セキュリティ
ONTAP Technical Reports

NetApp
January 23, 2026

目次

セキュリティ

ONTAPセキュリティテクニカルレポート

ONTAPは進化を続けており、セキュリティは解決策に不可欠な要素となっています。ONTAPの最新リリースには多数のセキュリティ機能が新たに追加されており、ハイブリッドクラウド全体でデータを保護し、ランサムウェア攻撃を防止し、業界の推奨プラクティスに準拠するうえで、組織にとって計り知れない価値があります。これらの新機能は、組織のゼロトラストモデルへの移行もサポートします。

これらのテクニカルレポートには、製品ドキュメントの詳細が記載され"ONTAPセキュリティとデータ暗号化"ています。

ONTAPサイバーボールト

"ONTAPサイバーボールト"NetAppのONTAPベースのサイバーボールトは、最も重要なデータ資産を保護するための包括的で柔軟なソリューションを組織に提供します。ONTAPでは、論理的なエアギャップと堅牢な強化手法を活用することで、進化するサイバー脅威に対して耐障害性に優れた、セキュアで分離されたストレージ環境を構築できます。ONTAPを使用すると、ストレージインフラの即応性と効率性を維持しながら、データの機密性、整合性、可用性を確保できます。

ランサムウェア

"TR-4572：『The NetApp 解決策for ransomware』" ランサムウェアに対応したNetAppソリューションを使用して、ランサムウェアがどのように進化したか、攻撃を特定し、拡散を防止し、できるだけ迅速にリカバリする方法をご紹介します。このドキュメントで提供されるガイダンスとソリューションは、情報システムの機密性、整合性、可用性に関する所定のセキュリティ目標を達成しながら、サイバーレジリエントなソリューションを組織に提供することを目的としています。

"TR-4526：『Compliant WORM storage using NetApp SnapLock』"
多くの企業では、コンプライアンス要件を満たすため、または単にデータ保護戦略にレイヤを追加するために、Write Once、Read Many（WORM）データストレージをある程度使用しています。ONTAPのWORM解決策であるSnapLockを、WORMデータストレージが必要な環境に統合する方法を説明します。

ゼロトラスト

"NetAppとゼロトラスト" ゼロトラストは、従来、マイクロコアと境界（MCAP）を構築してデータ、サービス、アプリケーション、資産を保護するネットワーク中心のアプローチであり、セグメンテーションゲートウェイと呼ばれる制御機能を備えていました。ONTAPは、ゼロトラストに対してデータ主体のアプローチを採用しています。このアプローチでは、ストレージ管理システムがセグメンテーションゲートウェイとなり、お客様のデータへのアクセスを保護および監視します。特に、FPolicyゼロトラストエンジンとFPolicyパートナーエコシステムは、正常なデータアクセスパターンと異常なデータアクセスパターンを詳細に把握し、内部の脅威を特定するためのコントロールセンターとなります。

多要素認証

"TR-4647：『Multifactor authentication in ONTAP best practices and Implementation guide』"
System Manager、Active IQ Unified Manager、およびONTAP Secure Shell（SSH）CLI認証を使用した管理

者アクセス用のONTAPの多要素認証機能について説明します。

"TR-4717：『ONTAP SSH authentication with a common access card』"
サードパーティのSSHクライアントをActivClientソフトウェアと組み合わせて設定し、Common Access Card（CAC;共通アクセスカード）に保存されている公開鍵を使用してONTAPストレージ管理者を認証する方法について説明します（ONTAPで設定されている場合）。

マルチテナンシー

"TR-4160：『Secure multitenancy in ONTAP』"
ONTAPでStorage VMを使用してセキュアマルチテナンシーを実装する方法と、設計上の考慮事項や推奨事項について説明します。

標準

"TR-4401：『PCI-DSS 4.0 and ONTAP』"
PCI DSS 4.0規格に照らしてシステムを検証する方法と、NetApp ONTAPシステムに適用する制御の要件を満たす方法について説明します。

属性ベースのアクセス制御

"ONTAPによる属性ベースのアクセス制御"NFSv4.2のセキュリティラベルと拡張属性（xattrs）を設定してRole-Based Access Control（RBAC；ロールベースアクセス制御）とAttribute-Based Access Control（ABAC；属性ベースアクセス制御）をサポートする方法について説明します。ABACは、ユーザ、リソース、および環境の属性に基づいて権限を定義する認証方式です。

ランサムウェア向け**NetApp**ソリューション

ランサムウェアと**NetApp**の保護ポートフォリオ

ランサムウェアは、2024年に組織のビジネス中断を引き起こす最も重大な脅威の1つです。の "Sophosランサムウェアの現状2024"調査によると、ランサムウェア攻撃は調査対象者の72%に影響を及ぼしています。ランサムウェア攻撃はより高度で標的型に進化しており、脅威アクターは人工知能などの高度な手法を採用して影響と利益を最大化しています。

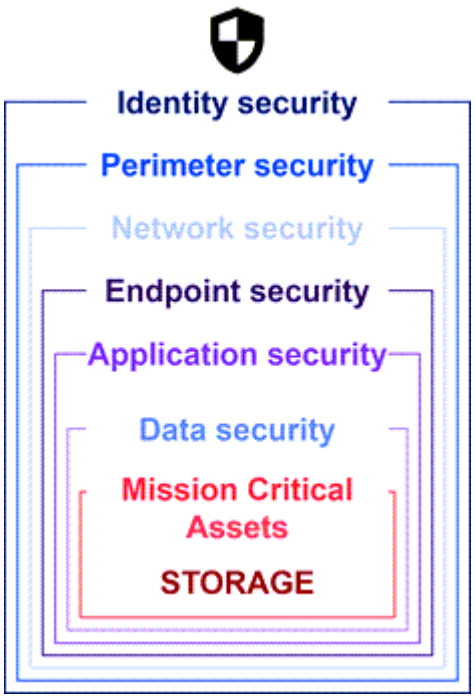
組織は、境界、ネットワーク、ID、アプリケーション、データの保存場所など、セキュリティ体制全体をストレージレベルで把握し、これらのレイヤを保護する必要があります。今日の脅威の状況では、ストレージレイヤでサイバー保護にデータ主体のアプローチを採用することが不可欠です。単一のソリューションですべての攻撃を阻止することはできませんが、パートナーシップやサードパーティなどのソリューションポートフォリオを使用することで、多層的な防御を実現できます。

にはNetApp製品ポートフォリオ、可視化、検出、修復のためのさまざまな効果的なツールが用意されており、ランサムウェアの早期発見、拡散の防止、必要に応じた迅速なリカバリを支援して、コストのかかるダウンタイムを回避できます。可視化と検出のためのサードパーティやパートナーソリューションと同様に、従来の階層型防御ソリューションは依然として普及しています。効果的な修復は、あらゆる脅威への対応において依然として重要な部分を占めています。書き換え不能なNetApp SnapshotテクノロジとSnapLockの論理的エアギャップソリューションを活用する業界独自のアプローチは、ランサムウェア対策機能における業界の差別化要因であり、業界のベストプラクティスでもあります。

2024年7月以降、以前PDFとして公開されていたテクニカルレポート『TR-4572：NetApp Ransomware Protection_』のコンテンツがdocs.netapp.comで公開されました。

データが主なターゲット

サイバー犯罪者は、データの価値を認識し、データを直接ターゲットにすることが増えています。境界、ネットワーク、およびアプリケーションのセキュリティは重要ですが、バイパスすることができます。ソースであるストレージレイヤでのデータ保護に重点を置き、重要な最終防衛線を提供します。ランサムウェア攻撃の目的は、本番環境のデータにアクセスして暗号化したりアクセス不能にしたりすることです。そのためには、攻撃者は境界からアプリケーションのセキュリティまで、今日組織によって導入されている既存の防御をすでに貫通している必要があります。



残念ながら、多くの組織はデータレイヤのセキュリティ機能を利用していません。そこで登場するのが、NetAppランサムウェア対策ポートフォリオであり、最前線でお客様を保護します。

ランサムウェアの真のコスト

身代金の支払い自体は、ビジネスへの最大の金銭的影響ではありません。支払い額はわずかではありませんが、ランサムウェアインシデントの被害によるダウンタイムコストと比べると、わずかです。

身代金の支払いは、ランサムウェア攻撃に対処する際のリカバリコストの要素の1つにすぎません。支払われた身代金を除くと、2024年の組織の報告によると、ランサムウェア攻撃からの復旧に要する平均コストは2730万ドルであり、2023年に報告された1820万ドルから100万ドル近く増加して "2024 Sophosランサムウェアの現状"います。Eコマース、株式取引、医療など、ITの可用性に大きく依存している組織の場合、コストは10倍以上になる可能性があります。

また、被保険企業がランサムウェア攻撃を受ける可能性が非常に高いことから、サイバー保険のコストも上昇し続けています。

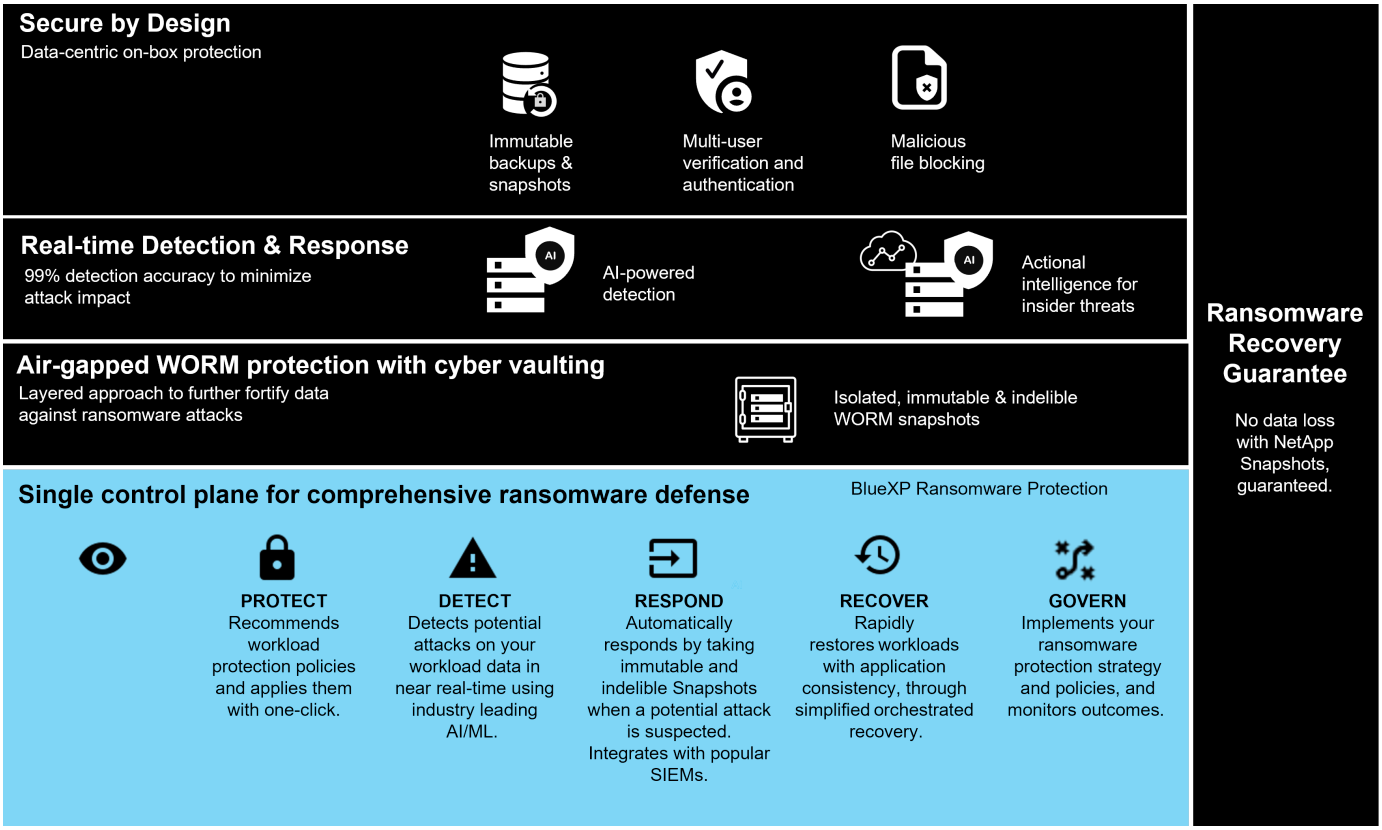
データレイヤでのランサムウェア対策

NetAppは、境界からストレージレイヤでのデータの配置場所まで、組織全体にわたってセキュリティ体制が広く深く浸透していることを認識しています。セキュリティスタックは複雑であり、テクノロジスタックのあらゆるレベルでセキュリティを提供する必要があります。

データレイヤでのリアルタイムの保護は、さらに重要であり、独自の要件があります。効果的に機能するには、この層のソリューションが次の重要な属性を提供する必要があります。

- *設計によるセキュリティ*により、攻撃が成功する可能性を最小限に抑える
- *リアルタイムの検出と対応*により、攻撃が成功した場合の影響を最小限に抑えます。
- *エアギャップによるWORM保護*重要なデータのバックアップを分離
- *単一のコントロールプレーン*による包括的なランサムウェア防御

NetAppはこれらすべてを実現し、さらに多くの機能を提供します。



NetAppのランサムウェア対策ポートフォリオ

NetAppは、"組み込みのランサムウェア対策"重要なデータに対してリアルタイムで堅牢かつ多面的な防御を提供します。その中核である、AIを活用した高度な検出アルゴリズムは、データパターンを継続的に監視し、99%の精度で潜在的なランサムウェアの脅威を迅速に特定します。攻撃に迅速に対応することで、ネットアップのストレージはデータのスナップショットを迅速に作成し、コピーを保護して迅速なリカバリを実現します。

データをさらに強化するために、NetAppの"サイバーヴォールティング"機能は論理的なエアギャップでデータを分離します。重要なデータを保護することで、迅速なビジネス継続性を確保します。

NetApp"NetAppランサムウェア保護"単一のコントロール プレーンで運用上の負担を軽減し、エンドツーエンドのワークロード中心のランサムウェア防御をインテリジェントに調整および実行します。これにより、リスクのある重要なワークロード データを 1 回のクリックで識別して保護し、潜在的な攻撃の影響を制限するために正確かつ自動的に検出して対応し、数日ではなく数分以内にワークロードを回復して、貴重なワークロード データを保護し、コストのかかる中断を最小限に抑えることができます。

データへの不正アクセスを保護するためのネイティブの組み込みONTAPソリューションとして、"マルチ管理者認証（MAV）"ボリュームの削除、管理ユーザの追加作成、Snapshotの削除などの処理を、2人目の指定管理者から承認を得た場合にのみ実行できる堅牢な機能セットを備えています。これにより、侵害された管理者や悪意のある管理者、経験の浅い管理者が望ましくない変更やデータ削除を行うのを防ぐことができます。スナップショットを削除する前に、指定された管理者承認者を必要な数だけ設定できます。

NetApp ONTAPは、Webベースの "多要素認証（MFA）"System ManagerおよびSSH CLI認証の要件に対応しています。

NetAppのランサムウェア対策は、進化し続ける脅威の状況にも安心して対応します。その包括的なアプローチは、現在のランサムウェア攻撃から防御するだけでなく、新たな脅威にも適応し、データインフラに長期的なセキュリティを提供します。

その他の保護オプションについて

- "Digital Advisorによるランサムウェア対策"
- "Data Infrastructure Insights、ストレージ、ワークロードのセキュリティ"
- "FPolicy"
- "SnapLockと改ざん防止スナップショット"

ランサムウェアからのリカバリ保証

NetAppは、ランサムウェア攻撃が発生した場合にSnapshotデータをリストアすることを保証します。当社の保証：スナップショットデータのリストアをサポートできない場合は、適切に対応します。この保証は、AFF Aシリーズ、AFF Cシリーズ、ASA、FASシステムの新規購入時に利用できます。

詳細

- "リカバリ保証サービスの説明"
- "ランサムウェア対策保証ブログ"です。

関連情報

- "NetAppサポートサイトのリソースページ"
- "NetApp製品のセキュリティ"

SnapLockと改ざん防止スナップショットでランサムウェアを保護

NetAppのスナップ兵器の重要な武器は、ランサムウェアの脅威からの保護に非常に効果的であることが証明されているSnapLockです。不正なデータ削除を防止することで、SnapLockは追加のセキュリティレイヤを提供し、悪意のある攻撃が発生した場合でも重要なデータに影響を与えずにアクセスできるようにします。

SnapLock Compliance

SnapLock Compliance（SLC）は、データを消去できない方法で保護します。SLCでは、管理者がアレイを再初期化しようとした場合でも、データの削除が禁止されています。他の競合製品とは異なり、SnapLock Complianceはそれらの製品のサポートチームを通じてソーシャルエンジニアリングのハッキングに対して脆弱ではありません。SnapLock Complianceボリュームで保護されているデータは、そのデータが有効期限に達するまでリカバリできます。

SnapLockを有効にするには"ONTAP One"、ライセンスが必要です。

詳細

- "SnapLockのドキュメント"

スナップショットの改ざん防止

改ざん防止Snapshot（TPS）コピーを使用すると、悪意のある行為からデータを簡単かつ迅速に保護できます。SnapLock Complianceとは異なり、TPSは通常、ユーザが決められた時間データを保護し、高速リカバリのためにローカルに残しておくことができるプライマリシステムや、プライマリシステムからデータをレプリケートする必要がないプライマリシステムで使用されます。TPSはSnapLockテクノロジを使用して、同じSnapLock保持期限を使用しているONTAP管理者でもプライマリSnapshotが削除されないようにします。SnapLockが有効になっていなくても、Snapshotは削除できません。ただしSnapshotには、SnapLock Complianceと同じ消去不能な性質はありません。

スナップショットの改ざんを防止するには、"ONTAP One"ライセンスが必要です。

詳細

- "Snapshotをロックしてランサムウェア攻撃から保護"です。

FPolicyファイルブロッキング

FPolicyは、エンタープライズクラスのストレージアプライアンスへの不要なファイルの保存をブロックします。FPolicyは、既知のランサムウェアファイル拡張子をブロックする方法も提供します。ユーザには引き続きホームフォルダに対するフルアクセス権限がありますが、FPolicyでは管理者がブロック済みとしてマークしたファイルを格納することはできません。これらのファイルがMP3ファイルであるか、既知のランサムウェアファイル拡張子であるかは関係ありません。

FPolicyネイティブモードで悪意のあるファイルをブロック

NetApp FPolicyのネイティブモード（ファイルポリシーという名前を発展させたもの）は、不要なファイル拡張子が環境に侵入するのをブロックできるファイル拡張子ブロックフレームワークです。10年以上にわたってONTAPの一部として提供されており、ランサムウェアからの保護に非常に役立ちます。このゼロトラストエンジンは、Access Control List（ACL;アクセスコントロールリスト）権限以外にもセキュリティ対策を追加できるため、価値があります。

ONTAP System Manager およびNetApp Consoleでは、3000 を超えるファイル拡張子のリストを参照できます。

一部の拡張機能はご使用の環境では正当なものであり、ブロックすると予期しない問題が発生する可能性があります。ネイティブFPolicyを設定する前に、環境に適した独自のリストを作成してください。

ONTAPのネイティブモードはすべてのライセンスに含まれています。

詳細

- "ブログ：ランサムウェアとの戦い：パート3—ONTAP FPolicy、もう1つの強力なネイティブ（別名フリー）ツール"

FPolicy外部モードを使用したユーザとエンティティの動作分析（**UEBA**）の有効化

FPolicy外部モードは、ファイルアクティビティとユーザアクティビティを可視化するための、ファイルアクティビティの通知および制御フレームワークです。これらの通知は、外部ソリューションでAIベースの分析を実行して悪意のある動作を検出するために使用できます。

FPolicy外部モードは、特定のアクティビティを許可する前にFPolicyサーバからの承認を待機するように設定することもできます。このような複数のポリシーを1つのクラスタに設定できるため、柔軟性に優れています。

承認を提供するように設定されている場合、FPolicyサーバはFPolicy要求に応答する必要があります。そうしないと、ストレージシステムのパフォーマンスが低下する可能性があります。

FPolicy外部モードはに含まれてい"スヘテノONTAPライセンス"ます。

詳細

- "ブログ：Fighting Ransomware: Part Four—UBA and ONTAP with FPolicy external mode"

Data Infrastructure Insights、ストレージ、ワークロードのセキュリティ

ストレージ ワークロード セキュリティ (SWS) は、 ONTAP環境のセキュリティ体制、回復性、アカウンタビリティを大幅に強化するNetApp Data Infrastructure Insightsの機能です。SWSはユーザ中心のアプローチを採用し、環境内のすべての認証済みユーザからのすべてのファイル アクティビティを追跡します。高度な分析を使用して、すべてのユーザの通常のアクセス パターンと季節的なアクセス パターンを確立します。これらのパターンは、ランサムウェア シグネチャを使用せずに疑わしい動作を迅速に特定するために使用されます。

SWS は、潜在的なランサムウェアやデータ削除を検出すると、次のような自動アクションを実行できます。

- 該当するボリュームのSnapshotを作成します。
- 悪意のあるアクティビティの疑いがあるユーザアカウントとIPアドレスをブロックします。
- 管理者にアラートを送信します。

SWSは、内部の脅威を迅速に阻止し、すべてのファイルアクティビティを追跡する自動化されたアクションを実行できるため、ランサムウェアイベントからのリカバリをはるかに簡単かつ迅速に実行できます。高度な監査ツールとフォレンジックツールが組み込まれているため、攻撃の影響を受けたボリュームやファイル、攻撃元のユーザアカウント、実行された悪意のあるアクションをすぐに確認できます。Snapshotの自動作成に

より、被害を軽減し、ファイルのリストアを高速化します。

ONTAPのAutonomous Ransomware Protection（ARP;自律型ランサムウェア対策）によるアラートもSWSに表示されるため、ARPとSWSの両方を使用してランサムウェア攻撃から保護する単一のインターフェイスが提供されます。

詳細

- "NetAppData Infrastructure Insights"

NetApp ONTAPに搭載されたAIベースの検出と応答機能

ランサムウェアの脅威がますます巧妙になるにつれ、防御メカニズムも進化していきます。NetAppの自律型ランサムウェア対策（ARP）は、ONTAPに組み込まれたインテリジェントな異常検出機能を備えたAIを基盤としています。オンにすると、サイバーレジリエンスに新たな防御レイヤを追加できます。

ARPとARP / AIは、ONTAPの組み込みの管理インターフェイスとSystem Managerを使用して設定でき、ボリューム単位で有効にできます。

自律型ランサムウェア防御（**ARP**）

ONTAP 9.10.1以降のもう1つのネイティブ組み込みONTAPソリューションである自律型ランサムウェア対策（ARP）では、NASストレージボリュームのワークロードのファイルアクティビティとデータエントロピーを調べて、潜在的なランサムウェアを自動的に検出します。ARPは、管理者にリアルタイムの検出、分析情報、データリカバリポイントを提供し、これまでにないオンボックスの潜在的なランサムウェア検出を可能にします。

ARPをサポートするONTAP 9 .15.1以前のバージョンでは、ARPは学習モードで開始され、一般的なワークロードのデータアクティビティを学習します。ほとんどの環境では、この処理に7日かかることがあります。ラーニングモードが完了すると、ARPは自動的にアクティブモードに切り替わり、ランサムウェアの可能性がある異常なワークロードアクティビティを探し始めます。

異常なアクティビティが検出された場合は、即座にSnapshotが自動作成され、感染データを最小限に抑えながら、可能な限り攻撃時点に近いリストアポイントが提供されます。同時に、管理者が異常なファイルアクティビティを確認できる自動アラート（設定可能）が生成され、アクティビティが実際に悪意のあるものかどうかを判断して適切なアクションを実行できるようになります。

アクティビティが想定されるワークロードである場合、管理者は簡単に誤検出としてマークできます。ARPはこの変更を通常のワークロードアクティビティとして学習し、今後の潜在的な攻撃としてフラグを立てなくな

ります。

ARPをイネーブルにするには"ONTAP One"、ライセンスが必要です。

詳細

- "自律型ランサムウェア対策"

自律型ランサムウェア対策 **/ AI**（**ARP / AI**）

ONTAP 9.15.1で技術プレビューとして導入されたARP / AIを使用することで、NASストレージ システムの組み込みのリアルタイム検出は次のレベルに引き上げられます。AIを活用した新しい検出テクノロジは、100万件を超えるファイルやさまざまな既知のランサムウェア攻撃についてトレーニングされています。ARPで使用される信号に加えて、ARP/AIはヘッダー暗号化も検出します。AIパワーと追加信号により、ARP/AIは99%以上の検出精度を実現します。これは、ARP/AIに最高のAAA評価を与えた独立したテストラボであるSE Labsによって検証されています。

モデルのトレーニングはクラウドで継続的に行われるため、ARP / AIはラーニングモードを必要としません。オンになった瞬間にアクティブになります。継続的なトレーニングとは、ARP / AIが発生したときに常に新しいタイプのランサムウェア攻撃に対して検証されることも意味します。ARP/AIには、自動更新機能も搭載されており、ランサムウェアの検出を最新の状態に保つために、すべてのお客様に新しいパラメータを提供します。ARPの他のすべての検出、インサイト、およびデータ復旧ポイント機能は、ARP/AI用に維持されます。

ARP/AIを有効にするには"ONTAP One"、ライセンスが必要です。

詳細

- "ブログ：NetAppのAI-based real-time ransomware detection solution achieves AAA rating"

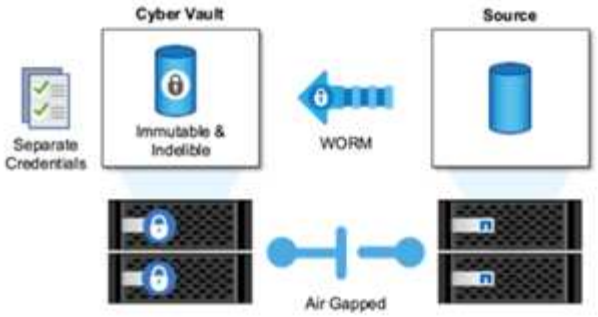
ONTAPでのサイバーヴォールティングによるエアギャップによる**WORM**保護

NetAppのサイバーボールトへのアプローチは、論理的にエアギャップを埋めるサイバーボールトのために構築されたリファレンスアーキテクチャです。このアプローチでは、SnapLockなどのセキュリティ強化テクノロジやコンプライアンステクノロジを活用して、変更や消去が不可能なSnapshotを作成できます。

SnapLock Complianceと論理的なエアギャップによるサイバーヴォールティング

攻撃者がバックアップコピーを破棄し、場合によっては暗号化する傾向が高まっています。そのため、サイバーセキュリティ業界の多くが、全体的なサイバーレジリエンス戦略の一環としてエアギャップバックアップを使用することを推奨しています。

問題は、従来のエアギャップ（テープとオフラインメディア）によってリストア時間が大幅に増加し、ダウンタイムと全体的な関連コストが増加することです。エアギャップソリューションに対するより現代的なアプローチでさえ、問題が発生する可能性があります。たとえば、新しいバックアップコピーを受信するためにバックアップヴォールトを一時的に開いてから、プライマリデータへのネットワーク接続を切断して閉じ、再び「エアギャップ」状態にすると、攻撃者はこの一時的なオープンを利用する可能性があります。接続がオンラインになっている間に、攻撃者がデータを侵害または破壊する可能性があります。このタイプの設定は、一般に不要な複雑さを追加します。論理的なエアギャップは、バックアップをオンラインに維持しながらセキュリティ保護の原則が同じであるため、従来のエアギャップや最新のエアギャップの代替として最適です。NetAppでは、変更不可のスナップショットとNetApp SnapLock Complianceを使用して、テープやディスクのエアギャップの複雑さを論理的なエアギャップで解決できます。



NetAppは、医療保険の携行性と責任に関する法律（HIPAA）、サーベンスオクスリー法、その他の規制データ規則など、データコンプライアンスの要件に対応するために、10年以上前にSnapLock機能をリリースしました。また、プライマリSnapshotをSnapLockボリュームにバックアップしてコピーをWORM状態にコミットし、削除を回避することもできます。SnapLockライセンスには、SnapLock ComplianceとSnapLock Enterpriseの2つのバージョンがあります。NetAppでは、ランサムウェア対策のためにSnapLock Complianceを推奨しています。ONTAP管理者やNetAppサポートがSnapshotをロックして削除できない特定の保持期間を設定できるためです。

詳細

- "ブログ：ONTAP cyber vault overview"

スナップショットの改ざん防止

SnapLock Complianceを論理的なエアギャップとして活用することで、攻撃者によるバックアップコピーの削除を防止できますが、SnapVaultを使用してSnapshotをセカンダリSnapLock対応ボリュームに移動する必要があります。そのため、多くのお客様がネットワーク経由でセカンダリストレージにこの構成を導入しています。これにより、プライマリストレージにプライマリボリュームのSnapshotをリストアするよりもリストア時間が長くなる可能性があります。

ONTAP 9.12.1以降では、改ざん防止スナップショットを使用して、プライマリストレージとプライマリボリュームのスナップショットをほぼSnapLock Complianceレベルで保護できます。SnapVaultを使用してSnapLockedのセカンダリボリュームにSnapshotをバックアップする必要はありません。改ざんを防止するSnapshotには、SnapLockテクノロジを使用して、ONTAPのフル管理者が同じSnapLock保持期限を使用していても、プライマリSnapshotが削除されないようにします。これにより、リストア時間が短縮され、改ざん防止されたSnapshotを使用してFlexCloneボリュームをバックアップできるようになります。これは、従来のSnapLock Complianceで保存されたSnapshotではできません。

SnapLock Compliance SnapLock Complianceスナップショットと改ざん防止スナップショットの主な違いは、保存されたスナップショットがまだ有効期限に達していない場合、SnapLock ComplianceではONTAPアレイの初期化と消去を実行できない点です。スナップショットの改ざんを防止するには、SnapLock Complianceライセンスが必要です。

詳細

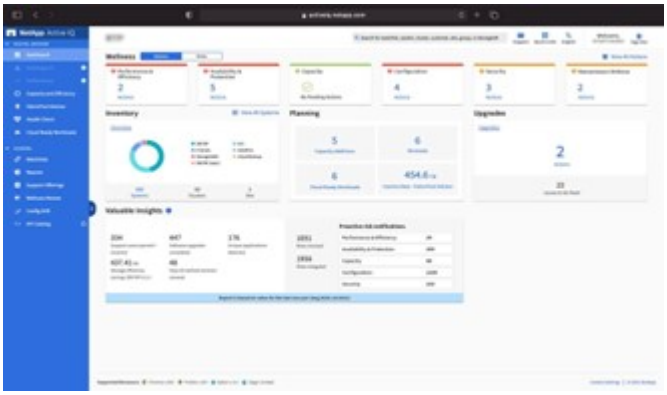
- "Snapshotをロックしてランサムウェア攻撃から保護"

Digital Advisorによるランサムウェア対策

Active IQを基盤とするDigital Advisorは、NetAppストレージのプロアクティブなケアと最適化を、実用的なインテリジェンスによって簡素化し、最適なデータ管理を実現します。多様なインストールベースから得られるテレメトリデータを活用し、高度なAIとML

技術を駆使して、リスクを軽減し、ストレージ環境のパフォーマンスと効率を向上させる機会を発見します。

だけで "NetAppデジタルアドバイザ" "セキュリティの脆弱性を排除"なく、ランサムウェアからの保護に特化した分析情報やガイダンスも提供します。専用の健全性カードに必要な対処方法と対処されたリスクが表示されるため、システムがこれらのベストプラクティスの推奨事項を満たしていることを確認できます。



[Ransomware Defense Wellness]ページで追跡されるリスクとアクションには、次のものが含まれます（その他多数）。

- ボリュームのSnapshot数が少ないため、ランサムウェアによる保護の可能性が低下しています。
- NASプロトコル用に設定されたすべてのStorage Virtual Machine（SVM）でFPolicyが有効になっているわけではありません。

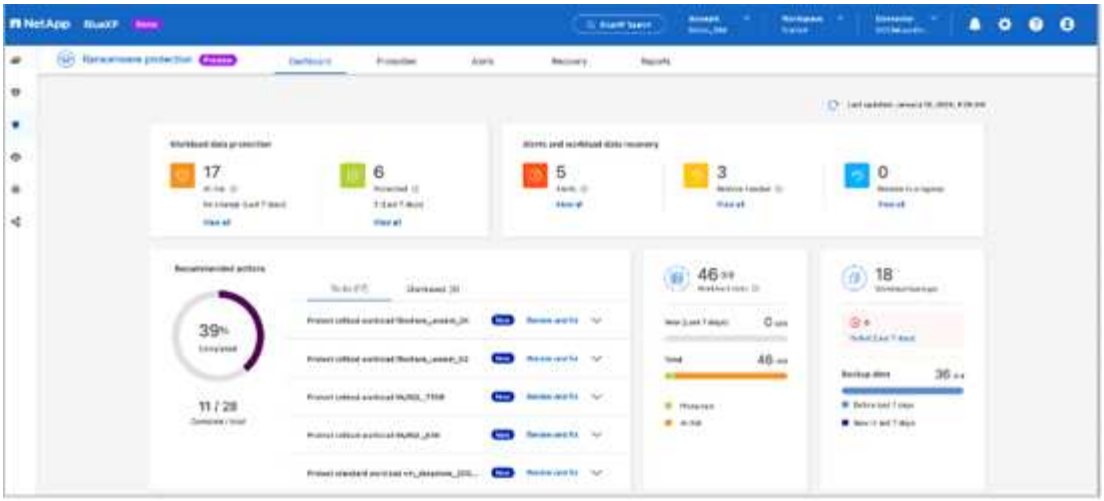
ランサムウェア対策の実際の動作については、を参照してください"Digital Advisor"。

NetAppランサムウェア保護による包括的な回復力

ランサムウェアの検出は、拡散を防ぎ、コストのかかるダウンタイムを回避できるように、できるだけ早く実施することが重要です。しかし、ランサムウェアを効果的に検出するには、複数の保護レイヤが必要です。NetApp のランサムウェア保護は、NetApp Consoleを使用したデータ サービスにまで拡張されるリアルタイムのオンボックス機能と、サイバー ボールティング用の分離された階層化ソリューションを含む包括的なアプローチを採用しています。

NetAppランサムウェア保護

NetApp Consoleは、包括的かつワークロード中心のランサムウェア防御をインテリジェントにオーケストレーションする単一のコントロール プレーンです。 NetAppランサムウェア保護は、ARP、FPolicy、改ざん防止スナップショットなどのONTAPの強力なサイバーレジリエンス機能と、 NetApp Backup and Recoveryなどのネットアップデータ サービスを組み合わせています。自動化されたワークフローによる推奨事項やガイダンスも追加されており、単一のUIでエンドツーエンドの防御を実現します。ワークロード レベルで動作し、業務を支えるアプリケーションを保護して、攻撃が発生した場合に可能なかぎり迅速にリカバリを行えるようにします。



お客様にもたらされるメリット：

- ランサムウェアへの備えを支援することで、運用上のオーバーヘッドを軽減し、効果を向上
- AI / MLを活用した異常検出により、高い精度と迅速な対応でリスクを抑制
- アプリケーションと整合性のあるガイド付きリストアにより、ワークロードを数分で簡単にリカバリできます。

"NetAppランサムウェア保護"これらの NIST 機能をより簡単に実現できます。

- アプリケーションベースの最上位のワークロードに重点を置いて、NetAppストレージ*内のデータを自動的に*検出*し、優先順位を付けます*。
- トップワークロードのデータバックアップ、不変で安全な構成、悪意のあるファイルブロッキング、さまざまなセキュリティドメインのワンクリック保護。
- 次世代の**AI**ベースの異常検出*を使用して、*ランサムウェアを*可能な限り*迅速に*正確に検出*します。
- 自動化された応答とワークフロー、およびトップ* SIEMおよびXDRソリューションとの統合*。
- シンプルな*オーケストレーションされたリカバリ*を使用してデータを迅速にリストアし、アプリケーションのアップタイムを短縮します。
- ランサムウェア対策*戦略と*ポリシー*を導入し、*成果を監視*します。

NetAppとゼロトラスト

NetAppとゼロトラスト

ゼロトラストは、従来、マイクロコアと境界（MCAP）を構築してデータ、サービス、アプリケーション、資産を保護するネットワーク中心のアプローチであり、セグメンテーションゲートウェイと呼ばれる制御機能を備えていました。NetApp ONTAPは、ゼロトラストに対してデータ主体のアプローチを採用しています。このアプローチでは、ストレージ管理システムが、お客様のデータへのアクセスを保護および監視するためのセグメンテーションゲートウェイになります。特に、FPolicyゼロトラストエンジンとFPolicyパートナーエコシステムは、正常なデータアクセスパターンと異常なデータアクセスパターンを詳細に把握し、内部の脅威を特定するためのコントロールセンターとなります。

2024年7月より、以前はPDF形式で公開されていたテクニカルレポート『TR-4829：NetApp and Zero Trust：Enabling a data-centric Zero Trust model_』のコンテンツがdocs.netapp.comで公開されました。

データは組織が所有する最も重要な資産です。2022年の調査によると、内部の脅威はデータ漏えいの18%の原因です "Verizon Data Breach Investigationsレポート"。NetApp ONTAPデータ管理ソフトウェアを使用して、業界をリードするゼロトラストコントロールをデータに導入することで、組織は警戒を強化できます。

ゼロトラストとは

ゼロトラストモデルは、Forrester ResearchのJohn Kindervagによって最初に開発されました。外部からではなく内部からのネットワークセキュリティを想定しています。 Inside-Out Zero Trustアプローチは、マイクロコアと境界（MCAP）を特定します。MCAPは、包括的な制御セットで保護するデータ、サービス、アプリケーション、資産の内部定義です。安全な外部境界の概念は廃止されています。信頼され、境界を介して正常に認証されることが許可されているエンティティは、組織を攻撃に対して脆弱にする可能性があります。内部関係者は、定義上、すでに安全な境界内にいます。従業員、請負業者、およびパートナーは内部関係者であり、組織のインフラストラクチャ内で役割を実行するための適切な制御で運用できるようにする必要があります。

ゼロトラストは、2019年9月に国防総省に約束する技術として言及されました "FY19-23 DoDのデジタル最新化戦略"。Zero Trustは、「データ漏えいを阻止するためにアーキテクチャ全体にセキュリティを組み込むサイバーセキュリティ戦略です。このデータ中心のセキュリティモデルは、信頼できるネットワーク、デバイス、ペルソナ、またはプロセスという概念を排除し、最小特権アクセスの概念の下で認証および承認ポリシーを可能にするマルチ属性ベースの信頼レベルに移行します。ゼロトラストを実装するには、既存のインフラストラクチャを使用して、よりシンプルで効率的な方法でセキュリティを実装する方法を再考する必要があります。

2020年8月、NISTは(ZTA)を発表しまし "Special Pub 800-207ゼロトラストアーキテクチャ" た。ZTAは、ネットワークセグメントではなくリソースの保護に重点を置いています。これは、ネットワークの場所がリソースのセキュリティ体制の主要なコンポーネントではなくなったためです。リソースとはデータとコンピューティングです。ZTA戦略は、エンタープライズネットワークアーキテクト向けです。ZTAでは、元のForresterの概念から新しい用語がいくつか導入されています。ポリシー決定ポイント（PDP）およびポリシー施行ポイント（PEP）と呼ばれる保護メカニズムは、Forresterセグメンテーションゲートウェイに似ています。ZTAでは、次の4つの導入モデルを導入

- デバイスエージェントまたはゲートウェイベースの展開
- Enclaveベースの導入（Forrester MCAPに似ています）
- リソースポータルベースの導入
- デバイスアプリケーションのサンドボックス化

このドキュメントの目的のために、NIST ZTAではなくForrester Researchの概念と用語を使用しています。

セキュリティリソース

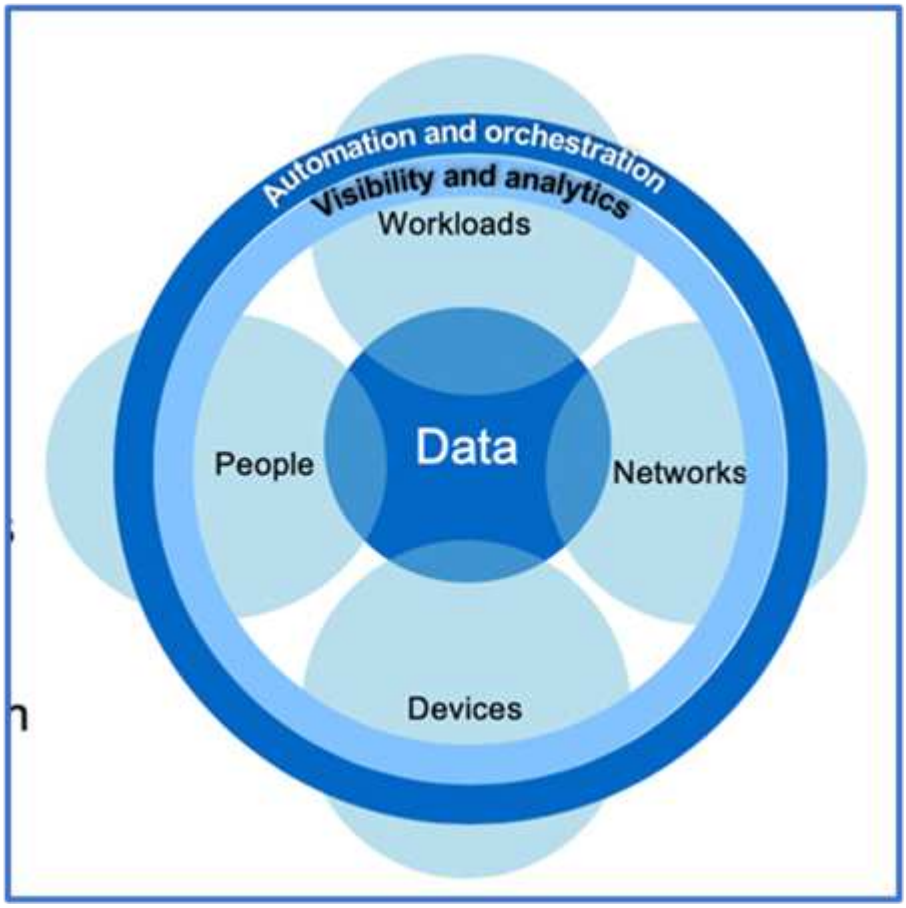
脆弱性とインシデントの報告、NetAppのセキュリティ対応、および顧客の機密性の詳細については、を参照してください "NetAppセキュリティポータル"。

ONTAPでデータ主体のアプローチでゼロトラストを実現

ゼロトラストネットワークは、データ中心のアプローチによって定義され、セキュリティ制御は可能な限りデータに近いものにする必要があります。ONTAPの機能とNetApp FPolicyパートナーエコシステムを組み合わせることで、データ中心のゼロトラストモデ

ルに必要な制御を提供できます。

ONTAPは、NetAppが提供するセキュリティリッチなデータ管理ソフトウェアです。FPolicyゼロトラストエンジンは業界をリードするONTAP機能で、きめ細かなファイルベースのイベント通知インターフェイスを提供します。NetAppのFPolicyパートナーは、このインターフェイスを使用して、ONTAP内のデータアクセスの照度を高めることができます。



ゼロトラストのデータ主体の**MCAP**を設計

データ中心のゼロトラストMCAPを設計するには、次の手順を実行します。

1. すべての組織データの場所を特定します。
2. データを分類
3. 不要になったデータを安全に破棄できます。
4. データ分類へのアクセス権を持つ役割を理解する。
5. 最小権限の原則を適用して、アクセス制御を適用します。
6. 管理アクセスとデータアクセスに多要素認証を使用します。
7. 保存中のデータと転送中のデータに暗号化を使用
8. すべてのアクセスを監視してログに記録します。
9. 不審なアクセスまたは動作を警告します。

すべての組織データの場所を特定する

ONTAPのFPolicy機能とパートナーのNetAppアライアンスパートナーエコシステムを組み合わせることで、組織のデータがどこに存在し、誰がデータにアクセスできるかを特定できます。これには、データアクセスパターンが有効かどうかを特定するユーザ行動分析が使用されます。ユーザーの行動分析の詳細については、「すべてのアクセスを監視してログに記録する」を参照してください。データがどこにあり、誰がデータにアクセスできるかを理解していない場合、ユーザー行動分析は、経験的観察から分類とポリシーを構築するためのベースラインを提供できます。

データを分類

ゼロ トラスト モデルという用語の文脈では、データ分類の過程で高リスク データを特定する必要があります。高リスク データとは、組織外への公開が意図されていない機密データのことを指します。有害なデータの開示は、規制コンプライアンスに違反し、組織の評判を損なう可能性があります。規制遵守の観点から、有害データには、 "クレジットカード業界の データ セキュリティ 標準 (PCI-DSS)" EUの個人データ "一般データ保護規則（GDPR）"、またはヘルスケアデータ "医療保険の携行性と責任に関する法律（HIPAA）"。NetAppを利用できます "NetApp Data Classification"(旧称 Cloud Data Sense) は、AI を活用したツールキットで、データを自動的にスキャン、分析、分類します。

不要になったデータを安全に廃棄

組織のデータを分類した後、一部のデータが不要になったり、組織の機能と関連性がなくなったりすることがあります。不要なデータの保持は責任であり、そのようなデータは削除する必要があります。暗号化によってデータを消去する高度なメカニズムについては、「保存データの暗号化」でのセキュアパージの説明を参照してください。

データ分類へのアクセス権が必要な役割を理解し、アクセス制御を実施するために最小権限の原則を適用する

機密データへのアクセスをマッピングし、最小権限の原則を適用すると、組織内のユーザーに、業務の遂行に必要なデータのみにアクセスできるようになります。このプロセスにはロールベースアクセス制御が含まれ("RBAC"ます）。これは、データアクセスと管理アクセスに適用されます。

ONTAPでは、Storage Virtual Machine（SVM）を使用して、ONTAPクラスタ内のテナントによる組織のデータアクセスを分割できます。RBACは、SVMへのデータアクセスと管理アクセスに適用できます。RBACはクラスタ管理レベルでも適用できます。

RBACに加えて、ONTAP（MAV）を使用して、またはなどのコマンドの承認を1人以上の管理者に要求することができます "マルチ管理者認証" `volume delete` `volume snapshot delete`。MAVを有効にすると、MAVを変更または無効にするには、MAV管理者の承認が必要になります。

スナップショットを保護するもう1つの方法は、ONTAP"Snapshotロック"です。Snapshotロックは、ボリュームSnapshotポリシーの保持期間に応じて手動または自動でSnapshotを消去できないようにするSnapLock機能です。スナップショットロックは、改ざん防止スナップショットロックとも呼ばれます。スナップショットロックの目的は、不正な管理者や信頼されていない管理者が、プライマリおよびセカンダリONTAPシステム上のスナップショットを削除するのを防ぐことです。ランサムウェアによって破損したボリュームをリストアするために、プライマリシステム上のロックされたSnapshotの迅速なリカバリを実現できます。

管理アクセスとデータアクセスに多要素認証を使用

クラスタ管理のRBACに加えて、 "多要素認証（MFA）" ONTAP Web管理アクセスおよびSecure Shell（SSH）コマンドラインアクセス用にも導入できます。管理者アクセスのためのMFAは、米国の公共機関またはPCI-DSSに従う必要がある組織の要件です。MFAを使用すると、攻撃者がユーザー名とパスワードのみを使用してアカウントを侵害することが不可能になります。MFAでは、認証に2つ以上の独立した要素が必要です。二要素認証の例としては、秘密鍵などのユーザが所有するものや、パスワードなどのユーザが知っているものが

あります。ONTAP System ManagerまたはActiveIQ Unified Managerへの管理Webアクセスは、Security Assertion Markup Language（SAML）2.0で有効になります。SSHコマンドラインアクセスでは、公開鍵とパスワードを使用したチェーン型の2要素認証が使用されます。

ONTAPのIDおよびアクセス管理機能を使用して、APIを使用してユーザおよびマシンのアクセスを制御できます。

- ユーザ：
  - *認証と承認。*SMBとNFSのNASプロトコル機能を介して提供
  - *監査。*アクセスおよびイベントのsyslog。認証ポリシーと許可ポリシーをテストするためのCIFSプロトコルの詳細な監査ログ。詳細なNASアクセスをファイルレベルできめ細かくFPolicyで監査
- デバイス：
  - *認証。*APIアクセス用の証明書ベースの認証。
  - *承認。*デフォルトまたはカスタムのRole-Based Access Control（RBAC；ロールベースアクセス制御）。
  - *監査。*実行されたすべてのアクションのsyslog。

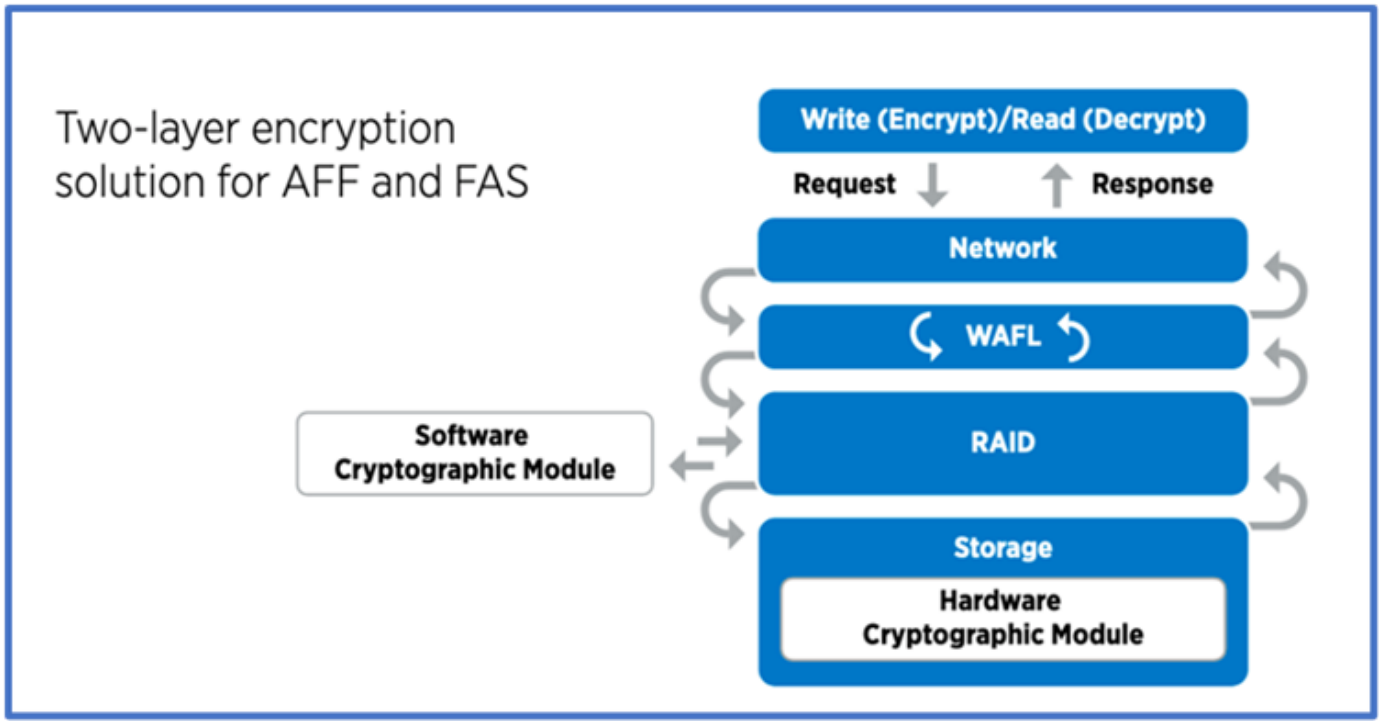
保存中のデータと転送中のデータに暗号化を使用

保存データ暗号化

組織がドライブの転用、故障したドライブの返却、大容量ドライブの販売や取り引きを行ってドライブをアップグレードする際に、ストレージシステムのリスクとインフラのギャップを軽減するための新たな要件が日々 発生しています。 ストレージエンジニアには、データの管理者や運用者として、データのライフサイクルを通じて安全にデータを管理、維持することが求められています。 "NetAppストレージ暗号化（NSE）；NetAppボリューム暗号化（NVE）；およびNetAppアグリゲート暗号化" 毒性があるかどうかにかかわらず、日常の運用に影響を与えることなく、保管中のすべてのデータを常に暗号化できます。 "NSE" は、FIPS 140-2レベル2認定自己暗号化ドライブを使用するONTAPハードウェアソリューションです "保存データ" 。 "NVE および NAE" は、を使用するONTAPソフトウェアソリューションです "保存データ" "FIPS 140-2レベル1認定NetApp暗号モジュール"。NVEおよびNAEでは、ハードドライブまたはソリッドステートドライブのいずれかを使用して保存データを暗号化できます。さらに、NSEドライブを使用して、暗号化の冗長性とセキュリティを強化するネイティブの階層型暗号化ソリューションを提供できます。1つのレイヤに違反しても、2つ目のレイヤでデータが保護されます。これらの機能により、ONTAPはに適しています "Quantum対応の暗号化"。

NVEには、機密ファイルが分類されていないボリュームに書き込まれたときに、暗号化によってデータ流出から有害なデータを削除するという機能もあります。 "セキュアパージ"

ONTAPに組み込まれているキー管理ツールであるを "オンボードキーマネージャ（ OKM ）"使用するか、 "承認済み" またはサードパーティ製品 "カイフキカンリツル" をNSEおよびNVEと併用して、キー情報をセキュアに格納できます。



上の図に示すように、ハードウェアベースとソフトウェアベースの暗号化を組み合わせることができます。この機能により、ではトップシークレットデータの保存が可能になり "分類されたプログラムのためのNSAの商用ソリューションへのONTAPの検証" ました。

転送中データの暗号化

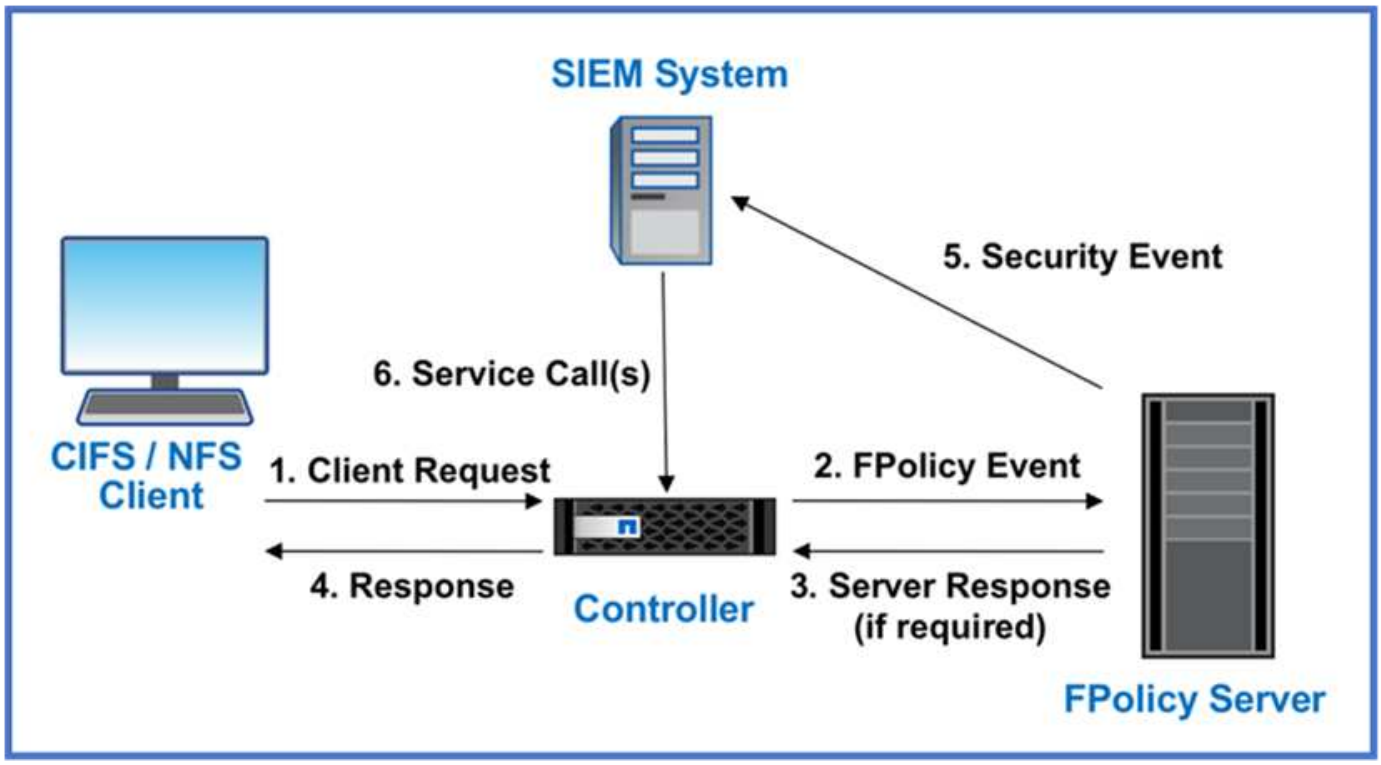
ONTAPの転送中データ暗号化により、ユーザデータアクセスとコントロールプレーンアクセスが保護されます。ユーザデータアクセスは、Microsoft CIFS共有アクセスの場合はSMB 3.0暗号化、NFS Kerberos 5の場合はkrb5pによって暗号化できます。ユーザデータアクセスは、を使用してCIFS、NFS、iSCSIの暗号化することもできます "IPSec" 。コントロールプレーンアクセスは、Transport Layer Security（TLS）で暗号化されます。ONTAPには、コントロールプレーンアクセスのコンプライアンスモードが用意されて"FIPS"います。このモードでは、FIPS承認のアルゴリズムが有効になり、FIPS承認でないアルゴリズムが無効になります。データレプリケーションはで暗号化され "クラスタピア暗号化"ます。これにより、ONTAP SnapVaultテクノロジとSnapMirrorテクノロジが暗号化されます。

すべてのアクセスを監視してログに記録

RBACポリシーを設定したら、アクティブな監視、監査、アラートを導入する必要があります。NetApp ONTAPのFPolicyゼロトラストエンジンとを組み合わせること "NetApp FPolicyパートナーエコシステム"で、データ主体のゼロトラストモデルに必要な制御を実現できます。NetApp ONTAPは、セキュリティが充実したデータ管理ソフトウェアであり "FPolicy" 、きめ細かなファイルベースのイベント通知インターフェイスを提供する、業界をリードするONTAP機能です。NetAppのFPolicyパートナーは、このインターフェイスを使用して、ONTAP内のデータアクセスの照度を高めることができます。ONTAPのFPolicy機能とFPolicyパートナーのNetAppアライアンスパートナーエコシステムを組み合わせることで、組織のデータがどこに存在し、誰がデータにアクセスできるかを特定できます。これには、データアクセスパターンが有効かどうかを特定するユーザ行動分析が使用されます。ユーザの行動分析を使用すると、通常のパターンから外れた不審なデータアクセスや異常なデータアクセスをアラートで通知し、必要に応じてアクセスを拒否するアクションを実行できます。

FPolicyパートナーは、ユーザ行動分析にとどまらず、機械学習（ML）や人工知能（AI）に移行しつつあります。これにより、イベントの忠実度が向上し、誤検出があった場合にはそれを減らすことができます。すべてのイベントは、syslogサーバ、またはMLやAIを使用できるセキュリティ情報イベント管理（SIEM）システム

に記録する必要があります。



NetAppの "DII ストレージ ワークロード セキュリティ"クラウドとオンプレミスの両方のONTAPストレージ システムで FPolicy インターフェイスとユーザー行動分析を利用して、悪意のあるユーザー行動に関するリアルタイムのアラートを提供します。また、高度な機械学習と異常検出機能により、悪意のあるユーザやセキュリティ侵害を受けたユーザが組織のデータを不正利用できないよう保護します。ストレージ ワークロード セキュリティは、ランサムウェア攻撃やその他の不正行為を識別し、スナップショットを呼び出して悪意のあるユーザーを隔離できます。また、フォレンジック機能により、ユーザとエンティティのアクティビティを詳細に把握できます。ストレージ ワークロード セキュリティは、 NetApp Data Infrastructure Insightsの一部です。

ONTAPには、ストレージワークロードのセキュリティに加えて、（ARP）と呼ばれるランサムウェア検出機能が搭載され "自律型ランサムウェア対策" ています。ARPは機械学習を使用して、ランサムウェア攻撃が進行中であることを示す異常なファイルアクティビティがないかどうかを判断し、スナップショットを呼び出して管理者にアラートを送信します。Storage Workload Securityは、ONTAPと統合してARPイベントを受信し、追加の分析機能と自動応答レイヤを提供します。

この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

ONTAPの外部にあるNetAppセキュリティの自動化とオーケストレーションの制御

自動化を使用すると、最小限の人間の支援でプロセスや手順を実行できます。自動化により、組織はゼロトラスト環境を手動の手順をはるかに超えて拡張し、自動化された不正なアクティビティから保護できます。

Ansibleは、オープンソースのソフトウェアプロビジョニング、構成管理、アプリケーション導入ツールです。多くのUnixライクなシステムで動作し、Microsoft Windowsと同様にUnixライクなシステムの両方を構成することができる。システム構成を記述するための独自の宣言言語が含まれています。AnsibleはMichael DeHaanによって書かれ、2015年にRed Hatに買収された。Ansibleはエージェントレスで、SSHまたはWindowsリモート管理（リモートPowerShell実行可能）を使用して一時的にリモート接続し、タスクを実

行します。NetAppはさらに多くの製品を開発し "ONTAPソフトウェア向け150個のAnsibleモジュール" 、Ansible自動化フレームワークとのさらなる統合を可能にしています。NetApp向けのAnsibleモジュールは、必要な状態を定義してターゲットのNetApp環境にリレーする方法に関する一連の指示を提供します。モジュールは、ライセンスのセットアップ、アグリゲートとStorage Virtual Machineの作成、ボリュームの作成、Snapshotのリストアなどのタスクをサポートするように構築されています。Ansibleのロールは "GitHubで公開" 、NetApp DoD Unified Capabilities（UC）Deployment Guideに固有のものです。

利用可能なモジュールのライブラリを使用することで、Ansibleプレイブックを簡単に開発し、独自のアプリケーションやビジネスニーズに合わせてカスタマイズして、日常的なタスクを自動化できます。作成したプレイブックを実行して指定したタスクを実行することで、時間を節約し、生産性を向上させることができます。NetAppでは、サンプルのプレイブックを作成して共有しています。プレイブックは直接使用することも、ニーズに合わせてカスタマイズすることもできます。

Data Infrastructure Insightsは、インフラストラクチャ全体の可視性を提供するインフラストラクチャ監視ツールです。 Data Infrastructure Insightsを使用すると、パブリック クラウド インスタンスやプライベート データ センターを含むすべてのリソースを監視、トラブルシューティング、最適化できます。 Data Infrastructure Insights を使用すると、平均解決時間を 90% 短縮し、クラウドの問題の 80% がエンド ユーザーに影響を与えるのを防ぐことができます。クラウド インフラのコストを平均で33%削減可能なほか、実用的なインテリジェンスによりデータを保護し、内部の脅威に対するリスクも軽減できます。 Data Infrastructure Insightsのストレージ ワークロード セキュリティ機能により、AI と ML を使用したユーザー行動分析が可能になり、内部脅威によって異常なユーザー行動が発生したときに警告を発することができます。ONTAPの場合、Storage Workload SecurityではゼロトラストFPolicyエンジンを使用します。

ゼロトラストとハイブリッドクラウド環境

NetAppは、ハイブリッド クラウドのデータに関するオーソリティです。NetAppは、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud、その他の主要なクラウド プロバイダーを使用して、オンプレミスのデータ管理システムをハイブリッド クラウドに拡張するためのさまざまなオプションを提供しています。NetAppのハイブリッド クラウド ソリューションは、オンプレミスのONTAPシステムおよびONTAP Select Software-Defined Storageで採用されているものと同じゼロ トラスト セキュリティ対策に対応しています。

AWS (FSxN)、Google Cloud (GCNV)、および Microsoft Azure 向けAzure NetApp Files向けのエンタープライズ クラスのクラウドネイティブ ファイル サービスを使用することで、一般的な CAPEX 制約なしにパブリック クラウドの容量を簡単に拡張できます。これらは分析やDevOpsなど、データを大量に使用するワークロードに最適なクラウド データ サービスであり、NetAppの柔軟性のあるオンデマンド ストレージ サービスと、ONTAPデータ管理機能をフルマネージド形式で組み合わせて利用できます。

ONTAP は、 NetApp SnapMirrorデータ レプリケーション ソフトウェアを使用して、オンプレミスのONTAPシステムと AWS、Google Cloud、または Azure ストレージ環境間でデータを移動できるようにします。

属性ベースのアクセス制御

ONTAPによる属性ベースのアクセス制御

9.12.1以降では、NFSv4.2セキュリティラベルおよび拡張属性（xattrs）を使用してONTAPを設定し、属性および属性ベースアクセス制御（ABAC）を使用したロールベースアクセス制御（RBAC）をサポートできます。

ABACは、ユーザ属性、リソース属性、および環境条件に基づいて権限を定義する認可戦略です。ONTAPとNFS v4.2セキュリティラベルおよびxattrsの統合は、NIST Special Publication 800-162に規定されているABACソリューションのNIST標準に準拠しています。

NFS v4.2セキュリティラベルとxattrsを使用して、ファイルにユーザ定義の属性とラベルを割り当てることができます。ONTAPは、ABAC指向のIDおよびアクセス管理ソフトウェアと統合して、これらの属性とラベルに基づいてきめ細かなファイルおよびフォルダのアクセス制御ポリシーを適用できます。

関連情報

- "ONTAPを使用したABACへのアプローチ"
- "NetApp ONTAPのNFS：ベストプラクティスおよび実装ガイド"

ONTAPでの属性ベースアクセス制御（ABAC）のアプローチ

ONTAPには、NFS v4.2セキュリティラベルやNFSを使用した拡張属性（xattrs）など、ファイルレベルの属性ベースアクセス制御（ABAC）を実現するために使用できるいくつかのアプローチが用意されています。

NFS v4.2セキュリティラベル

ONTAP 9.9.1以降では、NFS v4.2の「ラベル付きNFS」機能がサポートされます。

NFS v4.2セキュリティラベルは、SELinuxラベルとMandatory Access Control（MAC；強制アクセス制御）を使用して、ファイルやフォルダへのきめ細かなアクセスを管理する方法です。これらのMACラベルはファイルとフォルダに格納され、UNIX権限およびNFS v4.x ACLと連携して機能します。

NFS v4.2セキュリティラベルがサポートされたことで、ONTAPはNFSクライアントのSELinuxラベル設定を認識して認識できるようになりました。NFS v4.2セキュリティラベルはRFC-7204で規定されています。

NFS v4.2セキュリティラベルのユースケースには、次のようなものがあります。

- 仮想マシン（VM）イメージのMACラベル付け
- 公共機関のデータセキュリティ分類（シークレット、トップシークレット、その他の分類）
- セキュリティコンプライアンス
- ディスクレス Linux

NFS v4.2セキュリティラベルを有効にする

NFS v4.2セキュリティラベルを有効または無効にするには、次のコマンドを使用します（advanced権限が必要）。

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

の詳細については `vserver nfs modify`、を"ONTAPコマンド リファレンス"参照してください。

NFS v4.2セキュリティラベルの適用モード

ONTAP 9.9.1以降では、ONTAPで次の強制モードがサポートされています。

- 制限付きサーバーモード：ONTAPはラベルを強制できませんが、ラベルを保存および送信できます。

  MACラベルを変更する機能は、強制するクライアントによって異なります。

- ゲストモード：クライアントにNFS対応（v4.1以前）のラベルが付けられていない場合、MACラベルは送信されません。

  ONTAPは現在、フルモード（MACラベルの保存と適用）をサポートしていません。

NFS v4.2セキュリティラベルの例

次の設定例は、Red Hat Enterprise Linuxリリース9.3（Plow）を使用した概念を示しています。

このユーザ `jrsmith`は、John R. Smithのクレデンシャルに基づいて作成され、次のアカウントPrivilegesを持ちます。

- ユーザ名= `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

ロールには2つあります。管理者アカウントは、次のMLS Privilegesの表で説明されているように、特権ユーザおよびユーザ `jrsmith`です。

ユーザ	ロール	タイプ	レベル
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

この例の環境では、ユーザー `jrsmith`はに `s3`あるレベルのファイルにアクセスできます `s0`。以下に概説する既存のセキュリティ分類を強化して、管理者がユーザー固有のデータにアクセスできないようにすることができます。

- S0 =権限管理者ユーザデータ
- S0 =未分類データ
- S1 =社外秘
- S2 =シークレットデータ
- S3 =トップシークレットデータ

MCSヲシヨウシタNFS v4.2セキュリティラベルノレイ

マルチレベルセキュリティ（MLS）に加えて、マルチカテゴリセキュリティ（MCS）と呼ばれる別の機能を使用すると、プロジェクトなどのカテゴリを定義できます。

NFSセキュリティラベル	値
entitySecurityMark	t:s01 = UNCLASSIFIED

拡張属性（**xattrs**）

ONTAP 9.12.1以降では、ONTAPはxattrs.xattrsをサポートしています。xattrsを使用すると、アクセス制御リスト(ACL)やユーザ定義属性など、システムによって提供されるもの以外のファイルやディレクトリにメタデータを関連付けることができます。

xattrsを実装するには、Linuxでと `getfattr`コマンドラインユーティリティを使用できます `setfattr`。これらのツールを使用すると、ファイルやディレクトリの追加メタデータを強力に管理できます。不適切な使用は予期しない動作やセキュリティ上の問題につながる可能性があるため、注意して使用する必要があります。使用方法の詳細については、および `getfattr`のマニュアルページを参照するか、信頼性の高いその他のドキュメントを参照して `setfattr`ください。

ONTAPファイルシステムでxattrsが有効になっている場合'ユーザーはファイルの任意の属性を設定'変更'取得できますこれらの属性は、アクセス制御情報など、標準のファイル属性セットではキャプチャされないファイルに関する追加情報を格納するために使用できます。

ONTAPでxattrsを使用するには、いくつかの要件と制限があります。

- Red Hat Enterprise Linux 8.4以降
- Ubuntu 22.04以降
- 各ファイルには最大128個のxattrsを含めることができます。
- xattrキーは255バイトに制限されています
- キーまたは値の合計サイズは'xattrごとに1,729バイトです
- ディレクトリとファイルはxattrsを持つことができる
- xattrsを設定および取得するには、ユーザおよびグループに対して書き込みモードビットが有効になっている必要があります。 `w`

Xattrsはユーザーネームスペース内で使用され、ONTAP自体に本質的な意味を持たない。代わりに、それらの実用的なアプリケーションは、ファイルシステムとやり取りするクライアント側のアプリケーションによって排他的に決定され、管理されます。

xattrの使用例：

- ファイルの作成を担当するアプリケーションの名前の記録
- ファイルの取得元の電子メールメッセージへの参照の維持
- ファイルオブジェクトを整理するための分類フレームワークの確立
- 元のダウンロード元のURLを使用したファイルのラベル付け

xattrsの管理用コマンド

- `setfattr`ファイルまたはディレクトリの拡張属性を設定します。

```
setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
```

コマンド例：

```
setfattr -n user.comment -v test example.txt
```

- `getfattr`特定の拡張属性の値を取得するか、ファイルまたはディレクトリのすべての拡張属性を一覧表示します。

  特定の属性：
  `getfattr -n <attribute_name> <file or directory name>`

  すべての属性：
  `getfattr <file or directory name>`

  コマンド例：

```
getfattr -n user.comment example.txt
```

xattrキーと値のペアの例

次の表に、2つのxattrキー値ペアの例を示します。

xattr	値
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

xattrsのACEを使用したユーザー権限

Access Control Entry（ACE；アクセス制御エントリ）は、ファイルやディレクトリなどの特定のリソースに対して個 々 のユーザまたはユーザグループに付与されるアクセス権または権限を定義するACL内のコンポーネントです。各ACEは、許可または拒否されるアクセスのタイプを指定し、特定のセキュリティプリンシパル（ユーザまたはグループのID）に関連付けます。

xattrsに必要なアクセス制御エントリ（ACE）

- Retrieve xattr：ユーザがファイルまたはディレクトリの拡張属性を読み取るために必要な権限。「R」は、読み取り権限が必要であることを示します。
- set xattrs：拡張属性を変更または設定するために必要な権限。"A"、"w"、"T"は、append、write、xattrsに関連する特定のパーミッションなど、パーミッションの異なる例を表しています。
- ファイル:拡張属性を設定するには、追加、書き込み、およびxattrsに関連する特別な権限が必要です。
- ディレクトリ:拡張属性を設定するには、特定の権限「T」が必要です。

ファイルタイプ	**xattr**の取得	**xattrs**の設定
ファイル	R	A、w、T
ディレクトリ	R	T

ABAC IDおよびアクセス制御ソフトウェアとの統合

ABACの機能を最大限に活用するために、ONTAPはABAC指向のIDおよびアクセス管理ソフトウェアと統合できます。

ABACシステムでは、Policy Enforcement Point (PEP)とPolicy Decision Point (PDP)が重要な役割を果たす。PEPはアクセス制御ポリシーの適用を担当し、PDPはポリシーに基づいてアクセスを許可するか拒否するかを決定します。

実際的な設定では、NFSセキュリティラベルとxattrsを組み合わせて使用します。これらは、分類、セキュリティ、アプリケーション、コンテンツなど、さまざまなメタデータを表すために使用されます。これらはすべてABACの決定を行うのに役立ちます。xattrsは、PDPが意思決定プロセスに使用するリソース属性を格納するために使用できます。属性は、ファイルの分類レベルを表すように定義できます（「未分類」、「機密」、「シークレット」、「トップシークレット」など）。その後、PDPはこの属性を使用して、ユーザーがクリアランスレベル以下の分類レベルを持つファイルのみにアクセスするように制限するポリシーを適用できます。

> このコンテンツでは、お客様のID、認証、およびアクセスサービスに、ファイルシステムへのアクセスの仲介者として機能するPEPおよびPDPが少なくとも1つ含まれていることを前提としています。

ABACのプロセスフローの例

1. ユーザは、PEPへのシステムアクセスにクレデンシャル（PKI、OAuth、SAMLなど）を提示し、PDPから結果を取得します。

   PEPの役割は、ユーザのアクセス要求を代行受信してPDPに転送することです。

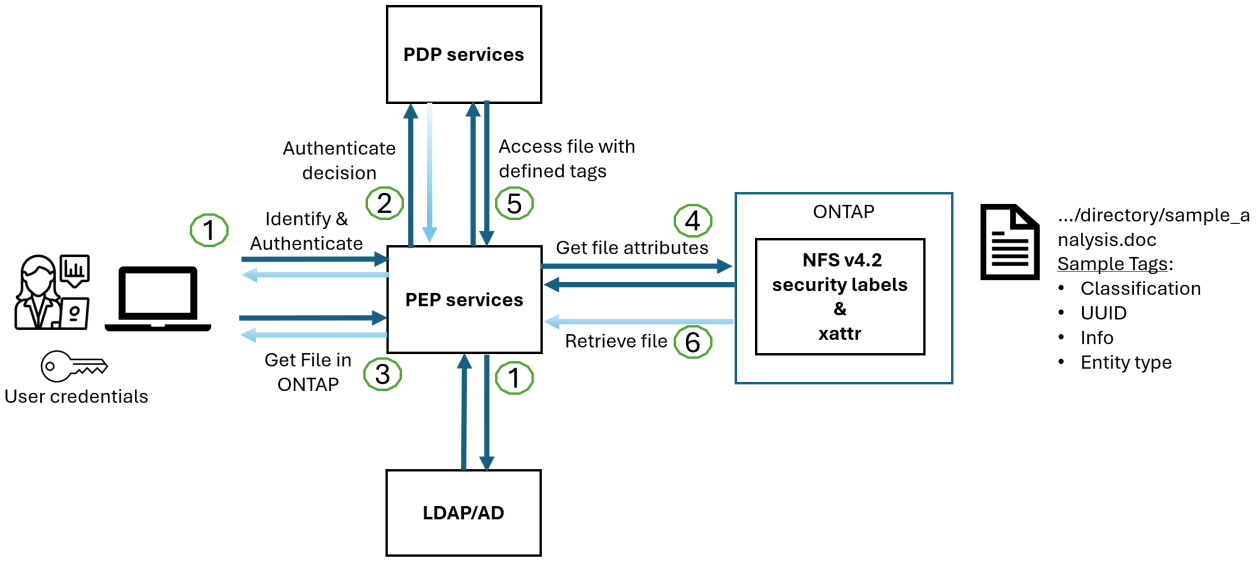
2. PDPは、確立されたABACポリシーに照らしてこの要求を評価します。

   これらのポリシーでは、ユーザー、問題のリソース、および周囲の環境に関連するさまざまな属性が考慮されます。これらのポリシーに基づいて、PDPはアクセスを許可するか拒否するかを決定し、その決定をPEPに伝えます。

   PDPはPEPにポリシーを提供して実施します。PEPはこの決定を実行し、PDPの決定に従ってユーザーのアクセス要求を許可または拒否します。

3. 要求が成功すると、ユーザはONTAPに格納されているファイル（AFF、AFF -Cなど）を要求します。
4. 要求が成功すると、PEPはドキュメントから詳細なアクセス制御タグを取得します。
5. PEPは、そのユーザの証明書に基づいてユーザのポリシーを要求します。
6. ユーザがファイルにアクセスできる場合、PEPはポリシーとタグに基づいて決定を行い、ユーザがファイルを取得できるようにします。

> 実際のアクセスはトークンを使用して行われる場合があります。



ONTAPクローニングと**SnapMirror**

ONTAPのクローニングおよびSnapMirrorテクノロジは、効率的で信頼性の高いデータレプリケーションおよびクローニング機能を提供するように設計されています。xattrsは、ファイルに関連付けられた追加のメタデータ（セキュリティラベル、アクセス制御情報、ユーザ定義データなど）を保存するため、ファイルのコンテキストと整合性の維持に不可欠です。xattrsは重要です。

ONTAPのFlexCloneテクノロジを使用してボリュームをクローニングすると、ボリュームの完全な書き込み可能なレプリカが作成されます。このクローニングプロセスは瞬時に実行されるスペース効率に優れており、すべてのファイルデータとメタデータが含まれているため、xattrsを完全にレプリケートできます。同様に、SnapMirrorでは、データが完全に忠実にセカンダリシステムにミラーリングされます。これにはxattrsも含まれます。xattrsは、このメタデータに依存するアプリケーションが正しく機能するために非常に重要です。

NetApp ONTAPでは、クローニング処理とレプリケーション処理の両方にxattrsを含めることで、プライマリストレージシステムとセカンダリストレージシステム全体で、すべての特性を含む完全なデータセットを使用して一貫性を確保します。この包括的なデータ管理アプローチは、一貫したデータ保護、迅速なリカバリ、コンプライアンスと規制基準への準拠を必要とする組織にとって不可欠です。また、オンプレミスでもクラウドでも、さまざまな環境にわたってデータの管理が簡易化されるため、ユーザはプロセス中もデータが完全で変更されていないという安心感を得ることができます。

NFS v4.2セキュリティラベルには、に定義された注意事項NFS v4.2セキュリティラベルがあります。

ラベルに対する変更の監査

xattrsまたはNFSセキュリティラベルに対する変更の監査は、ファイルシステムの管理とセキュリティの重要な側面です。標準のファイルシステム監査ツールを使用すると、xattrsやセキュリティラベルの変更など、ファイルシステムに対するすべての変更を監視およびロギングできます。

Linux環境では、 `auditd`ファイルシステムイベントの監査を確立するために一般にデーモンが使用されます。管理者は、`xattr`の変更（、 `lsetxattr`など）に関連する特定のシステムコールを監視し、 `fsetxattr`属性と、 `lremovexattr`fremovexattr`の設定、および`removexattr`属性の削除を監視するルールを設定でき`setxattr`ます。

ONTAP FPolicyは、ファイル操作をリアルタイムで監視および制御するための堅牢なフレームワークを提供することで、これらの機能を拡張します。FPolicyは、さまざまな属性xattrイベントをサポートするように設定できます。これにより、ファイル操作をきめ細かく制御したり、包括的なデータ管理ポリシーを適用したりできます。

xattrsを使用するユーザ、特にNFS v3およびNFS v4環境では、監視対象としてサポートされるファイル操作とフィルタの特定の組み合わせのみが対象となります。FPolicyによるNFS v3およびNFS v4のファイルアクセスイベントの監視でサポートされるファイル操作とフィルタの組み合わせを次に示します。

サポートされているファイル操作	サポートされているフィルタ
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

属性設定操作の**auditd**ログスニペットの例：

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

ユーザがxattrsを使用できるようにする"ONTAP FPolicy"と、ファイルシステムの整合性とセキュリティを維持するために不可欠な可視性と制御のレイヤが提供されます。FPolicyの高度な監視機能を活用することで、組織はxattrsに対するすべての変更を追跡、監査し、セキュリティおよびコンプライアンス基準に準拠させることができます。ファイルシステム管理に対するこのプロアクティブなアプローチが、データガバナンスと保護戦略を強化したいと考えている組織にとって、ONTAP FPolicyを有効にすることが強く推奨される理由です。

データアクセスの制御例

John R. SmithのPKI証明書に格納されているデータの次のエントリ例は、NetAppのアプローチをファイルに適用し、きめ細かなアクセス制御を提供する方法を示しています。

> これらの例は説明を目的としたものであり、NFS v4.2セキュリティラベルおよびxattrsに関連付けられているメタデータはお客様の責任で確認してください。わかりやすいように更新とラベルの保持の詳細は省略しています。

- PKI証明書値の例*

キー	値
entitySecurityMark	T：S01 =未分類

情報	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

仕様	"DoD"
UUID	b4111349-7875-4115-AD30-0928565f2e15

管理組織	{
	"value": "DoD"
	}

キー	値

ブリーフィング	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

市民権ステータス	{
	"value": "US"
	}

クリアランス	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

加盟国	[
	{
	"value": "USA"
	}
	]

キー	値

デジタル識別子	<pre>{
	  "classification": "UNCLASSIFIED",
	  "value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}</pre>

転送先	<pre>{
	  "value": "DoD"
	}</pre>

DutyOrganization	<pre>{
	  "value": "DoD"
	}</pre>

エンティティタイプ	<pre>{
	  "value": "GOV"
	}</pre>

FineAccessControls	<pre>[
	  {
	  "value": "SI"
	  },
	  {
	  "value": "TK"
	  },
	  {
	  "value": "NSYS"
	  }
	]</pre>

これらのPKIエンタイトルメントには、データ型やアトリビューションによるアクセスなど、John R. Smithのアクセスの詳細が表示されます。

IC-TDFメタデータがファイルとは別に格納されているシナリオでは、NetAppは詳細なアクセス制御レイヤを追加することを推奨しています。これには、アクセス制御情報がディレクトリレベルおよび各ファイルに関連付けられて格納されることが含まれます。例として、次のタグがファイルにリンクされているとします。

- NFS v4.2セキュリティラベル：セキュリティの決定に使用
- xattrs：ファイルおよび組織のプログラム要件に関連する補足情報を提供します。

次のキーと値のペアは、xattrsとして保存できるメタデータの例であり、ファイルの作成者と関連するセキュリティ分類に関する詳細情報を提供します。クライアントアプリケーションでこのメタデータを使用すると、十分な情報に基づいてアクセスに関する意思決定を行い、組織の標準や要件に従ってファイルを整理できます。

- xattrキーと値のペアの例*

キー	値
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

キー	値

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

キー	値
user.geo_point	[-78.7941, 35.7956]

```
    }
  }
```

関連情報

- "NetApp ONTAPのNFS：ベストプラクティスおよび実装ガイド"
- "ONTAPコマンド リファレンス"
- コメント要求（RFC）
  - "RFC 7204:ラベル付きNFSの要件"
  - "RFC 2203：RPCSEC_GSS Protocol Specification"
  - "RFC 3530：Network File System (NFS) Version 4 Protocol"

著作権に関する情報

商標に関する情報