# Cluster-Sicherheitsziele managen

## Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-918/health-checker/concept_manage_cluster_security_objectives.html on November 13, 2026. Always check docs.netapp.com for the latest.

# Inhalt


Cluster-Sicherheitsziele managen . . . 1
- Verwalten von Cluster-Sicherheitszielen in Active IQ Unified Manager . . . 1
- Welche Sicherheitskriterien werden bewertet . . . 1
  - Informationen dazu, wie Active IQ Unified Manager Sicherheitskriterien auswertet . . . 1
  - Cluster Compliance Kategorien in Active IQ Unified Manager . . . 2
  - Grundlegendes zu den Konformitätskategorien von Storage VMs in Active IQ Unified Manager . . . 5
  - Konformitätskategorien für Volumes in Active IQ Unified Manager . . . 6
- Informationen zum Compliance-Status von Clustern und SVMs in Active IQ Unified Manager . . . 7
- Sicherheitsstatus für Cluster und Storage VMs in Active IQ Unified Manager anzeigen . . . 7
  - Anzeigen des Sicherheitsstatus auf Objektebene auf der Seite „Sicherheit“ . . . 7
  - Die Sicherheitsdetails aller Cluster finden Sie auf der Seite „Clusters“. . . . 8
  - Die Sicherheitsdetails aller Cluster sind auf der Seite „Storage VMs“ einsehbar. . . . 8
- Sicherheitsereignisse, die möglicherweise Software- oder Firmware-Updates in Active IQ Unified Manager erfordern, können angezeigt werden . . . 9
- Anzeige, wie Cluster die Benutzerauthentifizierung auf allen Clustern in Active IQ Unified Manager verwalten . . . 9
- Der Verschlüsselungsstatus aller Volumes in Active IQ Unified Manager kann angezeigt werden . . . 10
- Der Anti-Ransomware-Status aller Volumes und Speicher-VMs in Active IQ Unified Manager kann angezeigt werden . . . 10
  - Sicherheitsdetails aller Volumes mit Anti-Ransomware-Erkennung . . . 11
  - Anzeige der Sicherheitsdetails aller Storage VMs mit Anti-Ransomware-Erkennung . . . 11
- Alle aktiven Sicherheitsereignisse in Active IQ Unified Manager anzeigen . . . 11
- Hinzufügen von Warnmeldungen für Sicherheitsereignisse in Active IQ Unified Manager . . . 12
- Deaktivieren bestimmter Sicherheitsereignisse in Active IQ Unified Manager . . . 12
- Sicherheitsereignisse in Active IQ Unified Manager anzeigen . . . 13

# Cluster-Sicherheitsziele managen

## Verwalten von Cluster-Sicherheitszielen in Active IQ Unified Manager

Unified Manager bietet ein Dashboard, das identifiziert, wie sicher Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes auf Basis der im *NetApp Security Hardening Guide for ONTAP 9* definierten Empfehlungen sind.

Ziel des Sicherheits-Dashboards ist es, alle Bereiche anzuzeigen, in denen Ihre ONTAP Cluster nicht mit den von NetApp empfohlenen Richtlinien übereinstimmen, sodass diese potenziellen Probleme behoben werden können. In den meisten Fällen werden die Probleme mithilfe von ONTAP System Manager oder der ONTAP CLI behoben. Ihr Unternehmen befolgt möglicherweise nicht alle Empfehlungen, sodass in manchen Fällen keine Änderungen erforderlich sind.

Ausführliche Empfehlungen und Lösungen finden Sie im "NetApp Security Hardening Guide für ONTAP 9" (TR-4569).

Zusätzlich zur Meldung des Sicherheitsstatus generiert Unified Manager auch Sicherheitsereignisse für jeden Cluster oder jede SVM mit Sicherheitsverstößen. Sie können diese Probleme auf der Bestandsseite der Ereignisverwaltung verfolgen und Warnmeldungen für diese Ereignisse konfigurieren, sodass Ihr Storage-Administrator benachrichtigt wird, wenn neue Sicherheitsereignisse auftreten.

Weitere Informationen sind unter "Welche Sicherheitskriterien werden bewertet" verfügbar.

## Welche Sicherheitskriterien werden bewertet

### Informationen dazu, wie Active IQ Unified Manager Sicherheitskriterien auswertet

Im Allgemeinen werden die Sicherheitskriterien für Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes anhand der Empfehlungen im *NetApp Security Hardening Guide for ONTAP 9* bewertet.

Zu den Sicherheitsüberprüfungen gehören unter anderem:

- ob ein Cluster ein sicheres Authentifizierungsverfahren wie SAML verwendet
- ob die Kommunikation zwischen den Peer-Clustern verschlüsselt ist
- ob für eine Storage VM das Revisionsprotokoll aktiviert ist
- ob für Ihre Volumes Software- oder Hardwareverschlüsselung aktiviert ist

Ausführliche Informationen enthalten die Themen zu Compliance-Kategorien und dem "NetApp Security Hardening Guide für ONTAP 9".

> Upgrade-Ereignisse, die von der Active IQ Plattform gemeldet werden, gelten ebenfalls als Sicherheitsereignisse. Diese Ereignisse kennzeichnen Probleme, deren Behebung ein Upgrade der ONTAP Software, der Node-Firmware oder der Betriebssystemsoftware erfordert (bei Sicherheitshinweisen). Diese Ereignisse werden nicht im Sicherheitsbereich angezeigt, sind aber auf der Bestandsseite für Event Management verfügbar.

Weitere Informationen sind unter "Management von Cluster-Sicherheitszielen" verfügbar.

## Cluster Compliance Kategorien in Active IQ Unified Manager

Diese Tabelle beschreibt die Cluster-Sicherheits-Compliance-Parameter, die Unified Manager auswertet, die NetApp Empfehlung und ob der Parameter die Gesamtbewertung beeinflusst, ob der Cluster konform ist oder nicht.

Nicht konforme SVMs auf einem Cluster wirken sich auf den Compliance-Wert des Clusters aus. Daher kann es in manchen Fällen erforderlich sein, ein Sicherheitsproblem mit einer SVM zu beheben, bevor die Clustersicherheit als konform gilt.

Es ist zu beachten, dass nicht jeder der unten aufgeführten Parameter bei allen Installationen angezeigt wird. Wenn Sie beispielsweise keine Cluster-Peering-Beziehungen haben oder AutoSupport in einem Cluster deaktiviert haben, werden auf der UI-Seite die Elemente „Cluster Peering“ oder „AutoSupport HTTPS Transport“ nicht angezeigt.

| Parameter | Beschreibung | Empfehlung | Beeinträchtigt die Cluster-Compliance |
|---|---|---|---|
| Globales FIPS | Zeigt an, ob der globale FIPS (Federal Information Processing Standard) 140-2-Compliance-Modus aktiviert oder deaktiviert ist. Wenn FIPS aktiviert ist, sind TLSv1 und SSLv3 deaktiviert, und nur TLSv1.1 und TLSv1.2 sind zulässig. | Aktiviert | Ja |
| Telnet | Zeigt an, ob der Telnet-Zugriff auf das System aktiviert oder deaktiviert ist. NetApp empfiehlt Secure Shell (SSH) für einen sicheren Fernzugriff. | Deaktiviert | Ja |
| Unsichere SSH-Einstellungen | Zeigt an, ob SSH unsichere Verschlüsselungsverfahren verwendet, z. B. solche, die mit *cbc beginnen. | Nein | Ja |
| Anmeldebanner | Zeigt an, ob das Anmeldebanner für Benutzer, die auf das System zugreifen, aktiviert oder deaktiviert ist. | Aktiviert | Ja |

| Parameter | Beschreibung | Empfehlung | Beeinträchtigt die Cluster-Compliance |
|---|---|---|---|
| Cluster-Peering | Gibt an, ob die Kommunikation zwischen gepeerten Clustern verschlüsselt oder unverschlüsselt ist. Die Verschlüsselung muss sowohl auf dem Quell- als auch auf dem Zielcluster konfiguriert sein, damit dieser Parameter als konform gilt. | Verschlüsselt | Ja |
| Netzwerkzeitprotokoll | Zeigt an, ob der Cluster einen oder mehrere konfigurierte NTP-Server besitzt. Für Redundanz und optimalen Service empfiehlt NetApp, dem Cluster mindestens drei NTP-Server zuzuordnen. | Konfiguriert | Ja |
| OCSP | Ab 9.14.1 stellt Active IQ Unified Manager Statusinformationen zum Online Certificate Status Protocol (OCSP) auf Ebene der Storage Virtual Machine (SVM, früher als Vserver bezeichnet) bereit. Dies bedeutet, dass die OCSP-Validierung auf alle zur SVM hergestellten SSL/TLS-Verbindungen angewendet wird und die Integrität und Gültigkeit der in diesen Verbindungen verwendeten Zertifikate sicherstellt. | Aktiviert | Nein |
| Remote-Revisionsprotokollierung | Gibt an, ob die Protokollweiterleitung (Syslog) verschlüsselt oder nicht verschlüsselt ist. | Verschlüsselt | Ja |
| AutoSupport HTTPS-Transport | Gibt an, ob HTTPS als Standardtransportprotokoll zum Senden von AutoSupport Nachrichten an den NetApp Support verwendet wird. | Aktiviert | Ja |

| Parameter | Beschreibung | Empfehlung | Beeinträchtigt die Cluster-Compliance |
|---|---|---|---|
| Standard-Admin-Benutzer | Zeigt an, ob der Standard-Administratorbenutzer (integriert) aktiviert oder deaktiviert ist. NetApp empfiehlt, nicht benötigte integrierte Konten zu sperren (zu deaktivieren). | Deaktiviert | Ja |
| SAML Benutzer | Zeigt an, ob SAML konfiguriert ist. SAML ermöglicht die Konfiguration der Multi-Faktor-Authentifizierung (MFA) als Anmeldemethode für Single Sign-On. | Nein | Nein |
| Active Directory Benutzer | Zeigt 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 gegenüber lokalen Benutzern die bevorzugten Authentifizierungsmechanismen für Benutzer, die Cluster verwalten. | Nein | Nein |
| Zertifikatsbenutzer | Zeigt an, ob ein Benutzerzertifikat für die Anmeldung am Cluster konfiguriert ist. | Nein | Nein |
| Lokale Benutzer | Zeigt an, ob lokale Benutzer für die Anmeldung am Cluster konfiguriert sind. | Nein | Nein |
| Remote Shell | Zeigt an, ob RSH aktiviert ist. Aus Sicherheitsgründen sollte RSH deaktiviert sein. Secure Shell (SSH) wird für sicheren Fernzugriff bevorzugt. | Deaktiviert | Ja |

| Parameter | Beschreibung | Empfehlung | Beeinträchtigt die Cluster-Compliance |
|---|---|---|---|
| MD5 im Einsatz | Zeigt an, ob ONTAP Benutzerkonten die weniger sichere MD5 Hashfunktion verwenden. Die Migration von MD5 gehashten Benutzerkonten zu einer sichereren kryptografischen Hashfunktion wie SHA-512 wird empfohlen. | Nein | Ja |
| Zertifikatsausstellertyp | Gibt die Art des verwendeten digitalen Zertifikats an. | CA-signiert | Nein |

## Grundlegendes zu den Konformitätskategorien von Storage VMs in Active IQ Unified Manager

Diese Tabelle beschreibt die Sicherheits-Compliance-Kriterien für Storage Virtual Machine (SVM), die Unified Manager auswertet, die NetApp Empfehlung und ob der Parameter die Gesamtbewertung beeinflusst, ob die SVM konform ist oder nicht.

| Parameter | Beschreibung | Empfehlung | Beeinträchtigt SVM Compliance |
|---|---|---|---|
| Audit-Protokoll | Zeigt an, ob die Audit-Protokollierung aktiviert oder deaktiviert ist. | Aktiviert | Ja |
| Unsichere SSH-Einstellungen | Zeigt an, ob SSH unsichere Verschlüsselungsverfahren verwendet, zum Beispiel solche, die mit `cbc*` beginnen. | Nein | Ja |
| Anmeldebanner | Zeigt an, ob das Anmeldebanner für Benutzer, die auf SVMs im System zugreifen, aktiviert oder deaktiviert ist. | Aktiviert | Ja |
| LDAP Verschlüsselung | Zeigt an, ob die LDAP-Verschlüsselung aktiviert oder deaktiviert ist. | Aktiviert | Nein |
| NTLM-Authentifizierung | Zeigt an, ob die NTLM-Authentifizierung aktiviert oder deaktiviert ist. | Aktiviert | Nein |

| Parameter | Beschreibung | Empfehlung | Beeinträchtigt SVM Compliance |
|---|---|---|---|
| LDAP Nutzdatensignierung | Zeigt an, ob die LDAP-Payload-Signierung aktiviert oder deaktiviert ist. | Aktiviert | Nein |
| CHAP Einstellungen | Zeigt an, ob CHAP aktiviert oder deaktiviert ist. | Aktiviert | Nein |
| Kerberos V5 | Zeigt an, ob die Kerberos V5 Authentifizierung aktiviert oder deaktiviert ist. | Aktiviert | Nein |
| NIS-Authentifizierung | Zeigt an, ob die Verwendung der NIS-Authentifizierung konfiguriert ist. | Deaktiviert | Nein |
| FPolicy Status Aktiv | Zeigt an, ob eine FPolicy erstellt wurde oder nicht. | Ja | Nein |
| SMB-Verschlüsselung aktiviert | Gibt an, ob SMB Signing und Sealing nicht aktiviert ist. | Ja | Nein |
| SMB Signierung aktiviert | Gibt an, ob die SMB Signierung nicht aktiviert ist. | Ja | Nein |

## Konformitätskategorien für Volumes in Active IQ Unified Manager

Diese Tabelle beschreibt die Parameter der Volumenverschlüsselung, die Unified Manager auswertet, um festzustellen, ob die Daten auf Ihren Volumes ausreichend vor dem Zugriff durch unbefugte Benutzer geschützt sind.

Die Parameter der Volume-Verschlüsselung haben keinen Einfluss darauf, ob der Cluster oder die Storage VM als konform gilt.

| Parameter | Beschreibung |
|---|---|
| Softwareverschlüsselt | Zeigt die Anzahl der Volumes an, die mit den Software-Verschlüsselungslösungen NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) geschützt sind. |
| Hardware-verschlüsselt | Zeigt die Anzahl der Volumes an, die mit der Hardwareverschlüsselung NetApp Storage Encryption (NSE) geschützt sind. |
| Software- und hardwareverschlüsselt | Zeigt die Anzahl der Volumes an, die sowohl durch Software- als auch durch Hardwareverschlüsselung geschützt sind. |

| Parameter | Beschreibung |
| --- | --- |
| Nicht verschlüsselt | Zeigt die Anzahl der nicht verschlüsselten Volumes an. |

# Informationen zum Compliance-Status von Clustern und SVMs in Active IQ Unified Manager

Clusters und Storage Virtual Machines (SVMs) gelten als nicht konform, wenn eines der Sicherheitskriterien, die anhand der Empfehlungen im *NetApp Security Hardening Guide for ONTAP 9* bewertet werden, nicht erfüllt ist. Zusätzlich gilt ein Cluster als nicht konform, wenn eine SVM als nicht konform gekennzeichnet ist.

Die Statussymbole auf den Sicherheitskarten haben in Bezug auf ihre Compliance die folgenden Bedeutungen:

- - Der Parameter ist wie empfohlen konfiguriert.
- - Der Parameter ist nicht wie empfohlen konfiguriert.
- - Entweder ist die Funktionalität im Cluster nicht aktiviert oder der Parameter ist nicht wie empfohlen konfiguriert, aber dieser Parameter trägt nicht zur Compliance des Objekts bei.

Der Status der Volume-Verschlüsselung hat keinen Einfluss darauf, ob der Cluster oder die SVM als konform gelten.

# Sicherheitsstatus für Cluster und Storage VMs in Active IQ Unified Manager anzeigen

Active IQ Unified Manager ermöglicht Ihnen, den Sicherheitsstatus der Storage Objekte in Ihrer Umgebung an verschiedenen Stellen der Benutzeroberfläche anzuzeigen. Sie können Informationen und Berichte anhand definierter Parameter erfassen und analysieren sowie verdächtiges Verhalten oder unautorisierte Systemänderungen auf den überwachten Clustern und Storage VMs erkennen.

Die Sicherheitsempfehlungen finden Sie unter "NetApp Security Hardening Guide für ONTAP 9"

## Anzeigen des Sicherheitsstatus auf Objektebene auf der Seite „Sicherheit“

Als Systemadministrator können Sie auf der Seite **Sicherheit** Transparenz über die Sicherheitsstärke Ihrer ONTAP Cluster und Storage VMs auf Datacenter- und Standortebene erhalten. Die unterstützten Objekte sind Cluster, Storage VMs und Volumes. Die folgenden Schritte sind erforderlich:

**Schritte**

1. Im linken Navigationsbereich auf **Dashboard** klicken.
2. Je nachdem, ob der Sicherheitsstatus für alle überwachten Cluster oder für einen einzelnen Cluster angezeigt werden soll, erfolgt die Auswahl im Dropdown-Menü über **Alle Cluster** oder über einen einzelnen Cluster.
3. Im Bereich **Sicherheit** erfolgt ein Klick auf den Pfeil nach rechts. Die Seite **Sicherheit** wird angezeigt.

Durch Klicken auf die Balkendiagramme, Anzahlangaben und `View Reports` Links gelangen Sie zur Seite „Volumes“, „Clusters“ oder „Storage VMs“, auf der die entsprechenden Details angezeigt oder bei Bedarf Berichte erstellt werden können.

Auf der Seite „Sicherheit“ werden die folgenden Bereiche angezeigt:

- **Cluster Compliance**: der Sicherheitsstatus (Anzahl der Compliance-konformen bzw. nicht Compliance-konformen Cluster) aller Cluster in einem Datacenter
- **Storage VM Compliance**: der Sicherheitsstatus (Anzahl der Storage VMs, die konform oder nicht konform sind) für alle Storage VMs in Ihrem Datacenter
- **Volume-Verschlüsselung**: der Verschlüsselungsstatus (Anzahl der verschlüsselten bzw. unverschlüsselten Volumes) aller Volumes in Ihrer Umgebung
- **Status des Ransomware-Schutzes auf Volume-Ebene**: der Sicherheitsstatus (Anzahl der Volumes mit aktiviertem oder deaktiviertem Ransomware-Schutz) aller Volumes in Ihrer Umgebung
- **Clusterauthentifizierung und Zertifikate**: die Anzahl der Cluster, die die jeweiligen Authentifizierungsverfahren wie SAML, Active Directory oder Zertifikate und lokale Authentifizierung verwenden. Das Panel zeigt außerdem die Anzahl der Cluster an, deren Zertifikate entweder abgelaufen sind oder in den nächsten 60 Tagen ablaufen.

## Die Sicherheitsdetails aller Cluster finden Sie auf der Seite „Clusters“.

Die Detailseite **Clusters / Security** ermöglicht die Anzeige des Sicherheits-Compliance-Status auf Cluster-Level.

**Schritte**

1. Im linken Navigationsbereich **Storage > Clusters** auswählen.
2. Die Auswahl erfolgt über **Ansicht > Sicherheit > Alle Cluster**.

Standard-Sicherheitsparameter wie Global FIPS, Telnet, unsichere SSH-Einstellungen, Anmeldebanner, Netzwerkzeitprotokoll, AutoSupport HTTPS-Transport und der Status des Ablaufs des Clusterzertifikats werden angezeigt.

Sie können auf die ⋮ Schaltfläche „Weitere Optionen“ klicken und die Sicherheitsdetails auf der Seite **Security** von Unified Manager oder in System Manager anzeigen. Für die Anzeige der Details in System Manager sind gültige Anmeldeinformationen erforderlich.

> ⓘ Wenn ein Cluster über ein abgelaufenes Zertifikat verfügt, können Sie unter **Gültigkeit des Clusterzertifikats** auf `expired` klicken und es in System Manager (9.10.1 und höher) erneuern. Auf `expired` können Sie nicht klicken, wenn die System Manager Instanz älter als 9.10.1 ist.

## Die Sicherheitsdetails aller Cluster sind auf der Seite „Storage VMs“ einsehbar.

Die Detailseite **Storage VMs / Security** ermöglicht die Anzeige des Status der Sicherheits-Compliance auf Storage-VM-Ebene.

**Schritte**

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage > Storage VMs**.
2. Die Auswahl erfolgt über **Ansicht > Sicherheit > Alle Speicher-VMs**. Eine Liste der Cluster mit den Sicherheitsparametern wird angezeigt.

Ein Standardüberblick über die Sicherheits-Compliance der Storage VMs ergibt sich aus der Überprüfung der Sicherheitsparameter wie Storage VMs, Cluster, Anmeldebanner, Revisionsprotokoll und unsichere SSH-Einstellungen.

Sie können auf die Schaltfläche „Weitere Optionen“ klicken und die Sicherheitsdetails auf der Seite **Security** von Unified Manager oder in System Manager anzeigen. Für die Anzeige der Details in System Manager sind gültige Anmeldeinformationen erforderlich.

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

# Sicherheitsereignisse, die möglicherweise Software- oder Firmware-Updates in Active IQ Unified Manager erfordern, können angezeigt werden

Es gibt bestimmte Sicherheitsereignisse, die den Wirkungsbereich „Upgrade“ haben. Diese Ereignisse werden von der Active IQ Plattform gemeldet und identifizieren Probleme, deren Behebung ein Upgrade der ONTAP Software, der Node-Firmware oder der Betriebssystemsoftware (bei Sicherheitshinweisen) erfordert.

**Bevor Sie beginnen**

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Bei einigen dieser Probleme können möglicherweise sofortige Korrekturmaßnahmen erforderlich sein, während andere bis zur nächsten planmäßigen Wartung warten können. Alle diese Ereignisse können angezeigt und Benutzern zugewiesen werden, die die Probleme beheben können. Wenn es bestimmte Ereignisse für Sicherheitsupgrades gibt, zu denen Sie nicht benachrichtigt werden möchten, kann diese Liste bei der Identifizierung dieser Ereignisse helfen, damit sie deaktiviert werden können.

**Schritte**

1. Im linken Navigationsbereich auf **Event Management** klicken.

   Standardmäßig werden auf der Inventarseite „Event Management“ alle aktiven Ereignisse (Neu und Bestätigt) angezeigt.

2. Im Menü „View“ erfolgt die Auswahl von **Upgrade events**.

   Die Seite zeigt alle aktiven Upgrade-Sicherheitsereignisse an.

# Anzeige, wie Cluster die Benutzerauthentifizierung auf allen Clustern in Active IQ Unified Manager verwalten

Die Sicherheitsseite zeigt die Arten der Authentifizierung an, die zur Benutzerauthentifizierung auf jedem Cluster verwendet werden, sowie die Anzahl der Benutzer, die mit der jeweiligen Art auf den Cluster zugreifen. Damit lässt sich überprüfen, ob die Benutzerauthentifizierung gemäß den Vorgaben Ihres Unternehmens sicher durchgeführt wird.

**Schritte**

1. Im linken Navigationsbereich auf **Dashboard** klicken.
2. Oben im Dashboard erfolgt die Auswahl **Alle Cluster** über das Dropdown-Menü.
3. Im Bereich **Sicherheit** führt ein Klick auf den Pfeil nach rechts zur Seite **Sicherheit**.
4. Auf der Karte **Cluster-Authentifizierung** ist die Anzahl der Benutzer zu sehen, die mit dem jeweiligen Authentifizierungstyp auf das System zugreifen.
5. Auf der Karte **Cluster Security** sehen Sie, welche Authentifizierungsmechanismen zur Authentifizierung von Benutzern auf den einzelnen Clustern verwendet werden.

Wenn einige Benutzer mit einer unsicheren Methode oder mit einer Methode, die von NetApp nicht empfohlen wird, auf das System zugreifen, können Sie diese Methode deaktivieren.

# Der Verschlüsselungsstatus aller Volumes in Active IQ Unified Manager kann angezeigt werden

Sie können eine Liste aller Volumes und deren aktuellen Verschlüsselungsstatus einsehen, um festzustellen, ob die Daten auf Ihren Volumes ausreichend vor dem Zugriff durch unbefugte Benutzer geschützt sind.

**Bevor Sie beginnen**

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Für ein Volume sind folgende Verschlüsselungsarten möglich:

- Software - Volumes, die mit den Softwareverschlüsselungslösungen NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) geschützt sind.
- Hardware - Volumes, die mit der Hardwareverschlüsselung NetApp Storage Encryption (NSE) geschützt sind.
- Software und Hardware - Volumes, die sowohl durch Software- als auch durch Hardwareverschlüsselung geschützt sind.
- Keine - Volumes, die nicht verschlüsselt sind.

**Schritte**

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Systemstatus** > **Volume-Verschlüsselung**
3. In der Ansicht **Systemstatus: Volume-Verschlüsselung** können Sie nach dem Feld **Verschlüsselungstyp** sortieren oder mithilfe des Filters Volumes anzeigen, die einen bestimmten Verschlüsselungstyp aufweisen oder die nicht verschlüsselt sind (Verschlüsselungstyp “None”).

# Der Anti-Ransomware-Status aller Volumes und Speicher-VMs in Active IQ Unified Manager kann angezeigt werden

Sie können eine Liste aller Volumes und Storage VMs (SVMs) sowie deren aktuellen Anti-Ransomware-Status einsehen, um festzustellen, ob die Daten auf Ihren Volumes und SVMs ausreichend vor Ransomware-Angriffen geschützt sind.

**Bevor Sie beginnen**

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

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

### Sicherheitsdetails aller Volumes mit Anti-Ransomware-Erkennung

**Schritte**

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“: **Systemstatus** > **Sicherheit** > **Anti-Ransomware**
3. In der Ansicht **Sicherheit: Anti-Ransomware** können Sie nach den verschiedenen Feldern sortieren oder den Filter verwenden.

> Anti-Ransomware wird für Offline-Volumes, eingeschränkte Volumes, SnapLock Volumes, FlexGroup Volumes, FlexCache Volumes, ausschließlich SAN-basierte Volumes, Volumes von gestoppten Storage VMs, Root-Volumes von Storage VMs oder Datensicherungs-Volumes nicht unterstützt.

### Anzeige der Sicherheitsdetails aller Storage VMs mit Anti-Ransomware-Erkennung

**Schritte**

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage > Storage VMs**.
2. **Ansicht > Sicherheit > Anti-Ransomware** auswählen. Eine Liste der SVMs mit dem Anti-Ransomware-Status wird angezeigt.

> Die Anti-Ransomware-Überwachung wird auf Storage VMs, auf denen das NAS-Protokoll nicht aktiviert ist, nicht unterstützt.

# Alle aktiven Sicherheitsereignisse in Active IQ Unified Manager anzeigen

Sie können alle aktiven Sicherheitsereignisse einsehen und jedes einzelne einem Benutzer zuweisen, der das Problem beheben kann. Falls Sie bestimmte Sicherheitsereignisse nicht erhalten möchten, hilft Ihnen diese Liste außerdem dabei, die zu deaktivierenden Ereignisse zu identifizieren.

**Bevor Sie beginnen**

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

**Schritte**

1. Im linken Navigationsbereich auf **Event Management** klicken.

   Standardmäßig zeigt die Inventarseite „Event Management“ neue und bestätigte Ereignisse an.

2. Im Menü „Ansicht“ ist die Option „Aktive Sicherheitsereignisse“ auszuwählen.

   Die Seite zeigt alle neuen und bestätigten Sicherheitsereignisse an, die in den letzten 7 Tagen generiert wurden.

# Hinzufügen von Warnmeldungen für Sicherheitsereignisse in Active IQ Unified Manager

Sie können Benachrichtigungen für einzelne Sicherheitsereignisse genauso konfigurieren wie für alle anderen Ereignisse, die von Unified Manager empfangen werden. Außerdem können Sie, wenn alle Sicherheitsereignisse gleich behandelt werden sollen und eine E-Mail an dieselbe Person gesendet werden soll, eine einzelne Benachrichtigung erstellen, die Sie informiert, sobald Sicherheitsereignisse ausgelöst werden.

**Bevor Sie beginnen**

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Das folgende Beispiel zeigt, wie eine Warnung für das Sicherheitsereignis “Telnet Protocol Enabled” erstellt wird. Dadurch wird eine Warnung gesendet, wenn der Telnet-Zugriff für den administrativen Fernzugriff auf den Cluster konfiguriert ist. Diese Vorgehensweise kann verwendet werden, um Warnungen für alle Sicherheitsereignisse zu erstellen.

**Schritte**

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alarmeinstellungen Hinzufügen** auswählen.
3. Im Dialogfeld **Warnung hinzufügen** auf **Name** klicken und einen Namen sowie eine Beschreibung für die Warnung eingeben.
4. Unter **Ressourcen** erfolgt die Auswahl des Clusters oder der Cluster, für den bzw. die diese Warnung aktiviert werden soll.
5. Nach Auswahl von **Events** können die folgenden Aktionen durchgeführt werden:
   a. In der Liste „Ereignisschweregrad“ wird die Option **Warnung** ausgewählt.
   b. In der Liste „Übereinstimmende Ereignisse“ ist **Telnet Protocol Enabled** auszuwählen.
6. Unter **Aktionen** folgt im Feld **Diese Benutzer benachrichtigen** die Auswahl des Namens des Benutzers, der die Benachrichtigungs-E-Mail erhalten soll.
7. Auf dieser Seite können alle weiteren Optionen für die Benachrichtigungshäufigkeit, das Auslösen von SNMP-Taps und das Ausführen eines Skripts konfiguriert werden.
8. Auf **Speichern** klicken.

# Deaktivieren bestimmter Sicherheitsereignisse in Active IQ Unified Manager

Alle Ereignisse sind standardmäßig aktiviert. Sie können bestimmte Ereignisse deaktivieren, um zu verhindern, dass Benachrichtigungen für Ereignisse generiert werden, die in Ihrer Umgebung nicht relevant sind. Sie können deaktivierte Ereignisse wieder aktivieren, wenn Sie wieder Benachrichtigungen dafür erhalten möchten.

**Bevor Sie beginnen**

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Wenn Sie Ereignisse deaktivieren, werden die zuvor im System generierten Ereignisse als veraltet markiert, und die für diese Ereignisse konfigurierten Warnmeldungen werden nicht ausgelöst. Wenn Sie deaktivierte

Ereignisse wieder aktivieren, werden die Benachrichtigungen für diese Ereignisse ab dem nächsten Überwachungszyklus generiert.

**Schritte**

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Ereigniseinrichtung**.
2. Auf der Seite **Event** Setup können Ereignisse deaktiviert oder aktiviert werden, indem eine der folgenden Optionen ausgewählt wird:

| Wenn Sie möchten… | Fahren Sie dann wie folgt fort… |
|---|---|
| Ereignisse deaktivieren | a. Klicken Sie auf **Deaktivieren**.<br>b. Im Dialogfeld „Ereignisse deaktivieren“ wird der Schweregrad **Warning** ausgewählt. Dies ist die Kategorie für alle Sicherheitsereignisse.<br>c. In der Spalte „Übereinstimmende Ereignisse“ lassen sich die Sicherheitsereignisse auswählen, die deaktiviert werden sollen; anschließend lassen sich diese Ereignisse mit dem Pfeil nach rechts in die Spalte „Ereignisse deaktivieren“ verschieben.<br>d. Anschließend erfolgt die Auswahl von **Save and Close**.<br>e. Stellen Sie sicher, dass die deaktivierten Ereignisse in der Listenansicht der Seite „Ereigniseinrichtung“ angezeigt werden. |
| Ereignisse aktivieren | a. In der Liste der deaktivierten Ereignisse erfolgt die Auswahl des Kästchens für das Ereignis oder die Ereignisse, die wieder aktiviert werden sollen.<br>b. Klicken Sie auf **Enable**. |

# Sicherheitsereignisse in Active IQ Unified Manager anzeigen

Sicherheitsereignisse liefern Ihnen Informationen zum Sicherheitsstatus von ONTAP Clustern, Storage Virtual Machines (SVMs) und Volumes basierend auf den im *NetApp Security Hardening Guide for ONTAP 9* definierten Parametern. Diese Ereignisse benachrichtigen Sie über potenzielle Probleme, sodass Sie deren Schweregrad bewerten und das Problem gegebenenfalls beheben können.

Sicherheitsereignisse sind nach Quelltyp gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel und den Schweregrad. Diese Ereignisse werden in den Ereigniskategorien für Cluster und Storage VM angezeigt.

**Copyright-Informationen**

Copyright © 2026 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.