テクニカル レポート

NetAppとZero Trust
データ主体のゼロトラストモデルの実現

NetApp
Dan Tulledge
2023年3月| TR-4829

概要

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となります。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。

目次

図一覧

はじめに

従来のモデルは、信頼して検証することです。これからの新しいモデルは「検証し、信頼しない」というアプローチを取ります。

データは組織が所有する最も重要な資産です。2022年の Verizon Data Breach Investigations Reportによると、内部の脅威はデータ漏えいの18%の原因です。たとえば、内部関係者のチェルシー（旧ブラッドリー）マニングとエドワード・スノーデンは機密データを漏らしましたが、業務を遂行するためにそのデータにアクセスする必要はありませんでした。では、誰が信頼されるべきなのでしょうか。誰もいない組織は、DEFCON 1への警戒を強化する必要がありますが、どうすればよいでしょうか。NetApp ONTAPデータ管理ソフトウェアを使用して、データに関する業界をリードするゼロトラストコントロールを導入します。

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、パートナーは内部関係者であるため、組織のインフラ内で役割を果たすために適切な管理を行って運用できるようにする必要があります。

ゼロトラストは10年以上の歴史がありますが、最近多くの注目を集めています。Zero Trustは、最近のBlack HatおよびRSAセキュリティ会議で中心的な話題でした。

Zero Trustは、2019年9月の DoD Digital Modernization StrategyでDoDに約束するテクノロジとして言及されました。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どのように活用して、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かを再考する必要があります。同時に、業務に支障はありません」

2020年8月、NISTは Special Pub 800-207 Zero Trust Architecture(ZTA)を発表した。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

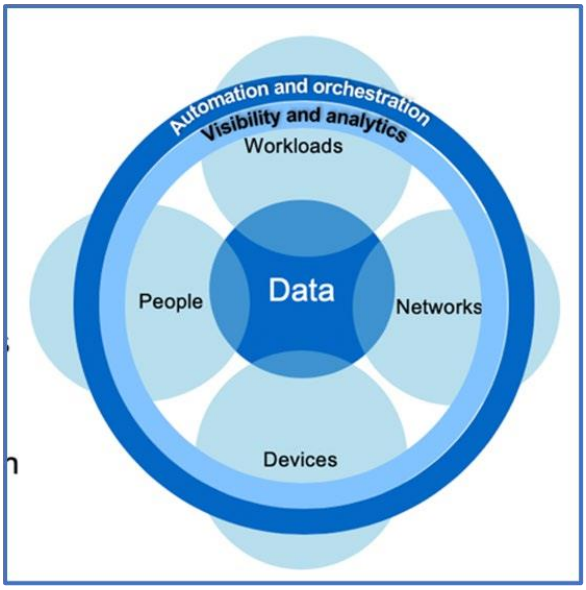
本テクニカルレポートでは、NIST ZTAではなくForrester Researchの概念と用語を使用しています。

『Achieving a Data-Centric Approach to Zero Trust with ONTAP』

ゼロトラストネットワークを構築するには、データ中心のアプローチを適用できます。セキュリティ制御は、可能な限りデータに近い場所に配置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。

図1）ゼロトラストアーキテクチャ



ゼロトラストのデータ主体のMCAPを設計する手順

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、組織のデータの存在場所とそのデータへのアクセス権を持つユーザを特定できます。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の用語では、データの分類には毒性データの識別が含まれます。有害データとは、組織の外部に公開することを意図していない機密データです。有害なデータの開示は、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。規制への準拠に関しては、有毒データには Payment Card Industry Data Security Standard（PCI-DSS;ペイメントカード業界データセキュリティ基準）のカード所有者データ、EU一般データ保護規則（GDPR）の個人データが含まれます。または、医療保険の携行性と責任に関する法律（HIPAA）のための医療データ。NetApp BlueXP分類（旧称Cloud Data Sense）はAIベースのツールキットで、データのスキャン、分析、分類を自動的に実行できます。

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、『概要of secure purge in Data at Rest encryption』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、環境のデータアクセスと管理アクセスであるRole-Based Access Control（RBAC；ロールベースアクセス制御）が含まれます。

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 Multi-admin Verification（MAV；マルチ管理者検証）を使用して、 `volume delete` またはなどのコマンドを1人以上の管理者に承認させることができます `volume snapshot delete`。有効にしたMAVを変更または無効にするには、MAV管理者の承認が必要です。

Snapshotコピーを保護するもう1つの方法として、ONTAP Snapshotコピーのロックがあります。Snapshotコピーロックは、ボリュームSnapshotコピーポリシーの保持期間に応じて手動または自動でSnapshotコピーを消去できないようにするSnapLock機能です。Snapshotコピーロックは、改ざん防止Snapshotコピーロックとも呼ばれます。Snapshotコピーロックの目的は、悪意のある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Snapshotコピーを削除しないようにすることです。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コピーを迅速にリカバリできます。

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RBACに加えて、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多要素認証（MFA）も導入できます。米国政府機関では、管理者アクセスのためのMFAが必要です。公共機関またはPCI-DSSに従う必要がある組織。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になります。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。
NetApp 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：
  - **認証と許可：**SMBとNFSのNASプロトコル機能を介して提供
  - **監査の権利。**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。
  - **許可：**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）。
  - **監査の権利。**実行されたすべてのアクションのsyslog。

保存データと転送中データの暗号化保存データの

暗号化

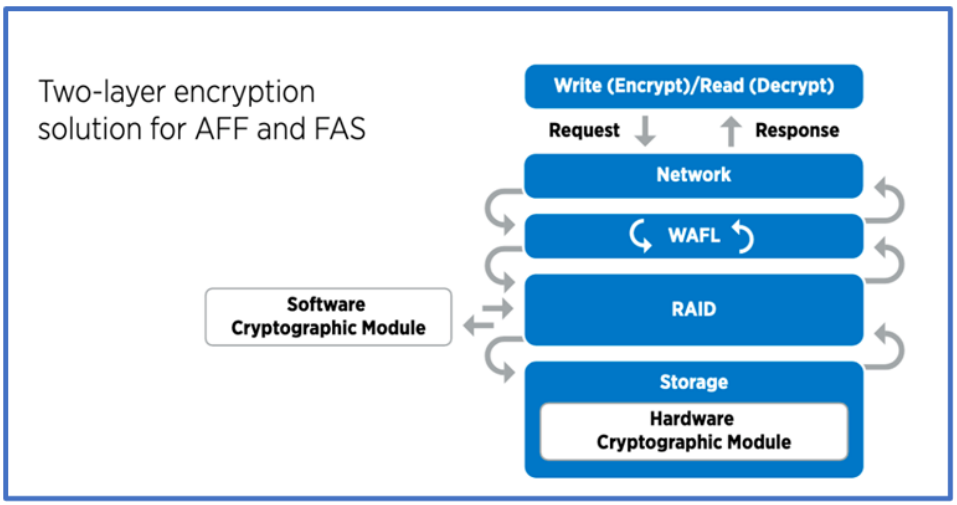
組織がドライブの転用、故障したドライブの返却、大容量ドライブの販売や取り引きを行ってドライブをアップグレードする際に、ストレージシステムのリスクとインフラのギャップを軽減するための新たな要件が日々発生しています。ストレージエンジニアには、データの管理者や運用者として、データのライフサイクルを通じて安全にデータを管理、維持することが求められています。NetAppストレージ暗号化（NSE）、NetAppボリューム暗号化（NVE）、NetAppアグリゲート暗号化を使用すると、毒性の有無にかかわらず、日常の運用に影響を与えることなく、保管中のすべてのデータを常に暗号化できます。

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ハードウェア保管データ解決策です。NVEとNAEは、FIPS 140-2レベル1認定NetApp暗号化モジュールを使用するONTAPソフトウェア保存データ解決策です。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解決策を提供できます。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は量子暗号化に適しています。

NVEは セキュアパージと呼ばれる機能も備えており、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オーバーフローから有害なデータを削除します。

ONTAPに組み込まれているキー管理ツールであるオンボードキーマネージャ（OKM）または認定済みのサードパーティ製外部キー管理ツールを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。

図2）AFFとFASの2レイヤ暗号化解決策



上の図2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。この能力は、最高機密データの保存を可能にする機密プログラムのためのNSAの商用ソリューションにONTAPを検証することにつながりました。

転送中データの暗号化

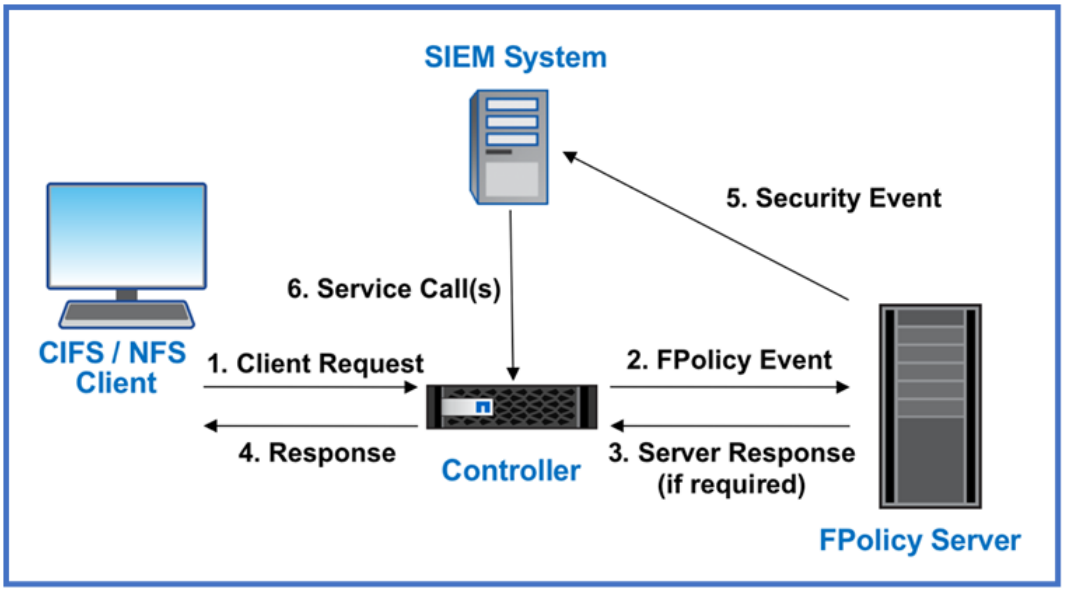
ONTAPの転送中データ暗号化により、ユーザデータアクセスとコントロールプレーンアクセスが保護されます。ユーザデータアクセスは、Microsoft CIFS共有アクセスの場合はSMB 3.0暗号化、NFS Kerberos 5の場合はkrb5pによって暗号化できます。ユーザデータアクセスは、SMB、NFS、iSCSIのIPsecを使用して暗号化することもできます。コントロールプレーンアクセスは、Transport Layer Security（TLS）で暗号化されます。ONTAPには、コントロールプレーンアクセス用のFIPS準拠モードが用意されています。このモードでは、FIPS承認のアルゴリズムが有効になり、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クラスタピア暗号化で暗号化されます。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 NetApp FPolicyパートナーエコシステムを組み合わせることで、データ主体のゼロトラストモデルに必要な制御を提供します。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は業界をリードするONTAP機能であり、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。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、組織のデータの存在場所とそのデータにアクセスできるユーザを特定できます。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。

図3）FPolicyのアーキテクチャ



ネットアップのストレージワークロードセキュリティ（旧称 Cloud Secure）は、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行動分析を使用して、悪意のあるユ

ーザの行動に関するリアルタイムのアラートを提供します。Storage Workload Securityは、高度な機械学習と異常検出機能を通じて、悪意のあるユーザや不正ユーザによる不正使用を防ぎます。Storage Workload Securityは、ランサムウェア攻撃やその他の不正な動作を特定し、Snapshotコピーを起動して、悪意のあるユーザを隔離します。Storage Workload Securityには、ユーザとエンティティのアクティビティの詳細を表示するフォレンジック機能もあります。ストレージワークロードセキュリティはNetApp Cloud 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、Autonomous Ransomware Protection（ARP）と呼ばれるランサムウェア検出機能が搭載されています。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、Snapshotコピー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。

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または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、NetApp ElementおよびONTAPソフトウェア向けに60以上のAnsibleモジュールを開発し、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の役割は、NetApp DoD Unified Capabilities (UC) Deployment Guideに固有のGitHubで公開されています。

利用可能なモジュールのライブラリを使用すると、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。

Cloud Insightsは、インフラ全体を可視化できるインフラ監視ツールです。Cloud 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、すべてのリソースの監視、トラブルシューティング、最適化を実行できます。Cloud Insightsを使用すると、平均問題解決時間を90%短縮し、クラウドの問題の80%がエンドユーザに影響を及ぼすのを防止できます。また、実用的な情報に基づいてデータを保護することで、クラウドインフラのコストを平均33%削減し、内部の脅威によるリスクを軽減できます。Cloud Insightsのストレージワークロードセキュリティ機能を使用すると、内部の脅威が原因でユーザの異常な行動が発生した場合に、AIやMLを使用したユーザ行動分析でアラートを生成できます。ONTAPの場合、ストレージワークロードセキュリティはゼロトラストFPolicyエンジンを使用します。

クラウドの導入

NetAppは、ハイブリッドクラウド環境におけるデータ管理のオーソリティです。NetAppは、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud Platform（GCP）などの主要なクラウドプロバイダを利用して、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システムとONTAP SelectのSoftware-Defined Storageと同じゼロトラストセキュリティ管理をサポートします。

業界初のエンタープライズクラスのAWS / GCP向けクラウドネイティブファイルサービスであるNetApp Cloud Volumes Serviceと、Azure NetApp Files for Microsoft Azureを使用すれば、一般的なCAPEX（設備投資）の制約を受けることなくパブリッククラウドの容量を簡単に拡張できます。分析やDevOpsなど、大量のデータを処理するワークロードに最適なこのクラウドデータサービスは、NetAppの柔軟なオンデマンドストレージサービスとONTAPデータ管理機能を組み合わせたフルマネージドサービスです。

AWS EBSやS3、Azureストレージなど、クラウドブロックサービスやオブジェクトストレージサービス向けの高度なデータサービスをお探しの場合は、Cloud Volumes ONTAPを使用すれば、オンプレミス環境とパブリッククラウド間のデータ管理を単一の共通ビューで管理できます。AWSまたはAzureでオンデマンドインスタンスとして実行されるCloud Volumes ONTAPは、ONTAPソフトウェアのStorage Efficiency、可用性、拡張性を提供します。ONTAPでは、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またはAzureのストレージ環境の間でデータを移動できます。

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、NetApp セキュリティポータルを参照してください。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを参照してください。

- Verizon Data Breach Investigationsレポート
  https://enterprise.verizon.com/resources/reports/dbir/
- ウィキリークス事件でブラッドリー・マニングが35年の判決を下した
  https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html
- エドワード・スノーデンがnsaのリーク源として
  https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html
- 国防総省のデジタル最新化戦略
  https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF
- NIST SP 800-207ゼロトラストアーキテクチャ
  https://csrc.nist.gov/publications/detail/sp/800-207/final
- NetApp Partner Connect：セキュリティアライアンスパートナー
  https://www.netapp.com/partners/partner-connect/#t=Partners&sort=%40partnerweight%20descending&layout=card&numberOfResults=25&f:@facet_language_mktg=[English]&f:@facet_partnertype_mktg=[Technology%20Alliance]&f:@facet_techsolution_mktg=[Security]
- SVMでのFPolicyによるファイルの監視と管理
  https://docs.netapp.com/us-en/ontap/nas-audit/two-parts-fpolicy-solution-concept.html
- PCI-DSS 3.2 ONTAP 9
  https://www.netapp.com/us/media/tr-4401.pdf
- 一般データ保護規則（GDPR）
  https://www.netapp.com/us/info/gdpr.aspx
- HIPPAプライバシールールの概要
  https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- NetApp BlueXP分類サービス
  https://bluexp.netapp.com/netapp-cloud-data-sense

- マルチ管理者認証
  https://docs.netapp.com/us-en/ontap/multi-admin-verify/index.html
- Snapshotコピー ロックの改ざん防止
  https://docs.netapp.com/us-en/ontap/snaplock/snapshot-lock-concept.html
- ONTAP 9での多要素認証
  https://www.netapp.com/us/media/tr-4647.pdf
- NetAppストレージ暗号化、NVMe自己暗号化ドライブ、NetAppボリューム暗号化、NetAppアグリゲート暗号化
  https://www.netapp.com/us/media/ds-3898.pdf
- NetApp Storage Encryption
  https://www.netapp.com/us/media/ds-3213-en.pdf
- NetApp Volume Encryption and NetApp Aggregate Encryption
  https://www.netapp.com/us/media/ds-3899.pdf
- NetApp暗号モジュールFIPS-140-2証明書
  https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144
- NetAppによるQuantum対応の保管データ暗号化
  https://www.netapp.com/us/media/sb-3952.pdf
- セキュリティでイノベーション：NetAppとOntrackがフラッシュメモリサミットアワードを受賞
  https://blog.netapp.com/flash-memory-summit-award/
- オンボードキー管理の有効化
  https://docs.netapp.com/us-en/ontap/encryption-at-rest/enable-onboard-key-management-96-later-nve-task.html
- NetApp Interoperability Matrix Tool
  https://mysupport.netapp.com/matrix/imt.jsp?components=69551;&solution=1156&isHWU&src=IMT
- 外部キー管理の設定
  https://docs.netapp.com/us-en/ontap/encryption-at-rest/configure-external-key-management-concept.html
- 分類された企業向けソリューション
  https://www.netapp.com/blog/netapp-ontap-CSfC-validation/
- ONTAP IPSec
  https://docs.netapp.com/us-en/ontap/networking/configure_ip_security_@ipsec@_over_wire_encryption.html
- security config modifyを使用してFIPSモードを有効にする
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr-950/security__config__modify.html
- 既存のピア関係でのクラスタピアリング暗号化の有効化
  https://docs.netapp.com/us-en/ontap/peering/enable-cluster-peering-encryption-existing-task.html
- ストレージワークロードのセキュリティ（Cloud Secure）
  https://docs.netapp.com/us-en/cloudinsights/cs_intro.html
- NetAppとAnsibleで開発ワークフローを自動化する方法をご紹介します
  https://www.netapp.com/us/getting-started-with-netapp-approved-ansible-modules/index.aspx
- NetApp DoD Unified Capabilities（UC）導入ガイドに固有のAnsibleモジュール。
  https://github.com/NetApp/ansible/tree/master/nar_ontap_security_ucd_guide
- 管理者認証とRBAC
  https://docs.netapp.com/us-en/ontap/authentication/index.html
- ONTAP保存データの暗号化
  https://docs.netapp.com/us-en/ontap/encryption-at-rest/index.html
- TR-4569『Security Hardening Guide for NetApp ONTAP 9』
  https://www.netapp.com/us/media/tr-4569.pdf

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン1.0	2020年4月	初版リリース
バージョン1.1	2023年3月	ONTAPの新しい機能に関する最新情報：MAV、改ざん防止Snapshotコピー、IPsecとBlueXPの分類、Commercial Solutions for Classified Program（CSfC）、Storage Workload Security

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4829-0323-JP