# 评估的安全条件

## Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/active-iq-unified-manager-918/health-checker/concept_what_security_criteria_is_being_evaluated.html on November 13, 2026. Always check docs.netapp.com for the latest.

# 目录

评估的安全条件 . . . . . 1
了解 Active IQ Unified Manager 如何评估安全标准 . . . . . 1
了解 Active IQ Unified Manager 中的集群合规性类别 . . . . . 1
了解 Active IQ Unified Manager 中的 Storage VM 合规性类别 . . . . . 3
了解 Active IQ Unified Manager 中的卷合规性类别 . . . . . 4

# 评估的安全条件

## 了解 Active IQ Unified Manager 如何评估安全标准

一般来说，将根据 *NetApp Security Hardening Guide for ONTAP 9* 中定义的建议评估您的 ONTAP 集群、存储虚拟机（SVM）和卷的安全标准。

其中一些安全检查包括：

- 集群是否正在使用安全身份验证方法，例如 SAML
- 对等集群的通信是否已加密
- storage VM 是否已启用其审核日志
- 您的卷是否启用了软件或硬件加密

有关详细信息，请参见有关合规类别和 "适用于 ONTAP 9 的 NetApp 安全强化指南"的主题。

> 从 Active IQ 平台报告的升级事件也被视为安全事件。这些事件指出了需要升级 ONTAP 软件、节点固件或操作系统软件（针对安全公告）才能解决的问题。这些事件不会显示在安全面板中，但可以从事件管理清单页面中获取。

有关详细信息，请参见"管理集群安全目标"。

## 了解 Active IQ Unified Manager 中的集群合规性类别

此表描述了 Unified Manager 评估的集群安全合规性参数、NetApp 建议，以及该参数是否影响集群合规或不合规的整体判定。

在集群上具有不合规的 SVM 将影响集群的合规值。因此，在某些情况下，在集群安全被视为合规之前，您可能需要解决 SVM 的安全问题。

请注意，并非所有安装都会显示下面列出的所有参数。例如，如果没有对等群集，或者在群集上禁用了 AutoSupport，则不会在 UI 页面中看到群集对等或 AutoSupport HTTPS 传输项目。

| 参数 | 问题描述 | 建议 | 影响集群合规性 |
| --- | --- | --- | --- |
| 全局 FIPS | 指示是否启用或禁用全球 FIPS（联邦信息处理标准）140-2 合规模式。启用 FIPS 后，TLSv1 和 SSLv3 将被禁用，只允许 TLSv1.1 和 TLSv1.2。 | 已启用 | 是 |
| Telnet | 指示对系统的 Telnet 访问是启用还是禁用。NetApp 建议使用安全 Shell（SSH）进行安全远程访问。 | 已禁用 | 是 |

| 参数 | 问题描述 | 建议 | 影响集群合规性 |
| --- | --- | --- | --- |
| 不安全 SSH 设置 | 指示 SSH 是否使用不安全密码，例如以 *cbc 开头的密码。 | 否 | 是 |
| 登录横幅 | 指示是否为访问系统的用户启用或禁用登录横幅。 | 已启用 | 是 |
| 创建集群对等关系 | 指示对等集群之间的通信是加密还是未加密。必须在源和目标集群上配置加密，才能将此参数视为合规。 | 已加密 | 是 |
| 网络时间协议 | 指示集群是否具有一个或多个配置的 NTP 服务器。为了保证冗余和最佳服务，NetApp 建议至少将三个 NTP 服务器与集群相关联。 | 已配置 | 是 |
| OCSP | 从 9.14.1 开始，Active IQ Unified Manager 在 Storage Virtual Machine（SVM，以前称为 Vserver）级别提供在线证书状态协议（OCSP）状态信息。这意味着 OCSP 验证将应用于与 SVM 建立的所有 SSL/TLS 连接，并确保这些连接中使用的证书的完整性和有效性。 | 已启用 | 否 |
| 远程审核日志记录 | 指示日志转发（Syslog）是否已加密。 | 已加密 | 是 |
| AutoSupport HTTPS 传输 | 指示是否使用 HTTPS 作为默认传输协议，用于向 NetApp 支持发送 AutoSupport 消息。 | 已启用 | 是 |
| 默认管理员用户 | 指示是否启用或禁用默认管理员用户（内置）。NetApp 建议锁定（禁用）任何不需要的内置帐户。 | 已禁用 | 是 |
| SAML 用户 | 指示是否配置了 SAML。通过 SAML，您可以将多因素身份验证（MFA）配置为单点登录的登录方法。 | 否 | 否 |

| 参数 | 问题描述 | 建议 | 影响集群合规性 |
| --- | --- | --- | --- |
| Active Directory 用户 | 指示是否配置了 Active Directory。Active Directory 和 LDAP 是用户访问集群的首选身份验证机制。 | 否 | 否 |
| LDAP 用户 | 指示是否配置了 LDAP。相比本地用户，Active Directory 和 LDAP 是管理集群的用户首选的身份验证机制。 | 否 | 否 |
| 证书用户 | 指示是否已将证书用户配置为登录到集群。 | 否 | 否 |
| 本地用户 | 指示是否将本地用户配置为登录到集群。 | 否 | 否 |
| 远程 Shell | 指示是否启用了 RSH。出于安全原因，应禁用 RSH。首选用于安全远程访问的 Secure Shell (SSH)。 | 已禁用 | 是 |
| MD5 正在使用 | 指示 ONTAP 用户帐户是否使用不太安全的 MD5 哈希函数。最好将 MD5 哈希用户帐户迁移到更安全的加密哈希函数，如 SHA-512。 | 否 | 是 |
| 证书颁发者类型 | 指示使用的数字证书的类型。 | CA 签名 | 否 |

# 了解 **Active IQ Unified Manager** 中的 **Storage VM** 合规性类别

此表描述了 Unified Manager 评估的 Storage Virtual Machine (SVM) 安全合规性标准、NetApp 建议，以及该参数是否影响对 SVM 合规或不合规的整体判定。

| 参数 | 问题描述 | 建议 | 影响 **SVM** 合规性 |
| --- | --- | --- | --- |
| 审核日志 | 指示是否启用或禁用审核日志记录。 | 已启用 | 是 |
| 不安全 SSH 设置 | 指示 SSH 是否使用不安全的密码，例如以 `cbc*`开头的密码。 | 否 | 是 |
| 登录横幅 | 指示用户访问系统上的 SVM 时，登录横幅是否已启用或禁用。 | 已启用 | 是 |
| LDAP 加密 | 指示 LDAP 加密是否已启用或禁用。 | 已启用 | 否 |

| 参数 | 问题描述 | 建议 | 影响 **SVM** 合规性 |
| --- | --- | --- | --- |
| NTLM 身份验证 | 指示 NTLM 身份验证是否已启用或禁用。 | 已启用 | 否 |
| LDAP 负载签名 | 指示是启用还是禁用 LDAP 负载签名。 | 已启用 | 否 |
| CHAP 设置 | 指示 CHAP 是启用还是禁用。 | 已启用 | 否 |
| Kerberos V5 | 指示是启用还是禁用 Kerberos V5 身份验证。 | 已启用 | 否 |
| NIS 身份验证 | 指示是否配置了使用 NIS 身份验证。 | 已禁用 | 否 |
| FPolicy 状态活动 | 指示是否已创建 FPolicy。 | 是 | 否 |
| 已启用 SMB 加密 | 指示是否未启用 SMB - 签名和密封。 | 是 | 否 |
| 已启用 SMB 签名 | 指示是否未启用 SMB - 签名。 | 是 | 否 |

# 了解 **Active IQ Unified Manager** 中的卷合规性类别

此表描述了 Unified Manager 评估的卷加密参数，以确定卷上的数据是否得到充分保护，防止未经授权的用户访问。

请注意，卷加密参数不影响集群或存储 VM 是否被视为合规。

| 参数 | 问题描述 |
| --- | --- |
| 软件加密 | 显示使用 NetApp 卷加密（NVE）或 NetApp 聚合加密（NAE）软件加密解决方案保护的卷数。 |
| 硬件加密 | 显示使用 NetApp 存储加密（NSE）硬件加密保护的卷数。 |
| 软件加密和硬件加密 | 显示受软件和硬件加密保护的卷数。 |
| 未加密 | 显示未加密的卷数。 |

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。