Verwalten von Zielen für die Cluster-Sicherheit

Active IQ Unified Manager 9.9

NetApp
January 31, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-99/health-checker/reference-cluster-compliance-categories.html on January 31, 2025. Always check docs.netapp.com for the latest.

Inhalt

Verwalten von Zielen für die Cluster-Sicherheit . . . 1
- Welche Sicherheitskriterien werden bewertet . . . 1
- Was bedeutet nicht, dass Compliance-Anforderungen erfüllt werden . . . 6
- Anzeigen des Sicherheitsstatus eines Clusters im hohen Level . . . 6
- Anzeigen des detaillierten Sicherheitsstatus für Cluster und SVMs . . . 7
- Anzeigen von Sicherheitsereignissen, für die möglicherweise Software- oder Firmware-Updates erforderlich sind . . . 8
- Anzeige des Managements der Benutzerauthentifizierung auf allen Clustern . . . 8
- Anzeigen des Verschlüsselungsstatus aller Volumes . . . 9
- Anzeigen aller aktiven Sicherheitsereignisse . . . 9
- Hinzufügen von Warnmeldungen für Sicherheitsereignisse . . . 10
- Bestimmte Sicherheitsereignisse deaktivieren . . . 11
- Sicherheitsereignisse . . . 12

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.

Detaillierte Empfehlungen und Entschließungen finden Sie im "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9" (TR-4569).

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

Ausführliche Informationen finden Sie in den Themen zu Compliance-Kategorien und im "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9" .

> 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 beginnen `*cbc`.	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.	Keine Empfehlungen	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.	Keine Empfehlungen	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.	Keine Empfehlungen	Nein
Zertifikatbenutzer	Zeigt an, ob ein Zertifikatbenutzer zur Anmeldung beim Cluster konfiguriert ist.	Keine Empfehlungen	Nein
Lokale Benutzer	Zeigt an, ob lokale Benutzer für die Anmeldung am Cluster konfiguriert sind.	Keine Empfehlungen	Nein

SVM-Compliance-Kategorien

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.
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

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 eines Clusters im hohen Level

Das Security Panel im Unified ManagerDashboard zeigt abhängig von der aktuellen Ansicht den allgemeinen Sicherheitsstatus aller Cluster oder für ein einzelnes Cluster an.

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. Öffnen Sie das Fenster **Sicherheit**, um den Gesamtstatus anzuzeigen.

   In diesem Fenster wird Folgendes angezeigt:

   - Eine Liste der Sicherheitsereignisse, die in den letzten 24 Stunden eingehen
   - Ein Link von jeder dieser Veranstaltungen zur Seite Veranstaltungsdetails
   - Ein Link, mit dem Sie alle aktiven Sicherheitsereignisse auf der Seite „Ereignisverwaltung“ anzeigen können
   - Cluster-Sicherheitsstatus (Anzahl an kompatiblen oder nicht kompatiblen Clustern)
   - Der SVM-Sicherheitsstatus (Anzahl an konformen oder nicht konformen SVMs)
   - Status der Volume-Verschlüsselung (Anzahl der verschlüsselten oder nicht verschlüsselten Volumes)
4. Klicken Sie auf den Rechtspfeil oben im Bedienfeld, um die Sicherheitsinformationen auf der Seite **Sicherheit** anzuzeigen.

Anzeigen des detaillierten Sicherheitsstatus für Cluster und SVMs

Die Seite Sicherheit zeigt den allgemeinen Sicherheitsstatus aller Cluster sowie einen detaillierten Sicherheitsstatus für einzelne Cluster an. Der detaillierte Cluster-Status umfasst Cluster-Compliance, SVM-Compliance und Volume-Verschlüsselung.

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.

   Auf der Seite Sicherheit werden die folgenden Informationen angezeigt:

   - Cluster-Sicherheitsstatus (Anzahl an kompatiblen oder nicht kompatiblen Clustern)
   - Der SVM-Sicherheitsstatus (Anzahl an konformen oder nicht konformen SVMs)
   - Status der Volume-Verschlüsselung (Anzahl der verschlüsselten oder nicht verschlüsselten Volumes)
   - Die Cluster-Authentifizierungsmethoden, die in den einzelnen Clustern verwendet werden
4. Eine Anleitung, wie Sie alle Ihre Cluster, SVMs und Volumes mit den NetApp Sicherheitsempfehlungen konform gestalten, finden Sie im "NetApp Leitfaden zur verstärkte Sicherheit in ONTAP 9" .

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.

Bevor Sie beginnen

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

Über diese Aufgabe

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.

Ergebnisse

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.

Bevor Sie beginnen

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

Über diese Aufgabe

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**Encryption Type**, oder verwenden Sie den Filter, um Volumes anzuzeigen, die einen bestimmten Verschlüsselungstyp haben, oder die nicht verschlüsselt sind (Verschlüsselungstyp von “None”).

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.

Bevor Sie beginnen

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.

Bevor Sie beginnen

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

Über diese Aufgabe

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.

Bevor Sie beginnen

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

Über diese Aufgabe

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 Setup* Ereignisse, indem Sie eine der folgenden Optionen auswählen:

Ihr Ziel ist	Dann tun Sie das…
Deaktivieren von Ereignissen	1. Klicken Sie Auf **Deaktivieren**. 2. Wählen Sie im Dialogfeld Ereignisse deaktivieren den Schweregrad * Warnung* aus. Dies ist die Kategorie für alle Sicherheitsereignisse. 3. 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. 4. Klicken Sie auf **Speichern und Schließen**. 5. 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	1. Aktivieren Sie in der Liste der deaktivierten Ereignisse das Kontrollkästchen für das Ereignis oder die Ereignisse, die Sie erneut aktivieren möchten. 2. 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.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.