Verwalten von Zielen für die Cluster-Sicherheit

Active IQ Unified Manager 9.11

NetApp
December 18, 2023

Inhalt

Verwalten von Zielen für die Cluster-Sicherheit . . . 1
Welche Sicherheitskriterien werden bewertet . . . 1
Was bedeutet nicht, dass Compliance-Anforderungen erfüllt werden . . . 7
Anzeigen des Sicherheitsstatus für Cluster und Storage VMs . . . 7
Anzeigen von Sicherheitsereignissen, für die möglicherweise Software- oder Firmware-Updates erforderlich sind . . . 9
Anzeige des Managements der Benutzerauthentifizierung auf allen Clustern . . . 10
Anzeigen des Verschlüsselungsstatus aller Volumes . . . 10
Anzeigen des Anti-Ransomware-Status aller Volumes und Storage-VMs . . . 11
Anzeigen aller aktiven Sicherheitsereignisse . . . 12
Hinzufügen von Warnmeldungen für Sicherheitsereignisse . . . 12
Bestimmte Sicherheitsereignisse deaktivieren . . . 13
Sicherheitsereignisse . . . 14

Verwalten von Zielen für die Cluster-Sicherheit

Unified Manager bietet ein Dashboard an, in dem die Sicherheit Ihrer ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes anhand der Empfehlungen ermittelt wird, die im *NetApp Security Hardening Guide for ONTAP 9* definiert wurden.

Ziel des Sicherheits-Dashboards ist es, Bereiche anzuzeigen, in denen die ONTAP Cluster nicht mit den von NetApp empfohlenen Richtlinien übereinstimmen, damit Sie die potenziellen Probleme beheben können. In den meisten Fällen werden Sie die Probleme mit dem ONTAP System Manager oder der ONTAP CLI beheben. Ihr Unternehmen befolgt möglicherweise nicht alle Empfehlungen, daher müssen Sie in einigen Fällen keine Änderungen vornehmen.

Siehe "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9" (TR-4569) Detaillierte Empfehlungen und Lösungen.

Zusätzlich zum Berichten des Sicherheitsstatus generiert Unified Manager auch Sicherheitsereignisse für alle Cluster oder SVMs mit Sicherheitsverletzungen. Sie können diese Probleme auf der Seite „Ereignismanagement-Bestand“ verfolgen und Warnmeldungen für diese Ereignisse so konfigurieren, dass Ihr Speicheradministrator benachrichtigt wird, wenn neue Sicherheitsereignisse auftreten.

Welche Sicherheitskriterien werden bewertet

Im Allgemeinen werden die Sicherheitskriterien für Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes im Vergleich zu den im „ *NetApp Security Hardening Guide for ONTAP 9*“ definierten Empfehlungen evaluiert.

Einige der Sicherheitsprüfungen umfassen:

- Gibt an, ob ein Cluster eine sichere Authentifizierungsmethode wie SAML verwendet
- Unabhängig davon, ob Peering-Cluster ihre Kommunikation verschlüsselt haben
- Gibt an, ob das Auditprotokoll auf einer Storage-VM aktiviert ist
- Ob Ihre Volumes eine Software- oder Hardwareverschlüsselung aktiviert haben

Weitere Informationen finden Sie unter Compliance-Kategorien und im "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9" Ausführliche Informationen finden Sie unter.

> Auch Upgrade-Ereignisse, die von der Active IQ-Plattform gemeldet werden, gelten als Sicherheitsereignisse. Diese Ereignisse erkennen Probleme, wenn für die Lösung ein Upgrade der ONTAP Software, Node-Firmware oder Betriebssystemsoftware erforderlich ist (für Sicherheitsempfehlungen). Diese Ereignisse werden nicht im Fenster „Sicherheit“ angezeigt, sind aber auf der Seite „Ereignisverwaltung“ verfügbar.

Cluster-Compliance-Kategorien

In dieser Tabelle werden die Parameter für die Einhaltung der Cluster-Sicherheits-Compliance beschrieben, die von Unified Manager bewertet werden, die Empfehlung von NetApp und ob der Parameter sich auf die allgemeine Bestimmung des Clusters auswirkt, das eine Beschwerde ist oder nicht.

Die Verfügbarkeit nicht konformer SVMs auf einem Cluster wirkt sich auf den Compliance-Wert des Clusters aus. In einigen Fällen müssen Sie also möglicherweise ein Sicherheitsprobleme mit einer SVM beheben, bevor Ihre Cluster-Sicherheit konform erkannt wird.

Beachten Sie, dass nicht alle unten aufgeführten Parameter für alle Installationen angezeigt werden. Wenn Sie beispielsweise keine Peered Cluster haben oder AutoSupport auf einem Cluster deaktiviert haben, werden die Elemente Cluster Peering oder AutoSupport HTTPS Transport auf der UI-Seite nicht angezeigt.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Globaler FIPS	Gibt an, ob der Compliance-Modus Global FIPS (Federal Information Processing Standard) 140-2 aktiviert oder deaktiviert ist. Wenn FIPS aktiviert ist, sind TLSv1 und SSLv3 deaktiviert und nur TLSv1.1 und TLSv1.2 zulässig.	Aktiviert	Ja.
Telnet	Gibt an, ob Telnet-Zugriff auf das System aktiviert oder deaktiviert ist. NetApp empfiehlt Secure Shell (SSH) für den sicheren Remote-Zugriff.	Deaktiviert	Ja.
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit *cbc beginnen.	Nein	Ja.
Anmelde-Banner	Zeigt an, ob das Anmeldebanner für Benutzer, die auf das System zugreifen, aktiviert oder deaktiviert ist.	Aktiviert	Ja.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Cluster-Peering	Gibt an, ob die Kommunikation zwischen Peering-Clustern verschlüsselt oder unverschlüsselt ist. Für diesen Parameter muss sowohl auf den Quell- als auch auf den Ziel-Clustern konfiguriert werden, damit er als konform betrachtet werden kann.	Verschlüsselt	Ja.
Network Time Protocol	Gibt an, ob das Cluster über einen oder mehrere konfigurierte NTP-Server verfügt. Aus Gründen der Redundanz und des besten Service empfiehlt NetApp, mindestens drei NTP-Server mit dem Cluster zu verknüpfen.	Konfiguriert	Ja.
OCSP	Gibt an, ob in ONTAP Anwendungen vorhanden sind, die nicht mit OCSP konfiguriert sind (Online Certificate Status Protocol) und daher keine Verschlüsselung der Kommunikation erfolgt. Die nicht kompatiblen Anwendungen werden aufgelistet.	Aktiviert	Nein
Remote Audit-Protokollierung	Gibt an, ob die Protokollweiterleitung (Syslog) verschlüsselt ist oder nicht verschlüsselt ist.	Verschlüsselt	Ja.
AutoSupport HTTPS-Übertragung	Zeigt an, ob HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an den NetApp Support verwendet wird.	Aktiviert	Ja.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Standard-Admin-Benutzer	Gibt an, ob der standardmäßige Admin-Benutzer (integriert) aktiviert oder deaktiviert ist. NetApp empfiehlt, alle nicht benötigten integrierten Konten zu sperren (zu deaktivieren).	Deaktiviert	Ja.
SAML-Benutzer	Gibt an, ob SAML konfiguriert ist. Mit SAML können Sie Multi-Faktor-Authentifizierung (MFA) als Anmeldemethode für Single-Sign-On konfigurieren.	Nein	Nein
Active Directory-Benutzer	Gibt an, ob Active Directory konfiguriert ist. Active Directory und LDAP sind die bevorzugten Authentifizierungsmechanismen für Benutzer, die auf Cluster zugreifen.	Nein	Nein
LDAP-Benutzer	Gibt an, ob LDAP konfiguriert ist. Active Directory und LDAP sind die bevorzugten Authentifizierungsmechanismen für Benutzer, die Cluster über lokale Benutzer managen.	Nein	Nein
Zertifikatbenutzer	Zeigt an, ob ein Zertifikatbenutzer zur Anmeldung beim Cluster konfiguriert ist.	Nein	Nein
Lokale Benutzer	Zeigt an, ob lokale Benutzer für die Anmeldung am Cluster konfiguriert sind.	Nein	Nein

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
Remote Shell	Zeigt an, ob RSH aktiviert ist. Aus Sicherheitsgründen sollte RSH deaktiviert werden. Vorzugsweise ist Secure Shell (SSH) für sicheren Remote-Zugriff.	Deaktiviert	Ja.
MD5 wird verwendet	Zeigt an, ob ONTAP-Benutzerkonten die weniger sichere MD5-Hash-Funktion verwenden. Die MD5-Hashed-Benutzerkonten-Migration auf die sicherere kryptografische Hash-Funktion wie SHA-512 wird bevorzugt.	Nein	Ja.
Zertifikataussteller Typ	Gibt den Typ des verwendeten digitalen Zertifikats an.	CA-signiert	Nein

Compliance-Kategorien für Storage-VMs

Diese Tabelle beschreibt die Compliance-Kriterien für die Storage Virtual Machine (SVM), die von Unified Manager bewertet werden, die NetApp Empfehlung und ob der Parameter sich auf die allgemeine Feststellung einer Beschwerde bzw. nicht auf eine Beschwerde des SVM auswirkt.

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM-Compliance
Überwachungsprotokoll	Gibt an, ob die Überwachungsprotokollierung aktiviert oder deaktiviert ist.	Aktiviert	Ja.
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, z. B. Chiffren, die mit beginnen `cbc*`.	Nein	Ja.

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM-Compliance
Anmelde-Banner	Zeigt an, ob das Anmeldebanner für Benutzer, die auf SVMs im System zugreifen, aktiviert oder deaktiviert ist.	Aktiviert	Ja.
LDAP-Verschlüsselung	Gibt an, ob LDAP-Verschlüsselung aktiviert oder deaktiviert ist.	Aktiviert	Nein
NTLM-Authentifizierung	Gibt an, ob die NTLM-Authentifizierung aktiviert oder deaktiviert ist.	Aktiviert	Nein
LDAP Payload-Signatur	Gibt an, ob LDAP-Payload-Signatur aktiviert oder deaktiviert ist.	Aktiviert	Nein
CHAP-Einstellungen	Gibt an, ob CHAP aktiviert oder deaktiviert ist.	Aktiviert	Nein
Kerberos V5	Gibt an, ob die Kerberos-V5-Authentifizierung aktiviert oder deaktiviert ist.	Aktiviert	Nein
NIS-Authentifizierung	Gibt an, ob die Verwendung der NIS-Authentifizierung konfiguriert ist.	Deaktiviert	Nein
FPolicy Status aktiv	Zeigt an, ob FPolicy erstellt wird oder nicht.	Ja.	Nein
SMB-Verschlüsselung aktiviert	Gibt an, ob SMB -Signing & Sealing nicht aktiviert ist.	Ja.	Nein
SMB-Signatur aktiviert	Gibt an, ob SMB -Signing nicht aktiviert ist.	Ja.	Nein

Volume Compliance-Kategorien

Diese Tabelle beschreibt die Verschlüsselungsparameter des Volumes, die von Unified Manager geprüft werden, um zu ermitteln, ob die Daten auf Ihren Volumes vor dem

Zugriff durch unbefugte Benutzer angemessen geschützt sind.

Zu beachten ist, dass die Verschlüsselungsparameter des Volumes keine Auswirkung haben, ob das Cluster oder die Storage-VM als konform betrachtet wird.

Parameter	Beschreibung
Softwareverschlüsselung	Zeigt die Anzahl der Volumes an, die mit Softwarelösungen für die NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) gesichert sind.
Hardware Verschlüsselt	Zeigt die Anzahl der Volumes an, die mit NSE-Hardwareverschlüsselung (NetApp Storage Encryption) gesichert sind.
Verschlüsselt für Software und Hardware	Zeigt die Anzahl der Volumes an, die sowohl durch Software- als auch durch Hardwareverschlüsselung geschützt sind.
Nicht Verschlüsselt	Zeigt die Anzahl der nicht verschlüsselten Volumes an.

Was bedeutet nicht, dass Compliance-Anforderungen erfüllt werden

Cluster und Storage Virtual Machines (SVMs) gelten als nicht kompatibel, wenn eine der untersuchten Sicherheitskriterien den im *NetApp Security Hardening Guide for ONTAP 9* definierten Empfehlungen entsprechen. Darüber hinaus gilt ein Cluster als nicht kompatibel, wenn eine SVM als nicht konform gekennzeichnet ist.

Die Statussymbole in den Sicherheitskarten haben in Bezug auf ihre Konformität die folgende Bedeutung:

- - Der Parameter ist wie empfohlen konfiguriert.
- - Der Parameter ist nicht wie empfohlen konfiguriert.
- - Entweder die Funktion ist auf dem Cluster nicht aktiviert oder der Parameter wurde nicht als empfohlen konfiguriert, aber dieser Parameter trägt nicht zur Compliance des Objekts bei.

Beachten Sie, dass der Volume-Verschlüsselungsstatus nicht dazu beiträgt, ob das Cluster oder die SVM als konform betrachtet werden.

Anzeigen des Sicherheitsstatus für Cluster und Storage VMs

Active IQ Unified Manager ermöglicht Ihnen, den Sicherheitsstatus der Storage-Objekte in Ihrer Umgebung von verschiedenen Punkten der Schnittstelle aus anzuzeigen. Sie können Informationen und Berichte auf der Basis definierter Parameter erfassen und

analysieren und verdächtige Verhaltensweisen oder nicht autorisierte Systemänderungen auf den überwachten Clustern und Storage-VMs erkennen.

Informationen zu den Sicherheitsempfehlungen finden Sie im "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9"

Anzeigen des Sicherheitsstatus auf Objektebene auf der Sicherheitsseite

Als Systemadministrator können Sie die Seite **Sicherheit** verwenden, um einen Überblick über die Sicherheitskraft Ihrer ONTAP Cluster und Storage VMs auf Datacenter- und Standortebene zu erhalten. Die unterstützten Objekte sind Cluster, Storage VMs und Volumes. Führen Sie hierzu folgende Schritte aus:

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Je nachdem, ob Sie den Sicherheitsstatus für alle überwachten Cluster oder für einen einzelnen Cluster anzeigen möchten, wählen Sie **Alle Cluster** oder wählen Sie einen einzelnen Cluster aus dem Dropdown-Menü aus.
3. Klicken Sie im Fenster **Sicherheit** auf den Rechtspfeil. Die Seite Sicherheit wird angezeigt.

Klicken Sie auf die Balkendiagramme, -Zählungen und `View Reports` Über Links gelangen Sie zur Seite Volumes, Cluster oder Storage VMs, auf der Sie die entsprechenden Details anzeigen oder Berichte erstellen können.

Auf der Seite Sicherheit werden die folgenden Felder angezeigt:

- **Cluster Compliance**: Der Sicherheitsstatus (Anzahl der Cluster, die konform sind oder nicht kompatibel sind) aller Cluster in einem Rechenzentrum
- **Storage VM Compliance**: Der Sicherheitsstatus (Anzahl der konformen oder nicht konformen Storage VMs) für alle Storage VMs in Ihrem Datacenter
- **Volume Encryption**: Der Volume-Verschlüsselungsstatus (Anzahl der verschlüsselten oder nicht verschlüsselten Volumes) aller Volumes in Ihrer Umgebung
- **Volume Anti-Ransomware Status**: Der Sicherheitsstatus (Anzahl der Volumes mit aktivierter oder deaktivierter Anti-Ransomware-Funktion) aller Volumes in Ihrer Umgebung
- **Clusterauthentifizierung und Zertifikate**: Die Anzahl der Cluster, die jede Art von Authentifizierungsmethode verwenden, wie SAML, Active Directory oder über Zertifikate und lokale Authentifizierung. Im Panel wird auch die Anzahl der Cluster angezeigt, deren Zertifikate entweder abgelaufen sind oder in 60 Tagen ablaufen.

Zeigen Sie auf der Seite Cluster die Sicherheitsdetails aller Cluster an

Auf der Seite **Cluster / Security** Details können Sie den Sicherheits-Compliance-Status auf Clusterebene anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage > Cluster**.
2. Wählen Sie **Ansicht > Sicherheit > Alle Cluster**.

Standardsicherheitsparameter wie Global FIPS, Telnet, unsichere SSH-Einstellungen, Anmeldebanner, Netzwerkzeitprotokoll, AutoSupport HTTPS-Transport und der Status des Cluster-Zertifikats werden angezeigt.

Sie können auf klicken ⋮ Weitere Optionen und wählen Sie, um die Sicherheitsinformationen auf der Seite **Sicherheit** von Unified Manager oder auf System Manager anzuzeigen. Sie sollten gültige Anmeldeinformationen zum Anzeigen der Details in System Manager haben.

> Wenn ein Cluster ein abgelaufenes Zertifikat besitzt, können Sie auf klicken `expired` Unter **Cluster Certificate Validität**, und erneuern Sie es von System Manager (9.10.1 und höher). Sie können nicht auf klicken `expired` Wenn die System Manager Instanz eine Version vor 9.10.1 enthält.

Details zur Sicherheit aller Cluster finden Sie auf der Seite Storage-VMs

Auf der Seite **Storage VMs / Security** Details können Sie den Sicherheits-Compliance-Status auf Storage VM-Ebene anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage > Storage VMs**.
2. Wählen Sie **Ansicht > Sicherheit > Alle Storage VMs**. Es wird eine Liste der Cluster mit den Sicherheitsparametern angezeigt.

Sie können die Sicherheitskonformität der Speicher-VMs standardmäßig anzeigen, indem Sie die Sicherheitsparameter wie Storage-VMs, Cluster, Anmeldebanner, Revisionsprotokoll und unsichere SSH-Einstellungen überprüfen.

Sie können auf klicken ⋮ Weitere Optionen und wählen Sie, um die Sicherheitsinformationen auf der Seite **Sicherheit** von Unified Manager oder auf System Manager anzuzeigen. Sie sollten gültige Anmeldeinformationen zum Anzeigen der Details in System Manager haben.

Einzelheiten zur Sicherheit gegen Ransomware-Angriffe für Volumes und Storage-VMs finden Sie unter "Anzeigen des Anti-Ransomware-Status aller Volumes und Storage-VMs".

Anzeigen von Sicherheitsereignissen, für die möglicherweise Software- oder Firmware-Updates erforderlich sind

Es gibt bestimmte Sicherheitsereignisse, die einen Impact-Bereich von „`Upgrade`“ haben. Diese Ereignisse werden von der Active IQ Plattform gemeldet. Sie erkennen Probleme, wenn für die Lösung ein Upgrade der ONTAP Software, der Node-Firmware oder der Betriebssystemsoftware (für Sicherheitsempfehlungen) erforderlich ist.

Was Sie brauchen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Möglicherweise möchten Sie für einige dieser Probleme sofortige Korrekturmaßnahmen durchführen, während andere Probleme möglicherweise bis zur nächsten geplanten Wartung warten können. Sie können alle diese Ereignisse anzeigen und sie Benutzern zuweisen, die die Probleme lösen können. Außerdem können Sie anhand dieser Liste bestimmte Ereignisse für Sicherheitsaspekte identifizieren, über die Sie keine Benachrichtigung erhalten möchten, damit Sie diese Ereignisse deaktivieren können.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**.

   Standardmäßig werden alle aktiven (neuen und bestätigten) Ereignisse auf der Seite „Ereignismanagement-Bestand“ angezeigt.

2. Wählen Sie im Menü Ansicht die Option **Ereignisse aktualisieren** aus.

   Auf der Seite werden alle aktiven Sicherheitsereignisse für Upgrades angezeigt.

Anzeige des Managements der Benutzerauthentifizierung auf allen Clustern

Auf der Seite Sicherheit werden die Authentifizierungstypen angezeigt, die zur Authentifizierung von Benutzern in jedem Cluster verwendet werden, sowie die Anzahl der Benutzer, die mit jedem Typ auf das Cluster zugreifen. So können Sie überprüfen, ob die Benutzerauthentifizierung gemäß den Anforderungen Ihres Unternehmens sicher durchgeführt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Wählen Sie oben im Dashboard im Dropdown-Menü * Alle Cluster* aus.
3. Klicken Sie im Fenster **Sicherheit** auf den rechten Pfeil, und die Seite **Sicherheit** wird angezeigt.
4. Zeigen Sie die **Cluster Authentication**-Karte an, um die Anzahl der Benutzer anzuzeigen, die mit jedem Authentifizierungstyp auf das System zugreifen.
5. Zeigen Sie die **Cluster Security**-Karte an, um die Authentifizierungsmechanismen anzuzeigen, die zur Authentifizierung von Benutzern in jedem Cluster verwendet werden.

Wenn einige Benutzer über eine unsichere Methode auf das System zugreifen oder eine Methode verwenden, die von NetApp nicht empfohlen wird, können Sie die Methode deaktivieren.

Anzeigen des Verschlüsselungsstatus aller Volumes

Sie können eine Liste aller Volumes und ihren aktuellen Verschlüsselungsstatus anzeigen, um zu ermitteln, ob die Daten auf Ihren Volumes vor dem Zugriff durch nicht autorisierte Benutzer angemessen geschützt sind.

Was Sie brauchen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Auf ein Volume können folgende Verschlüsselungsarten angewendet werden:

- Software – Volumes, die mit Hilfe von NetApp Volume Encryption (NVE) oder NetApp Software-Verschlüsselungslösungen (NAE) gesichert werden.
- Hardware – Volumes, die mit der Hardware-Verschlüsselung von NetApp Storage Encryption (NSE) gesichert werden.
- Software- und Hardware-Volumes, die sowohl durch Software- als auch durch Hardware-Verschlüsselung geschützt sind.

- Keine - Volumen, die nicht verschlüsselt sind.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Gesundheit** > **Volumen-Verschlüsselung**
3. Sortieren Sie in der Ansicht **Health: Volumes Encryption** das Feld **Verschlüsselungstyp**, oder verwenden Sie den Filter, um Volumes mit einem bestimmten Verschlüsselungstyp anzuzeigen oder die nicht verschlüsselt sind (Verschlüsselungstyp von „`Keine`“).

Anzeigen des Anti-Ransomware-Status aller Volumes und Storage-VMs

Eine Liste aller Volumes und Storage VMs (SVMs) und ihres aktuellen Status gegen Ransomware können Sie feststellen, ob die Daten auf Ihren Volumes und SVMs ausreichend vor Ransomware-Angriffen geschützt sind.

Was Sie brauchen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Weitere Informationen zu den verschiedenen Status gegen Ransomware finden Sie unter "ONTAP: Anti-Ransomware".

Anzeigen der Sicherheitsinformationen aller Volumes mit Ransomware-Erkennung

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage** > **Volumes**.
2. Wählen Sie im Menü Ansicht die Option **Gesundheit** > **Sicherheit** > **Anti-Ransomware**
3. In der **Sicherheit: Anti-Ransomware** Ansicht können Sie nach den verschiedenen Feldern sortieren oder den Filter verwenden.

> Anti-Ransomware wird nicht für Offline Volumes, eingeschränkte Volumes, SnapLock Volumes, FlexGroup Volumes, FlexCache Volumes und SAN-only Volumes, Volumes von angestoppten Storage-VMs, Root-Volumes von Storage-VMs oder Datensicherungs-Volumes

Anzeigen der Sicherheitsinformationen aller Storage-VMs mit Ransomware-Erkennung

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage > Storage VMs**.
2. Wählen Sie **Ansicht > Sicherheit > Anti-Ransomware**. Eine Liste der SVMs mit dem Ransomware-Status wird angezeigt.

> Das Ransomware-Monitoring wird auf Storage-VMs, die kein NAS-Protokoll besitzen, nicht unterstützt.

Anzeigen aller aktiven Sicherheitsereignisse

Sie können alle aktiven Sicherheitsereignisse anzeigen und sie anschließend einem Benutzer zuweisen, der das Problem lösen kann. Wenn bestimmte Sicherheitsereignisse vorliegen, die Sie nicht empfangen möchten, kann Ihnen diese Liste helfen, die Ereignisse zu identifizieren, die Sie deaktivieren möchten.

Was Sie brauchen

Sie müssen über die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisverwaltung**.

   Standardmäßig werden neue und bestätigte Ereignisse auf der Seite „Ereignismanagement-Bestand“ angezeigt.

2. Wählen Sie im Menü Ansicht die Option **Aktive Sicherheitsereignisse** aus.

   Auf der Seite werden alle neuen und bestätigten Sicherheitsereignisse angezeigt, die in den letzten 7 Tagen generiert wurden.

Hinzufügen von Warnmeldungen für Sicherheitsereignisse

Sie können Benachrichtigungen für einzelne Sicherheitsereignisse so konfigurieren, wie es auch bei allen anderen Ereignissen, die Unified Manager empfangen hat. Wenn Sie außerdem alle Sicherheitsereignisse gleich behandeln und E-Mails an dieselbe Person senden möchten, können Sie eine einzelne Benachrichtigung erstellen, um Sie darüber zu informieren, wenn Sicherheitsereignisse ausgelöst werden.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Das folgende Beispiel zeigt, wie eine Warnung für das Sicherheitsereignis „`Telnet Protocol Enabled`“ erstellt wird. Dadurch wird eine Meldung ausgegeben, wenn ein Telnet-Zugriff für den Remote-Administratorzugriff auf das Cluster konfiguriert ist. Sie können diese Methode verwenden, um Warnungen für alle Sicherheitsereignisse zu erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Alarm-Setup**.
2. Klicken Sie auf der Seite **Alarm-Setup** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Alarm hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für den Alarm ein.
4. Klicken Sie auf **Ressourcen** und wählen Sie den Cluster oder den Cluster aus, auf dem Sie diese Warnung aktivieren möchten.
5. Klicken Sie auf **Events** und führen Sie die folgenden Aktionen aus:
   a. Wählen Sie in der Liste Ereignis Severity die Option **Warnung** aus.

b. Wählen Sie in der Liste passende Ereignisse die Option **Telnet-Protokoll aktiviert**.

6. Klicken Sie auf **Aktionen** und wählen Sie dann den Namen des Benutzers aus, der die Benachrichtigung per E-Mail im Feld * Diese Benutzer benachrichtigen* erhält.
7. Konfigurieren Sie alle anderen Optionen auf dieser Seite, um die Benachrichtigungshäufigkeit zu erhöhen, SNMP-Taps auszugeben und ein Skript auszuführen.
8. Klicken Sie Auf **Speichern**.

Bestimmte Sicherheitsereignisse deaktivieren

Standardmäßig sind alle Ereignisse aktiviert. Sie können bestimmte Ereignisse deaktivieren, um die Generierung von Benachrichtigungen für Ereignisse zu verhindern, die in Ihrer Umgebung nicht wichtig sind. Sie können Ereignisse aktivieren, die deaktiviert sind, wenn Sie den Empfang von Benachrichtigungen für sie fortsetzen möchten.

Was Sie brauchen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn Sie Ereignisse deaktivieren, werden die zuvor generierten Ereignisse im System als veraltet markiert und die für diese Ereignisse konfigurierten Warnmeldungen werden nicht ausgelöst. Wenn Sie deaktivierte Ereignisse aktivieren, werden die Benachrichtigungen für diese Ereignisse mit dem nächsten Überwachungszyklus generiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Storage-Management** > **Event-Setup**.
2. Deaktivieren oder aktivieren Sie auf der Seite * Event* die Ereignisse, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren von Ereignissen	a. Klicken Sie Auf **Deaktivieren**. b. Wählen Sie im Dialogfeld Ereignisse deaktivieren den Schweregrad * Warnung* aus. Dies ist die Kategorie für alle Sicherheitsereignisse. c. Wählen Sie in der Spalte Abpassende Ereignisse die zu deaktivierenden Sicherheitsereignisse aus, und klicken Sie dann auf den rechten Pfeil, um diese Ereignisse in die Spalte Ereignisse deaktivieren zu verschieben. d. Klicken Sie auf **Speichern und Schließen**. e. Stellen Sie sicher, dass die deaktivierten Ereignisse in der Listenansicht der Seite Event Setup angezeigt werden.

Ihr Ziel ist	Dann tun Sie das…
Aktivieren von Ereignissen	a. Aktivieren Sie in der Liste der deaktivierten Ereignisse das Kontrollkästchen für das Ereignis oder die Ereignisse, die Sie erneut aktivieren möchten. b. Klicken Sie Auf **Aktivieren**.

Sicherheitsereignisse

Sicherheitsereignisse ermöglichen Ihnen Informationen zum Sicherheitsstatus von ONTAP Clustern, Storage Virtual Machines (SVMs) und Volumes auf der Grundlage von Parametern, die im „ *NetApp Security Hardening Guide for ONTAP 9*“ definiert sind. Diese Ereignisse benachrichtigen Sie über potenzielle Probleme, sodass Sie den Schweregrad Ihrer Maßnahmen überprüfen und das Problem ggf. beheben können.

Sicherheitsereignisse werden nach Quelltyp gruppiert und enthalten den Ereignis- und Trap-Namen, den Impact-Level und den Schweregrad. Diese Ereignisse werden in den Ereigniskategorien für Cluster und Storage-VMs angezeigt.