Sicherheit

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

Sicherheit

Client-Authentifizierung und -Autorisierung

ONTAP nutzt Standardmethoden, um den Zugriff von Clients und Administratoren auf den Storage zu sichern und gegen Viren zu schützen. Fortschrittliche Technologien stehen zur Verschlüsselung von Daten im Ruhezustand und ALS WORM Storage zur Verfügung.

ONTAP authentifiziert einen Client-Computer und einen Benutzer, indem die Identität mit einer vertrauenswürdigen Quelle überprüft wird. ONTAP autorisiert einen Benutzer für den Zugriff auf eine Datei oder ein Verzeichnis, indem die Anmeldeinformationen des Benutzers mit den für die Datei oder das Verzeichnis konfigurierten Berechtigungen verglichen werden.

Authentifizierung

Sie können lokale oder Remote-Benutzerkonten erstellen:

- Bei einem lokalen Konto handelt es sich um ein Konto, in dem die Kontoinformationen auf dem Speichersystem gespeichert sind.
- Bei einem Remote-Konto werden Kontoinformationen auf einem Active Directory-Domänencontroller, einem LDAP-Server oder einem NIS-Server gespeichert.

ONTAP verwendet lokale oder externe Namensdienste, um Informationen zur Zuordnung von Host-Namen, Benutzer, Gruppe, Netzgruppe und Namen abzurufen. ONTAP unterstützt folgende Namensdienste:

- Lokale Benutzer
- DNS
- Externe NIS-Domänen
- Externe LDAP-Domänen

Eine Switch-Tabelle *Name Service* gibt die Quellen für die Suche nach Netzwerkinformationen und die Reihenfolge an, in der sie durchsucht werden sollen (Bereitstellung der entsprechenden Funktionalität der Datei /etc/nsswitch.conf auf UNIX-Systemen). Wenn ein NAS-Client eine Verbindung zur SVM herstellt, überprüft ONTAP die angegebenen Namensservices, um die erforderlichen Informationen abzurufen.

Kerberos-Unterstützung Kerberos ist ein Netzwerk-Authentifizierungsprotokoll, das durch Verschlüsselung von Benutzerpasswörtern in Client-Server-Implementierungen “sTrong Authentication” bereitstellt. ONTAP unterstützt Kerberos 5-Authentifizierung mit Integritätsprüfung (krb5i) und Kerberos 5-Authentifizierung mit Datenschutzprüfung (krb5p).

Autorisierung

ONTAP bewertet drei Sicherheitsstufen, um zu ermitteln, ob eine Einheit autorisiert ist, eine angeforderte Aktion für Dateien und Verzeichnisse, die sich auf einer SVM befinden, durchzuführen. Der Zugriff wird durch die effektiven Berechtigungen nach Auswertung der Sicherheitsstufen bestimmt:

- Exportsicherheit (NFS) und Freigabe (SMB)

  Die Export- und Share-Sicherheit gilt für den Client-Zugriff auf einen bestimmten NFS-Export oder eine

bestimmte SMB-Freigabe. Benutzer mit Administratorrechten können die Sicherheit von Export- und Share-Ebene über SMB- und NFS-Clients managen.

- Sicherheit von Datei- und Verzeichnisdateien auf Storage-Ebene

  Die Sicherheit der Storage-Level Access Guard-Lösung gilt für den Zugriff von SMB- und NFS-Clients auf SVM Volumes. Es werden nur NTFS-Zugriffsberechtigungen unterstützt. Damit ONTAP auf UNIX-Benutzern Sicherheitsüberprüfungen für den Zugriff auf Daten auf Volumes durchführen kann, für die der Storage-Level Access Guard angewendet wurde, muss der UNIX-Benutzer einem Windows-Benutzer auf der SVM, der auch Eigentümer des Volumes ist, zuordnen.

- Native Sicherheit auf Dateiebene durch NTFS, UNIX und NFSv4

  Die Datei oder das Verzeichnis, die das Storage-Objekt repräsentieren, enthält native Sicherheit auf Dateiebene. Sie können die Sicherheit auf Dateiebene von einem Client aus festlegen. Die Dateiberechtigungen haben unabhängig davon, ob SMB oder NFS für den Zugriff auf die Daten verwendet wird.

Administratorauthentifizierung und RBAC

Administratoren authentifizieren sich mithilfe von lokalen oder Remote-Anmeldekonten beim Cluster und der SVM. Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) legt die Befehle fest, auf die ein Administrator zugreifen kann.

Authentifizierung

Sie können lokale oder Remote-Cluster und SVM-Administratorkonten erstellen:

- Bei einem lokalen Konto handelt es sich um ein Konto, in dem die Kontoinformationen, der öffentliche Schlüssel oder das Sicherheitszertifikat im Speichersystem gespeichert sind.
- Bei einem Remote-Konto werden Kontoinformationen auf einem Active Directory-Domänencontroller, einem LDAP-Server oder einem NIS-Server gespeichert.

Mit Ausnahme von DNS verwendet ONTAP dieselben Namensservices, um Administratorkonten zu authentifizieren, wie sie zum Authentifizieren von Clients verwendet werden.

RBAC

Die einem Administrator zugewiesene *Rolle* bestimmt die Befehle, auf die der Administrator Zugriff hat. Sie weisen die Rolle beim Erstellen des Kontos für den Administrator zu. Sie können je nach Bedarf eine andere Rolle zuweisen oder benutzerdefinierte Rollen definieren.

Virus-Scan

Sie können die integrierte Virenschutzfunktionalität des Storage-Systems verwenden, um Daten vor Viren oder anderen schädlichen Angriffen zu schützen. ONTAP Virus Scanning, genannt *Vscan*, kombiniert erstklassige Antivirensoftware von Drittanbietern mit ONTAP-Funktionen, die Ihnen die Flexibilität geben, die Sie benötigen, um zu kontrollieren, welche Dateien gescannt werden und wann.

Storage-Systeme verlagern Scanvorgänge auf externe Server, auf denen Virenschutz-Software von Drittanbietern gehostet wird. Der von NetApp bereitgestellte *ONTAP Antivirus Connector* wickelt die Kommunikation zwischen dem Storage-System und der Virenschutz-Software ab. Er wird auf dem externen Server installiert.

- Sie können *On-Access Scanning* verwenden, um nach Viren zu suchen, wenn Clients Dateien über SMB öffnen, lesen, umbenennen oder schließen. Der Dateivorgang wird angehalten, bis der externe Server den Scanstatus der Datei meldet. Wenn die Datei bereits gescannt wurde, ermöglicht ONTAP den Dateivorgang. Andernfalls fordert er einen Scan vom Server an.

  Das Scannen beim Zugriff wird für NFS nicht unterstützt.

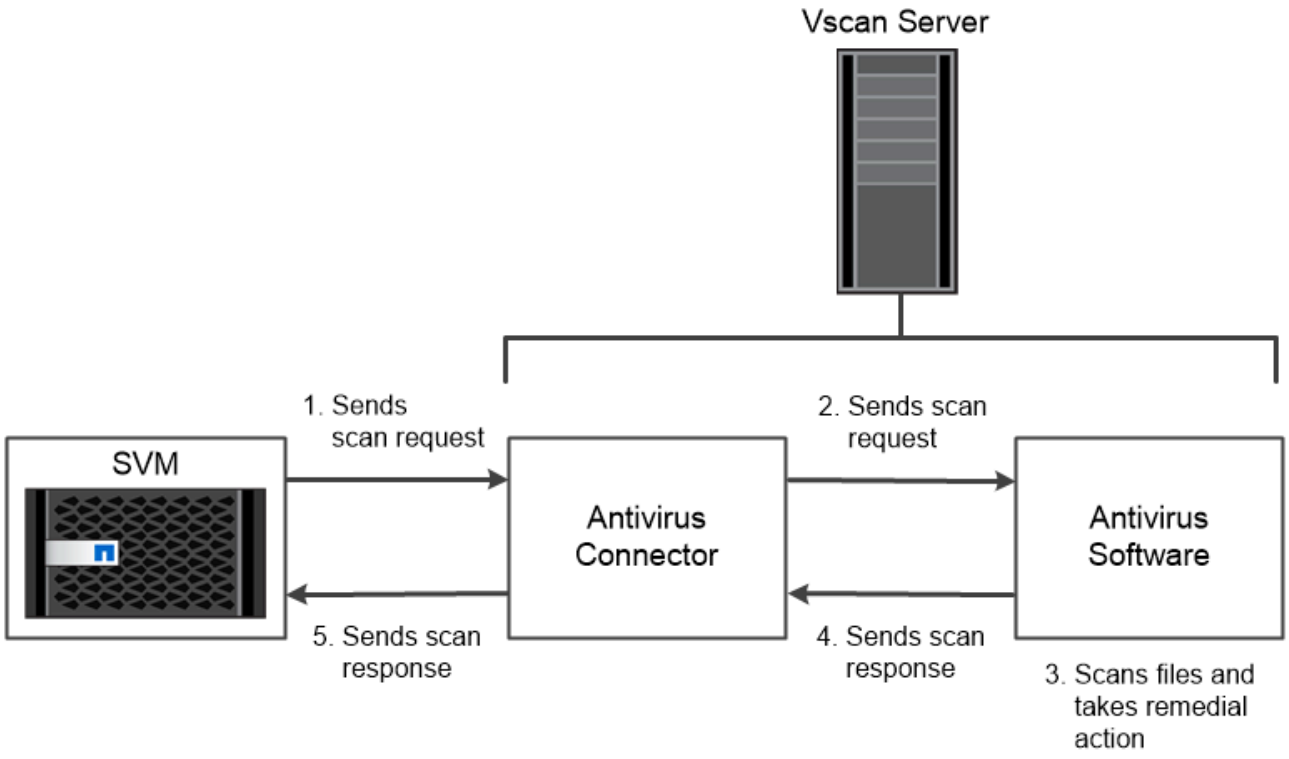
- Sie können *On-Demand Scan* verwenden, um Dateien sofort oder nach Zeitplan auf Viren zu überprüfen. Möglicherweise sollten Sie Scans nur außerhalb der Stoßzeiten durchführen, z. B.. Der externe Server aktualisiert den Scanstatus der überprüften Dateien, sodass die Verzögerung beim Dateizugriff für diese Dateien (sofern sie nicht geändert wurden) in der Regel beim nächsten Zugriff über SMB reduziert wird.

  Der bedarfsorientierte Scan eignet sich für jeden Pfad im SVM Namespace. Dies gilt auch für Volumes, die nur über NFS exportiert werden.

Sie aktivieren normalerweise beide Scanmodi auf einer SVM. In beiden Modi übernimmt die Antivirus-Software basierend auf Ihren Einstellungen in der Software eine Störungsbehebung bei infizierten Dateien.

Virus-Scanning in Disaster Recovery- und MetroCluster-Konfigurationen

Für Disaster Recovery- und MetroCluster-Konfigurationen müssen separate Vscan-Server für lokale und Partner-Cluster eingerichtet werden.



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

Verschlüsselung

ONTAP bietet sowohl Software- als auch hardwarebasierte Verschlüsselungstechnologien, sodass Daten im Ruhezustand nicht gelesen werden können, wenn das Storage-Medium neu verwendet, zurückgegeben, verloren gegangen oder gestohlen wird.

ONTAP entspricht den Federal Information Processing Standards (FIPS) 140-2 für alle SSL-Verbindungen. Sie können die folgenden Verschlüsselungslösungen verwenden:

- Hardwarelösungen:
  - NetApp Storage Encryption (NSE)

    NSE ist eine Hardware-Lösung, die Self-Encrypting Drives (SEDs) verwendet.

  - NVMe SEDs

    ONTAP bietet vollständige Festplattenverschlüsselung für NVMe SEDs, die nicht über eine FIPS-140-2-Zertifizierung verfügen.
- Softwarelösungen:
  - NetApp Aggregatverschlüsselung (NAE)

    NAE ist eine Software-Lösung, die die Verschlüsselung beliebiger Daten-Volumes auf jedem beliebigen Laufwerkstyp ermöglicht und bei jedem Aggregat mit eindeutigen Schlüsseln aktiviert wird.

  - NetApp Volume Encryption (NVE)

    NVE ist eine Softwarelösung, die die Verschlüsselung von beliebigen Daten-Volumes auf jedem Festplattentyp, auf der diese aktiviert ist, mit einem eindeutigen Schlüssel für jedes Volume ermöglicht.

Doppelte Verschlüsselung im Ruhezustand: Sowohl Software- (NAE oder NVE) als auch Hardware-Verschlüsselungslösungen (NSE oder NVMe SED) können verwendet werden. Storage-Effizienz wird nicht durch NAE- oder NVE-Verschlüsselung beeinträchtigt.

NetApp Storage Encryption

NetApp Storage Encryption (NSE) unterstützt SEDs, die Daten beim Schreiben verschlüsseln. Ohne einen auf der Festplatte gespeicherten Verschlüsselungsschlüssel können die Daten nicht gelesen werden. Der Verschlüsselungsschlüssel wiederum ist nur für einen authentifizierten Knoten zugänglich.

Bei einer I/O-Anforderung authentifiziert sich ein Node mithilfe eines Authentifizierungsschlüssels, der von einem externen Schlüsselverwaltungsserver oder dem Onboard Key Manager abgerufen wird:

- Der externe Verschlüsselungsmanagement-Server ist ein Drittanbietersystem in der Storage-Umgebung, das Authentifizierungsschlüssel für Nodes mithilfe des Key Management Interoperability Protocol (KMIP) bereitstellt.
- Der integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt.

NSE unterstützt HDDs und SSDs mit automatischer Verschlüsselung. Mit NetApp Volume Encryption mit NSE lassen sich Daten auf NSE-Laufwerken verdoppeln.

NVMe Self-Encrypting Drives

NVMe SEDs haben keine FIPS 140-2-2-Zertifizierung. Diese Festplatten verwenden jedoch eine transparente AES-256-Bit-Festplattenverschlüsselung zum Schutz von Daten im Ruhezustand.

Datenverschlüsselungsvorgänge wie das Generieren eines Authentifizierungsschlüssels werden intern durchgeführt. Der Authentifizierungsschlüssel wird beim ersten Zugriff des Speichersystems auf die Festplatte generiert. Danach sichern die Festplatten die Daten im Ruhezustand, da bei der Anforderung von Datenoperationen eine Storage-Systemauthentifizierung erforderlich ist.

NetApp Aggregatverschlüsselung

NetApp Aggregate Encryption (NAE) ist eine softwarebasierte Technologie zur Verschlüsselung aller Daten auf einem Aggregat. Ein Vorteil von NAE besteht darin, dass Volumes in der Deduplizierung auf Aggregatebene enthalten sind, während NVE Volumes ausgeschlossen sind.

Bei aktiviertem NAE können die Volumes im Aggregat mit aggregierten Schlüsseln verschlüsselt werden.

Ab ONTAP 9.7 werden neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn Sie über die NVE-Lizenz und das integrierte oder externe Verschlüsselungsmanagement verfügen.

NetApp Volume Encryption

NetApp Volume Encryption (NVE) ist eine softwarebasierte Technologie, mit der Daten im Ruhezustand um ein Volume gleichzeitig verschlüsselt werden. Ein Verschlüsselungsschlüssel, auf den nur das Storage-System zugreifen kann, stellt sicher, dass Volume-Daten nicht gelesen werden können, wenn das zugrunde liegende Gerät vom System getrennt ist.

Beide Daten, einschließlich Snapshot Kopien und Metadaten sind verschlüsselt. Der Zugriff auf die Daten erfolgt über einen eindeutigen XTS-AES-256-Schlüssel, einen pro Volume. Ein integrierter Onboard Key Manager sichert die Schlüssel auf demselben System mit Ihren Daten.

NVE kann für jeden Aggregattyp (HDD, SSD, Hybrid, Array LUN), mit jedem RAID-Typ und in jeder unterstützten ONTAP Implementierung, einschließlich ONTAP Select, eingesetzt werden. Darüber hinaus kann NVE mit NetApp Storage Encryption (NSE) eingesetzt werden, um Daten auf NSE-Laufwerken zu verdoppeln.

When to Use KMIP Servers Obwohl es kostengünstiger und in der Regel bequemer ist, den Onboard Key Manager zu verwenden, sollten Sie KMIP Server einrichten, wenn einer der folgenden zutrifft:

- Ihre Lösung für das Verschlüsselungsmanagement muss den Federal Information Processing Standards (FIPS) 140-2 oder DEM OASIS KMIP Standard entsprechen.
- Sie benötigen eine Multi-Cluster-Lösung. KMIP-Server unterstützen mehrere Cluster mit zentralem Schlüsselmanagement.

  KMIP-Server unterstützen mehrere Cluster mit zentralem Schlüsselmanagement.

- Ihr Unternehmen erfordert die zusätzliche Sicherheit beim Speichern von Authentifizierungsschlüsseln auf einem System oder an einem anderen Speicherort als den Daten.

  KMIP-Server speichern Authentifizierungsschlüssel getrennt von Ihren Daten.

Verwandte Informationen

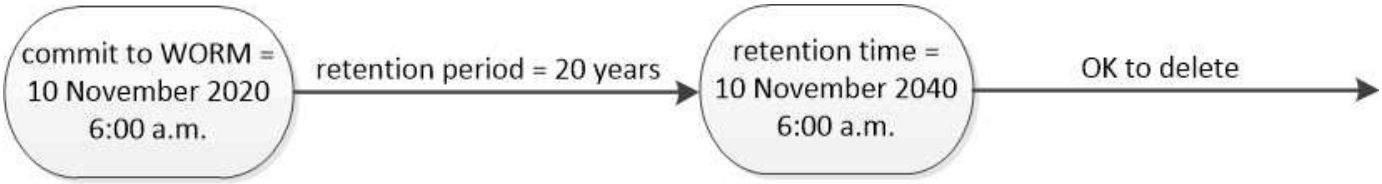
"FAQ – NetApp Volume Encryption und NetApp Aggregate Encryption"

WORM-Storage

SnapLock ist eine hochperformante Compliance-Lösung für Unternehmen, die WORM_-Storage (Write Once, Read Many) verwenden, um kritische Dateien zu regulatorischen und Governance-Zwecken in unveränderter Form aufzubewahren.

Eine einzige Lizenz berechtigt Sie zur Verwendung von SnapLock im strengen *Compliance-Modus,* zur Erfüllung externer Vorgaben wie SEC Rule 17a-4 und einem gelockeren *Enterprise-Modus*, um die intern vorgeschriebenen Vorschriften zum Schutz digitaler Assets zu erfüllen. SnapLock bestimmt anhand eines manipulationssicheren *ComplianceClock*, wann der Aufbewahrungszeitraum für EINE WORM-Datei abgelaufen ist.

Mithilfe von *SnapLock für SnapVault* können Sie Snapshot Kopien MIT WORM-Schutz auf dem Sekundärspeicher schützen. AUSSERDEM KÖNNEN WORM-Dateien zur Disaster Recovery und zu anderen Zwecken an einem anderen geografischen Standort repliziert werden.



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