클러스터 보안 목표 관리

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/active-iq-unified-manager-918/health-checker/concept_manage_cluster_security_objectives.html on November 13, 2026. Always check docs.netapp.com for the latest.

목차

클러스터 보안 목표 관리 . . . 1
Active IQ Unified Manager에서 클러스터 보안 목표 관리 . . . 1
어떤 보안 기준이 평가되고 있습니까 . . . 1
Active IQ Unified Manager 보안 기준을 평가하는 방법을 이해하십시오. . . . 1
Active IQ Unified Manager의 클러스터 규정 준수 범주 이해 . . . 1
Active IQ Unified Manager에서 스토리지 VM 규정 준수 범주 이해 . . . 4
Active IQ Unified Manager에서 볼륨 규정 준수 범주 이해 . . . 5
Active IQ Unified Manager에서 클러스터 및 SVM 규정 준수 상태에 대해 알아보기 . . . 6
Active IQ Unified Manager에서 클러스터 및 스토리지 VM의 보안 상태를 봅니다 . . . 6
보안 페이지에서 오브젝트 수준 보안 상태 보기 . . . 6
클러스터 페이지에서 모든 클러스터의 보안 세부 정보 보기 . . . 7
스토리지 VM 페이지에서 모든 클러스터의 보안 세부 정보를 볼 수 있습니다. . . . 7
Active IQ Unified Manager에서 소프트웨어 또는 펌웨어 업데이트가 필요할 수 있는 보안 이벤트 보기 . . . 8
Active IQ Unified Manager의 모든 클러스터에서 클러스터가 사용자 인증을 관리하는 방법을 확인합니다 . . . 8
Active IQ Unified Manager에서 모든 볼륨의 암호화 상태 보기 . . . 9
Active IQ Unified Manager에서 모든 볼륨 및 스토리지 VM의 랜섬웨어 방지 상태를 봅니다 . . . 9
랜섬웨어 탐지 기능이 있는 모든 볼륨의 보안 세부 정보 보기 . . . 9
랜섬웨어 탐지 기능이 있는 모든 스토리지 VM의 보안 세부 정보 보기 . . . 10
Active IQ Unified Manager에서 모든 활성 보안 이벤트 보기 . . . 10
Active IQ Unified Manager의 보안 이벤트에 대한 알림 추가 . . . 10
Active IQ Unified Manager에서 특정 보안 이벤트 비활성화 . . . 11
Active IQ Unified Manager에서 보안 이벤트 보기 . . . 12

클러스터 보안 목표 관리

Active IQ Unified Manager에서 클러스터 보안 목표 관리

Unified Manager는 _NetApp ONTAP 9용 보안 강화 가이드_에 정의된 권장 사항을 기반으로 ONTAP 클러스터, 스토리지 가상 머신(SVM) 및 볼륨의 보안 수준을 확인할 수 있는 대시보드를 제공합니다.

보안 대시보드의 목표는 ONTAP 클러스터가 NetApp 권장 지침을 준수하지 않는 부분을 표시하여 잠재적인 문제를 해결할 수 있도록 하는 것입니다. 대부분의 경우 ONTAP System Manager 또는 ONTAP CLI를 사용하여 문제를 해결합니다. 조직에서 모든 권장 사항을 따르지 않을 수도 있으므로 경우에 따라 변경할 필요가 없을 수도 있습니다.

자세한 권장 사항 및 해결 방안은 "NetApp ONTAP 9 보안 강화 가이드" (TR-4569)를 참조하십시오.

Unified Manager는 보안 상태를 보고하는 것 외에도 보안 위반이 발생한 클러스터 또는 SVM에 대한 보안 이벤트를 생성합니다. 이벤트 관리 인벤토리 페이지에서 이러한 문제를 추적할 수 있으며, 새로운 보안 이벤트가 발생할 때 스토리지 관리자에게 알림이 전송되도록 이러한 이벤트에 대한 경고를 구성할 수 있습니다.

자세한 내용은 "어떤 보안 기준이 평가되고 있습니까"를 참조하십시오.

어떤 보안 기준이 평가되고 있습니까

Active IQ Unified Manager 보안 기준을 평가하는 방법을 이해하십시오.

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

보안 검사에는 다음과 같은 사항들이 포함됩니다:

- 클러스터가 SAML 등 보안 인증 방법을 사용하는지 여부
- 피어링된 클러스터의 통신이 암호화되는지 여부
- 스토리지 VM에서 감사 로그가 활성화되어 있는지 여부
- 볼륨에 소프트웨어 또는 하드웨어 암호화가 활성화되어 있는지 여부

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

> Active IQ 플랫폼에서 보고되는 업그레이드 이벤트는 보안 이벤트로도 간주됩니다. 이러한 이벤트는 해결을 위해 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어(보안 권고 사항의 경우)를 업그레이드해야 하는 문제를 나타냅니다. 이러한 이벤트는 보안 패널에는 표시되지 않지만 이벤트 관리 인벤토리 페이지에서 확인할 수 있습니다.

자세한 내용은 "클러스터 보안 목표 관리"를 참조하십시오.

Active IQ Unified Manager의 클러스터 규정 준수 범주 이해

이 표는 Unified Manager가 평가하는 클러스터 보안 규정 준수 매개변수, NetApp 권장 사항,

그리고 해당 매개변수가 클러스터의 규정 준수 여부 최종 결정에 영향을 미치는지 여부를 설명합니다.

클러스터에 규정을 준수하지 않는 SVM이 있는 경우 클러스터의 규정 준수 값에 영향을 미칩니다. 따라서 경우에 따라 클러스터 보안이 규정을 준수하는 것으로 간주되기 전에 SVM의 보안 문제를 해결해야 할 수 있습니다.

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

매개변수	설명	권장 사항	클러스터 규정 준수에 영향을 미칩니다
글로벌 FIPS	글로벌 FIPS(연방 정보 처리 표준) 140-2 준수 모드 활성화 여부를 나타냅니다. FIPS가 활성화되면 TLSv1 및 SSLv3이 비활성화되고 TLSv1.1 및 TLSv1.2만 허용됩니다.	활성화됨	예
Telnet	시스템에 대한 Telnet 액세스가 활성화되었는지 비활성화되었는지 여부를 나타냅니다. NetApp은 안전한 원격 액세스를 위해 SSH(Secure Shell) 사용을 권장합니다.	비활성화됨	예
안전하지 않은 SSH 설정	SSH가 안전하지 않은 암호화 방식(예: *cbc로 시작하는 암호화 방식)을 사용하는지 여부를 나타냅니다.	아니요	예
로그인 배너	시스템에 접속하는 사용자에 대해 로그인 배너가 활성화 또는 비활성화되어 있는지 나타냅니다.	활성화됨	예
클러스터 피어링	피어링된 클러스터 간 통신이 암호화되는지 또는 암호화되지 않는지를 나타냅니다. 이 매개변수가 규정을 준수하는 것으로 간주되려면 소스 클러스터와 대상 클러스터 모두에 암호화가 구성되어 있어야 합니다.	암호화됨	예

매개변수	설명	권장 사항	클러스터 규정 준수에 영향을 미칩니다
네트워크 시간 프로토콜	클러스터에 하나 이상의 NTP 서버가 구성되어 있는지 여부를 나타냅니다. 이중화 및 최상의 서비스를 위해 NetApp은 클러스터에 최소 3개의 NTP 서버를 연결할 것을 권장합니다.	구성됨	예
OCSP	9.14.1부터 Active IQ Unified Manager는 스토리지 가상 머신(SVM, 이전 명칭: Vserver) 수준에서 온라인 인증서 상태 프로토콜(OCSP) 상태 정보를 제공합니다. 즉, SVM에 대한 모든 SSL/TLS 연결에 OCSP 유효성 검사가 적용되어 이러한 연결에 사용되는 인증서의 무결성과 유효성이 보장됩니다.	활성화됨	아니요
원격 감사 로깅	로그 전달(Syslog)이 암호화되었는지 여부를 나타냅니다.	암호화됨	예
AutoSupport HTTPS 전송	AutoSupport 메시지를 NetApp 지원팀에 전송할 때 HTTPS가 기본 전송 프로토콜로 사용되는지 여부를 나타냅니다.	활성화됨	예
기본 관리자 사용자	기본 관리자 사용자(내장)가 활성화되었는지 비활성화되었는지 나타냅니다. NetApp은 불필요한 내장 계정을 잠그는(비활성화하는) 것을 권장합니다.	비활성화됨	예
SAML 사용자	SAML이 구성되었는지 여부를 나타냅니다. SAML을 사용하면 싱글 사인온을 위한 로그인 방법으로 다단계 인증(MFA)을 구성할 수 있습니다.	아니요	아니요

매개변수	설명	권장 사항	클러스터 규정 준수에 영향을 미칩니다
Active Directory 사용자	Active Directory가 구성되었는지 여부를 나타냅니다. Active Directory와 LDAP는 클러스터에 액세스하는 사용자를 위한 권장 인증 메커니즘입니다.	아니요	아니요
LDAP 사용자	LDAP 구성 여부를 나타냅니다. Active Directory 및 LDAP는 로컬 사용자보다 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 쉘	RSH 활성화 여부를 나타냅니다. 보안상의 이유로 RSH는 비활성화해야 합니다. 안전한 원격 접속을 위해서는 SSH(Secure Shell) 사용을 권장합니다.	비활성화됨	예
사용 중인 MD5	ONTAP 사용자 계정이 보안 수준이 낮은 MD5 해시 함수를 사용하는지 여부를 나타냅니다. MD5 해시를 사용하는 사용자 계정을 SHA-512와 같은 더 안전한 암호화 해시 함수로 마이그레이션하는 것이 좋습니다.	아니요	예
인증서 발급자 유형	사용된 디지털 인증서의 유형을 나타냅니다.	CA 서명됨	아니요

Active IQ Unified Manager에서 스토리지 **VM** 규정 준수 범주 이해

이 표는 Unified Manager가 평가하는 스토리지 가상 머신(SVM) 보안 규정 준수 기준, NetApp 권장 사항, 그리고 해당 매개변수가 SVM의 규정 준수 여부 최종 결정에 영향을 미치는지 여부를 설명합니다.

매개변수	설명	권장 사항	**SVM** 규정 준수에 영향을 미칩니다
감사 로그	감사 로깅이 활성화되었는지 비활성화되었는지를 나타냅니다.	활성화됨	예
안전하지 않은 SSH 설정	SSH가 안전하지 않은 암호(예: `cbc*`(으)로 시작하는 암호)를 사용하는지 여부를 나타냅니다.	아니요	예
로그인 배너	시스템에서 SVM에 액세스하는 사용자에게 로그인 배너가 활성화되는지 또는 비활성화되는지를 나타냅니다.	활성화됨	예
LDAP 암호화	LDAP 암호화가 활성화되었는지 비활성화되었는지를 나타냅니다.	활성화됨	아니요
NTLM 인증	NTLM 인증이 활성화되었는지 비활성화되었는지를 나타냅니다.	활성화됨	아니요
LDAP 페이로드 서명	LDAP 페이로드 서명 기능이 활성화되었는지 비활성화되었는지를 나타냅니다.	활성화됨	아니요
CHAP 설정	CHAP 활성화 여부를 나타냅니다.	활성화됨	아니요
Kerberos V5	Kerberos V5 인증이 활성화되었는지 비활성화되었는지를 나타냅니다.	활성화됨	아니요
NIS 인증	NIS 인증 사용이 구성되어 있는지 여부를 나타냅니다.	비활성화됨	아니요
FPolicy 상태 활성	FPolicy가 생성되었는지 여부를 나타냅니다.	예	아니요
SMB 암호화 활성화됨	SMB 서명 및 봉인 기능이 활성화되어 있지 않은지 여부를 나타냅니다.	예	아니요
SMB 서명 활성화됨	SMB 서명이 활성화되어 있지 않은지 여부를 나타냅니다.	예	아니요

Active IQ Unified Manager에서 볼륨 규정 준수 범주 이해

이 표는 Unified Manager가 볼륨의 데이터가 무단 사용자의 접근으로부터 적절하게 보호되는지

여부를 판단하기 위해 평가하는 볼륨 암호화 매개변수를 설명합니다.

참고로 볼륨 암호화 매개변수는 클러스터 또는 스토리지 VM의 규정 준수 여부에 영향을 미치지 않습니다.

매개변수	설명
소프트웨어 암호화	NetApp 볼륨 암호화(NVE) 또는 NetApp 애그리게이트 암호화(NAE) 소프트웨어 암호화 솔루션을 사용하여 보호되는 볼륨 수를 표시합니다.
하드웨어 암호화	NetApp 스토리지 암호화(NSE) 하드웨어 암호화를 사용하여 보호되는 볼륨 수를 표시합니다.
소프트웨어 및 하드웨어 암호화	소프트웨어 및 하드웨어 암호화로 모두 보호되는 볼륨 수를 표시합니다.
암호화되지 않음	암호화되지 않은 볼륨 수를 표시합니다.

Active IQ Unified Manager에서 클러스터 및 SVM 규정 준수 상태에 대해 알아보기

클러스터 및 스토리지 가상 머신(SVM)은 _NetApp ONTAP 9용 보안 강화 가이드_에 정의된 권장 사항에 대한 평가 대상 보안 기준 중 하나라도 충족되지 않으면 규정을 준수하지 않는 것으로 간주됩니다. 또한, SVM 중 하나라도 규정을 준수하지 않는 것으로 표시되면 해당 클러스터는 규정을 준수하지 않는 것으로 간주됩니다.

보안 카드에 있는 상태 아이콘은 규정 준수와 관련하여 다음과 같은 의미를 갖습니다:

- - 매개변수는 권장 설정대로 구성되었습니다.
- - 해당 매개변수가 권장 설정대로 구성되지 않았습니다.
- - 클러스터에서 기능이 활성화되지 않았거나 매개변수가 권장대로 구성되지 않았지만, 이 매개변수는 오브젝트의 규정 준수에 기여하지 않습니다.

참고로 볼륨 암호화 상태는 클러스터 또는 SVM의 규정 준수 여부에 영향을 미치지 않습니다.

Active IQ Unified Manager에서 클러스터 및 스토리지 VM의 보안 상태를 봅니다

Active IQ Unified Manager를 사용하면 인터페이스의 다양한 지점에서 환경 내 스토리지 오브젝트의 보안 상태를 확인할 수 있습니다. 정의된 매개변수를 기반으로 정보 및 보고서를 수집하고 분석할 수 있으며, 모니터링 대상 클러스터 및 스토리지 VM에서 의심스러운 동작이나 무단 시스템 변경을 감지할 수 있습니다.

보안 권장 사항은 다음을 참조하십시오. "NetApp ONTAP 9 보안 강화 가이드"

보안 페이지에서 오브젝트 수준 보안 상태 보기

시스템 관리자로서 보안 페이지를 사용하여 데이터 센터 및 사이트 수준에서 ONTAP 클러스터와 스토리지 VM의 보안

수준을 확인할 수 있습니다. 지원되는 오브젝트는 클러스터, 스토리지 VM 및 볼륨입니다. 다음 단계를 따르십시오.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭합니다.
2. 모니터링 대상 클러스터 전체의 보안 상태를 볼지, 아니면 특정 클러스터의 보안 상태를 볼지에 따라 *모든 클러스터*를 선택하거나 드롭다운 메뉴에서 특정 클러스터를 선택하십시오.
3. 보안 패널에서 오른쪽 화살표를 클릭합니다. 보안 페이지가 표시됩니다.

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

보안 페이지에는 다음과 같은 패널이 표시됩니다:

- 클러스터 규정 준수: 데이터 센터 내 모든 클러스터의 보안 상태(규정을 준수하는 클러스터와 준수하지 않는 클러스터의 수)
- 스토리지 **VM** 규정 준수: 데이터 센터 내 모든 스토리지 VM의 보안 상태(규정을 준수하는 VM과 준수하지 않는 VM의 수)
- 볼륨 암호화: 환경 내 모든 볼륨의 볼륨 암호화 상태(암호화되거나 암호화되지 않은 볼륨 수)
- 볼륨 랜섬웨어 방지 상태: 환경 내 모든 볼륨의 보안 상태(랜섬웨어 방지 기능이 활성화 또는 비활성화된 볼륨 수)
- 클러스터 인증 및 인증서: SAML, Active Directory, 인증서 및 로컬 인증 등 각 인증 방법을 사용하는 클러스터 수입니다. 이 패널에는 인증서가 만료되었거나 60일 이내에 만료될 예정인 클러스터 수도 표시됩니다.

클러스터 페이지에서 모든 클러스터의 보안 세부 정보 보기

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

단계

1. 왼쪽 탐색 창에서 *스토리지 > 클러스터*를 클릭합니다.
2. *보기 > 보안 > 모든 클러스터*를 선택하십시오.

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

⋮ 추가 옵션 버튼을 클릭하고 Unified Manager의 보안 페이지 또는 System Manager에서 보안 세부 정보를 보도록 선택할 수 있습니다. System Manager에서 세부 정보를 보려면 유효한 자격 증명이 있어야 합니다.

> ⓘ 클러스터의 인증서가 만료된 경우 클러스터 인증서 유효성 아래의 `expired`을(를) 클릭하고 System Manager(9.10.1 이상)에서 갱신할 수 있습니다. System Manager 인스턴스가 9.10.1 이전 릴리스인 경우 `expired`을(를) 클릭할 수 없습니다.

스토리지 **VM** 페이지에서 모든 클러스터의 보안 세부 정보를 볼 수 있습니다.

스토리지 **VM**/보안 세부 정보 페이지를 사용하면 스토리지 VM 수준에서 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 매개변수가 포함된 클러스터 목록이 표시됩니다.

스토리지 VM, 클러스터, 로그인 배너, 감사 로그 및 안전하지 않은 SSH 설정 등 보안 매개변수를 확인하여 스토리지 VM의 보안 규정 준수에 대한 기본 보기를 확인할 수 있습니다.

추가 옵션 버튼을 클릭하고 Unified Manager의 보안 페이지 또는 System Manager에서 보안 세부 정보를 보도록 선택할 수 있습니다. System Manager에서 세부 정보를 보려면 유효한 자격 증명이 있어야 합니다.

볼륨 및 스토리지 VM에 대한 랜섬웨어 방지 보안 세부 정보는 "모든 볼륨 및 스토리지 VM의 랜섬웨어 방지 상태 보기 "을(를) 참조하십시오.

Active IQ Unified Manager에서 소프트웨어 또는 펌웨어 업데이트가 필요할 수 있는 보안 이벤트 보기

영향 영역이 "`Upgrade`"인 특정 보안 이벤트가 있습니다. 이러한 이벤트는 Active IQ 플랫폼에서 보고되며, 해결을 위해 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어(보안 권고 사항의 경우)를 업그레이드해야 하는 문제를 식별합니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

일부 문제는 즉시 시정 조치를 취해야 할 수 있지만, 다른 문제는 다음 정기 유지보수까지 기다릴 수 있습니다. 이러한 모든 이벤트를 확인하고 문제를 해결할 수 있는 사용자에게 할당할 수 있습니다. 또한 알림을 받고 싶지 않은 특정 보안 업그레이드 이벤트가 있는 경우 이 목록을 사용하여 해당 이벤트를 식별하고 비활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *이벤트 관리*를 클릭합니다.

   기본적으로 모든 활성 이벤트(새로 생성된 이벤트 및 승인된 이벤트)가 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 메뉴에서 *업그레이드 이벤트*를 선택합니다.

   이 페이지에는 현재 활성화된 모든 업그레이드 보안 이벤트가 표시됩니다.

Active IQ Unified Manager의 모든 클러스터에서 클러스터가 사용자 인증을 관리하는 방법을 확인합니다

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 수행되고 있는지 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 *대시보드*를 클릭합니다.
2. 대시보드 상단의 드롭다운 메뉴에서 *모든 클러스터*를 선택합니다.
3. **Security** 패널에서 오른쪽 화살표를 클릭하면 **Security** 페이지가 표시됩니다.
4. 클러스터 인증 카드를 보면 각 인증 유형을 사용하여 시스템에 접속하는 사용자 수를 확인할 수 있습니다.

5. 클러스터 보안 카드를 참조하여 각 클러스터에서 사용자를 인증하는 데 사용되는 인증 메커니즘을 확인하십시오.

안전하지 않은 방법을 사용하거나 NetApp에서 권장하지 않는 방법을 사용하여 시스템에 액세스하는 사용자가 있는 경우 해당 방법을 비활성화할 수 있습니다.

Active IQ Unified Manager에서 모든 볼륨의 암호화 상태 보기

모든 볼륨 목록과 현재 암호화 상태를 확인하여 볼륨의 데이터가 권한 없는 사용자의 접근으로부터 적절하게 보호되고 있는지 판단할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨에 적용할 수 있는 암호화 유형은 다음과 같습니다.

- 소프트웨어 - NetApp 볼륨 암호화(NVE) 또는 NetApp 애그리게이트 암호화(NAE) 소프트웨어 암호화 솔루션을 사용하여 보호되는 볼륨입니다.
- 하드웨어 - NetApp 스토리지 암호화(NSE) 하드웨어 암호화를 사용하여 보호되는 볼륨입니다.
- 소프트웨어 및 하드웨어 - 소프트웨어 및 하드웨어 암호화 모두로 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 유형을 가진 볼륨 또는 암호화되지 않은 볼륨(암호화 유형이 “None”)을 표시합니다.

Active IQ Unified Manager에서 모든 볼륨 및 스토리지 VM의 랜섬웨어 방지 상태를 봅니다

모든 볼륨 및 스토리지 가상 머신(SVM) 목록과 현재 랜섬웨어 방지 상태를 확인하여 볼륨 및 SVM의 데이터가 랜섬웨어 공격으로부터 적절하게 보호되고 있는지 판단할 수 있습니다.

시작하기 전에

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다양한 랜섬웨어 방지 상태에 대한 자세한 내용은 "ONTAP: 랜섬웨어 방지 기능 활성화"을(를) 참조하십시오.

랜섬웨어 탐지 기능이 있는 모든 볼륨의 보안 세부 정보 보기

단계

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

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 대해서는 랜섬웨어 방지 기능이 지원되지 않습니다.

랜섬웨어 탐지 기능이 있는 모든 스토리지 **VM**의 보안 세부 정보 보기

단계

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

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

Active IQ Unified Manager에서 모든 활성 보안 이벤트 보기

활성화된 모든 보안 이벤트를 확인하고 각 이벤트를 문제 해결이 가능한 사용자에게 할당할 수 있습니다. 또한 수신을 원하지 않는 특정 보안 이벤트가 있는 경우 이 목록을 통해 비활성화할 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 승인된 이벤트는 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 메뉴에서 *활성 보안 이벤트*를 선택합니다.

   이 페이지에는 지난 7일 동안 발생한 모든 신규 및 승인된 보안 이벤트가 표시됩니다.

Active IQ Unified Manager의 보안 이벤트에 대한 알림 추가

Unified Manager에서 수신하는 다른 이벤트와 마찬가지로 개별 보안 이벤트에 대한 알림을 구성할 수 있습니다. 또한 모든 보안 이벤트를 동일하게 처리하고 동일한 담당자에게 이메일을 보내려면 보안 이벤트가 발생할 때마다 알림을 받도록 단일 알림을 생성할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 예시는 “Telnet Protocol Enabled” 보안 이벤트에 대한 알림을 생성하는 방법을 보여줍니다. 이렇게 하면 클러스터에 원격 관리자 액세스용으로 Telnet 액세스가 구성된 경우 알림이 전송됩니다. 이와 동일한 방법을 사용하여 모든 보안 이벤트에 대한 알림을 생성할 수 있습니다.

단계

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

2. 알림 설정 페이지에서 *추가*를 클릭합니다.
3. 경고 추가 대화 상자에서 *이름*을 클릭하고 경고의 이름과 설명을 입력합니다.
4. *리소스*를 클릭하고 이 알림을 활성화할 클러스터를 선택합니다.
5. *이벤트*를 클릭하고 다음 작업을 수행하십시오:
   a. 이벤트 심각도 목록에서 *경고*를 선택합니다.
   b. 일치하는 이벤트 목록에서 *Telnet 프로토콜 사용*을 선택합니다.
6. 작업*을 클릭한 다음 *알림을 받을 사용자 필드에서 알림 이메일을 받을 사용자의 이름을 선택하십시오.
7. 이 페이지에서 알림 빈도, SNMP 탭 발행 및 스크립트 실행에 대한 기타 옵션을 구성하십시오.
8. *저장*을 클릭합니다.

Active IQ Unified Manager에서 특정 보안 이벤트 비활성화

모든 이벤트는 기본적으로 활성화되어 있습니다. 환경에서 중요하지 않은 이벤트에 대한 알림 생성을 방지하려면 특정 이벤트를 비활성화할 수 있습니다. 알림을 다시 받으려면 비활성화된 이벤트를 다시 활성화할 수 있습니다.

시작하기 전에

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트를 비활성화하면 시스템에 이전에 생성된 이벤트는 더 이상 사용되지 않는 것으로 표시되고, 해당 이벤트에 대해 구성된 알림은 트리거되지 않습니다. 비활성화된 이벤트를 활성화하면 다음 모니터링 주기부터 해당 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 비활성화 또는 활성화하십시오:

원하신다면...	그런 다음 이렇게 하십시오...
이벤트 비활성화	a. *비활성화*를 클릭합니다. b. 이벤트 비활성화 대화 상자에서 심각도를 *경고*로 선택합니다. 이는 모든 보안 이벤트에 적용되는 범주입니다. c. 일치하는 이벤트 열에서 비활성화할 보안 이벤트를 선택한 다음 오른쪽 화살표를 클릭하여 해당 이벤트를 비활성화 이벤트 열로 이동합니다. d. *저장 후 닫기*를 클릭하십시오. e. 비활성화한 이벤트가 이벤트 설정 페이지의 목록 보기에 표시되는지 확인하십시오.
이벤트 활성화	a. 비활성화된 이벤트 목록에서 다시 활성화하려는 이벤트의 확인란을 선택합니다. b. *활성화*를 클릭합니다.

Active IQ Unified Manager에서 보안 이벤트 보기

보안 이벤트는 _NetApp Security Hardening Guide 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 심각도를 평가하고 필요한 경우 문제를 해결할 수 있습니다.

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

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.