protokollformats, der Änderung der Kategorien von zu prüfenden Ereignissen, der automatischen Speicherung von Protokolldateien und der maximalen Anzahl der zu speicherenden Protokolldateien.

Ihr Ziel ist	Befehl
Ändern Sie den Protokollzielpfad	`vserver audit modify` Mit dem `-destination` Parameter

Ändern Sie die Kategorie der zu prüfenden Ereignisse	`vserver audit modify` Mit dem `-events` Parameter Zur Prüfung von Staging von zentralen Zugriffsrichtlinien muss die SMB-Serveroption Dynamic Access Control (DAC) auf der Storage Virtual Machine (SVM) aktiviert sein.
Ändern Sie das Protokollformat	`vserver audit modify` Mit dem `-format` Parameter
Aktivieren von automatischen Speichern basierend auf der internen Protokolldateigröße	`vserver audit modify` Mit dem `-rotate-size` Parameter
Durch Aktivieren der automatischen Einsparung auf Basis eines Zeitintervalls	`vserver audit modify` Mit dem `-rotate -schedule-month`, `-rotate-schedule -dayofweek`, `-rotate-schedule-day`, `-rotate -schedule-hour`, und `-rotate-schedule -minute` Parameter
Festlegen der maximalen Anzahl von gespeicherten Protokolldateien	`vserver audit modify` Mit dem `-rotate-limit` Parameter

Löschen einer Überwachungskonfiguration

Wenn Datei- und Verzeichnisereignisse für die Storage Virtual Machine (SVM) nicht mehr geprüft und keine Auditing-Konfiguration auf der SVM beibehalten werden soll, können Sie die Audit-Konfiguration löschen.

Schritte

1. Deaktivieren der Überwachungskonfiguration:

   ```
   vserver audit disable -vserver vserver_name
   ```

   ```
   vserver audit disable -vserver vs1
   ```

2. Löschen Sie die Überwachungskonfiguration:

   ```
   vserver audit delete -vserver vserver_name
   ```

   ```
   vserver audit delete -vserver vs1
   ```

Auswirkungen des Zurücks des Clusters benennen

Wenn Sie den Cluster zurücksetzen möchten, sollten Sie auf den ONTAP für den Umkehrprozess achten, wenn es im Cluster Audit-fähige Storage Virtual Machines (SVMs) gibt. Sie müssen bestimmte Aktionen durchführen, bevor Sie den Wechsel

rückgängig machen.

Zurücksetzen auf eine Version von ONTAP, die keine Unterstützung für das Auditing von SMB-Anmeldeereignissen und Abmeldungs-Ereignissen sowie von Staging-Ereignissen für zentrale Zugriffsrichtlinien bietet

Clustered Data ONTAP 8.3 unterstützt das Auditing von SMB-Anmeldeereignissen und Abmeldung sowie von zentralen Zugriffs-Policy-Staging-Ereignissen. Wenn Sie zurück zu einer Version von ONTAP wechseln, die diese Ereignistypen nicht unterstützt, und Sie verfügen über Auditing-Konfigurationen, die diese Ereignistypen überwachen, müssen Sie vor dem Zurücksetzen die Prüfungskonfiguration für diese revisionssigemeinsam verwendeten SVMs ändern. Sie müssen die Konfiguration so ändern, dass nur Datei-op-Ereignisse überprüft werden.

Fehlerbehebung bei Problemen mit Auditing und Staging von Volume-Speicherplatz

Probleme können auftreten, wenn entweder auf den Staging-Volumes oder auf dem Volume, das die Audit-Ereignisprotokolle enthält, nicht genügend Speicherplatz vorhanden ist. Wenn nicht genügend Speicherplatz vorhanden ist, können keine neuen Audit-Datensätze erstellt werden. Dies verhindert, dass Clients auf Daten zugreifen und Zugriffsanforderungen fehlschlagen. Sie sollten wissen, wie Sie diese Probleme mit Volume-Speicherplatz beheben und beheben.

Behebung von Platzproblemen im Zusammenhang mit den Ereignisprotokollvolumes

Wenn Volumes mit Ereignisprotokolldateien nicht mehr genügend Speicherplatz haben, können Protokolldatensätze durch Auditing nicht in Protokolldateien konvertiert werden. Dies führt zu einem Ausfall des Client-Zugriffs. Sie müssen wissen, wie die Behebung von Platzproblemen im Zusammenhang mit Ereignisprotokollvolumen behoben wird.

- Storage Virtual Machine (SVM) und Cluster-Administratoren können feststellen, ob ein unzureichender Volume-Speicherplatz vorhanden ist, indem Informationen über die Auslastung und Konfiguration der Volumes und Aggregate angezeigt werden.
- Falls in den Volumes, die Ereignisprotokolle enthalten, nicht genügend Speicherplatz verfügbar ist, können SVM- und Cluster-Administratoren diese Platzprobleme beheben, indem sie einige der Ereignisprotokolldateien entfernen oder die Größe des Volume erhöhen.

  > Wenn das Aggregat, das das Ereignisprotokoll enthält, voll ist, muss die Größe des Aggregats erhöht werden, bevor Sie die Größe des Volumes erhöhen können. Nur ein Cluster-Administrator kann die Größe eines Aggregats erhöhen.

- Der Zielpfad für die Ereignisprotokolldateien kann durch Ändern der Überwachungskonfiguration in ein Verzeichnis auf einem anderen Volume geändert werden.

  > Der Datenzugriff wird in den folgenden Fällen verweigert:
  >
  > - Wenn das Zielverzeichnis gelöscht wird.
  > - Wenn die Dateibegrenzung für ein Volume, das das Zielverzeichnis hostet, die Höchststufe erreicht.

Weitere Informationen:

- "So erhalten Sie Informationen zu Volumes und zur Vergrößerung des Volumes".
- "Anzeigen von Informationen zu Aggregaten und zum Managen von Aggregaten".

Behebung von Platzproblemen im Zusammenhang mit den Staging-Volumes

Sollte einer der Volumes, die Staging-Dateien für die SVM (Storage Virtual Machine) enthalten, nicht mehr genügend Speicherplatz haben, kann die Prüfung Protokolldatensätze nicht in Staging-Dateien schreiben. Dies führt zu einem Ausfall des Client-Zugriffs. Um dieses Problem zu beheben, müssen Sie ermitteln, ob die in der SVM verwendeten Staging-Volumes durch die Anzeige von Informationen zur Volume-Nutzung vollständig sind.

Wenn das Volume, das die konsolidierten Ereignisprotokolldateien enthält, genügend Speicherplatz hat, aber aufgrund eines unzureichenden Speicherplatzes beim Client-Zugriff weiterhin besteht, sind die Staging-Volumes möglicherweise nicht mehr genügend Platz. Der SVM-Administrator muss sich mit Ihnen in Verbindung setzen, um zu ermitteln, ob die Staging-Volumes, die Staging-Dateien für die SVM enthalten, über unzureichenden Speicherplatz verfügen. Das Audit-Subsystem generiert ein EMS-Ereignis, wenn Überwachungsereignisse nicht generiert werden können, weil der Speicherplatz in einem Staging-Volume nicht ausreicht. Die folgende Meldung wird angezeigt: `No space left on device`. Nur Informationen zu Staging Volumes können angezeigt werden. SVM-Administratoren können dies nicht.

Alle Staging-Volume-Namen beginnen mit `MDV_aud_` Anschließend die UUID des Aggregats, das das Staging-Volume enthält. Das folgende Beispiel zeigt vier System-Volumes auf der Administrator-SVM, die automatisch erstellt wurden, wenn eine Fileservices-Auditing-Konfiguration für eine Daten-SVM im Cluster erstellt wurde:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

Wenn der Speicherplatz in den Staging-Volumes nicht ausreicht, können Sie die Platzprobleme beheben, indem Sie die Größe des Volumes erhöhen.

> Ist das Aggregat, das das Staging-Volume enthält, voll, muss die Größe des Aggregats erhöht werden, bevor Sie die Volume-Größe erhöhen können. Nur Sie können die Größe eines Aggregats erhöhen, was SVM-Administratoren nicht können.

Wenn ein oder mehrere Aggregate einen verfügbaren Speicherplatz von weniger als 2 GB aufweisen, schlägt die SVM-Audit-Erstellung fehl. Wenn die Erstellung der SVM-Audits fehlschlägt, werden die erstellten Staging-Volumes gelöscht.

FPolicy ermöglicht Datei-Monitoring und -Management auf SVMs

FPolicy verstehen

Was die beiden Teile der FPolicy Lösung sind

FPolicy ist ein Benachrichtigungs-Framework für den Dateizugriff, mit dem Ereignisse für den Dateizugriff auf Storage Virtual Machines (SVMs) über Partnerlösungen überwacht und gemanagt werden können. Partnerlösungen unterstützen Sie bei der Bewältigung verschiedener Anwendungsfälle wie Daten-Governance und Compliance, Ransomware-Schutz und Datenmobilität.

Bei den Partnerlösungen zählen sowohl von NetApp unterstützte Lösungen von Drittanbietern als auch NetApp Produkte Workload Security und Cloud Data Sense.

Es gibt zwei Teile zu einer FPolicy Lösung. Das ONTAP FPolicy Framework verwaltet Aktivitäten im Cluster und sendet Benachrichtigungen an die Partnerapplikation (auch externe FPolicy Server genannt). Externe FPolicy Server verarbeiten Benachrichtigungen, die von ONTAP FPolicy gesendet werden, um Kundennutzungsfälle zu erfüllen.

Das ONTAP Framework erstellt und pflegt die FPolicy Konfiguration, überwacht Dateiereignisse und sendet Benachrichtigungen an externe FPolicy Server. ONTAP FPolicy bietet die Infrastruktur für die Kommunikation zwischen externen FPolicy Servern und Storage Virtual Machine (SVM) Nodes.

Das FPolicy-Framework stellt eine Verbindung zu externen FPolicy-Servern her und sendet Benachrichtigungen für bestimmte Dateisystemereignisse an die FPolicy-Server, wenn diese Ereignisse als Folge des Client-Zugriffs auftreten. Die externen FPolicy Server verarbeiten die Benachrichtigungen und senden Antworten zurück auf den Knoten. Was als Folge der Benachrichtigungsverarbeitung geschieht, hängt von der Anwendung ab und ob die Kommunikation zwischen Knoten und externen Servern asynchron oder synchron ist.

Was sind synchrone und asynchrone Benachrichtigungen

FPolicy sendet Benachrichtigungen über die FPolicy Schnittstelle an externe FPolicy Server. Die Benachrichtigungen werden entweder im synchronen oder asynchronen Modus gesendet. Der Benachrichtigungsmodus bestimmt, was ONTAP nach dem Senden von Benachrichtigungen an FPolicy-Server tut.

- **Asynchronous Notifications**

  Bei asynchronen Benachrichtigungen wartet der Node nicht auf eine Antwort des FPolicy Servers, wodurch der Gesamtdurchsatz des Systems verbessert wird. Diese Art der Benachrichtigung ist für Anwendungen geeignet, bei denen der FPolicy-Server aufgrund der Benachrichtigungsbewertung keine Maßnahmen erfordert. Asynchrone Benachrichtigungen kommen beispielsweise zum Einsatz, wenn der SVM-Administrator (Storage Virtual Machine) den Dateizugriff überwachen und prüfen möchte.

Wenn bei einem FPolicy-Server im asynchronen Modus ein Netzwerkausfall auftritt, werden FPolicy Benachrichtigungen, die während des Ausfalls generiert wurden, auf dem Storage-Node gespeichert. Wenn der FPolicy-Server wieder online geschaltet wird, wird er über die gespeicherten Benachrichtigungen benachrichtigt und kann sie vom Speicher-Node abrufen. Die Länge der Speicherung der Benachrichtigungen während eines Ausfalls kann so bis zu 10 Minuten betragen.

Ab ONTAP 9.14.1 können Sie mit FPolicy einen persistenten Speicher einrichten, um Dateizugriffsereignisse für asynchrone, nicht obligatorische Richtlinien auf der SVM zu erfassen. Persistente Speicher können die Client-I/O-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu verringern. Synchrone (obligatorische oder nicht obligatorische) und asynchrone obligatorische Konfigurationen werden nicht unterstützt.

- **Synchrone Benachrichtigungen**

  Wenn der FPolicy-Server für die Ausführung im synchronen Modus konfiguriert ist, muss er jede Benachrichtigung bestätigen, bevor der Clientvorgang fortgesetzt werden kann. Diese Art der Benachrichtigung wird verwendet, wenn eine Aktion erforderlich ist, basierend auf den Ergebnissen der Auswertung der Benachrichtigung. Synchrone Benachrichtigungen werden beispielsweise verwendet, wenn der SVM-Administrator Anfragen basierend auf den auf dem externen FPolicy-Server festgelegten Kriterien zulassen oder ablehnen möchte.

Synchrone und asynchrone Applikationen

Es gibt viele mögliche Einsatzmöglichkeiten für FPolicy-Applikationen, sowohl asynchron als auch synchron.

Asynchrone Applikationen sind solche, bei denen der externe FPolicy-Server den Zugriff auf Dateien oder Verzeichnisse nicht verändert oder Daten auf der Storage Virtual Machine (SVM) verändert. Beispiel:

- Dateizugriff und Revisionsprotokollierung
- Storage-Ressourcenmanagement

Synchrone Applikationen sind solche, bei denen der Datenzugriff geändert wird oder die Daten vom externen FPolicy-Server geändert werden. Beispiel:

- Kontingentverwaltung
- Blockierung des Dateizugriffs
- Dateiarchivierung und hierarchisches Storage-Management
- Verschlüsselungs- und Entschlüsselungsdienste
- Komprimierungs- und Dekomprimierungsservices

FPolicy persistente Speicher

Ab ONTAP 9.14.1 können Sie mit FPolicy einen persistenten Speicher einrichten, um Dateizugriffsereignisse für asynchrone, nicht obligatorische Richtlinien auf der SVM zu erfassen. Persistente Speicher können die Client-I/O-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu verringern. Synchrone (obligatorische oder nicht obligatorische) und asynchrone obligatorische Konfigurationen werden nicht unterstützt.

Diese Funktion ist nur im externen FPolicy-Modus verfügbar. Die Partneranwendung, die Sie verwenden, muss diese Funktion unterstützen. Stellen Sie sicher, dass diese FPolicy-Konfiguration von Ihrem Partner unterstützt

wird.

Best Practices in sich vereint

Cluster-Administratoren müssen ein Volume für den persistenten Speicher jeder SVM konfigurieren, für die FPolicy aktiviert ist. Bei der Konfiguration erfasst ein persistenter Speicher alle übereinstimmenden FPolicy-Ereignisse, die weiter in der FPolicy-Pipeline verarbeitet und an den externen Server gesendet werden.

Der persistente Speicher bleibt so, wie er zu dem Zeitpunkt war, zu dem das letzte Ereignis empfangen wurde, wenn ein unerwarteter Neustart erfolgt ist, oder FPolicy wird deaktiviert und erneut aktiviert. Nach einer Übernahme werden neue Ereignisse vom Partner-Node gespeichert und verarbeitet. Nach einem Giveback-Vorgang setzt der persistente Speicher die Verarbeitung aller nicht verarbeiteten Ereignisse fort, die möglicherweise vom Zeitpunkt der Node-Übernahme entfernt bleiben. Live-Events würden Vorrang vor nicht verarbeiteten Ereignissen erhalten.

Wenn das persistente Speicher-Volume in derselben SVM von einem Node zu einem anderen verschoben wird, werden die noch zu verarbeitenden Benachrichtigungen auch in den neuen Node verschoben. Sie müssen den erneut ausführen `fpolicy persistent-store create` Befehl auf einem der Knoten nach dem Verschieben des Volumes, um sicherzustellen, dass die ausstehende Benachrichtigung an den externen Server gesendet wird.

Das persistente Speicher-Volume wird auf SVM-Basis eingerichtet. Sie müssen für jede FPolicy aktivierte SVM ein persistentes Speicher-Volume erstellen.

Erstellen Sie das persistente Speicher-Volume auf dem Node mit LIFs, die davon ausgehen, dass der maximale Datenverkehr durch FPolicy überwacht wird.

Wenn die im persistenten Speicher angesammelten Benachrichtigungen die Größe des bereitgestellten Volumes überschreiten, beginnt FPolicy die eingehende Benachrichtigung mit den entsprechenden EMS-Nachrichten zu löschen.

Der Name des persistenten Speichervolumes und der zum Zeitpunkt der Volume-Erstellung angegebene Verbindungspfad müssen übereinstimmen.

Lassen Sie die Snapshot-Richtlinie auf festlegen `none` Für dieses Volume anstelle von `default`. Dadurch wird sichergestellt, dass keine versehentliche Wiederherstellung des Snapshots zum Verlust aktueller Ereignisse führt und eine mögliche doppelte Ereignisverarbeitung verhindert wird.

Machen Sie das persistente Speicher-Volume für den externen Zugriff auf das Benutzerprotokoll (CIFS/NFS) unzugänglich, um versehentliche Beschädigungen oder das Löschen von permanenten Ereignisdatensätzen zu vermeiden. Um dies zu erreichen, heben Sie nach Aktivierung von FPolicy die Bereitstellung des Volumes in ONTAP auf, um den Verbindungspfad zu entfernen. Dies macht ihn für den Benutzerprotokollzugriff unzugänglich.

Weitere Informationen finden Sie unter "Erstellen persistenter Speicher".

FPolicy-Konfigurationstypen

Es gibt zwei grundlegende FPolicy-Konfigurationstypen. Eine Konfiguration verwendet externe FPolicy Server zur Verarbeitung und Bearbeitung von Benachrichtigungen. Die andere Konfiguration verwendet keine externen FPolicy Server; stattdessen verwendet es den internen, nativen FPolicy Server von ONTAP für einfaches File Blocking auf Basis von Erweiterungen.

- **Konfiguration des externen FPolicy Servers**

  Die Benachrichtigung wird an den FPolicy-Server gesendet, der die Anforderung einliest und Regeln anwendet, um zu bestimmen, ob der Knoten den angeforderten Dateibetrieb zulassen soll. Für synchrone Richtlinien sendet der FPolicy-Server dann eine Antwort an den Node, um die angeforderte Dateioperation zu ermöglichen oder zu blockieren.

- **Native FPolicy Server-Konfiguration**

  Die Benachrichtigung wird intern gescreent. Die Anforderung wird zulässig oder abgelehnt, basierend auf den im FPolicy-Umfang konfigurierten Dateiendungeinstellungen.

  Hinweis: Nicht ablehnte Dateiendungsanfragen werden protokolliert.

Wann eine native FPolicy Konfiguration erstellt werden soll

Native FPolicy-Konfigurationen verwenden die interne ONTAP FPolicy Engine, um Dateivorgänge basierend auf der Dateierweiterung zu überwachen und zu blockieren. Diese Lösung erfordert keine externen FPolicy Server (FPolicy Server). Wenn diese einfache Lösung benötigt wird, ist die Verwendung einer nativen File Blocking-Konfiguration angemessen.

Das native File Blocking ermöglicht Ihnen die Überwachung aller Dateivorgänge, die mit konfigurierten Vorgängen und Filterereignissen übereinstimmen, und verweigert dann den Zugriff auf Dateien mit bestimmten Erweiterungen. Dies ist die Standardkonfiguration.

Mit dieser Konfiguration wird der Dateizugriff nur auf Basis der Dateiendung blockiert. Beispielsweise zum Blockieren von Dateien, die enthalten `mp3` Erweiterungen: Sie konfigurieren eine Richtlinie, um Benachrichtigungen für bestimmte Vorgänge mit Zieldateierweiterungen von bereitzustellen `mp3`. Die Richtlinie ist so konfiguriert, dass sie verweigert wird `mp3` Dateianforderungen für Vorgänge, die Benachrichtigungen generieren

Das gilt für native FPolicy-Konfigurationen:

- Dieselben Filter und Protokolle, die von FPolicy Server-basierten Dateiscreening unterstützt werden, werden auch für das native File Blocking unterstützt.
- Native File Blocking- und FPolicy-basierte Datei-Screening-Applikationen können gleichzeitig konfiguriert werden.

  Dazu können Sie zwei separate FPolicy Richtlinien für die Storage Virtual Machine (SVM) konfigurieren, wobei eine für natives File Blocking konfiguriert ist und eine für FPolicy-Server-basierte Datei-Screening konfiguriert ist.

- Die native File Blocking-Funktion nur Bildschirme Dateien auf der Grundlage der Erweiterungen und nicht auf den Inhalt der Datei.
- Bei symbolischen Links verwendet das native File Blocking die Dateiendung der Root-Datei.

Weitere Informationen zu "FPolicy: Native Dateisperrung".

Wenn eine Konfiguration erstellt werden soll, die externe FPolicy-Server verwendet

FPolicy-Konfigurationen, die für die Verarbeitung und das Management von Benachrichtigungen über externe FPolicy-Server verfügen, bieten zuverlässige Lösungen für Anwendungsfälle, in denen mehr als einfaches File Blocking auf Basis einer Dateierweiterung erforderlich ist.

Sie sollten eine Konfiguration erstellen, die externe FPolicy-Server verwendet, wenn Sie solche Dinge wie Überwachung und Aufzeichnung von Dateizugriffsereignissen, Bereitstellung von Quotendiensten, Durchführung von Dateiblockierung auf der Grundlage von Kriterien andere als einfache Dateierweiterungen, Bereitstellung von Datenmigrationsservices unter Verwendung von hierarchischen Speichermanagement-Anwendungen, Alternativ können Sie feingranulare Richtlinien anbieten, die nur eine Teilmenge an Daten in der Storage Virtual Machine (SVM) überwachen.

Rollen, die Cluster-Komponenten bei FPolicy Implementierung spielen

In einer FPolicy Implementierung spielen der Cluster, die enthaltenen Storage Virtual Machines (SVMs) und Daten-LIFs eine Rolle.

- * Cluster*

  Das Cluster enthält das FPolicy Management-Framework und verwaltet Informationen zu allen FPolicy-Konfigurationen im Cluster.

- **SVM**

  Eine FPolicy-Konfiguration wird auf SVM-Ebene definiert. Der Konfigurationsumfang ist die SVM, die nur auf SVM-Ressourcen ausgeführt wird. Eine SVM-Konfiguration kann keine Benachrichtigungen für Dateizugriffsanfragen überwachen und senden, die sich auf Daten auf einer anderen SVM befinden.

  FPolicy-Konfigurationen können auf der Admin-SVM definiert werden. Nachdem die Konfigurationen auf der Administrator-SVM definiert wurden, können sie in allen SVMs angezeigt und verwendet werden.

- **Daten-LIFs**

  Verbindungen zu den FPolicy-Servern werden über Daten-LIFs, die zur SVM mit der FPolicy-Konfiguration gehören, hergestellt. Die für diese Verbindungen verwendeten Daten-LIFs können ein Failover auf dieselbe Weise durchführen wie die Daten-LIFs für den normalen Client-Zugriff.

Wie FPolicy mit externen FPolicy-Servern funktioniert

Nachdem FPolicy auf der Storage Virtual Machine (SVM) konfiguriert und aktiviert wurde, wird FPolicy auf jedem Node ausgeführt, an dem die SVM teilnimmt. FPolicy ist für die Einrichtung und Wartung von Verbindungen mit externen FPolicy-Servern (FPolicy-Servern), für die Benachrichtigungsverarbeitung und das Management von Benachrichtigungsmeldungen zu und von FPolicy-Servern verantwortlich.

Darüber hinaus hat FPolicy im Rahmen des Verbindungsmanagements folgende Aufgaben:

- Stellt sicher, dass die Dateibenachrichtigung durch die richtige LIF an den FPolicy-Server fließt.
- Stellt sicher, dass beim Senden von Benachrichtigungen an die FPolicy-Server ein Lastausgleich erfolgt, wenn mehrere FPolicy-Server mit einer Richtlinie verknüpft sind.
- Versucht, die Verbindung wiederherzustellen, wenn eine Verbindung zu einem FPolicy-Server unterbrochen wird.
- Sendet Benachrichtigungen über eine authentifizierte Sitzung an FPolicy Server.
- Verwaltet die vom FPolicy-Server für die Verarbeitung von Clientanforderungen festgelegte Passthrough-Datenverbindung, wenn das Passthrough-Lesevorgang aktiviert ist.

Wie Kontrollkanäle für die FPolicy Kommunikation verwendet werden

FPolicy initiiert eine Steuerkanalverbindung zu einem externen FPolicy Server von den Daten-LIFs jedes Nodes, der an einer Storage Virtual Machine (SVM) beteiligt ist. FPolicy verwendet Kontrollkanäle für die Übertragung von Dateibenachrichtigungen. Daher können bei einem FPolicy-Server je nach SVM-Topologie mehrere Kontrollkanalverbindungen zu erkennen sein.

Verwendung von privilegierten Datenzugriffskanälen für die synchrone Kommunikation

Bei synchronen Anwendungsfällen greift der FPolicy Server über einen privilegierten Datenpfad auf die auf der Storage Virtual Machine (SVM) befindlichen Daten zu. Der Zugriff über den privilegierten Pfad stellt dem FPolicy-Server das komplette Dateisystem zur Verfügung. Es kann auf Datendateien zugreifen, um Informationen zu sammeln, Dateien zu scannen, Dateien zu lesen oder in Dateien zu schreiben.

Da der externe FPolicy-Server über den privilegierten Datenkanal vom Root der SVM auf das gesamte Filesystem zugreifen kann, muss die Verbindung mit dem privilegierten Datenkanal sicher sein.

Verwendung von FPolicy Connection Anmeldeinformationen mit privilegierten Datenzugriffskanälen

Der FPolicy-Server stellt privilegierte Datenzugangsverbindungen zu Cluster-Knoten mithilfe einer bestimmten Windows-Benutzeranmeldeinformationen bereit, die mit der FPolicy-Konfiguration gespeichert werden. SMB ist das einzige unterstützte Protokoll für eine Verbindung mit einem privilegierten Channel für den Datenzugriff.

Wenn der FPolicy-Server einen privilegierten Datenzugriff erfordert, müssen die folgenden Bedingungen erfüllt sein:

- Eine SMB-Lizenz muss auf dem Cluster aktiviert sein.
- Der FPolicy-Server muss unter den in der FPolicy-Konfiguration konfigurierten Anmeldeinformationen ausgeführt werden.

Beim Herstellen einer Datenkanalverbindung verwendet FPolicy die Anmeldeinformationen für den angegebenen Windows-Benutzernamen. Der Datenzugriff erfolgt über den Admin-Anteil „ONTAP_ADMIN“.

Was die Gewährung von Super-User-Anmeldeinformationen für privilegierten Datenzugriff bedeutet

ONTAP verwendet die Kombination aus der IP-Adresse und den in der FPolicy-Konfiguration konfigurierten Benutzerberechtigungen, um dem FPolicy-Server Super-Benutzeranmeldeinformationen zu erteilen.

Der Superuser-Status gewährt die folgenden Berechtigungen, wenn der FPolicy-Server auf Daten zugreift:

- Vermeiden Sie Berechtigungsprüfungen

  Der Benutzer vermeidet Überprüfungen von Dateien und Verzeichniszugriff.

- Besondere Sperrrechte

  ONTAP ermöglicht Lese-, Schreib- oder Änderungszugriff auf beliebige Dateien, unabhängig von vorhandenen Sperren. Wenn der FPolicy-Server Byte-Sperren auf der Datei nimmt, werden bestehende Sperren auf der Datei sofort entfernt.

- Umgehen Sie alle FPolicy-Prüfungen

  Der Zugriff generiert keine FPolicy-Benachrichtigungen.

So managt FPolicy die Richtlinienverarbeitung

Ihrer Storage Virtual Machine (SVM) können mehrere FPolicy Richtlinien zugewiesen sein, von denen jede eine andere Priorität hat. Um eine entsprechende FPolicy-Konfiguration auf der SVM zu erstellen, ist es wichtig zu verstehen, wie FPolicy die Richtlinienverarbeitung managt.

Jede Dateizugriffsanforderung wird zunächst ausgewertet, um festzustellen, welche Richtlinien dieses Ereignis überwachen. Wenn es sich um ein überwachtes Ereignis handelt, werden Informationen über das überwachte Ereignis zusammen mit interessierten Richtlinien an FPolicy weitergeleitet, wo es ausgewertet wird. Jede Richtlinie wird in der Reihenfolge der zugewiesenen Priorität bewertet.

Beim Konfigurieren von Richtlinien sollten Sie die folgenden Empfehlungen berücksichtigen:

- Wenn eine Richtlinie immer vor anderen Richtlinien bewertet werden soll, konfigurieren Sie diese Richtlinie mit höherer Priorität.
- Wenn der Erfolg des angeforderten Dateizugriffs bei einem überwachten Ereignis eine Voraussetzung für eine Dateianforderung ist, die anhand einer anderen Richtlinie ausgewertet wird, geben Sie der Richtlinie, die den Erfolg oder den Fehler des ersten Dateivorgangs steuert, eine höhere Priorität.

  Wenn eine Richtlinie beispielsweise Funktionen zur Dateiarchivierung und -Wiederherstellung auf FPolicy managt und eine zweite Richtlinie Dateizugriffsvorgänge in der Online-Datei managt, Die Richtlinie für die Wiederherstellung von Dateien muss eine höhere Priorität haben, damit die Datei wiederhergestellt wird, bevor der Vorgang, der von der zweiten Richtlinie gemanagt wird, zulässig ist.

- Wenn Sie möchten, dass alle Richtlinien, die für einen Dateizugriffsvorgang gelten, ausgewertet werden, sollten Sie synchrone Richtlinien mit niedrigerer Priorität betrachten.

Sie können Richtlinienprioritäten für vorhandene Richtlinien neu anordnen, indem Sie die Nummer der Richtliniensequenz ändern. Um Richtlinien basierend auf der geänderten Prioritätsreihenfolge jedoch FPolicy bewerten zu können, müssen Sie die Richtlinie mit der geänderten Sequenznummer deaktivieren und erneut aktivieren.

Was ist der Kommunikationsprozess zwischen Knoten und externem FPolicy-Server

Um Ihre FPolicy-Konfiguration richtig zu planen, sollten Sie verstehen, was der Knoten-zu-externe FPolicy Server-Kommunikationsprozess ist.

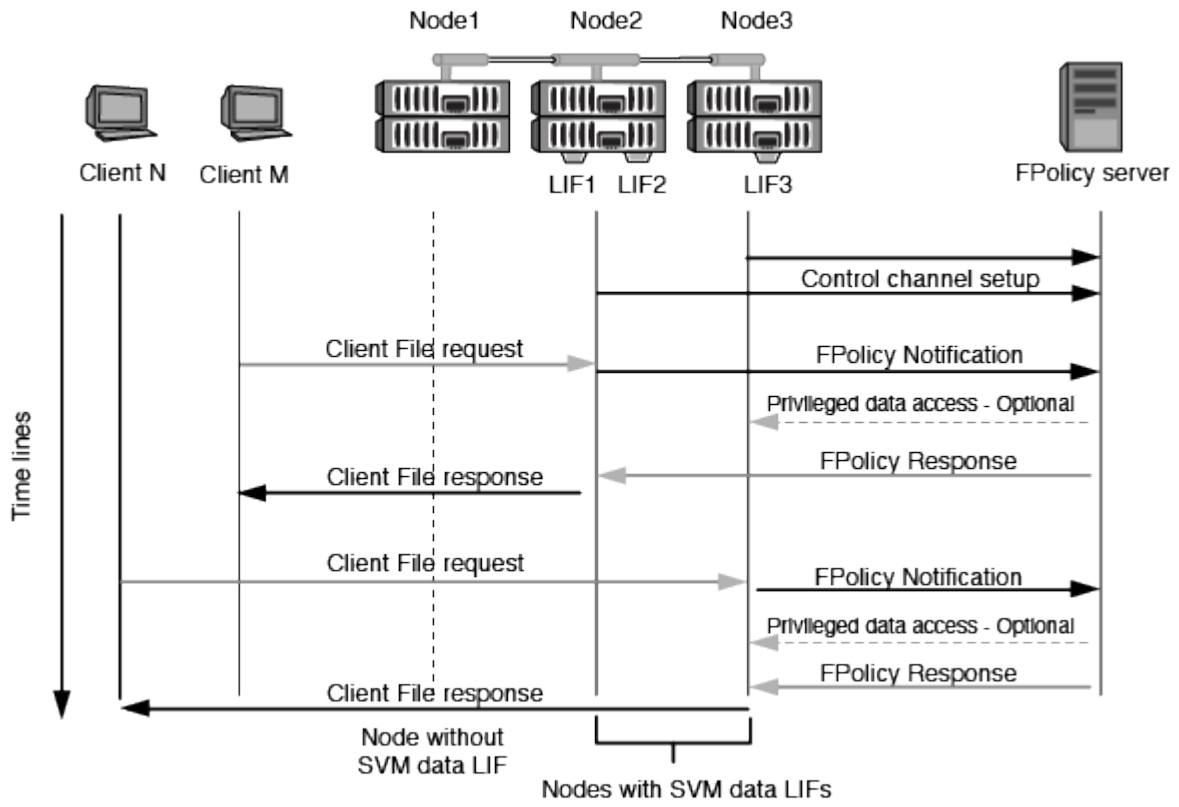
Jeder Node, der an jeder Storage Virtual Machine (SVM) teilnimmt, initiiert mithilfe von TCP/IP eine Verbindung zu einem externen FPolicy Server (FPolicy Server). Verbindungen zu den FPolicy-Servern werden mithilfe von Node-Daten-LIFs eingerichtet. Daher kann ein teilnehmender Node eine Verbindung nur einrichten, wenn der Node über eine funktionsfähige Daten-LIF für die SVM verfügt.

Jeder FPolicy-Prozess auf teilnehmenden Knoten versucht, eine Verbindung zum FPolicy-Server herzustellen, wenn die Richtlinie aktiviert ist. Sie verwendet die IP-Adresse und den Port der FPolicy-externen Engine, die in der Richtlinienkonfiguration angegeben ist.

Die Verbindung stellt von jedem der Nodes, die an jeder SVM teilnehmen, über die Daten-LIF einen Kontrollkanal zum FPolicy-Server bereit. Wenn IPv4- und IPv6-Daten-LIF-Adressen auf demselben teilnehmenden Node vorhanden sind, versucht FPolicy zudem, Verbindungen sowohl für IPv4 als auch für IPv6 herzustellen. Daher muss der FPolicy-Server in einem Szenario, in dem die SVM über mehrere Nodes erweitert wird oder wenn sowohl IPv4- als auch IPv6-Adressen vorhanden sind, bereit sein, nach Aktivierung der FPolicy auf der SVM mehrere Kontrollkanaleinrichtungsanfragen vom Cluster aus zu bearbeiten.

Wenn beispielsweise ein Cluster drei Nodes hat –-Node1, Node2 und Node3- und SVM-Daten-LIFs werden über nur Node2 und Node3 verteilt – werden die Kontrollkanäle nur von Node2 und Node3 aus initiiert,

unabhängig von der Verteilung der Daten-Volumes. Sagen wir, dass Node2 zwei Daten-LIFs hat --LIF1 und LIF2 — die zur SVM gehören und dass die anfängliche Verbindung von LIF1 ist. Wenn LIF1 fehlschlägt, versucht FPolicy, einen Kontrollkanal von LIF2 einzurichten.



So managt FPolicy die externe Kommunikation während LIF-Migration oder Failover

Daten-LIFs können zu Daten-Ports im selben Node oder zu Daten-Ports eines Remote Nodes migriert werden.

Bei einem Failover oder der Migration einer Daten-LIF wird eine neue Kontrollkanal-Verbindung zum FPolicy-Server hergestellt. FPolicy kann dann erneut versuchen SMB- und NFS-Client-Anforderungen zu versuchen, die abgelaufen sind. Mit dem Ergebnis, dass neue Benachrichtigungen an die externen FPolicy-Server gesendet werden. Der Node lehnt FPolicy-Serverantworten an ursprüngliche, zeitlich begrenzte SMB- und NFS-Anforderungen ab.

Wie FPolicy die externe Kommunikation beim Node Failover managt

Wenn der Cluster-Node, der die für die FPolicy Kommunikation verwendeten Daten-Ports hostet, ausfällt, bricht ONTAP die Verbindung zwischen dem FPolicy-Server und dem Node aus.

Die Auswirkungen eines Cluster Failover auf den FPolicy-Server können durch Konfiguration der Failover-Richtlinie reduziert werden, um den in der FPolicy-Kommunikation verwendeten Daten-Port zu einem anderen aktiven Node zu migrieren. Nach Abschluss der Migration wird über den neuen Daten-Port eine neue Verbindung hergestellt.

Wenn die Failover-Richtlinie nicht für die Migration des Daten-Ports konfiguriert ist, muss der FPolicy-Server warten, bis der ausgefallene Node angezeigt wird. Nachdem der Knoten aktiv ist, wird eine neue Verbindung von diesem Knoten mit einer neuen Session-ID initiiert.

Der FPolicy-Server erkennt unterbrochene Verbindungen mit der Keep-Alive-Protokollnachricht. Bei der Konfiguration von FPolicy wird die Zeitüberschreitung für das Löschen der Sitzungs-ID festgelegt. Die standardmäßige Keep-Alive-Zeitüberschreitung beträgt zwei Minuten.

So funktionieren FPolicy Services über SVM-Namespaces hinweg

ONTAP stellt einen Namespace für Unified Storage Virtual Machine (SVM) bereit. Volumes im Cluster werden gemeinsam mit Verbindungen zu einem einzigen logischen File-System verbunden. Der FPolicy-Server erkennt die Namespace-Topologie und bietet FPolicy Services für den gesamten Namespace.

Der Namespace ist spezifisch und in der SVM enthalten. Daher wird der Namespace nur aus dem SVM-Kontext angezeigt. Namespaces haben die folgenden Eigenschaften:

- In jeder SVM ist ein einziger Namespace vorhanden, wobei der Root-Namespace das Root-Volume ist und im Namespace als „Schrägstrich“ (/) dargestellt ist.
- Alle anderen Volumes verfügen über Verbindungspunkte unter dem Root (/).
- Volume-Verbindungen sind für Clients transparent.
- Ein einzelner NFS-Export kann Zugriff auf den vollständigen Namespace bieten. Andernfalls können Exportrichtlinien bestimmte Volumes exportieren.
- SMB-Shares können auf dem Volume oder qtrees innerhalb des Volume oder in jedem Verzeichnis im Namespace erstellt werden.
- Die Namespace-Architektur ist flexibel.

  Beispiele für typische Namespace-Architekturen:

  - Ein Namespace mit einem einzelnen Zweig aus dem Root
  - Ein Namespace mit mehreren Zweigen vom Root
  - Ein Namespace mit mehreren nicht verzweigten Volumes vom Root

FPolicy Passthrough-Read verbessert die Benutzerfreundlichkeit für hierarchisches Storage-Management

PassThrough-Read ermöglicht es dem FPolicy Server (funktioniert als hierarchischer Storage Management (HSM) Server) Lesezugriff auf Offline-Dateien zu bieten, ohne die Datei vom sekundären Storage-System auf das primäre Storage-System zurückrufen zu müssen.

Wenn ein FPolicy Server so konfiguriert wird, dass HSM für Dateien auf einem SMB-Server bereitgestellt wird, erfolgt eine richtlinienbasierte Dateimigration, bei der die Dateien offline auf dem Sekundärspeicher gespeichert werden, während nur eine Stub-Datei im Primärspeicher bleibt. Obwohl eine Stub-Datei für Clients als normale Datei erscheint, handelt es sich eigentlich um eine spärliche Datei, die die gleiche Größe der ursprünglichen Datei hat. In der spärlichen Datei ist das SMB-Offline-Bit gesetzt und verweist auf die eigentliche Datei, die zum sekundären Storage migriert wurde.

Wenn eine Leseanfrage für eine Offline-Datei eingeht, muss der angeforderte Inhalt in der Regel zurück im primären Storage abgerufen werden. Der Zugriff erfolgt dann über den Primär-Storage. Der Rückruf von Daten auf den primären Storage hat mehrere unerwünschte Auswirkungen. Zu den unerwünschten Auswirkungen gehört die höhere Latenz bei Client-Anfragen, die durch das Abrufen des Inhalts vor der Reaktion auf die

Anforderung verursacht werden, und der höhere Verbrauch an Speicherplatz, der für abgerufene Dateien im primären Storage benötigt wird.

FPolicy Passthrough-read ermöglicht dem HSM-Server (der FPolicy Server) einen Lesezugriff auf migrierte Offline-Dateien, ohne die Datei vom sekundären Storage-System auf das primäre Storage-System zurückrufen zu müssen. Statt die Dateien zurück auf den Primär-Storage zu zurückrufen, können Leseanforderungen direkt aus dem Sekundärspeicher abgerufen werden.

Copy Offload (ODX) wird bei FPolicy-Passthrough-Vorgang nicht unterstützt.

Passthrough-read verbessert die Benutzerfreundlichkeit durch die folgenden Vorteile:

- Lesezugriffe können auch dann bedient werden, wenn der primäre Storage nicht über genügend Speicherplatz verfügt, um die angeforderten Daten zurück auf den primären Storage abzurufen.
- Besseres Kapazitäts- und Performance-Management, wenn eine Zunahme des Datenaufrufs auftreten kann, beispielsweise wenn ein Skript oder eine Backup-Lösung auf viele Offline-Dateien zugreifen muss.
- Leseanforderungen für Offline-Dateien in Snapshot Kopien können verarbeitet werden.

  Da Snapshot-Kopien nur leseverwendet werden, kann der FPolicy Server die ursprüngliche Datei nicht wiederherstellen, wenn die Stub-Datei in einer Snapshot-Kopie befindet. Dieses Problem wird durch die Verwendung von Passthrough-Read behoben.

- Richtlinien können eingerichtet werden, die steuern, wenn Leseanforderungen über den Zugriff auf die Datei im sekundären Storage verarbeitet werden und wann die Offline-Datei an den primären Storage abgerufen werden soll.

  Beispielsweise kann eine Richtlinie auf dem HSM-Server erstellt werden, die die Anzahl der Zugriffszeiten für die Offline-Datei in einem bestimmten Zeitraum angibt, bis die Datei zurück zum primären Storage migriert wurde. Diese Art von Richtlinie verhindert das Abrufen von Dateien, auf die selten zugegriffen wird.

Wie Leseanforderungen gemanagt werden, wenn FPolicy Passthrough-read aktiviert ist

Sie sollten verstehen, wie Leseanforderungen gemanagt werden, wenn FPolicy Passthrough-Read aktiviert ist, damit Sie die Konnektivität zwischen der Storage Virtual Machine (SVM) und den FPolicy Servern optimal konfigurieren können.

Wenn FPolicy Passthrough-Read aktiviert ist und die SVM eine Anfrage für eine Offline-Datei erhält, sendet FPolicy über den Standard-Verbindungskanal eine Benachrichtigung an den FPolicy-Server (HSM-Server).

Nach Erhalt der Benachrichtigung liest der FPolicy-Server die Daten aus dem in der Benachrichtigung gesendeten Dateipfad und sendet die angeforderten Daten über die Verbindung mit privilegierten Lesevorgängen mit Passthrough-Lesevorgängen, die zwischen der SVM und dem FPolicy-Server hergestellt wurde.

Nach dem Senden der Daten reagiert der FPolicy-Server dann auf die Leseanforderung als ZULASSEN oder ABLEHNEN. Basierend darauf, ob die Leseanforderung zulässig oder verweigert wird, sendet ONTAP entweder die angeforderten Informationen oder sendet eine Fehlermeldung an den Client.

Planen der FPolicy-Konfiguration

Anforderungen, Überlegungen und Best Practices für die Konfiguration von FPolicy

Bevor Sie FPolicy Konfigurationen auf Ihren SVMs erstellen und konfigurieren, müssen

Sie bestimmte Anforderungen, Überlegungen und Best Practices für die Konfiguration von FPolicy kennen.

FPolicy-Funktionen werden entweder über die Befehlszeilenschnittstelle (CLI) oder über REST-APIs konfiguriert.

Anforderungen für die Einrichtung von FPolicy

Bevor Sie FPolicy auf Ihrer Storage Virtual Machine (SVM) konfigurieren und aktivieren, müssen Sie bestimmte Anforderungen kennen.

- Auf allen Nodes im Cluster muss eine Version von ONTAP ausgeführt werden, die FPolicy unterstützt.
- Wenn Sie nicht die native FPolicy Engine von ONTAP verwenden, müssen Sie externe FPolicy Server (FPolicy Server) installiert haben.
- Die FPolicy Server müssen auf einem Server installiert werden, auf den über die Daten-LIFs der SVM zugegriffen werden kann, wo FPolicy-Richtlinien aktiviert sind.

> Ab ONTAP 9.8 bietet ONTAP einen Client-LIF-Service für ausgehende FPolicy-Verbindungen, wobei das hinzugefügt wird `data-fpolicy-client` Service: "Weitere Informationen zu LIFs und Service-Richtlinien".

- Die IP-Adresse des FPolicy-Servers muss als primärer oder sekundärer Server in der Konfiguration einer externen FPolicy Engine konfiguriert werden.
- Wenn die FPolicy-Server über einen privilegierten Datenkanal auf Daten zugreifen, müssen die folgenden zusätzlichen Anforderungen erfüllt werden:
  - SMB muss auf dem Cluster lizenziert sein.

    Der privilegierte Datenzugriff erfolgt über SMB-Verbindungen.
  - Für den Zugriff auf Dateien über den privilegierten Datenkanal müssen Benutzeranmeldeinformationen konfiguriert werden.
  - Der FPolicy-Server muss unter den in der FPolicy-Konfiguration konfigurierten Anmeldeinformationen ausgeführt werden.
  - Alle Daten-LIFs, die für die Kommunikation mit den FPolicy-Servern verwendet werden, müssen konfiguriert werden `cifs` Als eines der zulässigen Protokolle.

    Dies schließt die LIFs ein, die für Passthrough-Read-Verbindungen verwendet werden.
- Ab ONTAP 9.14.1 können Sie mit FPolicy einen persistenten Speicher einrichten, um Dateizugriffsereignisse für asynchrone, nicht obligatorische Richtlinien auf der SVM zu erfassen. Persistente Speicher können die Client-I/O-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu verringern. Synchrone (obligatorische oder nicht obligatorische) und asynchrone obligatorische Konfigurationen werden nicht unterstützt.

Best Practices und Empfehlungen beim Einrichten von FPolicy

Wenn Sie FPolicy auf Storage Virtual Machines (SVMs) einrichten, lernen Sie die allgemeinen Best Practices und Empfehlungen der Konfiguration kennen. So können Sie sicherstellen, dass Ihre FPolicy-Konfiguration eine robuste Monitoring-Performance sowie Ergebnisse liefert, die Ihre Anforderungen erfüllen.

Arbeiten Sie mit Ihrer FPolicy-Partnerapplikation zusammen, um spezifische Richtlinien in Bezug auf

Performance, Größenbestimmung und Konfiguration zu erhalten.

Konfiguration von Richtlinien

Die Konfiguration der externen FPolicy Engine, Ereignisse und Umfang für SVMs können die Benutzerfreundlichkeit und die Sicherheit insgesamt verbessern.

- Konfiguration der FPolicy externen Engine für SVMs:
  - Zusätzliche Sicherheit ist mit Performance-Kosten verbunden. Die Aktivierung der SSL-Kommunikation (Secure Sockets Layer) wirkt sich auf die Leistung des Zugriffs auf Freigaben aus.
  - Die externe FPolicy Engine sollte mit mehr als einem FPolicy Server konfiguriert werden, um Ausfallsicherheit und Hochverfügbarkeit bei der Verarbeitung von FPolicy Serverbenachrichtigungen zu gewährleisten.
- Konfiguration von FPolicy Ereignissen für SVMs:

  Die Überwachung von Dateioperationen wirkt sich auf Ihre Gesamterfahrung aus. Das Filtern unerwünschter Dateioperationen auf der Storage-Seite verbessert beispielsweise die Benutzerfreundlichkeit. NetApp empfiehlt die Einrichtung der folgenden Konfiguration:

  - Überwachung der Mindestanforderungen an Dateioperationen und Aktivierung der maximalen Anzahl von Filtern ohne Unterbrechung des Anwendungsfalls.
  - Verwenden von Filtern für getattr-, Lese-, Schreib-, Öffnen- und Schließvorgänge. In den Home Directory-Umgebungen SMB und NFS kommt ein hoher Prozentsatz dieser Vorgänge zum Einsatz.
- Konfiguration des FPolicy Umfangs für SVMs:

  Schränken Sie die Richtlinien auf relevante Storage-Objekte wie Freigaben, Volumes und Exporte ein, anstatt sie über die gesamte SVM zu aktivieren. NetApp empfiehlt, die Verzeichniserweiterungen zu überprüfen. Wenn der `is-file-extension-check-on-directories-enabled` Parameter ist auf festgelegt `true`, Verzeichnis-Objekte werden den gleichen Erweiterungen Prüfungen wie normale Dateien unterzogen.

Netzwerkkonfiguration

Die Netzwerkverbindung zwischen dem FPolicy-Server und dem Controller sollte geringe Latenz aufweisen. NetApp empfiehlt die Trennung des FPolicy-Datenverkehrs vom Client-Verkehr über ein privates Netzwerk.

Außerdem sollten sich externe FPolicy Server (FPolicy-Server) in der Nähe des Clusters mit hoher Bandbreite befinden, um minimale Latenz und Konnektivität mit hoher Bandbreite zu ermöglichen.

> In einem Szenario, in dem die LIF für FPolicy-Datenverkehr auf einem anderen Port zur LIF für Client-Datenverkehr konfiguriert wird, kann die FPolicy LIF aufgrund eines Portausfalls einen Failover auf den anderen Node durchführen. Infolgedessen kann der FPolicy-Server von dem Node nicht mehr erreicht werden, was dazu führt, dass die FPolicy-Benachrichtigungen für Dateivorgänge auf dem Node fehlschlagen. Um dieses Problem zu vermeiden, überprüfen Sie, ob der FPolicy-Server über mindestens eine logische Schnittstelle auf dem Node erreichbar ist, um FPolicy-Anfragen für die Dateivorgänge zu verarbeiten, die auf diesem Node ausgeführt werden.

Hardwarekonfiguration

Der FPolicy-Server kann entweder auf einem physischen oder einem virtuellen Server ausgeführt werden.

Wenn sich der FPolicy-Server in einer virtuellen Umgebung befindet, sollten Sie dem virtuellen Server dedizierte Ressourcen (CPU, Netzwerk und Arbeitsspeicher) zuweisen.

Das Cluster-Node-to-FPolicy-Serververhältnis sollte optimiert werden, um sicherzustellen, dass FPolicy Server nicht überlastet sind. Dies kann Latenzen bedeuten, wenn die SVM auf Client-Anforderungen reagiert. Das optimale Verhältnis hängt von der Partnerapplikation ab, für die der FPolicy-Server verwendet wird. NetApp empfiehlt die Zusammenarbeit mit Partnern, um den geeigneten Wert zu ermitteln.

Konfiguration mehrerer Richtlinien

Die FPolicy-Richtlinie für natives Blockieren hat unabhängig von der Sequenznummer die höchste Priorität und Richtlinien zur Änderung der Entscheidungsfindung haben eine höhere Priorität als andere. Die Priorität der Richtlinie hängt von dem jeweiligen Anwendungsfall ab. NetApp empfiehlt die Zusammenarbeit mit Partnern, um die entsprechende Priorität zu bestimmen.

Überlegungen zur Größe

FPolicy überwacht SMB- und NFS-Vorgänge inline, sendet Benachrichtigungen an den externen Server und wartet je nach Kommunikationsmodus der externen Engine (synchron oder asynchron) auf eine Antwort. Dieser Prozess wirkt sich auf die Performance von SMB- und NFS-Zugriffs- sowie CPU-Ressourcen aus.

Um Probleme zu beheben, empfiehlt NetApp, gemeinsam mit Partnern die Umgebung zu bewerten und zu dimensionieren, bevor FPolicy aktiviert wird. Die Performance wird von verschiedenen Faktoren beeinflusst, darunter die Benutzeranzahl und Workload-Merkmale wie Vorgänge pro Benutzer und Datengröße, Netzwerklatenz sowie Ausfall- oder Server-Langsamkeit.

Monitoring der Performance

FPolicy ist ein auf Benachrichtigungen basierendes System. Benachrichtigungen werden zur Verarbeitung an einen externen Server gesendet, um eine Antwort an ONTAP zu generieren. Durch diesen Round-Trip-Prozess erhöht sich die Latenz für den Client-Zugriff.

Durch das Monitoring der Performance-Zähler auf dem FPolicy-Server und in ONTAP können Engpässe in der Lösung identifiziert und die Parameter nach Bedarf für eine optimale Lösung angepasst werden. Eine Zunahme der FPolicy-Latenz wirkt sich beispielsweise kaskadierend auf die Latenz des SMB- und NFS-Zugriffs aus. Daher sollten Sie sowohl die Workload- (SMB und NFS) als auch die FPolicy-Latenz überwachen. Zudem können Sie mithilfe von Quality-of-Service-Richtlinien in ONTAP einen Workload für jedes Volume oder jede SVM einrichten, die für FPolicy aktiviert ist.

NetApp empfiehlt, den auszuführen `statistics show –object workload` Befehl zum Anzeigen von Workload-Statistiken. Außerdem sollten Sie die folgenden Parameter überwachen:

- Durchschnittliche Lese-, Schreib- und Leselatenz
- Gesamtzahl der Vorgänge
- Zähler lesen und schreiben

Die Performance von FPolicy-Subsystemen kann mit den folgenden FPolicy-Zählern überwacht werden.

> Sie müssen sich im Diagnosemodus befinden, um Statistiken zu FPolicy zu sammeln.

Schritte

1. FPolicy-Zähler sammeln:
   a. `statistics start -object fpolicy -instance` *`instance_name`* `-sample-id` *`ID`*

b. `statistics start -object fpolicy_policy -instance` *`instance_name`* `-sample-id` *`ID`*

2. FPolicy-Zähler anzeigen:

   a. `statistics show -object fpolicy –instance` *`instance_name`* `-sample-id` *`ID`*

   b. `statistics show -object fpolicy_server –instance` *`instance_name`* `-sample-id` *`ID`*

Der `fpolicy` Und `fpolicy_server` Zähler bieten Informationen zu verschiedenen Leistungsparametern, die in der folgenden Tabelle beschrieben werden.

Zähler	Beschreibung
• „fpolicy“-Zähler*	Abgebrochene_Anforderungen
Anzahl der Bildschirmanforderungen, für die die Verarbeitung auf der SVM abgebrochen wird	Event_count
Liste der Ereignisse, die zu einer Benachrichtigung führen	max_request_Latenz
Maximale Verzögerung bei Bildschirmanforderungen	Ausstehende_Anforderungen
Gesamtanzahl der in Bearbeitung vorhandenen Bildschirmanforderungen	Verarbeitete_Anforderungen
Gesamtzahl der Bildschirmanforderungen, die die fpolicy-Verarbeitung auf der SVM durchlaufen haben	Request_Latency_hist
Histogramm der Latenz für Bildschirmanforderungen	Requests_sended_Rate
Anzahl der pro Sekunde versandten Bildschirmanfragen	Requests_received_Rate
Anzahl der empfangenen Bildschirmanforderungen pro Sekunde	• Zähler „fpolicy_Server“*
max_request_Latenz	Maximale Latenz für eine Bildschirmanforderung
Ausstehende_Anforderungen	Gesamtzahl der auf Antwort wartenden Bildschirmanforderungen
Request_Latency	Durchschnittliche Latenz für Bildschirmanforderung

Zähler	Beschreibung
Request_Latency_hist	Histogramm der Latenz für Bildschirmanforderungen
Request_sent_Rate	Anzahl der an den FPolicy-Server gesendeten Bildschirmanfragen pro Sekunde
Response_received_Rate	Anzahl der vom FPolicy-Server empfangenen Bildschirmantworten pro Sekunde

Managen Sie FPolicy Workflows und Abhängigkeit von anderen Technologien

NetApp empfiehlt, eine FPolicy-Richtlinie zu deaktivieren, bevor Sie Konfigurationsänderungen vornehmen. Wenn Sie beispielsweise eine IP-Adresse in der externen Engine hinzufügen oder ändern möchten, die für die aktivierte Richtlinie konfiguriert ist, deaktivieren Sie zunächst die Richtlinie.

Wenn Sie FPolicy zur Überwachung von NetApp FlexCache Volumes konfigurieren, empfiehlt NetApp, FPolicy nicht für die Überwachung von Lese- und getattr-Dateivorgängen zu konfigurieren. Zur Überwachung dieser Vorgänge in ONTAP ist der Abruf von I2P-Daten (Inode-to-Path) erforderlich. Da die I2P-Daten nicht von FlexCache-Volumes abgerufen werden können, müssen sie vom Ursprungs-Volume abgerufen werden. Daher eliminiert das Monitoring dieser Operationen die Performance-Vorteile, die FlexCache bieten kann.

Wenn FPolicy und eine Off-Box-Antivirus-Lösung implementiert werden, erhält die Virenschutzlösung zuerst Benachrichtigungen. Die FPolicy-Verarbeitung wird erst gestartet, nachdem die Virenprüfung abgeschlossen ist. Es ist wichtig, dass Sie Virenschutzlösungen korrekt dimensionieren, da ein langsamer Virenschutzscanner die Gesamtleistung beeinträchtigen kann.

Überlegungen zum Passthrough-Upgrade und Zurücksetzen

Es gibt bestimmte Überlegungen zum Upgrade und Zurücksetzen, die Sie vor dem Upgrade auf eine ONTAP-Version, die Passthrough-Read unterstützt, oder vor dem Zurücksetzen auf eine Version ohne Passthrough-Read wissen müssen.

Aktualisierung

Nachdem alle Knoten auf eine Version von ONTAP aktualisiert wurden, die FPolicy PassThrough-Read unterstützt, kann der Cluster die Passthrough-Read-Funktion nutzen; allerdings ist Passthrough-read bei bestehenden FPolicy-Konfigurationen standardmäßig deaktiviert. Um Passthrough-read für bestehende FPolicy-Konfigurationen zu verwenden, müssen Sie die FPolicy deaktivieren und die Konfiguration ändern und dann die Konfiguration erneut aktivieren.

Zurücksetzen

Bevor Sie auf eine Version von ONTAP zurücksetzen, die FPolicy Passthrough-Read nicht unterstützt, müssen Sie die folgenden Bedingungen erfüllen:

- Deaktivieren Sie alle Richtlinien mit Passthrough-read, und ändern Sie dann die betroffenen Konfigurationen, sodass sie keine Passthrough-Read-Einstellungen verwenden.
- Deaktivieren Sie FPolicy-Funktionen auf dem Cluster, indem Sie alle FPolicy-Richtlinien auf dem Cluster deaktivieren.

Stellen Sie vor dem Zurücksetzen auf eine Version von ONTAP, die keine persistenten Speicher unterstützt, sicher, dass keine der FPolicy-Richtlinien über einen konfigurierten persistenten Speicher verfügt. Wenn ein persistenter Speicher konfiguriert ist, schlägt die Wiederherstellung fehl.

Was sind die Schritte zum Einrichten einer FPolicy Konfiguration

Bevor FPolicy den Dateizugriff überwachen kann, muss auf der Storage Virtual Machine (SVM) eine FPolicy Konfiguration erstellt und aktiviert werden, für die FPolicy Services erforderlich sind.

Die folgenden Schritte zum Einrichten und Aktivieren einer FPolicy-Konfiguration auf der SVM sind:

1. Erstellen einer externen FPolicy Engine.

   Die externe FPolicy Engine identifiziert die externen FPolicy Server (FPolicy Server), die mit einer bestimmten FPolicy-Konfiguration assoziiert sind. Wenn die interne „`native` FPolicy Engine“ verwendet wird, um eine native File-Blocking-Konfiguration zu erstellen, müssen Sie keine FPolicy-externe Engine erstellen.

2. Erstellen eines FPolicy-Ereignisses.

   Ein FPolicy-Ereignis beschreibt, was die FPolicy überwachen sollte. Ereignisse bestehen aus den zu überwachenden Protokollen und Dateivorgängen und können eine Liste mit Filtern enthalten. Ereignisse verwenden Filter, um die Liste der überwachten Ereignisse einzugrenzen, für die die externe FPolicy-Engine Benachrichtigungen senden muss. Ereignisse geben außerdem an, ob die Richtlinie Volume-Vorgänge überwacht.

3. Erstellen einer FPolicy.

   Die FPolicy ist dafür verantwortlich, mit dem entsprechenden Umfang die zu überwachenden Ereignisse zu verknüpfen und für welche der überwachten Ereignisse Benachrichtigungen an den designierten FPolicy-Server (oder an die native Engine gesendet werden müssen, wenn keine FPolicy-Server konfiguriert sind). Die Richtlinie legt außerdem fest, ob der FPolicy-Server privilegierten Zugriff auf die Daten gewährt, für die er Benachrichtigungen erhält. Ein FPolicy-Server benötigt privilegierten Zugriff, wenn der Server auf die Daten zugreifen muss. Typische Anwendungsfälle, in denen privilegierter Zugriff erforderlich ist, sind das File Blocking, das Kontingentmanagement und das hierarchische Storage-Management. Mit der Richtlinie legen Sie fest, ob die Konfiguration für diese Richtlinie einen FPolicy-Server oder den internen „`nativen` FPolicy Server“ verwendet.

   Eine Richtlinie gibt an, ob das Screening erforderlich ist. Wenn das Screening zwingend erforderlich ist und alle FPolicy Server ausgefallen sind oder keine Antwort von den FPolicy-Servern innerhalb eines definierten Zeitlimits erhalten wird, wird der Dateizugriff verweigert.

   Die Grenzen einer Richtlinie sind die SVM. Eine Richtlinie kann nicht auf mehr als eine SVM angewendet werden. Für eine bestimmte SVM können jedoch mehrere FPolicy-Richtlinien gelten, wobei jedes einzelne von der gleichen oder einer anderen Kombination aus Scope-, Ereignis- und externen Serverkonfigurationen aufweisen kann.

4. Konfigurieren des Richtlinienumfangs.

   Der FPolicy-Umfang legt fest, welche Volumes, Shares oder Exportrichtlinien die Richtlinie für das Monitoring agiert oder nicht. Ein Umfang legt auch fest, welche Dateiendungen vom FPolicy Monitoring enthalten oder ausgeschlossen werden sollten.

   > Ausschlusslisten haben Vorrang vor include-Listen.

5. Aktivieren Sie die FPolicy.

Wenn die Richtlinie aktiviert ist, werden die Kontrollkanäle und optional die privilegierten Datenkanäle verbunden. Der FPolicy-Prozess auf den Nodes, an denen die SVM teilnimmt, beginnt mit der Überwachung der Datei- und Ordnerzugriff und sendet bei Ereignissen, die konfigurierte Kriterien erfüllen, Benachrichtigungen an die FPolicy Server (oder an die native Engine, wenn keine FPolicy-Server konfiguriert sind).

> Wenn die Richtlinie die native Blockierung von Dateien verwendet, wird eine externe Engine nicht konfiguriert oder mit der Richtlinie verknüpft.

Planen Sie die Konfiguration der externen FPolicy Engine

Planen Sie die Konfiguration der externen FPolicy Engine

Bevor Sie die FPolicy External Engine (externe Engine) konfigurieren, müssen Sie verstehen, was es bedeutet, eine externe Engine zu erstellen und welche Konfigurationsparameter verfügbar sind. Anhand dieser Informationen können Sie festlegen, welche Werte für jeden Parameter festgelegt werden sollen.

Informationen, die bei der Erstellung der externen FPolicy Engine definiert werden

Die Konfiguration der externen Engine definiert die Informationen, die FPolicy Verbindungen zu den externen FPolicy Servern (FPolicy-Servern) herstellen und verwalten muss, einschließlich der folgenden Informationen:

- SVM-Name
- Motorname
- Die IP-Adressen der primären und sekundären FPolicy Server und der zu verwendenden TCP-Portnummer für die Verbindung zu den FPolicy Servern
- Ob der Engine-Typ asynchron oder synchron ist
- Wie authentifiziert man die Verbindung zwischen dem Knoten und dem FPolicy-Server

  Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren, müssen Sie auch Parameter konfigurieren, die SSL-Zertifikatsinformationen bereitstellen.

- So verwalten Sie die Verbindung mit verschiedenen erweiterten Berechtigungseinstellungen

  Dazu gehören Parameter, die z. B. Timeout-Werte, Wiederholungswerte, Keep-Alive-Werte, maximale Anforderungswerte, Werte für gesendete und empfangbare Puffergrößen sowie Werte für Sitzungszeitüberschreitungen definieren.

Der `vserver fpolicy policy external-engine create` Mit dem Befehl wird eine FPolicy externe Engine erstellt.

Was sind die grundlegenden externen Motorparameter

Sie können die folgende Tabelle mit grundlegenden FPolicy Konfigurationsparametern verwenden, um Ihre Konfiguration zu planen:

Informationstyp	Option

SVM Gibt den SVM-Namen an, den Sie mit dieser externen Engine verknüpfen möchten. Jede FPolicy-Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienumfang und die Richtlinie, die gemeinsam eine FPolicy-Konfiguration erstellen, müssen mit derselben SVM verknüpft werden.	`-vserver vserver_name`
Motorname Gibt den Namen an, der der externen Engine-Konfiguration zugewiesen werden soll. Sie müssen den Namen der externen Engine später angeben, wenn Sie die FPolicy erstellen. Dadurch wird die externe Engine mit der Richtlinie verknüpft. Der Name kann bis zu 256 Zeichen lang sein. Wenn Sie den Namen der externen Engine in einer Disaster-Recovery-Konfiguration von MetroCluster oder SVM konfigurieren, sollte der Name bis zu 200 Zeichen lang sein. Der Name kann eine beliebige Kombination der folgenden Zeichen des ASCII-Bereichs enthalten: • `a` Bis `z` • `A` Bis `Z` • `0` Bis `9` • „_“,„-`", and ".`“	`-engine-name engine_name`
Primary FPolicy Server Gibt die primären FPolicy Server an, an die der Node Benachrichtigungen für eine bestimmte FPolicy sendet. Der Wert wird als kommagetrennte Liste von IP-Adressen angegeben. Wenn mehr als eine IP-Adresse für den primären Server angegeben wird, erstellt jeder Node, an dem die SVM teilnimmt, eine Kontrollverbindung zu jedem angegebenen primären FPolicy-Server zum Zeitpunkt der Aktivierung der Richtlinie. Wenn Sie mehrere primäre FPolicy-Server konfigurieren, werden Benachrichtigungen nach Round Robin-Verfahren an die FPolicy-Server gesendet. Wenn die externe Engine in einer MetroCluster- oder SVM-Disaster-Recovery-Konfiguration verwendet wird, sollten Sie die IP-Adressen der FPolicy-Server am Quellstandort als primäre Server angeben. Die IP-Adressen der FPolicy-Server am Zielstandort sollten als sekundäre Server angegeben werden.	`-primary-servers IP_address,...`

Portnummer Gibt die Portnummer des FPolicy-Dienstes an.	`-port integer`
Secondary FPolicy Server Gibt die sekundären FPolicy-Server an, an die Dateizugriffsereignisse für eine bestimmte FPolicy gesendet werden sollen. Der Wert wird als kommagetrennte Liste von IP-Adressen angegeben. Sekundäre Server werden nur verwendet, wenn keiner der primären Server erreichbar ist. Verbindungen zu sekundären Servern werden hergestellt, wenn die Richtlinie aktiviert ist. Benachrichtigungen werden jedoch nur an sekundäre Server gesendet, wenn keiner der primären Server erreichbar ist. Wenn Sie mehrere sekundäre Server konfigurieren, werden Benachrichtigungen nach Round Robin-Verfahren an die FPolicy-Server gesendet.	`-secondary-servers IP_address,...`
Externer Motortyp Gibt an, ob die externe Engine im synchronen oder asynchronen Modus arbeitet. FPolicy arbeitet standardmäßig im synchronen Modus. Wenn eingestellt auf `synchronous`, Die Verarbeitung von Dateianfragen sendet eine Benachrichtigung an den FPolicy-Server, wird aber dann erst fortgesetzt, nachdem eine Antwort vom FPolicy-Server erhalten wurde. In diesem Punkt wird der Anforderungsfluss entweder fortgesetzt oder die Verarbeitung führt zu Denial-DoS, je nachdem, ob die Antwort vom FPolicy-Server die angeforderte Aktion zulässt. Wenn eingestellt auf `asynchronous`, Die Verarbeitung von Dateianfragen sendet eine Benachrichtigung an den FPolicy-Server und wird dann fortgesetzt.	`-extern-engine-type external_engine_type` Der Wert für diesen Parameter kann einer der folgenden Werte sein: • `synchronous` • `asynchronous`

SSL-Option zur Kommunikation mit FPolicy Server Gibt die SSL-Option für die Kommunikation mit dem FPolicy-Server an. Dies ist ein erforderlicher Parameter. Sie können eine der Optionen basierend auf den folgenden Informationen auswählen: • Wenn eingestellt auf `no-auth`, Keine Authentifizierung erfolgt. Die Kommunikationsverbindung wird über TCP hergestellt. • Wenn eingestellt auf `server-auth`, Die SVM authentifiziert den FPolicy-Server mithilfe einer SSL-Server-Authentifizierung. • Wenn eingestellt auf `mutual-auth`. Gegenseitige Authentifizierung erfolgt zwischen der SVM und dem FPolicy-Server. Die SVM authentifiziert den FPolicy-Server und der FPolicy-Server authentifiziert die SVM. Wenn Sie die gegenseitige SSL-Authentifizierung konfigurieren, müssen Sie auch die konfigurieren `-certificate-common-name`, `-certificate-serial`, und `-certifcate-ca` Parameter.	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
Zertifikat FQDN oder benutzerdefinierter allgemeiner Name Gibt den Zertifikatsnamen an, der verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy-Server konfiguriert ist. Sie können den Zertifikatnamen als FQDN oder als benutzerdefinierten gemeinsamen Namen angeben. Wenn Sie angeben `mutual-auth` Für das `-ssl-option` Parameter. Sie müssen einen Wert für das angeben `-certificate-common-name` Parameter.	`-certificate-common -name` `text`
Seriennummer des Zertifikats Gibt die Seriennummer des Zertifikats an, das für die Authentifizierung verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy-Server konfiguriert ist. Wenn Sie angeben `mutual-auth` Für das `-ssl-option` Parameter. Sie müssen einen Wert für das angeben `-certificate-serial` Parameter.	`-certificate-serial` `text`
Zertifizierungsstelle Gibt den CA-Namen des Zertifikats an, das für die Authentifizierung verwendet wird, wenn die SSL-Authentifizierung zwischen der SVM und dem FPolicy-Server konfiguriert ist. Wenn Sie angeben `mutual-auth` Für das `-ssl-option` Parameter. Sie müssen einen Wert für das angeben `-certificate-ca` Parameter.	`-certificate-ca` `text`

Was sind die erweiterten Optionen der externen Engine

Sie können die folgende Tabelle mit erweiterten FPolicy Konfigurationsparametern verwenden, wenn Sie planen, Ihre Konfiguration mit erweiterten Parametern anzupassen. Mit diesen Parametern ändern Sie das Kommunikationsverhalten zwischen den Cluster-Nodes und den FPolicy-Servern:

Informationstyp	Option
Timeout zum Abbrechen einer Anfrage Gibt das Zeitintervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Dass der Knoten auf eine Antwort vom FPolicy-Server wartet. Wenn das Zeitüberschreitungsintervall abgelaufen ist, sendet der Node eine Anforderung zum Abbrechen an den FPolicy-Server. Der Node sendet dann die Benachrichtigung an einen alternativen FPolicy-Server. Dieses Timeout unterstützt den Umgang mit einem FPolicy-Server, der nicht reagiert, was die Reaktion von SMB/NFS-Clients verbessern kann. Das Abbrechen von Anfragen nach einem Timeout kann außerdem dazu beitragen, Systemressourcen freizugeben, da die Benachrichtigungsanfrage von einem heruntergedrückten/schlechten FPolicy-Server auf einen alternativen FPolicy-Server verschoben wird. Der Bereich für diesen Wert ist `0` Bis `100`. Wenn der Wert auf festgelegt ist `0`, Die Option ist deaktiviert und Cancel Request Nachrichten werden nicht an den FPolicy-Server gesendet. Die Standardeinstellung lautet `20s`.	`-reqs-cancel-timeout integer`[H m m m V natürlich]
Timeout für Abbruch einer Anfrage Gibt die Zeitüberschreitung in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Zum Abbruch einer Anfrage. Der Bereich für diesen Wert ist `0` Bis `200`.	`-reqs-abort-timeout` ` `integer`[H m m m V natürlich]
Intervall für das Senden von Statusanforderungen Gibt das Intervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Nach dem eine Statusanforderung an den FPolicy-Server gesendet wird. Der Bereich für diesen Wert ist `0` Bis `50`. Wenn der Wert auf festgelegt ist `0`, Die Option ist deaktiviert und Status Request Nachrichten werden nicht an den FPolicy-Server gesendet. Die Standardeinstellung lautet `10s`.	`-status-req-interval integer`[H m m m V natürlich]
Maximale Anzahl ausstehende Anforderungen auf dem FPolicy-Server Gibt die maximale Anzahl der ausstehenden Anforderungen an, die auf dem FPolicy-Server in die Warteschlange gestellt werden können. Der Bereich für diesen Wert ist `1` Bis `10000`. Die Standardeinstellung lautet `500`.	`-max-server-reqs integer`

Timeout zum Trennen eines nicht ansprechenden FPolicy Servers Gibt das Zeitintervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Nach der die Verbindung zum FPolicy-Server beendet wird. Die Verbindung wird nach dem Timeout-Zeitraum nur beendet, wenn die Warteschlange des FPolicy-Servers die maximal zulässigen Anforderungen enthält und innerhalb des Timeout-Zeitraums keine Antwort empfangen wird. Es gibt entweder eine maximal zulässige Anzahl von Anforderungen `50` (Die Standardeinstellung) oder die vom angegebene Zahl `max-server-reqs-` Parameter. Der Bereich für diesen Wert ist `1` Bis `100`. Die Standardeinstellung lautet `60s`.	`-server-progress -timeout integer`[H m m m V natürlich]
Intervall zum Senden von Keep-Alive-Nachrichten an den FPolicy-Server Gibt das Zeitintervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Bei denen Keep-Alive-Nachrichten an den FPolicy-Server gesendet werden. Keep-Alive-Meldungen erkennen halboffene Verbindungen. Der Bereich für diesen Wert ist `10` Bis `600`. Wenn der Wert auf festgelegt ist `0`, Die Option ist deaktiviert und Keep-Alive-Nachrichten werden nicht an die FPolicy-Server gesendet. Die Standardeinstellung lautet `120s`.	`-keep-alive-interval-integer`[H m m m V natürlich]
Maximale Anzahl Verbindungsversuche Gibt die maximale Anzahl der Male an, die die SVM nach einer Verbindungsherstellung versucht, eine Verbindung zum FPolicy-Server herzustellen. Der Bereich für diesen Wert ist `0` Bis `20`. Die Standardeinstellung lautet `5`.	`-max-connection-retries integer`
Puffergröße empfangen Gibt die Empfangsbuffer-Größe des angeschlossenen Sockets für den FPolicy-Server an. Der Standardwert ist 256 Kilobyte (KB). Wenn der Wert auf 0 gesetzt ist, wird die Größe des Empfangspuffers auf einen vom System definierten Wert gesetzt. Wenn beispielsweise die Standard-Empfangspuffgröße des Sockets 65536 Byte beträgt, wird durch Setzen des einstellbaren Werts auf 0 die Socket-Puffergröße auf 65536 Byte gesetzt. Sie können einen beliebigen nicht-Standardwert verwenden, um die Größe (in Byte) des Empfangspuffers festzulegen.	`-recv-buffer-size integer`

Puffergröße senden Gibt die Sendepuffer-Größe des angeschlossenen Sockets für den FPolicy-Server an. Der Standardwert ist 256 Kilobyte (KB). Wenn der Wert auf 0 gesetzt ist, wird die Größe des Sendepuffers auf einen vom System definierten Wert gesetzt. Wenn beispielsweise die Standard-Sendepuffer-Größe des Sockets auf 65536 Byte eingestellt ist, indem der einstellbare Wert auf 0 gesetzt wird, wird die Socket-Puffergröße auf 65536 Byte gesetzt. Sie können einen beliebigen nicht-Standardwert verwenden, um die Größe (in Bytes) des Sendepuffers festzulegen.	`-send-buffer-size integer`
Timeout zum Löschen einer Sitzungs-ID während der erneuten Verbindung Gibt das Intervall in Stunden an (`h`), Minuten (`m`) Oder Sekunden (`s`) Anschließend wird während der erneuten Verbindungsversuche eine neue Sitzungs-ID an den FPolicy-Server gesendet. Wenn die Verbindung zwischen dem Speicher-Controller und dem FPolicy-Server beendet wird und eine erneute Verbindung innerhalb des hergestellt wird `-session-timeout` Intervall wird die alte Session-ID an den FPolicy Server gesendet, damit es Antworten für alte Benachrichtigungen senden kann. Der Standardwert ist 10 Sekunden.	`-session-timeout` [`integer`H][`integer`M][`integer`S]

Weitere Informationen zum Konfigurieren von FPolicy-externen Engines zur Verwendung von SSL-authentifizierten Verbindungen

Sie müssen einige zusätzliche Informationen wissen, wenn Sie die FPolicy externe Engine konfigurieren möchten, um SSL bei der Verbindung zu FPolicy-Servern zu verwenden.

SSL-Serverauthentifizierung

Wenn Sie die FPolicy-externe Engine für die SSL-Server-Authentifizierung konfigurieren, müssen Sie vor dem Erstellen der externen Engine das öffentliche Zertifikat der Zertifizierungsstelle (CA) installieren, die das FPolicy-Server-Zertifikat signiert hat.

Gegenseitige Authentifizierung

Wenn Sie FPolicy externe Engines konfigurieren, um bei der Verbindung von Storage Virtual Machine (SVM)-Daten-LIFs mit externen FPolicy-Servern SSL gegenseitige Authentifizierung zu verwenden, bevor Sie die externe Engine erstellen, Sie müssen das öffentliche Zertifikat der CA installieren, die das FPolicy-Serverzertifikat unterzeichnet hat, sowie das öffentliche Zertifikat und die Schlüsseldatei zur Authentifizierung der SVM. Sie dürfen dieses Zertifikat nicht löschen, während alle FPolicy-Richtlinien das installierte Zertifikat verwenden.

Wenn das Zertifikat gelöscht wird, während FPolicy es für gegenseitige Authentifizierung verwendet, wenn eine Verbindung zu einem externen FPolicy-Server hergestellt wird, können Sie eine deaktivierte FPolicy, die dieses

Zertifikat verwendet, nicht aktivieren. Die FPolicy kann in dieser Situation nicht wieder aktiviert werden, auch wenn ein neues Zertifikat mit denselben Einstellungen erstellt und auf der SVM installiert wird.

Wenn das Zertifikat gelöscht wurde, müssen Sie ein neues Zertifikat installieren, neue FPolicy-externe Engines erstellen, die das neue Zertifikat verwenden, und die neuen externen Engines mit der FPolicy verknüpfen, die Sie durch Ändern der FPolicy erneut aktivieren möchten.

Installieren Sie Zertifikate für SSL

Das öffentliche Zertifikat der CA, das zum Signieren des FPolicy-Server-Zertifikats verwendet wird, wird mithilfe der installiert `security certificate install` Befehl mit dem `-type` Parameter auf gesetzt `client-ca`. Der für die Authentifizierung der SVM erforderliche private Schlüssel und das öffentliche Zertifikat werden mithilfe des installiert `security certificate install` Befehl mit dem `-type` Parameter auf gesetzt `server`.

Zertifikate replizieren sich in SVM Disaster-Recovery-Beziehungen nicht mit einer Konfiguration, die keine IDs enthält

Sicherheitszertifikate, die für die SSL-Authentifizierung verwendet werden, wenn Verbindungen zu FPolicy-Servern hergestellt werden, replizieren keine SVM-Disaster-Recovery-Ziele mit Konfigurationen, die keine ID-Preserve enthalten. Obwohl die externe FPolicy-Engine-Konfiguration auf der SVM repliziert wird, werden Sicherheitszertifikate nicht repliziert. Sie müssen die Sicherheitszertifikate manuell auf dem Ziel installieren.

Wenn Sie eine SVM Disaster-Recovery-Beziehung einrichten, wählen Sie den Wert für `-identity -preserve` Option des `snapmirror create` Der Befehl bestimmt die Konfigurationsdetails, die in der Ziel-SVM repliziert werden.

Wenn Sie die einstellen `-identity-preserve` Option auf `true` (ID-Preserve) werden alle FPolicy Konfigurationsdetails repliziert, einschließlich der Informationen zum Sicherheitszertifikat. Sie müssen die Sicherheitszertifikate nur auf dem Ziel installieren, wenn Sie die Option auf festlegen `false` (Nicht-ID-Preserve).

Einschränkungen für externe Cluster-Scoped FPolicy Engines mit MetroCluster und SVM Disaster-Recovery-Konfigurationen

Sie können eine externe Cluster-Scoped FPolicy Engine erstellen, indem Sie die Cluster Storage Virtual Machine (SVM) der externen Engine zuweisen. Beim Erstellen einer externen Engine mit Cluster-Umfang in einer Disaster-Recovery-Konfiguration mit MetroCluster oder SVM gibt es jedoch bestimmte Einschränkungen bei der Auswahl der Authentifizierungsmethode, die die SVM für die externe Kommunikation mit dem FPolicy-Server verwendet.

Es gibt drei Authentifizierungsoptionen, die Sie bei der Erstellung von externen FPolicy-Servern wählen können: Keine Authentifizierung, SSL-Serverauthentifizierung und gegenseitige SSL-Authentifizierung. Obwohl die Auswahl der Authentifizierungsoption für den externen FPolicy-Server einer Daten-SVM nicht eingeschränkt ist, gibt es Einschränkungen bei der Erstellung einer externen Cluster-Scoped FPolicy Engine:

Konfiguration	Erlaubt?
Disaster Recovery mit MetroCluster oder SVM und eine externe Cluster-FPolicy-Scoped-Engine ohne Authentifizierung (SSL ist nicht konfiguriert)	Ja.

Disaster Recovery für MetroCluster oder SVM und eine externe Cluster-FPolicy Scoped Engine mit SSL-Server oder gegenseitige SSL-Authentifizierung	Nein

- Wenn eine externe Cluster-Scoped FPolicy Engine mit SSL-Authentifizierung vorhanden ist und Sie eine MetroCluster- oder SVM-Disaster-Recovery-Konfiguration erstellen möchten, müssen Sie diese externe Engine ändern, um keine Authentifizierung zu verwenden oder die externe Engine zu entfernen, bevor Sie die MetroCluster- oder SVM-Disaster Recovery-Konfiguration erstellen können.
- Falls die Disaster Recovery-Konfiguration von MetroCluster oder SVM bereits vorhanden ist, verhindert ONTAP die Erstellung einer externen FPolicy Engine mit Cluster-Umfang und SSL-Authentifizierung.

Füllen Sie das Konfigurationsarbeitsblatt für die externe FPolicy Engine aus

Mit diesem Arbeitsblatt können Sie die Werte aufzeichnen, die Sie während der Konfiguration der externen FPolicy Engine benötigen. Wenn ein Parameterwert erforderlich ist, müssen Sie vor der Konfiguration der externen Engine festlegen, welchen Wert für diese Parameter verwendet werden soll.

Informationen für eine grundlegende externe Engine-Konfiguration

Sie sollten aufzeichnen, ob Sie die einzelnen Parametereinstellungen in die externe Engine-Konfiguration aufnehmen möchten, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

Informationstyp	Erforderlich	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM	Ja.	Ja.	
Motorname	Ja.	Ja.	
Primäre FPolicy-Server	Ja.	Ja.	
Port-Nummer	Ja.	Ja.	
Sekundäre FPolicy Server	Nein		
Externer Motortyp	Nein		
SSL-Option zur Kommunikation mit externem FPolicy-Server	Ja.	Ja.	
FQDN des Zertifikats oder benutzerdefinierter allgemeiner Name	Nein		
Seriennummer des Zertifikats	Nein		
Zertifizierungsstelle	Nein		

Informationen für erweiterte externe Motorparameter

Um eine externe Engine mit erweiterten Parametern zu konfigurieren, müssen Sie den Konfigurationsbefehl im erweiterten Berechtigungsmodus eingeben.

Informationstyp	Erforderlich	Einschließlich	Ihre Werte
Zeitüberschreitung beim Abbrechen einer Anfrage	Nein		
Timeout beim Abbrechen einer Anfrage	Nein		
Intervall für das Senden von Statusanforderungen	Nein		
Maximale offene Anfragen auf dem FPolicy-Server	Nein		
Timeout zum Trennen eines nicht ansprechenden FPolicy-Servers	Nein		
Intervall für das Senden von Keep-Alive-Nachrichten an den FPolicy-Server	Nein		
Maximale Anzahl von Verbindungsversuchen	Nein		
Empfangspuffgröße	Nein		
Puffergröße senden	Nein		
Zeitüberschreitung beim Spülen einer Sitzungs-ID während der erneuten Verbindung	Nein		

Planen Sie die FPolicy Event-Konfiguration

Planen Sie die FPolicy Event-Konfiguration im Überblick

Bevor Sie FPolicy-Ereignisse konfigurieren, müssen Sie verstehen, was es bedeutet, ein FPolicy-Ereignis zu erstellen. Sie müssen festlegen, welche Protokolle das Ereignis überwachen soll, welche Ereignisse überwacht werden sollen und welche Ereignisfilter verwendet werden sollen. Mit diesen Informationen können Sie die Werte planen, die Sie festlegen möchten.

Was es bedeutet, ein FPolicy-Ereignis zu erstellen

Erstellen des FPolicy-Ereignisses bedeutet, Informationen zu definieren, die der FPolicy-Prozess bestimmen muss, welche Dateizugriffsvorgänge überwacht werden und für welche der überwachten Ereignisse

Benachrichtigungen an den externen FPolicy-Server gesendet werden sollen. Die FPolicy-Event-Konfiguration definiert die folgenden Konfigurationsinformationen:

- Name der Storage Virtual Machine (SVM
- Ereignis-Name
- Welche Protokolle zu überwachen sind

  FPolicy kann SMB-, NFSv3- und NFSv4-Dateizugriff überwachen.

- Welche Dateivorgänge zu überwachen sind

  Nicht alle Dateivorgänge sind für jedes Protokoll gültig.

- Welche Dateifilter konfiguriert werden sollen

  Es sind nur bestimmte Kombinationen von Dateioperationen und Filtern gültig. Jedes Protokoll verfügt über einen eigenen Satz unterstützter Kombinationen.

- Gibt an, ob die Volume-Mount- und Unmount-Vorgänge überwacht werden sollen

> Es gibt eine Abhängigkeit mit drei Parametern (`-protocol`, `-file-operations`, `-filters`). Die folgenden Kombinationen gelten für die drei Parameter:
>
> - Sie können den angeben `-protocol` Und `-file-operations` Parameter.
> - Sie können alle drei Parameter angeben.
> - Sie können keinen Parameter angeben.

Was die FPolicy-Event-Konfiguration enthält

Sie können die folgende Liste der verfügbaren FPolicy Event-Konfigurationsparameter verwenden, um Ihre Konfiguration zu planen:

Informationstyp	Option
SVM Gibt den SVM-Namen an, den Sie mit diesem FPolicy-Ereignis verknüpfen möchten. Jede FPolicy-Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienumfang und die Richtlinie, die gemeinsam eine FPolicy-Konfiguration erstellen, müssen mit derselben SVM verknüpft werden.	`-vserver vserver_name`

Ereignisname Gibt den Namen an, der dem FPolicy-Ereignis zugewiesen werden soll. Wenn Sie die FPolicy erstellen, verknüpfen Sie das FPolicy Ereignis mit der Richtlinie unter Verwendung des Ereignisnamens. Der Name kann bis zu 256 Zeichen lang sein. Der Name sollte bis zu 200 Zeichen lang sein, wenn das Ereignis in einer Disaster-Recovery-Konfiguration mit MetroCluster oder SVM konfiguriert wird. Der Name kann eine beliebige Kombination der folgenden Zeichen des ASCII-Bereichs enthalten: • `a` Bis `z` • `A` Bis `Z` • `0` Bis `9` • „`_`“, „`-``", and ".`“	`-event-name` `event_name`
Protokoll Gibt an, welches Protokoll für das FPolicy-Ereignis konfiguriert werden soll. Die Liste für `-protocol` Kann einen der folgenden Werte enthalten: • `cifs` • `nfsv3` • `nfsv4` Wenn Sie angeben `-protocol`, Dann müssen Sie einen gültigen Wert im angeben `-file-operations` Parameter. Wenn sich die Protokollversion ändert, können sich die gültigen Werte ändern.	`-protocol` `protocol`

Dateivorgänge Gibt die Liste der Dateivorgänge für das FPolicy-Ereignis an. Das Ereignis überprüft die in dieser Liste angegebenen Vorgänge von allen Client-Anforderungen mithilfe des in angegebenen Protokolls `-protocol` Parameter. Sie können ein oder mehrere Dateivorgänge mit einer durch Komma getrennten Liste auflisten. Die Liste für `-file-operations` Kann einen oder mehrere der folgenden Werte enthalten: • `close` Für Dateischließvorgänge • `create` Für Dateiererstellungsprozesse • `create-dir` Erstellen von Verzeichnisvorgängen • `delete` Für Dateilösch-Vorgänge • `delete_dir` Für Vorgänge zum Löschen von Verzeichnissen • `getattr` Für get-Attributvorgänge • `link` Für Verbindungsvorgänge • `lookup` Für Suchvorgänge • `open` Für Dateiöffnungsprozesse • `read` Für Dateilesevorgänge • `write` Für Dateischreibvorgänge • `rename` Für Dateiumbenennung • `rename_dir` Für Verzeichnisumbenennung • `setattr` Für Set-Attributvorgänge • `symlink` Für symbolische Link-Vorgänge ⓘ Wenn Sie angeben `-file-operations`, Dann müssen Sie ein gültiges Protokoll im angeben `-protocol` Parameter.	`-file-operations file_operations,...`

Filter Gibt die Liste der Filter für einen bestimmten Dateivorgang für das angegebene Protokoll an. Die Werte in `-filters` Mit dem Parameter werden Client-Anforderungen gefiltert. Die Liste kann eine oder mehrere der folgenden Elemente enthalten: Wenn Sie den angeben `-filters` Parameter, dann müssen Sie auch gültige Werte für das angeben `-file -operations` Und `-protocol` Parameter. • `monitor-ads` Option zum Filtern der Clientanforderung nach alternativen Datenströmen. • `close-with-modification` Option zum Filtern der Clientanfrage nach Abschluss mit Änderung. • `close-without-modification` Option zum Filtern der Clientanfrage nach Abschluss ohne Änderung. • `first-read` Option zum Filtern der Client-Anforderung nach dem ersten Lesen. • `first-write` Option zum Filtern der Client-Anforderung nach dem ersten Schreibvorgang. • `offline-bit` Option zum Filtern der Client-Anforderung nach Offline-Bit-Set. Wenn Sie diesen Filter festlegen, wird der FPolicy-Server nur benachrichtigt, wenn auf Offline-Dateien zugegriffen wird. • `open-with-delete-intent` Option zum Filtern der Client-Anforderung nach „Open with delete Intent“. Wenn Sie diesen Filter festlegen, wird der FPolicy-Server nur benachrichtigt, wenn versucht wird, eine Datei mit der Absicht zu öffnen, sie zu löschen. Dies wird von Dateisystemen verwendet, wenn die `FILE_DELETE_ON_CLOSE` Flag ist angegeben. • `open-with-write-intent` Option zum Filtern der Client-Anforderung nach Open mit Write Intent. Die Einstellung dieses Filters führt dazu, dass der FPolicy-Server eine Benachrichtigung nur erhält, wenn versucht wird, eine Datei mit der Absicht zu öffnen, etwas darin zu schreiben. • `write-with-size-change` Option zum Filtern der Client-Anfrage nach Schreiben mit Größenänderung.	`-filters filter, ...`

Filter Fortsetzung • `setattr-with-owner-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern des Inhabers einer Datei oder eines Verzeichnisses. • `setattr-with-group-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der Gruppe einer Datei oder eines Verzeichnisses. • `setattr-with-sacl-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der SACL in einer Datei oder einem Verzeichnis. Dieser Filter ist nur für die SMB- und NFSv4-Protokolle verfügbar. • `setattr-with-dacl-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der DACL in einer Datei oder einem Verzeichnis. Dieser Filter ist nur für die SMB- und NFSv4-Protokolle verfügbar. • `setattr-with-modify-time-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der Änderungszeit einer Datei oder eines Verzeichnisses. • `setattr-with-access-time-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der Zugriffszeit einer Datei oder eines Verzeichnisses. • `setattr-with-creation-time-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der Erstellungszeit einer Datei oder eines Verzeichnisses. Diese Option ist nur für das SMB-Protokoll verfügbar. • `setattr-with-mode-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der Modus-Bits in einer Datei oder einem Verzeichnis. • `setattr-with-size-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der Größe einer Datei. • `setattr-with-allocation-size-change` Option zum Filtern der Client-setattr-Anforderungen zum Ändern der Zuordnungsgröße einer Datei. Diese Option ist nur für das SMB-Protokoll verfügbar. • `exclude-directory` Option zum Filtern der Clientanforderungen nach Verzeichnisvorgängen. Wenn dieser Filter angegeben ist, werden die Verzeichnisvorgänge nicht überwacht.	`-filters filter, ...`

Ist Volumenvorgang erforderlich Gibt an, ob Monitoring für Volume-Mount- und Unmount-Vorgänge erforderlich ist. Die Standardeinstellung lautet `false`.	`-volume-operation` {`true`
`false`} `-filters filter`, ...	*FPolicy Zugriff verweigert Benachrichtigungen* Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen für fehlgeschlagene Dateivorgänge erhalten, da sie keine Berechtigungen haben. Diese Benachrichtigungen sind wertvoll für Sicherheit, Ransomware-Schutz und Governance. Es werden Benachrichtigungen für Dateioperationen generiert, die aufgrund fehlender Berechtigungen fehlgeschlagen sind. Dazu gehören: • Fehler aufgrund von NTFS-Berechtigungen. • Fehler aufgrund von Unix-Modus-Bits. • Fehler aufgrund von NFSv4-ACLs.
`-monitor-fileop-failure` {`true`	`false`}

Unterstützte Dateioperationen und Filterkombinationen, die FPolicy für SMB überwachen kann

Wenn Sie Ihr FPolicy-Ereignis konfigurieren, müssen Sie beachten, dass nur bestimmte Kombinationen von Dateioperationen und Filtern zur Überwachung von SMB-Dateizugriffsvorgängen unterstützt werden.

Die folgende Tabelle enthält eine Liste der unterstützten Dateivorgänge und Filterkombinationen für die FPolicy-Überwachung von SMB-Dateizugriffsereignissen:

Unterstützte Dateivorgänge	Unterstützte Filter
Schließen	Monitor-ads, Offline-Bit, Close-with-Modifizierung, Close-ohne-Änderung, Close-with-Read, Exclude-Verzeichnis
Erstellen	Monitor-ADS, Offline-Bit
Create_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.

Löschen	Monitor-ADS, Offline-Bit
Delete_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Getattr	Offline-Bit, exclude-dir
Offen	Monitor-ads, Offline-Bit, open-with-delete-Intent, open-with-write-Intent, exclude-dir
Lesen	Monitor-ADS, Offline-Bit, First-Read
Schreiben	Monitor-ads, Offline-Bit, First-Write, Write-with-size-Change
Umbenennen	Monitor-ADS, Offline-Bit
Umbenennen_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Sollwert	Monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_Group_change, setattr_with_Mode_change, Setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_Access_time_change, setattr_with_creation_time_change, Setattr_with_size_change, setattr_with_allokation_size_change, exclude_Directory

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen für fehlgeschlagene Dateivorgänge erhalten, da sie keine Berechtigungen haben. Die Liste der unterstützten Zugriffsverweigerung Dateioperationen und Filterkombinationen für das FPolicy Monitoring von SMB-Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützter Zugriff verweigert Dateivorgang	Unterstützte Filter
Offen	NA

Unterstützte Dateioperationen und Filterkombinationen, die FPolicy für NFSv3 überwachen kann

Wenn Sie Ihr FPolicy-Ereignis konfigurieren, müssen Sie beachten, dass nur bestimmte Kombinationen von Dateioperationen und Filtern für die Überwachung von NFSv3-Dateizugriffsoperationen unterstützt werden.

Die Liste der unterstützten Dateivorgänge und Filterkombinationen für die FPolicy-Überwachung von NFSv3-Dateizugriffsereignissen wird in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
Erstellen	Offline-Bit

Create_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Löschen	Offline-Bit
Delete_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Verlinken	Offline-Bit
Suchen	Offline-Bit, exclude-dir
Lesen	Offline-Bit, First-Read
Schreiben	Offline-Bit, First-Write, Write-with-size-change
Umbenennen	Offline-Bit
Umbenennen_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Sollwert	Offline-Bit, setattr_with_owner_change, setattr_with_Group_change, setattr_with_Mode_change, setattr_with_modify_time_change, Setattr_with_Access_time_change, setattr_with_size_change, exclude_Directory
Symbolischer Link	Offline-Bit

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen für fehlgeschlagene Dateivorgänge erhalten, da sie keine Berechtigungen haben. Die Liste der unterstützten Zugriffsverweigerung bei Dateioperationen und Filterkombinationen für das FPolicy Monitoring von NFSv3 Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützter Zugriff verweigert Dateivorgang	Unterstützte Filter
Datenzugriff	NA
Erstellen	NA
Create_dir	NA
Löschen	NA
Delete_dir	NA
Verlinken	NA
Lesen	NA

Umbenennen	NA
Umbenennen_dir	NA
Sollwert	NA
Schreiben	NA

Unterstützte Dateioperationen und Filterkombinationen, die FPolicy für NFSv4 überwachen kann

Wenn Sie Ihr FPolicy-Ereignis konfigurieren, müssen Sie beachten, dass nur bestimmte Kombinationen von Dateioperationen und Filtern für die Überwachung von NFSv4-Dateizugriffsvorgängen unterstützt werden.

Die Liste der unterstützten Dateivorgänge und Filterkombinationen für FPolicy-Überwachung von NFSv4-Dateizugriffsereignissen wird in der folgenden Tabelle aufgeführt:

Unterstützte Dateivorgänge	Unterstützte Filter
Schließen	Offline-Bit, exclude-Directory
Erstellen	Offline-Bit
Create_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Löschen	Offline-Bit
Delete_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.
Getattr	Offline-Bit, exclude-Directory
Verlinken	Offline-Bit
Suchen	Offline-Bit, exclude-Directory
Offen	Offline-Bit, exclude-Directory
Lesen	Offline-Bit, First-Read
Schreiben	Offline-Bit, First-Write, Write-with-size-change
Umbenennen	Offline-Bit
Umbenennen_dir	Derzeit wird kein Filter für diesen Dateivorgang unterstützt.

Sollwert	Offline-Bit, setattr_with_owner_change, setattr_with_Group_change, setattr_with_Mode_change, setattr_with_sacl_change, Setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_Access_time_change, setattr_with_size_change, exclude_Directory
Symbolischer Link	Offline-Bit

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen für fehlgeschlagene Dateivorgänge erhalten, da sie keine Berechtigungen haben. Die Liste der unterstützten Zugriffsverweigerung Dateioperationen und Filterkombinationen für das FPolicy Monitoring von NFSv4-Dateizugriffsereignissen ist in der folgenden Tabelle aufgeführt:

Unterstützter Zugriff verweigert Dateivorgang	Unterstützte Filter
Datenzugriff	NA
Erstellen	NA
Create_dir	NA
Löschen	NA
Delete_dir	NA
Verlinken	NA
Offen	NA
Lesen	NA
Umbenennen	NA
Umbenennen_dir	NA
Sollwert	NA
Schreiben	NA

Füllen Sie das Arbeitsblatt für die FPolicy Event-Konfiguration aus

Mit diesem Arbeitsblatt können Sie die Werte aufzeichnen, die Sie während der FPolicy-Ereigniskonfiguration benötigen. Wenn ein Parameterwert erforderlich ist, müssen Sie vor der Konfiguration des FPolicy-Ereignisses festlegen, welchen Wert für diese Parameter verwendet werden soll.

Sie sollten aufzeichnen, ob Sie die einzelnen Parametereinstellungen in die FPolicy Event-Konfiguration aufnehmen möchten, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

Informationstyp	Erforderlich	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM	Ja.	Ja.	
Ereignis-Name	Ja.	Ja.	
Protokoll	Nein		
Dateivorgänge	Nein		
Filter	Nein		
Volume-Betrieb	Nein		
Zugriff verweigert Ereignisse + (Unterstützung ab ONTAP 9.13)	Nein		

Planen Sie die FPolicy-Konfiguration

Planen Sie die FPolicy-Konfiguration im Überblick

Bevor Sie die FPolicy konfigurieren, müssen Sie verstehen, welche Parameter beim Erstellen der Richtlinie erforderlich sind sowie warum Sie bestimmte optionale Parameter konfigurieren möchten. Anhand dieser Informationen können Sie festlegen, welche Werte für jeden Parameter festgelegt werden sollen.

Beim Erstellen einer FPolicy verknüpfen Sie die Richtlinie mit der folgenden:

- Die Storage Virtual Machine (SVM)
- Ein oder mehrere FPolicy Events
- Eine externe FPolicy Engine

Sie können auch mehrere optionale Richtlinieneinstellungen konfigurieren.

Was die FPolicy-Konfiguration enthält

Sie können die folgende Liste der erforderlichen FPolicy und optionalen Parameter verwenden, um Ihre Konfiguration zu planen:

Informationstyp	Option	Erforderlich	Standard
SVM Name Gibt den Namen der SVM an, auf der eine FPolicy erstellt werden soll.	`-vserver vserver_name`	Ja.	Keine

Name der Richtlinie Gibt den Namen der FPolicy an. Der Name kann bis zu 256 Zeichen lang sein. Wenn die Richtlinie in einer MetroCluster- oder SVM-Disaster-Recovery-Konfiguration konfiguriert ist, sollte der Name bis zu 200 Zeichen lang sein. Der Name kann eine beliebige Kombination der folgenden Zeichen des ASCII-Bereichs enthalten: • `a` Bis `z` • `A` Bis `Z` • `0` Bis `9` • „_“, „-`", and ".`“	`-policy-name policy_name`	Ja.	Keine
Ereignisnamen Gibt eine kommagetrennte Liste von Ereignissen an, die mit der FPolicy verknüpft werden sollen. • Sie können einer Richtlinie mehrere Ereignisse zuordnen. • Ein Ereignis ist spezifisch für ein Protokoll. • Sie können eine einzelne Richtlinie verwenden, um Dateizugriffsereignisse für mehr als ein Protokoll zu überwachen, indem Sie für jedes Protokoll, das die Richtlinie überwachen soll, ein Ereignis erstellen und dann die Ereignisse mit der Richtlinie verknüpfen. • Die Ereignisse müssen bereits vorhanden sein.	`-events event_name, ...`	Ja.	Keine

Name der externen Engine Gibt den Namen der externen Engine an, die mit der FPolicy verknüpft werden soll. • Eine externe Engine enthält die vom Knoten benötigten Informationen zum Senden von Benachrichtigungen an einen FPolicy-Server. • Sie können FPolicy so konfigurieren, dass die native externe ONTAP Engine zum einfachen Blockieren von Dateien oder zur Verwendung einer externen Engine verwendet wird, die für die Verwendung von externen FPolicy-Servern (FPolicy-Servern) konfiguriert ist, um anspruchsvollere Datei-Blockierung und Dateimanagement zu ermöglichen. • Wenn Sie die native externe Engine verwenden möchten, können Sie entweder keinen Wert für diesen Parameter angeben oder angeben `native` Als Wert. • Wenn Sie FPolicy-Server verwenden möchten, muss die Konfiguration für die externe Engine bereits vorhanden sein.	`-engine engine_name`	Ja (es sei denn, diese Richtlinie nutzt die interne ONTAP-native Engine)	`native`
Ist obligatorisches Screening erforderlich Gibt an, ob eine obligatorische Überprüfung des Dateizugriffs erforderlich ist. • Die obligatorische Screening-Einstellung legt fest, welche Maßnahmen bei einem Dateizugriff getroffen werden sollen, wenn alle primären und sekundären Server ausgefallen sind oder keine Antwort von den FPolicy-Servern innerhalb eines bestimmten Zeitlimits erhalten wird. • Wenn eingestellt auf `true`, Dateizugriffsereignisse werden verweigert. • Wenn eingestellt auf `false`, Dateizugriffsereignisse sind erlaubt.	`-is-mandatory` {`true`	`false`}	Nein

`true`	*Privilegierten Zugriff zulassen* Gibt an, ob der FPolicy-Server über eine privilegierte Datenverbindung privilegierten Zugriff auf die überwachten Dateien und Ordner haben soll. Bei entsprechender Konfiguration können FPolicy Server über die privilegierte Datenverbindung auf Dateien vom Root der SVM zugreifen, die die überwachten Daten enthalten. Für den privilegierten Datenzugriff muss SMB auf dem Cluster lizenziert sein. Alle Daten-LIFs für die Verbindung mit den FPolicy Servern müssen konfiguriert werden `cifs` Als eines der zulässigen Protokolle. Wenn Sie die Richtlinie so konfigurieren möchten, dass ein privilegierter Zugriff möglich ist, müssen Sie auch den Benutzernamen für das Konto angeben, das der FPolicy-Server für privilegierten Zugriff verwenden soll.	`-allow -privileged -access` {`yes`	`no`}

Nein (es sei denn, Passthrough-read ist aktiviert)	`no`	*Privilegierter Benutzername* Gibt den Benutzernamen des Kontos an, das FPolicy-Server für privilegierten Datenzugriff verwenden. • Der Wert für diesen Parameter sollte das Format „`domain\user Name`“ verwenden. • Wenn `-allow -privileged -access` Ist auf festgelegt `no`, Jeder für diesen Parameter eingestellte Wert wird ignoriert.	`-privileged -user-name user_name`

Nein (sofern der privilegierte Zugriff nicht aktiviert ist)	Keine	*Passthrough-read* zulassen Gibt an, ob die FPolicy-Server PassThrough-Read-Services für Dateien bereitstellen können, die von den FPolicy-Servern in sekundären Speicher (Offline-Dateien) archiviert wurden: • Passthrough-read ist eine Möglichkeit, Daten von Offline-Dateien zu lesen, ohne die Daten auf den primären Speicher wiederherzustellen. Durch das Passthrough-Lesevorgang werden die Reaktionszeiten reduziert, da vor der Reaktion auf die Leseanforderung keine Dateien zurück auf den primären Storage zurückgerufen werden müssen. Zusätzlich optimiert das Passthrough-Lesevorgang die Storage-Effizienz, da es nicht mehr erforderlich ist, primären Storage mit Dateien zu belegen, die ausschließlich für Lesezugriffe abgerufen werden.	`-is-passthrough-read-enabled {true`

Anforderung für FPolicy-Konfigurationen, wenn die FPolicy die native Engine verwendet

Wenn Sie die FPolicy so konfigurieren, dass die native Engine verwendet wird, gibt es eine spezifische Anforderung dafür, wie Sie den FPolicy-Umfang definieren, der für die Richtlinie konfiguriert ist.

FPolicy-Umfang definiert die Grenzen, über die die FPolicy gilt, zum Beispiel, ob FPolicy auf bestimmte Volumes oder Freigaben angewendet wird. Es gibt eine Reihe von Parametern, die den Geltungsbereich der FPolicy weiter einschränken. Einer dieser Parameter, `-is-file-extension-check-on-directories-enabled`, Gibt an, ob Dateierweiterungen auf Verzeichnissen überprüft werden sollen. Der Standardwert ist `false`, Das bedeutet, dass Dateierweiterungen auf Verzeichnissen nicht überprüft werden.

Wenn eine FPolicy, die die native Engine nutzt, auf einem Share oder Volume und dem aktiviert wird `-is-file-extension-check-on-directories-enabled` Parameter ist auf festgelegt `false` Für den Umfang der Richtlinie wird der Zugriff auf das Verzeichnis verweigert. Da die Dateierweiterungen nicht auf Verzeichnisse überprüft werden, wird bei dieser Konfiguration ein Verzeichnisvorgang verweigert, wenn er unter den Geltungsbereich der Richtlinie fällt.

Um sicherzustellen, dass der Verzeichniszugriff erfolgreich ist, wenn Sie die native Engine verwenden, müssen Sie den festlegen `-is-file-extension-check-on-directories-enabled parameter` Bis `true` Beim Erstellen des Anwendungsbereichs.

Wenn dieser Parameter auf gesetzt ist `true`, Erweiterungsprüfungen erfolgen für Verzeichnisvorgänge und die Entscheidung, ob der Zugriff erlaubt oder verweigert wird, wird auf Grundlage der in der FPolicy Scope-Konfiguration enthaltenen oder ausgeschlossenen Erweiterungen getroffen.

- Wenn diese Option aktiviert ist, stellen die FPolicyServer die Daten für die Datei über einen separaten Datenkanal bereit, der speziell für Passdurchlesevorgänge geöffnet wurde.
- Wenn Sie Passthrough-read konfigurieren möchten, muss die Richtlinie auch so konfiguriert werden, dass ein privilegierter Zugriff möglich ist.

Füllen Sie das FPolicy-Arbeitsblatt aus

Mit diesem Arbeitsblatt können Sie die Werte erfassen, die Sie während der Konfiguration der Richtlinien für FPolicy benötigen. Sie sollten aufzeichnen, ob Sie die einzelnen Parametereinstellungen in die FPolicy-Konfiguration aufnehmen möchten, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

Informationstyp	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM	Ja.	
Name der Richtlinie	Ja.	
Ereignisnamen	Ja.	
Name der externen Engine		
Ist ein obligatorisches Screening erforderlich?		
Privilegierten Zugriff zulassen		
Privilegierter Benutzername		

Ist Passthrough-read aktiviert?		

Planen der FPolicy Scope-Konfiguration

Planen Sie die FPolicy Scope-Konfiguration im Überblick

Bevor Sie den FPolicy-Bereich konfigurieren, müssen Sie verstehen, was es bedeutet, einen Umfang zu erstellen. Sie müssen wissen, welche Umfang-Konfiguration enthält. Sie müssen auch verstehen, was die Anwendungsregeln von Vorrang sind. Diese Informationen können Ihnen bei der Planung der Werte helfen, die Sie festlegen möchten.

Was es bedeutet, einen FPolicy-Bereich zu erstellen

Beim Erstellen des FPolicy-Umfangs müssen die Grenzen definiert werden, für die die FPolicy gilt. Die Storage Virtual Machine (SVM) ist die grundlegende Grenze. Wenn Sie einen Bereich für eine FPolicy erstellen, müssen Sie die FPolicy definieren, für die sie gilt. Außerdem müssen Sie angeben, auf welche SVM der Umfang angewendet werden soll.

Es gibt verschiedene Parameter, die den Umfang innerhalb der angegebenen SVM weiter einschränken. Sie können den Umfang einschränken, indem Sie angeben, was im Umfang enthalten sein soll, oder indem Sie angeben, was vom Umfang ausgeschlossen werden soll. Nachdem Sie einen Bereich auf eine aktivierte Richtlinie angewendet haben, werden die Ereignisprüfungen für Richtlinien auf den durch diesen Befehl definierten Umfang angewendet.

Benachrichtigungen werden für Dateizugriffsereignisse generiert, bei denen Übereinstimmungen in den Optionen „`include`“ gefunden werden. Benachrichtigungen werden nicht für Dateizugriffsereignisse generiert, bei denen Übereinstimmungen in den Optionen „`exclude`“ gefunden werden.

Die FPolicy Scope-Konfiguration definiert die folgenden Konfigurationsinformationen:

- SVM-Name
- Name der Richtlinie
- Die Freigaben, die von dem, was überwacht wird, einbezogen oder ausgeschlossen werden sollen
- Die Exportrichtlinien, die von den überwachten Daten enthalten oder ausschließen sollen
- Die Volumes, die von den überwachten Volumes ein- oder ausgeschlossen werden sollen
- Die Dateierweiterungen, die das überwachte einschließen oder ausschließen sollen
- Ob Dateiendungsprüfungen für Verzeichnisobjekte durchgeführt werden sollen

> Es gibt besondere Überlegungen für den Umfang einer Cluster FPolicy. Die Cluster-FPolicy ist eine Richtlinie, die der Cluster-Administrator für den Administrator-SVM erstellt. Wenn der Cluster-Administrator auch diesen Umfang für diese Cluster FPolicy erstellt, kann der SVM-Administrator nicht für dieselbe Richtlinie ein Angebot erstellen. Wenn der Cluster-Administrator jedoch keinen Umfang für die Cluster FPolicy erstellt, kann ein SVM-Administrator den Umfang für diese Cluster-Richtlinie erstellen. Wenn der SVM-Administrator diese Cluster-Policy erstellt, kann der Cluster-Administrator nicht anschließend Cluster-Umfang für die gleiche Cluster-Richtlinie erstellen. Dies liegt daran, dass der Cluster-Administrator den Umfang für dieselbe Cluster-Richtlinie nicht außer Kraft setzen kann.

Was sind die Anwendungsregeln von Precedence

Für die Anwendungskonfigurationen gelten die folgenden Vorrangregeln:

- Wenn ein Share in das enthalten ist `-shares-to-include` Parameter und das übergeordnete Volumen des Share sind in enthalten `-volumes-to-exclude` Parameter, `-volumes-to-exclude` Hat Vorrang vor `-shares-to-include`.
- Wenn eine Exportrichtlinie in enthalten ist `-export-policies-to-include` Parameter und das übergeordnete Volume der Exportrichtlinie sind in enthalten `-volumes-to-exclude` Parameter, `-volumes-to-exclude` Hat Vorrang vor `-export-policies-to-include`.
- Ein Administrator kann beides angeben `-file-extensions-to-include` Und `-file-extensions -to-exclude` Listen.

  Der `-file-extensions-to-exclude` Der Parameter wird vor dem geprüft `-file-extensions-to -include` Parameter ist aktiviert.

Die FPolicy Scope-Konfiguration enthält

Sie können die folgende Liste der verfügbaren FPolicy Scope-Konfigurationsparameter verwenden, um Ihre Konfiguration zu planen:

> Bei der Konfiguration, welche Freigaben, Exportrichtlinien, Volumes und Dateierweiterungen ein- oder ausgeschlossen werden sollen, können die ein- und Ausschlussparameter Metacharacter wie „` enthalten?" `and` "*`“. Die Verwendung von regulären Ausdrücken wird nicht unterstützt.

Informationstyp	Option
SVM Gibt den SVM-Namen an, auf dem ein FPolicy Scope erstellt werden soll. Jede FPolicy-Konfiguration ist innerhalb einer einzelnen SVM definiert. Die externe Engine, das Richtlinienereignis, der Richtlinienumfang und die Richtlinie, die gemeinsam eine FPolicy-Konfiguration erstellen, müssen mit derselben SVM verknüpft werden.	`-vserver` `vserver_name`
Name der Richtlinie Gibt den Namen der FPolicy an, der der Umfang angehängt werden soll. Die FPolicy muss bereits bestehen.	`-policy-name` `policy_name`
Zu den Aktien gehören Gibt eine durch Komma getrennte Liste von Freigaben an, die für die Policy FPolicy überwacht werden sollen, auf die der Geltungsbereich angewendet wird.	`-shares-to-include` `share_name`, ...

Freigaben ausschließen Gibt eine durch Komma getrennte Liste von Freigaben an, die von der Überwachung der FPolicy ausgeschlossen werden sollen, auf die der Umfang angewendet wird.	`-shares-to-exclude share_name`, ...
Volumes To include gibt eine durch Komma getrennte Liste von Volumes an, die für die Policy überwacht werden sollen, auf die der Umfang angewendet wird.	`-volumes-to-include volume_name`, ...
Volumes zum Ausschließen Gibt eine kommagetrennte Liste von Volumes an, die von der Überwachung der FPolicy ausgeschlossen werden sollen, auf die der Umfang angewendet wird.	`-volumes-to-exclude volume_name`, ...
Exportrichtlinien, die eingeschlossen werden sollen Gibt eine kommagetrennte Liste von Exportrichtlinien an, die für die FPolicy überwacht werden sollen, auf die der Umfang angewendet wird.	`-export-policies-to -include export_policy_name`, ...
Exportrichtlinien zum Ausschließen Gibt eine kommagetrennte Liste von Exportrichtlinien an, die von der Überwachung der FPolicy ausgeschlossen werden soll, auf die der Umfang angewendet wird.	`-export-policies-to -exclude export_policy_name`, ...
Zu include. Dateierweiterungen Gibt eine durch Komma getrennte Liste von Dateierweiterungen an, die für die FPolicy überwacht werden sollen, auf die der Umfang angewendet wird.	`-file-extensions-to -include file_extensions`, ...
Dateierweiterung zum Ausschließen Gibt eine durch Komma getrennte Liste von Dateierweiterungen an, die von der Überwachung der FPolicy, auf die der Umfang angewendet wird, ausgeschlossen werden sollen.	`-file-extensions-to -exclude file_extensions`, ...
Ist die Dateierweiterung für das Verzeichnis aktiviert ? Gibt an, ob die Dateinamensprüfungen auch auf Verzeichnisobjekte angewendet werden. Wenn dieser Parameter auf festgelegt ist `true`, Die Verzeichnisobjekte werden den gleichen Erweiterungsprüfungen unterzogen wie normale Dateien. Wenn dieser Parameter auf festgelegt ist `false`, Die Verzeichnisnamen sind nicht für Erweiterungen abgestimmt und Benachrichtigungen werden für Verzeichnisse gesendet, auch wenn ihre Namenserweiterungen nicht übereinstimmen. Wenn die FPolicy, der der Bereich zugewiesen ist, für die Verwendung der nativen Engine konfiguriert ist, muss dieser Parameter auf festgelegt werden `true`.	`-is-file-extension -check-on-directories -enabled` {`true`. `false`}

Füllen Sie das FPolicy Scope-Arbeitsblatt aus

Mit diesem Arbeitsblatt können Sie die Werte aufzeichnen, die Sie während der Konfiguration des FPolicy Scope benötigen. Wenn ein Parameterwert erforderlich ist, müssen Sie vor der Konfiguration des FPolicy-Umfangs festlegen, welchen Wert für diese Parameter verwendet werden soll.

Sie sollten aufzeichnen, ob die einzelnen Parameter in die FPolicy Scope-Konfiguration einbezogen werden sollen, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

Informationstyp	Erforderlich	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM	Ja.	Ja.	
Name der Richtlinie	Ja.	Ja.	
Einzuschließen von Freigaben	Nein		
Auszuschließende Freigaben	Nein		
Volumes die einbezogen werden sollen	Nein		
Auszuschließende Volumes	Nein		
Richtlinien exportieren, die einbezogen werden sollen	Nein		
Auszuschließende Richtlinien exportieren	Nein		
Einzuschließen von Dateierweiterungen	Nein		
Auszuschließende Dateierweiterung	Nein		
Ist die Dateierweiterung für das Verzeichnis aktiviert?	Nein		

Erstellen Sie die FPolicy-Konfiguration

Erstellen Sie die externe FPolicy Engine

Sie müssen eine externe Engine erstellen, um mit der Erstellung einer FPolicy-Konfiguration zu beginnen. Die externe Engine definiert, wie FPolicy Verbindungen zu externen FPolicy-Servern macht und managt. Wenn Ihre Konfiguration die interne ONTAP Engine (die native externe Engine) für einfaches Blockieren von Dateien verwendet, müssen Sie keine separate FPolicy externe Engine konfigurieren und müssen diesen Schritt nicht ausführen.

Was Sie benötigen

Der "Externer Motor" Arbeitsblatt sollte ausgefüllt werden.

Über diese Aufgabe

Wenn die externe Engine in einer MetroCluster-Konfiguration verwendet wird, sollten Sie die IP-Adressen der FPolicy-Server am Quellstandort als primäre Server angeben. Die IP-Adressen der FPolicy-Server am Zielstandort sollten als sekundäre Server angegeben werden.

Schritte

1. Erstellen Sie die FPolicy-externe Engine mit dem `vserver fpolicy policy external-engine create` Befehl.

   Mit dem folgenden Befehl wird eine externe Engine auf der Storage Virtual Machine (SVM) vs1.example.com erstellt. Für die externe Kommunikation mit dem FPolicy-Server ist keine Authentifizierung erforderlich.

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. Überprüfen Sie die Konfiguration der externen FPolicy-Engine mit dem `vserver fpolicy policy external-engine show` Befehl.

   Mit dem folgenden Befehl werden Informationen zu allen auf SVM vs1.example.com konfigurierten externen Engines angezeigt:

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                   Primary        Secondary
   External
   Vserver            Engine       Servers        Servers       Port Engine
   Type
   ---------------    -----------  -------------- ----------- ------
   -----------
   vs1.example.com    engine1      10.1.1.2,      -             6789
   synchronous
                                   10.1.1.3
   ```

   Mit dem folgenden Befehl werden ausführliche Informationen zur externen Engine mit dem Namen „`Engine1`“ auf SVM vs1.example.com angezeigt:

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
   -name engine1
   ```

```
                                Vserver: vs1.example.com
                                 Engine: engine1
               Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
        Port Number of FPolicy Service: 6789
             Secondary FPolicy Servers: -
                  External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
                Certificate Authority: -
```

Erstellen Sie das FPolicy-Ereignis

Wenn Sie eine FPolicy-Konfiguration erstellen, müssen Sie ein FPolicy-Ereignis erstellen. Sie verknüpfen das Ereignis mit der FPolicy, wenn es erstellt wird. Ein Ereignis definiert, welches Protokoll überwacht werden soll und welche Dateizugriffsereignisse überwacht und gefiltert werden müssen.

Bevor Sie beginnen

Sie sollten das FPolicy Event abschließen "Arbeitsblatt".

Erstellen Sie das FPolicy-Ereignis

1. Erstellen Sie das FPolicy-Ereignis mit `vserver fpolicy policy event create` Befehl.

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. Überprüfen Sie die FPolicy-Event-Konfiguration mit `vserver fpolicy policy event show` Befehl.

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                     Event                 File                      Is Volume
   Vserver           Name      Protocols Operations    Filters   Operation
   ---------------   --------- --------- ------------- ---------
   ------------
   vs1.example.com   event1    cifs      open, close,  -         false
                                         read, write
   ```

Erstellen Sie die Ereignisse, bei denen der FPolicy Zugriff verweigert wird

Ab ONTAP 9.13.1 können Benutzer Benachrichtigungen für fehlgeschlagene Dateivorgänge erhalten, da sie keine Berechtigungen haben. Diese Benachrichtigungen sind wertvoll für Sicherheit, Ransomware-Schutz und Governance.

1. Erstellen Sie das FPolicy-Ereignis mit `vserver fpolicy policy event create` Befehl.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

Erstellen persistenter Speicher

Ab ONTAP 9.14.1 können Sie mit FPolicy eine einrichten "Persistente Speicher" So erfassen Sie Dateizugriffsereignisse für asynchrone, nicht obligatorische Richtlinien in der SVM: Persistente Speicher können die Client-I/O-Verarbeitung von der FPolicy-Benachrichtigungsverarbeitung entkoppeln, um die Client-Latenz zu verringern. Synchrone (obligatorische oder nicht obligatorische) und asynchrone obligatorische Konfigurationen werden nicht unterstützt.

Best Practices in sich vereint

- Bevor Sie die Funktion „persistenter Speicher“ verwenden, stellen Sie sicher, dass Ihre Partneranwendungen diese Konfiguration unterstützen.
- Das persistente Speicher-Volume wird auf SVM-Basis eingerichtet. Für jede FPolicy aktivierte SVM wird ein persistentes Speicher-Volume benötigt.
- Der Name des persistenten Speichervolumes und der bei der Volume-Erstellung angegebene Verbindungspfad müssen übereinstimmen.
- Erstellen Sie das persistente Speicher-Volume auf dem Node mit LIFs, die davon ausgehen, dass der maximale Datenverkehr durch FPolicy überwacht wird.
- Lassen Sie die Snapshot-Richtlinie auf festlegen `none` Für dieses Volume anstelle von `default`. Dadurch wird sichergestellt, dass keine versehentliche Wiederherstellung des Snapshots zum Verlust aktueller Ereignisse führt und eine mögliche doppelte Ereignisverarbeitung verhindert wird.
- Machen Sie das persistente Speicher-Volume für den externen Zugriff auf das Benutzerprotokoll (CIFS/NFS) unzugänglich, um versehentliche Beschädigungen oder das Löschen von permanenten Ereignisdatensätzen zu vermeiden. Um dies zu erreichen, heben Sie nach Aktivierung von FPolicy die Bereitstellung des Volumes in ONTAP auf, um den Verbindungspfad zu entfernen. Dies macht ihn für den Benutzerprotokollzugriff unzugänglich.

Schritte

1. Erstellen Sie ein leeres Volume auf der SVM, das für den persistenten Speicher bereitgestellt werden kann:

   ```
   volume create -vserver <SVM Name> -volume <volume> -state <online> -junction
   -path <path> -policy <default> -unix-permissions <777> -size <value>
   -aggregate <aggregate name> -snapshot-policy <none>
   ```

   - Die Größe des persistenten Speichervolumes basiert auf der Dauer, für die Sie die Ereignisse, die nicht an den externen Server (Partneranwendung) gesendet werden, fortführen möchten.

     Wenn Sie beispielsweise möchten, dass in einem Cluster 30 Minuten Ereignisse mit einer Kapazität von 30.000 Benachrichtigungen pro Sekunde erhalten bleiben:

     Erforderliche Volume-Größe = 30000 x 30 x 60 x 0,6 KB (Größe des Avg-Benachrichtigungsdatensatzes) = 32400000 KB = ~32 GB

   Um die ungefähre Benachrichtigungsrate zu ermitteln, können Sie sich entweder mit Ihrer FPolicy Partnerapplikation in Verbindung setzen oder den FPolicy-Zähler verwenden `requests_dispatched_rate`.

- Es wird erwartet, dass ein Administratorbenutzer mit ausreichenden RBAC-Berechtigungen (um ein Volume zu erstellen) ein Volume (mit dem cli-Befehl des Volumes oder der REST-API) der gewünschten Größe erstellt und den Namen dieses Volumes als bereitstellt `-volume` Erstellen Sie im persistenten Speicher einen CLI-Befehl oder eine REST-API.

2. Persistenten Speicher erstellen:

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store
<PS_name> -volume <volume>
```

   - Persistenter Speicher: Der Name des persistenten Speichers
   - Volume: Das persistente Speicher-Volume

3. Nachdem der persistente Speicher erstellt wurde, können Sie die FPolicy-Richtlinie erstellen und dieser Richtlinie den Namen des persistenten Speichers hinzufügen.
   Weitere Informationen finden Sie unter "Erstellen Sie die FPolicy".

Erstellen Sie die FPolicy

Wenn Sie die FPolicy erstellen, verknüpfen Sie eine externe Engine und ein oder mehrere Ereignisse mit der Richtlinie. Die Richtlinie legt außerdem fest, ob ein obligatorisches Screening erforderlich ist, ob die FPolicy Server privilegierten Zugriff auf Daten auf der Storage Virtual Machine (SVM) haben und ob Passthrough-Read für Offline-Dateien aktiviert ist.

Was Sie benötigen

- Das Arbeitsblatt für die FPolicy sollte ausgefüllt werden.
- Wenn Sie planen, die Richtlinie für FPolicy-Server zu konfigurieren, muss die externe Engine vorhanden sein.
- Mindestens ein FPolicy-Ereignis, das Sie auf eine Verknüpfung mit der FPolicy planen, muss existieren.
- Wenn Sie einen privilegierten Datenzugriff konfigurieren möchten, muss auf der SVM ein SMB-Server vorhanden sein.
- Um einen persistenten Speicher für eine Policy zu konfigurieren, muss der Engine-Typ **async** sein und die Policy muss **non-obligatorische** sein.

  Weitere Informationen finden Sie unter "Erstellen persistenter Speicher".

Schritte

1. Erstellen der FPolicy:

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name
policy_name -engine engine_name -events event_name, [-persistent-store
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
privileged-user-name domain\user_name] [-is-passthrough-read-enabled
{true|false}]
```

   - Sie können ein oder mehrere Events zur FPolicy hinzufügen.
   - Standardmäßig ist das obligatorische Screening aktiviert.
   - Wenn Sie privilegierten Zugriff zulassen möchten, setzen Sie die ein `-allow-privileged-access` Parameter an `yes`, Sie müssen auch einen privilegierten Benutzernamen für privilegierten Zugriff

konfigurieren.

- Wenn Sie Passthrough-read konfigurieren möchten, indem Sie die einstellen `-is-passthrough -read-enabled` Parameter an `true`, Sie müssen auch privilegierten Datenzugriff konfigurieren.

  Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen „`policy1`“ erstellt, in der das Ereignis „`event1`“ und die externe Engine „`Engine1`“ mit ihr verknüpft sind. Diese Richtlinie verwendet Standardwerte in der Richtlinienkonfiguration:
  `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

  Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen „`policy2`“ erstellt, in der das Ereignis „`event2`“ und die externe Engine „`Engine2`“ mit ihr verknüpft sind. Diese Richtlinie wurde für die Verwendung von privilegiertem Zugriff unter Verwendung des angegebenen Benutzernamens konfiguriert. Passthrough-read ist aktiviert:

  ```
  vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
  -events event2 -engine engine2 -allow-privileged-access yes -privileged-
  user-name example\archive_acct -is-passthrough-read-enabled true
  ```

  Mit dem folgenden Befehl wird eine Richtlinie mit dem Namen „`nativ1`“ erstellt, die das Ereignis „`event3`“ mit ihr verknüpft hat. Diese Richtlinie verwendet die native Engine und verwendet Standardwerte in der Richtlinienkonfiguration:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. Überprüfen Sie die FPolicy-Konfiguration mit `vserver fpolicy policy show` Befehl.

   Mit dem folgenden Befehl werden Informationen zu den drei konfigurierten FPolicy-Richtlinien angezeigt, einschließlich der folgenden Informationen:

   - Der Richtlinie zugeordnete SVM
   - Die externe Engine, die der Richtlinie zugeordnet ist
   - Die mit der Richtlinie verbundenen Ereignisse
   - Gibt an, ob eine obligatorische Überprüfung erforderlich ist
   - Gibt an, ob ein privilegierter Zugriff erforderlich ist
     `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                         Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

Erstellen Sie den FPolicy-Bereich

Nachdem Sie die FPolicy erstellt haben, müssen Sie einen FPolicy-Bereich erstellen. Bei der Erstellung des Anwendungsbereichs verknüpfen Sie den Geltungsbereich mit einer FPolicy. Ein Geltungsbereich definiert die Grenzen, für die die FPolicy gilt. Scopes können Dateien einschließen oder ausschließen, die auf Freigaben, Exportrichtlinien, Volumes und Dateierweiterungen basieren.

Was Sie benötigen

Das FPolicy Scope-Arbeitsblatt muss ausgefüllt werden. Die FPolicy muss mit einer zugeordneten externen Engine existieren (wenn die Richtlinie zur Verwendung externer FPolicy-Server konfiguriert ist) und über mindestens ein damit verbundener FPolicy-Ereignis verfügen.

Schritte

1. Erstellen Sie den FPolicy-Bereich mit `vserver fpolicy policy scope create` Befehl.

   ```
   vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
   policy1 -volumes-to-include datavol1,datavol2
   ```

2. Überprüfen Sie die FPolicy-Scope-Konfiguration mit `vserver fpolicy policy scope show` Befehl.

   ```
   vserver fpolicy policy scope show -vserver vs1.example.com -instance
   ```

   ```
                       Vserver: vs1.example.com
                        Policy: policy1
             Shares to Include: -
             Shares to Exclude: -
            Volumes to Include: datavol1, datavol2
            Volumes to Exclude: -
     Export Policies to Include: -
     Export Policies to Exclude: -
     File Extensions to Include: -
     File Extensions to Exclude: -
   ```

Aktivieren Sie die FPolicy

Nachdem Sie eine FPolicy-Konfiguration durchlaufen haben, aktivieren Sie die FPolicy. Durch das Aktivieren der Richtlinie wird die Priorität festgelegt und die Dateizugriffsüberwachung für die Richtlinie gestartet.

Was Sie benötigen

Die FPolicy muss mit einer zugeordneten externen Engine existieren (wenn die Richtlinie zur Verwendung externer FPolicy-Server konfiguriert ist) und über mindestens ein damit verbundener FPolicy-Ereignis verfügen. Der Richtlinienumfang von FPolicy muss vorhanden sein und der FPolicy zugewiesen werden.

Über diese Aufgabe

Die Priorität wird verwendet, wenn mehrere Richtlinien auf der Storage Virtual Machine (SVM) aktiviert sind und mehr als eine Richtlinie dasselbe Ereignis für den Dateizugriff abonniert hat. Richtlinien, die die native

Engine-Konfiguration verwenden, haben für jede andere Engine eine höhere Priorität als Richtlinien, unabhängig von der ihnen bei der Aktivierung der Richtlinie zugewiesenen Sequenznummer.

> Eine Richtlinie kann auf der Admin-SVM nicht aktiviert werden.

Schritte

1. Aktivieren Sie die FPolicy mithilfe von `vserver fpolicy enable` Befehl.

   ```
   vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
   -sequence-number 1
   ```

2. Überprüfen Sie, ob die FPolicy mit aktiviert wird `vserver fpolicy show` Befehl.

   ```
   vserver fpolicy show -vserver vs1.example.com
   ```

   ```
                                       Sequence
   Vserver          Policy Name         Number  Status   Engine
   ---------------  ----------------- --------  -------- ---------
   vs1.example.com  policy1                   1  on       engine1
   ```

Managen von FPolicy-Konfigurationen

Ändern Sie FPolicy-Konfigurationen

Befehle zum Ändern von FPolicy-Konfigurationen

Sie können FPolicy-Konfigurationen ändern, indem Sie die Elemente ändern, aus denen die Konfiguration besteht. Sie können externe Engines, FPolicy Ereignisse, FPolicy Scopes und FPolicy-Richtlinien ändern. Sie können FPolicy auch aktivieren oder deaktivieren. Wenn Sie die FPolicy deaktivieren, wird die Dateiüberwachung für diese Richtlinie eingestellt.

Es wird empfohlen, die FPolicy zu deaktivieren, bevor Sie die Konfiguration ändern.

Sie möchten Folgendes ändern:	Befehl
Externe Motoren	`vserver fpolicy policy external-engine modify`
Veranstaltungen	`vserver fpolicy policy event modify`
Bereich	`vserver fpolicy policy scope modify`
Richtlinien	`vserver fpolicy policy modify`

Weitere Informationen zu den Befehlen finden Sie auf den man-Pages.

Aktivieren oder Deaktivieren von FPolicy-Richtlinien

Sie können FPolicy-Richtlinien aktivieren, nachdem die Konfiguration abgeschlossen ist. Durch das Aktivieren der Richtlinie wird die Priorität festgelegt und die Dateizugriffsüberwachung für die Richtlinie gestartet. Sie können FPolicy-Richtlinien deaktivieren, wenn Sie die Dateizugriffsüberwachung für die Richtlinie beenden möchten.

Was Sie benötigen

Vor Aktivierung von FPolicy Richtlinien muss die FPolicy Konfiguration abgeschlossen sein.

Über diese Aufgabe

- Die Priorität wird verwendet, wenn mehrere Richtlinien auf der Storage Virtual Machine (SVM) aktiviert sind und mehr als eine Richtlinie dasselbe Ereignis für den Dateizugriff abonniert hat.
- Richtlinien, die die native Engine-Konfiguration verwenden, haben für jede andere Engine eine höhere Priorität als Richtlinien, unabhängig von der ihnen bei der Aktivierung der Richtlinie zugewiesenen Sequenznummer.
- Wenn Sie die Priorität einer FPolicy ändern möchten, müssen Sie die Richtlinie deaktivieren und dann mithilfe der neuen Sequenznummer erneut aktivieren.

Schritt

1. Führen Sie die entsprechende Aktion aus:

Ihr Ziel ist	Geben Sie den folgenden Befehl ein…
Aktivieren einer FPolicy	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
Deaktivieren Sie eine FPolicy	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

Zeigen Sie Informationen zu FPolicy-Konfigurationen an

Funktionsweise der Befehle show

Es ist hilfreich beim Anzeigen von Informationen über die FPolicy Konfiguration, um zu verstehen, wie das `show` Befehle funktionieren.

A `show` Durch Befehl ohne zusätzliche Parameter werden Informationen in einem Übersichtsformular angezeigt. Zusätzlich alle `show` Der Befehl weist die beiden gleichen optionalen Parameter auf, die sich gegenseitig ausschließen. `-instance` Und `-fields`.

Wenn Sie das verwenden `-instance` Parameter mit A `show` Mit dem Befehl werden in der Ausgabe des Befehls detaillierte Informationen in einem Listenformat angezeigt. In einigen Fällen kann die detaillierte Ausgabe langwierig sein und mehr Informationen enthalten, als Sie benötigen. Sie können das verwenden `-fields fieldname[,fieldname…]` Parameter, um die Ausgabe so anzupassen, dass nur Informationen für die von Ihnen angegebenen Felder angezeigt werden. Sie können bestimmen, welche Felder Sie angeben können, indem Sie sie eingeben `?` Nach dem `-fields` Parameter.

> Die Ausgabe von A `show` Befehl mit dem `-fields` Der Parameter zeigt möglicherweise weitere relevante und notwendige Felder in Bezug auf die angeforderten Felder an.

Alle `show` Befehl enthält mindestens einen optionalen Parameter, der die Ausgabe filtert und Sie können den Umfang der in der Befehlsausgabe angezeigten Informationen eingrenzen. Sie können festlegen, welche optionalen Parameter für einen Befehl zur Verfügung stehen, indem Sie eingeben `?` Nach dem `show` Befehl.

Der `show` Der Befehl unterstützt UNIX-Style-Muster und Wildcards, damit Sie in Argumenten mit Befehlsparametern mehrere Werte erfüllen können. Sie können beispielsweise den Platzhalter-Operator (*), DEN OPERATOR NOT (!), DEN OPERATOR ODER (\<), den Bereichsoperator (integer…integer), den kleiner-als-Operator (<), den größer-als-Operator (>), den Operator kleiner oder gleich (=) und den Operator größer oder gleich (>=) verwenden, wenn Sie Werte angeben.

Weitere Informationen zur Verwendung von UNIX-Stilmustern und Wildcards finden Sie im Über die ONTAP Befehlszeilenschnittstelle.

Befehle zum Anzeigen von Informationen zu FPolicy-Konfigurationen

Sie verwenden das `fpolicy show` Befehle zum Anzeigen von Informationen zur FPolicy Konfiguration, einschließlich Informationen zu externen FPolicy Engines, Ereignissen, Scopes und Richtlinien.

Wenn Sie Informationen über FPolicy anzeigen möchten…	Befehl
Externe Motoren	`vserver fpolicy policy external-engine show`
Veranstaltungen	`vserver fpolicy policy event show`
Bereich	`vserver fpolicy policy scope show`
Richtlinien	`vserver fpolicy policy show`

Weitere Informationen zu den Befehlen finden Sie auf den man-Pages.

Zeigt Informationen zum FPolicy-Status an

Sie können Informationen zum Status von FPolicy anzeigen, um zu bestimmen, ob eine Richtlinie aktiviert ist, welche externe Engine sie konfiguriert hat, welche Sequenznummer sie für die Richtlinie ist und welcher Storage Virtual Machine (SVM) die FPolicy zugeordnet ist.

Über diese Aufgabe

Wenn Sie keine Parameter angeben, werden mit dem Befehl die folgenden Informationen angezeigt:

- SVM-Name
- Name der Richtlinie
- Police-Sequenznummer

- Der Richtlinienstatus

Zusätzlich zum Anzeigen von Informationen zum Richtlinienstatus für auf dem Cluster oder einer bestimmten SVM konfigurierte Richtlinien können Sie mit Befehlsparametern die Ausgabe des Befehls anhand anderer Kriterien filtern.

Sie können den angeben `-instance` Parameter zum Anzeigen detaillierter Informationen zu aufgeführten Richtlinien Alternativ können Sie den verwenden `-fields` Parameter, mit dem nur die angegebenen Felder in der Befehlsausgabe oder angezeigt werden sollen `-fields ?` Um zu bestimmen, welche Felder Sie verwenden können.

Schritt

1. Zeigt gefilterte Informationen zum Richtlinienstatus mithilfe des entsprechenden Befehls an:

Wenn Sie Statusinformationen zu Richtlinien anzeigen möchten…	Geben Sie den Befehl ein…
Auf dem Cluster	`vserver fpolicy show`
Die den angegebenen Status aufweisen	`vserver fpolicy show -status {on
off}`	Auf einer angegebenen SVM
`vserver fpolicy show -vserver vserver_name`	Mit dem angegebenen Richtliniennamen
`vserver fpolicy show -policy-name policy_name`	Die die angegebene externe Engine verwenden

Beispiel

Im folgenden Beispiel werden die Informationen über FPolicy-Richtlinien auf dem Cluster angezeigt:

```
cluster1::> vserver fpolicy show
                                          Sequence
Vserver             Policy Name             Number  Status      Engine
------------------- ------------------- --------  ---------   ---------
FPolicy             cserver_policy      -         off         eng1
vs1.example.com     v1p1                -         off         eng2
vs1.example.com     v1p2                -         off         native
vs1.example.com     v1p3                -         off         native
vs1.example.com     cserver_policy      -         off         eng1
vs2.example.com     v1p1                3         on          native
vs2.example.com     v1p2                1         on          eng3
vs2.example.com     cserver_policy      2         on          eng1
```

Zeigen Sie Informationen zu aktivierten FPolicy-Richtlinien an

Sie können Informationen über aktivierte FPolicy Richtlinien anzeigen, um zu bestimmen, welche FPolicy externe Engine sie zu verwenden konfiguriert ist, welche Priorität für die Richtlinie hat und zu welcher Storage Virtual Machine (SVM) die FPolicy zugeordnet ist.

Über diese Aufgabe

Wenn Sie keine Parameter angeben, werden mit dem Befehl die folgenden Informationen angezeigt:

- SVM-Name
- Name der Richtlinie
- Richtlinienpriorität

Sie können mit den Befehlsparametern die Ausgabe des Befehls nach bestimmten Kriterien filtern.

Schritt

1. Informationen über aktivierte FPolicy-Richtlinien werden mit dem entsprechenden Befehl angezeigt:

Wenn Informationen über aktivierte Richtlinien angezeigt werden sollen…	Geben Sie den Befehl ein…
Auf dem Cluster	`vserver fpolicy show-enabled`
Auf einer angegebenen SVM	`vserver fpolicy show-enabled -vserver vserver_name`
Mit dem angegebenen Richtliniennamen	`vserver fpolicy show-enabled -policy-name policy_name`
Mit der angegebenen Sequenznummer	`vserver fpolicy show-enabled -priority integer`

Beispiel

Im folgenden Beispiel werden die Informationen über aktivierte FPolicy-Richtlinien auf dem Cluster angezeigt:

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

Verwalten von FPolicy-Serververbindungen

Verbindung zu externen FPolicy-Servern herstellen

Um die Dateiverarbeitung zu aktivieren, müssen Sie möglicherweise manuell eine Verbindung zu einem externen FPolicy-Server herstellen, wenn die Verbindung zuvor beendet wurde. Eine Verbindung wird beendet, nachdem das Server-Timeout erreicht wurde oder aufgrund eines Fehlers. Alternativ kann der Administrator eine Verbindung manuell beenden.

Über diese Aufgabe

Wenn ein schwerwiegender Fehler auftritt, kann die Verbindung zum FPolicy-Server beendet werden. Nachdem Sie das Problem behoben haben, das den schwerwiegenden Fehler verursacht hat, müssen Sie eine manuelle Verbindung zum FPolicy-Server herstellen.

Schritte

1. Stellen Sie eine Verbindung mit dem externen FPolicy-Server her `vserver fpolicy engine-connect` Befehl.

   Weitere Informationen zum Befehl finden Sie in den man-Pages.

2. Überprüfen Sie, ob der externe FPolicy-Server mit dem verbunden ist `vserver fpolicy show-engine` Befehl.

   Weitere Informationen zum Befehl finden Sie in den man-Pages.

Verbindung zu externen FPolicy-Servern trennen

Möglicherweise müssen Sie die Verbindung zu einem externen FPolicy Server manuell trennen. Dies kann wünschenswert sein, wenn der FPolicy Server Probleme mit der Bearbeitung von Benachrichtigungsanfragen hat oder wenn Sie Wartungsarbeiten auf dem FPolicy-Server durchführen müssen.

Schritte

1. Trennen Sie die Verbindung mit dem vom externen FPolicy-Server `vserver fpolicy engine-disconnect` Befehl.

   Weitere Informationen zum Befehl finden Sie in den man-Pages.

2. Überprüfen Sie, ob der externe FPolicy-Server mit dem getrennt wird `vserver fpolicy show-engine` Befehl.

   Weitere Informationen zum Befehl finden Sie in den man-Pages.

Zeigen Sie Informationen über Verbindungen zu externen FPolicy-Servern an

Sie können Statusinformationen über Verbindungen zu externen FPolicy Servern (FPolicy-Servern) für das Cluster oder für eine angegebene Storage Virtual Machine (SVM) anzeigen. Diese Informationen können Ihnen dabei helfen, festzustellen, welche FPolicy Server verbunden sind.

Über diese Aufgabe

Wenn Sie keine Parameter angeben, werden mit dem Befehl die folgenden Informationen angezeigt:

- SVM-Name
- Node-Name
- FPolicy-Name
- FPolicy-Server-IP-Adresse
- FPolicy-Serverstatus
- FPolicy-Servertyp

Zusätzlich zum Anzeigen von Informationen über FPolicy-Verbindungen auf dem Cluster oder einer bestimmten SVM können Sie mit Befehlsparametern die Ausgabe des Befehls um andere Kriterien filtern.

Sie können den angeben `-instance` Parameter zum Anzeigen detaillierter Informationen zu aufgeführten Richtlinien Alternativ können Sie den verwenden `-fields` Parameter, um nur die angegebenen Felder in der Befehlsausgabe anzuzeigen. Sie können eingeben `?` Nach dem `-fields` Parameter, um herauszufinden, welche Felder Sie verwenden können.

Schritt

1. Zeigen Sie gefilterte Informationen zum Verbindungsstatus zwischen dem Knoten und dem FPolicy-Server mithilfe des entsprechenden Befehls an:

Wenn Sie Verbindungsinformationen über FPolicy-Server anzeigen möchten…	Eingeben…
Die Sie angeben	`vserver fpolicy show-engine -server IP_address`
Für eine angegebene SVM	`vserver fpolicy show-engine -vserver vserver_name`
Die mit einer angegebenen Richtlinie verbunden sind	`vserver fpolicy show-engine -policy-name policy_name`
Mit dem von Ihnen angegebenen Serverstatus	`vserver fpolicy show-engine -server-status status` Für den Serverstatus kann einer der folgenden Werte angezeigt werden: • `connected` • `disconnected` • `connecting` • `disconnecting`

Mit dem angegebenen Typ	`vserver fpolicy show-engine -server-type type` Der FPolicy-Server-Typ kann einer der folgenden sein: • `primary` • `secondary`
Die Verbindung wurde mit dem angegebenen Grund getrennt	`vserver fpolicy show-engine -disconnect-reason text` Die Verbindung kann aus mehreren Gründen erfolgen. Die folgenden Gründe sind häufig für die Verbindung: • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

Beispiel

Dieses Beispiel zeigt Informationen zu externen Engine-Verbindungen mit FPolicy-Servern auf SVM vs1.example.com an:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                                Server-       Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

In diesem Beispiel werden nur Informationen zu verbundenen FPolicy-Servern angezeigt:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

Zeigen Sie Informationen zum Verbindungsstatus der FPolicy-Durchleseverbindung an

Sie können Informationen über den FPolicy Passthrough-Read-Verbindungsstatus zu externen FPolicy Servern (FPolicy-Server) für das Cluster oder für eine angegebene Storage Virtual Machine (SVM) anzeigen. Diese Informationen können Ihnen dabei helfen zu bestimmen, welche FPolicy-Server über Pass-Read-Datenverbindungen verfügen und für welche FPolicy-Server die Passthrough-Read-Verbindung getrennt haben.

Über diese Aufgabe

Wenn Sie keinen Parameter angeben, werden mit dem Befehl die folgenden Informationen angezeigt:

- SVM-Name
- FPolicy-Name
- Node-Name
- FPolicy-Server-IP-Adresse
- FPolicy-Verbindungsstatus beim Passthrough-Lesen

Zusätzlich zum Anzeigen von Informationen über FPolicy-Verbindungen auf dem Cluster oder einer bestimmten SVM können Sie mit Befehlsparametern die Ausgabe des Befehls um andere Kriterien filtern.

Sie können den angeben `-instance` Parameter zum Anzeigen detaillierter Informationen zu aufgeführten Richtlinien Alternativ können Sie den verwenden `-fields` Parameter, um nur die angegebenen Felder in der Befehlsausgabe anzuzeigen. Sie können eingeben `?` Nach dem `-fields` Parameter, um herauszufinden, welche Felder Sie verwenden können.

Schritt

1. Zeigen Sie gefilterte Informationen zum Verbindungsstatus zwischen dem Knoten und dem FPolicy-Server mithilfe des entsprechenden Befehls an:

Wenn Sie Informationen zum Verbindungsstatus anzeigen möchten über…	Geben Sie den Befehl ein…
FPolicy-Verbindungsstatus für Passthrough-Lesevorgang für das Cluster	`vserver fpolicy show-passthrough-read-connection`
FPolicy-Verbindungsstatus für Passthrough-Leseverbindungen für eine angegebene SVM	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`

FPolicy-Verbindungsstatus für eine bestimmte Richtlinie zum Passthrough-Lesen	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
Detaillierter Verbindungsstatus von FPolicy über Durchleseverbindungen für eine bestimmte Richtlinie	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`
FPolicy Passthrough-read Verbindungsstatus für den von Ihnen angegebenen Status	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` Für den Serverstatus kann einer der folgenden Werte angezeigt werden: • `connected` • `disconnected`

Beispiel

Mit dem folgenden Befehl werden Informationen zu Passthrough-Read-Verbindungen von allen FPolicy-Servern im Cluster angezeigt:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                            FPolicy           Server
Vserver          Policy Name   Node         Server            Status
---------------  ------------- ------------ -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01   2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01   1.1.1.1           connected
```

Mit dem folgenden Befehl werden ausführliche Informationen zu PassThrough-Read-Verbindungen von FPolicy-Servern angezeigt, die in der Richtlinie „`pol_cifs_1`“ konfiguriert sind:

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                          Node: FPolicy-01
                                       Vserver: vs1.example.com
                                        Policy: pol_cifs_1
                                        Server: 1.1.1.1
                Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                   Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

Überprüfen Sie den Zugriff mithilfe der Sicherheitskontrolle

Funktionsweise von Sicherheitspuren

Sie können Filter zur Berechtigungs-Verfolgung hinzufügen, um ONTAP anzuweisen, Informationen darüber zu protokollieren, warum SMB- und NFS-Server auf einer Storage Virtual Machine (SVM) einem Client oder Anwender die Anforderung zur Durchführung eines Vorgangs erlaubt oder ablehnt. Dies kann nützlich sein, wenn Sie überprüfen möchten, ob das Sicherheitsschema für den Dateizugriff geeignet ist oder wenn Sie Probleme mit dem Dateizugriff beheben möchten.

Mithilfe von Sicherheitspuren können Sie einen Filter konfigurieren, der Client-Vorgänge über SMB und NFS auf der SVM erkennt und alle Zugriffsprüfungen, die diesem Filter entsprechen, nachverfolgen. Sie können dann die Trace-Ergebnisse anzeigen, die eine praktische Zusammenfassung der Gründe liefert, warum der Zugriff erlaubt oder verweigert wurde.

Wenn Sie die Sicherheitseinstellungen für den SMB- oder NFS-Zugriff auf Dateien und Ordner auf Ihrer SVM überprüfen möchten oder wenn ein Zugriffsproblem vorliegt, können Sie schnell einen Filter hinzufügen, um die Berechtigungs-Verfolgung zu aktivieren.

In der folgenden Liste werden wichtige Fakten zur Funktionsweise von Sicherheitspuren aufgeführt:

- ONTAP wendet Sicherheitsspuren auf SVM-Ebene an.
- Jede eingehende Anforderung wird überprüft, ob sie Filterkriterien für aktivierte Sicherheitspuren erfüllt.
- Traces werden sowohl für Datei- als auch für Ordnerzugriffsanfragen ausgeführt.
- Traces können nach folgenden Kriterien filtern:
  - Client-IP
  - SMB- oder NFS-Pfad
  - Windows Name
  - UNIX-Name

- Die Anforderungen werden für die Ergebnisse der Zugriffsantwort „*allowed*“ und „*Denied*“ überprüft.
- Jede Anfrage, die den Filterkriterien der aktivierten Traces entspricht, wird im Protokoll der Trace-Ergebnisse aufgezeichnet.
- Der Speicheradministrator kann für einen Filter eine Zeitüberschreitung konfigurieren, um ihn automatisch zu deaktivieren.
- Wenn eine Anfrage mehreren Filtern entspricht, werden die Ergebnisse des Filters mit der höchsten Indexnummer aufgezeichnet.
- Der Speicheradministrator kann Ergebnisse aus dem Protokoll der Trace-Ergebnisse drucken, um zu bestimmen, warum eine Zugriffsanfrage zugelassen oder abgelehnt wurde.

Arten von Zugriffsprüfungen Sicherheits-Traces überwachen

Zugriffsprüfungen für eine Datei oder einen Ordner werden nach mehreren Kriterien durchgeführt. Sicherheitspuren überwachen Operationen nach all diesen Kriterien.

Folgende Arten von Zugriffsprüfungen werden von der Überwachung von Sicherheitspuren überwacht:

- Volume- und qtree-Sicherheitsstil
- Effektive Sicherheit des Dateisystems, das die Dateien und Ordner enthält, auf denen die Vorgänge angefordert werden
- Benutzerzuordnung
- Berechtigungen auf Share-Ebene
- Berechtigungen auf Exportebene
- Berechtigungen auf Dateiebene
- Sicherheit der Zugriffskontrolle auf Storage-Ebene

Überlegungen beim Erstellen von Sicherheitspuren

Bei der Erstellung von Sicherheitspuren auf Storage Virtual Machines (SVMs) sollten Sie mehrere Überlegungen in Hinterkopf behalten. Zum Beispiel müssen Sie wissen, auf welchen Protokollen Sie einen Trace erstellen können, welche Sicherheitsstile unterstützt werden und wie viele aktive Traces maximal sind.

- Sie können nur Sicherheitspuren auf SVMs erstellen.
- Jeder Eintrag von Security Trace-Filtern ist SVM-spezifisch.

  Sie müssen die SVM angeben, auf der Sie den Trace ausführen möchten.

- Sie können Filter für die Berechtigungs-Verfolgung von SMB- und NFS-Anfragen hinzufügen.
- Sie müssen den SMB- oder NFS-Server auf der SVM einrichten, auf der Sie Trace-Filter erstellen möchten.
- Sie können Sicherheitspuren für Dateien und Ordner auf NTFS, UNIX und gemischten Volumes und qtrees im Sicherheitsstil erstellen.
- Sie können maximal 10 Filter für die Ablaufverfolgung von Berechtigungen pro SVM hinzufügen.
- Sie müssen beim Erstellen oder Ändern eines Filters eine Filterindex-Nummer angeben.

Filter werden in der Reihenfolge der Indexnummer berücksichtigt. Die Kriterien in einem Filter mit einer höheren Indexnummer werden vor den Kriterien mit einer niedrigeren Indexnummer berücksichtigt. Wenn die zurückverfolgende Anfrage mit den Kriterien mehrerer aktivierter Filter übereinstimmt, wird nur der Filter mit der höchsten Indexnummer ausgelöst.

- Nachdem Sie einen Sicherheits-Trace-Filter erstellt und aktiviert haben, müssen Sie einige Datei- oder Ordneranforderungen auf einem Client-System durchführen, um Aktivitäten zu generieren, die der Trace-Filter im Trace-Ergebnisprotokoll erfassen und anmelden kann.
- Sie sollten Filter für Berechtigungs-Tracing hinzufügen, um die Überprüfung des Dateizugriffs oder die Fehlerbehebung zu prüfen.

  Das Hinzufügen von Berechtigungs-Tracing-Filtern hat eine geringe Auswirkung auf die Controller-Leistung.

  Wenn Sie mit Überprüfungs- oder Fehlerbehebungsaktivitäten fertig sind, sollten Sie alle Filter für die Berechtigungsprüfung deaktivieren oder entfernen. Darüber hinaus sollten die von Ihnen ausgewählten Filterkriterien so spezifisch wie möglich sein, damit ONTAP keine große Anzahl von Trace-Ergebnissen an das Protokoll sendet.

Führen Sie Sicherheitspuren durch

Übersicht über Sicherheitspuren durchführen

Beim Durchführen eines Sicherheitspurenfilters werden ein Sicherheitsverfolgungsfilter erstellt, die Filterkriterien überprüft, Zugriffsanfragen auf einem SMB- oder NFS-Client generiert, die den Filterkriterien entsprechen, und die Ergebnisse angezeigt.

Nachdem Sie mit einem Sicherheitsfilter die Trace-Informationen erfasst haben, können Sie den Filter ändern und erneut verwenden oder deaktivieren, wenn Sie ihn nicht mehr benötigen. Nach dem Anzeigen und Analysieren der Filter-Trace-Ergebnisse können Sie sie löschen, wenn sie nicht mehr benötigt werden.

Erstellen von Sicherheitsverfolgungsfiltern

Sie können Filter für Sicherheitsspuren erstellen, die SMB- und NFS-Client-Vorgänge auf Storage Virtual Machines (SVMs) erkennen und alle Zugriffsprüfungen verfolgen, die dem Filter entsprechen. Sie können die Ergebnisse aus Sicherheitspuren verwenden, um Ihre Konfiguration zu validieren oder um Zugriffsprobleme zu beheben.

Über diese Aufgabe

Für den Befehl vserver Security trace Filter create gibt es zwei erforderliche Parameter:

Erforderliche Parameter	Beschreibung
`-vserver vserver_name`	*SVM Name* Der Name der SVM, die die Dateien oder Ordner enthält, auf denen Sie den Filter für die Sicherheitsverfolgung anwenden möchten.

`-index index_number`	*Indexnummer Filter* Die Indexnummer, die auf den Filter angewendet werden soll. Sie dürfen pro SVM maximal 10 Trace-Filter verwenden. Die zulässigen Werte für diesen Parameter sind 1 bis 10.

Mit einer Reihe optionaler Filterparameter können Sie den Sicherheitsspurfilter so anpassen, dass Sie die Ergebnisse des Sicherheitspurenfilters eingrenzen können:

Filterparameter	Beschreibung
`-client-ip IP_Address`	Dieser Filter gibt die IP-Adresse an, von der der Benutzer auf die SVM zugreift.
`-path path`	Dieser Filter gibt den Pfad an, auf den der Berechtigungs-Trace-Filter angewendet werden soll. Der Wert für `-path` Es stehen folgende Formate zur Verfügung: • Der vollständige Pfad, beginnend mit dem Stammverzeichnis der Freigabe oder des Exports • Ein partieller Pfad, relativ zur Wurzel des Shares Im Pfadwert müssen Sie die Verzeichnistrennzeichen für das NFS-Style-Verzeichnis UNIX-Stil verwenden.
`-windows-name win_user_name` Oder `-unix -name``unix_user_name`	Sie können entweder den Windows-Benutzernamen oder den UNIX-Benutzernamen angeben, dessen Zugriffsanfragen Sie nachverfolgen möchten. Die Groß-/Kleinschreibung der Variable für den Benutzernamen wird nicht berücksichtigt. Sie können keinen Windows-Benutzernamen und keinen UNIX-Benutzernamen im selben Filter angeben. Auch wenn Sie SMB- und NFS-Zugriffsereignisse verfolgen können, können der zugewiesene UNIX Benutzer und die zugeordneten UNIX Benutzergruppen verwendet werden, wenn Zugriffsprüfungen für gemischte oder UNIX-Sicherheitsdaten durchgeführt werden.
`-trace-allow {yes`	`no}`
Für einen Sicherheits-Trace-Filter ist immer die Verfolgung von Deny-Ereignissen aktiviert. Sie können optional Ereignisse zulassen nachverfolgen. Um Ereignisse zuzulassen, legen Sie diesen Parameter auf fest `yes`.	`-enabled {enabled`

`disabled}`	Sie können den Filter für die Sicherheitsverfolgung aktivieren oder deaktivieren. Standardmäßig ist der Filter Security Trace aktiviert.
`-time-enabled integer`	Sie können eine Zeitüberschreitung für den Filter angeben, nach der er deaktiviert ist.

Schritte

1. Erstellen eines Sicherheits-Trace-Filters:

   `vserver security trace filter create -vserver vserver_name -index index_numberfilter_parameters`

   `filter_parameters` Ist eine Liste der optionalen Filterparameter.

   Weitere Informationen finden Sie auf den man-Pages für den Befehl.

2. Überprüfen Sie den Eintrag des Sicherheits-Trace-Filters:

   `vserver security trace filter show -vserver vserver_name -index index_number`

Beispiele

Mit dem folgenden Befehl wird ein Security Trace Filter für jeden Benutzer erstellt, der auf eine Datei mit einem Freigabepfad zugreift `\\server\share1\dir1\dir2\file.txt` Aus der IP-Adresse 10.10.10.7. Der Filter verwendet einen vollständigen Pfad für den `-path` Option. Die IP-Adresse des Clients, die für den Zugriff auf Daten verwendet wird, lautet 10.10.10.7. Der Filter wird nach 30 Minuten ausgezeiten:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

Mit dem folgenden Befehl wird ein Security Trace Filter unter Verwendung eines relativen Pfads für das erstellt `-path` Option. Der Filter verfolgt den Zugriff für einen Windows-Benutzer namens „`joe`“. Joe greift auf eine Datei mit einem Freigabepfad zu `\\server\share1\dir1\dir2\file.txt`. Die Filterspuren erlauben und verweigern Ereignisse:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                                Vserver: vs1
                           Filter Index: 2
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                      Windows User Name: mydomain\joe
                         UNIX User Name: -
                      Trace Allow Events: yes
                         Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Informationen zu Sicherheitsverfolgungsfiltern anzeigen

Sie können Informationen zu den auf Ihrer Storage Virtual Machine (SVM) konfigurierten Sicherheitstrace-Filtern anzeigen. So können Sie sehen, welche Arten von Zugriffsereignissen die einzelnen Filterspuren anzeigen.

Schritt

1. Zeigen Sie mithilfe des Informationen zu den Einträgen von Sicherheitsverfolgungsfiltern an `vserver security trace filter show` Befehl.

   Weitere Informationen über diese Verwendung dieses Befehls finden Sie in den man-Pages.

Beispiele

Mit dem folgenden Befehl werden Informationen zu allen SicherheitsTrace-Filtern in SVM vs1 angezeigt:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Zeigen Sie die Ergebnisse der Sicherheitspurenverfolgung an

Sie können die für Dateivorgänge generierten Ergebnisse von Sicherheitspuren anzeigen, die mit den Filtern von Sicherheitsnachverfolgung übereinstimmen. Anhand der Ergebnisse können Sie die Sicherheitskonfiguration für den Dateizugriff validieren oder Probleme mit dem SMB- und NFS-Dateizugriff beheben.

Was Sie benötigen

Es muss ein aktivierter Filter für Sicherheitsnachverfolgung vorhanden sein, und Vorgänge müssen von einem SMB- oder NFS-Client ausgeführt werden, der mit dem Security Trace-Filter übereinstimmt, um Ergebnisse von Sicherheitspuren zu generieren.

Über diese Aufgabe

Sie können eine Zusammenfassung aller Ergebnisse von Sicherheitspuren anzeigen oder durch Angabe optionaler Parameter anpassen, welche Informationen in der Ausgabe angezeigt werden. Dies kann hilfreich sein, wenn die Ergebnisse der Sicherheitspurenverfolgung eine große Anzahl von Datensätzen enthalten.

Wenn Sie keinen der optionalen Parameter angeben, wird Folgendes angezeigt:

- Name der Storage Virtual Machine (SVM
- Node-Name
- Indexnummer der Sicherheitsspur
- Sicherheitsstil
- Pfad
- Grund
- Benutzername

  Der Benutzername wird je nach Konfiguration des Trace-Filters angezeigt:

Wenn der Filter konfiguriert ist…	Dann…
Mit einem UNIX-Benutzernamen	Das Ergebnis der Sicherheitsverfolgung zeigt den UNIX-Benutzernamen an.
Mit einem Windows-Benutzernamen	Das Ergebnis der Sicherheitsverfolgung zeigt den Windows-Benutzernamen an.
Ohne Benutzernamen	Das Ergebnis der Sicherheitsverfolgung zeigt den Windows-Benutzernamen an.

Sie können die Ausgabe mit optionalen Parametern anpassen. Einige der optionalen Parameter, mit denen Sie die in der Befehlsausgabe zurückgegebenen Ergebnisse eingrenzen können, umfassen die folgenden:

Optionaler Parameter	Beschreibung
`-fields field_name, ...`	Zeigt die Ausgabe der ausgewählten Felder an. Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.
`-instance`	Zeigt detaillierte Informationen zu Sicherheits-Trace-Ereignissen an. Verwenden Sie diesen Parameter mit anderen optionalen Parametern, um detaillierte Informationen zu bestimmten Filterergebnissen anzuzeigen.

`-node node_name`	Zeigt nur Informationen zu Ereignissen auf dem angegebenen Node an.
`-vserver vserver_name`	Zeigt nur Informationen zu Ereignissen auf der angegebenen SVM an.
`-index integer`	Zeigt Informationen zu den Ereignissen an, die als Ergebnis des Filters der angegebenen Indexnummer aufgetreten sind.
`-client-ip IP_address`	Zeigt Informationen zu den Ereignissen an, die infolge des Dateizugriffs von der angegebenen Client-IP-Adresse aufgetreten sind.
`-path path`	Zeigt Informationen zu den Ereignissen an, die infolge des Dateizugriffs auf den angegebenen Pfad aufgetreten sind.
`-user-name user_name`	Zeigt Informationen zu Ereignissen an, die durch den Dateizugriff durch den angegebenen Windows- oder UNIX-Benutzer aufgetreten sind.
`-security-style security_style`	Zeigt Informationen zu Ereignissen an, die auf Dateisystemen mit dem angegebenen Sicherheitsstil aufgetreten sind.

Informationen zu anderen optionalen Parametern, die Sie mit dem Befehl verwenden können, finden Sie auf der man-Seite.

Schritt

1. Zeigen Sie die Ergebnisse des Filter für Sicherheitsnachverfolgung mithilfe des an `vserver security trace trace-result show` Befehl.

   ```
   vserver security trace trace-result show -user-name domain\user
   ```

   ```
   Vserver: vs1

   Node     Index   Filter Details         Reason
   -------- ------- ---------------------  ------------------------------
   node1    3       User:domain\user       Access denied by explicit ACE
                    Security Style:mixed
                    Path:/dir1/dir2/

   node1    5       User:domain\user       Access denied by explicit ACE
                    Security Style:unix
                    Path:/dir1/
   ```

Ändern Sie die Filter für die Sicherheitsverfolgung

Wenn Sie die optionalen Filterparameter ändern möchten, mit denen ermittelt wird, welche Zugriffsereignisse verfolgt werden, können Sie vorhandene Sicherheits-Trace-Filter ändern.

Über diese Aufgabe

Sie müssen ermitteln, welchen Sicherheits-Trace-Filter Sie ändern möchten, indem Sie den SVM-Namen (Storage Virtual Machine) angeben, auf den der Filter angewendet wird, und die Indexnummer des Filters. Sie können alle optionalen Filterparameter ändern.

Schritte

1. Bearbeiten eines Sicherheitsverfolgungsfilters:

   ```
   vserver security trace filter modify -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   - `vserver_name` Ist der Name der SVM, auf der Sie einen Sicherheits-Trace-Filter anwenden möchten.
   - `index_number` Ist die Indexnummer, die Sie auf den Filter anwenden möchten. Die zulässigen Werte für diesen Parameter sind 1 bis 10.
   - `filter_parameters` Ist eine Liste der optionalen Filterparameter.

2. Überprüfen Sie den Eintrag des Sicherheits-Trace-Filters:

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

Beispiel

Mit dem folgenden Befehl wird der Security Trace Filter mit der Indexnummer 1 geändert. Der Filter verfolgt Ereignisse für jeden Benutzer, der auf eine Datei mit einem Freigabepfad zugreift `\\server\share1\dir1\dir2\file.txt` Von einer beliebigen IP-Adresse aus. Der Filter verwendet einen vollständigen Pfad für den `-path` Option. Die Filterspuren erlauben und verweigern Ereignisse:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                Vserver: vs1
                           Filter Index: 1
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: -
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Löschen Sie die Sicherheitsverfolgungsfilter

Wenn Sie keinen Eintrag für den Sicherheits-Trace-Filter mehr benötigen, können Sie ihn löschen. Da Sie maximal 10 Sicherheitsverfolgungsfilter pro Storage Virtual Machine (SVM) verwenden können, können Sie durch das Löschen nicht benötigter Filter neue Filter erstellen, wenn Sie das Maximum erreicht haben.

Über diese Aufgabe

Um den zu löschenden Sicherheits-Trace-Filter eindeutig zu identifizieren, müssen Sie Folgendes angeben:

- Der Name der SVM, auf die der Trace-Filter angewendet wird
- Die Filterindex-Nummer des Trace-Filters

Schritte

1. Geben Sie die Filterindex-Nummer des zu löschenden Sicherheits-Trace-Filters an:

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. Löschen Sie den Filtereintrag mithilfe der Filterindex-Nummern aus dem vorherigen Schritt:

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number
   ```

   ```
   vserver security trace filter delete -vserver vs1 -index 1
   ```

3. Vergewissern Sie sich, dass der Eintrag für den Sicherheits-Trace-Filter gelöscht wurde:

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

Löschen von Sicherheits-Trace-Datensätzen

Nachdem Sie den Filter-Trace-Datensatz zur Überprüfung der Dateizugriffssicherheit verwendet oder Probleme mit dem Zugriff auf SMB- oder NFS-Clients behoben haben, können Sie den Security Trace-Datensatz aus dem Security Trace-Protokoll löschen.

Über diese Aufgabe

Bevor Sie einen Sicherheits-Trace-Datensatz löschen können, müssen Sie die Sequenznummer des Datensatzes kennen.

> Jede Storage Virtual Machine (SVM) kann maximal 128 Trace-Datensätze speichern. Wird das Maximum auf der SVM erreicht, werden die ältesten Trace-Datensätze automatisch gelöscht, sobald neue hinzugefügt werden. Wenn Sie Trace-Datensätze auf dieser SVM nicht manuell löschen möchten, können Sie ONTAP die ältesten Trace-Ergebnisse automatisch löschen lassen, nachdem das Maximum erreicht wurde, um Platz für neue Ergebnisse zu schaffen.

Schritte

1. Geben Sie die Sequenznummer des zu löschenden Datensatzes an:

   ```
   vserver security trace trace-result show -vserver vserver_name -instance
   ```

2. Löschen Sie den Sicherheits-Trace-Datensatz:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name -seqnum integer
   ```

   ```
   vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
   999
   ```

   - `-node node_name` Ist der Name des Cluster-Node, auf dem das Ereignis Berechtigungstrennung, das Sie löschen möchten, stattgefunden hat.

     Dies ist ein erforderlicher Parameter.

   - `-vserver vserver_name` Ist der Name der SVM, auf der das Ereignis für die Berechtigungs-Verfolgung, das Sie löschen möchten, stattgefunden hat.

     Dies ist ein erforderlicher Parameter.

   - `-seqnum integer` Ist die Sequenznummer des Protokollereignisses, das Sie löschen möchten.

     Dies ist ein erforderlicher Parameter.

Löschen Sie alle Sicherheits-Trace-Datensätze

Wenn Sie keine der vorhandenen Sicherheits-Trace-Datensätze speichern möchten, können Sie alle Datensätze auf einem Knoten mit einem einzigen Befehl löschen.

Schritt

1. Alle Sicherheitsaufzeichnungen löschen:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   ```

`vserver_name *`

- `-node node_name` Ist der Name des Cluster-Node, auf dem das Ereignis Berechtigungstrennung, das Sie löschen möchten, stattgefunden hat.
- `-vserver vserver_name` Ist der Name der Storage Virtual Machine (SVM), auf der das Ereignis für die Berechtigungs-Verfolgung, das Sie löschen möchten, stattgefunden hat.

Die Ergebnisse der Sicherheitsverfolgung interpretieren

Die Ergebnisse von Sicherheitspuren geben den Grund an, warum eine Anfrage zugelassen oder abgelehnt wurde. Die Ausgabe zeigt das Ergebnis als eine Kombination aus dem Grund für das Zulassen oder Ablehnen des Zugriffs und dem Ort innerhalb des Zugriffspunts an, auf dem der Zugriff erlaubt oder verweigert wird. Anhand der Ergebnisse können Sie bestimmen, warum Aktionen zulässig sind oder nicht.

Informationen zu den Listen der Ergebnistypen und Filterdetails finden

Sie finden die Listen der Ergebnistypen und Filterdetails, die in den Sicherheitspurenergebnissen in den man-Pages für die enthalten sind `vserver security trace trace-result show` Befehl.

Beispiel für die Ausgabe aus dem `Reason` Feld in einem `Allow` Ergebnistyp

Im Folgenden finden Sie ein Beispiel für die Ausgabe von `Reason` Feld, das im Protokoll der Trace-Ergebnisse in einem angezeigt wird `Allow` Ergebnistyp:

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

Beispiel für die Ausgabe aus dem `Reason` Feld in einem `Allow` Ergebnistyp

Im Folgenden finden Sie ein Beispiel für die Ausgabe von `Reason` Feld, das im Protokoll der Trace-Ergebnisse in A angezeigt wird `Deny` Ergebnistyp:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

Beispiel für die Ausgabe aus dem `Filter details` Feld

Im Folgenden finden Sie ein Beispiel für die Ausgabe von `Filter details` Feld im Protokoll der Trace-Ergebnisse, in dem der effektive Sicherheitsstil des Dateisystems mit Dateien und Ordnern aufgeführt wird, die den Filterkriterien entsprechen:

```
Security Style: MIXED and ACL
```

Wo Sie weitere Informationen finden

Nach dem erfolgreichen Testen des SMB-Client-Zugriffs können Sie eine erweiterte SMB-Konfiguration durchführen oder SAN-Zugriff hinzufügen. Nachdem Sie den NFS-Client-Zugriff erfolgreich getestet haben, können Sie die erweiterte NFS-Konfiguration oder den SAN-Zugriff hinzufügen. Nach Abschluss des Protokollzugriffs sollten Sie das Root-Volume der SVM schützen.

SMB-Konfiguration

Sie können den SMB-Zugriff noch weiter konfigurieren, indem Sie Folgendes verwenden:

- "SMB-Management"

  Beschreibt die Konfiguration und das Management des Dateizugriffs mithilfe des SMB-Protokolls.

- "Technischer Bericht 4191 von NetApp: Best Practices Guide for Clustered Data ONTAP 8.2 Windows File Services"

  Überblick über die SMB-Implementierung und andere Windows-Fileservices-Funktionen mit Empfehlungen und grundlegenden Informationen zur Fehlerbehebung für ONTAP

- "Technischer Bericht von NetApp: 3740 SMB 2 CIFS-Protokoll der nächsten Generation in Data ONTAP"

  Beschreibt die Funktionen von SMB 2, die Konfigurationsdetails und die Implementierung in ONTAP.

NFS-Konfiguration

Sie können darüber hinaus den NFS-Zugriff wie folgt konfigurieren:

- "NFS-Management"

  Beschreibt die Konfiguration und das Management des Dateizugriffs mithilfe des NFS-Protokolls.

- "NetApp Technical Report 4067: NFS Best Practice and Implementation Guide"

  Dient als NFSv3 und NFSv4-Betriebsanleitung und bietet einen Überblick über das ONTAP Betriebssystem mit Schwerpunkt auf NFSv4.

- "NetApp Technical Report 4668: Name Services Best Practices Guide"

  Dieser Service bietet eine umfassende Liste von Best Practices, Limits, Empfehlungen und Überlegungen beim Konfigurieren von LDAP-, NIS-, DNS- und lokalen Benutzer- und Gruppendateien für Authentifizierungszwecke.

- "Technischer Bericht von NetApp 4616: NFS Kerberos im ONTAP mit Microsoft Active Directory"
- "Technischer Bericht von NetApp 4835: Konfigurieren von LDAP in ONTAP"
- "Technischer Bericht von NetApp 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation"

  Beschreibt die Best Practices, die befolgt werden sollten bei der Implementierung von NFSv4-Komponenten auf AIX, Linux- oder Solaris-Clients, die mit Systemen verbunden sind, auf denen ONTAP ausgeführt wird.

Sicherung des Root-Volumes

Nach der Konfiguration von Protokollen auf der SVM sollten Sie sicherstellen, dass sein Root-Volume geschützt ist:

- "Datensicherung"

  Beschreibt die Erstellung einer Spiegelung zur Lastverteilung, die das Root-Volume der SVM sichert. Diese Best Practice ist bei NetApp für NAS-fähige SVMs enthalten. Beschreibt außerdem, wie man bei Volume-Ausfällen oder -Verlusten schnell eine Recovery durchführen kann, indem das SVM-Root-Volume von einer Spiegelung zur Lastverteilung bereitgestellt wird.

Management der Verschlüsselung mit System Manager

Verschlüsselung gespeicherter Daten mit softwarebasierter Verschlüsselung

Mit Volume-Verschlüsselung können Sie sicherstellen, dass Volume-Daten nicht gelesen werden können, wenn das zugrunde liegende Gerät neu verwendet, zurückgegeben, verlegt oder gestohlen wird. Für die Volume-Verschlüsselung sind keine speziellen Festplatten erforderlich, sondern für alle HDDs und SSDs geeignet.

Für die Volume-Verschlüsselung ist ein Schlüsselmanager erforderlich. Sie können den Onboard Key Manager mit System Manager konfigurieren. Sie können auch einen externen Schlüsselmanager verwenden, aber Sie müssen ihn zuerst mithilfe der ONTAP-CLI einrichten.

Nach der Konfiguration des Schlüsselmanagers werden neue Volumes standardmäßig verschlüsselt.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie unter **Verschlüsselung** auf ⚙ So konfigurieren Sie den Onboard Key Manager zum ersten Mal.
3. Um vorhandene Volumes zu verschlüsseln, klicken Sie auf **Storage > Volumes**.
4. Klicken Sie auf das gewünschte Volumen ⋮ Und klicken Sie dann auf **Bearbeiten**.
5. Wählen Sie **Verschlüsselung aktivieren**.

Verschlüsselung gespeicherter Daten mit Self-Encrypting Drives

Mit der Festplattenverschlüsselung können Sie sicherstellen, dass alle Daten in einer lokalen Tier nicht gelesen werden können, wenn das zugrunde liegende Gerät neu verwendet, zurückgegeben, verlegt oder gestohlen wird. Die Festplattenverschlüsselung erfordert spezielle Self-Encrypting Drives oder SSDs.

Die Festplattenverschlüsselung erfordert einen Schlüsselmanager. Sie können den integrierten Schlüsselmanager mithilfe von System Manager konfigurieren. Sie können auch einen externen Schlüsselmanager verwenden, aber Sie müssen ihn zuerst mithilfe der ONTAP-CLI einrichten.

Wenn ONTAP selbstverschlüsselnde Festplatten erkennt, werden Sie aufgefordert, den Onboard-Schlüsselmanager bei der Erstellung der lokalen Ebene zu konfigurieren.

Schritte

1. Klicken Sie unter **Verschlüsselung** auf ⚙ Zum Konfigurieren des Onboard-Schlüsselmanagers.
2. Wenn eine Meldung angezeigt wird, dass die Datenträger rekeying werden müssen, klicken Sie auf ⋮, Und klicken Sie dann auf **Rekey Disks**.

Management der Verschlüsselung über CLI

Übersicht über die NetApp Verschlüsselung

NetApp bietet sowohl Software- als auch hardwarebasierte Verschlüsselungstechnologien, um sicherzustellen, dass Daten im Ruhezustand nicht gelesen werden können, wenn das Storage-Medium neu verwendet, zurückgegeben, verloren gegangen oder gestohlen wird.

- Softwarebasierte Verschlüsselung unter Verwendung von NetApp Volume Encryption (NVE) unterstützt die Datenverschlüsselung für ein Volume gleichzeitig
- Hardwarebasierte Verschlüsselung mit NetApp Storage Encryption (NSE) unterstützt die vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) von Daten beim Schreiben.

NetApp Volume Encryption konfigurieren

NetApp Volume Encryption Übersicht konfigurieren

NetApp Volume Encryption (NVE) ist eine softwarebasierte Technologie, mit der Daten im Ruhezustand um ein Volume gleichzeitig verschlüsselt werden. Ein Verschlüsselungsschlüssel, auf den nur das Storage-System zugegriffen werden kann, stellt sicher, dass Volume-Daten nicht gelesen werden können, wenn das zugrunde liegende Gerät neu verwendet, zurückgegeben, verlegt oder gestohlen wird.

Allgemeines zu NVE

Mit NVE werden Metadaten und Daten (einschließlich Snapshot Kopien) verschlüsselt. Der Zugriff auf die Daten erfolgt über einen eindeutigen XTS-AES-256-Schlüssel, einen pro Volume. Ein externer Schlüsselmanagementserver oder Onboard Key Manager (OKM) bedient Schlüssel zu Knoten:

- Der externe Verschlüsselungsmanagement-Server ist ein Drittanbietersystem in der Storage-Umgebung, das mithilfe des Key Management Interoperability Protocol (KMIP) Schlüssel zu Nodes bereitstellt. Als Best Practice wird empfohlen, externe Verschlüsselungsmanagementserver auf einem anderen Storage-System zu Ihren Daten zu konfigurieren.
- Der Onboard Key Manager ist ein integriertes Tool, das Schlüssel zu Nodes aus demselben Storage-System wie Ihre Daten bereitstellt.

Ab ONTAP 9.7 ist die Aggregat- und Volume-Verschlüsselung standardmäßig aktiviert, wenn Sie über eine VE-Lizenz (Volume Encryption) verfügen und einen integrierten oder externen Schlüsselmanager verwenden. Die VE-Lizenz ist in enthalten "ONTAP One". Bei der Konfiguration eines externen oder integrierten Schlüsselmanagers ändert sich die Konfiguration der Verschlüsselung von Daten im Ruhezustand für brandneue Aggregate und brandneue Volumes. Bei neuen Aggregaten ist die NetApp Aggregate Encryption (NAE) standardmäßig aktiviert. Für brandneue Volumes, die nicht Teil eines NAE-Aggregats sind, ist NetApp Volume Encryption (NVE) standardmäßig aktiviert. Wenn eine Storage Virtual Machine (SVM) mit einem eigenen Schlüsselmanager über mandantenfähiges Verschlüsselungsmanagement konfiguriert wird, wird das für diese SVM erstellte Volume automatisch mit NVE konfiguriert.

Sie können die Verschlüsselung auf einem neuen oder vorhandenen Volume aktivieren. NVE unterstützt eine breite Palette an Storage-Effizienzfunktionen, einschließlich Deduplizierung und Komprimierung. Ab ONTAP 9.14.1 ist dies möglich Aktivieren Sie NVE bei vorhandenen SVM-Root-Volumes.

> Wenn Sie SnapLock verwenden, können Sie nur die Verschlüsselung auf neuen, leeren SnapLock Volumes aktivieren. Sie können die Verschlüsselung auf einem vorhandenen SnapLock-Volume nicht aktivieren.

NVE kann für jeden Aggregattyp (HDD, SSD, Hybrid, Array LUN), mit jedem RAID-Typ und in jeder unterstützten ONTAP Implementierung, einschließlich ONTAP Select, eingesetzt werden. NVE kann auch mit hardwarebasierter Verschlüsselung verwendet werden, um Daten auf Self-Encrypting Drives `double Encryption` zu verschlüsseln.

Wenn NVE aktiviert ist, wird der Core Dump ebenfalls verschlüsselt.

Verschlüsselung auf Aggregatebene

Normalerweise wird jedem verschlüsselten Volume ein eindeutiger Schlüssel zugewiesen. Wenn das Volume gelöscht wird, wird der Schlüssel mit ihm gelöscht.

Ab ONTAP 9.6 können Sie *NetApp Aggregate Encryption (NAE)* verwenden, um dem zugehörigen Aggregat Schlüssel zuzuweisen, damit die Volumes verschlüsselt werden. Beim Löschen eines verschlüsselten Volumes bleiben die Schlüssel für das Aggregat erhalten. Die Schlüssel werden gelöscht, wenn das gesamte Aggregat gelöscht wird.

Wenn Sie eine Inline- oder eine Hintergrund-Deduplizierung auf Aggregatebene durchführen möchten, muss die Verschlüsselung auf Aggregatebene verwendet werden. Deduplizierung auf Aggregatebene wird ansonsten von NVE nicht unterstützt.

Ab ONTAP 9.7 ist die Aggregat- und Volume-Verschlüsselung standardmäßig aktiviert, wenn Sie über eine VE-Lizenz (Volume Encryption) verfügen und einen integrierten oder externen Schlüsselmanager verwenden.

NVE und NAE-Volumes können gleichzeitig im selben Aggregat bestehen. Bei der Verschlüsselung von Volumes auf Aggregatebene sind standardmäßig NAE-Volumes enthalten. Sie können den Standardwert überschreiben, wenn Sie das Volume verschlüsseln.

Sie können das verwenden `volume move` Befehl zum Konvertieren eines NVE-Volumes in ein NAE-Volume und umgekehrt. Sie können ein NAE-Volume auf ein NVE Volume replizieren.

Verwenden Sie ihn nicht `secure purge` Befehle auf einem NAE-Volume.

Wann sollten Sie externe Verschlüsselungsmanagementserver verwenden

Die Verwendung des Onboard-Schlüsselmanagers ist kostengünstiger und in der Regel bequemer, doch Sie sollten KMIP-Server einrichten, wenn eine der folgenden Angaben zutrifft:

- Ihre Lösung für das Verschlüsselungsmanagement muss den Federal Information Processing Standards (FIPS) 140-2 oder DEM OASIS KMIP Standard entsprechen.
- Sie benötigen eine Multi-Cluster-Lösung mit zentralem Management von Verschlüsselungen.
- Ihr Unternehmen erfordert die zusätzliche Sicherheit beim Speichern von Authentifizierungsschlüsseln auf einem System oder an einem anderen Speicherort als den Daten.

Umfang des externen Schlüsselmanagements

Der Umfang des externen Verschlüsselungsmanagement bestimmt, ob wichtige Managementserver alle SVMs im Cluster oder nur ausgewählte SVMs sichern:

- Sie können ein_Cluster Scope_ verwenden, um das externe Verschlüsselungsmanagement für alle SVMs im Cluster zu konfigurieren. Der Clusteradministrator hat Zugriff auf jeden auf den Servern gespeicherten Schlüssel.
- Ab ONTAP 9.6 können Sie mithilfe eines Umfangs *SVM* externes Verschlüsselungsmanagement für eine im Cluster genannte SVM konfigurieren. Dies eignet sich am besten für mandantenfähige Umgebungen, in denen jeder Mandant eine andere SVM (oder einen Satz SVMs) zur Bereitstellung von Daten verwendet. Nur der SVM-Administrator für einen bestimmten Mandanten hat Zugriff auf die Schlüssel für den jeweiligen Mandanten.
- Ab ONTAP 9.10.1 können Sie dies nutzen Azure Key Vault und Google Cloud KMS Zum Schutz von NVE-Schlüsseln nur für Daten-SVMs Dies ist für KMS von AWS ab 9.12.0 verfügbar.

Sie können beide Bereiche im selben Cluster verwenden. Wenn Verschlüsselungsmanagement-Server für eine SVM konfiguriert wurden, verwendet ONTAP nur diese Server zur Sicherung der Schlüssel. Andernfalls sichert ONTAP Schlüssel mit den für den Cluster konfigurierten Verschlüsselungsmanagement-Servern.

Eine Liste validierter externer Schlüsselmanager finden Sie im "NetApp Interoperabilitäts-Matrix-Tool (IMT)". Sie können diese Liste finden, indem Sie in die Suchfunktion des IMT den Begriff „wichtige Manager“ eingeben.

Support-Details

In der folgenden Tabelle sind die Support-Details von NVE aufgeführt:

Ressource oder Funktion	Support-Details
Plattformen	Eine AES-NI-Offload-Funktion ist erforderlich. Überprüfen Sie im Hardware Universe (HWU), ob NVE und NAE für Ihre Plattform unterstützt werden.

Verschlüsselung	Ab ONTAP 9.7 werden neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn Sie eine VE-Lizenz (Volume Encryption) hinzufügen und einen integrierten oder externen Schlüsselmanager konfigurieren. Wenn Sie ein unverschlüsseltes Aggregat erstellen müssen, verwenden Sie den folgenden Befehl:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Wenn Sie ein Klartextvolume erstellen müssen, verwenden Sie den folgenden Befehl:
	
	`volume create -encrypt false`
	
	Die Verschlüsselung ist standardmäßig nicht aktiviert, wenn:
	
	• Die VE-Lizenz ist nicht installiert.
	• Schlüsselmanager ist nicht konfiguriert.
	• Plattform oder Software unterstützt keine Verschlüsselung.
	• Die Hardwareverschlüsselung ist aktiviert.

ONTAP	Alle Implementierungen von ONTAP. Unterstützung für ONTAP Cloud ist in ONTAP 9.5 und höher verfügbar.
Geräte	HDD, SSD, Hybrid, Array-LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Daten-Volumes und vorhandene SVM-Root-Volumes. Daten auf MetroCluster Metadaten-Volumes können nicht verschlüsselt werden. Bei älteren Versionen als ONTAP 9.14.1 können Daten auf dem SVM-Root-Volume nicht mit NVE verschlüsselt werden. Ab ONTAP 9.14.1 unterstützt ONTAP NVE auf SVM Root-Volumes.
Verschlüsselung auf Aggregatebene	Ab ONTAP 9.6 unterstützt NVE die Verschlüsselung auf Aggregatebene (NAE): • Wenn Sie eine Inline- oder eine Hintergrund-Deduplizierung auf Aggregatebene durchführen möchten, muss die Verschlüsselung auf Aggregatebene verwendet werden. • Sie können ein Verschlüsselungsvolume auf Aggregatebene nicht rekeykey. • Sichere Löschung wird auf Verschlüsselungs-Volumes auf Aggregatebene nicht unterstützt. • Neben Daten-Volumes unterstützt NAE auch die Verschlüsselung von SVM Root-Volumes und dem MetroCluster Metadaten-Volume. NAE unterstützt keine Verschlüsselung des Root-Volumes.
SVM-Umfang	Ab ONTAP 9.6 unterstützt NVE nicht Onboard Key Manager, sondern lediglich den Umfang von SVM für externes Verschlüsselungsmanagement. MetroCluster wird ab ONTAP 9.8 unterstützt.

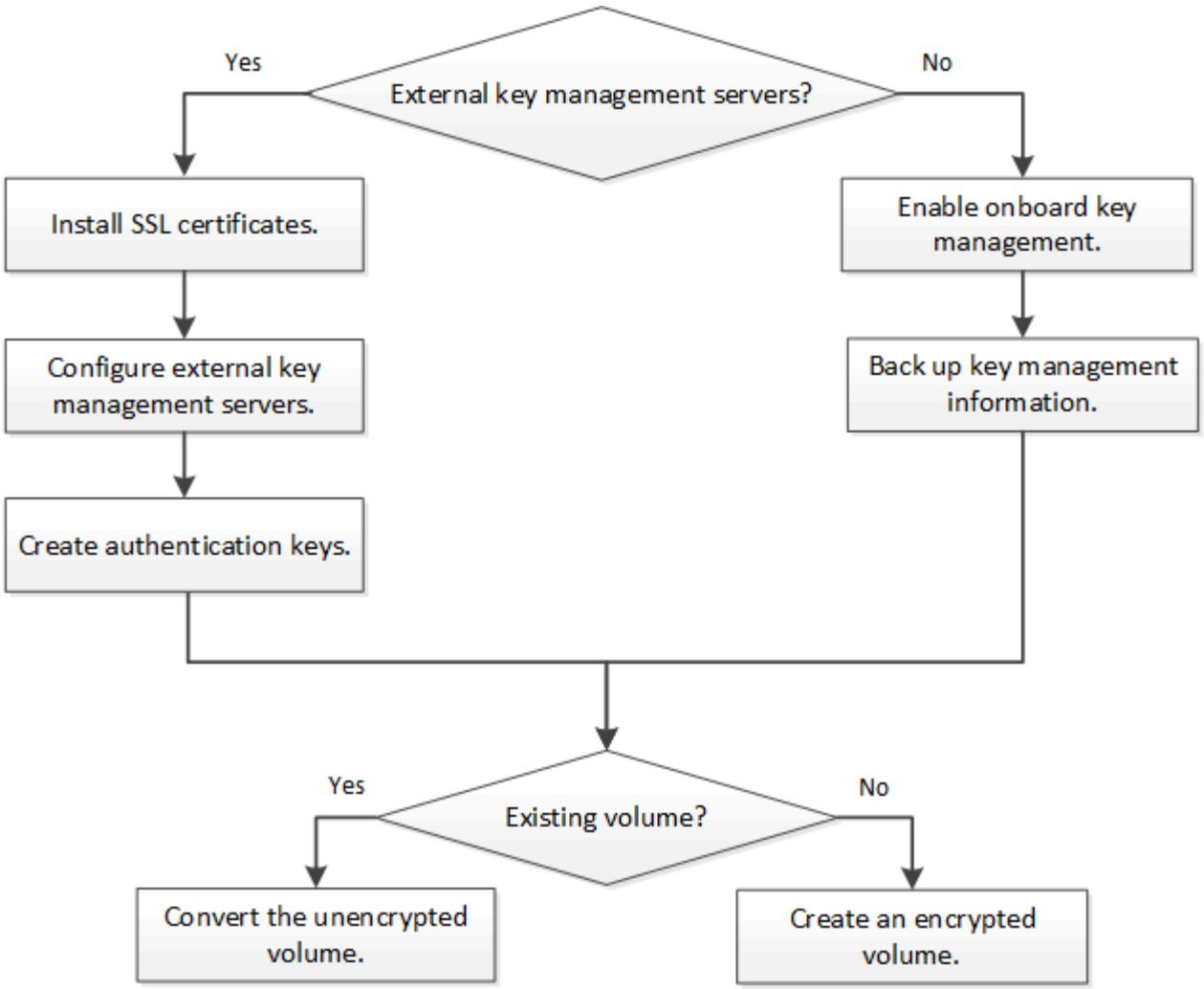
Storage-Effizienz	Deduplizierung, Komprimierung, Data-Compaction, FlexClone: Klone verwenden denselben Schlüssel wie das übergeordnete Objekt, auch nachdem der Klon vom übergeordneten Objekt geteilt wurde. Sie sollten eine durchführen `volume move` Auf einem geteilten Klon, nach dem der geteilte Klon einen anderen Schlüssel hat.
Replizierung	• Für die Volume-Replikation können die Quell- und Ziel-Volumes über unterschiedliche Verschlüsselungseinstellungen verfügen. Die Verschlüsselung kann für die Quelle konfiguriert und für das Ziel nicht konfiguriert und umgekehrt werden. • Bei der SVM-Replikation wird das Ziel-Volume automatisch verschlüsselt, es sei denn, das Ziel enthält keinen Node, der Volume Encryption unterstützt. In diesem Fall ist die Replikation erfolgreich, das Ziel-Volume ist jedoch nicht verschlüsselt. • Bei MetroCluster-Konfigurationen zieht jedes Cluster externe Verschlüsselungsmanagementschlüssel von den konfigurierten Schlüsselservern ab. OKM-Schlüssel werden vom Konfigurations-Replikationsservice auf den Partnerstandort repliziert.
Compliance	Ab ONTAP 9.2 wird SnapLock sowohl im Compliance- als auch im Enterprise-Modus unterstützt, nur für neue Volumes. Sie können die Verschlüsselung auf einem vorhandenen SnapLock-Volume nicht aktivieren.
FlexGroups	Ab ONTAP 9.2 werden FlexGroups unterstützt. Zielaggregate müssen vom gleichen Typ sein wie Quellaggregate, entweder auf Volume-Ebene oder auf Aggregatebene. Ab ONTAP 9.5 wird auch der in-Place-Rekey von FlexGroup Volumes unterstützt.
Umstieg von 7-Mode	Ab dem 7-Mode Transition Tool 3.3 können Sie mithilfe der CLI des 7-Mode Transition Tool eine Copy-basierte Transition zu NVE-fähigen Ziel-Volumes auf dem geclusterten System durchführen.

Verwandte Informationen

"FAQ – NetApp Volume Encryption und NetApp Aggregate Encryption"

NetApp Volume Encryption Workflow

Sie müssen Verschlüsselungsmanagementservices konfigurieren, bevor Sie die Volume-Verschlüsselung aktivieren können. Sie können die Verschlüsselung auf einem neuen Volume oder auf einem vorhandenen Volume aktivieren.



"Sie müssen die VE-Lizenz installieren" Und konfigurieren Sie Verschlüsselungsmanagement-Services, bevor Sie Daten mit NVE verschlüsseln können. Vor der Installation der Lizenz sollten Sie dies tun "Bestimmen Sie, ob NVE in Ihrer ONTAP-Version unterstützt wird".

Konfigurieren Sie NVE

Bestimmen Sie, ob Ihre Cluster-Version NVE unterstützt

Sie sollten vor der Installation der Lizenz festlegen, ob Ihre Cluster-Version NVE unterstützt. Sie können das verwenden `version` Befehl zum Bestimmen der Cluster-Version.

Über diese Aufgabe

Die Cluster-Version ist die niedrigste Version von ONTAP, die auf einem beliebigen Node im Cluster ausgeführt wird.

Schritt

1. Bestimmen Sie, ob Ihre Cluster-Version NVE unterstützt:

   ```
   version -v
   ```

   NVE wird nicht unterstützt, wenn in der Befehlsausgabe der Text „`1Ono-DARE`“ (für „`no Data at Rest`

`Encryption`“) angezeigt wird oder wenn Sie eine Plattform verwenden, die nicht in aufgeführt ist "Support-Details".

Mit dem folgenden Befehl wird festgelegt, ob NVE unterstützt wird `cluster1`.

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

Die Ausgabe von `1Ono-DARE` Gibt an, dass NVE bei Ihrer Cluster-Version nicht unterstützt wird.

Installieren Sie die Lizenz

Eine VE-Lizenz berechtigt Sie zur Nutzung der Funktion auf allen Knoten im Cluster. Diese Lizenz ist erforderlich, bevor Sie Daten mit NVE verschlüsseln können. Es ist in enthalten "ONTAP One".

Vor ONTAP One war die VE-Lizenz im Verschlüsselungspaket enthalten. Das Encryption Bundle wird nicht mehr angeboten, ist aber weiterhin gültig. Bestehende Kunden können diese Option wählen, obwohl sie derzeit nicht benötigt werden "Upgrade auf ONTAP One".

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen den VE-Lizenzschlüssel von Ihrem Vertriebsmitarbeiter erhalten haben oder ONTAP One installiert haben.

Schritte

1. "Überprüfen Sie, ob die VE-Lizenz installiert ist".

   Der Name des VE-Lizenzpakets lautet `VE`.

2. Wenn die Lizenz nicht installiert ist, "Verwenden Sie System Manager oder die ONTAP CLI, um sie zu installieren".

Externes Verschlüsselungsmanagement konfigurieren

Externes Verschlüsselungsmanagement – Übersicht konfigurieren

Sie können einen oder mehrere externe Verschlüsselungsmanagementserver verwenden, um die Schlüssel zu sichern, die das Cluster zum Zugriff auf verschlüsselte Daten verwendet. Ein externer Verschlüsselungsmanagement-Server ist ein Drittanbietersystem in Ihrer Storage-Umgebung, der mithilfe des Key Management Interoperability Protocol (KMIP) Schlüssel zu Nodes bereitstellt.

> Bei ONTAP 9.1 und älteren Versionen müssen Node-Management-LIFs Ports zugewiesen werden, die mit der Node-Managementrolle konfiguriert sind, bevor Sie den externen Schlüsselmanager verwenden können.

NetApp Volume Encryption (NVE) unterstützt Onboard Key Manager in ONTAP 9.1 und höher. Ab ONTAP 9.3 unterstützt NVE externes Verschlüsselungsmanagement (KMIP) und Onboard Key Manager. Ab ONTAP

9.10.1 können Sie dies nutzen Azure Key Vault oder Google Cloud Key Manager Service Zum Schutz Ihrer NVE-Schlüssel Ab ONTAP 9.11.1 können Sie mehrere externe Schlüsselmanager in einem Cluster konfigurieren. Siehe Konfigurieren Sie Cluster-Key-Server.

Management von externen Schlüsselmanagern mit System Manager

Ab ONTAP 9.7 können Sie die Authentifizierung und Verschlüsselung mit dem Onboard Key Manager speichern und managen. Ab ONTAP 9.13.1 können Sie diese Schlüssel auch mit externen Schlüsselmanagern speichern und verwalten.

Der integrierte Schlüsselmanager speichert und managt Schlüssel in einer sicheren, Cluster-internen Datenbank. Sein Umfang ist das Cluster. Ein externer Schlüsselmanager speichert und managt Schlüssel außerhalb des Clusters. Sein Umfang kann das Cluster oder die Storage-VM sein. Es können ein oder mehrere externe Schlüsselmanager verwendet werden. Es gelten die folgenden Bedingungen:

- Wenn der Onboard Key Manager aktiviert ist, kann ein externer Schlüsselmanager nicht auf Cluster-Ebene aktiviert werden, er kann jedoch auf Storage-VM-Ebene aktiviert werden.
- Wenn ein externer Schlüsselmanager auf Cluster-Ebene aktiviert ist, kann der Onboard Key Manager nicht aktiviert werden.

Beim Einsatz von externen Schlüsselmanagern können Sie bis zu vier primäre Schlüsselserver pro Storage-VM und Cluster registrieren. Jeder primäre Schlüsselserver kann mit bis zu drei sekundären Schlüsselservern gruppiert werden.

Konfigurieren Sie einen externen Schlüsselmanager

Zum Hinzufügen eines externen Schlüsselmanagers für eine Storage-VM sollten Sie beim Konfigurieren der Netzwerkschnittstelle für die Storage-VM ein optionales Gateway hinzufügen. Wenn die Speicher-VM ohne den Netzwerk-Route erstellt wurde, müssen Sie die Route explizit für den externen Schlüsselmanager erstellen. Siehe "LIF erstellen (Netzwerkschnittstelle)".

Schritte

Sie können einen externen Schlüsselmanager von verschiedenen Standorten in System Manager aus konfigurieren.

1. Führen Sie einen der folgenden Startschritte durch, um einen externen Schlüsselmanager zu konfigurieren.

Workflow	Navigation	Startschritt
Konfigurieren Sie Key Manager	**Cluster** > **Einstellungen**	Blättern Sie zum Abschnitt **Sicherheit**. Wählen Sie unter **Verschlüsselung** die Option aus ⚙. Wählen Sie **External Key Manager**.
Lokale Ebene hinzufügen	**Storage** > **Tiers**	Wählen Sie **+ Lokale Ebene Hinzufügen**. Aktivieren Sie das Kontrollkästchen „Key Manager konfigurieren“. Wählen Sie **External Key Manager**.
Storage vorbereiten	**Dashboard**	Wählen Sie im Abschnitt **Kapazität** die Option **Speicher vorbereiten** aus. Wählen Sie dann „Configure Key Manager“ aus. Wählen Sie **External Key Manager**.

Konfiguration der Verschlüsselung (nur Schlüsselmanager im Umfang von Storage-VMs)	**Storage** > **Storage VMs**	Wählen Sie die Storage-VM aus. Wählen Sie die Registerkarte **Einstellungen**. Wählen Sie im Abschnitt **Verschlüsselung** unter **Sicherheit** die Option aus ⚙.

2. Um einen primären Schlüsselserver hinzuzufügen, wählen Sie aus + Add Und füllen Sie die Felder **IP-Adresse oder Hostname** und **Port** aus.
3. Vorhandene installierte Zertifikate sind in den Feldern **KMIP Server CA Certificates** und **KMIP Client Certificate** aufgeführt. Sie können eine der folgenden Aktionen durchführen:
   - Wählen Sie ⌄ Zum Auswählen installierter Zertifikate, die dem Schlüsselmanager zugeordnet werden sollen. (Es können mehrere Service-CA-Zertifikate ausgewählt werden, es kann jedoch nur ein Client-Zertifikat ausgewählt werden.)
   - Wählen Sie **Neues Zertifikat hinzufügen**, um ein Zertifikat hinzuzufügen, das noch nicht installiert wurde, und ordnen Sie es dem externen Schlüsselmanager zu.
   - Wählen Sie × Neben dem Zertifikatnamen, um installierte Zertifikate zu löschen, die Sie nicht dem externen Schlüsselmanager zuordnen möchten.
4. Um einen sekundären Schlüsselserver hinzuzufügen, wählen Sie **Add** in der Spalte **Secondary Key Server** aus und geben Sie seine Details an.
5. Wählen Sie **Speichern**, um die Konfiguration abzuschließen.

Bearbeiten Sie einen vorhandenen externen Schlüsselmanager

Wenn Sie bereits einen externen Schlüsselmanager konfiguriert haben, können Sie dessen Einstellungen ändern.

Schritte

1. Führen Sie einen der folgenden Startschritte durch, um die Konfiguration eines externen Schlüsselmanagers zu bearbeiten.

Umfang	Navigation	Startschritt
Externer Schlüsselmanager für den Clusterbereich	**Cluster** > **Einstellungen**	Blättern Sie zum Abschnitt **Sicherheit**. Wählen Sie unter **Verschlüsselung** die Option aus ⋮ Wählen Sie dann **External Key Manager bearbeiten**.
Externer Schlüsselmanager für Storage VM	**Storage** > **Storage VMs**	Wählen Sie die Storage-VM aus. Wählen Sie die Registerkarte **Einstellungen**. Wählen Sie im Abschnitt **Verschlüsselung** unter **Sicherheit** die Option aus ⋮ Wählen Sie dann **External Key Manager bearbeiten**.

2. Vorhandene Schlüsselserver sind in der Tabelle **Schlüsselserver** aufgeführt. Sie können folgende Vorgänge durchführen:
   - Fügen Sie einen neuen Schlüsselserver hinzu, indem Sie auswählen + Add .
   - Löschen Sie einen Schlüsselserver, indem Sie auswählen ⋮ Am Ende der Tabellenzelle, die den Namen des Schlüsselservers enthält. Die sekundären Schlüsselserver, die dem primären Schlüsselserver zugeordnet sind, werden ebenfalls aus der Konfiguration entfernt.

Löschen Sie einen externen Schlüsselmanager

Ein externer Schlüsselmanager kann gelöscht werden, wenn die Volumes unverschlüsselt sind.

Schritte

1. Führen Sie einen der folgenden Schritte aus, um einen externen Schlüsselmanager zu löschen.

Umfang	Navigation	Startschritt
Externer Schlüsselmanager für den Clusterbereich	**Cluster** > **Einstellungen**	Blättern Sie zum Abschnitt **Sicherheit**. Wählen Sie unter **Verschlüsselung** die Option SELECT aus ⋮Wählen Sie dann **External Key Manager löschen**.
Externer Schlüsselmanager für Storage VM	**Storage** > **Storage VMs**	Wählen Sie die Storage-VM aus. Wählen Sie die Registerkarte **Einstellungen**. Wählen Sie im Abschnitt **Verschlüsselung** unter **Sicherheit** die Option aus ⋮Wählen Sie dann **External Key Manager löschen**.

Schlüssel zwischen Schlüsselmanagern migrieren

Wenn mehrere Schlüsselmanager auf einem Cluster aktiviert sind, müssen Schlüssel von einem Schlüsselmanager zu einem anderen migriert werden. Dieser Vorgang wird mit System Manager automatisch abgeschlossen.

- Wenn der Onboard Key Manager oder ein externer Schlüsselmanager auf Cluster-Ebene aktiviert ist und einige Volumes verschlüsselt werden, Wenn Sie dann einen externen Schlüsselmanager auf Ebene der Storage-VM konfigurieren, müssen die Schlüssel vom Onboard Key Manager oder externen Schlüsselmanager auf Cluster-Ebene zum externen Schlüsselmanager auf Ebene der Storage-VM migriert werden. Dieser Prozess wird automatisch durch System Manager abgeschlossen.
- Wenn Volumes ohne Verschlüsselung auf einer Storage-VM erstellt wurden, müssen Schlüssel nicht migriert werden.

Installieren Sie SSL-Zertifikate auf dem Cluster

Das Cluster und der KMIP-Server verwenden KMIP SSL-Zertifikate, um die Identität des jeweils anderen zu überprüfen und eine SSL-Verbindung herzustellen. Vor dem Konfigurieren der SSL-Verbindung mit dem KMIP-Server müssen die KMIP-Client-SSL-Zertifikate für das Cluster und das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle des KMIP-Servers installiert werden.

Über diese Aufgabe

In einem HA-Paar müssen beide Nodes dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden. Wenn Sie mehrere HA-Paare mit demselben KMIP-Server verbinden, müssen alle Nodes der HA-Paare dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden.

Bevor Sie beginnen

- Die Zeit muss auf dem Server synchronisiert werden, der die Zertifikate, den KMIP-Server und das Cluster erstellt.

- Sie müssen das öffentliche SSL KMIP-Client-Zertifikat für den Cluster erhalten haben.
- Sie müssen den privaten Schlüssel für das SSL KMIP Client-Zertifikat für das Cluster erhalten haben.
- Das SSL KMIP-Client-Zertifikat darf nicht durch ein Passwort geschützt sein.
- Sie müssen das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers erhalten haben.
- In einer MetroCluster-Umgebung müssen Sie auf beiden Clustern dieselben KMIP-SSL-Zertifikate installieren.

> Sie können die Client- und Serverzertifikate vor oder nach der Installation der Zertifikate auf dem Cluster auf dem KMIP-Server installieren.

Schritte

1. Installieren Sie die SSL KMIP-Client-Zertifikate für das Cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Sie werden aufgefordert, die öffentlichen und privaten SSL KMIP-Zertifikate einzugeben.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Installieren Sie das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Externes Verschlüsselungsmanagement in ONTAP 9.6 und höher (NVE)

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Ab ONTAP 9.6 haben Sie die Möglichkeit, einen separaten externen Schlüsselmanager zum Sichern der Schlüssel zu konfigurieren, die von der SVM für den Zugriff auf verschlüsselte Daten verwendet werden.

Ab ONTAP 9.11.1 können Sie bis zu 3 sekundäre Schlüsselserver pro primären Schlüsselserver hinzufügen, um einen geclusterten Schlüsselserver zu erstellen. Weitere Informationen finden Sie unter Konfigurieren Sie externe geclusterte Schlüsselserver.

Über diese Aufgabe

Mit einem Cluster oder einer SVM können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Der Umfang des externen Verschlüsselungsmanagement bestimmt, ob wichtige Managementserver alle SVMs im Cluster oder nur ausgewählte SVMs sichern:

- Sie können ein_Cluster Scope_ verwenden, um das externe Verschlüsselungsmanagement für alle SVMs im Cluster zu konfigurieren. Der Clusteradministrator hat Zugriff auf jeden auf den Servern gespeicherten Schlüssel.
- Ab ONTAP 9.6 können Sie mithilfe eines Umfangs *SVM* externes Verschlüsselungsmanagement für eine

Daten-SVM im Cluster konfigurieren. Dies eignet sich am besten für mandantenfähige Umgebungen, in denen jeder Mandant eine andere SVM (oder einen Satz SVMs) zur Bereitstellung von Daten verwendet. Nur der SVM-Administrator für einen bestimmten Mandanten hat Zugriff auf die Schlüssel für den jeweiligen Mandanten.

- Installieren Sie für mandantenfähige Umgebungen eine Lizenz für *MT_EK_MGMT*, indem Sie den folgenden Befehl verwenden:

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

Sie können beide Bereiche im selben Cluster verwenden. Wenn Verschlüsselungsmanagement-Server für eine SVM konfiguriert wurden, verwendet ONTAP nur diese Server zur Sicherung der Schlüssel. Andernfalls sichert ONTAP Schlüssel mit den für den Cluster konfigurierten Verschlüsselungsmanagement-Servern.

Die integrierte Verschlüsselungsmanagement lässt sich für den Cluster-Umfang und das externe Verschlüsselungsmanagement auf der SVM-Ebene konfigurieren. Sie können das verwenden `security key-manager key migrate` Befehl zur Migration von Schlüsseln vom Onboard-Verschlüsselungsmanagement im Cluster-Umfang an externe Schlüsselmanager des Umfangs der SVM

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Wenn Sie externes Verschlüsselungsmanagement für eine MetroCluster Umgebung aktivieren möchten, muss MetroCluster vollständig konfiguriert sein, bevor Sie externes Verschlüsselungsmanagement unterstützen können.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern installieren.

Schritte

1. Konfigurieren Sie die Schlüsselmanager-Konnektivität für das Cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   - Der `security key-manager external enable` Mit dem Befehl wird der ersetzt `security key-manager setup` Befehl. Wenn Sie den Befehl an der Eingabeaufforderung für die Anmeldung beim Cluster ausführen, *`admin_SVM`* Standardmäßig wird der Admin-SVM des aktuellen Clusters festgelegt. Sie müssen der Cluster-Administrator sein, um den Clusterumfang zu konfigurieren. Sie können die ausführen `security key-manager external modify` Befehl zum Ändern der Konfiguration für das externe Verschlüsselungsmanagement.
   - Wenn Sie in einer MetroCluster-Umgebung externes Verschlüsselungsmanagement für den Administrator-SVM konfigurieren, müssen Sie die wiederholen `security key-manager external enable` Befehl auf dem Partner-Cluster.

   Mit dem folgenden Befehl wird die externe Schlüsselverwaltung für aktiviert `cluster1` Mit drei externen Schlüsselservern zu verwenden. Der erste Schlüsselserver wird mit seinem Hostnamen und Port angegeben, der zweite mit einer IP-Adresse und dem Standardport und der dritte mit einer IPv6-Adresse und einem IPv6-Port:

```
clusterl::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Konfiguration eines Schlüsselmanagers einer SVM:

   `security key-manager external enable -vserver SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

   - Wenn Sie den Befehl an der SVM-Anmeldeaufforderung ausführen, `SVM` Standardeinstellung ist die aktuelle SVM. Zum Konfigurieren des SVM-Umfangs müssen Sie ein Cluster oder SVM-Administrator sein. Sie können die ausführen `security key-manager external modify` Befehl zum Ändern der Konfiguration für das externe Verschlüsselungsmanagement.
   - Wenn Sie in einer MetroCluster Umgebung externes Verschlüsselungsmanagement für eine Daten-SVM konfigurieren, müssen Sie die nicht wiederholen `security key-manager external enable` Befehl auf dem Partner-Cluster.

   Mit dem folgenden Befehl wird die externe Schlüsselverwaltung für aktiviert `svm1` Wenn ein Server mit einer einzigen Taste auf dem Standardport 5696 angehört:

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Wiederholen Sie den letzten Schritt für alle weiteren SVMs.

   Sie können auch die verwenden `security key-manager external add-servers` Befehl zum Konfigurieren weiterer SVMs. Der `security key-manager external add-servers` Mit dem Befehl wird der ersetzt `security key-manager add` Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page.

4. Vergewissern Sie sich, dass alle konfigurierten KMIP-Server verbunden sind:

   `security key-manager external show-status -node node_name`

   Der `security key-manager external show-status` Mit dem Befehl wird der ersetzt `security key-manager show -status` Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   ```
   volume encryption conversion start
   ```

   Ein externer Schlüsselmanager muss vollständig konfiguriert sein, bevor Sie die Volumes konvertieren. In einer MetroCluster-Umgebung muss auf beiden Seiten ein externer Schlüsselmanager konfiguriert werden.

Ermöglichen Sie externes Verschlüsselungsmanagement in ONTAP 9.5 und früher

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Mit einem Node können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Über diese Aufgabe

ONTAP konfiguriert die KMIP-Serverkonnektivität für alle Nodes im Cluster.

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern installieren.

Schritte

1. Konfigurieren Sie die Schlüsselmanager-Konnektivität für Cluster-Nodes:

   ```
   security key-manager setup
   ```

   Die Konfiguration des Schlüsselmanagers wird gestartet.

   > In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

2. Geben Sie an jeder Eingabeaufforderung die entsprechende Antwort ein.
3. Hinzufügen eines KMIP-Servers:

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   > In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

4. Fügen Sie aus Redundanzgründen einen zusätzlichen KMIP-Server hinzu:

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   > In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

5. Vergewissern Sie sich, dass alle konfigurierten KMIP-Server verbunden sind:

   ```
   security key-manager show -status
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> security key-manager show -status

   Node             Port      Registered Key Manager  Status
   --------------   ----      -----------------------  ---------------
   cluster1-01      5696      20.1.1.1                available
   cluster1-01      5696      20.1.1.2                available
   cluster1-02      5696      20.1.1.1                available
   cluster1-02      5696      20.1.1.2                available
   ```

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

```
volume encryption conversion start
```

Ein externer Schlüsselmanager muss vollständig konfiguriert sein, bevor Sie die Volumes konvertieren. In einer MetroCluster-Umgebung muss auf beiden Seiten ein externer Schlüsselmanager konfiguriert werden.

Schlüsselmanagement bei einem Cloud-Provider

Ab ONTAP 9.10.1 können Sie dies nutzen "Azure Key Vault (AKV)" Und "Der Verschlüsselungsmanagement-Service (Cloud KMS) der Google Cloud-Plattform" Zum Schutz Ihrer ONTAP-Verschlüsselungen in einer Cloud-gehosteten Applikation. Ab ONTAP 9.12.0 können Sie auch NVE-Schlüssel mit schützen "KMS VON AWS".

AWS KMS, AKV und Cloud KMS können zum Schutz eingesetzt werden "NetApp Volume Encryption (NVE)-Schlüssel" Nur für Data SVMs.

Über diese Aufgabe

Das Verschlüsselungsmanagement mit einem Cloud-Provider kann über die CLI oder die ONTAP REST-API aktiviert werden.

Wenn Sie zum Schutz Ihrer Schlüssel einen Cloud-Provider verwenden, beachten Sie, dass standardmäßig eine Daten-SVM-LIF zur Kommunikation mit dem Cloud-Schlüsselmanagement-Endpunkt verwendet wird. Über ein Node-Managementnetzwerk kommunizieren Sie mit den Authentifizierungsservices des Cloud-Providers (login.microsoftonline.com für Azure, oauth2.googleapis.com für Cloud KMS). Wenn das Cluster-Netzwerk nicht korrekt konfiguriert ist, nutzt das Cluster den Verschlüsselungsmanagementservice nicht ordnungsgemäß.

Wenn Sie einen Cloud-Provider-Managementservice nutzen, sollten Sie sich die folgenden Einschränkungen bewusst sein:

- Das Verschlüsselungsmanagement von Cloud-Providern ist für die NetApp Storage-Verschlüsselung (NSE) und die NetApp Aggregate Encryption (NAE) nicht verfügbar. "Externe KMIPs" Kann stattdessen verwendet werden.
- Das Verschlüsselungsmanagement bei MetroCluster-Konfigurationen ist nicht für Cloud-Provider verfügbar.
- Das Verschlüsselungsmanagement von Cloud-Providern kann nur auf einer Daten-SVM konfiguriert werden.

Bevor Sie beginnen

- Sie müssen den KMS auf dem entsprechenden Cloud-Provider konfiguriert haben.
- Die Nodes des ONTAP Clusters müssen NVE unterstützen.
- "Sie müssen die Lizenzen für Volume Encryption (VE) und Multi-Tenant Encryption Key Management (MTEKM) installiert haben". Diese Lizenzen sind in enthalten "ONTAP One".
- Sie müssen ein Cluster- oder SVM-Administrator sein.
- Die Daten-SVM darf keine verschlüsselten Volumes enthalten oder einen Schlüsselmanager beschäftigen. Wenn die Daten-SVM verschlüsselte Volumes enthält, müssen Sie sie vor der Konfiguration des KMS migrieren.

Externes Verschlüsselungsmanagement

Die Aktivierung des externen Schlüsselmanagements hängt von dem jeweiligen Schlüsselmanager ab, den Sie

verwenden. Wählen Sie die Registerkarte des entsprechenden Schlüsselmanagers und der entsprechenden Umgebung aus.

AWS

Bevor Sie beginnen

- Sie müssen einen Zuschuss für den AWS-KMS-Schlüssel erstellen, der von der IAM-Rolle zum Managen der Verschlüsselung verwendet wird. Die IAM-Rolle muss eine Richtlinie enthalten, die die folgenden Operationen zulässt:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

  Weitere Informationen finden Sie in der AWS-Dokumentation für "Zuschüsse".

Aktivieren Sie AWS KMV auf einer ONTAP SVM

1. Bevor Sie beginnen, erhalten Sie sowohl die Zugriffsschlüssel-ID als auch den geheimen Schlüssel von Ihrem AWS KMS.
2. Legen Sie die Berechtigungsebene auf erweitert fest:
   `set -priv advanced`
3. AWS KMS aktivieren:
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Geben Sie den geheimen Schlüssel ein, wenn Sie dazu aufgefordert werden.
5. Überprüfen Sie, ob der AWS-KMS ordnungsgemäß konfiguriert wurde:
   `security key-manager external aws show -vserver` *`svm_name`*

Azure

Aktivieren Sie Azure Key Vault auf einer ONTAP SVM

1. Bevor Sie beginnen, müssen Sie die entsprechenden Authentifizierungsdaten von Ihrem Azure-Konto beziehen, entweder ein Clientgeheimnis oder ein Zertifikat. Sie müssen außerdem sicherstellen, dass alle Nodes im Cluster sich in einem ordnungsgemäßen Zustand befinden. Sie können dies mit dem Befehl überprüfen `cluster show`.
2. Setzen Sie die privilegierte Stufe auf „Erweiterd“
   `set -priv advanced`
3. Aktivieren Sie AKV auf der SVM
   `security key-manager external azure enable -client-id *client_id* -tenant-id *tenant_id* -name -key-id *key_id* -authentication-method {certificate|client-secret}` Geben Sie bei der entsprechenden Aufforderung entweder das Clientzertifikat oder den Clientschlüssel aus Ihrem Azure-Konto ein.
4. Überprüfen Sie, ob AKV richtig aktiviert ist:
   `security key-manager external azure show vserver` *`svm_name`*
   Wenn die Erreichbarkeit des Service nicht in Ordnung ist, stellen Sie die Verbindung zum AKV Key Management Service über die LIF der Daten-SVM her.

Google Cloud

Aktivieren Sie Cloud-KMS auf einer ONTAP SVM

1. Bevor Sie beginnen, erhalten Sie den privaten Schlüssel für die Google Cloud KMS-Kontoschlüsseldatei in einem JSON-Format. Dieser Punkt ist in Ihrem GCP-Konto enthalten.
   Sie müssen außerdem sicherstellen, dass alle Nodes im Cluster sich in einem ordnungsgemäßen

Zustand befinden. Sie können dies mit dem Befehl überprüfen `cluster show`.

2. Privilegierte Ebene auf erweitert setzen:
   `set -priv advanced`
3. Aktivieren Sie Cloud KMS auf der SVM
   `security key-manager external gcp enable -vserver` *`svm_name`* `-project-id` *`project_id`*`-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*
   Geben Sie bei entsprechender Aufforderung den Inhalt der JSON-Datei mit dem privaten Schlüssel für Dienstkonto ein
4. Vergewissern Sie sich, dass Cloud KMS mit den korrekten Parametern konfiguriert ist:
   `security key-manager external gcp show vserver` *`svm_name`*
   Der Status von `kms_wrapped_key_status` Wird sein "`UNKNOWN`" Wenn keine verschlüsselten Volumes erstellt wurden.
   Wenn die Serviceability nicht in Ordnung ist, stellen Sie die Konnektivität zum GCP-Schlüsselmanagement-Service über die Daten-SVM LIF her.

Wenn bereits ein oder mehrere verschlüsselte Volumes für eine Daten-SVM konfiguriert sind und die entsprechenden NVE Schlüssel vom Onboard-Schlüsselmanager des Admin-SVM gemanagt werden, sollten diese Schlüssel zu dem externen Verschlüsselungsmanagement-Service migriert werden. Führen Sie dazu den Befehl mit der CLI aus:
`security key-manager key migrate -from-Vserver *admin_SVM* -to-Vserver *data_SVM*` Erst dann können neue verschlüsselte Volumes für die Daten-SVM des Mandanten erstellt werden, wenn alle NVE-Schlüssel der Daten-SVM erfolgreich migriert wurden.

Verwandte Informationen

- "Verschlüsseln von Volumes mit NetApp Verschlüsselungslösungen für Cloud Volumes ONTAP"

Integriertes Verschlüsselungsmanagement in ONTAP 9.6 und höher (NVE)

Mit dem integrierten Key Manager werden die Schlüssel gesichert, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie müssen den Onboard Key Manager für jedes Cluster aktivieren, das auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

Sie müssen den ausführen `security key-manager onboard sync` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen.

Wenn Sie über eine MetroCluster-Konfiguration verfügen, müssen Sie den ausführen `security key-manager onboard enable` Führen Sie zunächst den Befehl auf dem lokalen Cluster aus, und führen Sie dann den aus `security key-manager onboard sync` Auf dem Remote-Cluster unter Verwendung derselben Passphrase auf beiden. Wenn Sie den ausführen `security key-manager onboard enable` Vom lokalen Cluster aus und dann auf dem Remote-Cluster synchronisieren, müssen Sie den nicht ausführen `enable` Führen Sie einen neuen Befehl aus dem Remote-Cluster aus.

Standardmäßig müssen Sie beim Neustart eines Node nicht die Passphrase für das Schlüsselmanagement eingeben. Sie können das verwenden `cc-mode-enabled=yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Passphrase eingeben.

Wenn Sie die Einstellung für NVE verwenden `cc-mode-enabled=yes`, Volumen, die Sie mit erstellen

`volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Für `volume create`, Sie müssen nicht angeben `-encrypt true`. Für `volume move start`, Sie müssen nicht angeben `-encrypt-destination true`.

Bei der Konfiguration der Verschlüsselung von ONTAP-Daten im Ruhezustand müssen Sie NSE mit NVE gewährleisten, dass der integrierte Schlüsselmanager im Common Criteria-Modus aktiviert ist, um die Anforderungen für kommerzielle Lösungen für die Klassifizierung (CSfC) zu erfüllen. Siehe "CSfC Lösungsüberblick" Weitere Informationen zu CSfC.

> Wenn der Onboard Key Manager im Common Criteria-Modus aktiviert ist (`cc-mode-enabled=yes`Das Systemverhalten wird folgendermaßen geändert:
>
> - Das System überwacht bei der Verwendung im Common Criteria-Modus auf aufeinanderfolgende fehlgeschlagene Cluster-Passphrase.
>
> Wenn Sie beim Booten nicht die richtige Cluster-Passphrase eingeben, werden verschlüsselte Volumes nicht angehängt. Um dies zu korrigieren, müssen Sie den Node neu booten und die richtige Cluster-Passphrase eingeben. Sobald das System gebootet wurde, können bis zu 5 aufeinanderfolgende Versuche unternommen werden, um für jeden Befehl, für den die Cluster-Passphrase als Parameter erforderlich ist, in einem Zeitraum von 24 Stunden korrekt einzugeben. Wenn das Limit erreicht wird (beispielsweise konnten Sie den Cluster-Passphrase 5 Mal hintereinander nicht korrekt eingeben), müssen Sie entweder warten, bis der 24-Stunden-Timeout abgelaufen ist, oder Sie müssen den Node neu booten, um das Limit zurückzusetzen.
>
> - Updates für das System-Image nutzen das Code-Signing-Zertifikat von NetApp RSA-3072 zusammen mit dem von SHA-384 signierten Code, um die Image-Integrität anstelle des üblichen NetApp RSA-2048-Code-Signaturzertifikats und den von SHA-256 signierten Digests zu überprüfen.
>
> Der Upgrade-Befehl überprüft, ob der Bildinhalt durch Überprüfen verschiedener digitaler Signaturen nicht verändert oder beschädigt wurde. Der Image-Aktualisierungsprozess wird mit dem nächsten Schritt fortgesetzt, wenn die Validierung erfolgreich ist. Andernfalls schlägt die Image-Aktualisierung fehl. Siehe `cluster image` Man-Page für Informationen zu Systemaktualisierungen.

> Der Onboard Key Manager speichert Schlüssel im volatilen Speicher. Der Inhalt von flüchtigem Speicher wird gelöscht, wenn das System neu gestartet oder angehalten wird. Unter normalen Betriebsbedingungen wird der Inhalt von flüchtigem Speicher innerhalb von 30 s gelöscht, wenn ein System angehalten wird.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster-Umgebung konfigurieren, bevor Sie den Onboard Key Manager konfigurieren.

Schritte

1. Starten Sie die Konfiguration des Schlüsselmanagers:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

> Einstellen `cc-mode-enabled=yes` Um zu verlangen, dass Benutzer nach einem Neustart die Kennverwaltung-Passphrase eingeben. Wenn Sie die Einstellung für NVE verwenden `cc-mode-enabled=yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Der `- cc-mode-enabled` Die Option wird in MetroCluster-Konfigurationen nicht unterstützt. Der `security key-manager onboard enable` Mit dem Befehl wird der ersetzt `security key-manager setup` Befehl.

Das folgende Beispiel startet den Befehl zum Einrichten des Schlüsselmanagers in cluster1, ohne dass nach jedem Neustart die Passphrase eingegeben werden muss:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Geben Sie an der Eingabeaufforderung für die Passphrase eine Passphrase zwischen 32 und 256 Zeichen oder für „`cc-Mode`“ eine Passphrase zwischen 64 und 256 Zeichen ein.

> Wenn die angegebene „`cc-Mode`“-Passphrase weniger als 64 Zeichen beträgt, liegt eine Verzögerung von fünf Sekunden vor, bevor die Eingabeaufforderung für das Setup des Schlüsselmanagers die Passphrase erneut anzeigt.

3. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.
4. Vergewissern Sie sich, dass die Authentifizierungsschlüssel erstellt wurden:

```
security key-manager key query -key-type NSE-AK
```

> Der `security key-manager key query` Mit dem Befehl wird der ersetzt `security key-manager query key` Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel wird überprüft, ob Authentifizierungsschlüssel für erstellt wurden `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                Key Type Encryption   Restored

------------------------------------  -------- ------------ --------

node1                                  NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                  NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   `volume encryption conversion start`

   Der Onboard Key Manager muss vor der Konvertierung der Volumes vollständig konfiguriert sein. In einer MetroCluster-Umgebung muss der Onboard Key Manager auf beiden Standorten konfiguriert sein.

Nachdem Sie fertig sind

Kopieren Sie die Passphrase zur späteren Verwendung an einen sicheren Ort außerhalb des Storage-Systems.

Wenn Sie die Onboard Key Manager-Passphrase konfigurieren, sollten Sie die Informationen auch manuell an einem sicheren Ort außerhalb des Speichersystems sichern, um sie bei einem Notfall zu verwenden. Siehe "Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement".

Integriertes Verschlüsselungsmanagement in ONTAP 9.5 und früher (NVE)

Mit dem integrierten Key Manager werden die Schlüssel gesichert, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie müssen Onboard Key Manager für jedes Cluster aktivieren, das auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

Sie müssen den ausführen `security key-manager setup` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen.

Wenn Sie über eine MetroCluster-Konfiguration verfügen, überprüfen Sie diese Richtlinien:

- In ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.
- Vor ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Warten Sie auf dem lokalen Cluster etwa 20 Sekunden, und führen Sie dann den Betrieb aus `security key-manager setup` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.

Standardmäßig müssen Sie beim Neustart eines Node nicht die Passphrase für das Schlüsselmanagement eingeben. Ab ONTAP 9.4 können Sie den verwenden `-enable-cc-mode yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Passphrase eingeben.

Wenn Sie die Einstellung für NVE verwenden `-enable-cc-mode yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Für `volume create`, Sie müssen nicht angeben `-encrypt true`. Für `volume move start`, Sie müssen nicht angeben `-encrypt-destination true`.

> Nach einem fehlgeschlagenen Passphrase-Versuch müssen Sie den Node erneut neu booten.

Bevor Sie beginnen

- Wenn Sie NSE oder NVE mit einem externen KMIP-Server (Key Management) verwenden, müssen Sie die externe Schlüsselmanager-Datenbank gelöscht haben.

  "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster-Umgebung konfigurieren, bevor Sie den Onboard Key Manager konfigurieren.

Schritte

1. Starten Sie die Konfiguration des Schlüsselmanagers:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > Ab ONTAP 9.4 können Sie den verwenden `-enable-cc-mode yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Kennwortphrase für das Schlüsselmanagement eingeben. Wenn Sie die Einstellung für NVE verwenden `-enable-cc-mode yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt.

   Das folgende Beispiel beginnt mit dem Einrichten des Schlüsselmanagers auf Clustered 1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Eingabe `yes` An der Eingabeaufforderung zur Konfiguration des Onboard-Verschlüsselungsmanagement.
3. Geben Sie an der Eingabeaufforderung für die Passphrase eine Passphrase zwischen 32 und 256 Zeichen oder für „`cc-Mode`“ eine Passphrase zwischen 64 und 256 Zeichen ein.

> Wenn die angegebene „`cc-Mode`“-Passphrase weniger als 64 Zeichen beträgt, liegt eine Verzögerung von fünf Sekunden vor, bevor die Eingabeaufforderung für das Setup des Schlüsselmanagers die Passphrase erneut anzeigt.

4. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.
5. Vergewissern Sie sich, dass die Schlüssel für alle Nodes konfiguriert sind:

   `security key-manager key show`

   Die vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   ```
   volume encryption conversion start
   ```

   Der Onboard Key Manager muss vor der Konvertierung der Volumes vollständig konfiguriert sein. In einer MetroCluster-Umgebung muss der Onboard Key Manager auf beiden Standorten konfiguriert sein.

Nachdem Sie fertig sind

Kopieren Sie die Passphrase zur späteren Verwendung an einen sicheren Ort außerhalb des Storage-Systems.

Wenn Sie die Onboard Key Manager-Passphrase konfigurieren, sollten Sie die Informationen auch manuell an einem sicheren Ort außerhalb des Speichersystems sichern, um sie bei einem Notfall zu verwenden. Siehe "Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement".

Integriertes Verschlüsselungsmanagement bei neu hinzugefügten Nodes

Mit dem integrierten Key Manager werden die Schlüssel gesichert, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie müssen Onboard Key Manager für jedes Cluster aktivieren, das auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

> Für ONTAP 9.5 und früher müssen Sie den ausführen `security key-manager setup` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen.
>
> Für ONTAP 9.6 und höher müssen Sie den ausführen `security key-manager sync` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen.
>
> Wenn Sie einem Cluster einen Node hinzufügen, für das das integrierte Verschlüsselungsmanagement konfiguriert ist, führen Sie diesen Befehl aus, um die fehlenden Schlüssel zu aktualisieren.

Wenn Sie über eine MetroCluster-Konfiguration verfügen, überprüfen Sie diese Richtlinien:

- Ab ONTAP 9.6 müssen Sie ausgeführt werden `security key-manager onboard enable` Führen Sie zuerst auf dem lokalen Cluster aus `security key-manager onboard sync` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.
- In ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.
- Vor ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Warten Sie auf dem lokalen Cluster etwa 20 Sekunden, und führen Sie dann den Betrieb aus `security key-manager setup` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.

Standardmäßig müssen Sie beim Neustart eines Node nicht die Passphrase für das Schlüsselmanagement eingeben. Ab ONTAP 9.4 können Sie den verwenden `-enable-cc-mode yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Passphrase eingeben.

Wenn Sie die Einstellung für NVE verwenden `-enable-cc-mode yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Für `volume create`, Sie müssen nicht angeben `-encrypt true`. Für `volume move start`, Sie müssen nicht angeben

`-encrypt-destination true`.

> Nach einem fehlgeschlagenen Passphrase-Versuch müssen Sie den Node erneut neu booten.

Verschlüsseln von Volume-Daten mit NVE

Übersicht über NVE zur Verschlüsselung von Volume-Daten

Ab ONTAP 9.7 ist die Aggregat- und Volume-Verschlüsselung standardmäßig aktiviert, wenn Sie über die VE-Lizenz und die integrierte oder externe Schlüsselverwaltung verfügen. Für ONTAP 9.6 und eine frühere Version können Sie die Verschlüsselung auf einem neuen Volume oder auf einem vorhandenen Volume aktivieren. Bevor Sie die Volume-Verschlüsselung aktivieren können, müssen Sie die VE-Lizenz und die aktivierte Schlüsselverwaltung installiert haben. NVE entspricht FIPS-140-2 Level 1.

Verschlüsselung auf Aggregatebene mit VE-Lizenz aktivieren

Ab ONTAP 9.7 sind neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn sie das haben "VE-Lizenz" Integriertes oder externes Management der Schlüssel Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschlüsselt werden können.

Über diese Aufgabe

Wenn Sie eine Inline- oder eine Hintergrund-Deduplizierung auf Aggregatebene durchführen möchten, muss die Verschlüsselung auf Aggregatebene verwendet werden. Deduplizierung auf Aggregatebene wird ansonsten von NVE nicht unterstützt.

Ein Aggregat, das für die Verschlüsselung auf Aggregatebene aktiviert ist, wird als *NAE Aggregat* (für NetApp Aggregatverschlüsselung) bezeichnet. Alle Volumes in einem NAE-Aggregat müssen mit NAE- oder NVE-Verschlüsselung verschlüsselt sein. Bei der Verschlüsselung auf Aggregatebene werden die im Aggregat erstellten Volumes standardmäßig mit NAE-Verschlüsselung verschlüsselt. Sie können die Standardeinstellung für die Verwendung von NVE-Verschlüsselung überschreiben.

Klartextvolumen werden in NAE-Aggregaten nicht unterstützt.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Aktivieren oder Deaktivieren der Verschlüsselung auf Aggregatebene:

An…	Befehl
Erstellen Sie ein NAE Aggregat mit ONTAP 9.7 oder höher	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*

Erstellen Sie ein NAE-Aggregat mit ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Konvertieren Sie ein nicht-NAE Aggregat in ein NAE Aggregat	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Konvertieren Sie ein NAE Aggregat in ein nicht-NAE Aggregat	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

Der folgende Befehl ermöglicht die Verschlüsselung auf Aggregatebene `aggr1`:

- ONTAP 9.7 oder höher:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 oder früher:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Vergewissern Sie sich, dass das Aggregat für die Verschlüsselung aktiviert ist:

   `storage aggregate show -fields encrypt-with-aggr-key`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Mit dem folgenden Befehl wird das überprüft `aggr1` Für Verschlüsselung aktiviert:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

Nachdem Sie fertig sind

Führen Sie die aus `volume create` Befehl zum Erstellen der verschlüsselten Volumes.

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, sendet ONTAP bei der

Verschlüsselung eines Volumes automatisch „`schiebt`“ einen Verschlüsselungsschlüssel an den Server.

Aktivieren Sie die Verschlüsselung auf einem neuen Volume

Sie können das verwenden `volume create` Befehl zum Aktivieren der Verschlüsselung auf einem neuen Volume.

Über diese Aufgabe

Sie können Volumes mit NetApp Volume Encryption (NVE) und ab ONTAP 9.6 mit NetApp Aggregate Encryption (NAE) verschlüsseln. Weitere Informationen zu NAE und NVE finden Sie im Übersicht über Volume-Verschlüsselung.

Das Verfahren zur Aktivierung der Verschlüsselung auf einem neuen Volume in ONTAP variiert abhängig von der verwendeten ONTAP Version und der spezifischen Konfiguration:

- Beginnend mit ONTAP 9.4, wenn Sie aktivieren `cc-mode` Wenn Sie den Onboard Key Manager einrichten, erstellen Sie die Volumes mit dem `volume create` Der Befehl wird automatisch verschlüsselt, unabhängig davon, ob Sie angegeben haben `-encrypt true`.
- In ONTAP 9.6 und älteren Versionen müssen Sie verwenden `-encrypt true` Mit `volume create` Befehle zur Aktivierung der Verschlüsselung (vorausgesetzt, Sie haben die Verschlüsselung nicht aktiviert `cc-mode`).
- Wenn Sie ein NAE-Volume in ONTAP 9.6 erstellen möchten, müssen Sie NAE auf Aggregatebene aktivieren. Siehe Aktivieren Sie die Verschlüsselung auf Aggregatebene mit der VE-Lizenz Für weitere Details zu dieser Aufgabe.
- Ab ONTAP 9.7 werden neu erstellte Volumes standardmäßig verschlüsselt, wenn Sie über den verfügen "VE-Lizenz" Integriertes oder externes Management der Schlüssel Standardmäßig sind neue Volumes, die in einem NAE-Aggregat erstellt werden, vom Typ NAE anstatt von NVE aus.
  - Fügen Sie ONTAP 9.7 und höher hinzu `-encrypt true` Bis zum `volume create` Befehl zum Erstellen eines Volumes in einem NAE-Aggregat erhält das Volume NVE-Verschlüsselung statt NAE. Alle Volumes in einem NAE-Aggregat müssen entweder mit NVE oder NAE verschlüsselt sein.

> Klartext-Volumes werden in NAE-Aggregaten nicht unterstützt.

Schritte

1. Erstellen Sie ein neues Volume, und geben Sie an, ob die Verschlüsselung auf dem Volume aktiviert ist. Wenn das neue Volume sich in einem NAE-Aggregat befindet, ist das Volume standardmäßig ein NAE-Volume:

Zu erstellen…	Befehl
Ein NAE-Band	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*

Ein NVE Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + In ONTAP 9.6 und früher, wo NAE nicht unterstützt wird, `-encrypt true` Gibt an, dass das Volume mit NVE verschlüsselt werden soll. In ONTAP 9.7 und höher wo Volumes in NAE-Aggregaten erstellt werden, `-encrypt true` Überschreibt stattdessen den Standardverschlüsselungstyp von NAE, um ein NVE Volume zu erstellen.
Nur-Text-Lautstärke	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

Eine vollständige Befehlssyntax finden Sie auf der Befehlsseite für Link:https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html[`volume create`^].

2. Vergewissern Sie sich, dass Volumes für die Verschlüsselung aktiviert sind:

   `volume show -is-encrypted true`

   Eine vollständige Befehlssyntax finden Sie im "Befehlsreferenz".

Ergebnis

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, „sendet“ ONTAP bei der Verschlüsselung eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

=
:allow-uri-read:

Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume

Sie können entweder die verwenden `volume move start` Oder im `volume encryption conversion start` Den Befehl, um die Verschlüsselung auf einem vorhandenen Volume zu aktivieren.

Über diese Aufgabe

- Ab ONTAP 9.3 können Sie den verwenden `volume encryption conversion start` Befehl, um die Verschlüsselung eines vorhandenen Volume „in place“ zu aktivieren, ohne das Volume an einen anderen Speicherort verschieben zu müssen. Alternativ können Sie den verwenden `volume move start` Befehl.
- Bei ONTAP 9.2 und älteren Versionen können Sie nur die verwenden `volume move start` Befehl zum Aktivieren der Verschlüsselung durch Verschieben eines vorhandenen Volumes

Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl zur Konvertierung der Volume-Verschlüsselung

Ab ONTAP 9.3 können Sie den verwenden `volume encryption conversion start` Befehl, um die Verschlüsselung eines vorhandenen Volume „in place“ zu aktivieren, ohne das Volume an einen anderen Speicherort verschieben zu müssen.

Nachdem Sie eine Konvertierung gestartet haben, muss diese abgeschlossen sein. Wenn während des Vorgangs ein Leistungsproblem auftritt, können Sie das ausführen `volume encryption conversion pause` Befehl zum Anhalten des Vorgangs, und `volume encryption conversion resume` Befehl zum Fortsetzen des Vorgangs.

> Verwenden Sie ihn nicht `volume encryption conversion start` Um ein SnapLock Volume zu konvertieren.

Schritte

1. Verschlüsselung auf einem vorhandenen Volume aktivieren:

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

   Die gesamte Befehlssyntax finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl wird die Verschlüsselung für ein vorhandenes Volume aktiviert `vol1`:

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   Das System erstellt einen Verschlüsselungsschlüssel für das Volume. Die Daten auf dem Volume werden verschlüsselt.

2. Überprüfen Sie den Status des Konvertierungsvorgangs:

   `volume encryption conversion show`

   Die gesamte Befehlssyntax finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl wird der Status des Konvertierungsvorgangs angezeigt:

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. Wenn der Konvertierungsvorgang abgeschlossen ist, überprüfen Sie, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Die gesamte Befehlssyntax finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die verschlüsselten Volumes auf angezeigt `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Ergebnis

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, sendet ONTAP bei der Verschlüsselung eines Volumes automatisch „`schiebt`“ einen Verschlüsselungsschlüssel an den Server.

Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl Volume move Start

Sie können das verwenden `volume move start` Befehl zum Aktivieren der Verschlüsselung durch Verschieben eines vorhandenen Volumes Sie müssen verwenden `volume move start` In ONTAP 9.2 und früher. Sie können dasselbe oder ein anderes Aggregat verwenden.

Über diese Aufgabe

- Ab ONTAP 9.8 können Sie dies nutzen `volume move start` Aktivieren der Verschlüsselung auf einem SnapLock oder FlexGroup Volume
- Beginnend mit ONTAP 9.4, wenn Sie beim Einrichten des Onboard Key Managers „`cc-Mode`“ aktivieren, werden die mit dem erstellten Volumes erstellt `volume move start` Befehl wird automatisch verschlüsselt. Sie müssen nicht angeben `-encrypt-destination true`.
- Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschoben werden können. Ein mit einem eindeutigen Schlüssel verschlüsseltes Volume wird als „*NVE Volume*“ bezeichnet (d. h., es verwendet NetApp Volume Encryption). Ein mit einem Aggregatschlüssel verschlüsseltes Volume wird als *NAE Volume* (für NetApp Aggregate Encryption) bezeichnet. Klartext-Volumes werden in NAE-Aggregaten nicht unterstützt.
- Ab ONTAP 9.14.1 können Sie ein SVM Root-Volume mit NVE verschlüsseln. Weitere Informationen finden Sie unter Konfiguration der NetApp-Volume-Verschlüsselung auf einem SVM-Root-Volume.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe durchzuführen, oder ein SVM-Administrator, an den der Cluster-Administrator die Berechtigungen delegiert hat.

"Delegieren von Berechtigungen zum Ausführen des Befehls zum Verschieben von Volumes"

Schritte

1. Verschieben Sie ein vorhandenes Volume und geben Sie an, ob die Verschlüsselung auf dem Volume aktiviert ist:

Konvertieren…	Befehl
Ein Klartext-Volume auf ein NVE Volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`

Ein NVE oder Klartext Volume auf ein NAE Volume (vorausgesetzt, die Verschlüsselung auf Aggregatebene ist auf dem Zielsystem aktiviert)	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`
Ein NAE-Volume auf ein NVE Volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
Ein NAE-Volumen zu einem Klartext-Volumen	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
Ein NVE Volume auf ein Klartext-Volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

Die gesamte Befehlssyntax finden Sie auf der man-Page für den Befehl.

Mit dem folgenden Befehl wird ein Klartext-Volume mit dem Namen konvertiert `vol1` Zu einem NVE Volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Wenn die Verschlüsselung auf Aggregatebene auf dem Zielsystem aktiviert ist, wird mit dem folgenden Befehl ein NVE oder ein Klartext Volume mit dem Namen konvertiert `vol1` Zu einem NAE-Band:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

Mit dem folgenden Befehl wird ein NAE-Volume mit dem Namen konvertiert `vol2` Zu einem NVE Volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

Mit dem folgenden Befehl wird ein NAE-Volume mit dem Namen konvertiert `vol2` Zu einem Klartext-Volumen:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

Mit dem folgenden Befehl wird ein NVE-Volume mit dem Namen konvertiert `vol2` Zu einem Klartext-Volumen:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. Zeigen Sie den Verschlüsselungstyp von Cluster Volumes an:

   `volume show -fields encryption-type none|volume|aggregate`

   Der `encryption-type` Field steht in ONTAP 9.6 und höher zur Verfügung.

   Die gesamte Befehlssyntax finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl wird der Verschlüsselungstyp von Volumes in angezeigt `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Vergewissern Sie sich, dass Volumes für die Verschlüsselung aktiviert sind:

   `volume show -is-encrypted true`

   Die gesamte Befehlssyntax finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die verschlüsselten Volumes auf angezeigt `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Ergebnis

Wenn Sie einen KMIP-Server zur Speicherung der Verschlüsselungsschlüssel für einen Node verwenden, überträgt ONTAP bei der Verschlüsselung eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

Konfiguration der NetApp-Volume-Verschlüsselung auf einem SVM-Root-Volume

Ab ONTAP 9.14.1 können Sie die NetApp Volume Encryption (NVE) auf einem Storage

VM (SVM) Root-Volume aktivieren. Mit NVE wird das Root-Volume mit einem eindeutigen Schlüssel verschlüsselt, was für mehr Sicherheit auf der SVM sorgt.

Über diese Aufgabe

NVE auf einem SVM-Root-Volume kann nur aktiviert werden, nachdem die SVM erstellt wurde.

Bevor Sie beginnen

- Das SVM-Root-Volume darf sich nicht auf einem mit der NetApp-Aggregatverschlüsselung (NAE) verschlüsselten Aggregat befinden.
- Sie müssen die Verschlüsselung mit dem Onboard Key Manager oder einem externen Schlüsselmanager aktiviert haben.
- Sie müssen ONTAP 9.14.1 oder höher ausführen.
- Um eine SVM, die ein mit NVE verschlüsseltes Root-Volume enthält, zu migrieren, müssen Sie das SVM-Root-Volume nach Abschluss der Migration in ein Klartextvolume konvertieren und anschließend das SVM-Root-Volume neu verschlüsseln.
  - Wenn das Zielaggregat der SVM Migration NAE verwendet, übernimmt das Root-Volume standardmäßig NAE.
- Wenn sich die SVM in einer SVM-Disaster-Recovery-Beziehung befindet:
  - Verschlüsselungseinstellungen auf einer gespiegelten SVM werden nicht an das Ziel kopiert. Wenn Sie NVE auf dem Quell- oder Zielsystem aktivieren, müssen Sie NVE auf dem gespiegelten SVM Root-Volume separat aktivieren.
  - Wenn alle Aggregate im Ziel-Cluster NAE verwenden, verwendet das SVM Root-Volume NAE.

Schritte

Sie können NVE auf einem SVM Root-Volume mit der ONTAP CLI oder mit System Manager aktivieren.

CLI

Sie können NVE auf dem Root-Volume der SVM aktivieren oder das Volume zwischen den Aggregaten verschieben.

Verschlüsseln Sie das Root-Volume

1. Konvertieren Sie das Root-Volume in ein verschlüsseltes Volume:

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. Bestätigen Sie, dass die Verschlüsselung erfolgreich war. Der `volume show -encryption-type volume` Zeigt eine Liste aller Volumes mit NVE an.

Verschlüsseln Sie das SVM-Root-Volume durch Verschieben

1. Volume-Verschiebung initiieren:

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   Finden Sie weitere Informationen zu `volume move`, Siehe Verschieben Sie ein Volume.

2. Bestätigen Sie das `volume move` Vorgang erfolgreich mit dem ausgeführt `volume move show` Befehl. Der `volume show -encryption-type volume` Zeigt eine Liste aller Volumes mit NVE an.

System Manager

1. Navigieren Sie zu **Storage** > **Volumes**.
2. Wählen Sie neben dem Namen des SVM-Root-Volumes, das Sie verschlüsseln möchten, die Option aus ⋮ Dann **Bearbeiten**.
3. Wählen Sie unter der Überschrift **Speicherung und Optimierung** die Option **Verschlüsselung aktivieren**.
4. Wählen Sie **Speichern**.

Node-Root-Volume-Verschlüsselung aktivieren

Ab ONTAP 9.8 können Sie NetApp Volume Encryption zum Schutz des Root-Volumes des Nodes verwenden.

> **Über diese Aufgabe**
>
> Dieses Verfahren gilt für das Root-Volume des Nodes. Sie gilt nicht für SVM-Root-Volumes. Root-Volumes von SVM können durch Verschlüsselung auf Aggregatebene geschützt werden, Ab ONTAP 9.14.1 ist NVE der Fall.

Sobald die Verschlüsselung des Root-Volumes beginnt, muss sie abgeschlossen sein. Sie können den Vorgang nicht unterbrechen. Nach Abschluss der Verschlüsselung können Sie dem Root-Volume keinen neuen Schlüssel zuweisen und keine sichere Löschung durchführen.

Bevor Sie beginnen

- Ihr System muss eine HA-Konfiguration verwenden.

- Das Root-Volume des Nodes muss bereits erstellt werden.
- Ihr System muss über einen integrierten Schlüsselmanager oder einen externen Verschlüsselungsmanagement-Server mit dem Key Management Interoperability Protocol (KMIP) verfügen.

Schritte

1. Verschlüsseln Sie das Root-Volume:

   `volume encryption conversion start -vserver` *`SVM_name`* `-volume` *`root_vol_name`*

2. Überprüfen Sie den Status des Konvertierungsvorgangs:

   `volume encryption conversion show`

3. Nach Abschluss des Konvertierungsvorgangs muss überprüft werden, ob das Volume verschlüsselt ist:

   `volume show -fields`

   Das folgende zeigt eine Beispielausgabe für ein verschlüsseltes Volume.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

Konfigurieren Sie die hardwarebasierte NetApp Verschlüsselung

Konfiguration der hardwarebasierten NetApp Verschlüsselung – Übersicht

Die hardwarebasierte Verschlüsselung von NetApp unterstützt die vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) von Daten beim Schreiben. Ohne einen auf der Firmware gespeicherten Verschlüsselungsschlüssel können die Daten nicht gelesen werden. Der Verschlüsselungsschlüssel wiederum ist nur für einen authentifizierten Knoten zugänglich.

Allgemeines zur hardwarebasierten Verschlüsselung von NetApp

Ein Node authentifiziert sich selbst auf einem Self-Encrypting Drive, wobei ein Authentifizierungsschlüssel von einem externen Verschlüsselungsmanagement-Server oder Onboard Key Manager abgerufen wird:

- Der externe Verschlüsselungsmanagement-Server ist ein Drittanbietersystem in der Storage-Umgebung, das mithilfe des Key Management Interoperability Protocol (KMIP) Schlüssel zu Nodes bereitstellt. Als Best Practice wird empfohlen, externe Verschlüsselungsmanagementserver auf einem anderen Storage-System zu Ihren Daten zu konfigurieren.
- Der integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt.

Mit NetApp Volume Encryption mit hardwarebasierter Verschlüsselung können Daten auf Self-Encrypting Drives `double Encryption` verschlüsselt werden.

Bei Aktivierung von Self-Encrypting Drives wird der Core Dump ebenfalls verschlüsselt.

> Wenn ein HA-Paar SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verwendet, müssen Sie die Anweisungen im Thema befolgen Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren Für alle Laufwerke innerhalb des HA-Paars vor der Initialisierung des Systems (Boot-Optionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Unterstützte Self-Encrypting Drives

Es werden zwei Arten von Self-Encrypting Drives unterstützt:

- FIPS-zertifizierte Self-Encrypting-SAS- oder NVMe-Laufwerke werden auf allen FAS und AFF Systemen unterstützt. Diese Laufwerke, so genannte *FIPS-Laufwerke*, entsprechen den Anforderungen der Federal Information Processing Standard Publication 140-2, Level 2. Die zertifizierten Funktionen ermöglichen neben der Verschlüsselung auch Schutz, beispielsweise die Verhinderung von Denial-of-Service-Angriffen auf dem Laufwerk. FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.
- Ab ONTAP 9.6 werden Self-Encrypting-NVMe-Laufwerke, die noch keine FIPS-Tests durchlaufen haben, auf AFF A800, A320 und neueren Systemen unterstützt. Diese Laufwerke, sogenannte *SEDs*, bieten dieselben Verschlüsselungsfunktionen wie FIPS-Laufwerke, können aber ohne Verschlüsselung von Laufwerken auf demselben Node oder HA-Paar kombiniert werden.
- Alle FIPS-validierten Laufwerke verwenden ein kryptografisches Firmware-Modul, das durch die FIPS-Validierung erfolgt. Das FIPS-Laufwerk-kryptografische Modul verwendet keine Schlüssel, die außerhalb des Laufwerks generiert werden (die Authentifizierungs-Passphrase, die an das Laufwerk eingegeben wird, wird vom Laufwerk-Firmware-kryptographic-Modul verwendet, um einen Schlüssel zu erhalten).

> Laufwerke ohne Verschlüsselung sind Laufwerke, die keine SEDs oder FIPS-Laufwerke sind.

> Wenn Sie NSE in einem System mit einem Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten im Flash Cache Modul.

Wann Sie externes Verschlüsselungsmanagement verwenden sollten

Obwohl es kostengünstiger und in der Regel bequemer ist, den Onboard-Schlüsselmanager zu verwenden, sollten Sie ein externes Verschlüsselungsmanagement nutzen, wenn eine der folgenden zutrifft:

- Die Richtlinie Ihres Unternehmens erfordert eine Verschlüsselungsmanagementlösung, die ein kryptografisches Modul nach FIPS 140-2 Level 2 (oder höher) verwendet.
- Sie benötigen eine Multi-Cluster-Lösung mit zentralem Management von Verschlüsselungen.
- Ihr Unternehmen erfordert die zusätzliche Sicherheit beim Speichern von Authentifizierungsschlüsseln auf einem System oder an einem anderen Speicherort als den Daten.

Support-Details

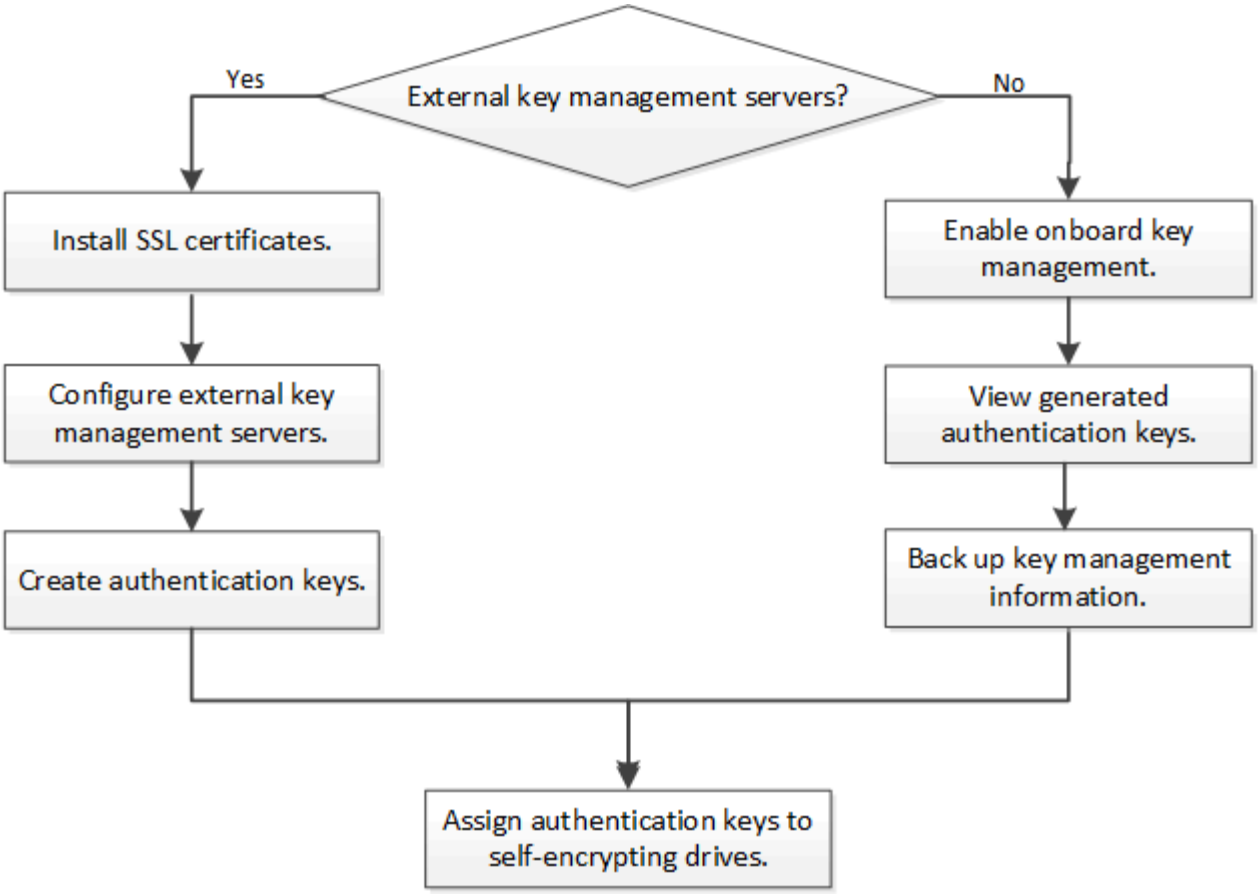
In der folgenden Tabelle sind wichtige Details zur Unterstützung der Hardwareverschlüsselung aufgeführt. In der Interoperabilitäts-Matrix finden Sie die neuesten Informationen zu unterstützten KMIP-Servern, Storage-Systemen und Festplatten-Shelfs.

Ressource oder Funktion	Support-Details

Nicht homogene Festplattengruppen	• FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. Die Einhaltung der HA-Paare kann bei nicht übereinstimmenden HA-Paaren im selben Cluster vorhanden sein. • SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.
Laufwerkstyp	• FIPS-Laufwerke können SAS- oder NVMe-Laufwerke sein. • SEDs müssen NVMe-Laufwerke sein.
10-GB-Netzwerkschnittstellen	Ab ONTAP 9.3 unterstützen die KMIP-Verschlüsselungsmanagementkonfigurationen 10 GB-Netzwerkschnittstellen für die Kommunikation mit externen Verschlüsselungsmanagement-Servern.
Ports für die Kommunikation mit dem Schlüsselverwaltungsserver	Ab ONTAP 9.3 können Sie jeden beliebigen Storage Controller Port zur Kommunikation mit dem Schlüsselmanagement-Server verwenden. Andernfalls sollten Sie Port E0M für die Kommunikation mit Schlüsselmanagement-Servern verwenden. Je nach Storage-Controller-Modell sind während des Bootvorgangs möglicherweise bestimmte Netzwerkschnittstellen zur Kommunikation mit wichtigen Management-Servern nicht verfügbar.
MetroCluster (MCC)	• NVMe-Laufwerke unterstützen MCC. • SAS-Laufwerke unterstützen MCC nicht.

Hardwarebasierter Verschlüsselungs-Workflow

Sie müssen Verschlüsselungsmanagementdienste konfigurieren, bevor sich das Cluster auf dem Self-Encrypting Drive authentifizieren kann. Sie können einen externen Verschlüsselungsmanagementserver oder einen integrierten Schlüsselmanager verwenden.



Verwandte Informationen

- "NetApp Hardware Universe"
- "NetApp Volume Encryption und NetApp Aggregate Encryption"

Externes Verschlüsselungsmanagement konfigurieren

Externes Verschlüsselungsmanagement – Übersicht konfigurieren

Sie können einen oder mehrere externe Verschlüsselungsmanagementserver verwenden, um die Schlüssel zu sichern, die das Cluster zum Zugriff auf verschlüsselte Daten verwendet. Ein externer Verschlüsselungsmanagement-Server ist ein Drittanbietersystem in Ihrer Storage-Umgebung, der mithilfe des Key Management Interoperability Protocol (KMIP) Schlüssel zu Nodes bereitstellt.

Bei ONTAP 9.1 und älteren Versionen müssen Node-Management-LIFs Ports zugewiesen werden, die mit der Node-Managementrolle konfiguriert sind, bevor Sie den externen Schlüsselmanager verwenden können.

NetApp Volume Encryption (NVE) kann mit Onboard Key Manager in ONTAP 9.1 und höher implementiert werden. NVE kann in ONTAP 9.3 oder höher mit externem Verschlüsselungsmanagement (KMIP) und Onboard Key Manager implementiert werden. Ab ONTAP 9.11.1 können Sie mehrere externe Schlüsselmanager in einem Cluster konfigurieren. Siehe Konfigurieren Sie Cluster-Key-Server.

Erfassen Sie Netzwerkinformationen in ONTAP 9.2 und früher

Wenn Sie ONTAP 9.2 oder eine frühere Version verwenden, sollten Sie das Arbeitsblatt

zur Netzwerkkonfiguration ausfüllen, bevor Sie die externe Schlüsselverwaltung aktivieren.

Ab ONTAP 9.3 erkennt das System automatisch alle benötigten Netzwerkinformationen.

Element	Hinweise	Wert
Name der Key-Management-Netzwerkschnittstelle		
IP-Adresse für die wichtige Management-Netzwerkschnittstelle	IP-Adresse der LIF für das Node-Management im IPv4- oder IPv6-Format	
Key-Management-Netzwerkschnittstelle IPv6-Netzwerk-Präfixlänge	Wenn Sie IPv6 verwenden, Länge des IPv6-Netzwerkpräfixes	
Subnetzmaske für das Schlüsselmanagement-Netzwerk-Interface		
Gateway-IP-Adresse für die wichtige Management-Netzwerkschnittstelle		
IPv6-Adresse für die Cluster-Netzwerkschnittstelle	Nur erforderlich, wenn Sie IPv6 für die Netzwerkschnittstelle des Verschlüsselungsmanagements verwenden	
Port-Nummer für jeden KMIP-Server	Optional Die Portnummer muss für alle KMIP-Server identisch sein. Wenn Sie keine Portnummer angeben, wird standardmäßig der Port 5696 verwendet. Dies ist der für KMIP zugewiesene Port (Internet Assigned Numbers Authority, IANA).	
Tag-Schlüsselname	Optional Der Key-Tag-Name wird verwendet, um alle Schlüssel zu einem Knoten zu identifizieren. Der Standardname für das Tag der Schlüssel ist der Node-Name.	

Verwandte Informationen

"Technischer Bericht 3954 von NetApp: Vorherige Installation der NetApp Storage Encryption Anforderungen und Verfahren für IBM Tivoli Lifetime Key Manager"

"Technischer Bericht 4074 von NetApp: Vorabinstallation der Anforderungen und Verfahren für SafeNet KeySecure"

Installieren Sie SSL-Zertifikate auf dem Cluster

Das Cluster und der KMIP-Server verwenden KMIP SSL-Zertifikate, um die Identität des jeweils anderen zu überprüfen und eine SSL-Verbindung herzustellen. Vor dem Konfigurieren der SSL-Verbindung mit dem KMIP-Server müssen die KMIP-Client-SSL-Zertifikate für das Cluster und das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle des KMIP-Servers installiert werden.

Über diese Aufgabe

In einem HA-Paar müssen beide Nodes dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden. Wenn Sie mehrere HA-Paare mit demselben KMIP-Server verbinden, müssen alle Nodes der HA-Paare dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden.

Bevor Sie beginnen

- Die Zeit muss auf dem Server synchronisiert werden, der die Zertifikate, den KMIP-Server und das Cluster erstellt.
- Sie müssen das öffentliche SSL KMIP-Client-Zertifikat für den Cluster erhalten haben.
- Sie müssen den privaten Schlüssel für das SSL KMIP Client-Zertifikat für das Cluster erhalten haben.
- Das SSL KMIP-Client-Zertifikat darf nicht durch ein Passwort geschützt sein.
- Sie müssen das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers erhalten haben.
- In einer MetroCluster-Umgebung müssen Sie auf beiden Clustern dieselben KMIP-SSL-Zertifikate installieren.

> Sie können die Client- und Serverzertifikate vor oder nach der Installation der Zertifikate auf dem Cluster auf dem KMIP-Server installieren.

Schritte

1. Installieren Sie die SSL KMIP-Client-Zertifikate für das Cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Sie werden aufgefordert, die öffentlichen und privaten SSL KMIP-Zertifikate einzugeben.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Installieren Sie das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Externes Verschlüsselungsmanagement in ONTAP 9.6 und höher (HW-basiert)

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Mit einem Node können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Ab ONTAP 9.11.1 können Sie pro Primärschlüsselserver bis zu 3 sekundäre Schlüsselserver hinzufügen, um einen geclusterten Schlüsselserver zu erstellen. Weitere Informationen finden Sie unter Konfigurieren Sie externe geclusterte Schlüsselserver.

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern installieren.

Schritte

1. Konfigurieren Sie die Schlüsselmanager-Konnektivität für das Cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > - Der `security key-manager external enable` Mit dem Befehl wird der ersetzt `security key-manager setup` Befehl. Sie können die ausführen `security key-manager external modify` Befehl zum Ändern der Konfiguration für das externe Verschlüsselungsmanagement. Eine vollständige Befehlssyntax finden Sie in den man-Pages.
   > - Wenn Sie in einer MetroCluster-Umgebung externes Verschlüsselungsmanagement für den Administrator-SVM konfigurieren, müssen Sie die wiederholen `security key-manager external enable` Befehl auf dem Partner-Cluster.

   Mit dem folgenden Befehl wird die externe Schlüsselverwaltung für aktiviert `cluster1` Mit drei externen Schlüsselservern zu verwenden. Der erste Schlüsselserver wird mit seinem Hostnamen und Port angegeben, der zweite mit einer IP-Adresse und dem Standardport und der dritte mit einer IPv6-Adresse und einem IPv6-Port:

   ```
   clusterl::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. Vergewissern Sie sich, dass alle konfigurierten KMIP-Server verbunden sind:

   ```
   security key-manager external show-status -node node_name -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

   > Der `security key-manager external show-status` Mit dem Befehl wird der ersetzt `security key-manager show -status` Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

Ermöglichen Sie externes Verschlüsselungsmanagement in ONTAP 9.5 und früher

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Mit einem Node können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Über diese Aufgabe

ONTAP konfiguriert die KMIP-Serverkonnektivität für alle Nodes im Cluster.

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern installieren.

Schritte

1. Konfigurieren Sie die Schlüsselmanager-Konnektivität für Cluster-Nodes:

   ```
   security key-manager setup
   ```

   Die Konfiguration des Schlüsselmanagers wird gestartet.

   > In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

2. Geben Sie an jeder Eingabeaufforderung die entsprechende Antwort ein.

3. Hinzufügen eines KMIP-Servers:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.1
   ```

   In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

4. Fügen Sie aus Redundanzgründen einen zusätzlichen KMIP-Server hinzu:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

   In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

5. Vergewissern Sie sich, dass alle konfigurierten KMIP-Server verbunden sind:

   `security key-manager show -status`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> security key-manager show -status

   Node            Port      Registered Key Manager  Status
   --------------  ----      -----------------------  ---------------
   cluster1-01     5696      20.1.1.1                available
   cluster1-01     5696      20.1.1.2                available
   cluster1-02     5696      20.1.1.1                available
   cluster1-02     5696      20.1.1.2                available
   ```

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   `volume encryption conversion start`

   Ein externer Schlüsselmanager muss vollständig konfiguriert sein, bevor Sie die Volumes konvertieren. In einer MetroCluster-Umgebung muss auf beiden Seiten ein externer Schlüsselmanager konfiguriert werden.

Konfigurieren Sie externe geclusterte Schlüsselserver

Ab ONTAP 9.11.1 können Sie die Konnektivität mit externen Verschlüsselungsmanagement-Servern auf einer SVM konfigurieren. Mit geclusterten Key Servern können Sie primäre und sekundäre Schlüsselserver auf einer SVM

zuweisen. Bei der Registrierung von Schlüsseln versucht ONTAP zuerst, auf einen primären Schlüsselserver zuzugreifen, bevor nacheinander versucht wird, auf sekundäre Server zuzugreifen, bis der Vorgang erfolgreich abgeschlossen ist. Dadurch wird die Duplizierung von Schlüsseln verhindert.

Externe Schlüsselserver können für NSE-, NVE-, NAE- und SED-Schlüssel verwendet werden. Eine SVM kann bis zu vier primäre externe KMIP-Server unterstützen. Jeder primäre Server kann bis zu drei sekundäre Schlüsselserver unterstützen.

Bevor Sie beginnen

- "KMIP-Verschlüsselungsmanagement muss für die SVM aktiviert sein".
- Dieser Prozess unterstützt nur wichtige Server, die KMIP verwenden. Eine Liste der unterstützten Schlüsselserver finden Sie in "NetApp Interoperabilitäts-Matrix-Tool".
- Alle Nodes im Cluster müssen ONTAP 9.11.1 oder höher ausführen.
- In der Reihenfolge der Server sind die Argumente im aufgelistet `-secondary-key-servers` Der Parameter gibt die Zugriffsreihenfolge der KMIP-Server (External Key Management) wieder.

Erstellen Sie einen Cluster-Schlüsselserver

Das Konfigurationsverfahren hängt davon ab, ob Sie einen primären Schlüsselserver konfiguriert haben oder nicht.

Hinzufügen von primären und sekundären Schlüsselservern zu einer SVM

1. Vergewissern Sie sich, dass für das Cluster kein Verschlüsselungsmanagement aktiviert wurde:
   `security key-manager external show -vserver` *`svm_name`*
   Wenn für die SVM bereits maximal vier primäre Schlüsselserver aktiviert sind, müssen Sie einen der vorhandenen primären Schlüsselserver entfernen, bevor Sie einen neuen hinzufügen.
2. Aktivieren Sie den primären Schlüsselmanager:
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Ändern Sie den primären Schlüsselserver, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` Der Parameter akzeptiert eine kommagetrennte Liste mit bis zu drei Schlüsselservern.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

Fügen Sie einem vorhandenen primären Schlüsselserver sekundäre Schlüsselserver hinzu

1. Ändern Sie den primären Schlüsselserver, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` Der Parameter akzeptiert eine kommagetrennte Liste mit bis zu drei Schlüsselservern.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   Weitere Informationen zu sekundären Schlüsselservern finden Sie unter [mod-secondary].

Cluster-Key-Server ändern

Sie können externe Schlüsselserver-Cluster ändern, indem Sie den Status (primäre oder sekundäre) bestimmter Schlüsselserver ändern, sekundäre Schlüsselserver hinzufügen und entfernen oder die Zugriffsreihenfolge von sekundären Schlüsselservern ändern.

Konvertieren Sie primäre und sekundäre Schlüsselserver

Um einen primären Schlüsselserver in einen sekundären Schlüsselserver zu konvertieren, müssen Sie ihn zuerst mit der von der SVM entfernen `security key-manager external remove-servers` Befehl.

Um einen sekundären Schlüsselserver in einen primären Schlüsselserver zu konvertieren, müssen Sie zuerst den sekundären Schlüsselserver vom vorhandenen primären Schlüsselserver entfernen. Siehe [mod-secondary]. Wenn Sie einen sekundären Schlüsselserver beim Entfernen eines vorhandenen Schlüssels in einen primären Server konvertieren, kann der Versuch, einen neuen Server hinzuzufügen, bevor Sie den Schlüssel entfernen und konvertieren, zu einer doppelten Tastenanfügung führen.

Ändern Sie sekundäre Schlüsselserver

Sekundäre Schlüsselserver werden mit dem verwaltet `-secondary-key-servers` Parameter von `security key-manager external modify-server` Befehl. Der `-secondary-key-servers` Parameter akzeptiert eine kommagetrennte Liste. Die angegebene Reihenfolge der sekundären Schlüsselserver in der Liste bestimmt die Zugriffssequenz für die sekundären Schlüsselserver. Die Zugriffsreihenfolge kann durch Ausführen des Befehls geändert werden `security key-manager external modify-server` Bei der Eingabe der sekundären Schlüssel-Server in einer anderen Reihenfolge.

Um einen sekundären Schlüsselserver zu entfernen, wird der verwendet `-secondary-key-servers` Argumente sollten die wichtigsten Server enthalten, die Sie beibehalten möchten, während Sie die zu entfernenden nicht zulassen. Um alle sekundären Schlüsselserver zu entfernen, verwenden Sie das Argument `-`, Keine zu deuten.

Weitere Informationen finden Sie im `security key-manager external` Auf der "Befehlsreferenz für ONTAP".

Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.6 und höher

Sie können das verwenden `security key-manager key create` Befehl zum Erstellen der Authentifizierungsschlüssel für einen Node und Speichern auf den konfigurierten KMIP-Servern.

Über diese Aufgabe

Wenn Sie in Ihrer Sicherheitseinrichtung unterschiedliche Schlüssel für die Datenauthentifizierung und die FIPS 140-2-Authentifizierung verwenden müssen, sollten Sie jeweils einen separaten Schlüssel erstellen. Ist dies nicht der Fall, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden wie für den Datenzugriff.

ONTAP erstellt Authentifizierungsschlüssel für alle Nodes im Cluster.

- Dieser Befehl wird nicht unterstützt, wenn Onboard Key Manager aktiviert ist. Es werden jedoch automatisch zwei Authentifizierungsschlüssel erstellt, wenn der Onboard Key Manager aktiviert ist. Die Tasten können mit dem folgenden Befehl angezeigt werden:

  ```
  security key-manager key query -key-type NSE-AK
  ```

- Sie erhalten eine Warnung, wenn auf den konfigurierten Schlüsselverwaltungsservern bereits mehr als 128 Authentifizierungsschlüssel gespeichert werden.
- Sie können das verwenden `security key-manager key delete` Befehl zum Löschen von nicht verwendeten Schlüsseln. Der `security key-manager key delete` Befehl schlägt fehl, wenn der angegebene Schlüssel derzeit von ONTAP verwendet wird. (Sie müssen über mehr als „`admin`“ verfügen, um diesen Befehl verwenden zu können.)

> Bevor Sie einen Schlüssel in einer MetroCluster-Umgebung löschen, müssen Sie sicherstellen, dass der Schlüssel nicht im Partner-Cluster verwendet wird. Sie können auf dem Partner-Cluster folgende Befehle verwenden, um zu überprüfen, ob der Schlüssel nicht verwendet wird:
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Authentifizierungsschlüssel für Cluster-Nodes erstellen:

   ```
   security key-manager key create -key-tag passphrase_label -prompt-for-key
   true|false
   ```

   > Einstellung `prompt-for-key=true` Bewirkt, dass das System den Cluster-Administrator zur Verwendung der Passphrase bei der Authentifizierung verschlüsselter Laufwerke auffordert. Andernfalls generiert das System automatisch eine 32-Byte-Passphrase. Der `security key-manager key create` Mit dem Befehl wird der ersetzt `security key-manager create-key` Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Authentifizierungsschlüssel für erstellt `cluster1`, Automatisch eine 32-Byte-Passphrase generieren:

   ```
   cluster1::> security key-manager key create
   Key ID:
   00000000000000000200000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

2. Vergewissern Sie sich, dass die Authentifizierungsschlüssel erstellt wurden:

   ```
   security key-manager key query -node node
   ```

   > Der `security key-manager key query` Mit dem Befehl wird der ersetzt `security key-manager query key` Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page. Die in der Ausgabe angezeigte Schlüssel-ID ist eine Kennung, die auf den Authentifizierungsschlüssel verweist. Es handelt sich nicht um den tatsächlichen Authentifizierungsschlüssel oder den Datenverschlüsselung.

Im folgenden Beispiel wird überprüft, ob Authentifizierungsschlüssel für erstellt wurden `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
0000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.5 und früher

Sie können das verwenden `security key-manager create-key` Befehl zum Erstellen der Authentifizierungsschlüssel für einen Node und Speichern auf den konfigurierten KMIP-Servern.

Über diese Aufgabe

Wenn Sie in Ihrer Sicherheitseinrichtung unterschiedliche Schlüssel für die Datenauthentifizierung und die FIPS 140-2-Authentifizierung verwenden müssen, sollten Sie jeweils einen separaten Schlüssel erstellen. Falls dies nicht der Fall ist, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden, den Sie für den Datenzugriff verwenden.

ONTAP erstellt Authentifizierungsschlüssel für alle Nodes im Cluster.

- Dieser Befehl wird nicht unterstützt, wenn das integrierte Verschlüsselungsmanagement aktiviert ist.
- Sie erhalten eine Warnung, wenn auf den konfigurierten Schlüsselverwaltungsservern bereits mehr als 128 Authentifizierungsschlüssel gespeichert werden.

  Sie können die Verschlüsselungsmanagement-Server-Software verwenden, um alle nicht verwendeten Schlüssel zu löschen, und führen den Befehl erneut aus.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Authentifizierungsschlüssel für Cluster-Nodes erstellen:

   `security key-manager create-key`

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   > Die in der Ausgabe angezeigte Schlüssel-ID ist eine Kennung, die auf den Authentifizierungsschlüssel verweist. Es handelt sich nicht um den tatsächlichen Authentifizierungsschlüssel oder den Datenverschlüsselung.

   Im folgenden Beispiel werden die Authentifizierungsschlüssel für erstellt `cluster1`:

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. Vergewissern Sie sich, dass die Authentifizierungsschlüssel erstellt wurden:

   `security key-manager query`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird überprüft, ob Authentifizierungsschlüssel für erstellt wurden `cluster1`:

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED (External Key Management)

Sie können das verwenden `storage encryption disk modify` Befehl zum Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED. Clusterknoten verwenden diesen Schlüssel zum Sperren oder Entsperren verschlüsselter Daten auf dem Laufwerk.

Über diese Aufgabe

Ein selbstverschlüsselndes Laufwerk ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen nicht standardmäßigen Wert eingestellt ist. Der Hersteller Secure ID (MSID), der die Schlüssel-ID 0x0 hat, ist der Standardvorgabewert für SAS-Laufwerke. Bei NVMe-Laufwerken ist der Standardwert ein Null-Schlüssel, der als leere Schlüssel-ID dargestellt wird. Wenn Sie einem selbstverschlüsselnden Laufwerk die Schlüssel-ID zuweisen, ändert das System seine Authentifizierungsschlüssel-ID in einen nicht standardmäßigen Wert.

Dieses Verfahren ist nicht störend.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED:

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   > Sie können das verwenden `security key-manager query -key-type NSE-AK` Befehl zum Anzeigen von Schlüssel-IDs.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. Vergewissern Sie sich, dass die Authentifizierungsschlüssel zugewiesen wurden:

   `storage encryption disk show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ----------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   [...]
   ```

Integriertes Verschlüsselungsmanagement

Ermöglichen Sie integriertes Verschlüsselungsmanagement in ONTAP 9.6 und höher

Mit dem Onboard Key Manager können Clusterknoten auf einem FIPS-Laufwerk oder SED authentifiziert werden. Der integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt. Der Onboard Key Manager ist nach FIPS-140-2 Level 1 zertifiziert.

Mit dem integrierten Key Manager werden die Schlüssel gesichert, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie müssen Onboard Key Manager für jedes Cluster aktivieren, das auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

Sie müssen den ausführen `security key-manager onboard enable` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen. In MetroCluster Konfigurationen müssen Sie ausführen `security key-manager onboard enable` Führen Sie zuerst auf dem lokalen Cluster aus `security key-manager onboard sync` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.

Standardmäßig müssen Sie beim Neustart eines Node nicht die Passphrase für das Schlüsselmanagement eingeben. Außer in MetroCluster können Sie den verwenden `cc-mode-enabled=yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Passphrase eingeben.

Wenn der Onboard Key Manager im Common Criteria-Modus aktiviert ist (`cc-mode-enabled=yes`Das Systemverhalten wird folgendermaßen geändert:

- Das System überwacht bei der Verwendung im Common Criteria-Modus auf aufeinanderfolgende fehlgeschlagene Cluster-Passphrase.

  Wenn NetApp Storage Encryption (NSE) aktiviert ist und Sie beim Booten nicht die richtige Cluster-Passphrase eingeben, kann sich das System nicht auf seinen Laufwerken authentifizieren und automatisch neu starten. Um dies zu korrigieren, müssen Sie an der Boot-Eingabeaufforderung die richtige Cluster-Passphrase eingeben. Sobald das System gebootet wurde, können bis zu 5 aufeinanderfolgende Versuche unternommen werden, um für jeden Befehl, für den die Cluster-Passphrase als Parameter erforderlich ist, in einem Zeitraum von 24 Stunden korrekt einzugeben. Wenn das Limit erreicht wird (beispielsweise konnten Sie den Cluster-Passphrase 5 Mal hintereinander nicht korrekt eingeben), müssen Sie entweder warten, bis der 24-Stunden-Timeout abgelaufen ist, oder Sie müssen den Node neu booten, um das Limit zurückzusetzen.

- Updates für das System-Image nutzen das Code-Signing-Zertifikat von NetApp RSA-3072 zusammen mit dem von SHA-384 signierten Code, um die Image-Integrität anstelle des üblichen NetApp RSA-2048-Code-Signaturzertifikats und den von SHA-256 signierten Digests zu überprüfen.

  Der Upgrade-Befehl überprüft, ob der Bildinhalt durch Überprüfen verschiedener digitaler Signaturen nicht verändert oder beschädigt wurde. Der Image-Aktualisierungsprozess wird mit dem nächsten Schritt fortgesetzt, wenn die Validierung erfolgreich ist. Andernfalls schlägt die Image-Aktualisierung fehl. Informationen zu System-Updates finden Sie auf der man-Page „`Cluster Image`“.

Der Onboard Key Manager speichert Schlüssel im volatilen Speicher. Der Inhalt von flüchtigem Speicher wird gelöscht, wenn das System neu gestartet oder angehalten wird. Unter normalen Betriebsbedingungen wird der Inhalt von flüchtigem Speicher innerhalb von 30 s gelöscht, wenn ein System angehalten wird.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen KMIP-Server (Key Management) verwenden, müssen Sie die externe Schlüsselmanager-Datenbank gelöscht haben.

  "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Starten Sie den Key Manager Setup-Befehl:

   `security key-manager onboard enable -cc-mode-enabled yes|no`

   > Einstellen `cc-mode-enabled=yes` Um zu verlangen, dass Benutzer nach einem Neustart die Kennverwaltung-Passphrase eingeben. Der `- cc-mode-enabled` Die Option wird in MetroCluster-Konfigurationen nicht unterstützt. Der `security key-manager onboard enable` Mit dem Befehl wird der ersetzt `security key-manager setup` Befehl.

   Das folgende Beispiel startet den Befehl zum Einrichten des Schlüsselmanagers in cluster1, ohne dass nach jedem Neustart die Passphrase eingegeben werden muss:

   ```
   cluster1::> security key-manager onboard enable

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. Geben Sie an der Eingabeaufforderung für die Passphrase eine Passphrase zwischen 32 und 256 Zeichen oder für „`cc-Mode`“ eine Passphrase zwischen 64 und 256 Zeichen ein.

   > Wenn die angegebene „`cc-Mode`“-Passphrase weniger als 64 Zeichen beträgt, liegt eine Verzögerung von fünf Sekunden vor, bevor die Eingabeaufforderung für das Setup des Schlüsselmanagers die Passphrase erneut anzeigt.

3. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.
4. Vergewissern Sie sich, dass die Authentifizierungsschlüssel erstellt wurden:

   `security key-manager key query -node node`

   > Der `security key-manager key query` Mit dem Befehl wird der ersetzt `security key-manager query key` Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird überprüft, ob Authentifizierungsschlüssel für erstellt wurden `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Nachdem Sie fertig sind

Kopieren Sie die Passphrase zur späteren Verwendung an einen sicheren Ort außerhalb des Storage-Systems.

Alle Informationen zum Verschlüsselungsmanagement werden automatisch in der replizierten Datenbank (RDB) für den Cluster gesichert. Sie sollten die Informationen auch manuell für den Notfall sichern.

Ermöglichen Sie integriertes Verschlüsselungsmanagement in ONTAP 9.5 und früher

Mit dem Onboard Key Manager können Clusterknoten auf einem FIPS-Laufwerk oder SED authentifiziert werden. Der integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt. Der Onboard Key Manager ist nach FIPS-140-2 Level 1 zertifiziert.

Mit dem integrierten Key Manager werden die Schlüssel gesichert, die das Cluster für den Zugriff auf

verschlüsselte Daten verwendet. Sie müssen Onboard Key Manager für jedes Cluster aktivieren, das auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

Sie müssen den ausführen `security key-manager setup` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen.

Wenn Sie über eine MetroCluster-Konfiguration verfügen, überprüfen Sie diese Richtlinien:

- In ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.
- Vor ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Warten Sie auf dem lokalen Cluster etwa 20 Sekunden, und führen Sie dann den Betrieb aus `security key-manager setup` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.

Standardmäßig müssen Sie beim Neustart eines Node nicht die Passphrase für das Schlüsselmanagement eingeben. Ab ONTAP 9.4 können Sie den verwenden `-enable-cc-mode yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Passphrase eingeben.

Wenn Sie die Einstellung für NVE verwenden `-enable-cc-mode yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Für `volume create`, Sie müssen nicht angeben `-encrypt true`. Für `volume move start`, Sie müssen nicht angeben `-encrypt-destination true`.

> Nach einem fehlgeschlagenen Passphrase-Versuch müssen Sie den Node erneut neu booten.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen KMIP-Server (Key Management) verwenden, müssen Sie die externe Schlüsselmanager-Datenbank gelöscht haben.

  "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Starten Sie die Konfiguration des Schlüsselmanagers:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > Ab ONTAP 9.4 können Sie den verwenden `-enable-cc-mode yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Kennwortphrase für das Schlüsselmanagement eingeben. Wenn Sie die Einstellung für NVE verwenden `-enable-cc-mode yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt.

   Das folgende Beispiel beginnt mit dem Einrichten des Schlüsselmanagers auf Clustered 1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Eingabe `yes` An der Eingabeaufforderung zur Konfiguration des Onboard-Verschlüsselungsmanagement.
3. Geben Sie an der Eingabeaufforderung für die Passphrase eine Passphrase zwischen 32 und 256 Zeichen oder für „`cc-Mode`“ eine Passphrase zwischen 64 und 256 Zeichen ein.

> Wenn die angegebene „`cc-Mode`“-Passphrase weniger als 64 Zeichen beträgt, liegt eine Verzögerung von fünf Sekunden vor, bevor die Eingabeaufforderung für das Setup des Schlüsselmanagers die Passphrase erneut anzeigt.

4. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.
5. Vergewissern Sie sich, dass die Schlüssel für alle Nodes konfiguriert sind:

   `security key-manager key show`

   Die vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

Nachdem Sie fertig sind

Alle Informationen zum Verschlüsselungsmanagement werden automatisch in der replizierten Datenbank (RDB) für den Cluster gesichert.

Wenn Sie die Onboard Key Manager-Passphrase konfigurieren, sollten Sie die Informationen auch manuell an einem sicheren Ort außerhalb des Speichersystems sichern, um sie bei einem Notfall zu verwenden. Siehe "Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement".

Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED (Onboard Key Management)

Sie können das verwenden `storage encryption disk modify` Befehl zum Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED. Cluster-Nodes verwenden diesen Schlüssel für den Zugriff auf die Daten auf dem Laufwerk.

Über diese Aufgabe

Ein selbstverschlüsselndes Laufwerk ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen nicht standardmäßigen Wert eingestellt ist. Der Hersteller Secure ID (MSID), der die Schlüssel-ID 0x0 hat, ist der Standardvorgabewert für SAS-Laufwerke. Bei NVMe-Laufwerken ist der Standardwert ein Null-Schlüssel, der als leere Schlüssel-ID dargestellt wird. Wenn Sie einem selbstverschlüsselnden Laufwerk die Schlüssel-ID zuweisen, ändert das System seine Authentifizierungsschlüssel-ID in einen nicht standardmäßigen Wert.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED:

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   > Sie können das verwenden `security key-manager key query -key-type NSE-AK` Befehl zum Anzeigen von Schlüssel-IDs.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. Vergewissern Sie sich, dass die Authentifizierungsschlüssel zugewiesen wurden:

   `storage encryption disk show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
000000000000000002000000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

Weisen Sie einem FIPS 140-2-2-Authentifizierungsschlüssel zu

Sie können das verwenden `storage encryption disk modify` Befehl mit dem `-fips-key-id` Option zum Zuweisen eines FIPS-140-2-Authentifizierungsschlüssels zu einem FIPS-Laufwerk. Cluster-Nodes verwenden diesen Schlüssel für andere Laufwerksvorgänge als Datenzugriff, z. B. zur Verhinderung von Denial-of-Service-Angriffen auf das Laufwerk.

Über diese Aufgabe

In Ihrer Sicherheitseinrichtung müssen Sie unter Umständen unterschiedliche Schlüssel zur Datenauthentifizierung und zur FIPS 140-2-2-Authentifizierung verwenden. Falls dies nicht der Fall ist, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden, den Sie für den Datenzugriff verwenden.

Dieses Verfahren ist nicht störend.

Bevor Sie beginnen

Die Laufwerk-Firmware muss FIPS 140-2-2-konform unterstützen. Der "NetApp Interoperabilitäts-Matrix-Tool" Enthält Informationen zu unterstützten Festplatten-Firmware-Versionen.

Schritte

1. Sie müssen zunächst sicherstellen, dass Sie einen Datenauthentifizierungsschlüssel zugewiesen haben. Dies kann mit einem erfolgen Externer Schlüsselmanager Oder an Integriertes Verschlüsselungsmanagement. Vergewissern Sie sich, dass der Schlüssel mit dem Befehl zugewiesen ist `storage encryption disk show`.
2. SEDs einen FIPS 140-2-Authentifizierungsschlüssel zuweisen:

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

   Sie können das verwenden `security key-manager query` Befehl zum Anzeigen von Schlüssel-IDs.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

3. Vergewissern Sie sich, dass der Authentifizierungsschlüssel zugewiesen wurde:

   `storage encryption disk show -fips`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
--------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

Cluster-weiter FIPS-konformer Modus für KMIP-Serververbindungen

Sie können das verwenden `security config modify` Befehl mit dem `-is-fips-enabled` Option zur Aktivierung des clusterweiten FIPS-konformen Modus für genutzte Daten Dadurch wird die Verwendung von OpenSSL im FIPS-Modus erzwingt, wenn eine Verbindung zu KMIP-Servern hergestellt wird.

Über diese Aufgabe

Wenn Sie den FIPS-konformen Cluster-Modus aktivieren, verwendet das Cluster automatisch nur TLS1.2 und FIPS-validierte Chiffre Suites. Der clusterweite FIPS-konforme Modus ist standardmäßig deaktiviert.

Sie müssen die Cluster-Nodes manuell neu booten, nachdem Sie die Cluster-weite Sicherheitskonfiguration geändert haben.

Bevor Sie beginnen

- Der Storage Controller muss im FIPS-konformen Modus konfiguriert sein.
- Alle KMIP-Server müssen TLSv1.2 unterstützen. Das System benötigt TLSv1.2, um die Verbindung zum KMIP-Server abzuschließen, wenn der clusterweite FIPS-konforme Modus aktiviert ist.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set -privilege advanced`

2. Vergewissern Sie sich, dass TLSv1.2 unterstützt wird:

   ```
   security config show -supported-protocols
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> security config show
             Cluster                                                Cluster
   Security
   Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
   Ready
   --------- ---------- ----------------------- -----------------
   ----------------
   SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                                !aNULL:!EXP:
                                                !eNULL
   ```

3. Cluster-weiten, FIPS-konformen Modus aktivieren:

   ```
   security config modify -is-fips-enabled true -interface SSL
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

4. Manuelles Neubooten der Cluster-Nodes
5. Vergewissern Sie sich, dass der FIPS-konforme Cluster-weite Modus aktiviert ist:

   ```
   security config show
   ```

   ```
   cluster1::> security config show
             Cluster                                                Cluster
   Security
   Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
   Ready
   --------- ---------- ----------------------- -----------------
   ----------------
   SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                                !aNULL:!EXP:
                                                !eNULL:!RC4
   ```

NetApp Verschlüsselung managen

Verschlüsseln Sie Volume-Daten

Sie können das verwenden `volume move start` Befehl zum Verschieben und Entschlüsseln von Volume-Daten.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen. Alternativ können Sie ein SVM-Administrator sein, an den der Cluster-Administrator Berechtigungen delegiert hat. Weitere Informationen finden Sie unter "Delegieren von Berechtigungen zum Ausführen des Befehls Volume Move".

Schritte

1. Verschieben eines vorhandenen verschlüsselten Volumes und Entschlüsseln der Daten auf dem Volume:

   `volume move start -vserver` *`SVM_name`* `-volume volume_name -destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl wird ein vorhandenes Volume mit dem Namen verschoben `vol1` Auf das Zielaggregat `aggr3` Und entverschlüsselt die Daten auf dem Volume:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   Das System löscht den Verschlüsselungsschlüssel für das Volume. Die Daten auf dem Volume werden unverschlüsselt.

2. Vergewissern Sie sich, dass das Volume zur Verschlüsselung deaktiviert ist:

   `volume show -encryption`

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl wird angezeigt, ob Volumes auf ausgeführt werden `cluster1` Verschlüsselt:

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

Verschieben Sie ein verschlüsseltes Volume

Sie können das verwenden `volume move start` Befehl zum Verschieben eines verschlüsselten Volumes. Das verschobene Volume kann auf demselben Aggregat oder einem anderen Aggregat residieren.

Über diese Aufgabe

Die Verschiebung schlägt fehl, wenn der Ziel-Node oder das Ziel-Volume die Volume-Verschlüsselung nicht unterstützt.

Der `-encrypt-destination` Option für `volume move start` Standardmäßig auf „true“ für verschlüsselte Volumes gesetzt. Wenn Sie angeben müssen, dass das Ziel-Volume nicht verschlüsselt werden soll, wird

sichergestellt, dass die Verschlüsselung der Daten auf dem Volume nicht versehentlich aufgehoben wird.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen. Alternativ können Sie ein SVM-Administrator sein, an den der Cluster-Administrator Berechtigungen delegiert hat. Weitere Informationen finden Sie unter "Delegieren Sie die Autorität, um den Befehl Volume move auszuführen".

Schritte

1. Verschieben Sie ein vorhandenes verschlüsseltes Volume, und lassen Sie die Daten auf dem Volume verschlüsselt:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl wird ein vorhandenes Volume mit dem Namen verschoben `vol1` Auf das Zielaggregat `aggr3` Und lassen die Daten auf dem Volume verschlüsselt:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. Vergewissern Sie sich, dass das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die verschlüsselten Volumes auf angezeigt `cluster1`:

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  --------- ----
   vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
   ```

Delegieren von Berechtigungen zum Ausführen des Befehls Volume Move

Sie können das verwenden `volume move` Befehl zum Verschlüsseln eines vorhandenen Volumes, Verschieben eines verschlüsselten Volumes oder Entschlüsseln eines Volumes Cluster-Administratoren können ausgeführt werden `volume move` Entweder selbst einen Befehl ausführen oder sie können die Berechtigungen delegieren, um den Befehl an SVM-Administratoren auszuführen.

Über diese Aufgabe

Standardmäßig werden SVM-Administratoren das zugewiesen `vsadmin` Rolle, die nicht die Berechtigung zum Verschieben von Volumes beinhaltet. Sie müssen den zuweisen `vsadmin-volume` Rolle für SVM-

Administratoren, damit sie in der Lage sind `volume move` Befehl.

Schritt

1. Delegieren Sie die Berechtigung zum Ausführen des `volume move` Befehl:

   `security login modify -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`vsadmin-volume`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl erhält der SVM-Administrator die Berechtigung, den auszuführen `volume move` Befehl.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   SVM-admin -application ssh -authmethod domain -role vsadmin-volume
   ```

Ändern Sie den Verschlüsselungsschlüssel für ein Volume mit dem Befehl „Start der Volume-Verschlüsselung“

Es handelt sich hierbei um eine Best Practice für Sicherheit, den Verschlüsselungsschlüssel für ein Volume regelmäßig zu ändern. Ab ONTAP 9.3 können Sie den verwenden `volume encryption rekey start` Befehl zum Ändern des Verschlüsselungsschlüssels.

Über diese Aufgabe

Sobald Sie einen Rekeyvorgang starten, muss er abgeschlossen sein. Es gibt keine Rückkehr zum alten Schlüssel. Wenn während des Vorgangs ein Leistungsproblem auftritt, können Sie das ausführen `volume encryption rekey pause` Befehl zum Anhalten des Vorgangs, und `volume encryption rekey resume` Befehl zum Fortsetzen des Vorgangs.

Bis der Vorgang des Neuschlüssels abgeschlossen ist, verfügt das Volume über zwei Tasten. Neue Schreibzugriffe und die entsprechenden Lesezugriffe nutzen den neuen Schlüssel. Andernfalls wird der alte Schlüssel bei den Lesevorgängen verwendet.

> Verwenden Sie ihn nicht `volume encryption rekey start` Um ein SnapLock Volume erneut zu keyNeuschlüssel.

Schritte

1. Ändern eines Verschlüsselungsschlüssels:

   `volume encryption rekey start -vserver SVM_name -volume volume_name`

   Der Verschlüsselungsschlüssel für wird mit dem folgenden Befehl geändert `vol1` Auf SVM`vs1`:

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. Überprüfen Sie den Status der Rekeybedienung:

   `volume encryption rekey show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl wird der Status der Rekeyoperation angezeigt:

```
cluster1::> volume encryption rekey show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   ---------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. Vergewissern Sie sich nach Abschluss des Rekeyvorgangs, dass das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die verschlüsselten Volumes auf angezeigt `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Ändern Sie den Verschlüsselungsschlüssel für ein Volume mit dem Befehl Volume move Start

Es handelt sich hierbei um eine Best Practice für Sicherheit, den Verschlüsselungsschlüssel für ein Volume regelmäßig zu ändern. Sie können das verwenden `volume move start` Befehl zum Ändern des Verschlüsselungsschlüssels. Sie müssen verwenden `volume move start` In ONTAP 9.2 und früher. Das verschobene Volume kann auf demselben Aggregat oder einem anderen Aggregat residieren.

Über diese Aufgabe

Verwenden Sie ihn nicht `volume move start` Um einen SnapLock oder FlexGroup Volume erneut zu keyNeuschlüssel zu erhalten.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen. Alternativ können Sie ein SVM-Administrator sein, an den der Cluster-Administrator Berechtigungen delegiert hat. Weitere Informationen finden Sie unter "Delegieren Sie die Autorität, um den Befehl Volume move auszuführen".

Schritte

1. Verschieben eines vorhandenen Volumes und Ändern des Verschlüsselungsschlüssels:

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -generate-destination-key true`

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl wird ein vorhandenes Volume mit dem Namen verschoben **`vol1`** Auf das Zielaggregat **`aggr2`** Und ändert den Verschlüsselungsschlüssel:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr2 -generate-destination-key true
   ```

   Für das Volume wird ein neuer Verschlüsselungsschlüssel erstellt. Die Daten auf dem Volume bleiben verschlüsselt.

2. Vergewissern Sie sich, dass das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl werden die verschlüsselten Volumes auf angezeigt `cluster1`:

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  --------- ----
   vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
   ```

Drehen Sie die Authentifizierungsschlüssel für die NetApp Storage Encryption

Sie können die Authentifizierungsschlüssel mit der NetApp Storage Encryption (NSE) drehen.

Über diese Aufgabe

Die rotierenden Authentifizierungsschlüssel in einer NSE-Umgebung werden unterstützt, wenn Sie External Key Manager (KMIP) verwenden.

> Rotierende Authentifizierungsschlüssel in einer NSE-Umgebung werden von Onboard Key Manager (OKM) nicht unterstützt.

Schritte

1. Verwenden Sie die `security key-manager create-key` Befehl zum Generieren neuer Authentifizierungsschlüssel.

   Sie müssen neue Authentifizierungsschlüssel generieren, bevor Sie die Authentifizierungsschlüssel ändern

können.

2. Verwenden Sie die `storage encryption disk modify -disk * -data-key-id` Befehl zum Ändern der Authentifizierungsschlüssel.

Löschen Sie ein verschlüsseltes Volume

Sie können das verwenden `volume delete` Befehl zum Löschen eines verschlüsselten Volumes.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen. Alternativ können Sie ein SVM-Administrator sein, an den der Cluster-Administrator Berechtigungen delegiert hat. Weitere Informationen finden Sie unter "Delegieren Sie die Autorität, um den Befehl Volume move auszuführen".
- Das Volume muss sich offline befinden.

Schritt

1. Verschlüsseltes Volume löschen:

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.

   Mit dem folgenden Befehl wird ein verschlüsseltes Volume mit dem Namen gelöscht `vol1`:

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   Eingabe `yes` Wenn Sie zur Bestätigung des Löschvorgangs aufgefordert werden.

   Das System löscht den Verschlüsselungsschlüssel für das Volume nach 24 Stunden.

   Nutzung `volume delete` Mit dem `-force true` Option zum sofortigen Löschen eines Volumes und Löschen des entsprechenden Verschlüsselungsschlüssels. Dieser Befehl erfordert erweiterte Berechtigungen. Weitere Informationen finden Sie auf der man-Page.

Nachdem Sie fertig sind

Sie können das verwenden `volume recovery-queue` Befehl zum Wiederherstellen eines gelöschten Volumes während der Aufbewahrungsfrist nach Ausgabe des `volume delete` Befehl:

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"So verwenden Sie die Volume Recovery-Funktion"

Löschen Sie Daten auf einem verschlüsselten Volume sicher

Löschen Sie Daten sicher auf einer Übersicht über ein verschlüsseltes Volume

Ab ONTAP 9.4 können Sie Daten auf NVE-fähigen Volumes durch sicheres Löschen unterbrechungsfrei abspeichern. Das Scrubbing von Daten auf einem verschlüsselten Volume stellt sicher, dass sie nicht von physischen Medien wiederhergestellt werden

können, beispielsweise bei „`s` pillage“, bei denen Spuren von Daten beim Überschreiben von Blöcken hinterlassen wurden oder zum sicheren Löschen der Daten eines Mandanten.

Secure Purge ist nur für zuvor gelöschte Dateien auf Volumes mit NVE geeignet. Sie können ein unverschlüsseltes Volume nicht abreiben. Sie müssen KMIP-Server für die Schlüsselverwendung verwenden, nicht für den integrierten Schlüsselmanager.

Überlegungen zur Verwendung einer sicheren Löschung

- Volumes, die in einem Aggregat erstellt wurden, das für NetApp Aggregate Encryption (NAE) aktiviert ist, unterstützen das sichere Löschen nicht.
- Secure Purge ist nur für zuvor gelöschte Dateien auf Volumes mit NVE geeignet.
- Sie können ein unverschlüsseltes Volume nicht abreiben.
- Sie müssen KMIP-Server für die Schlüsselverwendung verwenden, nicht für den integrierten Schlüsselmanager.

Sichere Spülfunktionen je nach Version von ONTAP unterschiedlich.

ONTAP 9.8 und höher

- Sicheres Löschen wird von MetroCluster und FlexGroup unterstützt.
- Wenn das zu löckige Volume die Quelle einer SnapMirror-Beziehung ist, müssen Sie die SnapMirror-Beziehung nicht unterbrechen, um eine sichere Löschung durchzuführen.
- Die Umverschlüsselungsmethode unterscheidet sich bei Volumes, die SnapMirror Datensicherung verwenden, im Gegensatz zu Volumes, die keine SnapMirror Datensicherung (DP) verwenden, oder solchen, die SnapMirror erweiterte Datensicherung nutzen.
  - Standardmäßig werden Daten bei Volumes im SnapMirror Data Protection (DP)-Modus mit der erneuten Verschlüsselungsmethode für Volume Move neu verschlüsselt.
  - Standardmäßig verwenden Volumes, die keine SnapMirror Datensicherung oder Volumes verwenden, die den XDP-Modus (Extended Data Protection) von SnapMirror verwenden, die in-Place-Reverschlüsselungsmethode.
  - Diese Standardeinstellungen können mit dem geändert werden `secure purge re-encryption-method [volume-move|in-place-rekey]` Befehl.
- Standardmäßig werden alle Snapshot-Kopien in FlexVol Volumes während des sicheren Löschvorgangs automatisch gelöscht. Standardmäßig werden Snapshots in FlexGroup Volumes und Volumes mit SnapMirror Datensicherung nicht automatisch während des sicheren Löschvorgangs gelöscht. Diese Standardeinstellungen können mit dem geändert werden `secure purge delete-all-snapshots [true|false]` Befehl.

ONTAP 9.7 und früher:

- Sicheres Löschen unterstützt Folgendes nicht:
  - FlexClone
  - SnapVault
  - FabricPool
- Wenn das zu löckige Volume die Quelle einer SnapMirror-Beziehung ist, müssen Sie die SnapMirror-Beziehung unterbrechen, bevor Sie das Volume löschen können.

  Falls im Volume bereits Snapshot-Kopien vorhanden sind, müssen Sie die Snapshot-Kopien freigeben, bevor Sie das Volume löschen können. Beispielsweise müssen Sie ein FlexClone Volume unter Umständen von seinem übergeordneten Volume trennen.

- Durch das erfolgreiche Aufrufen der Funktion zum sicheren Löschen wird eine Volume-Verschiebung ausgelöst, die die verbleibenden, nicht gelöschten Daten mit einem neuen Schlüssel erneut verschlüsselt.

  Das verschobene Volume bleibt im aktuellen Aggregat. Der alte Schlüssel wird automatisch zerstört und stellt sicher, dass die gelöschten Daten nicht von den Speichermedien wiederhergestellt werden können.

Löschen Sie Daten auf einem verschlüsselten Volume sicher ohne SnapMirror Beziehung

Ab ONTAP 9.4 können Sie auf NVE-fähigen Volumes sichere Datenlöschung auch für unterbrechungsfreie „`sCrub`“-Daten verwenden.

Über diese Aufgabe

Die sichere Löschung kann in Abhängigkeit von der Datenmenge in den gelöschten Dateien mehrere Minuten bis viele Stunden dauern. Sie können das verwenden `volume encryption secure-purge show` Befehl zum Anzeigen des Status des Vorgangs. Sie können das verwenden `volume encryption secure-purge abort` Befehl zum Beenden des Vorgangs.

> Um eine sichere Löschung auf einem SAN-Host durchzuführen, müssen Sie die gesamte LUN löschen, die die zu löschenden Dateien enthält. Alternativ können Sie Löcher in der LUN für die Blöcke lochen, die zu den Dateien gehören, die gelöscht werden sollen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem keine Stanzlöcher in der LUN unterstützt, können Sie keine sichere Löschung durchführen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Löschen Sie die Dateien oder die LUN, die Sie löschen möchten.
   - Löschen Sie auf einem NAS-Client die Dateien, die Sie sicher löschen möchten.
   - Löschen Sie auf einem SAN-Host die LUN, die Sie löschen oder Löcher in der LUN sicher löschen möchten, damit die Blöcke zu den Dateien gehören, die gelöscht werden sollen.
2. Ändern Sie im Storage-System die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

3. Wenn die Dateien, die Sie sicher löschen möchten, in Snapshots gespeichert sind, löschen Sie die Snapshots:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. Löschen Sie gelöschte Dateien sicher:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   Mit dem folgenden Befehl werden die gelöschten Dateien auf sicher gelöscht `vol1` Auf SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Überprüfen Sie den Status des Secure-Purge-Vorgangs:

   ```
   volume encryption secure-purge show
   ```

Löschen Sie Daten mit einer asynchronen SnapMirror-Beziehung sicher auf einem verschlüsselten Volume

Ab ONTAP 9.8 kann auf NVE-fähigen Volumes mit einer asynchronen SnapMirror-Beziehung ein sicheres Löschen von Daten verwendet werden, die unterbrechungsfrei „`sCrub`“ Daten erzeugen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Über diese Aufgabe

Die sichere Löschung kann in Abhängigkeit von der Datenmenge in den gelöschten Dateien mehrere Minuten bis viele Stunden dauern. Sie können das verwenden `volume encryption secure-purge show` Befehl zum Anzeigen des Status des Vorgangs. Sie können das verwenden `volume encryption secure-purge abort` Befehl zum Beenden des Vorgangs.

> Um eine sichere Löschung auf einem SAN-Host durchzuführen, müssen Sie die gesamte LUN löschen, die die zu löschenden Dateien enthält. Alternativ können Sie Löcher in der LUN für die Blöcke lochen, die zu den Dateien gehören, die gelöscht werden sollen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem keine Stanzlöcher in der LUN unterstützt, können Sie keine sichere Löschung durchführen.

Schritte

1. Wechseln Sie auf dem Speichersystem auf die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Löschen Sie die Dateien oder die LUN, die Sie löschen möchten.
   - Löschen Sie auf einem NAS-Client die Dateien, die Sie sicher löschen möchten.
   - Löschen Sie auf einem SAN-Host die LUN, die Sie löschen oder Löcher in der LUN sicher löschen möchten, damit die Blöcke zu den Dateien gehören, die gelöscht werden sollen.
3. Bereiten Sie das Zielvolumen in der asynchronen Beziehung vor, die sicher gelöscht werden soll:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Wiederholen Sie diesen Schritt für jedes Volume in Ihrer asynchronen SnapMirror-Beziehung.

4. Wenn die Dateien, die Sie sicher löschen möchten, in Snapshot-Kopien gespeichert sind, löschen Sie die Snapshot-Kopien:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. Wenn sich die Dateien, die Sie sicher löschen möchten, in den Basiskopien befinden, führen Sie folgende Schritte aus:

   a. Erstellung einer Snapshot Kopie auf dem Ziel-Volume in der asynchronen SnapMirror Beziehung:

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. Aktualisieren Sie SnapMirror, um die Snapshot Basiskopie nach vorn zu verschieben:

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   Wiederholen Sie diesen Schritt für jedes Volume in der asynchronen SnapMirror-Beziehung.

a. Wiederholen Sie die Schritte (A) und (b) entsprechend der Anzahl der Basis-Snapshot-Kopien plus einer.

   Wenn Sie beispielsweise zwei Basis-Snapshot-Kopien haben, sollten Sie die Schritte (A) und (b) dreimal wiederholen.

b. Überprüfen Sie, ob die Snapshot Basiskopie vorhanden ist:

   ```
   snapshot show -vserver SVM_name -volume volume_name
   ```

c. Löschen Sie die Snapshot Basiskopie:

   ```
   snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
   ```

6. Löschen Sie gelöschte Dateien sicher:

   ```
   volume encryption secure-purge start -vserver svm_name -volume volume_name
   ```

   Wiederholen Sie diesen Schritt für jedes Volume in der asynchronen SnapMirror-Beziehung.

   Mit dem folgenden Befehl werden die gelöschten Dateien auf „`vol1`“ auf SVM „`vs1`“ sicher gelöscht:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

7. Überprüfen Sie den Status des sicheren Löschvorgangs:

   ```
   volume encryption secure-purge show
   ```

Scrub die Daten auf einem verschlüsselten Volume mit einer synchronen SnapMirror-Beziehung ab

Ab ONTAP 9.8 können Sie ein sicheres Löschen verwenden, um Daten auf NVE-fähigen Volumes mit einer synchronen SnapMirror Beziehung unterbrechungsfrei „zu verschieben“.

Über diese Aufgabe

Eine sichere Löschung kann in Abhängigkeit von der Datenmenge in den gelöschten Dateien von mehreren Minuten bis zu vielen Stunden dauern. Sie können das verwenden `volume encryption secure-purge show` Befehl zum Anzeigen des Status des Vorgangs. Sie können das verwenden `volume encryption secure-purge abort` Befehl zum Beenden des Vorgangs.

> Um eine sichere Löschung auf einem SAN-Host durchzuführen, müssen Sie die gesamte LUN löschen, die die zu löschenden Dateien enthält. Alternativ können Sie Löcher in der LUN für die Blöcke lochen, die zu den Dateien gehören, die gelöscht werden sollen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem keine Stanzlöcher in der LUN unterstützt, können Sie keine sichere Löschung durchführen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Ändern Sie im Storage-System die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Löschen Sie die Dateien oder die LUN, die Sie löschen möchten.
   - Löschen Sie auf einem NAS-Client die Dateien, die Sie sicher löschen möchten.
   - Löschen Sie auf einem SAN-Host die LUN, die Sie löschen oder Löcher in der LUN sicher löschen möchten, damit die Blöcke zu den Dateien gehören, die gelöscht werden sollen.

3. Bereiten Sie das Zielvolumen in der asynchronen Beziehung vor, die sicher gelöscht werden soll:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Wiederholen Sie diesen Schritt für das andere Volume in Ihrer synchronen SnapMirror Beziehung.

4. Wenn die Dateien, die Sie sicher löschen möchten, in Snapshot-Kopien gespeichert sind, löschen Sie die Snapshot-Kopien:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

5. Falls sich die Datei für die sichere Löschung im Basistelefon oder allgemeinen Snapshot Kopien befindet, aktualisieren Sie das SnapMirror, um die allgemeine Snapshot Kopie vorwärts zu verschieben:

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   Es gibt zwei gemeinsame Snapshot Kopien. Dieser Befehl muss also zweimal ausgeführt werden.

6. Falls sich die sichere Spüldatei in der applikationskonsistenten Snapshot Kopie befindet, löschen Sie die Snapshot Kopie auf beiden Volumes in der synchronen SnapMirror Beziehung:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

   Führen Sie diesen Schritt auf beiden Volumes durch.

7. Löschen Sie gelöschte Dateien sicher:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   Wiederholen Sie diesen Schritt für jedes Volume in der synchronen SnapMirror-Beziehung.

   Mit dem folgenden Befehl werden die gelöschten Dateien auf „`vol1`“ auf SMV „`vs1`“ sicher gelöscht.

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. Überprüfen Sie den Status des sicheren Löschvorgangs:

   ```
   volume encryption secure-purge show
   ```

Ändern Sie die Onboard-Passphrase für das Verschlüsselungsmanagement

Es handelt sich um eine Best Practice für Sicherheit, die Passphrase für das Onboard-Verschlüsselungsmanagement regelmäßig zu ändern. Sie sollten die neue Onboard-Passphrase für das Verschlüsselungsmanagement zur späteren Verwendung an einen sicheren Ort außerhalb des Storage-Systems kopieren.

Bevor Sie beginnen

- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Ändern Sie die Onboard-Passphrase für das Verschlüsselungsmanagement:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager onboard update-passphrase`
ONTAP 9.5 und früher	`security key-manager update-passphrase`

   Eine vollständige Befehlssyntax finden Sie in den man-Pages.

   Mit dem folgenden Befehl von ONTAP 9.6 können Sie die Passphrase für das Onboard-Verschlüsselungsmanagement ändern `cluster1`:

   ```
   clusterl::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. Eingabe `y` Bei der Eingabeaufforderung zum Ändern der Onboard-Passphrase für das Verschlüsselungsmanagement.
4. Geben Sie die aktuelle Passphrase an der aktuellen Passphrase-Eingabeaufforderung ein.
5. Geben Sie an der neuen Passphrase-Eingabeaufforderung eine Passphrase zwischen 32 und 256 Zeichen oder für „`cc-Mode`“ eine Passphrase zwischen 64 und 256 Zeichen ein.

   Wenn die angegebene „`cc-Mode`“-Passphrase weniger als 64 Zeichen beträgt, liegt eine Verzögerung von fünf Sekunden vor, bevor die Eingabeaufforderung für das Setup des Schlüsselmanagers die Passphrase erneut anzeigt.

6. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.

Nachdem Sie fertig sind

In einer MetroCluster Umgebung müssen Sie die Passphrase im Partner-Cluster aktualisieren:

- In ONTAP 9.5 und früher müssen Sie ausgeführt werden `security key-manager update-passphrase` Mit derselben Passphrase im Partner-Cluster.
- In ONTAP 9.6 und höher werden Sie zur Ausführung aufgefordert `security key-manager onboard sync` Mit derselben Passphrase im Partner-Cluster.

Sie sollten die integrierte Passphrase für das Verschlüsselungsmanagement zur späteren Verwendung an einen sicheren Ort außerhalb des Storage-Systems kopieren.

Sie sollten die Informationen zum Verschlüsselungsmanagement manuell sichern, wenn Sie die Passphrase für das Onboard-Verschlüsselungsmanagement ändern.

"Manuelles Backup der integrierten Verschlüsselungsmanagementinformationen"

Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement

Wenn Sie die Onboard-Passphrase für das Verschlüsselungsmanagement an einen sicheren Ort außerhalb des Storage-Systems konfigurieren, sollten Sie die Onboard-Verschlüsselungsmanagement-Informationen an einen sicheren Ort kopieren.

Was Sie benötigen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Über diese Aufgabe

Alle Informationen zum Verschlüsselungsmanagement werden automatisch in der replizierten Datenbank (RDB) für den Cluster gesichert. Außerdem sollten Sie die Informationen zum Verschlüsselungsmanagement manuell für den Notfall sichern.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Anzeigen der Backup-Informationen für das Verschlüsselungsmanagement für das Cluster:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager onboard show-backup`
ONTAP 9.5 und früher	`security key-manager backup show`

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

+ mit dem folgenden 9.6 Befehl werden die Backup-Informationen zum Schlüsselmanagement für angezeigt `cluster1`:

+

```
cluster1::> security key-manager onboard show-backup

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAAoAAAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAAAACQAAAAAAAAAAAgAAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAAAACIAAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAACgAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAAoAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAAA
     gAAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

1. Backup-Informationen sollten bei einem Notfall an einen sicheren Ort außerhalb des Storage-Systems kopiert werden.

Wiederherstellung der integrierten Verschlüsselungsschlüssel für das Verschlüsselungsmanagement

Das Verfahren zur Wiederherstellung der integrierten Verschlüsselungsschlüssel für das Verschlüsselungsmanagement variiert je nach Ihrer Version von ONTAP.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen KMIP-Server (Key Management) verwenden, müssen Sie die externe Schlüsselmanager-Datenbank gelöscht haben. Weitere Informationen finden Sie unter "Transition zum

Onboard-Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

> Wenn Sie NSE in einem System mit einem Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten im Flash Cache Modul.

ONTAP 9.8 und höher mit verschlüsseltem Root-Volume

> Wenn Sie ONTAP 9.8 oder höher ausführen und Ihr Root-Volume nicht verschlüsselt ist, befolgen Sie das Verfahren für ONTAP 9.6 oder höher.

Wenn Sie ONTAP 9.8 und höher verwenden und Ihr Root-Volume verschlüsselt ist, müssen Sie mit dem Boot-Menü eine integrierte Recovery-Passphrase für das Verschlüsselungsmanagement festlegen. Dieser Vorgang ist auch erforderlich, wenn Sie einen Bootmedienaustausch durchführen.

1. Starten Sie den Knoten im Startmenü, und wählen Sie Option `(10) Set onboard key management recovery secrets`.
2. Eingabe `y` Um diese Option zu verwenden.
3. Geben Sie an der Eingabeaufforderung die integrierte Passphrase für das Verschlüsselungsmanagement für das Cluster ein.
4. Geben Sie an der Eingabeaufforderung die Backup-Schlüsseldaten ein.

   Der Node kehrt zum Startmenü zurück.

5. Wählen Sie im Startmenü Option `(1) Normal Boot`.

ONTAP 9.6 und höher

1. Vergewissern Sie sich, dass der Schlüssel wiederhergestellt werden muss:
   `security key-manager key query -node` *`node`*
2. Stellen Sie den Schlüssel wieder her:
   `security key-manager onboard sync`

   Eine vollständige Befehlssyntax finden Sie in den man-Pages.

   Mit dem folgenden ONTAP 9.6-Befehl werden die Schlüssel in der Onboard-Schlüsselhierarchie synchronisiert:

   ```
   cluster1::> security key-manager onboard sync

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   ```

3. Geben Sie an der Eingabeaufforderung für die Passphrase die integrierte Passphrase für das Verschlüsselungsmanagement für das Cluster ein.

ONTAP 9.5 und früher

1. Vergewissern Sie sich, dass der Schlüssel wiederhergestellt werden muss:
   `security key-manager key show`
2. Wenn Sie ONTAP 9.8 und höher verwenden und Ihr Root-Volume verschlüsselt ist, führen Sie folgende Schritte aus:

   Wenn Sie ONTAP 9.6 oder 9.7 verwenden oder ONTAP 9.8 oder höher verwenden und Ihr Root-Volume nicht verschlüsselt ist, überspringen Sie diesen Schritt.

3. Stellen Sie den Schlüssel wieder her:
   `security key-manager setup -node node`

   Eine vollständige Befehlssyntax finden Sie in den man-Pages.

4. Geben Sie an der Eingabeaufforderung für die Passphrase die integrierte Passphrase für das Verschlüsselungsmanagement für das Cluster ein.

Wiederherstellung der externen Verschlüsselungsschlüssel für das Verschlüsselungsmanagement

Sie können die externen Verschlüsselungsschlüssel zum Verschlüsselungsmanagement manuell wiederherstellen und sie auf einen anderen Node verschieben. Dies sollten Sie tun, wenn Sie einen Node neu starten, der während des Erstellungsens der Schlüssel für das Cluster vorübergehend nicht verfügbar war.

Über diese Aufgabe

In ONTAP 9.6 und höher können Sie die verwenden `security key-manager key query -node node_name` Befehl zum Überprüfen, ob Ihr Schlüssel wiederhergestellt werden muss.

In ONTAP 9.5 und früher können Sie die verwenden `security key-manager key show` Befehl zum Überprüfen, ob Ihr Schlüssel wiederhergestellt werden muss.

> Wenn Sie NSE in einem System mit einem Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten im Flash Cache Modul.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Wenn Sie ONTAP 9.8 oder höher verwenden und Ihr Root-Volume verschlüsselt ist, gehen Sie wie folgt vor:

   Wenn Sie ONTAP 9.7 oder früher oder ONTAP 9.8 oder höher verwenden und Ihr Root-Volume nicht verschlüsselt ist, überspringen Sie diesen Schritt.

   a. Legen Sie die Bootargs fest:
      ```
      setenv kmip.init.ipaddr <ip-address>+
      setenv kmip.init.netmask <netmask>+
      setenv kmip.init.gateway <gateway>+
      setenv kmip.init.interface e0M+
      boot_ontap
      ```

b. Starten Sie den Knoten im Startmenü, und wählen Sie Option `(11) Configure node for external key management`.

c. Befolgen Sie die Anweisungen zum Eingeben des Managementzertifikats.

   Nachdem alle Informationen zum Managementzertifikat eingegeben wurden, kehrt das System zum Boot-Menü zurück.

d. Wählen Sie im Startmenü Option `(1) Normal Boot`.

2. Wiederherstellen des Schlüssels:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 und früher

> `node` Standardeinstellung für alle Knoten. Eine vollständige Befehlssyntax finden Sie in den man-Pages. Dieser Befehl wird nicht unterstützt, wenn das integrierte Verschlüsselungsmanagement aktiviert ist.

Mit dem folgenden ONTAP 9.6-Befehl werden die Authentifizierungsschlüssel des externen Schlüsselmanagements auf alle Nodes in wiederhergestellt `cluster1`:

```
clusterl::> security key-manager external restore
```

Ersetzen Sie SSL-Zertifikate

Alle SSL-Zertifikate haben ein Ablaufdatum. Sie müssen Ihre Zertifikate aktualisieren, bevor sie ablaufen, um den Verlust des Zugriffs auf Authentifizierungsschlüssel zu verhindern.

Bevor Sie beginnen

- Sie müssen das öffentliche Ersatzzertifikat und den privaten Schlüssel für das Cluster (KMIP-Client-Zertifikat) erhalten haben.
- Sie müssen das öffentliche Ersatzzertifikat für den KMIP-Server (KMIP-Server-Ca-Zertifikat) erhalten haben.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern ersetzen.

> Sie können den Ersatz-Client und die Serverzertifikate vor oder nach der Installation der Zertifikate auf dem Cluster auf dem KMIP-Server installieren.

Schritte

1. Installieren Sie das neue KMIP Server-Ca-Zertifikat:

```
security certificate install -type server-ca -vserver <>
```

2. Installieren Sie das neue KMIP-Client-Zertifikat:

```
security certificate install -type client -vserver <>
```

3. Aktualisieren Sie die Konfiguration des Schlüsselmanagers, um die neu installierten Zertifikate zu verwenden:

```
security key-manager external modify -vserver <> -client-cert <> -server-ca
-certs <>
```

Wenn Sie ONTAP 9.6 oder höher in einer MetroCluster-Umgebung ausführen und die Schlüsselmanager-Konfiguration auf der Admin-SVM ändern möchten, müssen Sie den Befehl in der Konfiguration auf beiden Clustern ausführen.

> Wenn Sie die Konfiguration des Schlüsselmanagers zur Verwendung der neu installierten Zertifikate aktualisieren, wird ein Fehler ausgegeben, wenn sich die öffentlichen/privaten Schlüssel des neuen Clientzertifikats von den zuvor installierten Schlüsseln unterscheiden. Weitere Informationen finden Sie im Knowledge Base-Artikel "Das neue öffentliche oder private Clientzertifikat unterscheidet sich vom vorhandenen Clientzertifikat" Anweisungen zum Überschreiben dieses Fehlers finden Sie unter.

Ein FIPS-Laufwerk oder SED austauschen

Sie können ein FIPS-Laufwerk oder SED auf dieselbe Weise ersetzen, wie Sie eine normale Festplatte ersetzen. Stellen Sie sicher, dass Sie dem Ersatzlaufwerk neue Datenauthentifizierungsschlüssel zuweisen. Bei einem FIPS-Laufwerk kann auch ein neuer FIPS 140-2-Authentifizierungsschlüssel zugewiesen werden.

> Wenn ein HA-Paar nutzt "Verschlüsselung von SAS- oder NVMe-Laufwerken (SED, NSE, FIPS)", Sie müssen die Anweisungen im Thema folgen "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren" Für alle Laufwerke innerhalb des HA-Paars vor der Initialisierung des Systems (Boot-Optionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Bevor Sie beginnen

- Sie müssen die Schlüssel-ID für den vom Laufwerk verwendeten Authentifizierungsschlüssel kennen.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Stellen Sie sicher, dass die Festplatte als fehlgeschlagen markiert wurde:

```
storage disk show -broken
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. Entfernen Sie die ausgefallene Festplatte, und ersetzen Sie sie durch ein neues FIPS-Laufwerk oder eine neue SED. Befolgen Sie die Anweisungen im Hardware-Leitfaden für das Festplatten-Shelf-Modell.
3. Besitzer der neu ersetzten Festplatte zuweisen:

   `storage disk assign -disk disk_name -owner node`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. Vergewissern Sie sich, dass die neue Festplatte zugewiesen wurde:

   `storage encryption disk show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. Weisen Sie den Datenauthentifizierungsschlüssel dem FIPS-Laufwerk oder der SED zu.

   "Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED (externes Verschlüsselungsmanagement)"

6. Weisen Sie bei Bedarf dem FIPS-Laufwerk einen FIPS 140-2-Authentifizierungsschlüssel zu.

   "Zuweisung eines FIPS 140-2-Authentifizierungsschlüssels zu einem FIPS-Laufwerk"

Daten auf einem FIPS-Laufwerk oder SED-Laufwerk können nicht darauf zugegriffen werden

Machen Sie Daten auf einem FIPS-Laufwerk oder SED unzugänglich Übersicht

Wenn Daten auf einem FIPS- oder SED-Laufwerk dauerhaft nicht zugänglich sind, aber den nicht genutzten Speicherplatz des Laufwerks für neue Daten beibehalten werden sollen, kann die Festplatte bereinigen. Wenn Sie Daten dauerhaft unzugänglich machen und Sie das Laufwerk nicht wiederverwenden müssen, können Sie es zerstören.

- Festplattenbereinigung

  Wenn Sie ein selbstverschlüsselndes Laufwerk desinfizieren, ändert das System den Verschlüsselungsschlüssel in einen neuen zufälligen Wert, setzt den Einschloß-Status auf false zurück und setzt die Schlüssel-ID auf einen Standardwert, entweder die Herstellersichere ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch werden die Daten auf der Festplatte nicht mehr zugänglich und können nicht abgerufen werden. Sie können desinfizierte Festplatten als nicht auf Null bereinigte Ersatzfestplatten wiederverwenden.

- Festplatte zerstören

  Wenn Sie ein FIPS- oder SED-Laufwerk zerstören, setzt das System den Schlüssel für die Festplattenverschlüsselung auf einen unbekannten zufälligen Wert und sperrt die Festplatte unwiderruflich. Dadurch wird die Festplatte permanent nicht nutzbar und die Daten darauf dauerhaft zugänglich gemacht.

Es können einzelne Self-Encrypting Drives oder alle Self-Encrypting Drives eines Node bereinigen oder

zerstört werden.

Ein FIPS-Laufwerk oder SED infizieren

Wenn Daten auf einem FIPS- oder SED-Laufwerk dauerhaft zugänglich gemacht und das Laufwerk für neue Daten verwendet werden soll, können Sie das verwenden `storage encryption disk sanitize` Befehl zum Löschen des Laufwerks.

Über diese Aufgabe

Wenn Sie ein selbstverschlüsselndes Laufwerk desinfizieren, ändert das System den Verschlüsselungsschlüssel in einen neuen zufälligen Wert, setzt den Einschloß-Status auf false zurück und setzt die Schlüssel-ID auf einen Standardwert, entweder die Herstellersichere ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch werden die Daten auf der Festplatte nicht mehr zugänglich und können nicht abgerufen werden. Sie können desinfizierte Festplatten als nicht auf Null bereinigte Ersatzfestplatten wiederverwenden.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Migrieren Sie alle Daten, die in einem Aggregat auf einer anderen Festplatte aufbewahrt werden müssen.
2. Löschen Sie das Aggregat auf dem FIPS-Laufwerk oder der SED, das bereinigt werden soll:

   `storage aggregate delete -aggregate` *`aggregate_name`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Festplatten-ID für das zu desinfizierte FIPS-Laufwerk oder SED ermitteln:

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Wenn ein FIPS-Laufwerk im FIPS-Compliance-Modus ausgeführt wird, legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf den Standard MSID 0x0:

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   Sie können das verwenden `security key-manager query` Befehl zum Anzeigen von Schlüssel-IDs.

   ```
   cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

   Info: Starting modify on 1 disk.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

5. Antrieb desinfizieren:

   `storage encryption disk sanitize -disk disk_id`

   Mit diesem Befehl können Sie nur Hot-Spare- oder defekte Festplatten bereinigen. Um alle Festplatten unabhängig vom Typ zu desinfizieren, verwenden Sie das `-force-all-state` Option. Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ONTAP fordert Sie auf, eine Bestätigungsaufforderung einzugeben, bevor Sie fortfahren. Geben Sie den Ausdruck genau so ein, wie er auf dem Bildschirm angezeigt wird.

   ```
   cluster1::> storage encryption disk sanitize -disk 1.10.2

   Warning: This operation will cryptographically sanitize 1 spare or
   broken self-encrypting disk on 1 node.
            To continue, enter sanitize disk: sanitize disk

   Info: Starting sanitize on 1 disk.
         View the status of the operation using the
         storage encryption disk show-status command.
   ```

Ein FIPS-Laufwerk oder SED zerstören

Wenn Daten auf einem FIPS- oder SED-Laufwerk dauerhaft zugänglich gemacht werden sollen und Sie das Laufwerk nicht wiederverwenden müssen, können Sie das verwenden `storage encryption disk destroy` Befehl zum Zerstören der Festplatte.

Über diese Aufgabe

Wenn Sie ein FIPS- oder SED-Laufwerk zerstören, setzt das System den Schlüssel für die Festplattenverschlüsselung auf einen unbekannten zufälligen Wert und sperrt das Laufwerk unwiderruflich. Dadurch wird die Festplatte praktisch nicht nutzbar und die Daten auf ihr dauerhaft zugänglich. Sie können die Festplatte jedoch mithilfe der physischen sicheren ID (PSID) auf dem Etikett des Datenträgers auf die werkseitig konfigurierten Einstellungen zurücksetzen. Weitere Informationen finden Sie unter "Ein FIPS-Laufwerk oder eine SED-Appliance wird zurückgegeben, wenn Authentifizierungsschlüssel verloren gehen".

> Ein FIPS- oder SED-Laufwerk darf nur zerstört werden, wenn Sie über den Non-Returnable Disk Plus-Service (NRD Plus) verfügen. Beim Zerstören einer Festplatte wird die Gewährleistung nicht mehr abgedeckt.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Migrieren Sie alle Daten, die in einem Aggregat auf einer anderen, unterschiedlichen Festplatte aufbewahrt werden müssen.
2. Löschen Sie das Aggregat auf dem zu zerstörenden FIPS-Laufwerk oder SED:

   ```
   storage aggregate delete -aggregate aggregate_name
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identifizieren Sie die Festplatten-ID für das zu zerstörenden FIPS-Laufwerk oder die SED:

   ```
   storage encryption disk show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Zerstören Sie die Festplatte:

   ```
   storage encryption disk destroy -disk disk_id
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > Sie werden aufgefordert, einen Bestätigungsphrase einzugeben, bevor Sie fortfahren. Geben Sie den Ausdruck genau so ein, wie er auf dem Bildschirm angezeigt wird.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

Notfall shred Daten auf einem FIPS-Laufwerk oder SED

Im Falle eines Sicherheitsnotfalls können Sie den Zugriff auf ein FIPS-Laufwerk oder eine SED umgehend verhindern, auch wenn dem Storage-System oder dem KMIP-Server keine Stromversorgung zur Verfügung steht.

Bevor Sie beginnen

- Wenn Sie einen KMIP-Server ohne Stromversorgung verwenden, muss der KMIP-Server mit einem einfach zerstörten Authentifizierungselement (z. B. eine Smartcard oder ein USB-Laufwerk) konfiguriert werden.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Daten im Notfall auf einem FIPS-Laufwerk oder SED sreddern:

Wenn…	Dann…

Das Storage-System verfügt über einen Stromanstieg, und Sie können das Storage-System normal offline schalten	a. Wenn das Storage-System als HA-Paar konfiguriert ist, deaktivieren Sie Takeover. b. Alle Aggregate offline schalten und löschen. c. Stellen Sie die Berechtigungsebene auf Erweiteriert: + ein `set -privilege advanced` d. Wenn sich das Laufwerk im FIPS-Compliance-Modus befindet, setzen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf die Standard-MSID: `storage encryption disk modify -disk * -fips-key-id 0x0` e. Stoppen Sie das Speichersystem. f. Booten Sie im Wartungsmodus. g. Desinfizieren oder zerstören Sie die Festplatten: ◦ Wenn Sie die Daten auf den Datenträgern unzugänglich machen und die Festplatten dennoch wiederverwenden können, desinfizieren Sie die Festplatten: `disk encrypt sanitize -all` ◦ Wenn Sie die Daten auf den Laufwerken unzugänglich machen möchten und Sie die Festplatten nicht speichern müssen, zerstören Sie die Festplatten: `disk encrypt destroy disk_id1 disk_id2 …`	Dem Storage-System steht Strom zur Verfügung, und Sie müssen die Daten sofort schüttelt haben

a. **Wenn Sie die Daten auf den Datenträgern unzugänglich machen und die Festplatten noch wiederverwenden können, desinfizieren Sie die Festplatten:**
b. Wenn das Storage-System als HA-Paar konfiguriert ist, deaktivieren Sie Takeover.
c. Legen Sie die Berechtigungsebene auf erweitert fest:
`set -privilege advanced`
d. Wenn sich das Laufwerk im FIPS-Compliance-Modus befindet, legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf die Standard-MSID fest:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Festplatte bereinigen:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Wenn Sie die Daten auf den Datenträgern unzugänglich machen und Sie nicht brauchen, um die Festplatten zu speichern, zerstören Sie die Festplatten:**
	b. Wenn das Storage-System als HA-Paar konfiguriert ist, deaktivieren Sie Takeover.
	c. Legen Sie die Berechtigungsebene auf erweitert fest:
	`set -privilege advanced`
	d. Zerstören Sie die Festplatten:
	`storage encryption disk destroy -disk * -force-all-states true`
		Das Speichersystem kommt zu einer Panik, sodass das System dauerhaft deaktiviert ist, während alle Daten gelöscht werden. Um das System erneut zu verwenden, müssen Sie es neu konfigurieren.

Der KMIP-Server mit Strom ist, nicht jedoch für das Storage-System verfügbar	a. Melden Sie sich beim KMIP-Server an. b. Vernichten Sie alle Schlüssel, die den FIPS-Laufwerken oder SEDs zugeordnet sind, die die Daten enthalten, auf die Sie Zugriff verhindern möchten. Dadurch wird der Zugriff auf die Festplattenverschlüsselung durch das Speichersystem verhindert.	Der KMIP-Server oder das Storage-System bieten keine Stromversorgung

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

Geben Sie ein FIPS-Laufwerk oder eine SED an den Dienst zurück, wenn Authentifizierungsschlüssel verloren gehen

Das System behandelt ein FIPS-Laufwerk oder eine SED als defekt, wenn die Authentifizierungsschlüssel dafür dauerhaft verloren gehen und nicht vom KMIP-Server abgerufen werden können. Obwohl Sie nicht auf die Daten auf der Festplatte zugreifen oder diese wiederherstellen können, können Sie Schritte Unternehmen, um den nicht genutzten Speicherplatz der SED für Daten erneut verfügbar zu machen.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Über diese Aufgabe

Sie sollten diesen Prozess nur verwenden, wenn Sie sicher sind, dass die Authentifizierungsschlüssel für das FIPS-Laufwerk oder die SED dauerhaft verloren gehen und nicht wiederhergestellt werden können.

Wenn die Festplatten partitioniert werden, müssen sie zunächst nicht partitioniert werden, bevor Sie diesen Prozess starten können.

> Der Befehl zum Entpartitionieren einer Festplatte ist nur auf der Diagnose-Ebene verfügbar und sollte nur unter NetApp Support Supervision durchgeführt werden. **Es wird dringend empfohlen, sich vor dem Fortfahren mit dem NetApp Support zu in Verbindung zu setzen.** Diese kann auch im Knowledge Base Artikel beschrieben werden "Wie man ein Ersatzlaufwerk in ONTAP entpartitionieren".

Schritte

1. Rückgabe eines FIPS-Laufwerks oder SED an den Dienst:

Wenn die SEDS…	Verwenden Sie die folgenden Schritte…

Nicht im FIPS-Compliance-Modus oder im FIPS-Compliance-Modus und der FIPS-Schlüssel ist verfügbar	a. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced` b. Setzen Sie den FIPS-Schlüssel auf die Standard-Herstellsichere ID 0x0: `storage encryption disk modify -fips-key-id 0x0 -disk` *`disk_id`* c. Überprüfen Sie, ob der Vorgang erfolgreich war: `storage encryption disk show-status`Wenn der Vorgang fehlgeschlagen ist, verwenden Sie den PSID-Prozess in diesem Thema. d. Bereinigen der defekten Scheibe: `storage encryption disk sanitize -disk` *`disk_id`*`Überprüfen Sie, ob der Vorgang mit dem Befehl erfolgreich war `storage encryption disk show-status` Bevor Sie mit dem nächsten Schritt fortfahren.  e. Entfernen Sie die desinfizierte Festplatte: `storage disk unfail -spare true -disk` *`disk_id`*  f. Prüfen Sie, ob die Festplatte einen Eigentümer hat: `storage disk show -disk` *`disk_id`*  Wenn der Datenträger keinen Eigentümer hat, weisen Sie einen zu. `storage disk assign -owner node -disk` *`disk_id`*  i. Geben Sie den Knotenpunkt für den Knoten ein, der die Festplatten besitzt, die Sie desinfizieren möchten:  `system node run -node` *`node_name`*  Führen Sie die aus `disk sanitize release` Befehl.  g. Verlassen Sie die Nodeshell. Fehler der Festplatte erneut aufheben: `storage disk unfail -spare true -disk` *`disk_id`*  h. Überprüfen Sie, ob die Festplatte nun frei und in einem Aggregat wiederverwendet werden kann: `storage disk show -disk` *`disk_id`*

Im FIPS-Compliance-Modus ist der FIPS-Schlüssel nicht verfügbar, und SEDs haben eine PSID auf dem Etikett	a. Beziehen Sie die PSID des Datenträgers von der Datenträgerbezeichnung. b. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced` c. Zurücksetzen der Festplatte auf die werkseitigen Einstellungen: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`*`Überprüfen Sie, ob der Vorgang mit dem Befehl erfolgreich war `storage encryption disk show-status` Bevor Sie mit dem nächsten Schritt fortfahren. d. Wenn Sie ONTAP 9.8P5 oder eine frühere Version verwenden, fahren Sie mit dem nächsten Schritt fort. Wenn Sie ONTAP 9.8P6 oder höher verwenden, nehmen Sie die bereinigte Festplatte wieder auf. `storage disk unfail -disk` *`disk_id`* e. Prüfen Sie, ob die Festplatte einen Eigentümer hat: `storage disk show -disk` *`disk_id`*  Wenn der Datenträger keinen Eigentümer hat, weisen Sie einen zu. `storage disk assign -owner node -disk` *`disk_id`*  i. Geben Sie den Knotenpunkt für den Knoten ein, der die Festplatten besitzt, die Sie desinfizieren möchten:  `system node run -node` *`node_name`*  Führen Sie die aus `disk sanitize release` Befehl.  f. Verlassen Sie die Nodeshell.. Fehler der Festplatte erneut aufheben: `storage disk unfail -spare true -disk` *`disk_id`* g. Überprüfen Sie, ob die Festplatte nun frei und in einem Aggregat wiederverwendet werden kann: `storage disk show -disk` *`disk_id`*

Eine vollständige Befehlssyntax finden Sie im "Befehlsreferenz".

Geben Sie ein FIPS-Laufwerk oder eine SED in den ungeschützten Modus zurück

Ein FIPS-Laufwerk oder SED ist nur dann vor unberechtigtem Zugriff geschützt, wenn die Authentifizierungsschlüssel-ID für den Knoten auf einen anderen Wert als den Standardwert gesetzt ist. Sie können ein FIPS-Laufwerk oder eine SED über den in den ungeschützten Modus versetzen `storage encryption disk modify` Befehl zum Festlegen der Schlüssel-ID auf Standard.

Wenn ein HA-Paar SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verwendet, müssen Sie diesen Prozess für alle Laufwerke innerhalb des HA-Paars befolgen, bevor das System initialisiert wird (Boot-Optionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Wenn ein FIPS-Laufwerk im FIPS-Compliance-Modus ausgeführt wird, legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf den Standard MSID 0x0:

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

   Sie können das verwenden `security key-manager query` Befehl zum Anzeigen von Schlüssel-IDs.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   Bestätigen Sie den Vorgang mit dem Befehl:

   ```
   storage encryption disk show-status
   ```

   Wiederholen Sie den Befehl show-Status, bis die Zahlen in „Disks gestartet“ und „Disks Fertig“ die gleichen sind.

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start                Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp            Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------   ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. Legen Sie die Daten-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID 0x0:

   ```
   storage encryption disk modify -disk disk_id -data-key-id 0x0
   ```

   Der Wert von `-data-key-id` Sollte auf 0x0 gesetzt werden, ob Sie ein SAS- oder NVMe-Laufwerk in den ungeschützten Modus zurücksenden.

   Sie können das verwenden `security key-manager query` Befehl zum Anzeigen von Schlüssel-IDs.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Bestätigen Sie den Vorgang mit dem Befehl:

```
storage encryption disk show-status
```

Wiederholen Sie den Befehl show-Status, bis die Zahlen identisch sind. Die Operation ist abgeschlossen, wenn die Zahlen in „Platten begonnen“ und „Platten fertig“ sind die gleichen.

Wartungsmodus

Ab ONTAP 9.7 können Sie eine FIPS-Festplatte aus dem Wartungsmodus neu Schlüssel aktivieren. Sie sollten den Wartungsmodus nur verwenden, wenn Sie die ONTAP-CLI-Anweisungen im vorherigen Abschnitt nicht verwenden können.

Schritte

1. Legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID 0x0:

   `disk encrypt rekey_fips 0x0 *disklist*`

2. Legen Sie die Daten-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID 0x0:

   `disk encrypt rekey 0x0 *disklist*`

3. Bestätigen Sie, dass der FIPS-Authentifizierungsschlüssel erfolgreich umcodiert wurde:

   `disk encrypt show_fips`

4. Bestätigung der erfolgreichen Verschlüsselung des Datenauthentifizierungsschlüssels mit:

   `disk encrypt show`

   In Ihrer Ausgabe wird wahrscheinlich entweder die Standard-MSID 0x0-Schlüssel-ID oder der 64-stellige Wert des Schlüsselservers angezeigt. Der `Locked?` Feld bezieht sich auf die Datensperrung.

```
Disk       FIPS Key ID                  Locked?
---------- ---------------------------- -------
0a.01.0    0x0                           Yes
```

Entfernen Sie eine externe Schlüsselmanager-Verbindung

Sie können einen KMIP-Server von einem Node trennen, wenn Sie den Server nicht mehr benötigen. Beispielsweise können Sie einen KMIP-Server trennen, wenn Sie die

Volume-Verschlüsselung umstellen.

Über diese Aufgabe

Wenn Sie einen KMIP Server von einem Node in einem HA-Paar trennen, trennt das System die Verbindung zwischen dem Server automatisch und allen Cluster-Nodes.

> Wenn Sie nach der Trennung eines KMIP Servers weiterhin externes Verschlüsselungsmanagement nutzen möchten, stellen Sie sicher, dass ein anderer KMIP Server für die Authentifizierung von Schlüsseln zur Verfügung steht.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritt

1. Trennen eines KMIP-Servers vom aktuellen Node:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9.5 und früher

In einer MetroCluster Umgebung müssen Sie die folgenden Befehle für beide Cluster für die Administrator-SVM wiederholen.

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

Mit dem folgenden ONTAP 9.6-Befehl werden die Verbindungen zu zwei externen Schlüsselverwaltungsservern für deaktiviert `cluster1`, Der erste benannte `ks1`, Hören auf dem Standardport 5696, der zweite mit der IP-Adresse 10.0.0.20, Hören auf Port 24482:

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Ändern Sie die Eigenschaften des Servers für die Verwaltung externer Schlüssel

Ab ONTAP 9.6 können Sie den verwenden `security key-manager external modify-server` Befehl zum Ändern der I/O-Zeitüberschreitung und des Benutzernamens eines externen Schlüsselverwaltungsservers.

Bevor Sie beginnen

- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.
- In einer MetroCluster Umgebung müssen Sie die folgenden Schritte auf beiden Clustern für den Administrator-SVM wiederholen.

Schritte

1. Ändern Sie im Storage-System die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Ändern der Eigenschaften eines externen Schlüsselmanagers-Servers für das Cluster:

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > Der Timeout-Wert wird in Sekunden angegeben. Wenn Sie den Benutzernamen ändern, werden Sie aufgefordert, ein neues Passwort einzugeben. Wenn Sie den Befehl an der Eingabeaufforderung für die Anmeldung beim Cluster ausführen, *admin_SVM* Standardmäßig wird der Admin-SVM des aktuellen Clusters festgelegt. Sie müssen der Cluster-Administrator sein, um die Eigenschaften eines externen Schlüsselmanager-Servers zu ändern.

   Mit dem folgenden Befehl wird der Zeitüberschreitungswert für das in 45 Sekunden geändert `cluster1` Externer Schlüsselverwaltungsserver, der auf dem Standardport 5696 zuhören wird:

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. Ändern Sie die Server-Eigenschaften von externen Verschlüsselungsmanagement für eine SVM (nur NVE):

   ```
   security key-manager external modify-server -vserver SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > Der Timeout-Wert wird in Sekunden angegeben. Wenn Sie den Benutzernamen ändern, werden Sie aufgefordert, ein neues Passwort einzugeben. Wenn Sie den Befehl an der SVM-Anmeldeaufforderung ausführen, *SVM* Standardeinstellung ist die aktuelle SVM. Zum Ändern der Eigenschaften des externen Schlüsselmanager-Servers müssen Sie der Cluster oder der SVM-Administrator sein.

   Mit dem folgenden Befehl werden der Benutzername und das Passwort des geändert `svm1` Externer Schlüsselverwaltungsserver, der auf dem Standardport 5696 zuhören wird:

   ```
   svml::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

4. Wiederholen Sie den letzten Schritt für alle weiteren SVMs.

Wechsel vom Onboard-Verschlüsselungsmanagement auf externes Verschlüsselungsmanagement

Wenn Sie von Onboard-Verschlüsselungsmanagement auf externes Verschlüsselungsmanagement wechseln möchten, müssen Sie die integrierte

Verschlüsselungsmanagementkonfiguration löschen, bevor Sie externes Verschlüsselungsmanagement aktivieren können.

Bevor Sie beginnen

- Bei der hardwarebasierten Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder SEDs auf den Standardwert zurückgesetzt werden.

  "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren"

- Bei softwarebasierter Verschlüsselung müssen Sie alle Volumes entschlüsseln.

  "Verschlüsselung von Volume-Daten aufheben"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Löschen der integrierten Verschlüsselungsmanagementkonfiguration für ein Cluster:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 und früher	`security key-manager delete-key-database`

Eine vollständige Befehlssyntax finden Sie im "Handbuch für ONTAP-Seiten".

Umstellung von externem Verschlüsselungsmanagement auf integriertes Verschlüsselungsmanagement

Wenn Sie von externem Verschlüsselungsmanagement auf integriertes Verschlüsselungsmanagement umsteigen möchten, müssen Sie die Konfiguration für das externe Verschlüsselungsmanagement löschen, bevor Sie integriertes Verschlüsselungsmanagement aktivieren können.

Bevor Sie beginnen

- Bei der hardwarebasierten Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder SEDs auf den Standardwert zurückgesetzt werden.

  "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren"

- Sie müssen alle externen Schlüsselmanager-Verbindungen gelöscht haben.

  "Löschen einer externen Schlüsselmanager-Verbindung"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Verfahren

Die Schritte zur Umstellung Ihres Schlüsselmanagements hängen von der verwendeten Version von ONTAP ab.

ONTAP 9.6 und höher

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Verwenden Sie den Befehl:

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   > In einer MetroCluster-Umgebung müssen Sie den Befehl für die Administrator-SVM auf beiden Clustern wiederholen.

ONTAP 9.5 und früher

Verwenden Sie den Befehl:
`security key-manager delete-kmip-config`

Was passiert, wenn während des Startvorgangs keine Schlüsselverwaltungsserver verfügbar sind

ONTAP ergreift Maßnahmen, um unerwünschte Verhaltensweisen zu vermeiden, wenn ein mit NSE konfiguriertes Storage-System während des Bootens keinen der angegebenen Verschlüsselungsmanagementserver erreichen kann.

Wenn das Storage-System für NSE konfiguriert ist, werden die SEDs rekeyed und gesperrt und die SEDs eingeschaltet. Das Storage-System muss die erforderlichen Authentifizierungsschlüssel von den Verschlüsselungsmanagement-Servern abrufen, um sich bei SEDs zu authentifizieren, bevor es auf die Daten zugreifen kann.

Das Storage-System versucht, bis zu drei Stunden lang die angegebenen Schlüsselmanagementserver zu kontaktieren. Sollte das Storage-System zu diesem Zeitpunkt keinen Zugang haben, wird der Bootvorgang abgebrochen und das Storage-System stoppt.

Wenn das Speichersystem einen bestimmten Schlüsselverwaltungsserver erfolgreich kontaktiert, versucht es dann, eine SSL-Verbindung für bis zu 15 Minuten herzustellen. Wenn das Storage-System keine SSL-Verbindung zu einem angegebenen Schlüsselmanagementserver herstellen kann, wird der Bootvorgang angehalten und das Speichersystem wird angehalten.

Während das Speichersystem versucht, sich mit wichtigen Managementservern zu verbinden und eine Verbindung herzustellen, werden in der CLI detaillierte Informationen über fehlgeschlagene Kontaktversuche angezeigt. Sie können die Kontaktversuche jederzeit unterbrechen, indem Sie Strg-C drücken

Als Sicherheitsmaßnahme erlauben SEDs nur eine begrenzte Anzahl von unbefugten Zugriffsversuchen, wonach sie den Zugriff auf die vorhandenen Daten deaktivieren. Wenn das Speichersystem keine bestimmten Schlüsselverwaltungsserver kontaktieren kann, um die richtigen Authentifizierungsschlüssel zu erhalten, kann es nur versuchen, sich mit dem Standardschlüssel zu authentifizieren, der zu einem fehlgeschlagenen Versuch und einem Panikzustand führt. Wenn das Storage-System so konfiguriert ist, dass es im Falle eines Panikzustands automatisch neu gestartet wird, wird eine Boot-Schleife erzeugt, die zu kontinuierlichen fehlgeschlagenen Authentifizierungsversuchen von SEDs führt.

Das Anhalten des Storage-Systems in diesen Szenarien ist durch das Design zu verhindern, dass das Storage-System in einen Boot-Loop und möglichen unbeabsichtigten Datenverlust durch die dauerhaft

gesperrten SEDs gelangt, da es die Sicherheitsgrenze einer bestimmten Anzahl aufeinander folgender fehlgeschlagener Authentifizierungsversuche überschreitet. Der Grenzwert und die Art des Sperrschutzes hängen von den Herstellungsspezifikationen und dem Typ der SED ab:

SED-Typ	Anzahl aufeinanderfolgender fehlgeschlagener Authentifizierungsversuche, die zu einer Sperrung führen	Sicherungstyp sperren, wenn die Sicherheitsgrenze erreicht ist
HDD	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.
X440_PHM2800MCTO 800 GB NSE SSDs mit Firmware-Versionen NA00 oder NA01	5	Temporär. Die Sperrung wird nur wirksam, bis die Festplatte aus- und wieder eingeschaltet wird.
X577_PHM2800MCTO 800 GB NSE SSDs mit Firmware-Versionen NA00 oder NA01	5	Temporär. Die Sperrung wird nur wirksam, bis die Festplatte aus- und wieder eingeschaltet wird.
X440_PHM2800MCTO 800 GB NSE SSDs mit höherer Firmware-Version	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.
X577_PHM2800MCTO 800 GB NSE SSDs mit höherer Firmware-Version	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.
Alle anderen SSD-Modelle	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.

Bei allen SED-Typen wird durch eine erfolgreiche Authentifizierung die Anzahl der Versuche auf Null zurückgesetzt.

Wenn dieses Szenario auftritt, bei dem das Speichersystem aufgrund eines Fehlers angehalten wird, um irgendwelche angegebenen Schlüsselverwaltungsserver zu erreichen, müssen Sie zuerst die Ursache für den Kommunikationsfehler identifizieren und korrigieren, bevor Sie versuchen, das Speichersystem weiterhin zu booten.

Deaktivieren Sie die Verschlüsselung standardmäßig

Ab ONTAP 9.7 ist die Aggregat- und Volume-Verschlüsselung standardmäßig aktiviert, wenn Sie über eine VE-Lizenz (Volume Encryption) verfügen und einen integrierten oder

externen Schlüsselmanager verwenden. Bei Bedarf können Sie die Verschlüsselung standardmäßig für den gesamten Cluster deaktivieren.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe durchzuführen, oder ein SVM-Administrator, an den der Cluster-Administrator die Berechtigungen delegiert hat.

Schritt

1. Führen Sie den folgenden Befehl aus, um die Verschlüsselung für das gesamte Cluster in ONTAP 9.7 oder höher standardmäßig zu deaktivieren:

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```