



What security criteria is being evaluated

Active IQ Unified Manager 9.9

NetApp
August 29, 2024

This PDF was generated from <https://docs.netapp.com/us-en/active-iq-unified-manager-99/health-checker/reference-cluster-compliance-categories.html> on August 29, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- What security criteria is being evaluated 1
 - Cluster compliance categories 1
 - SVM compliance categories 4
 - Volume compliance categories 5

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 Recommendations | No |
| Active Directory Users | Indicates if Active Directory is configured. Active Directory and LDAP are the preferred authentication mechanisms for users accessing clusters. | No Recommendations | 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 Recommendations | No |
| Certificate Users | Indicates if a certificate user is configured to log into the cluster. | No Recommendations | No |

| Parameter | Description | Recommendation | Affects Cluster Compliance |
|-------------|--|--------------------|----------------------------|
| Local Users | Indicates if local users are configured to log into the cluster. | No Recommendations | No |

SVM 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 compliant or not compliant.

| 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 <code>cbc*</code> . | 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 |

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. |

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.