클러스터 보안 목표 관리

Active IQ Unified Manager

NetApp
May 15, 2026

목차

클러스터 보안 목표 관리

Unified Manager는 _NetApp 보안 강화 가이드 for ONTAP 9_에 정의된 권장 사항을 기반으로 ONTAP 클러스터, 스토리지 가상 머신(SVM) 및 볼륨의 보안 수준을 파악하는 대시보드를 제공합니다.

보안 대시보드의 목적은 ONTAP 클러스터가 NetApp 권장 가이드라인과 일치하지 않는 영역을 표시하여 이러한 잠재적 문제를 해결할 수 있도록 하는 것입니다. 대부분의 경우 ONTAP 시스템 관리자나 ONTAP CLI를 사용하여 문제를 해결할 수 있습니다. 귀하의 조직이 모든 권장 사항을 따르지 않을 수 있으므로, 어떤 경우에는 아무런 변경도 할 필요가 없을 수도 있습니다.

를 참조하십시오 "ONTAP 9를 위한 NetApp 보안 강화 가이드" (TR-4569) 자세한 권장 사항과 해결책을 확인하세요.

Unified Manager는 보안 상태를 보고하는 것 외에도 보안 위반이 있는 모든 클러스터 또는 SVM에 대한 보안 이벤트를 생성합니다. 이벤트 관리 인벤토리 페이지에서 이러한 문제를 추적할 수 있으며, 이러한 이벤트에 대한 알림을 구성하여 새로운 보안 이벤트가 발생할 때 스토리지 관리자에게 알림을 보낼 수 있습니다.

자세한 내용은 다음을 참조하세요. "어떤 보안 기준이 평가되고 있습니까?".

어떤 보안 기준이 평가되고 있습니까?

일반적으로 ONTAP 클러스터, 스토리지 가상 머신(SVM) 및 볼륨에 대한 보안 기준은 _NetApp 보안 강화 가이드 for ONTAP 9_에 정의된 권장 사항을 기준으로 평가됩니다.

보안 검사에는 다음이 포함됩니다.

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

규정 준수 범주 및 다음 항목 참조 "ONTAP 9를 위한 NetApp 보안 강화 가이드" 자세한 내용은.

> Active IQ 플랫폼에서 보고된 업그레이드 이벤트도 보안 이벤트로 간주됩니다. 이러한 이벤트는 보안 권고에 따라 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어를 업그레이드해야 하는 문제를 식별합니다. 이러한 이벤트는 보안 패널에 표시되지 않지만 이벤트 관리 인벤토리 페이지에서 사용할 수 있습니다.

자세한 내용은 다음을 참조하세요. "클러스터 보안 목표 관리".

클러스터 규정 준수 범주

이 표에서는 Unified Manager가 평가하는 클러스터 보안 규정 준수 매개변수, NetApp 권장 사항, 그리고 매개변수가 클러스터의 전반적인 규정 준수 여부 결정에 영향을 미치는지 여부를 설명합니다.

클러스터에 규정을 준수하지 않는 SVM이 있으면 클러스터의 규정 준수 값에 영향을 미칩니다. 따라서 어떤 경우에는

클러스터 보안이 규정을 준수하는 것으로 간주되기 전에 SVM의 보안 문제를 해결해야 할 수도 있습니다.

아래 나열된 모든 매개변수가 모든 설치에 적용되는 것은 아닙니다. 예를 들어, 피어링된 클러스터가 없거나 클러스터에서 AutoSupport 비활성화한 경우 UI 페이지에 클러스터 피어링이나 AutoSupport HTTPS 전송 항목이 표시되지 않습니다.

매개변수	설명	추천	클러스터 규정 준수에 영향을 미칩니다
글로벌 FIPS	글로벌 FIPS(연방 정보 처리 표준) 140-2 준수 모드가 활성화되어 있는지 비활성화되어 있는지 여부를 나타냅니다. FIPS가 활성화되면 TLSv1과 SSLv3는 비활성화되고 TLSv1.1과 TLSv1.2만 허용됩니다.	활성화됨	예
텔넷	시스템에 대한 Telnet 액세스가 활성화되어 있는지 비활성화되어 있는지를 나타냅니다. NetApp 안전한 원격 액세스를 위해 Secure Shell(SSH)을 권장합니다.	장애가 있는	예
안전하지 않은 SSH 설정	SSH가 안전하지 않은 암호(예: *cbc로 시작하는 암호)를 사용하는지 여부를 나타냅니다.	아니요	예
로그인 배너	시스템에 액세스하는 사용자에게 로그인 배너가 활성화되어 있는지 비활성화되어 있는지 여부를 나타냅니다.	활성화됨	예
클러스터 피어링	피어링된 클러스터 간 통신이 암호화되었는지 암호화되지 않았는지 여부를 나타냅니다. 이 매개변수가 규정을 준수하는 것으로 간주되려면 소스 클러스터와 대상 클러스터 모두에서 암호화를 구성해야 합니다.	암호화됨	예

매개변수	설명	추천	클러스터 규정 준수에 영향을 미칩니다
네트워크 시간 프로토콜	클러스터에 하나 이상의 구성된 NTP 서버가 있는지 여부를 나타냅니다. 중복성과 최상의 서비스를 위해 NetApp 클러스터에 최소 3개의 NTP 서버를 연결할 것을 권장합니다.	구성됨	예
OCSP	9.14.1부터 Active IQ Unified Manager 스토리지 가상 머신(SVM, 이전에는 Vserver라고 함) 수준에서 OCSP(온라인 인증서 상태 프로토콜) 상태 정보를 제공합니다. 즉, OCSP 검증은 SVM에 대한 모든 SSL/TLS 연결에 적용되며 이러한 연결에 사용된 인증서의 무결성과 유효성을 보장합니다.	활성화됨	아니요
원격 감사 로깅	로그 전달(Syslog)이 암호화되었는지 여부를 나타냅니다.	암호화됨	예
AutoSupport HTTPS 전송	NetApp 지원팀에 AutoSupport 메시지를 보낼 때 HTTPS가 기본 전송 프로토콜로 사용되는지 여부를 나타냅니다.	활성화됨	예
기본 관리자 사용자	기본 관리자 사용자(기본 제공)가 활성화되어 있는지 비활성화되어 있는지를 나타냅니다. NetApp 불필요한 기본 제공 계정을 잠그거나 비활성화할 것을 권장합니다.	장애가 있는	예
SAML 사용자	SAML이 구성되었는지 여부를 나타냅니다. SAML을 사용하면 Single Sign-On에 대한 로그인 방법으로 다중 인증 요소(MFA)를 구성할 수 있습니다.	아니요	아니요

매개변수	설명	추천	클러스터 규정 준수에 영향을 미칩니다
Active Directory 사용자	Active Directory가 구성되었는지 여부를 나타냅니다. Active Directory와 LDAP는 클러스터에 액세스하는 사용자에게 선호되는 인증 메커니즘입니다.	아니요	아니요
LDAP 사용자	LDAP가 구성되었는지 여부를 나타냅니다. Active Directory와 LDAP는 로컬 사용자보다 클러스터를 관리하는 사용자에게 선호되는 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 활성화되어 있는지 여부를 나타냅니다. 보안상의 이유로 RSH를 비활성화해야 합니다. 안전한 원격 액세스를 위해서는 Secure Shell(SSH)을 사용하는 것이 좋습니다.	장애가 있는	예
MD5 사용 중	ONTAP 사용자 계정에서 보안 수준이 낮은 MD5 해시 함수를 사용하는지 여부를 나타냅니다. MD5 해시된 사용자 계정은 SHA-512와 같은 보다 안전한 암호화 해시 함수로 마이그레이션하는 것이 좋습니다.	아니요	예
인증서 발급자 유형	사용된 디지털 인증서의 유형을 나타냅니다.	CA 서명	아니요

스토리지 **VM** 규정 준수 범주

이 표에서는 Unified Manager가 평가하는 스토리지 가상 머신(SVM) 보안 준수 기준, NetApp 권장 사항, 그리고 매개변수가 SVM이 전반적으로 적합 판정에 영향을 미치는지 여부를 설명합니다.

매개변수	설명	추천	**SVM** 규정 준수에 영향을 미칩니다
감사 로그	감사 로깅이 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	예
안전하지 않은 SSH 설정	SSH가 안전하지 않은 암호(예: 로 시작하는 암호)를 사용하는지 여부를 나타냅니다. `cbc*` .	아니요	예
로그인 배너	시스템의 SVM에 액세스하는 사용자에 대해 로그인 배너가 활성화되어 있는지 비활성화되어 있는지 여부를 나타냅니다.	활성화됨	예
LDAP 암호화	LDAP 암호화가 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요
NTLM 인증	NTLM 인증이 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요
LDAP 페이로드 서명	LDAP 페이로드 서명이 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요
CHAP 설정	CHAP가 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요
케르베로스 V5	Kerberos V5 인증이 활성화되어 있는지 비활성화되어 있는지를 나타냅니다.	활성화됨	아니요

매개변수	설명	추천	**SVM** 규정 준수에 영향을 미칩니다
NIS 인증	NIS 인증 사용이 구성되었는지 여부를 나타냅니다.	장애가 있는	아니요
FPolicy 상태 활성화	FPolicy가 생성되었는지 여부를 나타냅니다.	예	아니요
SMB 암호화 활성화됨	SMB 서명 및 봉인이 활성화되어 있지 않은지 여부를 나타냅니다.	예	아니요
SMB 서명 활성화됨	SMB 서명이 활성화되어 있지 않은지 여부를 나타냅니다.	예	아니요

볼륨 준수 범주

이 표에서는 Unified Manager가 볼륨의 데이터가 무단 사용자의 액세스로부터 적절하게 보호되는지 여부를 판단하기 위해 평가하는 볼륨 암호화 매개변수를 설명합니다.

볼륨 암호화 매개변수는 클러스터 또는 스토리지 VM이 규정을 준수하는 것으로 간주되는지 여부에 영향을 미치지 않습니다.

매개변수	설명
소프트웨어 암호화	NetApp Volume Encryption(NVE) 또는 NetApp Aggregate Encryption(NAE) 소프트웨어 암호화 솔루션을 사용하여 보호되는 볼륨 수를 표시합니다.
하드웨어 암호화	NetApp Storage Encryption(NSE) 하드웨어 암호화를 사용하여 보호되는 볼륨 수를 표시합니다.
소프트웨어 및 하드웨어 암호화	소프트웨어 및 하드웨어 암호화로 보호되는 볼륨 수를 표시합니다.
암호화되지 않음	암호화되지 않은 볼륨의 수를 표시합니다.

규정을 준수하지 않는다는 것은 무엇을 의미합니까?

클러스터와 스토리지 가상 머신(SVM)은 _NetApp 보안 강화 가이드 for ONTAP 9_에 정의된 권장 사항에 대해 평가되는 보안 기준 중 하나라도 충족하지 못할 경우 규정을 준수하지 않는 것으로 간주됩니다. 또한, SVM 중 하나가 규정을 준수하지 않는 것으로 표시되면 클러스터는 규정을 준수하지 않는 것으로 간주됩니다.

보안 카드의 상태 아이콘은 규정 준수 여부에 따라 다음과 같은 의미를 갖습니다.

- - 매개변수는 권장사항에 따라 구성되었습니다.
- - 매개변수가 권장되는 대로 구성되지 않았습니다.
- - 클러스터에서 해당 기능이 활성화되지 않았거나 매개변수가 권장 사항대로 구성되지 않았지만, 이 매개변수는 개체의 규정 준수에 기여하지 않습니다.

볼륨 암호화 상태는 클러스터나 SVM이 규정을 준수하는 것으로 간주되는지 여부에 영향을 미치지 않습니다.

클러스터 및 스토리지 VM의 보안 상태 보기

Active IQ Unified Manager 사용하면 인터페이스의 다양한 지점에서 환경 내 스토리지 개체의 보안 상태를 볼 수 있습니다. 정의된 매개변수를 기반으로 정보와 보고서를 수집하고 분석하고, 모니터링되는 클러스터와 스토리지 VM에서 의심스러운 동작이나 승인되지 않은 시스템 변경을 감지할 수 있습니다.

보안 권장 사항은 다음을 참조하세요. "ONTAP 9를 위한 NetApp 보안 강화 가이드"

보안 페이지에서 개체 수준 보안 상태 보기

시스템 관리자는 보안 페이지를 사용하여 데이터 센터 및 사이트 수준에서 ONTAP 클러스터와 스토리지 VM의 보안 강도를 파악할 수 있습니다. 지원되는 개체는 클러스터, 스토리지 VM, 볼륨입니다. 다음 단계를 따르세요.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭합니다.
2. 모니터링되는 모든 클러스터의 보안 상태를 볼지 또는 단일 클러스터의 보안 상태를 볼지에 따라 *모든 클러스터*를 선택하거나 드롭다운 메뉴에서 단일 클러스터를 선택합니다.
3. 보안 패널에서 오른쪽 화살표를 클릭합니다. 보안 페이지가 표시됩니다.

막대형 차트, 개수 등을 클릭하면 `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 센터의 모든 클러스터의 보안 상태(규정을 준수하거나 준수하지 않는 클러스터 수)
- 저장소 **VM** 규정 준수: 데이터 센터의 모든 저장 VM에 대한 보안 상태(규정을 준수하거나 준수하지 않는 저장 VM 수)
- 볼륨 암호화: 사용자 환경의 모든 볼륨의 볼륨 암호화 상태(암호화되었거나 암호화되지 않은 볼륨 수)
- 볼륨 랜섬웨어 방지 상태: 사용자 환경의 모든 볼륨의 보안 상태(랜섬웨어 방지가 활성화 또는 비활성화된 볼륨 수)
- 클러스터 인증 및 인증서: SAML, Active Directory 또는 인증서 및 로컬 인증과 같은 각 유형의 인증 방법을 사용하는 클러스터 수입니다. 패널에는 인증서가 만료되었거나 60일 후에 만료될 예정인 클러스터 수도 표시됩니다.

클러스터 페이지에서 모든 클러스터의 보안 세부 정보를 확인하세요.

클러스터/보안 세부 정보 페이지에서는 클러스터 수준의 보안 준수 상태를 볼 수 있습니다.

단계

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

글로벌 FIPS, Telnet, 안전하지 않은 SSH 설정, 로그인 배너, 네트워크 시간 프로토콜, AutoSupport HTTPS 전송, 클러스터 인증서 만료 상태와 같은 기본 보안 매개변수가 표시됩니다.

클릭할 수 있습니다 추가 옵션 버튼을 클릭하고 Unified Manager의 보안 페이지 또는 System Manager에서 보안 세부 정보를 볼 수 있습니다. 시스템 관리자에서 세부 정보를 보려면 유효한 자격 증명이 있어야 합니다.

클러스터에 만료된 인증서가 있는 경우 다음을 클릭할 수 있습니다. `expired` *클러스터 인증서 유효성 *에서 System Manager(9.10.1 이상)에서 갱신하세요. 클릭할 수 없습니다 `expired` 시스템 관리자 인스턴스가 9.10.1 이전 릴리스인 경우.

스토리지 **VM** 페이지에서 모든 클러스터의 보안 세부 정보를 확인하세요**.**

저장소 **VM/**보안 세부 정보 페이지에서는 저장소 VM 수준의 보안 준수 상태를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *저장소 > 저장소 VM*을 클릭합니다.
2. *보기 > 보안 > 모든 저장소 VM*을 선택합니다. 보안 매개변수가 포함된 클러스터 목록이 표시됩니다.

스토리지 VM, 클러스터, 로그인 배너, 감사 로그, 안전하지 않은 SSH 설정 등의 보안 매개변수를 확인하여 스토리지 VM의 보안 준수 여부에 대한 기본 보기를 가질 수 있습니다.

클릭할 수 있습니다 추가 옵션 버튼을 클릭하고 Unified Manager의 보안 페이지 또는 System Manager에서 보안 세부 정보를 볼 수 있습니다. 시스템 관리자에서 세부 정보를 보려면 유효한 자격 증명이 있어야 합니다.

볼륨 및 스토리지 VM에 대한 랜섬웨어 방지 보안 세부 정보는 다음을 참조하세요."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, 보안 권고에 따라 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어를 업그레이드해야 하는 문제를 식별합니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

일부 문제는 즉시 시정 조치를 취해야 할 수도 있지만, 다른 문제는 다음에 예정된 유지 관리까지 기다릴 수 있습니다. 이러한 모든 이벤트를 보고 문제를 해결할 수 있는 사용자에게 할당할 수 있습니다. 또한, 알림을 받고 싶지 않은 특정 보안 업그레이드 이벤트가 있는 경우 이 목록을 통해 해당 이벤트를 식별하여 비활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.

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

2. 보기 메뉴에서 *이벤트 업그레이드*를 선택합니다.

   이 페이지에는 모든 활성 업그레이드 보안 이벤트가 표시됩니다.

모든 클러스터에서 사용자 인증이 어떻게 관리되는지 확인하세요.

보안 페이지에는 각 클러스터에서 사용자를 인증하는 데 사용되는 인증 유형과 각 유형을 사용하여 클러스터에 액세스하는 사용자 수가 표시됩니다. 이를 통해 조직에서 정의한 대로 사용자 인증이 안전하게 수행되는지 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭합니다.
2. 대시보드 상단의 드롭다운 메뉴에서 *모든 클러스터*를 선택합니다.
3. 보안 패널에서 오른쪽 화살표를 클릭하면 보안 페이지가 표시됩니다.
4. 클러스터 인증 카드를 보면 각 인증 유형을 사용하여 시스템에 액세스하는 사용자 수를 확인할 수 있습니다.
5. 클러스터 보안 카드를 보고 각 클러스터에서 사용자를 인증하는 데 사용되는 인증 메커니즘을 확인하세요.

일부 사용자가 안전하지 않은 방법을 사용하거나 NetApp 에서 권장하지 않는 방법을 사용하여 시스템에 액세스하는 경우 해당 방법을 비활성화할 수 있습니다.

모든 볼륨의 암호화 상태 보기

모든 볼륨과 현재 암호화 상태 목록을 보고 볼륨의 데이터가 무단 사용자의 접근으로부터 적절하게 보호되고 있는지 확인할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨에 적용할 수 있는 암호화 유형은 다음과 같습니다.

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

단계

1. 왼쪽 탐색 창에서 저장소 > *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 유형을 갖는 볼륨이나 암호화되지 않은 볼륨(암호화 유형이 "없음"인 볼륨)을 표시합니다.

모든 볼륨 및 스토리지 VM의 랜섬웨어 방지 상태 보기

모든 볼륨과 스토리지 VM(SVM) 목록과 현재 랜섬웨어 방지 상태를 확인하여 볼륨과 SVM의 데이터가 랜섬웨어 공격으로부터 적절하게 보호되고 있는지 확인할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다양한 랜섬웨어 방지 상태에 대한 자세한 내용은 다음을 참조하세요."ONTAP: 랜섬웨어 방지 기능 활성화" .

랜섬웨어 탐지 기능으로 모든 볼륨의 보안 세부 정보 보기

단계

1. 왼쪽 탐색 창에서 저장소 > *볼륨*을 클릭합니다.
2. 보기 메뉴에서 상태 > 보안 > *랜섬웨어 방지*를 선택하세요.
3. 보안: 랜섬웨어 방지 보기에서는 다양한 필드별로 정렬하거나 필터를 사용할 수 있습니다.

> 랜섬웨어 방지 기능은 오프라인 볼륨, 제한된 볼륨, SnapLock 볼륨, FlexGroup 볼륨, FlexCache 볼륨, SAN 전용 볼륨, 중지된 스토리지 VM의 볼륨, 스토리지 VM의 루트 볼륨 또는 데이터 보호 볼륨에 지원되지 않습니다.

랜섬웨어 감지 기능을 통해 모든 스토리지 VM의 보안 세부 정보를 확인하세요.

단계

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

> NAS 프로토콜이 활성화되지 않은 스토리지 VM에서는 랜섬웨어 방지 모니터링이 지원되지 않습니다.

모든 활성 보안 이벤트 보기

모든 활성 보안 이벤트를 보고 각 이벤트를 문제를 해결할 수 있는 사용자에게 할당할 수 있습니다. 또한, 수신하고 싶지 않은 특정 보안 이벤트가 있는 경우 이 목록을 통해 비활성화하려는 이벤트를 식별할 수 있습니다.

시작하기 전에

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 이벤트와 확인된 보안 이벤트가 표시됩니다.

보안 이벤트에 대한 알림 추가

Unified Manager에서 수신한 다른 이벤트와 마찬가지로 개별 보안 이벤트에 대한 알림을 구성할 수 있습니다. 또한, 모든 보안 이벤트를 동일하게 처리하고 같은 사람에게 이메일을 보내려는 경우 보안 이벤트가 발생할 때마다 알려주는 단일 알림을 만들 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 예에서는 "Telnet Protocol Enabled" 보안 이벤트에 대한 알림을 만드는 방법을 보여줍니다. 클러스터에 대한 원격 관리 액세스를 위해 Telnet 액세스가 구성된 경우 경고가 전송됩니다. 동일한 방법을 사용하여 모든 보안 이벤트에 대한 알림을 생성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *알림 설정*을 클릭합니다.
2. 알림 설정 페이지에서 *추가*를 클릭합니다.
3. 알림 추가 대화 상자에서 *이름*을 클릭하고 알림의 이름과 설명을 입력합니다.
4. *리소스*를 클릭하고 이 알림을 활성화하려는 클러스터 또는 클러스터를 선택합니다.
5. *이벤트*를 클릭하고 다음 작업을 수행하세요.
   a. 이벤트 심각도 목록에서 *경고*를 선택합니다.
   b. 일치하는 이벤트 목록에서 *Telnet 프로토콜 사용*을 선택합니다.
6. 작업*을 클릭한 다음 *다음 사용자에게 알림 필드에서 알림 이메일을 받을 사용자의 이름을 선택합니다.
7. 이 페이지에서 알림 빈도, SNMP 탭 발행, 스크립트 실행에 대한 다른 옵션을 구성합니다.
8. *저장*을 클릭하세요.

특정 보안 이벤트 비활성화

모든 이벤트는 기본적으로 활성화되어 있습니다. 사용자 환경에서 중요하지 않은 이벤트에 대한 알림이 생성되지 않도록 하려면 특정 이벤트를 비활성화할 수 있습니다. 비활성화된 이벤트에 대한 알림을 다시 받으려면 해당 이벤트를 활성화하면 됩니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트를 비활성화하면 시스템에서 이전에 생성된 이벤트는 더 이상 사용되지 않는 것으로 표시되고, 이러한 이벤트에 대해 구성된 알림은 트리거되지 않습니다. 비활성화된 이벤트를 활성화하면 다음 모니터링 주기부터 해당 이벤트에 대한 알림이 생성됩니다.

단계

1. 왼쪽 탐색 창에서 저장소 관리 > *이벤트 설정*을 클릭합니다.
2. 이벤트 설정 페이지에서 다음 옵션 중 하나를 선택하여 이벤트를 비활성화하거나 활성화합니다.

만약 당신이 원한다면...	그러면 이렇게 하세요...
이벤트 비활성화	a. *비활성화*를 클릭합니다. b. 이벤트 비활성화 대화 상자에서 경고 심각도를 선택합니다. 이는 모든 보안 이벤트에 대한 카테고리입니다. c. 일치하는 이벤트 열에서 비활성화하려는 보안 이벤트를 선택한 다음 오른쪽 화살표를 클릭하여 해당 이벤트를 비활성화 이벤트 열로 이동합니다. d. *저장 및 닫기*를 클릭하세요. e. 비활성화한 이벤트가 이벤트 설정 페이지의 목록 보기에 표시되는지 확인하세요.
이벤트 활성화	a. 비활성화된 이벤트 목록에서 다시 활성화하려는 이벤트의 확인란을 선택합니다. b. *활성화*를 클릭합니다.

보안 이벤트

보안 이벤트는 _NetApp 보안 강화 가이드 for ONTAP 9_에 정의된 매개변수를 기반으로 ONTAP 클러스터, 스토리지 가상 머신(SVM) 및 볼륨의 보안 상태에 대한 정보를 제공합니다. 이러한 이벤트는 잠재적인 문제를 알려주므로 문제의 심각성을 평가하고 필요한 경우 문제를 해결할 수 있습니다.

보안 이벤트는 소스 유형별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 심각도가 포함됩니다. 이러한 이벤트는 클러스터 및 스토리지 VM 이벤트 범주에 나타납니다.