评估的安全标准是什么

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

目录

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。

参数	Description	建议	影响集群合规性
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。
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

参数	Description	建议	影响集群合规性
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。
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。

参数	Description	建议	影响 SVM 合规性
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 Settings (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
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。