Welche Sicherheitskriterien werden bewertet?

Active IQ Unified Manager

NetApp
October 15, 2025

Inhalt

Welche Sicherheitskriterien werden bewertet

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

Zu den Sicherheitskontrollen gehören unter anderem:

- ob ein Cluster eine sichere Authentifizierungsmethode wie SAML verwendet
- ob die Kommunikation zwischen Peering-Clustern verschlüsselt ist
- ob für eine Speicher-VM das Überwachungsprotokoll aktiviert ist
- ob auf Ihren Volumes Software- oder Hardwareverschlüsselung aktiviert ist

Siehe die Themen zu Compliance-Kategorien und den "NetApp Security Hardening Guide für ONTAP 9" für detaillierte Informationen.

> Von der Active IQ Plattform gemeldete Upgrade-Ereignisse gelten ebenfalls als Sicherheitsereignisse. Diese Ereignisse identifizieren Probleme, bei denen zur Lösung ein Upgrade der ONTAP -Software, der Knoten-Firmware oder der Betriebssystemsoftware (für Sicherheitshinweise) erforderlich ist. Diese Ereignisse werden nicht im Sicherheitsbereich angezeigt, sind aber auf der Inventarseite der Ereignisverwaltung verfügbar.

Weitere Informationen finden Sie unter "Verwalten von Cluster-Sicherheitszielen".

Cluster-Compliance-Kategorien

Diese Tabelle beschreibt die von Unified Manager ausgewerteten Parameter zur Cluster-Sicherheitskonformität, die NetApp -Empfehlung und ob der Parameter die Gesamtfeststellung beeinflusst, ob der Cluster den Anforderungen entspricht oder nicht.

Wenn sich in einem Cluster nicht konforme SVMs befinden, wirkt sich dies auf den Konformitätswert des Clusters aus. Daher müssen Sie in einigen Fällen möglicherweise ein Sicherheitsproblem mit einem SVM beheben, bevor die Sicherheit Ihres Clusters als konform angesehen wird.

Beachten Sie, dass nicht jeder der unten aufgeführten Parameter bei allen Installationen angezeigt wird. Wenn Sie beispielsweise keine Peering-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	Beeinflusst die Cluster-Compliance
Globales FIPS	Gibt an, ob der Konformitätsmodus 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 sind zulässig.	Ermöglicht	Ja
Telnet	Gibt an, ob der Telnet-Zugriff auf das System aktiviert oder deaktiviert ist. NetApp empfiehlt Secure Shell (SSH) für sicheren Fernzugriff.	Deaktiviert	Ja
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit *cbc beginnen.	Nein	Ja
Login-Banner	Gibt an, ob das Anmeldebanner für Benutzer, die auf das System zugreifen, aktiviert oder deaktiviert ist.	Ermöglicht	Ja
Cluster-Peering	Gibt an, ob die Kommunikation zwischen Peering-Clustern verschlüsselt oder unverschlüsselt ist. Damit dieser Parameter als konform gilt, muss die Verschlüsselung sowohl auf dem Quell- als auch auf dem Zielcluster konfiguriert sein.	Verschlüsselt	Ja

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
Netzwerkzeitprotokoll	Gibt an, ob der Cluster über einen oder mehrere konfigurierte NTP-Server verfügt. Aus Redundanzgründen und für einen optimalen Service empfiehlt NetApp , dem Cluster mindestens drei NTP-Server zuzuordnen.	Konfiguriert	Ja
OCSP	Ab Version 9.14.1 bietet Active IQ Unified Manager Statusinformationen zum Online Certificate Status Protocol (OCSP) auf der Ebene der Storage Virtual Machine (SVM, früher als Vserver bezeichnet). Dies bedeutet, dass die OCSP-Validierung auf alle SSL/TLS-Verbindungen zum SVM angewendet wird und die Integrität und Gültigkeit der in diesen Verbindungen verwendeten Zertifikate gewährleistet.	Ermöglicht	Nein
Remote-Audit-Protokollierung	Gibt an, ob die Protokollweiterleitung (Syslog) verschlüsselt oder unverschlüsselt ist.	Verschlüsselt	Ja
AutoSupport HTTPS-Transport	Gibt an, ob HTTPS als Standardtransportprotokoll zum Senden von AutoSupport -Nachrichten an den NetApp Support verwendet wird.	Ermöglicht	Ja
Standard-Administratorbenutzer	Gibt an, ob der Standardadministratorbenutzer (integriert) aktiviert oder deaktiviert ist. NetApp empfiehlt, alle nicht benötigten integrierten Konten zu sperren (deaktivieren).	Deaktiviert	Ja

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
SAML-Benutzer	Gibt an, ob SAML konfiguriert ist. SAML ermöglicht Ihnen die Konfiguration der Multi-Faktor-Authentifizierung (MFA) als Anmeldemethode für Single Sign-On.	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 gegenüber lokalen Benutzern verwalten.	Nein	Nein
Zertifikatsbenutzer	Gibt an, ob ein Zertifikatsbenutzer für die Anmeldung beim Cluster konfiguriert ist.	Nein	Nein
Lokale Benutzer	Gibt an, ob lokale Benutzer für die Anmeldung beim Cluster konfiguriert sind.	Nein	Nein
Remote-Shell	Gibt an, ob RSH aktiviert ist. Aus Sicherheitsgründen sollte RSH deaktiviert werden. Für den sicheren Fernzugriff wird die Secure Shell (SSH) bevorzugt.	Deaktiviert	Ja

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
MD5 im Einsatz	Gibt an, ob ONTAP Benutzerkonten die weniger sichere MD5-Hash-Funktion verwenden. Die Migration von MD5-gehashten Benutzerkonten zur sichereren kryptografischen Hashfunktion wie SHA-512 wird bevorzugt.	Nein	Ja
Zertifikatsausstellertyp	Gibt den Typ des verwendeten digitalen Zertifikats an.	CA-signiert	Nein

Storage-VM-Compliance-Kategorien

Diese Tabelle beschreibt die Sicherheitskonformitätskriterien für virtuelle Speichermaschinen (SVMs), die Unified Manager auswertet, die NetApp -Empfehlung und ob der Parameter die Gesamtfeststellung beeinflusst, ob die SVM den Anforderungen entspricht oder nicht.

Parameter	Beschreibung	Empfehlung	Beeinflusst die SVM-Konformität
Prüfprotokoll	Gibt an, ob die Überwachungsprotokollierung aktiviert oder deaktiviert ist.	Ermöglicht	Ja
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit `cbc*` .	Nein	Ja
Login-Banner	Gibt an, ob das Anmeldebanner für Benutzer aktiviert oder deaktiviert ist, die auf SVMs im System zugreifen.	Ermöglicht	Ja
LDAP-Verschlüsselung	Gibt an, ob die LDAP-Verschlüsselung aktiviert oder deaktiviert ist.	Ermöglicht	Nein

Parameter	Beschreibung	Empfehlung	Beeinflusst die SVM-Konformität
NTLM-Authentifizierung	Gibt an, ob die NTLM-Authentifizierung aktiviert oder deaktiviert ist.	Ermöglicht	Nein
LDAP-Nutzlastsignatur	Gibt an, ob die LDAP-Nutzlastsignatur aktiviert oder deaktiviert ist.	Ermöglicht	Nein
CHAP-Einstellungen	Gibt an, ob CHAP aktiviert oder deaktiviert ist.	Ermöglicht	Nein
Kerberos V5	Gibt an, ob die Kerberos V5-Authentifizierung aktiviert oder deaktiviert ist.	Ermöglicht	Nein
NIS-Authentifizierung	Gibt an, ob die Verwendung der NIS-Authentifizierung konfiguriert ist.	Deaktiviert	Nein
FPolicy-Status „Aktiv“	Gibt an, ob FPolicy erstellt wurde oder nicht.	Ja	Nein
SMB-Verschlüsselung aktiviert	Gibt an, ob SMB-Signieren und Versiegeln nicht aktiviert ist.	Ja	Nein
SMB-Signierung aktiviert	Gibt an, ob die SMB-Signatur nicht aktiviert ist.	Ja	Nein

Volumen-Compliance-Kategorien

Diese Tabelle beschreibt die Volume-Verschlüsselungsparameter, die Unified Manager auswertet, um zu bestimmen, ob die Daten auf Ihren Volumes ausreichend vor dem Zugriff durch nicht autorisierte Benutzer geschützt sind.

Beachten Sie, dass die Volume-Verschlüsselungsparameter keinen Einfluss darauf haben, ob der Cluster oder die Speicher-VM als konform gilt.

Parameter	Beschreibung
Softwareverschlüsselt	Zeigt die Anzahl der Volumes an, die mit den Softwareverschlüsselungslösungen NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) geschützt sind.
Hardwareverschlüsselt	Zeigt die Anzahl der Volumes an, die mit der Hardwareverschlüsselung NetApp Storage Encryption (NSE) geschützt sind.
Software- und Hardwareverschlüsselung	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.