보안
ONTAP 9

NetApp
September 12, 2024

목차

보안

클라이언트 인증 및 권한 부여

ONTAP는 표준 방법을 사용하여 클라이언트 및 관리자의 스토리지 액세스를 보호하고 바이러스로부터 보호합니다. 사용되지 않는 데이터의 암호화 및 WORM 스토리지의 고급 기술을 사용할 수 있습니다.

ONTAP는 신뢰할 수 있는 소스로 ID를 확인하여 클라이언트 시스템과 사용자를 인증합니다. ONTAP는 사용자의 자격 증명을 파일 또는 디렉터리에 구성된 권한과 비교하여 사용자가 파일 또는 디렉터리에 액세스할 수 있도록 승인합니다.

인증

로컬 또는 원격 사용자 계정을 생성할 수 있습니다.

- 로컬 계정은 계정 정보가 스토리지 시스템에 상주하는 계정입니다.
- 원격 계정은 계정 정보가 Active Directory 도메인 컨트롤러, LDAP 서버 또는 NIS 서버에 저장되는 계정입니다.

ONTAP는 로컬 또는 외부 이름 서비스를 사용하여 호스트 이름, 사용자, 그룹, 넷그룹 및 이름 매핑 정보를 조회합니다. ONTAP는 다음과 같은 이름 서비스를 지원합니다.

- 로컬 사용자
- DNS
- 외부 NIS 도메인입니다
- 외부 LDAP 도메인입니다

_name 서비스 스위치 table_은 네트워크 정보를 검색할 소스 및 검색 순서를 지정합니다(UNIX 시스템의 /etc/nsswitch.conf 파일에 해당하는 기능 제공). NAS 클라이언트가 SVM에 연결되면 ONTAP는 지정된 이름 서비스를 확인하여 필요한 정보를 얻습니다.

- *Kerberos* 지원* Kerberos는 클라이언트-서버 구현에서 사용자 암호를 암호화하여 "성 인증"을 제공하는 네트워크 인증 프로토콜입니다. ONTAP는 무결성 검사(krb5i)와 Kerberos 5 인증 및 개인 정보 검사(krb5p)를 지원합니다.

권한 부여

ONTAP은 세 가지 보안 수준을 평가하여 엔티티가 SVM에 있는 파일 및 디렉토리에 대해 요청된 작업을 수행할 수 있는 권한이 있는지 확인합니다. 액세스 권한은 보안 수준을 평가한 후 유효한 사용 권한에 따라 결정됩니다.

- 내보내기(NFS) 및 공유(SMB) 보안

  내보내기 및 공유 보안은 지정된 NFS 내보내기 또는 SMB 공유에 대한 클라이언트 액세스에 적용됩니다. 관리 권한이 있는 사용자는 SMB 및 NFS 클라이언트의 내보내기 및 공유 수준 보안을 관리할 수 있습니다.

- 스토리지 레벨 Access Guard 파일 및 디렉토리 보안

  스토리지 레벨 액세스 가드 보안은 SMB 및 NFS 클라이언트가 SVM 볼륨에 액세스하는 데 적용됩니다. NTFS 액세스 권한만 지원됩니다. ONTAP에서 UNIX 사용자에 대한 보안 검사를 수행하여 스토리지 수준 액세스 가드가

적용된 볼륨의 데이터에 액세스하려면 UNIX 사용자는 볼륨을 소유한 SVM에서 Windows 사용자에게 매핑해야 합니다.

- NTFS, UNIX 및 NFSv4 네이티브 파일 레벨 보안

  네이티브 파일 레벨 보안은 스토리지 객체를 나타내는 파일 또는 디렉토리에 존재합니다. 클라이언트에서 파일 수준 보안을 설정할 수 있습니다. 파일 권한은 SMB 또는 NFS를 사용하여 데이터를 액세스하든 관계없이 유효합니다.

SAML을 통한 인증

ONTAP는 원격 사용자 인증을 위해 SAML(Security Assertion Markup Language)을 지원합니다. 몇 가지 인기 ID 공급자(IdP)가 지원됩니다. 지원되는 IdP 및 SAML 인증 설정에 대한 자세한 내용은 을 참조하십시오 "SAML 인증을 구성합니다".

ONTAP REST API 클라이언트가 포함된 OAuth 2.0

Open Authorization(OAuth 2.0) 프레임워크에 대한 지원은 ONTAP 9.14부터 제공됩니다. 클라이언트가 REST API를 사용하여 ONTAP에 액세스할 때 OAuth 2.0만 사용하여 권한 부여 및 액세스 결정을 제어할 수 있습니다. 하지만 CLI, System Manager, REST API를 포함한 모든 ONTAP 관리 인터페이스에서 기능을 구성하고 사용하도록 설정할 수 있습니다.

표준 OAuth 2.0 기능은 널리 사용되는 여러 인증 서버와 함께 지원됩니다. 상호 TLS를 기반으로 보낸 사람 제한 액세스 토큰을 사용하면 ONTAP 보안을 더욱 강화할 수 있습니다. 또한 자체 포함된 범위, ONTAP REST 역할 및 로컬 사용자 정의와의 통합 등 다양한 인증 옵션을 사용할 수 있습니다. 을 참조하십시오 "ONTAP OAuth 2.0 구축 개요" 를 참조하십시오.

관리자 인증 및 RBAC

관리자는 로컬 또는 원격 로그인 계정을 사용하여 클러스터 및 SVM에서 자신을 인증합니다. 역할 기반 액세스 제어(RBAC)는 관리자가 액세스할 수 있는 명령을 결정합니다.

인증

로컬 또는 원격 클러스터 및 SVM 관리자 계정을 생성할 수 있습니다.

- 로컬 계정은 계정 정보, 공개 키 또는 보안 인증서가 스토리지 시스템에 상주하는 계정입니다.
- 원격 계정은 계정 정보가 Active Directory 도메인 컨트롤러, LDAP 서버 또는 NIS 서버에 저장되는 계정입니다.

DNS를 제외하고 ONTAP는 클라이언트를 인증하는 데 사용되는 것과 동일한 이름 서비스를 사용하여 관리자 계정을 인증합니다.

RBAC

관리자에게 할당된 _role_은 관리자가 액세스할 수 있는 명령을 결정합니다. 관리자 계정을 만들 때 역할을 할당합니다. 필요에 따라 다른 역할을 할당하거나 사용자 지정 역할을 정의할 수 있습니다.

바이러스 검사

스토리지 시스템에서 통합 바이러스 백신 기능을 사용하여 바이러스나 기타 악성 코드에 의해

데이터가 손상되는 것을 방지할 수 있습니다. ONTAP 바이러스 검사(*Vscan*)는 동급 최강의 타사 바이러스 백신 소프트웨어와 ONTAP 기능을 결합하여 언제 어떤 파일을 스캔할지 제어하는 데 필요한 유연성을 제공합니다.

스토리지 시스템은 타사 공급업체의 안티바이러스 소프트웨어를 호스팅하는 외부 서버로 검사 작업을 오프로드합니다. NetApp에서 제공하고 외부 서버에 설치된 *ONTAP* 안티바이러스 커넥터 는 스토리지 시스템과 바이러스 백신 소프트웨어 간의 통신을 처리합니다.

- 액세스 시 검사 _ 를 사용하여 클라이언트가 SMB를 통해 파일을 열거나 읽거나 이름을 바꾸거나 닫을 때 바이러스를 검사할 수 있습니다. 외부 서버가 파일의 스캔 상태를 보고할 때까지 파일 작업이 일시 중단됩니다. 파일이 이미 스캔되면 ONTAP에서 파일 작업을 허용합니다. 그렇지 않으면 서버에서 스캔을 요청합니다.

  액세스 시 스캐닝은 NFS에서 지원되지 않습니다.

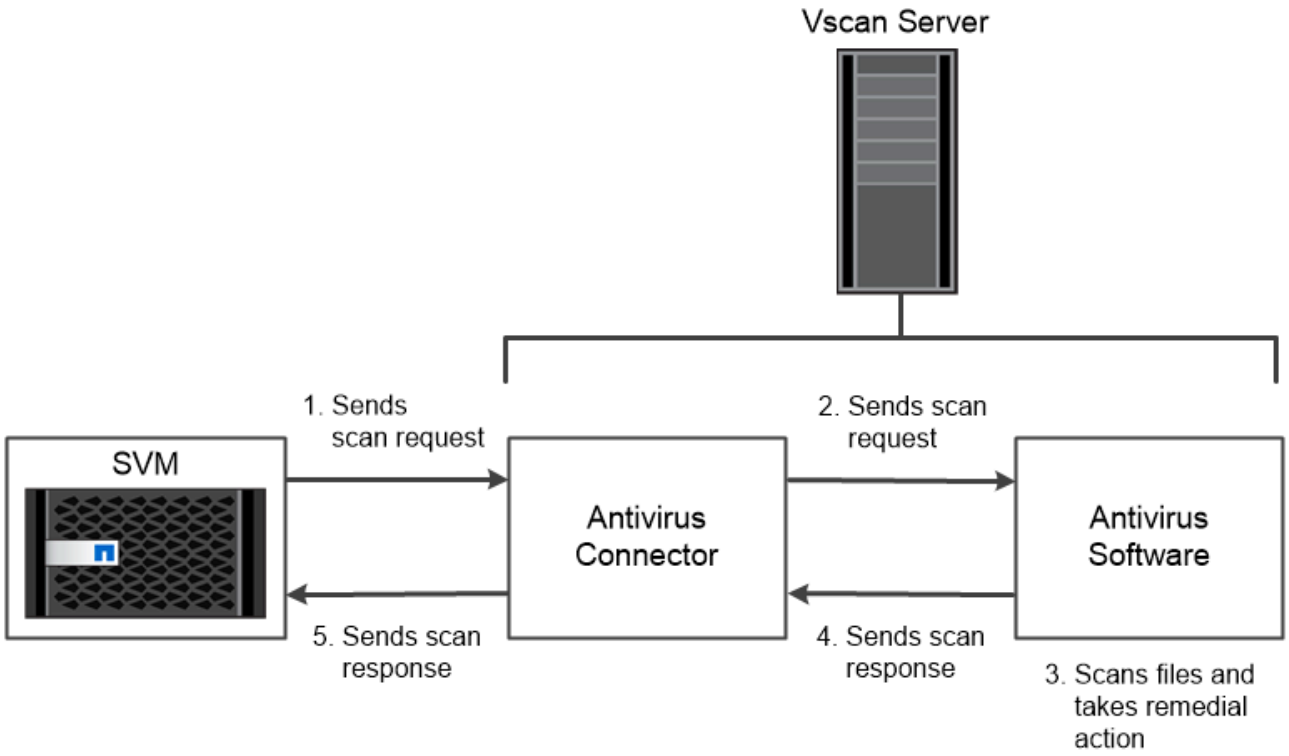
- 주문형 검사 _ 을(를) 사용하여 파일에 바이러스가 있는지 즉시 또는 일정에 따라 확인할 수 있습니다. 예를 들어, 사용량이 적은 시간에만 스캔을 실행할 수 있습니다. 외부 서버는 선택한 파일의 스캔 상태를 업데이트하므로 SMB를 통해 다음에 액세스할 때 해당 파일의 파일 액세스 지연 시간이 일반적으로 줄어듭니다.

  NFS를 통해서만 내보낸 볼륨에서도 SVM 네임스페이스에서 모든 경로에 대해 온디맨드 스캐닝을 사용할 수 있습니다.

일반적으로 SVM에서 두 스캐닝 모드를 모두 사용할 수 있습니다. 어느 모드에서든 바이러스 백신 소프트웨어는 소프트웨어의 설정에 따라 감염된 파일에 대한 치료 조치를 취합니다.

- _ 재해 복구 및 MetroCluster 구성에서 바이러스 검사 _ *

재해 복구 및 MetroCluster 구성을 위해서는 로컬 및 파트너 클러스터용으로 별도의 Vscan 서버를 설정해야 합니다.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

암호화

ONTAP는 소프트웨어 및 하드웨어 기반 암호화 기술을 모두 제공하여 스토리지 미디어가 용도 변경, 반환, 잘못된 위치 변경 또는 도난된 경우 유휴 데이터를 읽을 수 없도록 합니다.

ONTAP는 모든 SSL 연결에 대해 FIPS(Federal Information Processing Standards) 140-2를 준수합니다. 다음 암호화 솔루션을 사용할 수 있습니다.

- 하드웨어 솔루션:
  - NSE(NetApp 스토리지 암호화)

    NSE는 SED(자체 암호화 드라이브)를 사용하는 하드웨어 솔루션입니다.

  - NVMe SED

    ONTAP는 FIPS 140-2 인증이 없는 NVMe SED에 대한 전체 디스크 암호화를 제공합니다.

- 소프트웨어 솔루션:
  - NetApp 애그리게이트 암호화(NAE)

    NAE는 각 애그리게이트의 고유 키를 사용하여 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.

  - NetApp 볼륨 암호화(NVE)

NVE는 각 볼륨의 고유 키를 사용해 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.

소프트웨어(NAE 또는 NVE) 및 하드웨어(NSE 또는 NVMe SED) 암호화 솔루션을 모두 사용하여 유휴 데이터를 두 배로 암호화합니다. 스토리지 효율성은 NAE 또는 NVE 암호화의 영향을 받지 않습니다.

NetApp 스토리지 암호화

NSE(NetApp Storage Encryption)는 데이터를 쓸 때 암호화하는 SED를 지원합니다. 디스크에 저장된 암호화 키가 없으면 데이터를 읽을 수 없습니다. 암호화 키는 인증된 노드에서만 액세스할 수 있습니다.

I/O 요청 시 노드는 외부 키 관리 서버 또는 Onboard Key Manager에서 검색된 인증 키를 사용하여 SED에 대해 자신을 인증합니다.

- 외부 키 관리 서버는 KMIP(Key Management Interoperability Protocol)를 사용하여 노드에 인증 키를 제공하는 스토리지 환경의 타사 시스템입니다.
- Onboard Key Manager는 데이터와 동일한 스토리지 시스템의 노드에 인증 키를 제공하는 기본 제공 도구입니다.

NSE는 자체 암호화 HDD 및 SSD를 지원합니다. NSE와 함께 NetApp 볼륨 암호화를 사용하여 NSE 드라이브의 데이터를 이중 암호화할 수 있습니다.

> Flash Cache 모듈이 있는 시스템에서 NSE를 사용하는 경우, NVE 또는 NAE도 활성화해야 합니다. NSE는 Flash Cache 모듈에 상주하는 데이터를 암호화하지 않습니다.

NVMe 자체 암호화 드라이브

NVMe SED에는 FIPS 140-2 인증이 없지만, AES 256비트 투명 디스크 암호화를 사용하여 유휴 데이터를 보호합니다.

인증 키 생성과 같은 데이터 암호화 작업은 내부적으로 수행됩니다. 스토리지 시스템에서 디스크를 처음 액세스할 때 인증 키가 생성됩니다. 그런 다음, 데이터 작업이 요청될 때마다 스토리지 시스템 인증을 요구하여 유휴 데이터를 보호합니다.

NetApp 애그리게이트 암호화

NetApp Aggregate Encryption(NAE)은 애그리게이트의 모든 데이터를 암호화하는 소프트웨어 기반 기술입니다. NAE의 이점은 볼륨이 애그리게이트 레벨 중복제거에 포함되는 반면, NVE 볼륨은 제외된다는 것입니다.

NAE를 사용하도록 설정하면 애그리게이트 내의 볼륨을 애그리게이트 키로 암호화할 수 있습니다.

ONTAP 9.7부터"NVE 라이센스", 온보드 키 또는 외부 키 관리가 있는 경우 새로 생성된 애그리게이트와 볼륨은 기본적으로 암호화됩니다.

NetApp 볼륨 암호화

NetApp Volume Encryption(NVE)은 유휴 데이터를 한 번에 하나의 볼륨으로 암호화하는 소프트웨어 기반 기술입니다. 스토리지 시스템에서만 액세스할 수 있는 암호화 키를 사용하면 기본 디바이스가 시스템에서 분리되어 있는 경우 볼륨 데이터를 읽을 수 없습니다.

Snapshot 복사본과 메타데이터를 비롯한 두 데이터가 모두 암호화됩니다. 데이터에 대한 액세스는 볼륨별로 고유한 XTS-AES-256 키를 통해 제공됩니다. 내장 Onboard Key Manager는 동일한 시스템에 있는 키를 데이터와 함께

보호합니다.

NVE는 모든 유형의 애그리게이트(HDD, SSD, 하이브리드, 어레이 LUN), RAID 유형, ONTAP Select를 비롯한 지원되는 모든 ONTAP 구현에서 사용할 수 있습니다. NSE(NetApp 스토리지 암호화)와 NVE를 사용하여 NSE 드라이브의 데이터를 이중 암호화할 수 있습니다.

- *KMIP* 서버 사용 시기 * 저렴한 비용으로 일반적으로 Onboard Key Manager를 사용하는 것이 더 편리하지만, 다음 중 하나라도 해당되는 경우 KMIP 서버를 설치해야 합니다.
- 암호화 키 관리 솔루션은 FIPS(Federal Information Processing Standards) 140-2 또는 KMIP OASIS KMIP 표준을 준수해야 합니다.
- 다중 클러스터 솔루션이 필요합니다. KMIP 서버는 암호화 키를 중앙에서 관리하여 여러 클러스터를 지원합니다.

  KMIP 서버는 암호화 키를 중앙에서 관리하여 여러 클러스터를 지원합니다.

- 기업은 인증 키를 시스템 또는 데이터와 다른 위치에 저장하는 추가적인 보안을 필요로 합니다.

  KMIP 서버는 데이터와 별도로 인증 키를 저장합니다.

관련 정보

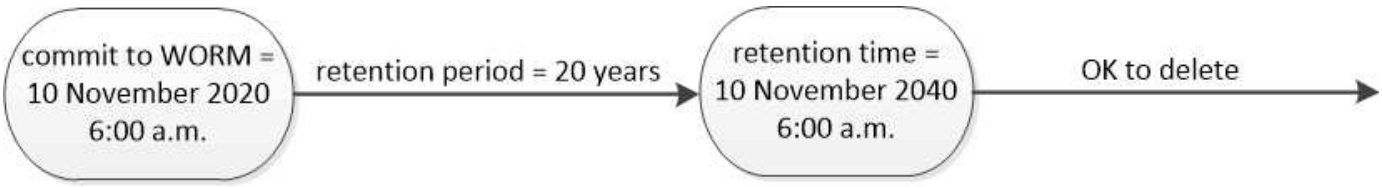
"FAQ - NetApp 볼륨 암호화 및 NetApp 애그리게이트 암호화"

WORM 스토리지

*SnapLock_*는 규정 및 거버넌스 목적을 위해 중요한 파일을 수정되지 않은 형태로 유지하기 위해 *_WORM(Write Once, Read Many)* 스토리지를 사용하는 조직을 위한 고성능 규정 준수 솔루션입니다.

단일 라이센스를 사용하면 SEC Rule 17a-4 및 L느슨한_Enterprise 모드와 같은 외부 규정을 충족하기 위해 엄격한 _규정 준수 모드에서 SnapLock를 사용할 수 있으며, 디지털 자산 보호를 위해 내부적으로 규정된 규정을 준수할 수 있습니다. SnapLock는 변조 방지 _ComplianceClock_을 사용하여 WORM 파일의 보존 기간이 경과되었는지 확인합니다.

SnapVault _ 에 _SnapLock를 사용하여 보조 스토리지에서 WORM 상태로 스냅샷 복사본을 보호할 수 있습니다. SnapMirror를 사용하여 재해 복구 및 기타 목적으로 WORM 파일을 다른 지리적 위치에 복제할 수 있습니다.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.