セキュリティ
ONTAP 9

NetApp
February 12, 2026

目次

セキュリティ

クライアント認証と許可

ONTAPは、クライアントと管理者のストレージへのアクセスを保護し、ウイルスから保護するために標準的な方法を使用しています。保存データの暗号化とWORMストレージには、高度なテクノロジーが利用可能です。

ONTAPは、信頼できるソースを使用してクライアントマシンとユーザーのIDを検証することで、それらを認証します。ONTAPは、ユーザーの認証情報とファイルまたはディレクトリに設定されている権限を比較することで、ユーザー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

ユーザ アカウントは、ローカルまたはリモート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、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

_ネーム サービス スイッチ テーブル_は、ネットワーク情報の検索元と検索順序を指定します（UNIXシステムの/etc/nsswitch.confファイルと同等の機能を提供します）。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 サポート Kerberos は、クライアント/サーバ実装においてユーザパスワードを暗号化することで「強力な認証」を実現するネットワーク認証プロトコルです。ONTAP は、整合性チェック機能付き Kerberos 5 認証（krb5i）とプライバシーチェック機能付き Kerberos 5 認証（krb5p）をサポートしています。

許可

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

  エクスポートおよび共有セキュリティは、特定のNFSエクスポートまたはSMB共有へのクライアント アクセスに適用されます。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は、SVMボリュームへのSMBおよびNFSクライアント アクセスに適用されます。NTFSのアクセス権のみがサポートされています。ONTAPが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は、リモート ユーザの認証にSecurity Assertion Markup Language（SAML）をサポートしています。いくつかの一般的なアイデンティティ プロバイダ（IdPs）がサポートされています。サポートされているIdPsとSAML認証を有効にする手順の詳細については、"SAML 認証の設定"を参照してください。

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。クライアントでREST APIを使用してONTAPにアクセスする場合、認証とアクセス制御には、OAuth 2.0しか使用できません。ただし、その機能を有効にするためには、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できます。

標準的なOAuth 2.0機能に加え、いくつかの一般的な認可サーバーもサポートされています。Mutual TLSに基づく送信者制約付き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、ONTAP RESTロールやローカルユーザー定義との統合など、幅広い認可オプションをご利用いただけます。詳細については、"ONTAP OAuth 2.0導入の概要"をご覧ください。

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。ロールベース アクセス制御（RBAC）によって、管理者がアクセスできるコマンドが決定されます。

認証

ローカルまたはリモートのクラスタおよび SVM 管理者アカウントを作成できます：

- ローカル アカウントとは、アカウント情報、公開キー、またはセキュリティ証明書がストレージ システム上に存在するアカウントです。
- 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。

DNS を除き、 ONTAP はクライアントの認証に使用するのと同じネーム サービスを使用して管理者アカウン

トを認証します。

RBAC

管理者に割り当てられた_ロール_によって、管理者がアクセスできるコマンドが決まります。このロールは、管理者のアカウントを作成する際に割り当てます。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することもできます。

ウイルススキャン

ストレージシステムに統合されたウイルス対策機能を使用することで、ウイルスやその他の悪意のあるコードによるデータの侵害を防ぐことができます。ONTAPウイルススキャン（*Vscan*）は、業界最高のサードパーティ製ウイルス対策ソフトウェアとONTAP機能を組み合わせることで、スキャンするファイルとそのタイミングを柔軟に制御できます。

ストレージシステムは、サードパーティベンダーのウイルス対策ソフトウェアをホストする外部サーバにスキャン処理をオフロードします。NetAppが提供し、外部サーバにインストールされる_ONTAP Antivirus Connector_が、ストレージシステムとウイルス対策ソフトウェア間の通信を処理します。

- _オンアクセススキャン_を使用すると、クライアントがSMB経由でファイルを開く、読み込む、名前を変更する、または閉じる際にウイルスチェックを行うことができます。外部サーバからファイルのスキャンステータスが報告されるまで、ファイル操作は一時停止されます。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。そうでない場合は、サーバにスキャンを要求します。

  NFS ではオンアクセス スキャンはサポートされていません。

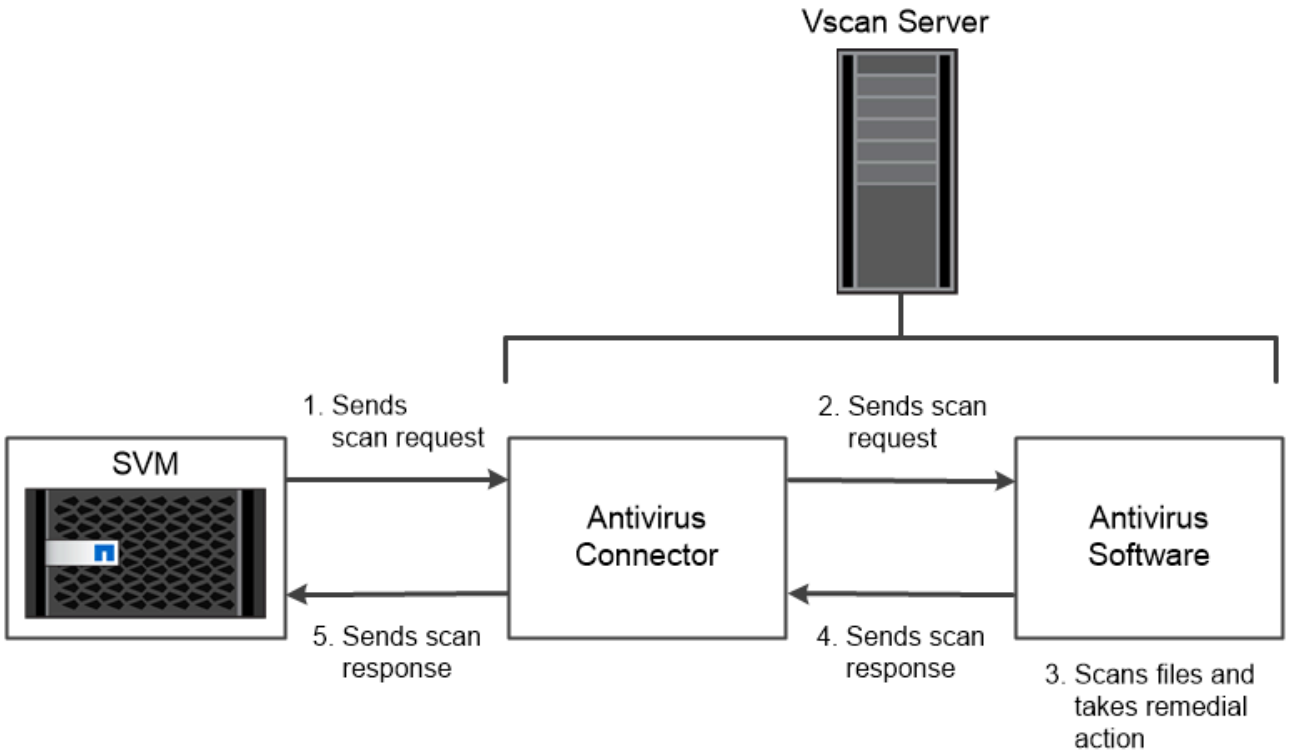
- _オンデマンドスキャン_を使用すると、ファイルのウイルスチェックを即時またはスケジュールに従って実行できます。例えば、オフピーク時にのみスキャンを実行したい場合などです。外部サーバーはチェック済みのファイルのスキャンステータスを更新するため、これらのファイル（変更されていない場合）への次回SMB経由アクセス時のファイルアクセス遅延は通常短縮されます。

  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。

一般的には、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イ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***構成におけるウイルススキャン

ディザスタ リカバリ構成および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接続について連邦情報処理標準（FIPS）140-2に準拠しています。使用可能な暗号化ソリューションは次のとおりです。

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

    NSEは、自己暗号化ドライブ（SED）を使用するハードウェア ソリューションです。
  - NVMe SED

    ONTAPでは、FIPS 140-2認定を取得していないNVMe SEDに対するフル ディスク暗号化が可能です。
- ソフトウェア ソリューション：
  - NetApp Aggregate Encryption（NAE）

    NetApp Aggregate Encryption（NAE）は、アグリゲートごとに一意のキーを使用して、あらゆるタイプのドライブのあらゆるデータ ボリュームを暗号化できるソフトウェア ソリューションです。

- NetApp Volume Encryption（NVE）

  NetApp Volume Encryption（NVE）は、ボリュームごとに一意のキーを使用して、あらゆるタイプのドライブのあらゆるデータ ボリュームを暗号化できるソフトウェア ソリューションです。

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することで、保存時の二重暗号化を実現できます。NAEまたはNVE暗号化はストレージ効率に影響を与えません。

NetApp Storage Encryption

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ず、その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とともに使用すれば、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では、Flash Cacheモジュール上のデータは暗号化されません。

NVMe自己暗号化ドライブ（SED）

NVMe SED は FIPS 140-2 認定を取得していませんが、これらのディスクは 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を保護します。

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 システムがディスクに初めてアクセスしたときに生成されます。以降、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て、ディスク上の保存データが保護されます。

NetApp Aggregate Encryption

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、ボリュームはアグリゲートレベルの重複排除の対象になりますが、NVEボリュームは除外される点です。

NAEを有効にすると、アグリゲート内のボリュームをアグリゲート キーで暗号化できるようになります。

ONTAP 9.7 以降では、"NVEライセンス"とオンボードまたは外部のキー管理がある場合、新しく作成されたアグリゲートとボリュームはデフォルトで暗号化されます。

NetApp Volume Encryption

NetApp Volume Encryption（NVE）は、一度に1ボリュームずつ保存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。

スナップショットを含むデータとメタデータは暗号化されています。データへのアクセスは、ボリュームごとに1つずつ、固有のXTS-AES-256キーによって許可されます。内蔵のOnboard Key Managerにより、これらのキーはデータと同じシステム上で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）とともに使用して、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 サーバーを使用する場合 オンボード キー マネージャーを使用する方がコストが安く、通常はより便利ですが、次のいずれかに該当する場合は KMIP サーバーを設定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ソリューションが必要な場合。
- マルチクラスタ ソリューションが必要な場合。KMIPサーバでは、複数のクラスタにわたる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、複数のクラスタにわたる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

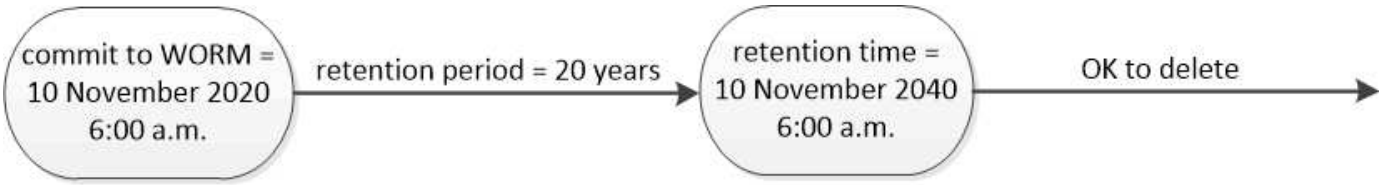
"FAQ - NetApp ボリューム暗号化とNetApp アグリゲート暗号化"

WORMストレージ

_SnapLock_は、規制やガバナンスの目的で重要なファイルを変更されていない形式で保持するために_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 コンプライアンス ソリューションです。

1つのライセンスでSnapLockを、SEC Rule 17a-4(f)などの外部規制を満たすための厳格な_コンプライアンス モード_と、デジタル資産の保護に関する内部規制を満たすためのより緩やかな_エンタープライズ モード_の両方で使用できます。SnapLockは、改ざん防止機能付きの_ComplianceClock_を使用して、WORMファイルの保存期間が経過したかどうかを判断します。

SnapLock for SnapVault を使用すると、セカンダリ ストレージ上のスナップショットを WORM 保護できます。SnapMirror を使用すると、災害復旧などの目的で、WORM ファイルを別の地理的な場所に複製できます。



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