Welche Sicherheitskriterien werden bewertet

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_what_security_criteria_is_being_evaluated.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Welche Sicherheitskriterien werden bewertet 1
Informationen dazu, wie Active IQ Unified Manager Sicherheitskriterien auswertet 1
Cluster Compliance Kategorien in Active IQ Unified Manager 1
Grundlegendes zu den Konformitätskategorien von Storage VMs in Active IQ Unified Manager 5
Konformitätskategorien für Volumes in Active IQ Unified Manager 6

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
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

Parameter	Beschreibung	Empfehlung	Beeinträchtigt die Cluster-Compliance
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
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

Parameter	Beschreibung	Empfehlung	Beeinträchtigt die Cluster-Compliance
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
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
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

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM Compliance
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.
Nicht verschlüsselt	Zeigt die Anzahl der nicht verschlüsselten Volumes an.

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.