Quali criteri di sicurezza vengono valutati

Active IQ Unified Manager 9.11

NetApp
December 18, 2023

This PDF was generated from https://docs.netapp.com/it-it/active-iq-unified-manager-911/health-checker/reference_cluster_compliance_categories.html on December 18, 2023. Always check docs.netapp.com for the latest.

Sommario

Quali criteri di sicurezza vengono valutati 1
Categorie di compliance del cluster 1
Categorie di conformità delle VM di storage 4
Categorie di compliance ai volumi 5

Quali criteri di sicurezza vengono valutati

In generale, i criteri di sicurezza per i cluster ONTAP, le macchine virtuali di storage (SVM) e i volumi vengono valutati in base ai consigli definiti nella *Guida per l'aumento della protezione di NetApp per ONTAP 9*.

Alcuni dei controlli di sicurezza includono:

- Se un cluster utilizza un metodo di autenticazione sicuro, ad esempio SAML
- se i cluster peered hanno la loro comunicazione crittografata
- Se una VM storage ha attivato il registro di controllo
- sia che i volumi dispongano della crittografia software o hardware abilitata

Consultare gli argomenti relativi alle categorie di conformità e a. "Guida al rafforzamento della sicurezza di NetApp per ONTAP 9" per informazioni dettagliate.

> Anche gli eventi di upgrade riportati dalla piattaforma Active IQ sono considerati eventi di sicurezza. Questi eventi identificano i problemi in cui la risoluzione richiede l'aggiornamento del software ONTAP, del firmware del nodo o del software del sistema operativo (per gli avvisi di sicurezza). Questi eventi non vengono visualizzati nel pannello sicurezza, ma sono disponibili nella pagina inventario gestione eventi.

Categorie di compliance del cluster

Questa tabella descrive i parametri di conformità della sicurezza del cluster che Unified Manager valuta, i consigli di NetApp e se il parametro influisce sulla determinazione generale del cluster che presenta un reclamo o meno.

La presenza di SVM non conformi su un cluster influisce sul valore di conformità del cluster. Pertanto, in alcuni casi potrebbe essere necessario risolvere problemi di sicurezza con una SVM prima che la sicurezza del cluster venga considerata conforme.

Si noti che non tutti i parametri elencati di seguito vengono visualizzati per tutte le installazioni. Ad esempio, se non si dispone di cluster peered o se AutoSupport è stato disattivato su un cluster, gli elementi di peering cluster o trasporto HTTPS AutoSupport non verranno visualizzati nella pagina dell'interfaccia utente.

Parametro	Descrizione	Consiglio	Influisce sulla conformità del cluster
FIPS globale	Indica se la modalità di conformità Global FIPS (Federal Information Processing Standard) 140-2 è attivata o disattivata. Quando FIPS è attivato, TLSv1 e SSLv3 sono disattivati e sono consentiti solo TLSv1.1 e TLSv1.2.	Attivato	Sì

Parametro	Descrizione	Consiglio	Influisce sulla conformità del cluster
Telnet	Indica se l'accesso Telnet al sistema è attivato o disattivato. NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro.	Disattivato	Sì
Impostazioni SSH non sicure	Indica se SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con *cbc.	No	Sì
Banner di accesso	Indica se il banner di accesso è attivato o disattivato per gli utenti che accedono al sistema.	Attivato	Sì
Peering dei cluster	Indica se la comunicazione tra i cluster in peering è crittografata o non crittografata. La crittografia deve essere configurata sia sul cluster di origine che su quello di destinazione affinché questo parametro sia considerato conforme.	Crittografato	Sì
Network Time Protocol	Indica se il cluster dispone di uno o più server NTP configurati. Per la ridondanza e il miglior servizio, NetApp consiglia di associare almeno tre server NTP al cluster.	Configurato	Sì
OCSP	Indica se in ONTAP sono presenti applicazioni non configurate con OCSP (Online Certificate Status Protocol) e quindi le comunicazioni non sono crittografate. Vengono elencate le applicazioni non conformi.	Attivato	No

Parametro	Descrizione	Consiglio	Influisce sulla conformità del cluster
Log di controllo remoto	Indica se l'inoltro dei log (Syslog) è crittografato o meno.	Crittografato	Sì
Trasporto HTTPS AutoSupport	Indica se HTTPS è utilizzato come protocollo di trasporto predefinito per l'invio di messaggi AutoSupport al supporto NetApp.	Attivato	Sì
Admin User predefinito	Indica se l'utente amministratore predefinito (incorporato) è attivato o disattivato. NetApp consiglia di bloccare (disabilitare) gli account integrati non necessari.	Disattivato	Sì
Utenti SAML	Indica se SAML è configurato. SAML consente di configurare l'autenticazione a più fattori (MFA) come metodo di accesso per il single sign-on.	No	No
Utenti di Active Directory	Indica se Active Directory è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti per gli utenti che accedono ai cluster.	No	No
Utenti LDAP	Indica se LDAP è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti per gli utenti che gestiscono i cluster su utenti locali.	No	No
Utenti certificati	Indica se un utente certificato è configurato per accedere al cluster.	No	No

Parametro	Descrizione	Consiglio	Influisce sulla conformità del cluster
Utenti locali	Indica se gli utenti locali sono configurati per l'accesso al cluster.	No	No
Shell remota	Indica se RSH è attivato. Per motivi di sicurezza, RSH deve essere disattivato. È preferibile utilizzare Secure Shell (SSH) per un accesso remoto sicuro.	Disattivato	Sì
MD5 in uso	Indica se gli account utente ONTAP utilizzano una funzione hash MD5 meno sicura. Si preferisce la migrazione degli account utente con hash MD5 alla funzione hash crittografica più sicura come SHA-512.	No	Sì
Tipo di autorità di certificazione	Indica il tipo di certificato digitale utilizzato.	Firma CA	No

Categorie di conformità delle VM di storage

Questa tabella descrive i criteri di conformità della sicurezza SVM (Storage Virtual Machine) che Unified Manager valuta, i consigli di NetApp e se il parametro influisce sulla determinazione generale della SVM che presenta un reclamo o meno.

Parametro	Descrizione	Consiglio	Influisce sulla conformità SVM
Log di audit	Indica se la registrazione dell'audit è attivata o disattivata.	Attivato	Sì
Impostazioni SSH non sicure	Indica se SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con `cbc*`.	No	Sì

Parametro	Descrizione	Consiglio	Influisce sulla conformità SVM
Banner di accesso	Indica se il banner di accesso è attivato o disattivato per gli utenti che accedono alle SVM sul sistema.	Attivato	Sì
Crittografia LDAP	Indica se la crittografia LDAP è attivata o disattivata.	Attivato	No
Autenticazione NTLM	Indica se l'autenticazione NTLM è attivata o disattivata.	Attivato	No
Firma del payload LDAP	Indica se la firma del payload LDAP è attivata o disattivata.	Attivato	No
Impostazioni CHAP	Indica se CHAP è attivato o disattivato.	Attivato	No
Kerberos V5	Indica se l'autenticazione Kerberos V5 è attivata o disattivata.	Attivato	No
Autenticazione NIS	Indica se è configurato l'utilizzo dell'autenticazione NIS.	Disattivato	No
Stato FPolicy attivo	Indica se FPolicy è stato creato o meno.	Sì	No
Crittografia SMB attivata	Indica se SMB -signing & sealing non è abilitato.	Sì	No
Firma SMB abilitata	Indica se la firma SMB non è abilitata.	Sì	No

Categorie di compliance ai volumi

Questa tabella descrive i parametri di crittografia del volume che Unified Manager valuta per determinare se i dati sui volumi sono adeguatamente protetti dall'accesso da parte di utenti non autorizzati.

Si noti che i parametri di crittografia del volume non influiscono sul fatto che la VM del cluster o dello storage sia considerata conforme.

Parametro	Descrizione
Software crittografato	Visualizza il numero di volumi protetti mediante le soluzioni di crittografia software NetApp Volume Encryption (NVE) o NetApp aggregate Encryption (NAE).
Crittografia hardware	Visualizza il numero di volumi protetti mediante la crittografia hardware NetApp Storage Encryption (NSE).
Crittografia software e hardware	Visualizza il numero di volumi protetti dalla crittografia software e hardware.
Non crittografato	Visualizza il numero di volumi non crittografati.

Informazioni sul copyright

Copyright © 2023 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.