Quels sont les critères de sécurité évalués

Active IQ Unified Manager 9.10

NetApp
December 18, 2023

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-910/health-checker/reference_cluster_compliance_categories.html on December 18, 2023. Always check docs.netapp.com for the latest.

Sommaire

Quels sont les critères de sécurité évalués 1
Catégories de conformité des clusters 1
Catégories de conformité des VM de stockage 5
Catégories de conformité des volumes 6

Quels sont les critères de sécurité évalués

De manière générale, les critères de sécurité des clusters ONTAP, des serveurs de stockage virtuels (SVM) et des volumes sont évalués avec les recommandations définies dans le *guide NetApp de renforcement de la sécurité de la solution ONTAP 9*.

Voici quelques-unes des vérifications de sécurité :

- Indique si un cluster utilise une méthode d'authentification sécurisée, par exemple SAML
- les communications des clusters utilisant des canaux de connexion sont chiffrées
- Indique si le journal des audits d'un serveur virtuel de stockage est activé
- que le chiffrement logiciel ou matériel soit activé pour vos volumes

Voir les rubriques sur les catégories de conformité et "Guide NetApp sur le renforcement de la sécurité des environnements ONTAP 9" pour des informations détaillées.

> Les événements de mise à niveau signalés sur la plate-forme Active IQ sont également considérés comme des événements de sécurité. Ces événements identifient les problèmes liés à la résolution des problèmes lorsque vous devez mettre à niveau le logiciel ONTAP, le firmware des nœuds ou le logiciel du système d'exploitation (pour les conseils de sécurité). Ces événements ne sont pas affichés dans le panneau sécurité, mais ils sont disponibles dans la page d'inventaire gestion des événements.

Catégories de conformité des clusters

Ce tableau décrit les paramètres de conformité de sécurité du cluster que Unified Manager évalue, la recommandation NetApp et si le paramètre affecte la détermination globale du cluster plainte ou non.

L'utilisation de SVM non conformes sur un cluster affecte la valeur de conformité du cluster. Dans certains cas, vous devrez peut-être corriger les problèmes de sécurité avec un SVM avant que la sécurité du cluster ne soit considérée comme conforme.

Notez que tous les paramètres répertoriés ci-dessous ne s'affichent pas pour toutes les installations. Par exemple, si vous n'avez pas de cluster avec peering, ou si vous avez désactivé AutoSupport sur un cluster, vous ne verrez pas les éléments de peering de cluster ni de transport AutoSupport HTTPS dans la page de l'interface utilisateur.

Paramètre	Description	Recommandation	Concerne la conformité du cluster
FIPS global	Indique si le mode de conformité Global FIPS (Federal information Processing Standard) 140-2 est activé ou désactivé. Lorsque FIPS est activé, TLSv1 et SSLv3 sont désactivés et seuls les modèles TLSv1.1 et TLSv1.2 sont autorisés.	Activé	Oui.
Telnet	Indique si l'accès Telnet au système est activé ou désactivé. NetApp recommande un accès sécurisé à distance (SSH).	Désactivé	Oui.
Paramètres SSH non sécurisés	Indique si SSH utilise des chiffrements non sécurisés, par exemple les chiffrements commençant par *cbc.	Non	Oui.
Bannière de connexion	Indique si la bannière connexion est activée ou désactivée pour les utilisateurs accédant au système.	Activé	Oui.
Peering de clusters	Indique si la communication entre les clusters avec points de connexion est cryptée ou non chiffrée. Le chiffrement doit être configuré sur les clusters source et de destination pour que ce paramètre soit considéré comme conforme.	Chiffrées	Oui.

Paramètre	Description	Recommandation	Concerne la conformité du cluster
Protocole de temps réseau	Indique si le cluster possède un ou plusieurs serveurs NTP configurés. Pour la redondance et le meilleur service, NetApp vous recommande d'associer au moins trois serveurs NTP au cluster.	Configuré	Oui.
OCSP	Indique si des applications dans ONTAP ne sont pas configurées avec le protocole OCSP (Online Certificate Status Protocol) et que les communications ne sont donc pas cryptées. Les applications non conformes sont répertoriées.	Activé	Non
Consignation d'audit à distance	Indique si le transfert de journal (Syslog) est crypté ou non.	Chiffrées	Oui.
Transport AutoSupport HTTPS	Indique si HTTPS est utilisé comme protocole de transport par défaut pour l'envoi des messages AutoSupport au support NetApp.	Activé	Oui.
Utilisateur Admin par défaut	Indique si l'utilisateur Admin par défaut (intégré) est activé ou désactivé. NetApp recommande de verrouiller (désactiver) tous les comptes intégrés inutiles.	Désactivé	Oui.

Paramètre	Description	Recommandation	Concerne la conformité du cluster
Utilisateurs SAML	Indique si le langage SAML est configuré. SAML permet de configurer l'authentification multifacteur (MFA) comme méthode de connexion pour l'authentification unique.	Non	Non
Utilisateurs Active Directory	Indique si Active Directory est configuré. Active Directory et LDAP sont les mécanismes d'authentification privilégiés pour les utilisateurs qui accèdent aux clusters.	Non	Non
Utilisateurs LDAP	Indique si LDAP est configuré. Active Directory et LDAP sont les mécanismes d'authentification préférés des utilisateurs gérant des clusters par le biais d'utilisateurs locaux.	Non	Non
Utilisateurs de certificats	Indique si un utilisateur de certificat est configuré pour se connecter au cluster.	Non	Non
Utilisateurs locaux	Indique si les utilisateurs locaux sont configurés pour se connecter au cluster.	Non	Non
Coque distante	Indique si le RSH est activé. Pour des raisons de sécurité, la fonction RSH doit être désactivée. Le protocole SSH (Secure Shell) est préféré pour un accès distant sécurisé.	Désactivé	Oui.

Paramètre	Description	Recommandation	Concerne la conformité du cluster
MD5 utilisé	Indique si les comptes utilisateur ONTAP utilisent la fonction de hachage MD5 moins sécurisée. Le MD5 hache les comptes utilisateur la migration vers la fonction de hachage cryptographique plus sécurisée comme SHA-512 est préférable.	Non	Oui.
Type émetteur de certificat	Indique le type de certificat numérique utilisé.	Signé CA	Non

Catégories de conformité des VM de stockage

Ce tableau décrit les critères de conformité de sécurité de la machine virtuelle de stockage (SVM) que Unified Manager évalue, la recommandation de NetApp et si le paramètre affecte la détermination globale de la plainte ou non de la SVM.

Paramètre	Description	Recommandation	Concerne la conformité des SVM
Journal d'audit	Indique si la journalisation d'audit est activée ou désactivée.	Activé	Oui.
Paramètres SSH non sécurisés	Indique si SSH utilise des chiffrements non sécurisés, par exemple, en commençant par le chiffrement `cbc*`.	Non	Oui.
Bannière de connexion	Indique si la bannière de connexion est activée ou désactivée pour les utilisateurs qui accèdent aux SVM sur le système.	Activé	Oui.
Cryptage LDAP	Indique si le chiffrement LDAP est activé ou désactivé.	Activé	Non

Paramètre	Description	Recommandation	Concerne la conformité des SVM
Authentification NTLM	Indique si l'authentification NTLM est activée ou désactivée.	Activé	Non
Signature de charge utile LDAP	Indique si la signature de charge utile LDAP est activée ou désactivée.	Activé	Non
Paramètres CHAP	Indique si CHAP est activé ou désactivé.	Activé	Non
Kerberos V5	Indique si l'authentification Kerberos V5 est activée ou désactivée.	Activé	Non
Authentification NIS	Indique si l'utilisation de l'authentification NIS est configurée.	Désactivé	Non
État FPolicy actif	Indique si FPolicy est créé ou non.	Oui.	Non
Chiffrement SMB activé	Indique si SMB - Signature & scellage n'est pas activé.	Oui.	Non
Signature SMB activée	Indique si SMB -Signing n'est pas activé.	Oui.	Non

Catégories de conformité des volumes

Ce tableau décrit les paramètres de chiffrement de volume que Unified Manager évalue pour déterminer si les données de vos volumes sont correctement protégées contre tout accès par des utilisateurs non autorisés.

Notez que les paramètres de chiffrement de volume n'affectent pas la conformité du cluster ou de la machine virtuelle de stockage.

Paramètre	Description
Chiffrement logiciel	Affiche le nombre de volumes protégés à l'aide des solutions logicielles de chiffrement NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).

Paramètre	Description
Chiffrement matériel	Affiche le nombre de volumes protégés à l'aide du chiffrement matériel NetApp Storage Encryption (NSE).
Cryptage logiciel et matériel	Affiche le nombre de volumes protégés par le chiffrement logiciel et matériel.
Non chiffré	Affiche le nombre de volumes qui ne sont pas chiffrés.

Informations sur le copyright

Copyright © 2023 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.