클러스터 보안 목표 관리

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

목차

클러스터 보안 목표 관리

Unified Manager는 ONTAP 9_에 대한_NetApp 보안 강화 가이드에 정의된 권장사항을 기반으로 ONTAP 클러스터, SVM(스토리지 가상 시스템), 볼륨이 얼마나 안전한지 식별하는 대시보드를 제공합니다.

보안 대시보드의 목표는 ONTAP 클러스터가 NetApp 권장 지침에 맞지 않는 영역을 보여서 이러한 잠재적 문제를 해결할 수 있도록 하는 것입니다. 대부분의 경우 ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 문제를 해결할 수 있습니다. 조직에서 모든 권장 사항을 따르지 않을 수 있으므로 변경할 필요가 없는 경우도 있습니다.

를 참조하십시오 "ONTAP 9에 대한 NetApp 보안 강화 가이드" (TR-4569)을 참조하십시오.

Unified Manager는 보안 상태를 보고하는 것 외에도 보안 위반 사례가 있는 클러스터 또는 SVM을 위한 보안 이벤트도 생성합니다. 이벤트 관리 인벤토리 페이지에서 이러한 문제를 추적하고 이러한 이벤트에 대한 알림을 구성하여 새로운 보안 이벤트가 발생할 때 스토리지 관리자에게 알릴 수 있습니다.

자세한 내용은 을 참조하십시오 "평가 대상 보안 기준".

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
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

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
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
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

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
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
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
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

매개 변수	설명	권장 사항	**SVM** 규정 준수에 영향을 줍니다
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.

규정을 준수하지 않는 것은 무엇을 의미합니까

ONTAP 9_에 대한 NetApp 보안 강화 가이드에 정의된 권장사항을 기준으로 평가 중인 보안 기준이 충족되지 않을 경우 클러스터 및 SVM(스토리지 가상 시스템)이 적합하지 않은 것으로 간주됩니다. 또한 SVM이 규정을 준수하지 않는 것으로 플래그가 지정된 클러스터는 규정을 준수하지 않는 것으로 간주됩니다.

보안 카드의 상태 아이콘은 규정 준수와 관련하여 다음과 같은 의미를 가집니다.

- 매개 변수가 권장 구성으로 구성되어 있습니다.
- 매개 변수가 권장 구성으로 구성되지 않았습니다.
- - 클러스터에서 기능이 활성화되지 않았거나 매개 변수가 권장 구성으로 구성되지 않았습니다. 하지만 이 매개 변수는 개체의 규정 준수에 영향을 주지 않습니다.

볼륨 암호화 상태는 클러스터 또는 SVM이 규정을 준수하는지 여부를 나타내는 것이 아닙니다.

클러스터 및 스토리지 VM의 보안 상태 보기

Active IQ Unified Manager를 사용하면 환경의 스토리지 객체 보안 상태를 인터페이스의 여러 지점에서 확인할 수 있습니다. 정의된 매개 변수를 기반으로 정보 및 보고서를 수집 및 분석하고, 모니터링되는 클러스터와 스토리지 VM에서 의심스러운 동작 또는 승인되지 않은 시스템 변경을 감지할 수 있습니다.

보안 권장 사항은 을 참조하십시오 "ONTAP 9에 대한 NetApp 보안 강화 가이드"

보안 페이지에서 개체 수준 보안 상태를 봅니다

시스템 관리자는 * 보안 * 페이지를 사용하여 데이터 센터 및 사이트 수준에서 ONTAP 클러스터 및 스토리지 VM의 보안 강도에 대한 가시성을 확보할 수 있습니다. 지원되는 객체는 클러스터, 스토리지 VM 및 볼륨입니다. 다음 단계를 수행하십시오.

단계

1. 왼쪽 탐색 창에서 * 대시보드 * 를 클릭합니다.
2. 모니터링되는 모든 클러스터에 대한 보안 상태를 볼 것인지 또는 단일 클러스터에 대한 보안 상태를 볼 것인지 여부에 따라 * All Clusters * 를 선택하거나 드롭다운 메뉴에서 단일 클러스터를 선택합니다.
3. Security * 패널에서 오른쪽 화살표를 클릭합니다. 보안 페이지가 표시됩니다.

막대 차트, 개수 및 를 클릭합니다 `View Reports` 링크를 클릭하면 볼륨, 클러스터 또는 스토리지 VM 페이지로 이동하여 필요에 따라 해당 세부 정보를 보거나 보고서를 생성할 수 있습니다.

보안 페이지에는 다음 패널이 표시됩니다.

- * 클러스터 규정 준수 *: 데이터 센터에 있는 모든 클러스터의 보안 상태(규정을 준수하거나 준수하지 않는 클러스터 수)입니다
- * 스토리지 VM 규정 준수 *: 데이터 센터의 모든 스토리지 VM에 대한 보안 상태(규정을 준수하거나 준수하지 않는 스토리지 VM 수)입니다
- * 볼륨 암호화 *: 사용자 환경의 모든 볼륨에 대한 볼륨 암호화 상태(암호화되거나 암호화되지 않은 볼륨 수)입니다
- * Volume Anti-랜섬웨어 Status *: 사용자 환경의 모든 볼륨에서 보안 상태(랜섬웨어 방지 기능이 활성화된 볼륨 수 또는 비활성화된 볼륨 수)입니다
- * 클러스터 인증 및 인증서 *: SAML, Active Directory 등의 각 인증 방법을 사용하거나 인증서 및 로컬 인증을 통해 클러스터 수입니다. 또한 이 패널에는 인증서가 만료되었거나 60일 후에 만료되려고 하는 클러스터의 수가 표시됩니다.

클러스터 페이지에서 모든 클러스터의 보안 세부 정보를 봅니다

클러스터/보안 * 세부 정보 페이지에서는 클러스터 수준에서 보안 규정 준수 상태를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * Storage > Clusters * 를 클릭합니다.
2. 보기 > 보안 > 모든 클러스터 * 를 선택합니다.

글로벌 FIPS, Telnet, 비보안 SSH 설정, 로그인 배너, 네트워크 시간 프로토콜 등의 기본 보안 매개 변수 AutoSupport

HTTPS 전송 과 클러스터 인증서 만료 상태가 표시됩니다.

를 클릭할 수 있습니다 ⋮ 추가 옵션 단추를 클릭하고 Unified Manager의 * 보안 * 페이지 또는 System Manager에서 보안 세부 정보를 표시하도록 선택합니다. System Manager에서 자세한 정보를 볼 수 있는 유효한 자격 증명이 있어야 합니다.

> ⓘ 클러스터에 만료된 인증서가 있으면 을(를) 클릭할 수 있습니다 `expired` Cluster Certificate Validity * 에서 System Manager(9.10.1 이상)에서 갱신합니다. 을(를) 클릭할 수 없습니다 `expired` System Manager 인스턴스가 9.10.1 이전 버전인 경우

스토리지 **VM** 페이지에서 모든 클러스터의 보안 세부 정보를 봅니다

스토리지 VM/보안 * 세부 정보 페이지에서는 스토리지 VM 레벨의 보안 규정 준수 상태를 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 보기 > 보안 > 모든 스토리지 VM * 을 선택합니다. 보안 매개 변수가 있는 클러스터 목록이 표시됩니다.

스토리지 VM, 클러스터, 로그인 배너, 감사 로그, 보안되지 않은 SSH 설정 등의 보안 매개 변수를 확인하여 스토리지 VM의 보안 규정 준수를 기본적으로 볼 수 있습니다.

를 클릭할 수 있습니다 ⋮ 추가 옵션 단추를 클릭하고 Unified Manager의 * 보안 * 페이지 또는 System Manager에서 보안 세부 정보를 표시하도록 선택합니다. System Manager에서 자세한 정보를 볼 수 있는 유효한 자격 증명이 있어야 합니다.

볼륨 및 스토리지 VM에 대한 랜섬웨어 방지 보안에 대한 자세한 내용은 을 참조하십시오 "모든 볼륨 및 스토리지 VM의 랜섬웨어 방지 상태 보기".

소프트웨어 또는 펌웨어 업데이트가 필요할 수 있는 보안 이벤트 보기

"업그레이드"의 영향 영역이 있는 특정 보안 이벤트가 있습니다. 이러한 이벤트는 Active IQ 플랫폼에서 보고되며, 해결 방법을 통해 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어(보안 권장 사항)를 업그레이드해야 하는 문제를 식별합니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이러한 문제 중 일부에 대해 즉각적인 수정 조치를 수행해야 하는 경우도 있지만, 다른 문제로 인해 예정된 다음 유지 관리 작업이 완료될 때까지 기다릴 수 있습니다. 이러한 이벤트를 모두 보고 문제를 해결할 수 있는 사용자에게 할당할 수 있습니다. 또한 알림을 받지 않을 특정 보안 업그레이드 이벤트가 있는 경우 이 목록을 사용하면 해당 이벤트를 식별하여 비활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.

   기본적으로 모든 활성(신규 및 확인됨) 이벤트가 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 메뉴에서 * 업그레이드 이벤트 * 를 선택합니다.

이 페이지에는 모든 활성 업그레이드 보안 이벤트가 표시됩니다.

모든 클러스터에서 사용자 인증을 관리하는 방법 보기

보안 페이지에는 각 클러스터의 사용자를 인증하는 데 사용되는 인증 유형과 각 유형을 사용하여 클러스터에 액세스하는 사용자 수가 표시됩니다. 이렇게 하면 조직에서 정의한 대로 사용자 인증이 안전하게 수행되고 있는지 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 대시보드 * 를 클릭합니다.
2. 대시보드 상단의 드롭다운 메뉴에서 * All Clusters * 를 선택합니다.
3. 보안* 패널에서 오른쪽 화살표를 클릭하면 * 보안 * 페이지가 표시됩니다.
4. 각 인증 유형을 사용하여 시스템에 액세스하는 사용자 수를 보려면 * 클러스터 인증 * 카드를 확인하십시오.
5. 각 클러스터의 사용자를 인증하는 데 사용되는 인증 메커니즘을 보려면 * 클러스터 보안 * 카드를 확인하십시오.

시스템에 액세스하는 일부 사용자가 안전하지 않은 방법을 사용하거나 NetApp에서 권장하지 않는 방법을 사용하는 경우, 이 방법을 사용하지 않도록 설정할 수 있습니다.

모든 볼륨의 암호화 상태 보기

모든 볼륨의 목록과 현재 암호화 상태를 볼 수 있으므로 볼륨의 데이터가 무단 사용자가 액세스하지 못하도록 적절하게 보호되는지 여부를 확인할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨에 적용할 수 있는 암호화 유형은 다음과 같습니다.

- 소프트웨어 - NVE(NetApp Volume Encryption) 또는 NetApp NAE(Aggregate Encryption) 소프트웨어 암호화 솔루션을 사용하여 보호되는 볼륨
- Hardware - NSE(NetApp Storage Encryption) 하드웨어 암호화를 사용하여 보호되는 볼륨입니다.
- 소프트웨어 및 하드웨어 - 소프트웨어 및 하드웨어 암호화로 보호되는 볼륨입니다.
- 없음 - 암호화되지 않은 볼륨입니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 상태 * > * 볼륨 암호화 * 를 선택합니다
3. 상태: 볼륨 암호화 * 보기에서 * 암호화 유형 * 필드를 기준으로 정렬하거나 필터를 사용하여 특정 암호화 유형이 있거나 암호화되지 않은 볼륨(암호화 유형 ""없음")을 표시합니다.

모든 볼륨 및 스토리지 VM의 랜섬웨어 방지 상태 보기

모든 볼륨 및 스토리지 VM(SVM)의 목록과 현재 안티 랜섬웨어 상태를 볼 수 있으므로 볼륨 및 SVM의 데이터가 랜섬웨어 공격으로부터 적절히 보호되는지 확인할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다양한 안티 랜섬웨어 상태에 대한 자세한 내용은 를 참조하십시오 "ONTAP: 랜섬웨어 방지 지원".

랜섬웨어 방지 감지를 사용하여 모든 볼륨의 보안 세부 정보를 봅니다

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 상태 * > * 보안 * > * 랜섬웨어 방지 * 를 선택합니다
3. Security: Anti-랜섬웨어 * 보기에서 다양한 필드를 기준으로 정렬하거나 필터를 사용할 수 있습니다.

오프라인 볼륨, 제한된 볼륨, SnapLock 볼륨, FlexGroup 볼륨, FlexCache 볼륨 및 SAN 전용 볼륨, 중지된 스토리지 VM의 볼륨, 스토리지 VM의 루트 볼륨 또는 데이터 보호 볼륨.

랜섬웨어 방지 감지를 사용하여 모든 스토리지 VM의 보안 세부 정보를 봅니다

단계

1. 왼쪽 탐색 창에서 * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 보기 > 보안 > 랜섬웨어 방지 * 를 선택합니다. 랜섬웨어 방지 상태가 표시된 SVM 목록이 표시됩니다.

랜섬웨어 방지 모니터링은 NAS 프로토콜이 활성화되지 않은 스토리지 VM에서 지원되지 않습니다.

모든 활성 보안 이벤트 보기

모든 활성 보안 이벤트를 확인한 다음 문제를 해결할 수 있는 사용자에게 각 이벤트를 할당할 수 있습니다. 또한 수신하지 않을 특정 보안 이벤트가 있는 경우 이 목록을 사용하여 비활성화할 이벤트를 확인할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.

   기본적으로 새 이벤트와 확인된 이벤트는 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 메뉴에서 * 활성 보안 이벤트 * 를 선택합니다.

이 페이지에는 지난 7일 동안 생성된 모든 새 보안 이벤트 및 확인된 보안 이벤트가 표시됩니다.

보안 이벤트에 대한 알림 추가

Unified Manager에서 수신한 다른 이벤트처럼 개별 보안 이벤트에 대한 알림을 구성할 수 있습니다. 또한 모든 보안 이벤트를 동일하게 처리하고 동일한 사용자에게 전자 메일을 보내려는 경우 보안 이벤트가 트리거되면 단일 알림을 생성하여 사용자에게 알릴 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 예제에서는 ""Telnet 프로토콜 사용"" 보안 이벤트에 대한 경고를 생성하는 방법을 보여 줍니다. 클러스터에 대한 원격 관리 액세스를 위해 텔넷 액세스가 구성된 경우 경고가 전송됩니다. 이와 동일한 방법을 사용하여 모든 보안 이벤트에 대한 알림을 만들 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. Alert Setup * 페이지에서 * Add * 를 클릭합니다.
3. 경고 추가 * 대화 상자에서 * 이름 * 을 클릭하고 경고의 이름과 설명을 입력합니다.
4. Resources * 를 클릭하고 이 경고를 활성화할 클러스터 또는 클러스터를 선택합니다.
5. 이벤트 * 를 클릭하고 다음 작업을 수행합니다.
   a. 이벤트 심각도 목록에서 * 경고 * 를 선택합니다.
   b. 일치하는 이벤트 목록에서 * 텔넷 프로토콜 사용 * 을 선택합니다.
6. Actions * 를 클릭한 다음 * Alert these users * 필드에서 경고 이메일을 수신할 사용자의 이름을 선택합니다.
7. 알림 빈도, SNMP 탭 실행 및 스크립트 실행을 위해 이 페이지의 다른 옵션을 구성합니다.
8. 저장 * 을 클릭합니다.

특정 보안 이벤트 비활성화

모든 이벤트는 기본적으로 활성화됩니다. 특정 이벤트를 비활성화하여 사용자 환경에서 중요하지 않은 이벤트에 대한 알림이 발생하지 않도록 할 수 있습니다. 알림 수신을 다시 시작하려면 사용하지 않는 이벤트를 설정할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트를 사용하지 않도록 설정하면 시스템에서 이전에 생성된 이벤트가 사용되지 않는 것으로 표시되고 이러한 이벤트에 대해 구성된 알림이 트리거되지 않습니다. 비활성화된 이벤트를 활성화하면 다음 모니터링 주기부터 이러한 이벤트에 대한 알림이 생성됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 이벤트 설정 * 을 클릭합니다.

2. 이벤트 * 설정 페이지에서 다음 옵션 중 하나를 선택하여 이벤트를 비활성화하거나 활성화합니다.

원하는 작업	다음을 수행하십시오.
이벤트를 비활성화합니다	a. 비활성화 * 를 클릭합니다. b. 이벤트 비활성화 대화 상자에서 * 경고 * 심각도를 선택합니다. 모든 보안 이벤트의 범주입니다. c. 일치하는 이벤트 열에서 비활성화할 보안 이벤트를 선택한 다음 오른쪽 화살표를 클릭하여 해당 이벤트를 이벤트 사용 안 함 열로 이동합니다. d. 저장 후 닫기 * 를 클릭합니다. e. 사용하지 않도록 설정한 이벤트가 이벤트 설정 페이지의 목록 보기에 표시되는지 확인합니다.
이벤트 활성화	a. 비활성화된 이벤트 목록에서 다시 사용할 이벤트 또는 이벤트의 확인란을 선택합니다. b. 사용 * 을 클릭합니다.

보안 이벤트

보안 이벤트는 ONTAP 9_에 대한_NetApp 보안 강화 가이드에 정의된 매개 변수를 기반으로 ONTAP 클러스터, SVM(스토리지 가상 머신) 및 볼륨의 보안 상태에 대한 정보를 제공합니다. 이러한 이벤트는 잠재적 문제를 사용자에게 알려주기 때문에 심각도를 평가하고 필요한 경우 문제를 해결할 수 있습니다.

보안 이벤트는 소스 유형별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준 및 심각도를 포함합니다. 이러한 이벤트는 클러스터 및 스토리지 VM 이벤트 범주에 표시됩니다.