Managing cluster security objectives

Active IQ Unified Manager

NetApp
May 05, 2022

Table of Contents

Managing cluster security objectives

Unified Manager provides a dashboard that identifies how secure your ONTAP clusters, storage virtual machines (SVMs), and volumes are based on recommendations defined in the *NetApp Security Hardening Guide for ONTAP 9*.

The goal of the security dashboard is to show any areas where your ONTAP clusters do not align with the NetApp recommended guidelines so that you can fix these potential issues. In most cases you will fix the issues using ONTAP System Manager or the ONTAP CLI. Your organization may not follow all of the recommendations, so in some cases you will not need to make any changes.

See the NetApp Security Hardening Guide for ONTAP 9 (TR-4569) for detailed recommendations and resolutions.

In addition to reporting security status, Unified Manager also generates security events for any cluster or SVM that has security violations. You can track these issues in the Event Management inventory page and you can configure alerts for these events so that your storage administrator is notified when new security events occur.

What security criteria are 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
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

Parameter	Description	Recommendation	Affects Cluster Compliance
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
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

Parameter	Description	Recommendation	Affects Cluster Compliance
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
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
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

Parameter	Description	Recommendation	Affects SVM Compliance
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.

What does not compliant mean

Clusters and storage virtual machines (SVMs) are considered not compliant when any of the security criteria that is being evaluated against the recommendations defined in the *NetApp Security Hardening Guide for ONTAP 9* are not met. Additionally, a cluster is considered not compliant when any SVM is flagged as being not compliant.

The status icons in the security cards have the following meanings in relation to their compliance:

- - The parameter is configured as recommended.
- - The parameter is not configured as recommended.
- - Either the functionality is not enabled on the cluster, or the parameter is not configured as recommended, but this parameter does not contribute to the compliance of the object.

Note that volume encryption status does not contribute to whether the cluster or SVM are considered compliant.

Viewing security status for clusters and Storage VMs

Active IQ Unified Manager enables you to view the security status of the storage objects in your environment from different points in the interface. You can collect and analyze information and reports based on defined parameters, and detect suspicious behavior or unauthorized system changes on the monitored clusters and storage VMs.

For the security recommendations, see the NetApp Security Hardening Guide for ONTAP 9

View object level security status on Security page

As a system administrator, you can use the **Security** page to get visibility into the security strength of your ONTAP clusters and storage VMs at the data center and site levels. The supported objects are cluster, storage VMs, and volumes. Follow these steps:

Steps

1. In the left navigation pane, click **Dashboard**.
2. Depending on whether you want to view security status for all monitored clusters or for a single cluster, select **All Clusters** or select a single cluster from the drop-down menu.
3. Click the right-arrow in the **Security** panel. The Security page is displayed.

Clicking the bar charts, counts, and `View Reports` links takes you to the Volumes, Clusters, or Storage VMs page for you to view the corresponding details or generate reports, as required.

The Security page displays the following panels:

- **Cluster Compliance**: the security status (number of clusters that are compliant or not compliant) of all the clusters in a data center
- **Storage VM Compliance**: the security status (number of storage VMs that are compliant or not compliant) for all the storage VMs in your data center
- **Volume Encryption**: the volume encryption status (number of volumes that are encrypted or not encrypted) of all the volumes in your environment
- **Volume Anti-ransomware Status**: the security status (number of volumes with anti-ransomware enabled or disabled) of all the volumes in your environment
- **Cluster Authentication and Certificates**: the number of clusters using each type of authentication method, such as SAML, Active Directory, or through certificates and local authentication. The panel also displays the number of clusters whose certificates have either expired or are about to expire in 60 days.

View security details of all clusters on the Clusters page

The **Clusters / Security** details page enables you to view the security compliance status at a cluster level.

Steps

1. In the left navigation pane, click **Storage > Clusters**.
2. Select **View > Security > All Clusters**.

Default security parameters, such as Global FIPS, Telnet, insecure SSH settings, login banner, network time protocol, AutoSupport HTTPS Transport, and the status of cluster certificate expiration are displayed.

You can click the ⋮ more options button and choose to view the security details on the **Security** page of Unified Manager or on System Manager. You should have valid credentials for viewing the details on System Manager.

ⓘ If a cluster has an expired certificate, you can click `expired` under **Cluster Certificate Validity**, and renew it from System Manager (9.10.1 and later). You cannot click `expired` if the System Manager instance is of a release earlier than 9.10.1.

View security details of all clusters from the storage VMs page

The **Storage VMs / Security** details page enables you to view the security compliance status at a storage VM level.

Steps

1. In the left navigation pane, click **Storage > Storage VMs**.
2. Select **View > Security > All Storage VMs**. A list of clusters with the security parameters is displayed.

You can have a default view of the storage VMs' security compliance by checking the security parameters, such as storage VMs, cluster, login banner, audit log, and insecure SSH settings.

You can click the ⋮ more options button and choose to view the security details on the **Security** page of Unified Manager or on System Manager. You should have valid credentials for viewing the details on System Manager.

For anti-ransomware security details for volumes and storage VMs, see Viewing the anti-ransomware status of all volumes and Storage VMs.

Viewing security events that may require software or firmware updates

There are certain security events that have an impact area of “Upgrade”. These events are reported from the Active IQ platform, and they identify issues where the resolution requires you to upgrade ONTAP software, node firmware, or operating system software (for security advisories).

What you’ll need

You must have the Operator, Application Administrator, or Storage Administrator role.

You may want to perform immediate corrective action for some of these issues, whereas other issues may be able to wait until your next scheduled maintenance. You can view all of these events and assign them to users who can resolve the issues. Additionally, if there are certain security upgrade events that you do not want to be notified about, this list can help you identify those events so that you can disable them.

Steps

1. In the left navigation pane, click **Event Management**.

   By default, all Active (New and Acknowledged) events are displayed on the Event Management inventory

page.

2. From the View menu, select **Upgrade events**.

   The page displays all active upgrade security events.

Viewing how user authentication is being managed on all clusters

The Security page displays the types of authentication being used to authenticate users on each cluster, and the number of users who are accessing the cluster using each type. This enables you to verify that user authentication is being performed securely as defined by your organization.

Steps

1. In the left navigation pane, click **Dashboard**.
2. At the top of the dashboard, select **All Clusters** from the drop-down menu.
3. Click the right-arrow in the **Security** panel and the **Security** page is displayed.
4. View the **Cluster Authentication** card to see the number of users who are accessing the system using each authentication type.
5. View the **Cluster Security** card to view the authentication mechanisms being used to authenticate users on each cluster.

If there are some users accessing the system using an insecure method, or using a method that is not recommended by NetApp, you can disable the method.

Viewing the encryption status of all volumes

You can view a list of all the volumes and their current encryption status so you can determine whether the data on your volumes is adequately protected from being accessed by unauthorized users.

What you'll need

You must have the Operator, Application Administrator, or Storage Administrator role.

The types of encryption that can be applied to a volume are:

- Software - Volumes that are protected using NetApp Volume Encryption (NVE) or NetApp Aggregate Encryption (NAE) software encryption solutions.
- Hardware - Volumes that are protected using NetApp Storage Encryption (NSE) hardware encryption.
- Software and Hardware - Volumes that are protected by both software and hardware encryption.
- None - Volumes that are not encrypted.

Steps

1. In the left navigation pane, click **Storage** > **Volumes**.
2. In the View menu, select **Health** > **Volumes Encryption**

3. In the **Health: Volumes Encryption** view, sort on the **Encryption Type** field, or use the Filter to display volumes that have a specific encryption type, or that are not encrypted (Encryption Type of “None”).

Viewing all active security events

You can view all the active security events and then assign each of them to a user who can resolve the issue. Additionally, if there are certain security events that you do not want to receive, this list can help you identify the events that you want to disable.

What you’ll need

You must have the Operator, Application Administrator, or Storage Administrator role.

Steps

1. In the left navigation pane, click **Event Management**.

   By default, New and Acknowledged events are displayed on the Event Management inventory page.

2. From the View menu, select **Active security events**.

   The page displays all New and Acknowledged Security events that have been generated in the past 7 days.

Adding alerts for security events

You can configure alerts for individual security events just like any other events received by Unified Manager. Additionally, if you want to treat all security events alike and have email sent to the same person, you can create a single alert to notify you when any security events are triggered.

What you’ll need

You must have the Application Administrator or Storage Administrator role.

The example below shows how to create an alert for the “Telnet Protocol Enabled” security event. This will send an alert if Telnet access is configured for remote administrative access into the cluster. You can use this same methodology to create alerts for all security events.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, click **Add**.
3. In the **Add Alert** dialog box, click **Name**, and enter a name and description for the alert.
4. Click **Resources** and select the cluster or cluster on which you want to enable this alert.
5. Click **Events** and perform the following actions:
   a. In the Event Severity list, select **Warning**.
   b. In the Matching Events list, select **Telnet Protocol Enabled**.
6. Click **Actions** and then select the name of the user who will receive the alert email in the **Alert these users** field.

7. Configure any other options on this page for notification frequency, issuing SNMP taps, and executing a script.
8. Click **Save**.

Disabling specific security events

All events are enabled by default. You can disable specific events to prevent the generation of notifications for those events that are not important in your environment. You can enable events that are disabled if you want to resume receiving notifications for them.

What you'll need

You must have the Application Administrator or Storage Administrator role.

When you disable events, the previously generated events in the system are marked obsolete, and the alerts that are configured for these events are not triggered. When you enable events that are disabled, the notifications for these events are generated starting with the next monitoring cycle.

Steps

1. In the left navigation pane, click **Storage Management** > **Event Setup**.
2. In the **Event** Setup page, disable or enable events by choosing one of the following options:

If you want to…	Then do this…
Disable events	a. Click **Disable**. b. In the Disable Events dialog box, select the **Warning** severity. This is the category for all security events. c. In the Matching Events column, select the security events that you want to disable, and then click the right arrow to move those events to the Disable Events column. d. Click **Save and Close**. e. Verify that the events that you disabled are displayed in the list view of the Event Setup page.
Enable events	a. From the list of disabled events, select the check box for the event, or events, that you want to reenable. b. Click **Enable**.

Security events

Security events provide you with information about the security status of ONTAP clusters, storage virtual machines (SVMs), and volumes based on parameters defined in the

NetApp Security Hardening Guide for ONTAP 9. These events notify you of potential issues so that you can evaluate their severity and fix the issue if necessary.

Security events are grouped by source type and include the event and trap name, impact level, and severity. These events appear in the cluster and storage VM event categories.

Copyright Information

Trademark Information