管理集群安全目标

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

目录

管理集群安全目标

Unified Manager 提供了一个信息板，用于根据适用于 ONTAP 9_ 的 _NetApp 安全加固指南中定义的建议确定 ONTAP 集群， Storage Virtual Machine （ SVM ）和卷的安全程度。

此安全信息板的目标是，显示 ONTAP 集群与 NetApp 建议的准则不一致的任何区域，以便您可以修复这些潜在问题。大多数情况下，您将使用 ONTAP 系统管理器或 ONTAP 命令行界面修复这些问题。您的组织可能不会遵循所有建议，因此在某些情况下，您不需要进行任何更改。

请参见 "《适用于 ONTAP 9 的 NetApp 安全加固指南》" （ TR-4569 ），了解详细的建议和解决方案。

除了报告安全状态之外， Unified Manager 还会为存在安全违规的任何集群或 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，并为这些事件配置警报，以便在发生新的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"。

正在评估哪些安全标准

通常，我们会根据适用于 ONTAP 9_ 的 _NetApp 安全加固指南中定义的建议评估 ONTAP 集群， Storage Virtual Machine （ SVM ）和卷的安全标准。

部分安全检查包括：

- 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 是否已启用审核日志
- 卷已启用软件加密还是硬件加密

请参见有关合规性类别的主题和 "《适用于 ONTAP 9 的 NetApp 安全加固指南》" 了解详细信息。

> 从 Active IQ 平台报告的升级事件也视为安全事件。这些事件确定了需要升级 ONTAP 软件，节点固件或操作系统软件才能解决的问题（针对安全建议）。这些事件不会显示在 " 安全性 " 面板中，但可从 " 事件管理 " 清单页面访问。

有关详细信息，请参见 "管理集群安全目标"。

集群合规性类别

下表介绍了 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对集群是否合规性的整体判断。

集群上存在不合规的 SVM 将影响集群的合规性值。因此，在某些情况下，您可能需要先修复 SVM 的安全问题，然后才能将集群安全性视为合规。

请注意，并非所有安装都显示以下列出的所有参数。例如，如果您没有对等集群，或者您在集群上禁用了 AutoSupport ，则您将不会在 UI 页面中看到集群对等或 AutoSupport HTTPS 传输项。

参数	**Description**	建议	影响集群合规性
全局 FIPS	指示是否已启用全局 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，并且仅允许使用 TLSv1.1 和 TLSv1.2 。	enabled	是的。
Telnet	指示是启用还是禁用了对系统的 Telnet 访问。NetApp 建议使用安全 Shell （ SSH ）进行安全远程访问。	已禁用	是的。
SSH 设置不安全	指示 SSH 是否使用不安全的密码，例如以 * CBC 开头的密码。	否	是的。
登录横幅	指示是否为访问系统的用户启用了登录横幅。	enabled	是的。
集群对等	指示对等集群之间的通信是加密的还是未加密的。必须在源集群和目标集群上配置加密，才能将此参数视为合规。	Encrypted	是的。
网络时间协议	指示集群是否已配置一个或多个 NTP 服务器。为了获得冗余和最佳服务，NetApp 建议至少将三个 NTP 服务器与集群相关联。	Configured	是的。
OCSP	指示 ONTAP 中是否存在未配置 OCSP （联机证书状态协议）的应用程序，因此通信不会加密。此时将列出不合规的应用程序。	enabled	否
远程审核日志记录	指示日志转发（ Syslog ）是加密还是未加密。	Encrypted	是的。

参数	**Description**	建议	影响集群合规性
AutoSupport HTTPS 传输	指示是否使用 HTTPS 作为向 NetApp 支持部门发送 AutoSupport 消息的默认传输协议。	enabled	是的。
默认管理员用户	指示是启用还是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	是的。
SAML 用户	指示是否已配置 SAML 。通过 SAML ，您可以将多因素身份验证（ Multi-Factor Authentication ，MFA ）配置为单点登录的登录方法。	否	否
Active Directory 用户	指示是否已配置 Active Directory 。Active Directory 和 LDAP 是访问集群的用户的首选身份验证机制。	否	否
LDAP 用户	指示是否已配置 LDAP 。对于通过本地用户管理集群的用户来说， Active Directory 和 LDAP 是首选身份验证机制。	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	指示是否已将本地用户配置为登录到集群。	否	否
远程 Shell	指示是否已启用 RSH 。出于安全原因，应禁用 RSH 。首选使用安全 Shell （ SSH ）进行安全远程访问。	已禁用	是的。

参数	Description	建议	影响集群合规性
MD5 正在使用中	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，例如 SHA-512 。	否	是的。
证书颁发者类型	指示使用的数字证书类型。	CA 签名	否

Storage VM 合规性类别

下表介绍了 Unified Manager 评估的 Storage Virtual Machine （ SVM ） 安全合规性标准， NetApp 建议以及参数是否影响对 SVM 是否合规的整体判断。

参数	Description	建议	影响 SVM 合规性
审核日志	指示是否已启用审核日志记录。	enabled	是的。
SSH 设置不安全	指示SSH是否使用不安全的密码、例如以开头的密码 `cbc*`。	否	是的。
登录横幅	指示是否为访问系统上 SVM 的用户启用了登录横幅。	enabled	是的。
LDAP 加密	指示是否已启用 LDAP 加密。	enabled	否
NTLM 身份验证	指示是否已启用 NTLM 身份验证。	enabled	否
LDAP 有效负载签名	指示是否已启用 LDAP 有效负载签名。	enabled	否
CHAP 设置	指示是否已启用 CHAP 。	enabled	否
Kerberos V5	指示是启用还是禁用 Kerberos V5 身份验证。	enabled	否
NIS 身份验证	指示是否配置了使用 NIS 身份验证。	已禁用	否

参数	Description	建议	影响 SVM 合规性
FPolicy 状态为活动	指示是否已创建 FPolicy 。	是的。	否
已启用 SMB 加密	指示是否未启用 SMB 签名和密封。	是的。	否
已启用 SMB 签名	指示是否未启用 SMB 签名。	是的。	否

卷合规性类别

下表介绍了 Unified Manager 评估的卷加密参数，这些参数用于确定卷上的数据是否受到充分保护，不会被未经授权的用户访问。

请注意，卷加密参数不会影响集群或 Storage VM 是否合规。

参数	Description
软件加密	显示使用 NetApp 卷加密（NetApp Volume Encryption， NVE）或 NetApp 聚合加密（NetApp Aggregate Encryption， NAE）软件加密解决方案保护的卷数。
硬件已加密	显示使用 NetApp 存储加密（NetApp Storage Encryption， NSE）硬件加密进行保护的卷数。
软件和硬件已加密	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。

不合规的含义

如果不满足根据适用于 ONTAP 9_ 的 _NetApp 安全加固指南中定义的建议评估的任何安全标准，则会将集群和 Storage Virtual Machine （SVM）视为不合规。此外，如果任何 SVM 被标记为不合规，则集群将被视为不合规。

安全卡中的状态图标对于其合规性具有以下含义：

- - 此参数已按照建议进行配置。
- - 未按建议配置参数。
- —未在集群上启用此功能，或者未按建议配置此参数，但此参数不会影响对象的合规性。

请注意，卷加密状态不会影响集群或 SVM 是否合规。

查看集群和Storage VM的安全状态

通过Active IQ Unified Manager 、您可以从界面的不同位置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Storage VM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 安全加固指南》"

在安全性页面上查看对象级别的安全状态

作为系统管理员、您可以使用*安全性*页面查看ONTAP 集群和Storage VM在数据中心和站点级别的安全优势。支持的对象包括集群、Storage VM和卷。请按照以下步骤操作：

步骤

1. 在左侧导航窗格中，单击 * 信息板 * 。
2. 根据您要查看所有受监控集群或单个集群的安全状态，选择 * 所有集群 * 或从下拉菜单中选择一个集群。
3. 单击 * 安全性 * 面板中的右箭头。此时将显示安全性页面。

单击条形图、计数和 `View Reports` 通过链接、您可以转到卷、集群或Storage VM页面、以便根据需要查看相应的详细信息或生成报告。

安全性页面将显示以下面板：

- 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)
- * Storage VM Compliance *：数据中心中所有Storage VM的安全状态(合规或不合规的Storage VM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)
- 卷反勒索软件状态：环境中所有卷的安全状态(启用或禁用了反勒索软件的卷数)
- 集群身份验证和证书：使用SAML、Active Directory等每种身份验证方法或通过证书和本地身份验证的集群数量。此面板还会显示证书已过期或将在60天后过期的集群数量。

在集群页面上查看所有集群的安全详细信息

通过*集群/安全性*详细信息页面、您可以查看集群级别的安全合规状态。

步骤

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

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、 此时将显示AutoSupport HTTPS传输以及集群证书到期状态。

您可以单击 ⋮ 更多选项按钮、然后选择在Unified Manager的*安全性*页面或System Manager上查看安全详细信息。您应具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 `expired` 在*集群证书有效期*下、并从System Manager (9.10.1及更高版本)续订此证书。您不能单击 `expired` System Manager实例的版本早于9.10.1。

从Storage VM页面查看所有集群的安全详细信息

通过*存储VM /安全性*详细信息页面、您可以查看Storage VM级别的安全合规状态。

步骤

1. 在左侧导航窗格中、单击*存储>存储VM*。
2. 选择*查看>安全性>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Storage VM、集群、登录横幅、审核日志和不安全的SSH设置)来查看Storage VM的安全合规性的默认视图。

您可以单击 ⋮ 更多选项按钮、然后选择在Unified Manager的*安全性*页面或System Manager上查看安全详细信息。您应具有有效的凭据才能在System Manager上查看详细信息。

有关卷和Storage 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"。

查看可能需要更新软件或固件的安全事件

某些安全事件的影响区域为 "`Upgrade` " 。这些事件是从 Active IQ 平台报告的，它们确定了需要升级 ONTAP 软件，节点固件或操作系统软件才能解决的问题（有关安全建议）。

- 您需要的内容 *

您必须具有操作员，应用程序管理员或存储管理员角色。

您可能希望对其中某些问题立即执行更正操作，而其他问题则可以等待您的下一次计划维护。您可以查看所有这些事件，并将其分配给可以解决这些问题的用户。此外，如果您不希望收到有关某些安全升级事件的通知，此列表可帮助您确定这些事件，以便您可以禁用它们。

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（新增和已确认）事件都会显示在事件管理清单页面上。

2. 从 " 视图 " 菜单中，选择 * 升级事件 * 。

   此页面将显示所有活动的升级安全事件。

查看如何在所有集群上管理用户身份验证

" 安全性 " 页面显示用于对每个集群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集群的用户数量。这样，您就可以验证是否按照贵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 * 信息板 * 。
2. 从信息板顶部的下拉菜单中选择 * 所有集群 * 。

3. 单击 * 安全性 * 面板中的右箭头，此时将显示 * 安全性 * 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。
5. 查看 * 集群安全性 * 卡，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。

如果某些用户使用不安全的方法或 NetApp 不建议的方法访问系统，您可以禁用此方法。

查看所有卷的加密状态

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

- 您需要的内容 *

您必须具有操作员，应用程序管理员或存储管理员角色。

可应用于卷的加密类型包括：

- 软件—使用 NetApp 卷加密（ NVE ）或 NetApp 聚合加密（ 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—受软件和硬件加密保护的卷。
- 无—未加密的卷。

步骤

1. 在左侧导航窗格中，单击 * 存储 * > * 卷 * 。
2. 在视图菜单中，选择 * 运行状况 * > * 卷加密 *
3. 在 * 运行状况：卷加密 * 视图中，对 * 加密类型 * 字段进行排序，或者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 "`None` "）。

查看所有卷和**Storage VM**的反勒索软件状态

您可以查看所有卷和Storage VM (SVM)及其当前防勒索软件状态的列表、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。

- 您需要的内容 *

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详细信息、请参见 "ONTAP ： 支持反勒索软件"。

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 * 存储 * > * 卷 * 。
2. 在视图菜单中、选择*运行状况*>*安全*>*防勒索软件*

3. 在*安全性：反勒索软件*视图中、您可以按各个字段进行排序或使用筛选器。

> 脱机卷、受限卷、SnapLock 卷、FlexGroup 卷、FlexCache 卷、 仅SAN卷、已停止Storage VM的卷、Storage VM的根卷或数据保护卷。

查看具有防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*存储>存储VM*。
2. 选择*查看>安全性>反勒索软件*。此时将显示具有防勒索软件状态的SVM列表。

> 未启用NAS协议的Storage VM不支持反勒索软件监控。

查看所有活动安全事件

您可以查看所有活动的安全事件，然后将每个事件分配给一个可以解决问题描述的用户。此外，如果您不想接收某些安全事件，此列表可帮助您确定要禁用的事件。

- 您需要的内容 *

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. 从 " 视图 " 菜单中，选择 * 活动安全事件 * 。

   此页面将显示过去 7 天生成的所有新增和已确认安全事件。

为安全事件添加警报

您可以为单个安全事件配置警报，就像 Unified Manager 收到的任何其他事件一样。此外，如果您希望对所有安全事件进行同样的处理并将电子邮件发送给同一个人，则可以创建一个警报，以便在触发任何安全事件时向您发出通知。

- 您需要的内容 *

您必须具有应用程序管理员或存储管理员角色。

以下示例显示了如何为 "`Telnet Protocol Enabled` " 安全事件创建警报。如果为远程管理访问集群配置了 Telnet 访问，则此操作将发送警报。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 * ，然后输入警报的名称和问题描述。
4. 单击 * 资源 * ，然后选择要启用此警报的集群。
5. 单击 * 事件 * 并执行以下操作：
   a. 在事件严重性列表中，选择 * 警告 * 。
   b. 在匹配事件列表中，选择 * 已启用 Telnet 协议 * 。
6. 单击 * 操作 * ，然后在 * 提醒这些用户 * 字段中选择要接收警报电子邮件的用户的名称。
7. 在此页面上配置任何其他选项，以确定通知频率，发出 SNMP 陷阱和执行脚本。
8. 单击 * 保存 * 。

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。如果要恢复接收已禁用事件的通知，可以启用这些事件。

- 您需要的内容 *

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，系统中先前生成的事件将标记为已废弃，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，将从下一个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：

如果您要 ...	然后执行此操作 ...
禁用事件	a. 单击 * 禁用 * 。 b. 在禁用事件对话框中，选择 * 警告 * 严重性。此类别适用于所有安全事件。 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 Event Setup 页面的列表视图中。
启用事件	a. 从已禁用事件列表中，选中要重新启用的一个或多个事件对应的复选框。 b. 单击 * 启用 * 。

安全事件

安全事件根据适用于 ONTAP 9_ 的 _NetApp 安全加固指南中定义的参数，为您提供有关 ONTAP 集群， Storage Virtual Machine （ SVM ）和卷的安全状态的信息。这些事件会向您通知潜在问题，以便您评估其严重性并在必要时修复问题描述。

安全事件按源类型分组，并包括事件和陷阱名称，影响级别和严重性。这些事件显示在集群和 Storage VM 事件类别中。