What security criteria is being evaluated

Active IQ Unified Manager

NetApp
May 24, 2022

Table of Contents

What security criteria is being evaluated

In general, security criteria for your ONTAP clusters, storage virtual machines (SVMs), and volumes are being evaluated against the recommendations defined in the *NetApp Security Hardening Guide for ONTAP 9*.

Some of the security checks include:

- whether a cluster is using a secure authentication method, such as SAML
- whether peered clusters have their communication encrypted
- whether a storage VM has its audit log enabled
- whether your volumes have software or hardware encryption enabled

See the topics on compliance categories and the NetApp Security Hardening Guide for ONTAP 9 for detailed information.

Upgrade events that are reported from the Active IQ platform are also considered security events. These events identify issues where the resolution requires you to upgrade ONTAP software, node firmware, or operating system software (for security advisories). These events are not displayed in the Security panel, but they are available from the Event Management inventory page.

Cluster compliance categories

This table describes the cluster security compliance parameters that Unified Manager evaluates, the NetApp recommendation, and whether the parameter affects the overall determination of the cluster being complaint or not complaint.

Having non-compliant SVMs on a cluster will affect the compliance value for the cluster. So in some cases you may need to fix a security issues with an SVM before your cluster security is seen as compliant.

Note that not every parameter listed below appears for all installations. For example, if you have no peered clusters, or if you have disabled AutoSupport on a cluster, then you will not see the Cluster Peering or AutoSupport HTTPS Transport items in the UI page.

Parameter	Description	Recommendation	Affects Cluster Compliance
Global FIPS	Indicates if Global FIPS (Federal Information Processing Standard) 140-2 compliance mode is enabled or disabled. When FIPS is enabled, TLSv1 and SSLv3 are disabled, and only TLSv1.1 and TLSv1.2 are allowed.	Enabled	Yes

Parameter	Description	Recommendation	Affects Cluster Compliance
Telnet	Indicates if Telnet access to the system is enabled or disabled. NetApp recommends Secure Shell (SSH) for secure remote access.	Disabled	Yes
Insecure SSH Settings	Indicates if SSH uses insecure ciphers, for example ciphers beginning with *cbc.	No	Yes
Login Banner	Indicates if the Login banner is enabled or disabled for users accessing the system.	Enabled	Yes
Cluster Peering	Indicates if communication between peered clusters is encrypted or unencrypted. Encryption must be configured on both the source and destination clusters for this parameter to be considered compliant.	Encrypted	Yes
Network Time Protocol	Indicates if the cluster has one or more configured NTP servers. For redundancy and best service NetApp recommends that you associate at least three NTP servers with the cluster.	Configured	Yes
OCSP	Indicates if there are applications in ONTAP that are not configured with OCSP (Online Certificate Status Protocol) and therefore communications are not encrypted. The non-compliant applications are listed.	Enabled	No

Parameter	Description	Recommendation	Affects Cluster Compliance
Remote Audit Logging	Indicates if log forwarding (Syslog) is encrypted or not encrypted.	Encrypted	Yes
AutoSupport HTTPS Transport	Indicates if HTTPS is used as the default transport protocol for sending AutoSupport messages to NetApp support.	Enabled	Yes
Default Admin User	Indicates if the Default Admin User (built-in) is enabled or disabled. NetApp recommends locking (disabling) any unneeded built-in accounts.	Disabled	Yes
SAML Users	Indicates if SAML is configured. SAML enables you to configure multi-factor authentication (MFA) as a login method for single sign-on.	No	No
Active Directory Users	Indicates if Active Directory is configured. Active Directory and LDAP are the preferred authentication mechanisms for users accessing clusters.	No	No
LDAP Users	Indicates if LDAP is configured. Active Directory and LDAP are the preferred authentication mechanisms for users managing clusters over local users.	No	No
Certificate Users	Indicates if a certificate user is configured to log into the cluster.	No	No

Parameter	Description	Recommendation	Affects Cluster Compliance
Local Users	Indicates if local users are configured to log into the cluster.	No	No
Remote Shell	Indicates if RSH is enabled. For security reasons, RSH should be disabled. The Secure Shell (SSH) for secure remote access is preferred.	Disabled	Yes
MD5 in Use	Indicates if ONTAP user accounts use less-secure MD5 Hash function. The MD5 Hashed user accounts migration to the more secure cryptographic hash function like SHA-512 is preferred.	No	Yes
Certificate Issuer Type	Indicates the type of digital certificate used.	CA-Signed	No

Storage VM compliance categories

This table describes the storage virtual machine (SVM) security compliance criteria that Unified Manager evaluates, the NetApp recommendation, and whether the parameter affects the overall determination of the SVM being complaint or not complaint.

Parameter	Description	Recommendation	Affects SVM Compliance
Audit Log	Indicates if Audit logging is enabled or disabled.	Enabled	Yes
Insecure SSH Settings	Indicates if SSH uses insecure ciphers, for example ciphers beginning with `cbc*`.	No	Yes
Login Banner	Indicates if the Login banner is enabled or disabled for users accessing SVMs on the system.	Enabled	Yes

Parameter	Description	Recommendation	Affects SVM Compliance
LDAP Encryption	Indicates if LDAP Encryption is enabled or disabled.	Enabled	No
NTLM Authentication	Indicates if NTLM Authentication is enabled or disabled.	Enabled	No
LDAP Payload Signing	Indicates if LDAP Payload Signing is enabled or disabled.	Enabled	No
CHAP Settings	Indicates if CHAP is enabled or disabled.	Enabled	No
Kerberos V5	Indicates if Kerberos V5 authentication is enabled or disabled.	Enabled	No
NIS Authentication	Indicates if the use of NIS authentication is configured.	Disabled	No
FPolicy Status Active	Indicates if FPolicy is created or not.	Yes	No
SMB Encryption Enabled	Indicates if SMB -Signing & Sealing is not enabled.	Yes	No
SMB Signing Enabled	Indicates if SMB -Signing is not enabled.	Yes	No

Volume compliance categories

This table describes the volume encryption parameters that Unified Manager evaluates to determine whether the data on your volumes is adequately protected from being accessed by unauthorized users.

Note that the volume encryption parameters do not affect whether the cluster or storage VM is considered compliant.

Parameter	Description
Software Encrypted	Displays the number of volumes that are protected using NetApp Volume Encryption (NVE) or NetApp Aggregate Encryption (NAE) software encryption solutions.
Hardware Encrypted	Displays the number of volumes that are protected using NetApp Storage Encryption (NSE) hardware encryption.
Software and Hardware Encrypted	Displays the number of volumes that are protected by both software and hardware encryption.
Not Encrypted	Displays the number of volumes that are not encrypted.