管理集群安全目标

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_manage_cluster_security_objectives.html on November 13, 2026. Always check docs.netapp.com for the latest.

目录

管理集群安全目标 1
在 Active IQ Unified Manager 中管理集群安全目标 1
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
了解 Active IQ Unified Manager 中的集群和 SVM 合规性状态 5
在 Active IQ Unified Manager 中查看集群和 Storage VM 的安全状态 5
在安全页面上查看对象级安全状态 5
在集群页面上查看所有集群的安全详细信息 6
从 Storage VMs 页面查看所有集群的安全详细信息 6
查看 Active IQ Unified Manager 中可能需要软件或固件更新的安全事件 6
查看集群如何在 Active IQ Unified Manager 中的所有集群上管理用户身份验证 7
查看 Active IQ Unified Manager 中所有卷的加密状态 7
查看 Active IQ Unified Manager 中所有卷和存储 VM 的反勒索软件状态 8
查看具有反勒索软件检测功能的所有卷的安全详细信息 8
查看具有反勒索软件检测功能的所有 Storage VM 的安全详细信息 8
查看 Active IQ Unified Manager 中的所有活动安全事件 8
在 Active IQ Unified Manager 中添加安全事件警报 9
在 Active IQ Unified Manager 中禁用特定安全事件 9
在 Active IQ Unified Manager 中查看安全事件 10

管理集群安全目标

在 **Active IQ Unified Manager** 中管理集群安全目标

Unified Manager 提供了一个仪表板，用于根据 *NetApp Security Hardening Guide for ONTAP 9* 中定义的建议，确定您的 ONTAP 集群、存储虚拟机（SVM）和卷的安全程度。

安全控制面板的目标是显示您的 ONTAP 集群与 NetApp 建议指南不一致的任何区域，以便您可以解决这些潜在问题。在大多数情况下，您可以使用 ONTAP System Manager 或 ONTAP CLI 解决问题。您的组织可能不会遵循所有建议，因此在某些情况下，您无需进行任何更改。

有关详细建议和解决方法，请参见 "适用于 ONTAP 9 的 NetApp 安全强化指南"（TR-4569）。

除了报告安全状态之外，Unified Manager 还会为存在安全违规的任何群集或 SVM 生成安全事件。您可以在“事件管理清单”页面中跟踪这些问题，还可以为这些事件配置警报，以便在发生新安全事件时通知存储管理员。

有关详细信息，请参见"正在评估哪些安全标准"。

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
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

参数	问题描述	建议	影响集群合规性
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
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
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。

了解 Active IQ Unified Manager 中的集群和 SVM 合规性状态

如果不符合根据 *NetApp Security Hardening Guide for ONTAP 9* 中定义的建议评估的任一安全条件，则集群和 Storage Virtual Machine (SVM) 将视为不合规。此外，如果任何 SVM 标记为不合规，则集群将视为不合规。

安全卡中的状态图标相对于其合规性具有下列含义：

- - 参数按建议配置。
- - 未按建议配置参数。
- - 此功能未在集群上启用，或此参数未按建议配置，但此参数不会影响对象的合规性。

请注意，卷加密状态与集群或 SVM 是否合规无关。

在 Active IQ Unified Manager 中查看集群和 Storage VM 的安全状态

Active IQ Unified Manager 允许您从界面中的不同点查看环境中存储对象的安全状态。您可以根据定义的参数收集和分析信息和报告，并检测受监控集群和存储虚拟机上的可疑行为或未经授权的系统更改。

有关安全建议，请参见 "适用于 ONTAP 9 的 NetApp 安全强化指南"

在安全页面上查看对象级安全状态

作为系统管理员，您可以使用 安全 页面了解您的 ONTAP 集群和存储虚拟机在数据中心和站点级别的安全强度。支持的对象是集群、存储虚拟机和卷。请按照以下步骤操作：

步骤

1. 在左侧导航窗格中，单击*仪表板*。
2. 根据您是要查看所有受监控集群还是单个集群的安全状态，选择 所有集群 或从下拉菜单中选择单个集群。
3. 单击*安全*面板中的右箭头。此时将显示“安全”页面。

单击条形图、计数和 `View Reports`链接将转到卷、群集或 Storage VM 页面，以便您根据需要查看相应的详细信息或生成报告。

安全页面显示以下面板：

- 集群合规性：数据中心中所有集群的安全状态（合规或不合规的集群数量）
- 存储虚拟机合规性：数据中心中所有存储虚拟机的安全状态（合规或不合规的存储虚拟机数量）
- 卷加密：环境中所有卷的卷加密状态（已加密或未加密的卷数量）
- 卷反勒索软件状态：环境中所有卷的安全状态（启用或禁用反勒索软件的卷数）
- 集群身份验证和证书：使用每种身份验证方法（如 SAML、Active Directory 或通过证书和本地身份验证）的集群数量。该面板还显示证书已过期或将在 60 天内过期的集群数量。

在集群页面上查看所有集群的安全详细信息

*集群/安全*详细信息页面使您能够查看集群级别的安全合规性状态。

步骤

1. 在左侧导航窗格中，单击*存储 > 群集*。
2. 选择 查看 **>** 安全 **>** 所有集群。

将显示默认安全参数，例如全局 FIPS、Telnet、不安全的 SSH 设置、登录横幅、网络时间协议、AutoSupport HTTPS 传输以及集群证书过期状态。

您可以单击 ⋮ 更多选项按钮，并选择在 Unified Manager 的*安全*页面或 System Manager 上查看安全详细信息。您应该拥有有效的凭据才能在 System Manager 上查看详细信息。

> ⓘ 如果集群的证书已过期，您可以单击 **Cluster Certificate Validity** 下的 `expired`，然后从 System Manager（9.10.1 及更高版本）续订。如果 System Manager 实例的版本早于 9.10.1，则无法单击 `expired`。

从 **Storage VMs** 页面查看所有集群的安全详细信息

可使用 存储 **VM /** 安全 详细信息页面查看存储 VM 级别的安全合规性状态。

步骤

1. 在左侧导航窗格中，单击 **Storage > Storage VMs**。
2. 选择 查看 **>** 安全 **>** 所有 **Storage VM**。此时将显示包含安全参数的集群列表。

您可以通过检查安全参数（例如存储 VM、集群、登录横幅、审计日志和不安全的 SSH 设置）来默认查看存储 VM 的安全合规性。

您可以单击 ⋮ 更多选项按钮，并选择在 Unified Manager 的*安全*页面或 System Manager 上查看安全详细信息。您应该拥有有效的凭据才能在 System Manager 上查看详细信息。

有关卷和存储 VM 的反勒索软件安全详细信息，请参见 "查看所有卷和 Storage VM 的反勒索软件状态"。

查看 **Active IQ Unified Manager** 中可能需要软件或固件更新的安全事件

某些安全事件的影响区域为“`Upgrade`”。这些事件由 Active IQ 平台报告，它们指出的问题需要您通过升级 ONTAP 软件、节点固件或操作系统软件（针对安全公告）来解决。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

您可能需要立即对其中一些问题执行纠正措施，而其他问题可能要等到下一次定期维护时才能解决。您可以查看所有这些事件，并将其分配给可以解决问题的用户。此外，如果存在某些您不希望收到通知的安全升级事件，此列表可以帮助您识别这些事件，以便您可以将其禁用。

步骤

1. 在左侧导航窗格中，单击*事件管理*。

   默认情况下，所有活动（新建和已确认）事件都将显示在事件管理清单页面上。

2. 在“视图”菜单中，选择 升级事件。

   此页面显示所有活动升级安全事件。

查看集群如何在 Active IQ Unified Manager 中的所有集群上管理用户身份验证

安全页面显示用于对每个群集上的用户进行身份验证的身份验证类型，以及使用每种类型访问群集的用户数。这使您能够验证是否按照组织的定义安全地执行用户身份验证。

步骤

1. 在左侧导航窗格中，单击*仪表板*。
2. 在仪表板的顶部，从下拉菜单中选择*所有集群*。
3. 单击*安全*面板中的右箭头，将显示*安全*页面。
4. 查看*集群身份验证*卡，查看使用每种身份验证类型访问系统的用户数量。
5. 查看*集群安全*卡以查看用于对每个集群上的用户进行身份验证的身份验证机制。

如果有一些用户使用不安全的方法或 NetApp 不推荐的方法访问系统，您可以禁用该方法。

查看 Active IQ Unified Manager 中所有卷的加密状态

您可以查看所有卷及其当前加密状态的列表，以便确定卷上的数据是否受到充分保护，防止未经授权的用户访问。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

可以应用于卷的加密类型包括：

- 软件 — 使用 NetApp 卷加密 (NetApp Volume Encryption, NVE) 或 NetApp 聚合加密 (NetApp Aggregate Encryption, NAE) 软件加密解决方案进行保护的卷。
- 硬件 — 使用 NetApp 存储加密 (NetApp Storage Encryption, NSE) 硬件加密进行保护的卷。
- 软件和硬件 — 同时使用软件和硬件加密进行保护的卷。
- 无 — 未加密的卷。

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在 View 菜单中，选择 **Health** > **Volumes Encryption**
3. 在*运行状况：卷加密*视图中，对*加密类型*字段进行排序，或使用筛选器显示具有特定加密类型或未加密的卷（加密类型为 “None”）。

查看 Active IQ Unified Manager 中所有卷和存储 VM 的反勒索软件状态

您可以查看所有卷和存储虚拟机（SVM）的列表及其当前反勒索软件状态，以便确定卷和 SVM 上的数据是否受到充分保护，免受勒索软件攻击。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

有关不同反勒索软件状态的更多信息，请参见 "ONTAP：启用反勒索软件"。

查看具有反勒索软件检测功能的所有卷的安全详细信息

步骤

1. 在左侧导航窗格中，单击 **Storage** > **Volumes**。
2. 在“视图”菜单中，选择 运行状况 > 安全 > 防勒索软件
3. 在*安全：反勒索软件*视图中，您可以按各个字段排序或使用筛选器。

离线卷、受限卷、SnapLock 卷、FlexGroup 卷、FlexCache 卷、仅 SAN 卷、已停止存储虚拟机的卷、存储虚拟机的根卷或数据保护卷不支持反勒索软件。

查看具有反勒索软件检测功能的所有 **Storage VM** 的安全详细信息

步骤

1. 在左侧导航窗格中，单击 **Storage > Storage VMs**。
2. 选择 查看 **>** 安全 **>** 反勒索软件。此时将显示具有反勒索软件状态的 SVM 列表。

未启用 NAS 协议的存储 VM 不支持防勒索软件监控。

查看 Active IQ Unified Manager 中的所有活动安全事件

您可以查看所有活动的安全事件，然后将每个事件分配给可以解决此问题的用户。此外，如果您不希望接收某些安全事件，此列表可帮助您确定要禁用的事件。

开始之前

您必须具有操作员、应用程序管理员或存储管理员角色。

步骤

1. 在左侧导航窗格中，单击*事件管理*。

   默认情况下，“新建”和“已确认”事件将显示在“事件管理”清单页面上。

2. 在“视图”菜单中，选择 活动安全事件。

   该页面显示过去 7 天生成的所有新建和已确认的安全事件。

在 Active IQ Unified Manager 中添加安全事件警报

您可以为单个安全事件配置警报，就像 Unified Manager 接收的任何其他事件一样。此外，如果您希望以相同方式处理所有安全事件，并将电子邮件发送给同一个人，则可以创建单个警报，以便在触发任何安全事件时通知您。

开始之前

您必须具有应用程序管理员或存储管理员角色。

下面的示例演示如何为“`Telnet Protocol Enabled`”安全事件创建警报。如果将 Telnet 访问配置为对集群进行远程管理访问，这将发送警报。您可以使用相同的方法为所有安全事件创建警报。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 警报设置。
2. 在*警报设置*页面中，单击*添加*。
3. 在*添加警报*对话框中，单击*名称*，并输入警报的名称和描述。
4. 单击*资源*并选择要启用此警报的集群或集群。
5. 单击 事件 并执行以下操作：
   a. 在事件严重程度列表中，选择*警告*。
   b. 在匹配事件列表中，选择 **Telnet Protocol Enabled**。
6. 单击*操作*，然后在*提醒这些用户*字段中选择将接收警报电子邮件的用户的名称。
7. 在此页面上配置有关通知频率、发出 SNMP 陷阱和执行脚本的任何其他选项。
8. 单击 **Save**。

在 Active IQ Unified Manager 中禁用特定安全事件

默认情况下，所有事件均处于启用状态。您可以禁用特定事件，以防止为环境中不重要的事件生成通知。如果您希望恢复接收有关这些事件的通知，可以启用已禁用的事件。

开始之前

您必须具有应用程序管理员或存储管理员角色。

禁用事件时，系统中以前生成的事件将被标记为已废弃，并且不会触发为这些事件配置的警报。启用已禁用的事件后，将从下一监控周期开始生成这些事件的通知。

步骤

1. 在左侧导航窗格中，单击*存储管理* > 事件设置。
2. 在*事件*设置页面中，通过选择以下选项之一禁用或启用事件：

目的	操作
禁用事件	a. 单击 **Disable**。 b. 在禁用事件对话框中，选择*警告*严重性。这是所有安全事件的类别。 c. 在匹配事件列中，选择要禁用的安全事件，然后单击右箭头将这些事件移动到禁用事件列。 d. 单击*保存并关闭*。 e. 验证已禁用的事件是否显示在“事件设置”页面的列表视图中。
启用事件	a. 从禁用事件列表中，选中要重新启用的事件的复选框。 b. 单击 启用。

在 **Active IQ Unified Manager** 中查看安全事件

安全事件根据 *NetApp Security Hardening Guide for ONTAP 9* 中定义的参数，为您提供有关 ONTAP 集群、存储虚拟机（SVM）和卷的安全状态信息。这些事件会通知您潜在的问题，以便您评估其严重程度，并在必要时解决问题。

安全事件按源类型分组，包括事件和陷阱名称、影响级别和严重程度。这些事件出现在集群和存储 VM 事件类别中。

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。