평가 대상 보안 기준

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

목차

평가 대상 보안 기준

일반적으로 ONTAP 클러스터, SVM(스토리지 가상 머신), 볼륨에 대한 보안 기준은 ONTAP 9_에 대한_NetApp 보안 강화 가이드에 정의된 권장사항을 기준으로 평가됩니다.

일부 보안 검사는 다음과 같습니다.

- 클러스터에서 SAML과 같은 보안 인증 방법을 사용하는지 여부
- 피어링된 클러스터의 통신이 암호화되었는지 여부
- 스토리지 VM에 감사 로그가 설정되었는지 여부
- 볼륨에 소프트웨어 또는 하드웨어 암호화가 활성화되어 있는지 여부

규정 준수 범주 및 에 대한 항목을 참조하십시오 "ONTAP 9에 대한 NetApp 보안 강화 가이드" 을 참조하십시오.

Active IQ 플랫폼에서 보고된 업그레이드 이벤트도 보안 이벤트로 간주됩니다. 이러한 이벤트는 문제 해결을 위해 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어(보안 권장 사항)를 업그레이드해야 하는 문제를 식별합니다. 이러한 이벤트는 보안 패널에 표시되지 않지만 이벤트 관리 인벤토리 페이지에서 사용할 수 있습니다.

자세한 내용은 을 참조하십시오 "클러스터 보안 목표 관리".

클러스터 규정 준수 범주

이 표에는 Unified Manager가 평가하는 클러스터 보안 규정 준수 매개 변수, NetApp 권장 사항 및 매개 변수가 불만 제기인지 여부와 관련된 클러스터의 전반적인 결정에 영향을 미치는지 여부가 정리되어 있습니다.

클러스터에서 규정을 준수하지 않는 SVM이 존재할 경우 클러스터의 규정 준수 값에 영향을 미칩니다. 따라서 클러스터 보안이 규정 준수 상태로 인식되기 전에 SVM에서 보안 문제를 해결해야 하는 경우도 있습니다.

아래 나열된 모든 매개변수가 모든 설치에 나타나는 것은 아닙니다. 예를 들어 피어링된 클러스터가 없거나 클러스터에서 AutoSupport를 비활성화한 경우 UI 페이지에 클러스터 피어링 또는 AutoSupport HTTPS 전송 항목이 표시되지 않습니다.

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
글로벌 FIPS	글로벌 FIPS(Federal Information Processing Standard) 140-2 준수 모드가 활성화되어 있는지 여부를 나타냅니다. FIPS가 활성화되면 TLSv1 및 SSLv3이 비활성화되고 TLSv1.1 및 TLSv1.2만 허용됩니다.	활성화됨	예

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
텔넷	시스템에 대한 텔넷 액세스가 활성화되었는지 여부를 나타냅니다. 보안 원격 액세스를 위해 SSH(Secure Shell)를 사용하는 것이 좋습니다.	사용 안 함	예
안전하지 않은 SSH 설정	SSH가 * CBC로 시작하는 암호 등의 안전하지 않은 암호를 사용하는지 여부를 나타냅니다.	아니요	예
로그인 배너	시스템에 액세스하는 사용자가 로그인 배너를 사용할 수 있는지 여부를 나타냅니다.	활성화됨	예
클러스터 피어링	피어링된 클러스터 간의 통신이 암호화되었는지 또는 암호화되지 않았음을 나타냅니다. 이 매개 변수를 준수하는 것으로 간주하려면 소스 클러스터와 대상 클러스터 모두에서 암호화를 구성해야 합니다.	암호화	예
Network Time Protocol의 약어입니다	클러스터에 구성된 NTP 서버가 하나 이상 있는지 여부를 나타냅니다. 이중화 및 최적의 서비스를 위해 최소 3개의 NTP 서버를 클러스터에 연결하는 것이 좋습니다.	구성됨	예
OCSP	ONTAP에 OCSP(온라인 인증서 상태 프로토콜)로 구성되지 않은 응용 프로그램이 있는지 여부를 나타내므로 통신이 암호화되지 않습니다. 비준수 애플리케이션이 나열됩니다.	활성화됨	아니요
원격 감사 로깅	로그 전달(Syslog)이 암호화되었는지 또는 암호화되지 않았음을 나타냅니다.	암호화	예

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
AutoSupport HTTPS 전송	HTTPS가 NetApp 지원으로 AutoSupport 메시지를 보내기 위한 기본 전송 프로토콜로 사용되는지 여부를 나타냅니다.	활성화됨	예
기본 관리자 사용자입니다	기본 관리자 사용자(기본 제공)가 활성화 또는 비활성화되었는지 여부를 나타냅니다. 불필요한 내장 계정을 잠금(비활성화)하는 것이 좋습니다.	사용 안 함	예
SAML 사용자	SAML이 구성되었는지 여부를 나타냅니다. SAML을 사용하면 SSO(Single Sign-On)에 대한 로그인 방법으로 MFA(Multi-Factor Authentication)를 구성할 수 있습니다.	아니요	아니요
Active Directory 사용자	Active Directory가 구성되었는지 여부를 나타냅니다. Active Directory 및 LDAP는 클러스터에 액세스하는 사용자가 선호하는 인증 메커니즘입니다.	아니요	아니요
LDAP 사용자	LDAP가 구성되었는지 여부를 나타냅니다. Active Directory 및 LDAP는 로컬 사용자를 통해 클러스터를 관리하는 사용자에게 권장되는 인증 메커니즘입니다.	아니요	아니요
인증서 사용자	인증서 사용자가 클러스터에 로그인하도록 구성되었는지 여부를 나타냅니다.	아니요	아니요
로컬 사용자	로컬 사용자가 클러스터에 로그인하도록 구성되었는지 여부를 나타냅니다.	아니요	아니요

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
원격 셸	RSH가 활성화되었는지 여부를 나타냅니다. 보안상의 이유로 RSH를 비활성화해야 합니다. 보안 원격 액세스를 위한 SSH(Secure Shell)가 권장됩니다.	사용 안 함	예
MD5가 사용 중입니다	ONTAP 사용자 계정이 덜 안전한 MD5 해시 기능을 사용하고 있는지 여부를 나타냅니다. MD5 해시 사용자 계정을 SHA-512와 같은 보다 안전한 암호화 해시 기능으로 마이그레이션하는 것이 좋습니다.	아니요	예
인증서 발급자 유형	사용된 디지털 인증서의 유형을 나타냅니다.	CA 서명	아니요

스토리지 **VM** 규정 준수 범주

이 표에서는 Unified Manager에서 평가하는 SVM(Storage Virtual Machine) 보안 규정 준수 기준, NetApp 권장 사항 및 매개 변수가 불만 사항이 아닌 SVM의 전반적인 결정에 영향을 미치는지 여부를 설명합니다.

매개 변수	설명	권장 사항	**SVM** 규정 준수에 영향을 줍니다
감사 로그	감사 로깅이 설정되었는지 여부를 나타냅니다.	활성화됨	예
안전하지 않은 SSH 설정	SSH가 로 시작하는 암호 등의 안전하지 않은 암호를 사용하는지 여부를 나타냅니다 `cbc*`.	아니요	예
로그인 배너	시스템에서 SVM에 액세스하는 사용자에 대해 로그인 배너가 활성화되어 있는지 또는 비활성화되어 있는지 여부를 나타냅니다.	활성화됨	예

매개 변수	설명	권장 사항	**SVM** 규정 준수에 영향을 줍니다
LDAP 암호화	LDAP 암호화가 활성화 또는 비활성화되었는지 여부를 나타냅니다.	활성화됨	아니요
NTLM 인증	NTLM 인증이 활성화 또는 비활성화되었는지 여부를 나타냅니다.	활성화됨	아니요
LDAP 페이로드 서명	LDAP 페이로드 서명이 활성화 또는 비활성화되었는지 여부를 나타냅니다.	활성화됨	아니요
CHAP 설정	CHAP가 설정되었는지 여부를 나타냅니다.	활성화됨	아니요
Kerberos V5	Kerberos V5 인증이 활성화 또는 비활성화되었는지 여부를 나타냅니다.	활성화됨	아니요
NIS 인증	NIS 인증 사용이 구성되었는지 여부를 나타냅니다.	사용 안 함	아니요
FPolicy 상태가 활성 상태입니다	FPolicy가 생성되었는지 여부를 나타냅니다.	예	아니요
SMB 암호화가 활성화되었습니다	SMB 서명 및 봉인 기능이 활성화되어 있지 않음을 나타냅니다.	예	아니요
SMB 서명이 활성화되었습니다	SMB 서명이 설정되어 있지 않음을 나타냅니다.	예	아니요

볼륨 규정 준수 범주

이 표에서는 Unified Manager에서 볼륨 암호화 매개 변수를 평가하여, 볼륨의 데이터가 무단 사용자에 의해 액세스되지 않도록 적절히 보호되는지 여부를 확인합니다.

볼륨 암호화 매개 변수는 클러스터 또는 스토리지 VM의 규정 준수 여부에 영향을 주지 않습니다.

매개 변수	설명
소프트웨어가 암호화되었습니다	NVE(NetApp Volume Encryption) 또는 NAE(NetApp Aggregate Encryption) 소프트웨어 암호화 솔루션을 사용하여 보호되는 볼륨 수를 표시합니다.
하드웨어가 암호화되었습니다	NSE(NetApp Storage Encryption) 하드웨어 암호화를 사용하여 보호되는 볼륨 수를 표시합니다.
소프트웨어 및 하드웨어가 암호화되었습니다	소프트웨어 및 하드웨어 암호화로 보호되는 볼륨의 수를 표시합니다.
암호화되지 않았습니다	암호화되지 않은 볼륨의 수를 표시합니다.