セキュリティ
ONTAP 9

NetApp
April 24, 2024

目次

セキュリティ

クライアントの認証と許可

ONTAP では、標準的な方法を使用して、クライアントや管理者によるストレージへのアクセスを保護し、ウィルスから保護します。保存データの暗号化や WORM ストレージでは、高度なテクノロジも使用できます。

ONTAP では、信頼できるソースで ID を検証してクライアントマシンおよびユーザを認証します。ONTAP は、ユーザのクレデンシャルとファイルまたはディレクトリに対して設定されている権限を比較して、ユーザにファイルまたはディレクトリへのアクセスを許可します。

認証

ローカルまたはリモートのユーザアカウントを作成できます。

- ローカルアカウントでは、アカウント情報がストレージシステムに格納されます。
- リモートアカウントでは、アカウント情報が Active Directory ドメインコントローラ、 LDAP サーバ、または NIS サーバに格納されます。

ONTAP は、ローカルまたは外部のネームサービスを使用して、ホスト名、ユーザ、グループ、ネットグループ、およびネームマッピング情報を検索します。ONTAP では、次のネームサービスをサポートしています。

- ローカルユーザ
- DNS
- 外部 NIS ドメイン
- 外部LDAPドメイン

a_name service switch table_ には、ネットワーク情報を検索するソースと、その検索順序を指定します（ UNIX システムの /etc/nsswitch.conf ファイルに相当する機能を提供します）。NAS クライアントが SVM に接続すると、 ONTAP は指定されたネームサービスをチェックして、必要な情報を取得します。

**kerberos support*Kerberos は ' クライアント / サーバ実装でユーザ・パスワードを暗号化することによって「三次認証」を提供するネットワーク認証プロトコルですONTAP では、整合性チェック機能を備えた Kerberos 5 認証（ krb5i ）とプライバシーチェック機能を備えた Kerberos 5 認証（ krb5p ）をサポートしています。

承認

ONTAP では、 3 つのレベルのセキュリティを評価して、 SVM 上にあるファイルおよびディレクトリに対して要求された処理を実行する権限がエンティティにあるかどうかを判断します。アクセスは、セキュリティレベルの評価後に有効な権限によって判断されます。

- エクスポート（ NFS ）および共有（ SMB ）セキュリティ

  指定された NFS エクスポートまたは SMB 共有へのエクスポートおよび共有セキュリティ環境クライアントアクセス管理者権限を持つユーザは、 SMB クライアントと NFS クライアントからエクスポートおよび

共有レベルのセキュリティを管理できます。

- ストレージレベルのアクセス保護のファイルおよびディレクトリセキュリティ

  ストレージレベルのアクセス保護セキュリティ環境 SVM ボリュームへの SMB および NFS クライアントアクセスNTFS のアクセス権のみがサポートされています。ONTAP で、ストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスする UNIX ユーザのセキュリティチェックを行うには、 UNIX ユーザがボリュームを所有する SVM 上の Windows ユーザにマッピングされている必要があります。

- NTFS 、 UNIX 、および NFSv4 のネイティブのファイルレベルのセキュリティ

  ストレージオブジェクトを表すファイルやディレクトリには、ネイティブのファイルレベルのセキュリティが存在します。ファイルレベルのセキュリティはクライアントから設定できます。ファイル権限は、データへのアクセスに SMB と NFS のどちらを使用するかに関係なく有効です。

SAMLによる認証

ONTAPでは、リモートユーザの認証でSecurity Assertion Markup Language（SAML）がサポートされます。いくつかの一般的なIDプロバイダ（IdP）がサポートされています。サポートされているIdPとSAML認証を有効にする手順の詳細については、を参照してください。 "SAML 認証を設定する"。

OAuth 2.0とONTAP REST APIクライアント

ONTAP 9.14以降では、Open Authorization（OAuth 2.0）フレームワークがサポートされています。クライアントがREST APIを使用してONTAPにアクセスする場合、OAuth 2.0のみを使用して認証とアクセス制御を行うことができます。ただし、この機能は、CLI、System Manager、REST APIなどの任意のONTAP管理インターフェイスを使用して設定および有効化できます。

標準のOAuth 2.0機能は、いくつかの一般的な認可サーバーとともにサポートされています。相互TLSに基づいて送信者に制限されたアクセストークンを使用することで、ONTAPのセキュリティをさらに強化できます。また、自己完結型スコープや、ONTAP RESTロールやローカルユーザ定義との統合など、さまざまな認証オプションを利用できます。を参照してください "ONTAP OAuth 2.0実装の概要" を参照してください。

管理者認証と RBAC

管理者は、ローカルまたはリモートのログインアカウントを使用してクラスタおよび SVM への認証を行います。管理者がアクセスできるコマンドは、ロールベースアクセス制御（ RBAC ）に基づいて決まります。

認証

クラスタおよび SVM の管理者アカウントは、ローカルまたはリモートのいずれかとして作成できます。

- ローカルアカウントでは、アカウント情報、公開鍵、セキュリティ証明書がストレージシステムに格納されます。
- リモートアカウントでは、アカウント情報が Active Directory ドメインコントローラ、 LDAP サーバ、または NIS サーバに格納されます。

ONTAP では、 DNS を除き、管理者アカウントの認証にクライアントの認証と同じネームサービスを使用し

ます。

RBAC

管理者がアクセスできるコマンドは、管理者に割り当てられている _role_assigned コマンドで決まります。ロールは管理者のアカウントを作成するときに割り当てます。必要に応じて、別のロールを割り当てたりカスタムロールを定義したりできます。

ウィルススキャン

ストレージシステムに統合されたウィルス対策機能を使用して、ウィルスやその他の悪意のあるプログラムからデータを保護することができます。ONTAP ウィルススキャン（ _vscan ）は、クラス最高のサードパーティ製ウィルス対策ソフトウェアと ONTAP 機能を組み合わせたもので、どのファイルをスキャンするか、いつスキャンするかを柔軟に制御できます。

スキャン処理は、サードパーティベンダーのウィルス対策ソフトウェアをホストする外部サーバで実行されます。ネットアップが提供し、外部サーバにインストールされる ONTAP Antivirus Connector は、ストレージシステムとウィルス対策ソフトウェア間の通信を処理します。

- クライアントが SMB 経由でファイルを開く、読み取る、名前を変更する、閉じるたびにウィルスチェックを行うには、 _on_access scanning_to を使用します。ファイル処理は、外部サーバからファイルのスキャンステータスがレポートされるまで中断されます。ファイルがすでにスキャンされている場合、ONTAP はファイル操作を許可します。それ以外の場合は、サーバからのスキャンを要求します。

  オンアクセススキャンは NFS ではサポートされていません。

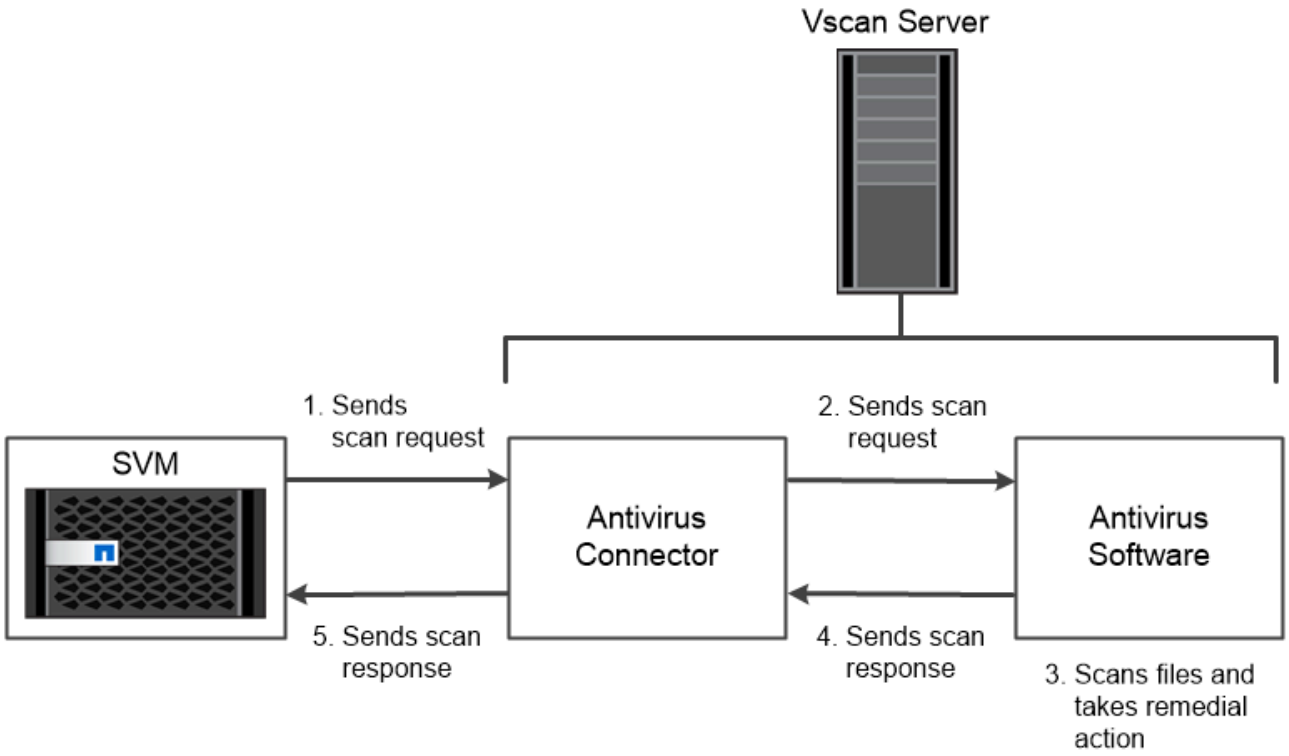
- オンデマンドスキャン _ を使用すると、ファイルのウィルスチェックをただちにまたはスケジュールに基づいて実行できます。たとえば、ピーク時を避けてスキャンを実行する場合などに便利です。外部サーバはチェックしたファイルのスキャンステータスを更新するため、 SMB 経由で次回それらのファイルがアクセスされたときには（ファイルが変更されていなければ）ファイルアクセスレイテンシが低減されます。

  オンデマンドスキャンは、 NFS 経由でのみエクスポートされたボリュームも含め、 SVM ネームスペース内のすべてのパスに対して使用できます。

通常、 SVM に対して両方のスキャンモードを有効にします。どちらのモードでも、感染したファイルにはウィルス対策ソフトウェアで設定した処理が実行されます。

*_ 災害復旧および MetroCluster 設定でのウイルススキャン _ *

ディザスタリカバリ構成と MetroCluster 構成では、ローカルクラスタとパートナークラスタのそれぞれに対して Vscan サーバを個別に設定する必要があります。



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

暗号化

ONTAP は、ストレージメディアの転用、返却、置き忘れ、盗難に際して保存データが読み取られることがないようにソフトウェアベースとハードウェアベースの暗号化テクノロジを提供します。

ONTAP は、すべての SSL 接続に対する連邦情報処理標準（ FIPS ） 140-2 に準拠しています。次の暗号化ソリューションを使用できます。

- ハードウェアソリューション：
  - NetApp Storage Encryption （ NSE ）

    NSE は、 Self-Encrypting Drive （ SED ；自己暗号化ドライブ）を使用するハードウェア解決策です。
  - NVMe SED

    ONTAP は、 FIPS 140-2 認定を取得していない NVMe SED の完全なディスク暗号化を提供します。
- ソフトウェアソリューション：
  - NetApp Aggregate Encryption （ NAE ）

    NAE は、あらゆるドライブタイプのあらゆるデータボリュームを暗号化できるソフトウェア解決策です。 NAE は、アグリゲートごとに固有のキーを使用して有効にします。

- NetApp Volume Encryption （ NVE ）

  NVE は、あらゆるドライブタイプのあらゆるデータボリュームを暗号化できるソフトウェア解決策です。ボリュームごとに一意のキーを使用して有効にします。

ソフトウェア（ NAE または NVE ）とハードウェア（ NSE または NVMe SED ）の両方の暗号化ソリューションを使用して、保存データを二重に暗号化できます。NAE または NVE 暗号化はストレージ効率に影響しません。

NetApp Storage Encryption の略

NetApp Storage Encryption （ NSE ）は、データを書き込み時に暗号化する SED をサポートします。ディスクに格納された暗号化キーがないとデータを読み取ることはできません。暗号化キーには認証されたノードからしかアクセスできません。

I/O 要求を受け取ったノードは、外部キー管理サーバまたはオンボードキーマネージャから取得した認証キーを使用して SED への認証を行います。

- 外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、 Key Management Interoperability Protocol （ KMIP ）を使用してノードに認証キーを提供します。
- オンボードキーマネージャは組み込みのツールで、データと同じストレージシステムからノードに認証キーを提供します。

NSE では、 HDD と SSD の自己暗号化ディスクをサポートしています。NetApp Volume Encryption を NSE とともに使用すると、 NSE ドライブのデータを二重に暗号化できます。

> Flash Cacheモジュールを搭載したシステムでNSEを使用する場合は、NVEまたはNAEも有効にする必要があります。NSEは、Flash Cacheモジュール上のデータを暗号化しません。

NVMe 自己暗号化ドライブ

NVMe SED には FIPS 140-2 認定はありませんが、これらのディスクでは AES 256 ビットの透過的なディスク暗号化を使用して保存データが保護されます。

認証キーの生成などのデータ暗号化処理は内部的に実行されます。認証キーは、ストレージシステムが初めてディスクにアクセスしたときに生成されます。その後、データ処理が要求されるたびにストレージシステム認証が要求されるため、保存データがディスクで保護されます。

NetApp Aggregate Encryption の略

NetApp Aggregate Encryption （ NAE ）は、アグリゲート内のすべてのデータを暗号化するためのソフトウェアベースのテクノロジです。NAE のメリットは、ボリュームがアグリゲートレベルの重複排除に含まれているのに対し、 NVE ボリュームは除外されることです。

NAE が有効になっている場合は、アグリゲートキーを使用してアグリゲート内のボリュームを暗号化できます。

ONTAP 9.7以降では、新規に作成したアグリゲートとボリュームがデフォルトで暗号化されます。 "NVEライセンス" およびオンボードまたは外部のキー管理

NetApp Volume Encryption の略

NetApp Volume Encryption （ NVE ）は、一度に 1 ボリュームずつ保管データを暗号化するためのソフトウェアベースのテクノロジです。暗号化キーにはストレージシステムからしかアクセスできないため、基盤のデバイスがシステムから分離されている場合、ボリュームのデータが読み取られることはありません。

Snapshot コピーとメタデータの両方が暗号化されます。データへのアクセスには、ボリュームごとに 1 つずつ、一意の XTS-AES-256 キーを使用します。このキーは、組み込みのオンボードキーマネージャによってデータと同じシステムに安全に保管されます。

NVE は、アグリゲートのタイプ（ HDD 、 SSD 、ハイブリッド、アレイ LUN ）や RAID タイプを問わず、サポートされるすべての ONTAP 環境（ ONTAP Select を含む）で使用できます。NVE を NetApp Storage Encryption （ NSE ）と併用して、 NSE ドライブのデータを二重に暗号化することもできます。

*_ KMIP サーバを使用するタイミング _ * オンボードキーマネージャを使用する方が安価で通常は便利ですが、次のいずれかに該当する場合は KMIP サーバをセットアップする必要があります。

- 連邦情報処理標準（ FIPS ） 140-2 または OASIS KMIP 標準に準拠した暗号化キー管理解決策が必要な場合。
- マルチクラスタ解決策が必要な場合。KMIP サーバでは、複数のクラスタの暗号化キーの一元管理がサポートされます。

  KMIP サーバでは、複数のクラスタの暗号化キーの一元管理がサポートされます。

- 認証キーをデータとは別のシステムや場所に格納してセキュリティを強化する必要がある場合。

  KMIP サーバでは、データとは別に認証キーが格納されます。

関連情報

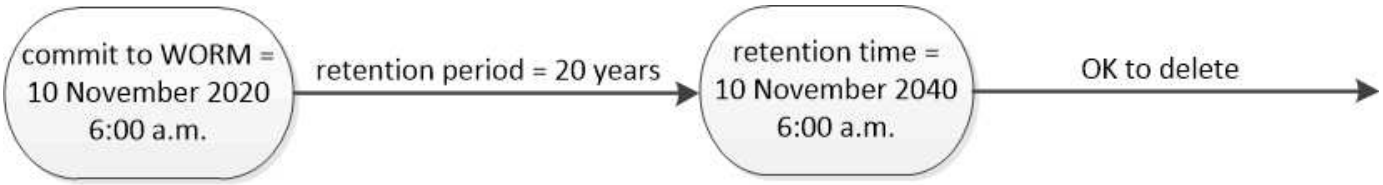
"FAQ - NetApp Volume EncryptionおよびNetApp Aggregate Encryption"

WORM ストレージ

_ 解決策 _ は、規制やガバナンスに準拠するために変更不可能な状態で重要なファイルを保管するために、 _Write Once 、 Read Many （ WORM ） _ ストレージを使用する組織向けの、ハイパフォーマンスなコンプライアンス SnapLock です。

1 つのライセンスで、 SEC Rule 17a-4 などの社外規定に準拠するための strict _ Compliance モードと、社内規定に準拠してデジタル資産を保護するためのより緩やかな _Enterprise モードで SnapLock を使用できます。SnapLock では、改ざん防止機能を備えた ComplianceClock _ を使用して、 WORM ファイルの保持期間が経過したかどうかを判断します。

SnapVault から WORM 方式でセカンダリストレージの Snapshot コピーを保護するには、 _ SnapLock for を使用します。SnapMirror を使用すると、ディザスタリカバリなどの目的で、地理的に離れた別の場所に WORM ファイルをレプリケートできます。



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