Welche Sicherheitskriterien werden bewertet

Active IQ Unified Manager 9.14

NetApp
March 07, 2024

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager/health-checker/reference_cluster_compliance_categories.html on March 07, 2024. Always check docs.netapp.com for the latest.

Inhalt

Welche Sicherheitskriterien werden bewertet 1
Cluster-Compliance-Kategorien 1
Compliance-Kategorien für Storage-VMs 5
Volume Compliance-Kategorien 6

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.

Weitere Informationen finden Sie unter "Verwalten von Zielen für die Cluster-Sicherheit".

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.
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.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
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.
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.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
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
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.

Parameter	Beschreibung	Empfehlung	Betrifft Cluster-Compliance
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.
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

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM-Compliance
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.

Copyright-Informationen

Copyright © 2024 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.