Sécurité

ONTAP 9

NetApp
April 24, 2024

Sommaire

Sécurité

Authentification et autorisation du client

ONTAP utilise des méthodes standard pour sécuriser l'accès client et administrateur au stockage et se protéger contre les virus. Des technologies avancées sont disponibles pour le chiffrement des données au repos et WORM.

ONTAP authentifie un ordinateur client et un utilisateur en vérifiant son identité avec une source de confiance. ONTAP autorise un utilisateur à accéder à un fichier ou à un répertoire en comparant les informations d'identification de l'utilisateur aux autorisations configurées sur le fichier ou le répertoire.

Authentification

Vous pouvez créer des comptes utilisateur locaux ou distants :

- Un compte local est un compte dans lequel les informations de compte résident sur le système de stockage.
- Un compte distant est un compte dans lequel les informations de compte sont stockées sur un contrôleur de domaine Active Directory, un serveur LDAP ou un serveur NIS.

ONTAP utilise des services de noms locaux ou externes pour rechercher les informations de nom d'hôte, d'utilisateur, de groupe, de groupe réseau et de mappage de noms. ONTAP prend en charge les noms suivants :

- Utilisateurs locaux
- DNS
- Domaines NIS externes
- Domaines LDAP externes

Un *name service switch table* spécifie les sources à rechercher des informations sur le réseau et l'ordre dans lequel les rechercher (fournissant la fonctionnalité équivalente du fichier /etc/nsswitch.conf sur les systèmes UNIX). Lorsqu'un client NAS se connecte au SVM, ONTAP vérifie les services de nom spécifiés pour obtenir les informations requises.

prise en charge de Kerberos Kerberos est un protocole d'authentification réseau qui fournit "`l'authentification`tongs" en cryptant les mots de passe utilisateur dans les implémentations client-serveur. ONTAP prend en charge l'authentification Kerberos 5 avec contrôle d'intégrité (krb5i) et l'authentification Kerberos 5 avec vérification de la confidentialité (krb5p).

Autorisation

ONTAP évalue trois niveaux de sécurité pour déterminer si une entité est autorisée à effectuer une action demandée sur les fichiers et répertoires résidant sur une SVM. L'accès est déterminé par les autorisations effectives après évaluation des niveaux de sécurité :

- Sécurité des exportations (NFS) et des partages (SMB)

  La sécurité des exportations et des partages s'applique à l'accès client à une exportation NFS ou à un

partage SMB donné. Les utilisateurs disposant de privilèges d'administration peuvent gérer la sécurité au niveau de l'exportation et du partage à partir des clients SMB et NFS.

- Sécurité des fichiers et répertoires Access Guard du niveau de stockage

  La sécurité Access Guard du niveau de stockage s'applique aux accès des clients SMB et NFS pour les volumes SVM. Seules les autorisations d'accès NTFS sont prises en charge. Pour que ONTAP puisse effectuer des vérifications de sécurité sur les utilisateurs UNIX afin d'accéder aux données sur les volumes pour lesquels Storage-Level Access Guard a été appliqué, l'utilisateur UNIX doit mapper un utilisateur Windows sur le SVM propriétaire du volume.

- Sécurité native au niveau des fichiers NTFS, UNIX et NFSv4

  La sécurité native au niveau du fichier existe sur le fichier ou le répertoire qui représente l'objet de stockage. Vous pouvez définir la sécurité au niveau des fichiers à partir d'un client. Les autorisations liées aux fichiers sont efficaces, que SMB ou NFS soit utilisé pour accéder aux données.

Authentification avec SAML

ONTAP prend en charge le langage SAML (Security assertion Markup Language) pour l'authentification des utilisateurs distants. Plusieurs fournisseurs d'identité (PDI) populaires sont pris en charge. Pour plus d'informations sur les PDI pris en charge et pour savoir comment activer l'authentification SAML, reportez-vous à la section "Configurez l'authentification SAML".

OAuth 2.0 avec clients API REST ONTAP

La prise en charge de l'infrastructure d'autorisation ouverte (OAuth 2.0) est disponible à partir de ONTAP 9.14. Vous ne pouvez utiliser OAuth 2.0 que pour prendre des décisions d'autorisation et de contrôle d'accès lorsque le client utilise l'API REST pour accéder à ONTAP. Toutefois, vous pouvez configurer et activer cette fonctionnalité avec n'importe quelle interface d'administration ONTAP, y compris l'interface de ligne de commandes, System Manager et l'API REST.

Les fonctionnalités standard d'OAuth 2.0 sont prises en charge avec plusieurs serveurs d'autorisation courants. Vous pouvez améliorer davantage la sécurité ONTAP en utilisant des jetons d'accès limités par l'expéditeur basés sur le protocole commun. De plus, de nombreuses options d'autorisation sont disponibles, notamment des étendues autonomes, ainsi que l'intégration avec les rôles REST ONTAP et les définitions d'utilisateur local. Voir "Présentation de la mise en œuvre de ONTAP OAuth 2.0" pour en savoir plus.

Authentification de l'administrateur et RBAC

Les administrateurs utilisent des comptes de connexion locaux ou distants pour s'authentifier auprès du cluster et du SVM. Le contrôle d'accès basé sur des rôles (RBAC) détermine les commandes à laquelle un administrateur a accès.

Authentification

Vous pouvez créer des comptes d'administrateur du cluster et des SVM locaux ou distants :

- Un compte local est un compte dans lequel les informations de compte, la clé publique ou le certificat de sécurité résident sur le système de stockage.
- Un compte distant est un compte dans lequel les informations de compte sont stockées sur un contrôleur de domaine Active Directory, un serveur LDAP ou un serveur NIS.

À l'exception du DNS, ONTAP utilise les mêmes services de noms pour authentifier les comptes d'administrateur qu'il utilise pour authentifier les clients.

RBAC

Le *role* attribué à un administrateur détermine les commandes auxquelles l'administrateur a accès. Vous attribuez le rôle lorsque vous créez le compte pour l'administrateur. Vous pouvez attribuer un autre rôle ou définir des rôles personnalisés selon vos besoins.

Analyse antivirus

Vous pouvez utiliser la fonctionnalité antivirus intégrée sur le système de stockage afin de protéger vos données contre les virus ou tout autre code malveillant. L'analyse antivirus ONTAP, appelée *Vscan*, associe le meilleur logiciel antivirus tiers à des fonctionnalités ONTAP, vous offrant ainsi la flexibilité nécessaire pour contrôler quels fichiers sont analysés et à quel moment.

Les systèmes de stockage délèguent des opérations d'analyse à des serveurs externes hébergeant le logiciel antivirus de fournisseurs tiers. Le *ONTAP antivirus Connector*, fourni par NetApp et installé sur le serveur externe, gère les communications entre le système de stockage et le logiciel antivirus.

- Vous pouvez utiliser *On-Access scan* pour rechercher des virus lorsque les clients ouvrent, lisent, renomment ou ferment des fichiers sur SMB. L'opération de fichier est suspendue jusqu'à ce que le serveur externe indique l'état de numérisation du fichier. Si le fichier a déjà été numérisé, ONTAP autorise l'opération de fichier. Dans le cas contraire, il demande un scan à partir du serveur.

  L'analyse lors de l'accès n'est pas prise en charge par NFS.

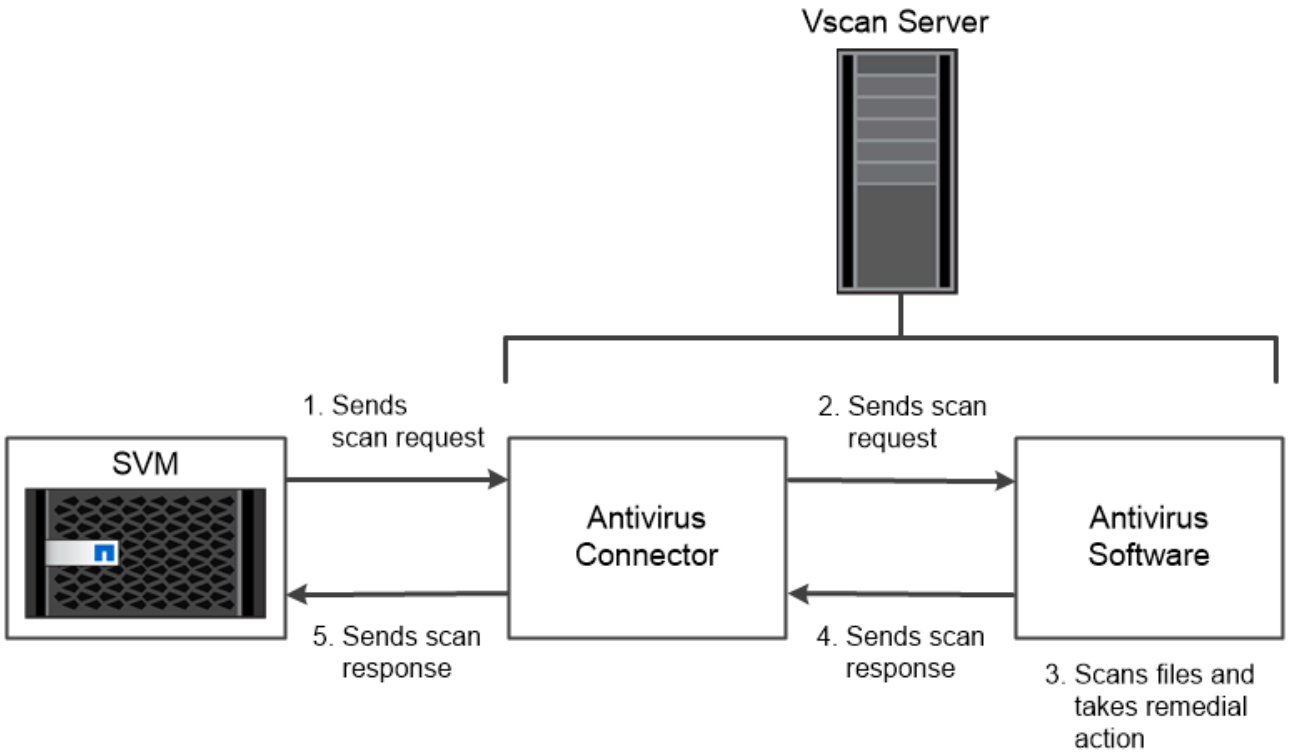
- Vous pouvez utiliser *On-Demand scan* pour vérifier immédiatement ou selon un planning les fichiers à la recherche de virus. Il se peut que vous souhaitiez exécuter des analyses uniquement pendant les heures creuses, par exemple. Le serveur externe met à jour l'état d'analyse des fichiers vérifiés, de sorte que la latence d'accès aux fichiers pour ces fichiers (en supposant qu'ils n'ont pas été modifiés) est généralement réduite lorsqu'ils sont ensuite accédés par SMB.

  Vous pouvez utiliser l'analyse à la demande pour n'importe quel chemin du namespace du SVM, même pour les volumes exportés uniquement via NFS.

Vous activez généralement les deux modes de scan sur un SVM. Dans les deux modes, le logiciel antivirus prend des mesures correctives sur les fichiers infectés en fonction de vos paramètres dans le logiciel.

analyse antivirus dans la reprise après sinistre et configurations MetroCluster

Pour la reprise sur incident et les configurations MetroCluster, il faut configurer des serveurs Vscan séparés pour les clusters locaux et partenaires.



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

Le cryptage

ONTAP propose des technologies de cryptage logicielles et matérielles qui permettent de garantir que les données au repos ne peuvent pas être lues si le support de stockage est requalifié, perdu ou volé.

ONTAP est conforme à la norme FIPS (Federal information Processing Standards) 140-2 pour toutes les connexions SSL. Vous pouvez utiliser les solutions de cryptage suivantes :

- Solutions matérielles :
  - NetApp Storage Encryption (NSE)

    NSE est une solution matérielle qui utilise des lecteurs auto-cryptés (SED).

  - Disques SED NVMe

    ONTAP fournit le chiffrement de disque intégral pour les disques SED NVMe qui ne sont pas certifiés FIPS 140-2.

- Solutions logicielles :
  - Chiffrement d'agrégat NetApp (NAE)

    NAE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque grâce à des clés uniques pour chaque agrégat.

  - NVE (NetApp Volume Encryption)

NVE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque où il est activé avec une clé unique pour chaque volume.

Utilisez les solutions de chiffrement logiciel (NAE ou NVE) et matériel (NSE ou NVMe SED) afin d'obtenir le double chiffrement au repos. L'efficacité du stockage n'est pas affectée par le chiffrement NAE ou NVE.

NetApp Storage Encryption

NetApp Storage Encryption (NSE) prend en charge les disques SED qui cryptent les données au fur et à mesure de leur écriture. Les données ne peuvent pas être lues sans une clé de chiffrement stockée sur le disque. La clé de chiffrement, à son tour, n'est accessible qu'à un nœud authentifié.

Lors d'une demande d'E/S, un nœud s'authentifie auprès d'un SED à l'aide d'une clé d'authentification extraite d'un serveur de gestion de clés externe ou d'un gestionnaire de clés intégré :

- Le serveur externe de gestion des clés est un système tiers de votre environnement de stockage qui transmet des clés d'authentification aux nœuds à l'aide du protocole KMIP (Key Management Interoperability Protocol).
- Le gestionnaire de clés intégré est un outil intégré qui sert des clés d'authentification aux nœuds du même système de stockage que vos données.

NSE prend en charge les disques durs et SSD à autocryptage. Vous pouvez utiliser NetApp Volume Encryption avec NSE pour doubler le chiffrement des données sur les disques NSE.

> Si vous utilisez NSE sur un système doté d'un module Flash cache, vous devez également activer NVE ou NAE. NSE ne chiffre pas les données qui résident sur le module Flash cache.

Disques à autochiffrement NVMe

Les disques SED NVMe ne disposent pas de la certification FIPS 140-2-2. Cependant, ces disques utilisent le chiffrement de disque transparent AES 256 bits pour protéger les données au repos.

Les opérations de chiffrement des données, telles que la génération d'une clé d'authentification, sont effectuées en interne. La clé d'authentification est générée la première fois que le système de stockage accède au disque. Les disques protègent ensuite les données au repos en demandant une authentification du système de stockage à chaque fois que des opérations de données sont demandées.

Chiffrement d'agrégat NetApp

NetApp Aggregate Encryption (NAE) est une technologie logicielle de chiffrement de toutes les données dans un agrégat. NAE a pour avantage de regrouper les volumes dans la déduplication au niveau des agrégats, là où les volumes NVE sont exclus.

NAE permet de chiffrer les volumes au sein de l'agrégat à l'aide de clés d'agrégat.

Depuis la version ONTAP 9.7, les nouveaux agrégats et volumes créés sont chiffrés par défaut lorsque vous disposez de "Licence NVE" et une gestion intégrée ou externe des clés.

NetApp Volume Encryption

NetApp Volume Encryption (NVE) est une technologie logicielle de chiffrement des données au repos d'un volume à la fois. Une clé de chiffrement accessible uniquement au système de stockage garantit que les

données du volume ne peuvent pas être lues si le périphérique sous-jacent est séparé du système.

Les données, y compris les copies Snapshot, et les métadonnées sont chiffrées. L'accès aux données est donné par une clé XTS-AES-256 unique, une par volume. Un gestionnaire de clés intégré sécurise les clés du même système avec vos données.

Vous pouvez utiliser NVE sur n'importe quel type d'agrégat (HDD, SSD, hybride, LUN de baie), avec n'importe quel type RAID et dans n'importe quelle implémentation ONTAP prise en charge, y compris ONTAP Select. Vous pouvez également utiliser NVE avec NetApp Storage Encryption (NSE) pour doubler le chiffrement des données sur les disques NSE.

quand utiliser des serveurs KMIP bien qu'il soit moins onéreux et généralement plus pratique pour utiliser le gestionnaire de clés intégré, vous devez configurer des serveurs KMIP si l'un des cas suivants est vrai :

- Votre solution de gestion des clés de chiffrement doit être conforme à la norme FIPS 140-2 (Federal information Processing Standards) ou OASIS KMIP.
- Vous avez besoin d'une solution à plusieurs clusters. Les serveurs KMIP prennent en charge plusieurs clusters avec une gestion centralisée des clés de chiffrement.

  Les serveurs KMIP prennent en charge plusieurs clusters avec une gestion centralisée des clés de chiffrement.

- Votre entreprise exige que les clés d'authentification soient sécurisées sur un système ou à un emplacement différent de celui des données.

  Les serveurs KMIP stockent les clés d'authentification séparément des données.

Informations associées

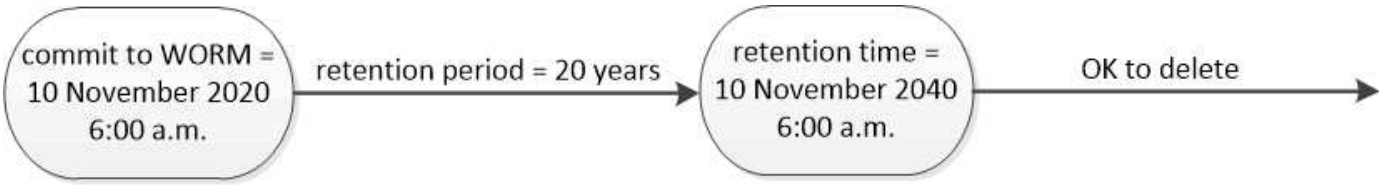
"FAQ : NetApp Volume Encryption et NetApp Aggregate Encryption"

Stockage WORM

SnapLock est une solution de conformité hautes performances pour les entreprises qui utilisent le stockage WORM (Write Once, Read Many)_ pour conserver les fichiers stratégiques sous une forme non modifiée à des fins réglementaires et de gouvernance.

Une seule licence vous donne droit à l'utilisation de SnapLock en mode strict *Compliance,* afin de répondre aux obligations externes telles que la règle SEC 17a-4 et un mode plus lâche *Enterprise* afin de respecter les réglementations internes régissant la protection des ressources numériques. SnapLock utilise un *ComplanceClock* inviolable pour déterminer quand la période de conservation d'un fichier WORM est écoulée.

Vous pouvez utiliser *SnapLock for SnapVault* pour protéger les copies Snapshot sur un stockage secondaire. Vous pouvez utiliser SnapMirror pour répliquer des fichiers WORM dans un autre emplacement géographique à des fins autres que la reprise après incident.



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