FlexPod とセキュリティ

FlexPod

NetApp
March 25, 2024

目次

FlexPod とセキュリティ

解決策、 FlexPod によるランサムウェア対策

TR-4802 ：『 FlexPod 、 the 解決策 to Ransomware 』

ネットアップ、 Arvind Ramakrinan 氏

協力：

ランサムウェアを理解するには、まず暗号化の重要なポイントを理解する必要があります。Cryptographical メソッドでは、共有秘密鍵（対称鍵暗号化）または鍵のペア（非対称鍵暗号化）を使用してデータを暗号化できます。このうちの 1 つは広く利用されている公開鍵で、もう 1 つは非公開の秘密鍵です。

ランサムウェアは、暗号化を使用して悪意のあるソフトウェアを構築する、暗号化に基づくマルウェアの一種です。このマルウェアは、対称キー暗号化と非対称キー暗号化の両方を利用して、被害者のデータをロックし、被害者のデータを復号化するための鍵を提供するように身代金を要求できます。

ランサムウェアの仕組み

次の手順では、ランサムウェアが暗号化を使用して、被害者による復号化やリカバリの範囲を伴わずに被害者のデータを暗号化する方法について説明します。

1. 攻撃者は、非対称キー暗号化のようにキーペアを生成します。生成された公開鍵はマルウェア内に置かれ、マルウェアは解放されます。
2. 被害者のコンピュータまたはシステムにマルウェアが侵入すると、擬似乱数生成器（ PRNG ）またはその他の実行可能な乱数生成アルゴリズムを使用してランダムな対称キーが生成されます。
3. マルウェアは、この対称キーを使用して被害者のデータを暗号化します。最終的には、マルウェアに埋め込まれた攻撃者の公開鍵を使用して、対称キーを暗号化します。このステップの出力は、暗号化された対称キーの非対称暗号テキストと、被害者のデータの対称暗号テキストです。
4. マルウェアは、被害者のデータとデータの暗号化に使用された対称キーをゼロ化（消去）し、リカバリの対象範囲を残しません。
5. これで、対称キーの非対称暗号テキストと、データの暗号化に使用された対称キーを取得するために支払わなければならない身代金の値が、 Victim に表示されます。
6. 被害者は身代金を支払って、攻撃者と非対称暗号テキストを共有します。攻撃者は自分の秘密鍵を使って暗号テキストを復号化し、その結果対称鍵が生成されます。
7. 攻撃者はこの対称キーを攻撃者と共有します。このキーを使用して、すべてのデータを復号化し、攻撃から回復できます。

課題

個人や組織がランサムウェア攻撃を受けた場合、次のような課題に直面します。

- 最も重要な課題は、組織または個人の生産性を即座に低下させることです。重要なファイルはすべて回復する必要があり、システムを保護する必要があるため、正常な状態に戻るのに時間がかかります。
- クライアントまたは顧客に属する機密情報を含むデータ侵害が発生し、組織が明確に回避したいという危機的状況につながる可能性があります。
- データが間違った手に入ったり、完全に消去されたりする可能性は非常に高いため、企業や個人にとって災害となる可能性のあるリターンポイントをゼロにすることができます。
- 身代金を支払った後、攻撃者がデータを復元するための鍵を提供する保証はありません。
- 身代金を支払っても機密データのブロードキャストを控えることは、攻撃者に保証されていません。
- 大規模な企業では、ランサムウェア攻撃の原因となった抜け穴を特定するのは面倒であり、すべてのシステムを保護するには多くの労力が必要です。

誰がリスクにさらされているか？

個人や大企業など、誰もがランサムウェア攻撃を受ける可能性があります。適切に定義されたセキュリティ対策や慣行を実装していない組織は、このような攻撃に対してさらに脆弱です。攻撃が大規模な組織に与える影響は、個人が耐えうる攻撃の数倍にも及ぶ可能性があります。

ランサムウェア攻撃はすべてのマルウェア攻撃の約 28% を占めています。つまり、マルウェアのインシデントが 4 つに 1 つ以上あり、ランサムウェア攻撃と言えます。ランサムウェアはインターネットを介して自動的に、または無差別に拡散する可能性があります。また、セキュリティ上の問題が発生した場合は、被害者のシステムに入り、他の接続されたシステムへの拡散を継続できます。攻撃者は、多くのファイル共有を実行したり、機密性の高い重要なデータを大量に取得したり、攻撃に対する保護を適切に維持したりする人や組織を標的にしている傾向があります。

攻撃者は、次の潜在的なターゲットに集中する傾向があります。

- 大学と学生コミュニティ
- 政府機関、政府機関
- 病院
- 銀行

これはターゲットの完全なリストではありません。これらのカテゴリのいずれかに該当しない場合は、攻撃から自分を守ることはできません。

ランサムウェアによるシステムへの移行やデータの拡散について教えてください。

ランサムウェアがシステムに移行したり、他のシステムに拡散したりする方法はいくつかあります。今日の世界では、ほとんどすべてのシステムがインターネット、 LAN 、 WAN などを介して相互に接続されています。これらのシステム間で生成および交換されるデータ量は増加しています。

ランサムウェアが拡散する最も一般的な方法には、データの共有やアクセスに日常的に使用する方法があります。

- E メール
- P2P ネットワーク
- ファイルのダウンロード
- ソーシャルネットワーキング

- モバイルデバイス
- 安全でないパブリックネットワークに接続しています
- Web URL へのアクセス

データ損失の影響

データ損失の影響は、企業が予想する以上に広範囲に及ぶ可能性があります。この影響は、ダウンタイムの期間、または組織がデータにアクセスできない期間によって異なります。攻撃が長ければ長いほど、組織の収益、ブランド、評判への影響は大きくなります。また、組織は法的な問題に直面し、生産性が大幅に低下する可能性もあります。

これらの問題は時間の経過とともに継続して発生するため、攻撃に対する対応方法によっては、拡大が始まり、組織の文化が変化する可能性があります。今日の世界では、組織に関する情報が急速に広まり、否定的なニュースが原因によってその評判に永久的な損害を与える可能性があります。企業は、データ損失に対する大きなペナルティに直面する可能性があり、結果としてビジネスの停止につながる可能性があります。

財務的影響

最近の "McAfee レポート"サイバー犯罪によって発生するグローバルコストは約 6 億ドルで、世界の GDP の約 0.8 %に相当します。この金額を世界的に増加するインターネット経済の 4.2 兆ドルと比較すると、成長に 14% の税金がかかることになります。

ランサムウェア攻撃は、このような金銭的コストを大幅に負担します。2018 年には、ランサムウェア攻撃によって発生したコストは約 80 億ドルでした。 2019 年には 115 億ドルに達すると予測されています。

解決策とは何ですか？

ダウンタイムを最小限に抑えたランサムウェア攻撃からのリカバリは、プロアクティブなディザスタリカバリ計画を実装することでのみ可能です。攻撃から回復する機能は優れていますが、攻撃を完全に阻止することが理想的です。

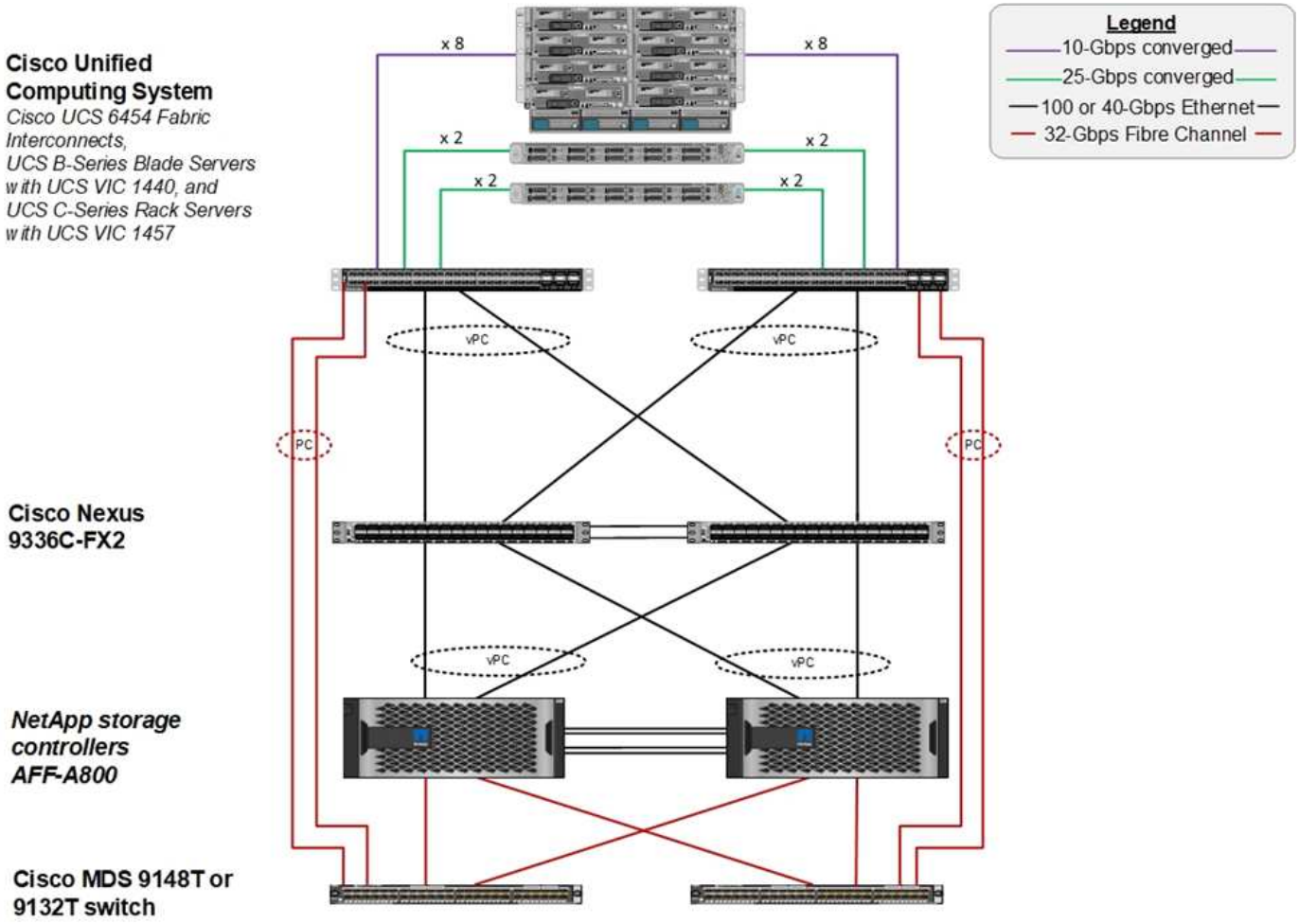
攻撃を防止するためにレビューと修正が必要な領域はいくつかありますが、攻撃を防止または復旧するためのコアコンポーネントはデータセンターです。

ネットワーク、コンピューティング、ストレージのエンドポイントを保護するデータセンターの設計と機能は、日常業務の安全な環境を構築する上で重要な役割を果たします。このドキュメントでは、 FlexPod ハイブリッドクラウドインフラストラクチャの機能が、攻撃の発生時に迅速にデータをリカバリするのにどのように役立つか、また攻撃を防御するのにどのように役立つかを説明します。

FlexPod の概要

FlexPod は、 Cisco Unified Computing System （ Cisco UCS ）サーバ、 Cisco Nexus ファミリーのスイッチ、 Cisco MDS ファブリックスイッチ、ネットアップストレージアレイを 1 つの柔軟なアーキテクチャに統合した、事前設計済みの統合された検証済みアーキテクチャです。FlexPod ソリューションは、単一点障害のない高可用性を実現するとともに、コスト効率と設計の柔軟性を維持して、さまざまなワークロードをサポートするように設計されています。FlexPod 設計では、さまざまなハイパーバイザーやベアメタルサーバをサポートでき、お客様のワークロードの要件に応じてサイジングや最適化も可能です。

次の図は FlexPod アーキテクチャを示しており、スタックのすべてのレイヤの高可用性を明確に示しています。ストレージ、ネットワーク、コンピューティングのインフラコンポーネントは、コンポーネントの 1 つに障害が発生した場合に、稼働しているパートナーに瞬時にフェイルオーバーできるように構成されます。



FlexPod システムの主な利点は、複数のワークロードに対して事前に設計、統合、検証されていることです。解決策の検証ごとに、詳細な設計ガイドと導入ガイドが公開されています。これらのドキュメントには、FlexPod でワークロードをシームレスに実行するために採用する必要があるベストプラクティスが含まれています。これらのソリューションは、業界最高レベルのコンピューティング、ネットワーク、ストレージ製品と、インフラ全体のセキュリティと強化に重点を置いた多数の機能で構成されています。

"IBM の X-Force Threat Intelligence Index を参照してください" 州、「不正なクラウドインフラストラクチャの歴史的な 424% の増加など、侵害されたレコードの 3 分の 2 を担当する人的ミス」

FlexPod システムでは、 Cisco Validated Design （ CVD ）および NetApp Verified Architectures （ NVA ）に記載されているベストプラクティスに従って、インフラのエンドツーエンドのセットアップを実行する Ansible プレイブックを使用して、インフラの構成ミスを回避できます。

ランサムウェアからの保護対策

ここでは、 NetApp ONTAP データ管理ソフトウェアの主な機能と、ランサムウェア攻撃から効果的に保護してリカバリするために使用できる Cisco UCS および Cisco Nexus のツールについて説明します。

ストレージ： **NetApp ONTAP**

ONTAP ソフトウェアには、データ保護に役立つさまざまな機能が用意されています。そのほとんどは、ONTAP システムをお持ちのお客様には無償で提供されています。次の機能を常に使用して、攻撃からデータを保護できます。

- * NetApp Snapshot テクノロジ。 * Snapshot コピーは、ボリュームの読み取り専用イメージであり、ファイルシステムの「ある瞬間」の状態をキャプチャしたものです。これらのコピーによって、システムパフォーマンスへの影響がなく、データが保護されると同時に、大量のストレージスペースが消費されることもありません。Snapshot コピーの作成スケジュールを作成することを推奨します。また、マルウェアの中には、感染後数週間または数か月後に休止して再アクティブ化できるものがあるため、長期の保存期間を維持する必要があります。攻撃が発生した場合、感染前に作成された Snapshot コピーを使用してボリュームをロールバックできます。
- * NetApp SnapRestore テクノロジ。 * SnapRestore データ・リカバリ・ソフトウェアは、データ破損からのリカバリや、ファイルの内容のみの復元に非常に役立ちます。SnapRestore はボリュームの属性をリバートせず、 Snapshot コピーからアクティブファイルシステムにファイルをコピーすることで、管理者が達成できる処理よりもはるかに高速です。データのリカバリ速度は、できるだけ多くのファイルをリカバリする必要がある場合に役立ちます。攻撃が発生した場合、この非常に効率的なリカバリプロセスにより、ビジネスを迅速にオンラインに戻すことができます。
- * NetApp SnapCenter テクノロジ。 * SnapCenter ソフトウェアは、ネットアップのストレージベースのバックアップ機能とレプリケーション機能を使用して、アプリケーションと整合性のあるデータ保護を実現します。このソフトウェアは、エンタープライズアプリケーションと統合され、アプリケーション固有およびデータベース固有のワークフローを提供して、アプリケーション、データベース、仮想インフラの管理者のニーズを満たします。SnapCenter は、使いやすいエンタープライズプラットフォームを提供し、アプリケーション、データベース、ファイルシステム全体でデータ保護をセキュアに調整、管理します。アプリケーションと整合性のあるデータ保護を提供できるかどうかは、整合性のある状態へのアプリケーションのリストアをより迅速に行えるようにするため、データリカバリの際に重要になります。
- * NetApp SnapLock テクノロジ。 * SnapLock は、消去や書き換えが不可能な状態でファイルを保存し、コミットできる特殊な目的のボリュームを提供します。FlexVol ボリュームに保存されているユーザーの本番データは、 NetApp SnapMirror または SnapVault テクノロジを使用して、それぞれ SnapLock ボリュームにミラーリングまたは保存できます。SnapLock ボリューム内のファイル、ボリューム自体、およびホストアグリゲートは、保持期間が終了するまで削除できません。
- * NetApp FPolicy テクノロジ。 * 特定の拡張子を持つファイルの操作を禁止することにより、 FPolicy ソフトウェアを使用して攻撃を防止します。FPolicy イベントは、特定のファイル操作に対してトリガーできます。イベントはポリシーに関連付けられており、ポリシーは使用する必要があるエンジンを呼び出します。ポリシーにはランサムウェアを含む可能性のある一連のファイル拡張子を設定できます。拡張子が許可されていないファイルで許可されていない操作を実行しようとすると、 FPolicy によりその操作が実行されなくなります。

ネットワーク： **Cisco Nexus**

Cisco NX-OS ソフトウェアは、ネットワーク異常およびセキュリティの検出を強化する NetFlow 機能をサポートしています。NetFlow は、ネットワーク上のすべてのカンバセーション、通信に関係する側、使用されているプロトコル、およびトランザクションの期間のメタデータをキャプチャします。情報を集約して分析すると、正常な動作に関する洞察を得ることができます。

収集されたデータを使用すると、疑わしいアクティビティのパターンを識別することもできます。たとえば、マルウェアがネットワーク全体に拡散し、これが気付かない場合があります。

NetFlow では、フローを使用してネットワークモニタリングの統計情報を提供します。フローは、送信元インターフェイス（または VLAN ）に着信し、キーの値が同じパケットの単方向ストリームです。キーは、パケット内のフィールドの識別された値です。フローレコードを使用してフローを作成し、フローに固有のキーを

定義します。フローエクスポータを使用して、 Cisco StealthWatch などのリモート NetFlow コレクタに NetFlow が収集するデータをエクスポートできます。StealthWatch では、この情報を使用してネットワークを継続的に監視し、ランサムウェアの発生が発生した場合にリアルタイムの脅威検出およびインシデント応答フォレンジックを提供します。

コンピューティング： **Cisco UCS**

Cisco UCS は、 FlexPod アーキテクチャのコンピューティングエンドポイントです。複数のシスコ製品を使用して、スタックのこのレイヤをオペレーティングシステムレベルで保護することができます。

コンピューティングレイヤまたはアプリケーションレイヤには、次の主要製品を実装できます。

- * エンドポイント向けの Cisco Advanced Malware Protection （ AMP ）。 * Microsoft Windows および Linux オペレーティングシステムでサポートされているこの解決策は、防止、検出、および応答機能を統合しています。このセキュリティソフトウェアは、セキュリティ侵害の防止、侵入ポイントでのマルウェアのブロック、ファイルおよびプロセスのアクティビティの継続的な監視と分析を行い、フロントライン防御を回避できる脅威を迅速に検出、阻止、修復します。

  AMP の Malicious Activity Protection （ MAP ）コンポーネントは、すべてのエンドポイントアクティビティを継続的に監視し、エンドポイント上の実行中のプログラムのランタイム検出と異常な動作のブロックを提供します。たとえば、エンドポイントの動作がランサムウェアを示している場合、攻撃の原因となっているプロセスは終了し、エンドポイントの暗号化を防ぎ、攻撃を停止します。

- * 電子メールセキュリティに関するシスコの高度なマルウェア対策。 * 電子メールは、マルウェアを拡散し、サイバー攻撃を実行するための主要な手段となっています。平均して、 1 日に約 1 、 000 億通の電子メールが交換されます。これにより、攻撃者はユーザーのシステムに非常に優れた侵入ベクトルを与えることができます。そのため、この種の攻撃を防御することは絶対に不可欠です。

  AMP は、ゼロデイ攻撃や悪意のある添付ファイルに隠された不潔なマルウェアなどの脅威を電子メールで分析します。また、業界をリードする URL インテリジェンスを使用して、悪意のあるリンクに対抗します。スピアフィッシング、ランサムウェア、その他の高度な攻撃から高度な保護を提供します。

- * 次世代侵入防御システム（ NGIPS ）。 * Cisco firepower NGIPS は、データセンターの物理アプライアンスとして、または VMware の仮想アプライアンスとして導入できます（ NGIPSv for VMware ）。この非常に効果的な侵入防御システムは、信頼性の高いパフォーマンスと低い総所有コストを実現します。オプションのサブスクリプションライセンスで脅威からの保護を拡張して、 AMP 、アプリケーションの可視化と制御、および URL フィルタリング機能を提供できます。仮想化された NGIPS は、仮想マシン（ VM ）間のトラフィックを検査し、リソースが限られたサイトで NGIPS ソリューションの導入と管理を容易にして、物理資産と仮想資産の両方の保護を強化します。

FlexPod でデータを保護し、リカバリできます

このセクションでは、攻撃が発生した場合にエンドユーザーのデータをどのように回復できるか、および FlexPod システムを使用して攻撃を防御する方法について説明します。

テストベッドの概要

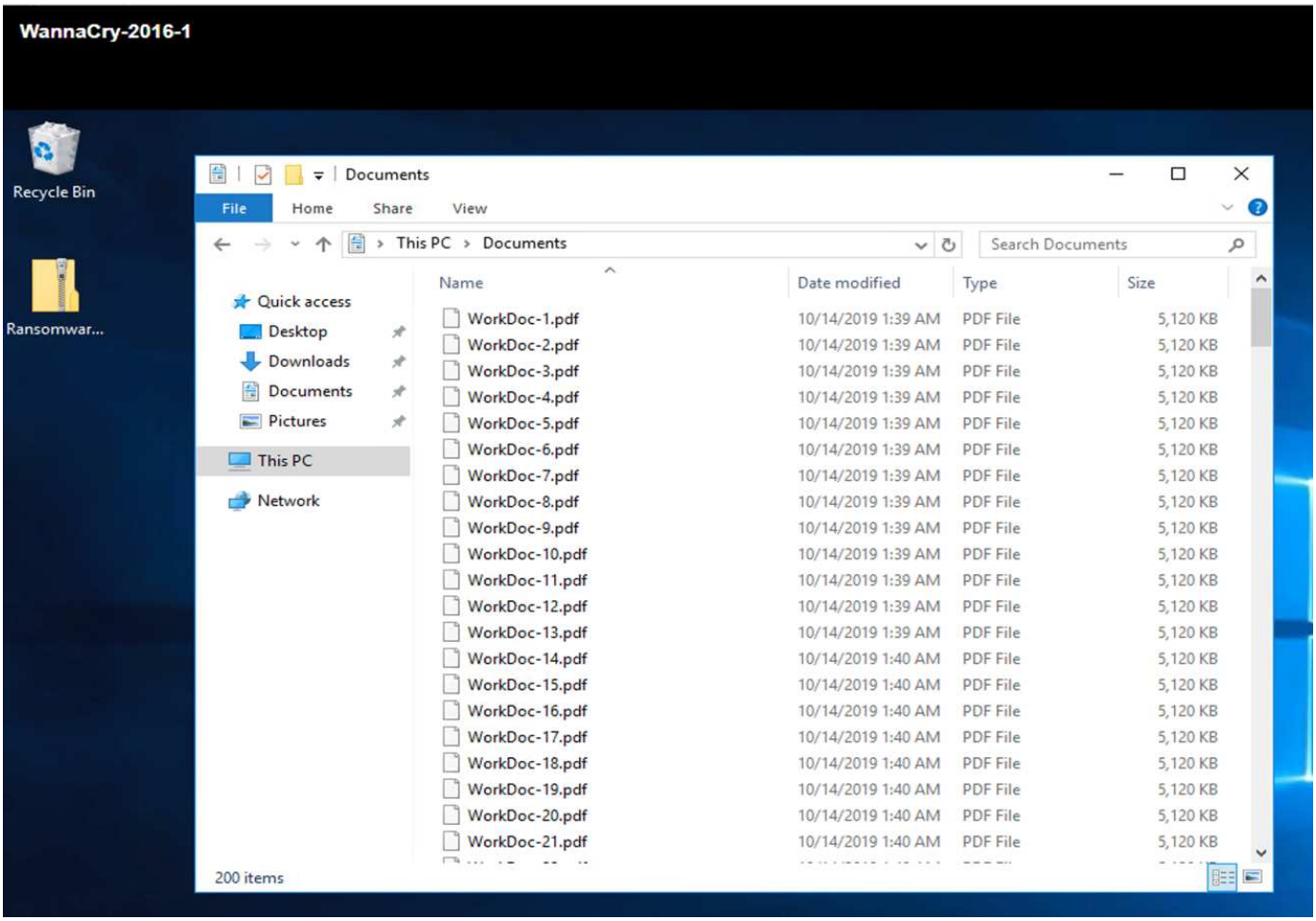
テストベッドは、 FlexPod の検出、修復、および防止を示すために、本ドキュメントの作成時点で使用可能な最新のプラットフォーム CVD で指定されているガイドラインに基づいて構築されています。 "FlexPod データセンターと VMware vSphere 6.7 U1 、 Cisco UCS 第 4 世代、および NetApp AFF A シリーズに関する CVD"。

NetApp ONTAP ソフトウェアの CIFS 共有を提供していた Windows 2016 VM は、 VMware vSphere インフラに導入されました。その後、特定の拡張子タイプのファイルが実行されないように、 CIFS 共有に NetApp FPolicy を設定しました。また、アプリケーションと整合性のある Snapshot コピーを作成するために、インフラ内の VM の Snapshot コピーを管理するために NetApp SnapCenter ソフトウェアを導入しました。

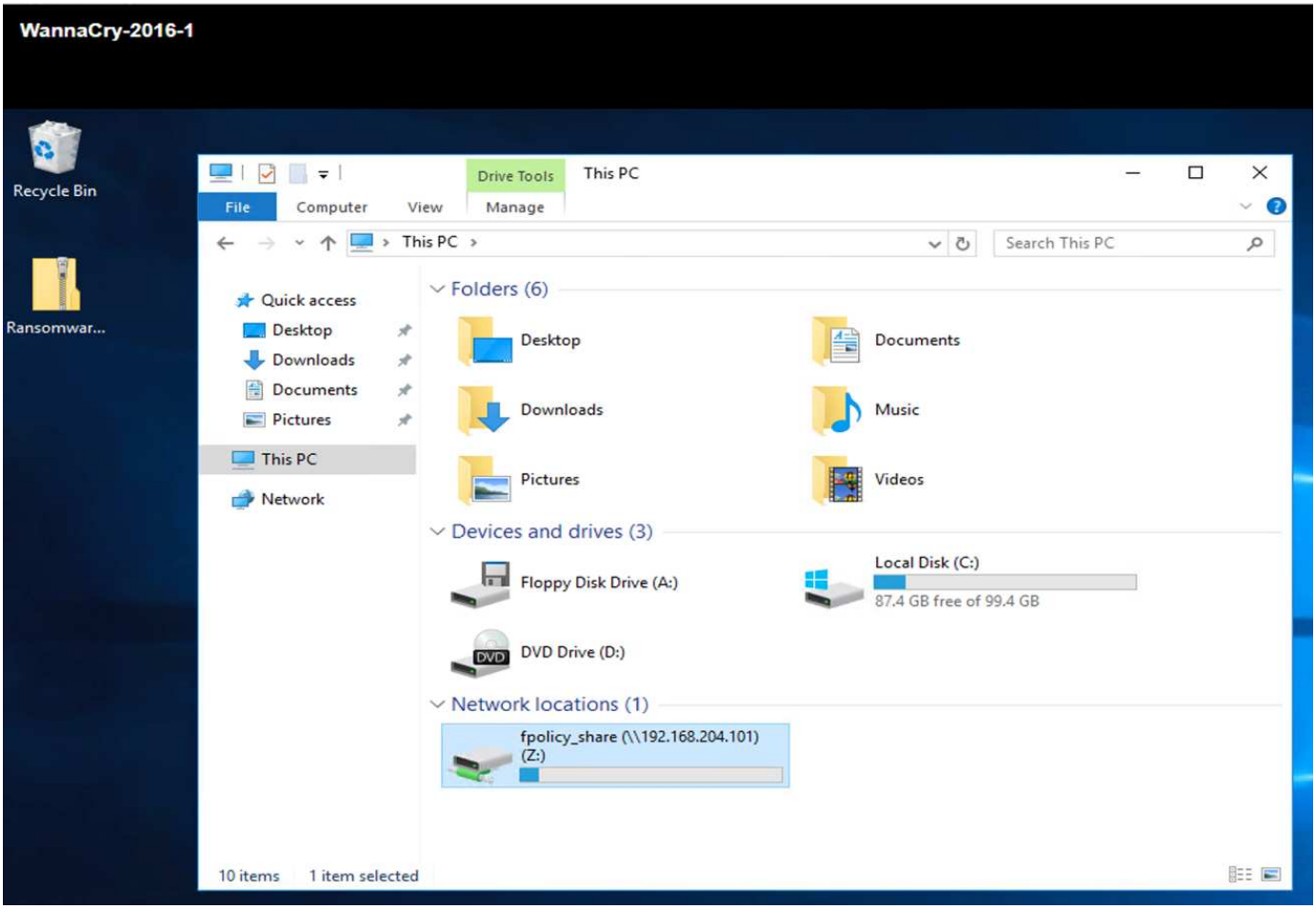
攻撃前の **VM** とそのファイルの状態

ここでは、 VM およびマッピングされている CIFS 共有に対する攻撃前のファイルの状態を示します。

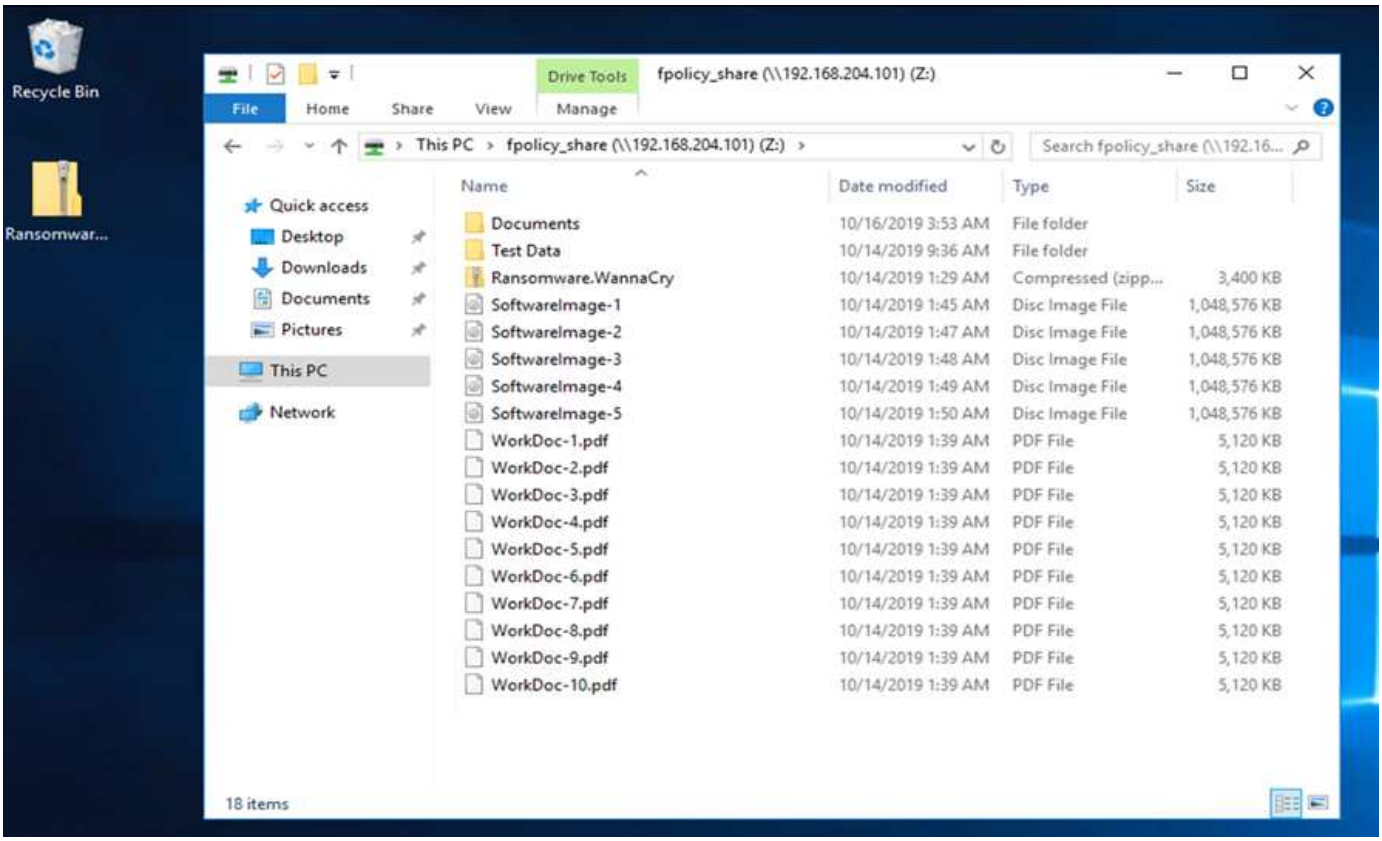
VM の Documents フォルダには、 WannaCry マルウェアによってまだ暗号化されていない PDF ファイルのセットがありました。



次のスクリーンショットは、 VM にマッピングされている CIFS 共有を示しています。



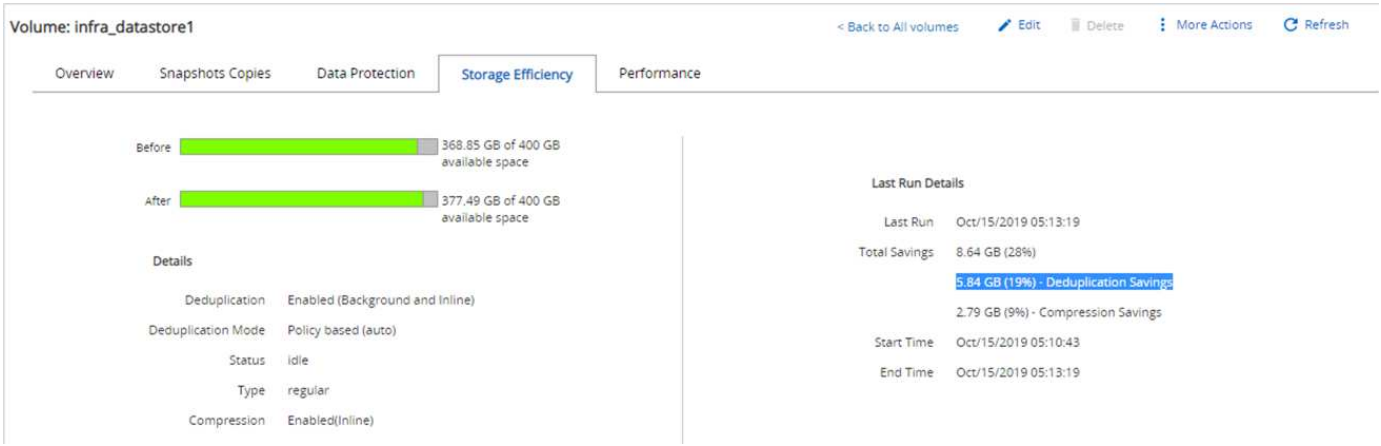
次のスクリーンショットは、 WannaCry マルウェアによってまだ暗号化されていない CIFS 共有 'fpolicy_share' 上のファイルを示しています。



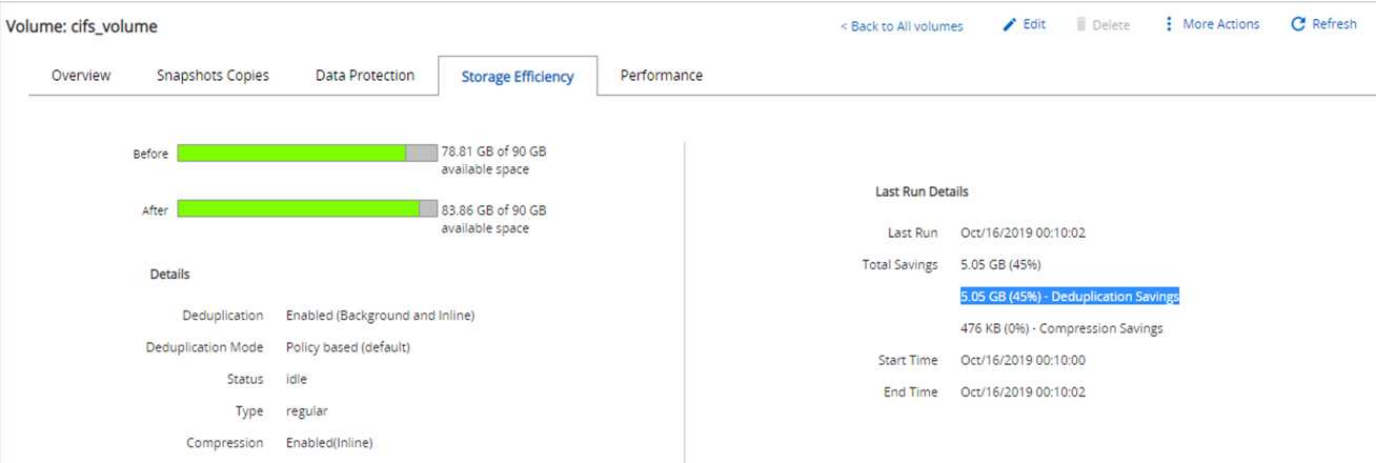
攻撃前の重複排除およびスナップショット情報

攻撃前の Snapshot コピーのストレージ効率の詳細およびサイズは、検出フェーズで参照用として示されます。

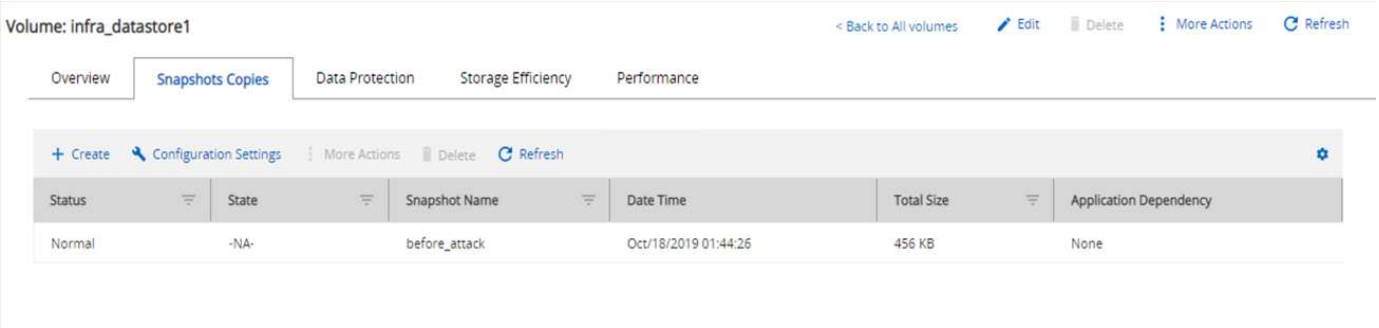
VM をホストするボリュームで重複排除を実行すると、ストレージを 19% 削減できました。



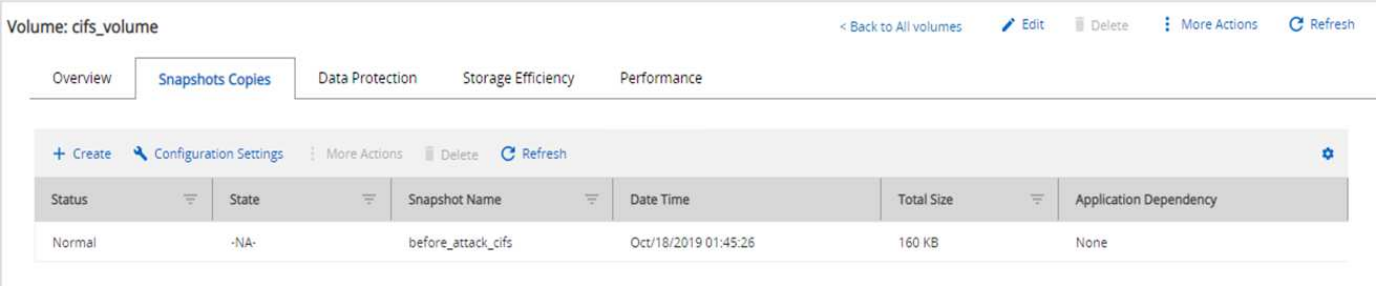
CIFS 共有「 fpolicy_share 」の重複排除により、 45% のストレージ節約を達成しました。



VM をホストしているボリュームの Snapshot コピーサイズとして、 456KB が観察されました。



CIFS 共有「 fpolicy_share 」に対しては、 160KB の Snapshot コピー・サイズが検出されました。



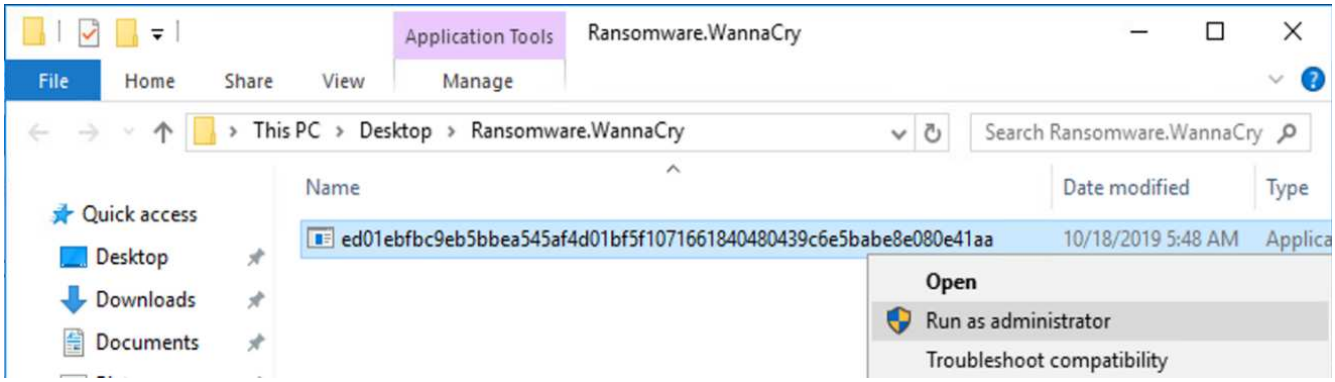
VM および **CIFS** 共有での **WannaCry** 感染

このセクションでは、 WannaCry マルウェアが FlexPod 環境にどのように導入されたか、および観察されたシステムにその後の変更がどのように加えられたかを説明します。

次の手順は、 WannaCry マルウェアバイナリが VM にどのように導入されたかを示しています。

1. 保護されたマルウェアが抽出されました。

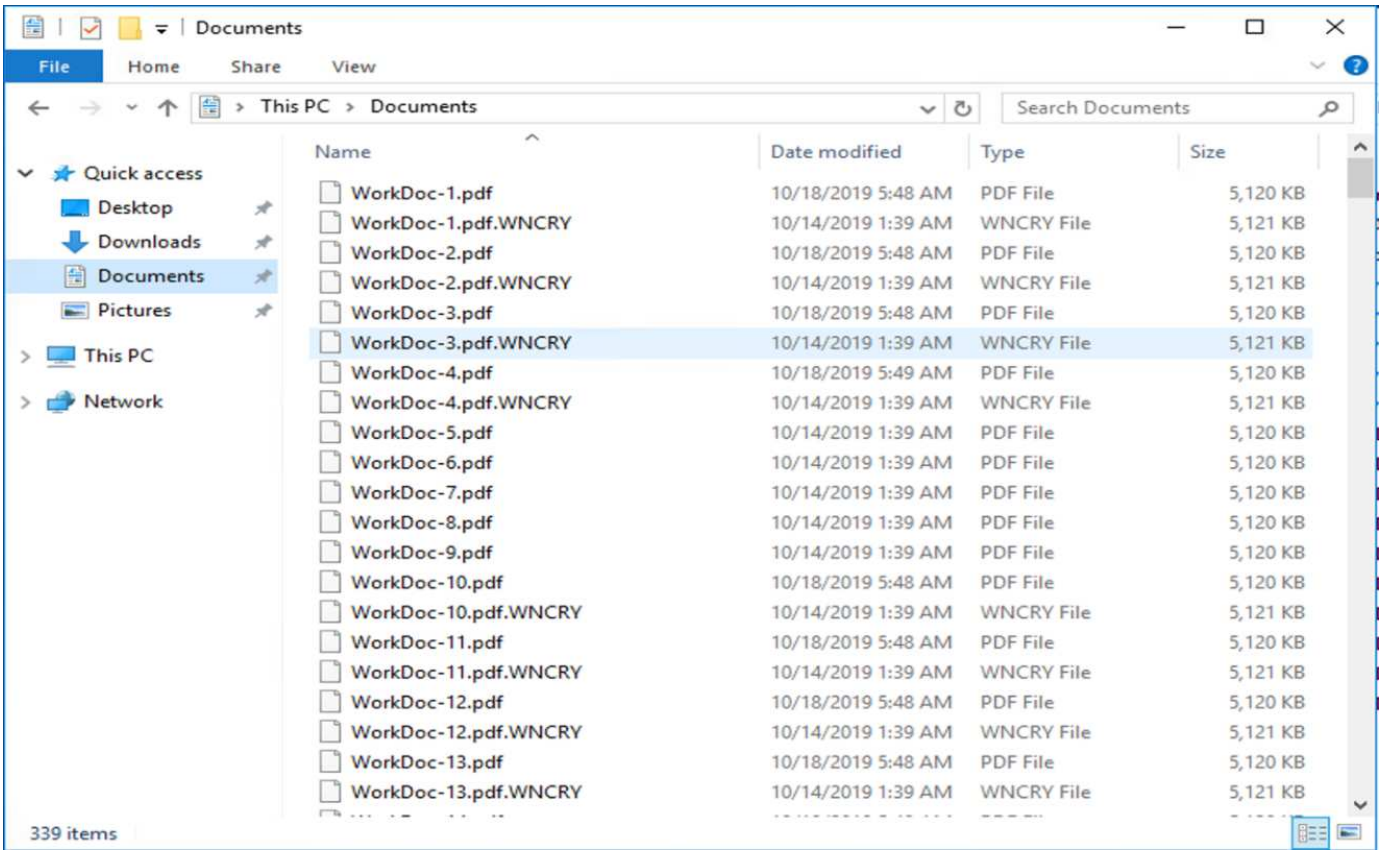
2. バイナリが実行されました。



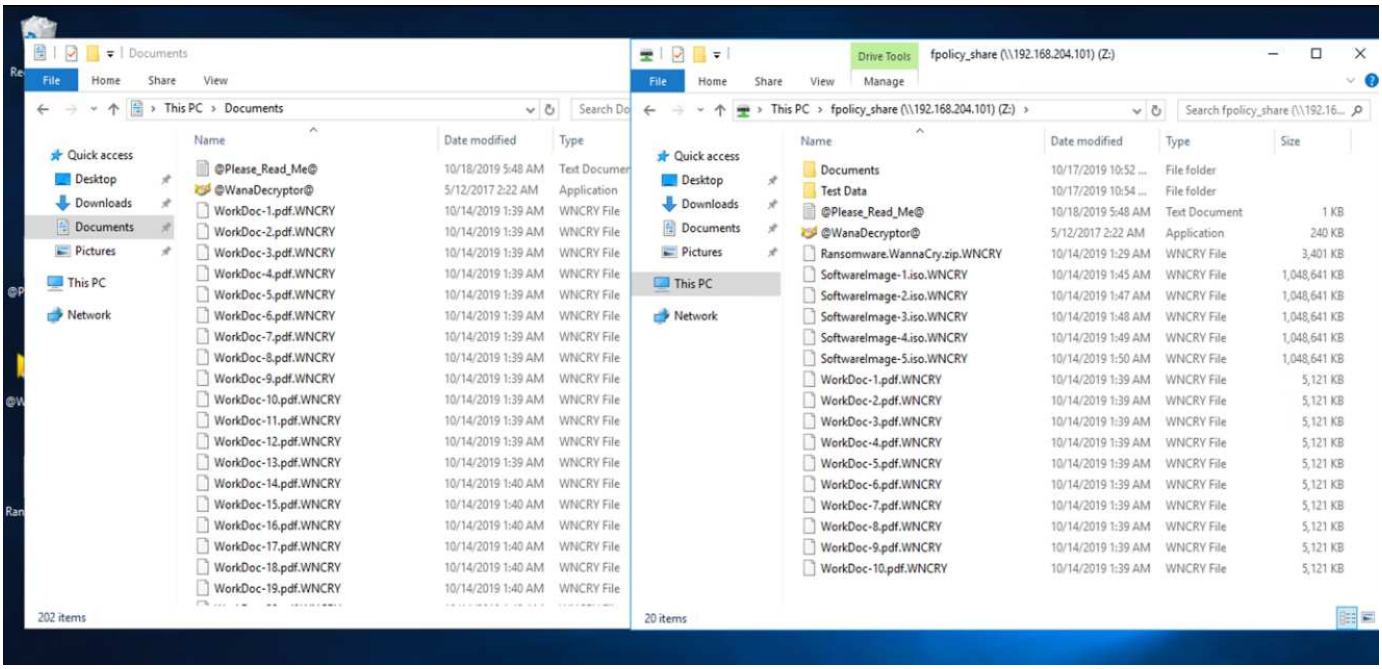
ケース **1** ： **WannaCry** は **VM** 内のファイルシステムを暗号化し、マッピングされた **CIFS** 共有を暗号化します

ローカルファイルシステムとマッピングされた CIFS 共有は、 WannaCry マルウェアによって暗号化されています。

マルウェアは WNCRY 拡張子でファイルを暗号化し始めます。



マルウェアは、ローカル VM およびマッピングされた共有内のすべてのファイルを暗号化します。

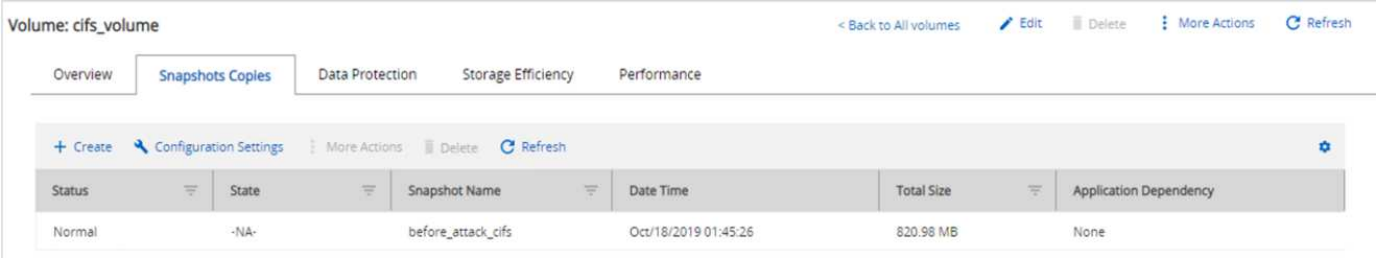


検出

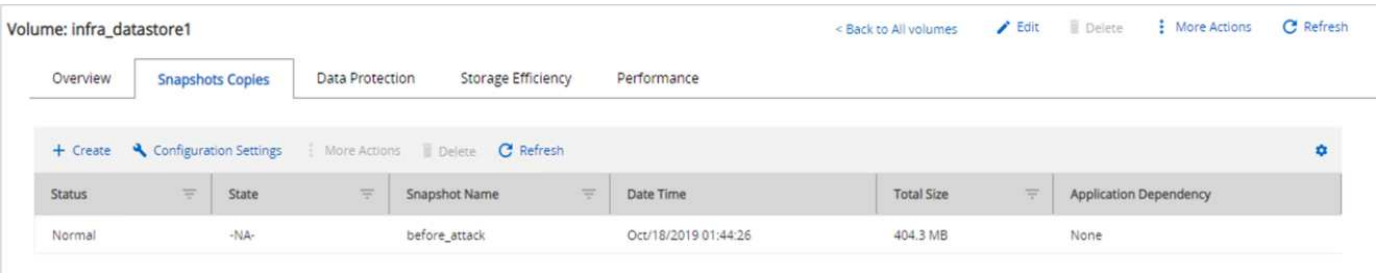
マルウェアがファイルの暗号化を開始した瞬間から、 Snapshot コピーのサイズが急激に増加し、ストレージ効率が急激に低下しました。

攻撃中に CIFS 共有をホストしているボリュームの Snapshot サイズが 820.98MB に急増していることが検出

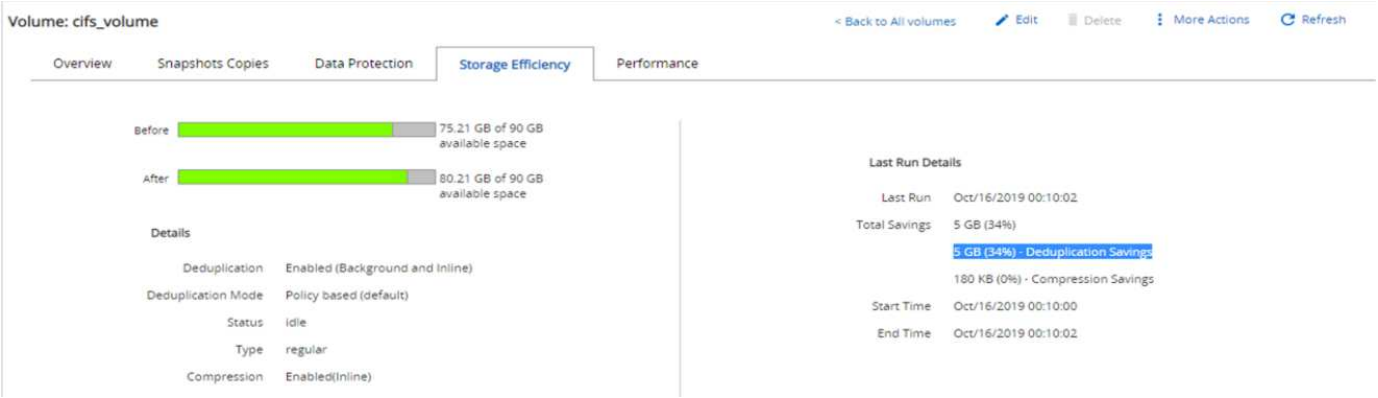
されました。



VM をホストしているボリュームの Snapshot コピーサイズが 404.3MB に増加していることが検出されました。



CIFS 共有をホストしているボリュームのストレージ効率は 34% に低下しています。



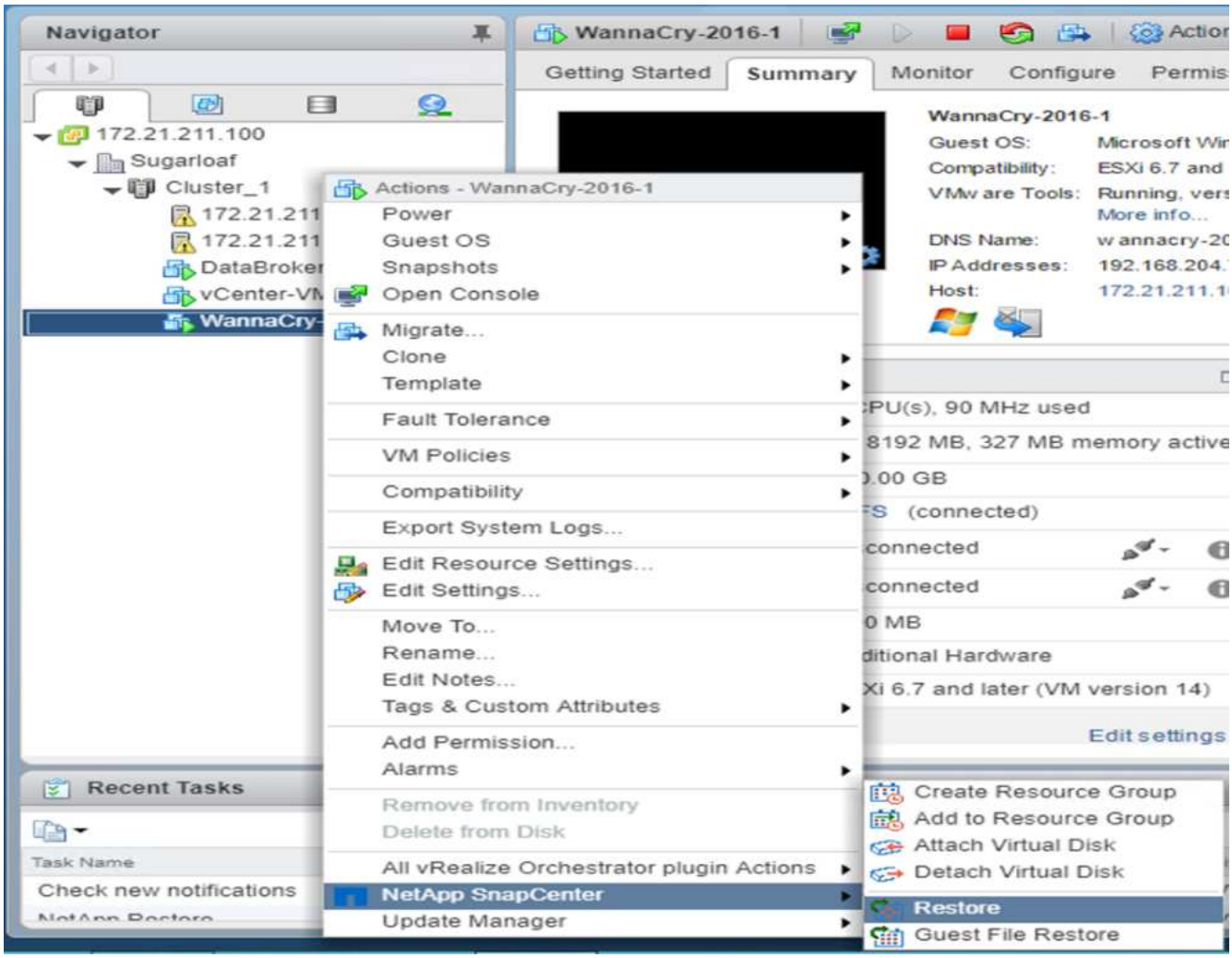
修正

攻撃の前に作成されたクリーンな Snapshot コピーを使用して、 VM およびマッピングされた CIFS 共有をリストアします。

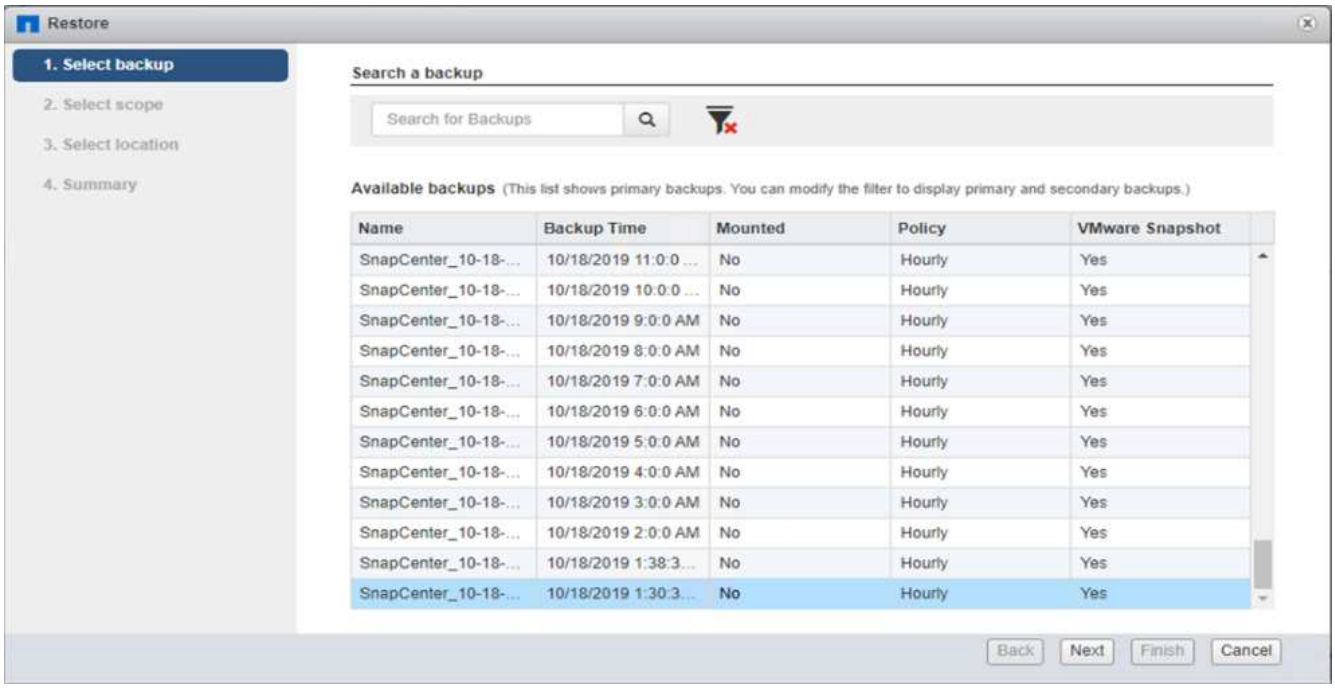
- リストア VM *

VM をリストアするには、次の手順を実行します。

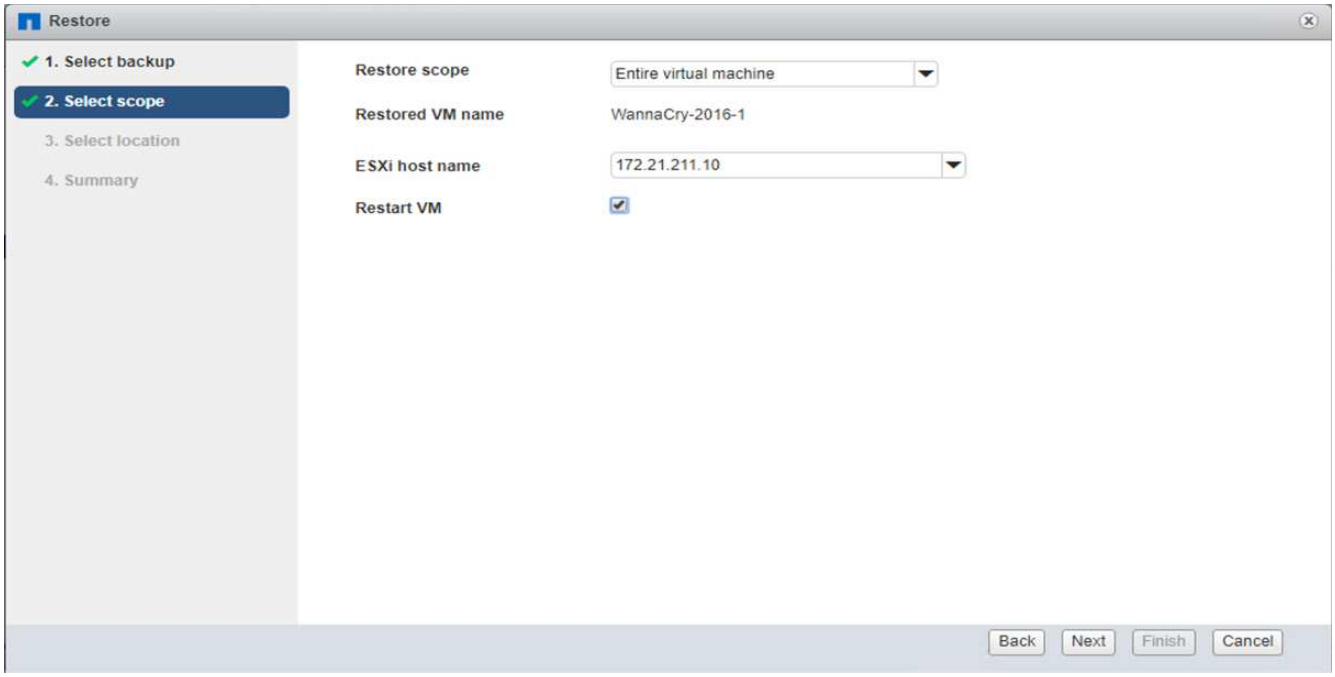
1. SnapCenter で作成した Snapshot コピーを使用して、 VM をリストアします。



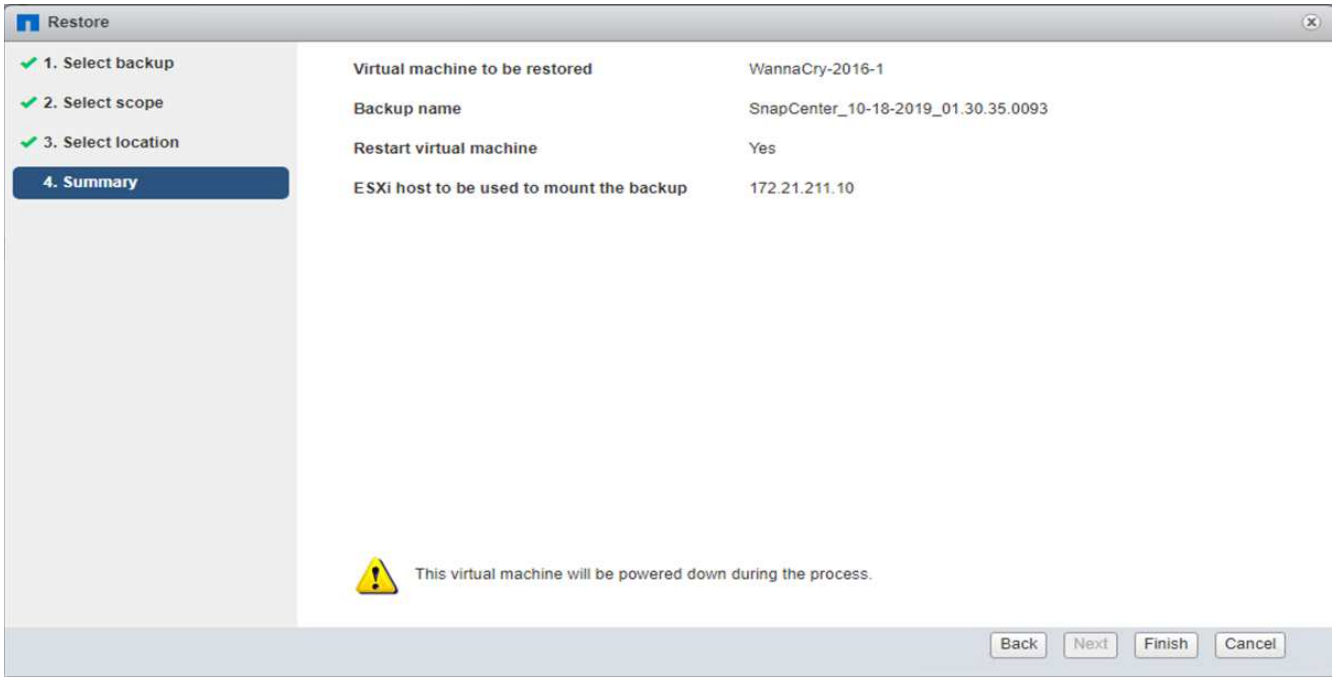
2. リストアに使用する VMware 整合性のある Snapshot コピーを選択します。



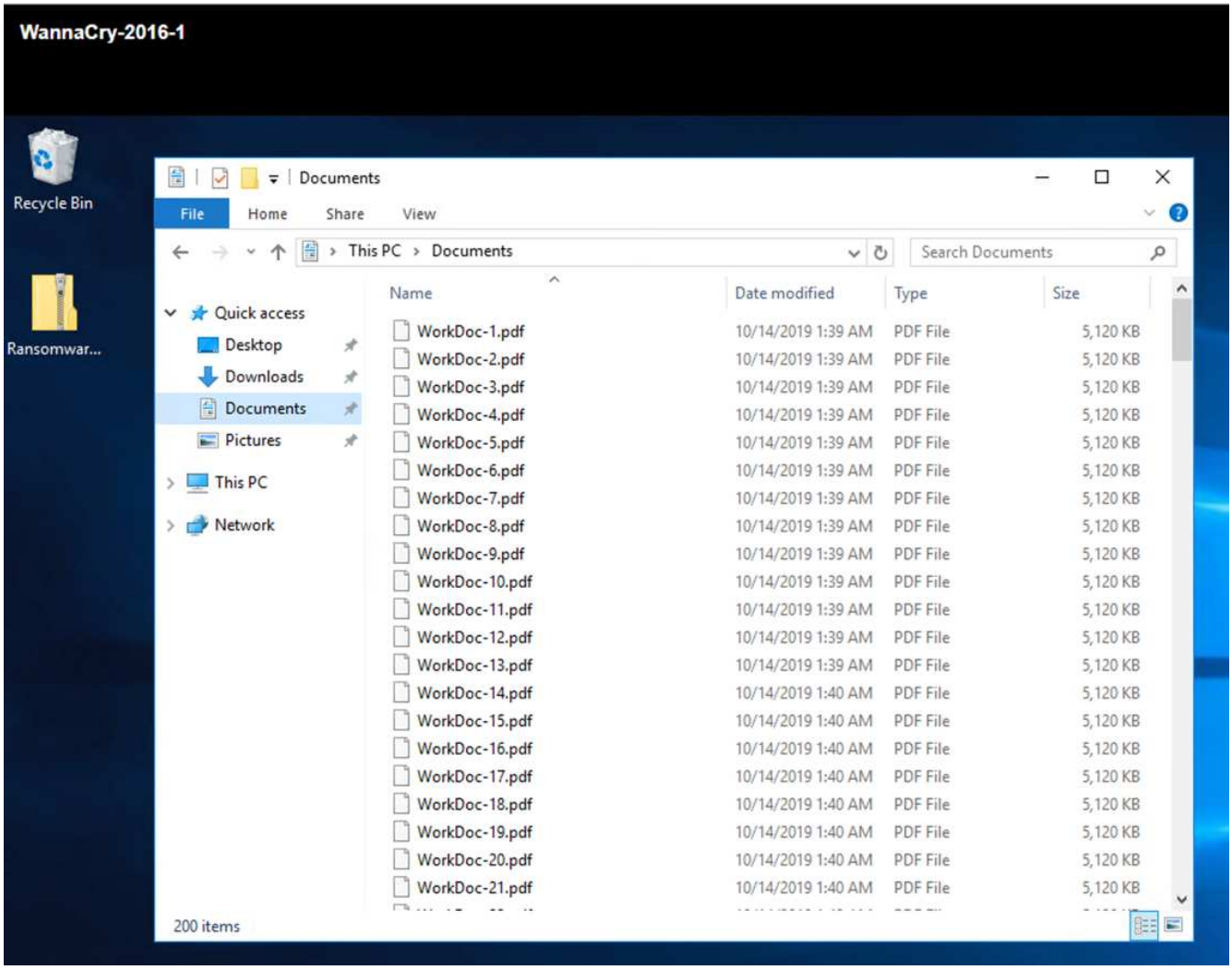
3. VM 全体がリストアされて再起動されます。



4. [完了] をクリックして、復元プロセスを開始します。



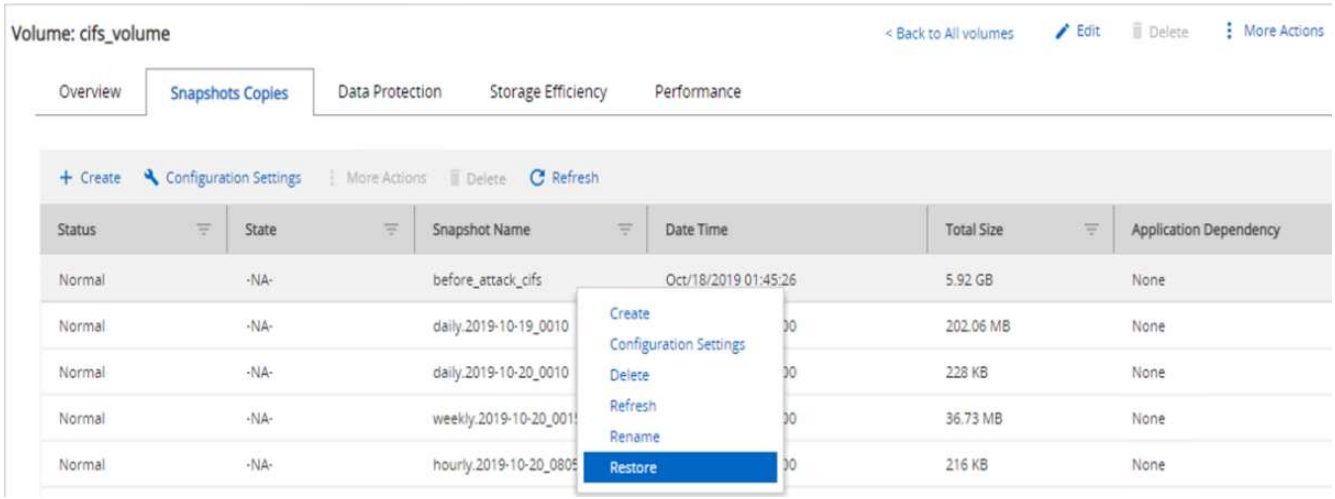
5. VM とそのファイルがリストアされます。



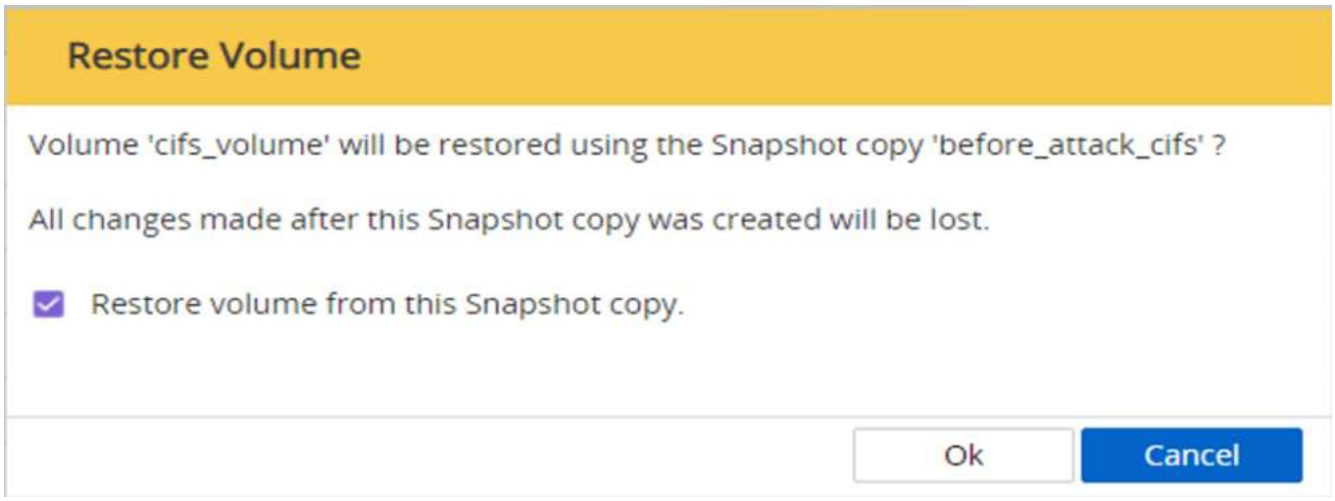
- CIFS 共有の復元 *

CIFS 共有をリストアするには、次の手順を実行します。

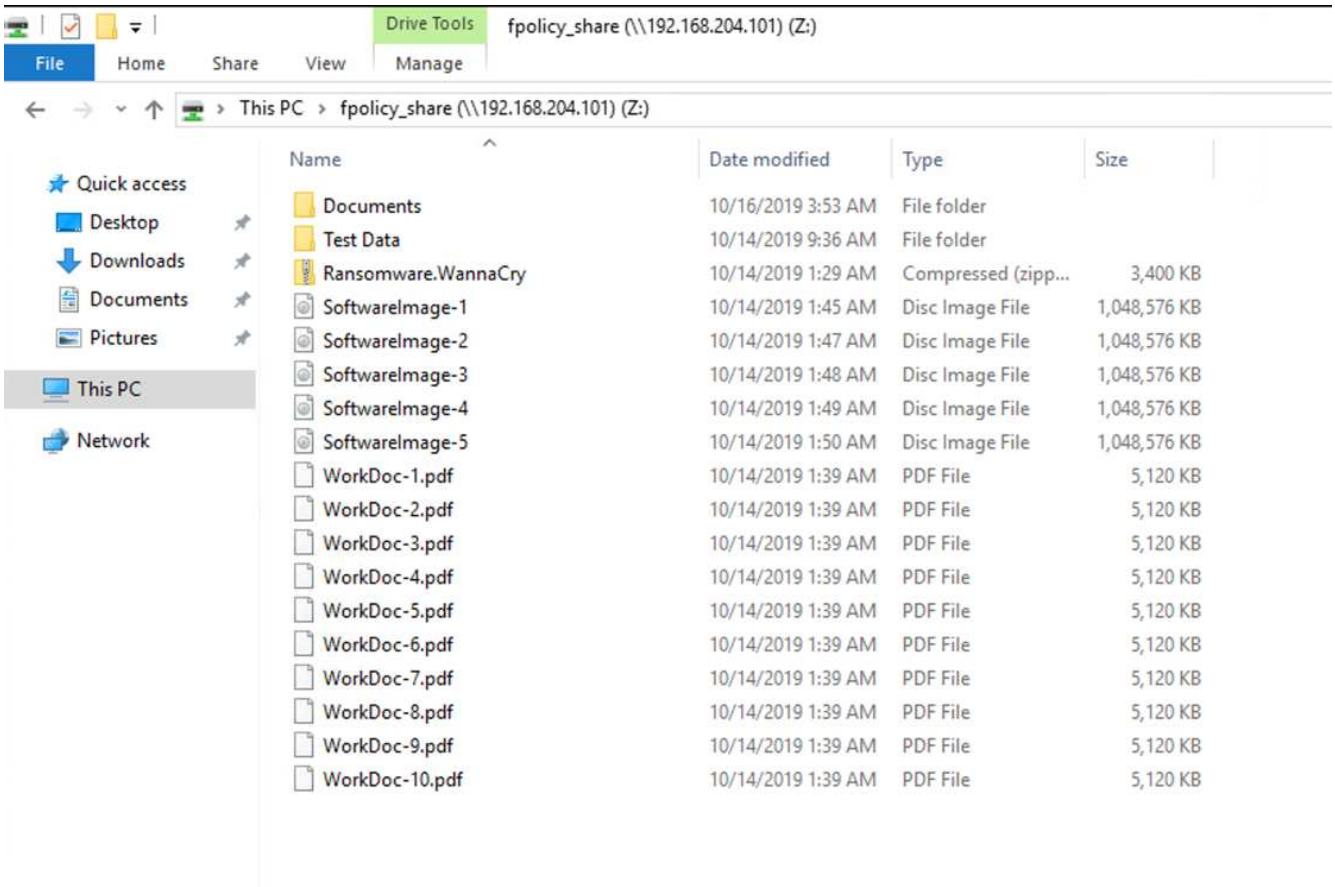
1. 攻撃の前に作成されたボリュームの Snapshot コピーを使用して、共有をリストアします。



2. [OK] をクリックしてリストア処理を開始します。



3. リストア後に CIFS 共有を表示する



ケース **2** ： **WannaCry** は **VM** 内のファイルシステムを暗号化し、 **FPolicy** で保護されているマッピングされた **CIFS** 共有を暗号化しようとします

防止

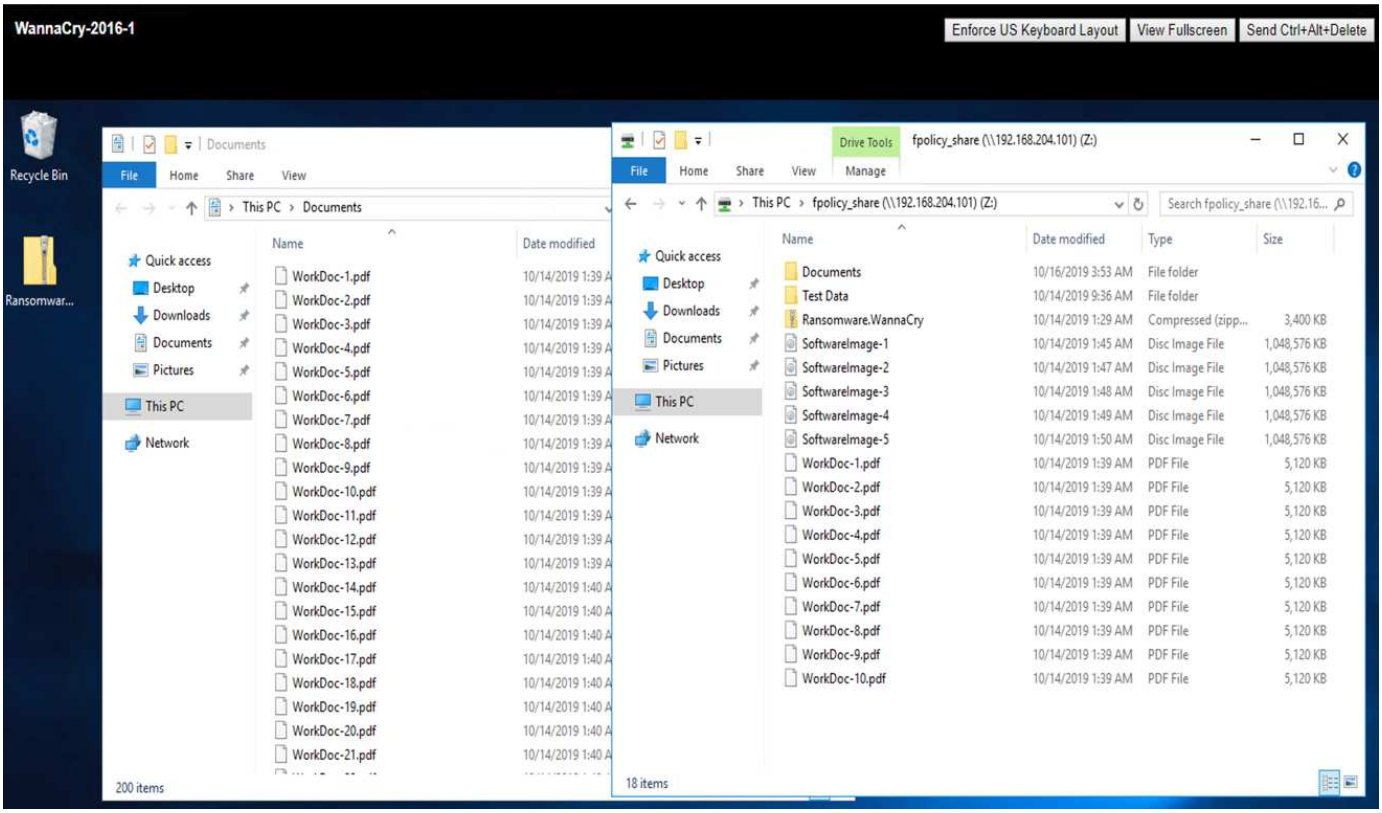
- FPolicy を設定 *

CIFS 共有に FPolicy を設定するには、 ONTAP クラスタで次のコマンドを実行します。

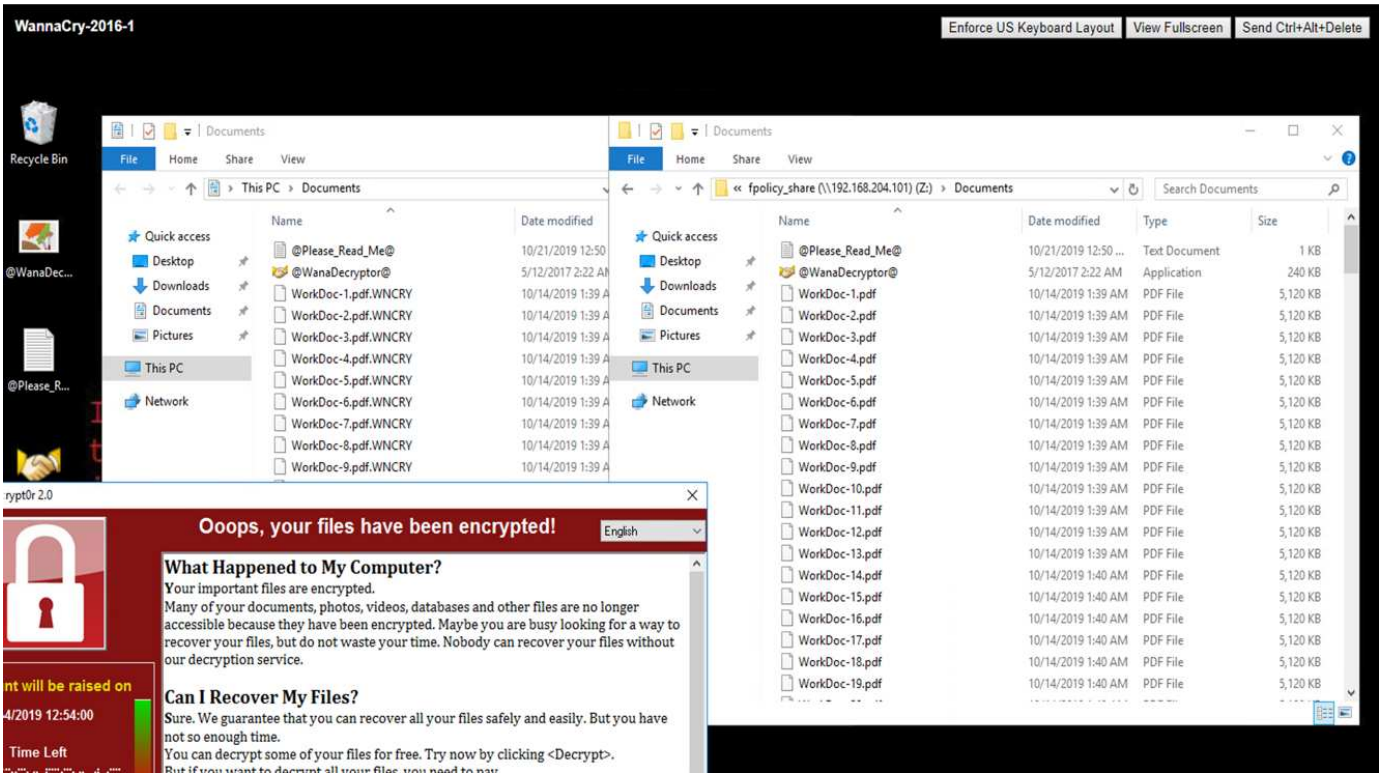
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

このポリシーでは、拡張子が WNCRY 、 Locky 、および ad4c のファイルは、ファイル操作の作成、名前変更、書き込み、または開くことができません。

攻撃前のファイルのステータスを表示します。ファイルは暗号化されておらず、クリーンなシステムにあります。



VM 上のファイルが暗号化されます。WannaCry マルウェアは CIFS 共有内のファイルの暗号化を試みますが、 FPolicy はファイルへの影響を防ぎます。



身代金を支払うことなく業務を継続

本ドキュメントで説明しているネットアップの機能は、攻撃を受けて数分以内にデータをリストアし、攻撃を未然に防ぐのに役立ちます。そのため、業務の中断を回避することができます。

Snapshot コピーのスケジュールは、目標復旧時点（ RPO ）を達成するように設定できます。Snapshot コピーベースのリストア処理は非常に高速なため、 RTO （目標復旧時間）は非常に低く抑えられます。

何よりも、攻撃の結果として身代金を支払わなくても、通常の運用にすばやく戻ることができます。

まとめ

ランサムウェアは組織犯罪の製品であり、攻撃者は倫理的に行動しません。身代金を受け取ったあとも、復号化の鍵を渡さないケースもあります。被害者は、データだけでなく多額の金銭も失うだけでなく、本番環境のデータ損失に伴う影響も被ることになります。

に従って "Forbes の記事です"では、身代金を支払ったあとにデータが戻ってくるのは、ランサムウェア攻撃者のわずか 19% です。そのため、攻撃が発生した場合に身代金を支払わないことを推奨します。金銭的な金銭的価値を提供することで、攻撃者のビジネスモデルに対する信頼が強化されます。

データのバックアップとリストアは、ランサムウェアからのリカバリの重要な要素です。そのため、ビジネス計画の不可欠な要素として含める必要があります。攻撃が発生した場合に復旧機能に妥協がないように、これらのオペレーションの実装には予算を割り当てる必要があります。

重要なのは、このプロセスで適切なテクノロジパートナーを選択することです。 FlexPod は、オールフラッシュ FAS システムで追加コストを発生させることなく、必要な機能のほとんどをネイティブに提供します。

謝辞

このドキュメントの作成にあたり、以下の方々のご協力に感謝します。

- ネットアップ、 Jorge Gomez Navarrete 氏
- ネットアップ、 Ganesh Kamath

追加情報

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。

- NetApp Snapshot ソフトウェア

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- SnapCenter によるバックアップ管理

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- SnapLock によるデータコンプライアンス

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- ネットアップの製品マニュアル

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco Advanced Malware Protection （ AMP ）

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco StealthWatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

医療機関向けの **FIPS 140-2** セキュリティ準拠の **FlexPod** 解決策

TR-4892 ：『 FIPS 140-2 security Compliant FlexPod 解決策 **for HealthCare** 』

Cisco 、 NetApp John McAbel 、 JayaKishore Esanakula 氏

経済・臨床医療法（ HITECH ）の医療情報技術には、 Federal Information Processing Standard （ FIPS ） 140-2 認証済みの電子保護医療情報（ ePHI ）暗号化が必要です。ヘルス情報テクノロジ（ HIT ）アプリケーションおよびソフトウェアは、相互運用性プログラム（旧称は有意義な使用インセンティブプログラム）認定を取得するために FIPS 140-2 に準拠している必要があります。対象となるプロバイダーおよび病院は、メディケアおよびメディケイドインセンティブを受けるために FIPS 140-2 （レベル 1 ）に準

拠した HIT を使用し、メディケアおよびメディケイドセンター（ CMS ）からの払い戻しペナルティを回避する必要があります。FIPS 140-2 認定暗号化アルゴリズムは、に求められる技術的な保護手段として認定されています "セキュリティルール" Health Information Portability and Accountability Act （ HIPAA ：医療情報の相互運用性と説明責任に関する法律）。

FIPS 140-2 は、米国機密情報を保護するハードウェア、ソフトウェア、およびファームウェアの暗号モジュールのセキュリティ要件を設定する政府標準。米国では、この規格への準拠が義務付けられていますまた、金融サービスや医療などの規制産業でもよく使用されています。本テクニカルレポートでは、 FIPS 140-2 のセキュリティ標準を高水準で理解する方法を紹介します。また、医療機関が直面しているさまざまな脅威を理解するのにも役立ちます。最後に、このテクニカルレポートでは、 FIPS 140-2 準拠の FlexPod システムを使用して FlexPod コンバージドインフラに導入した医療資産を保護する方法について説明します。

適用範囲

このドキュメントは、 FIPS 140-2 のセキュリティコンプライアンスを必要とする 1 つ以上の医療 IT アプリケーションやソリューションをホスティングするための、 Cisco Unified Computing System （ Cisco UCS ）、 Cisco Nexus 、 Cisco MDS 、および NetApp ONTAP ベースの FlexPod インフラの技術概要をまとめたものです。

対象者

本ドキュメントは、医療業界の技術リーダー、 Cisco とネットアップのパートナーソリューションエンジニア、およびプロフェッショナルサービス担当者を対象としています。本ドキュメントは、コンピューティングとストレージのサイジングの概念に加え、医療の脅威、医療セキュリティ、医療 IT システム、 Cisco UCS 、ネットアップストレージシステムに関する技術的な知識があることを前提としています。

"次は、医療業界におけるサイバーセキュリティの脅威です。"

医療業界におけるサイバーセキュリティの脅威

"前へ：はじめに。"

問題が発生するたびに、新型コロナウイルス感染症の流行により、このような機会の一例が提示されます。に従って "レポート" 新型コロナウイルス感染症対策は、米保健福祉省（ HHS ）サイバーセキュリティプログラムによってランサムウェア攻撃の数が増加したことに起因しています。2020 年 3 月第 3 週に 6,000 の新しいインターネット・ドメインが登録されました。ドメインの 50% 以上がマルウェアをホストしています。ランサムウェア攻撃は、 2020 年に医療データの侵害が発生し、 630 を超える医療機関と約 2,900 万件の医療記録に影響を及ぼしています。19 人のレイカー / サイトがこの伸長率を倍増させた。医療業界では、 2020 年にデータ侵害が最も多かったのは 24.5% です。

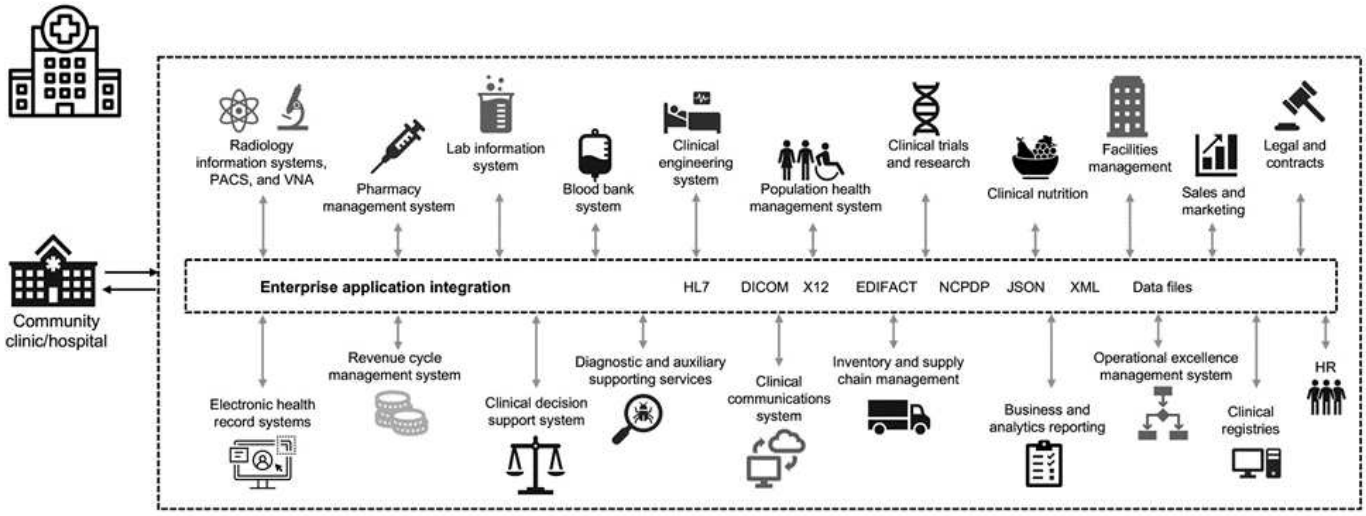
悪意のあるエージェントは、情報を販売するか、破壊または暴露を脅かして、保護された健康情報（ PHI ）のセキュリティおよびプライバシーを侵害しようとしました。ターゲットと大量ブロードキャストの試行は、ePHI への不正アクセスを得るために頻繁に行われます。2020 年後半の患者記録のうち、約 75% がビジネス関係者の侵害によるものでした。

次のリストの医療機関は、悪意のあるエージェントの標的になっていました。

- 病院システム

- ライフサイエンスラボ
- 研究室
- リハビリテーション施設
- 地域の病院や診療所

医療機関を構成するアプリケーションの多様性は否定できず、複雑さもますます増大しています。情報セキュリティ・オフィスは ' 膨大な IT システムと資産のガバナンスを提供するという課題に直面しています次の図は、一般的な病院システムの臨床的能力を示しています。



患者データはこの画像の中心にあります。患者データの消失と、デリケートな医療条件に関連する病状の消失は非常に現実的です。その他の重要な問題には、社会的排除、ブラックリスト、プロファイリング、ターゲットマーケティングの脆弱性、不正利用、支払者の権限を超えた医療情報に関する支払者に対する潜在的な金銭的責任などがあります。

医療への脅威は、本質的に多次元的なものであり、影響を及ぼします。世界各国の政府は、 ePHI を保護するためにさまざまな規定を制定しました。医療への脅威の悪影響と進化する性質により、医療機関はすべての脅威を防御することが困難になります。

以下に、医療業界で特定されている一般的な脅威のリストを示します。

- ランサムウェア攻撃
- 機密情報を含む機器またはデータの紛失または盗難
- フィッシング攻撃
- 患者の安全性に影響を与える可能性のある、接続された医療機器に対する攻撃
- 電子メールによるフィッシング攻撃
- 機器またはデータの紛失または盗難
- リモートデスクトッププロトコルの妥協
- ソフトウェアの脆弱性

医療機関は、デジタルエコシステムと同様に複雑な法的規制の環境で運用されています。この環境には、以下が含まれますが、これらに限定されません。

- 国立コーディネータオフィス（医療技術担当） ONC 認定電子医療情報技術相互運用性標準
- Medicare アクセスおよび子供の健康保険プログラムの再認可法 (MACRA) / 有意義な使用
- 食品医薬品局（ FDA ）に基づく複数の義務
- 共同委員会認定プロセス
- HIPAA の要件
- Hitch の要件
- 支払者の最低許容リスク基準
- プライバシーとセキュリティのルールを記述します
- 連邦情報セキュリティの近代化法の要件は、米国立衛生研究所などの機関を通じて、連邦政府との契約および研究助成金に組み込まれています
- クレジットカード業界の データ セキュリティ 標準 (PCI-DSS)
- 薬物乱用および精神保健管理（ SAMHSA ）の要件
- 金融処理法「 Gramm-Leach-Bliley Act
- 関連組織へのサービス提供に関するスターク法
- 高等教育に参加する機関向けの Family Educational Rights and Privacy Act （ FERPA ）
- 遺伝情報差別禁止法（ GINA ）
- 欧州連合の新しい一般データ保護規則（ GDPR ）

セキュリティアーキテクチャ標準は急速に進化しており、悪意のある攻撃者が医療情報システムに影響を与えないようになっています。その 1 つが FIPS 140-2 であり、 National Institute of Standards and Technology （ NIST ；米国標準技術研究所）で定義されています。FIPS 140-2 では、米国政府が詳しく公開されています政府による暗号モジュールの要件セキュリティ要件は、暗号モジュールの安全な設計および実装に関連する領域を対象としており、 HIT に適用できます。適切に定義された暗号化境界により、暗号モジュールを最新の状態に保ちながら、セキュリティ管理を容易にすることができます。これらの境界は、悪意のある攻撃者によって簡単に悪用される可能性のある暗号モジュールの脆弱性を防止するのに役立ちます。また、標準の暗号モジュールを管理するときに人為的ミスを防止することもできます。

NIST と Communications Security Establishment （ CSE ）は、 FIPS 140-2 認定レベルの暗号モジュールを認定する暗号モジュール検証プログラム（ CMVP ）を設立しました。FIPS 140-2 認定モジュールを使用する場合、連邦政府機関は、移動中だけでなく保管中も機密データや重要なデータを保護する必要があります。多くの医療システムでは、機密情報や貴重な情報を保護することが成功したため、 FIPS 140-2 暗号化モジュールを使用して、法的に必要な最低限のセキュリティレベルを超えて ePHI を暗号化することを選択しています。

FlexPod の FIPS 140-2 機能の活用と実装にかかる時間は、数日から数時間です。FIPS に準拠するようになることは、規模に関係なく、ほとんどの医療機関に求められる範囲内です。明確に定義された暗号化の境界と、十分に文書化されたシンプルな実装手順により、 FIPS 140-2 準拠の FlexPod アーキテクチャは、インフラストラクチャの強固なセキュリティ基盤を確立し、シンプルな拡張機能によってセキュリティ上の脅威に対する保護をさらに強化できます。

"次の例は、 FIPS 140-2 の概要を示しています。"

FIPS 140-2 の概要

"前の記事：医療業界におけるサイバーセキュリティの脅威。"

"FIPS 140-2" コンピュータおよび通信システムの機密情報を保護するセキュリティシステム内で使用される暗号モジュールのセキュリティ要件を指定します。暗号モジュールは、ハードウェア、ソフトウェア、ファームウェア、またはその組み合わせのセットである必要があります。FIPS 環境 暗号化アルゴリズム、キー生成、および暗号化境界内に含まれるキー管理ツール。FIPS 140-2 は、製品、アーキテクチャ、データ、エコシステムではなく、暗号モジュールに適用される点に注意してください。暗号モジュールは、このドキュメントで後述する重要な用語で定義されており、承認されたセキュリティ機能を実装する特定のコンポーネント（ハードウェア、ソフトウェア、ファームウェアのいずれか）です。また、 FIPS 140-2 では 4 つのレベルが規定されています。承認された暗号化アルゴリズムは、すべてのレベルで共通です。各セキュリティレベルの主な要素と要件は次のとおりです。

- * セキュリティレベル 1 *
  - 暗号モジュールの基本的なセキュリティ要件を指定します（少なくとも 1 つの承認されたアルゴリズムまたはセキュリティ機能が必要です）。
  - レベル 1 には、本番グレードのコンポーネントの基本要件を超える物理的なセキュリティメカニズムは必要ありません。
- * セキュリティレベル 2 *
  - コーティングやシール、取り外し可能なカバーや暗号モジュールのドアのロックなどの不正開封防止ソリューションを使用して、改ざん防止の要件を追加することで、物理的なセキュリティメカニズムを強化します。
  - 少なくとも、ロールベースアクセスコントロール（ RBAC ）が必要です。この RBAC では、暗号化モジュールがオペレータまたは管理者の許可を認証して、特定のロールを引き受け、対応する一連の機能を実行します。
- * セキュリティレベル 3 *
  - レベル 2 の不正改ざん防止要件を基に構築され、暗号化モジュール内の重要なセキュリティパラメータ（ CSP ）へのアクセスを防止しようとします。
  - レベル 3 で必要とされる物理的なセキュリティメカニズムは、物理的なアクセス、または暗号モジュールの使用または変更の試みを検出して応答する可能性が高いことを目的としています。たとえば、強力なエンクロージャ、改ざん検出、応答回路などがあり、暗号モジュールの取り外し可能なカバーを開いたときにすべてのプレーンテキスト CSP をゼロにします。
  - レベル 2 で指定された RBAC メカニズムのセキュリティを強化するために、 ID ベースの認証メカニズムが必要です。暗号モジュールは、オペレータの ID を認証し、オペレータが役割を使用して役割の機能を実行する権限を持っていることを確認します。
- * セキュリティレベル 4 *
  - FIPS 140-2 で最高レベルのセキュリティ。
  - 物理的に保護されていない環境での処理に最も有効なレベルです。
  - このレベルでは、物理的なセキュリティメカニズムは、物理的なアクセスでの不正な試みを検出して応答する責任を持つ、暗号モジュールに関する完全な保護を提供することを目的としています。
  - 暗号モジュールの侵入や露出は検出の可能性が高く、セキュアでない CSP やプレーンテキスト CSP がすべて初期化される可能性が高くなります。

"次に、コントロールプレーンとデータプレーンを比較します。"

コントロールプレーンとデータプレーンの比較

"以前： FIPS 140-2 の概要。"

FIPS 140-2 戦略を実装する場合は、保護対象を理解することが重要です。これは、コントロールプレーンとデータプレーンの 2 つの領域に簡単に分割できます。コントロールプレーンとは、ネットアップストレージコントローラ、 Cisco Nexus スイッチ、 Cisco UCS サーバへの管理アクセスなど、 FlexPod システム内のコンポーネントの制御と運用に影響する要素のことです。このレイヤでの保護は、管理者がデバイスへの接続や変更を行うために使用できるプロトコルと暗号化暗号化暗号化暗号化方式を制限することによって提供されます。データプレーンとは、 FlexPod システム内の PHI などの実際の情報を指します。これは、保存データを暗号化することで保護されます。 FIPS では、使用中の暗号モジュールが標準に準拠していることを確認できます。

"次に、 FlexPod の Cisco UCS コンピューティングと FIPS 140-2 を実行します。"

FlexPod Cisco UCS のコンピューティングと FIPS 140-2

"前：コントロールプレーンとデータプレーンの比較。"

FlexPod アーキテクチャは、 FIPS 140-2 に準拠した Cisco UCS サーバを使用して設計できます。米国に準拠しています…NIST 、 Cisco UCS サーバは、 FIPS 140-2 レベル 1 準拠モードで動作します。FIPS 準拠の Cisco コンポーネントの一覧については、を参照してください "シスコの FIPS 140 ページ"。Cisco UCS Manager は FIPS 140-2 認定済みです。

Cisco UCS とファブリックインターコネクト

Cisco UCS Manager は、 Cisco Fabric Interconnect （ FI ）から導入され、実行されます。

Cisco UCS および FIPS を有効にする方法の詳細については、を参照してください "Cisco UCS Manager のマニュアル"。

各ファブリック A および B で Cisco ファブリックインターコネクト上で FIPS モードをイネーブルにするには、次のコマンドを実行します。

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

> Cisco UCS Manager Release 3.2(3) より前のリリースのクラスタの FI を FI に置き換えるには、交換用の FI をクラスタに追加する前に、既存の FI で FIPS モードをディセーブル（「 FIPS-mode 」をディセーブル）にします。クラスタが形成されると、 Cisco UCS Manager のブートアップの一環として、 FIPS モードが自動的に有効になります。

シスコは、コンピューティングまたはアプリケーションレイヤに実装可能な次の主要製品を提供しています。

- * エンドポイント向けの Cisco Advanced Malware Protection （ AMP ）。 * Microsoft Windows および Linux オペレーティングシステムでサポートされているこの解決策 は、防止、検出、および応答機能を統合しています。このセキュリティソフトウェアは、セキュリティ侵害の防止、侵入ポイントでのマルウェアのブロック、ファイルおよびプロセスのアクティビティの継続的な監視と分析を行い、フロントライン防御を回避できる脅威を迅速に検出、阻止、修復します。AMP の Malicious Activity Protection （ MAP ）コンポーネントは、すべてのエンドポイントアクティビティを継続的に監視し、エンドポイント上の実行中のプログラムのランタイム検出と異常な動作のブロックを提供します。たとえば、エンドポイントの動作がランサムウェアを示している場合、攻撃の原因となっているプロセスは終了し、エンドポイントの暗号化を防ぎ、攻撃を停止します。
- * 電子メールセキュリティのための AMP 。 * 電子メールはマルウェアを拡散させ、サイバー攻撃を実行するための主要な手段となっています。平均して、 1 日に約 1 、 000 億通の電子メールが交換されます。これにより、攻撃者はユーザーのシステムに非常に優れた侵入ベクトルを与えることができます。そのため、この種の攻撃を防御することは絶対に不可欠です。AMP は、ゼロデイ攻撃や悪意のある添付ファイルに隠された不潔なマルウェアなどの脅威を電子メールで分析します。また、業界をリードする URL インテリジェンスを使用して、悪意のあるリンクに対抗します。スピアフィッシング、ランサムウェア、その他の高度な攻撃から高度な保護を提供します。
- * 次世代侵入防御システム（ NGIPS ）。 * Cisco firepower NGIPS は、データセンターの物理アプライアンスとして、または VMware （ NGIPSv for VMware ）の仮想アプライアンスとして導入できます。この非常に効果的な侵入防御システムは、信頼性の高いパフォーマンスと低い総所有コストを実現します。オプションのサブスクリプションライセンスで脅威からの保護を拡張して、 AMP 、アプリケーションの可視化と制御、および URL フィルタリング機能を提供できます。仮想化された NGIPS は、仮想マシン（ VM ）間のトラフィックを検査し、リソースが限られたサイトで NGIPS ソリューションの導入と管理を容易にして、物理資産と仮想資産の両方の保護を強化します。

"次のセクションでは、 FlexPod のシスコネットワークと FIPS 140-2 について説明します。"

FlexPod シスコのネットワークおよび FIPS 140-2

"前のリリース： FlexPod Cisco UCS のコンピューティングと FIPS 140-2"

Cisco MDS

ソフトウェア 8.4.x を搭載した Cisco MDS 9000 シリーズプラットフォームは、です "FIPS 140-2 に準拠しています"。Cisco MDS は、 SNMPv3 および SSH 用の暗号モジュールおよび次のサービスを実装しています。

- 各サービスをサポートするセッション確立
- 各サービスの主要な派生機能をサポートする、基盤となるすべての暗号化アルゴリズム
- 各サービスのハッシュ化
- 各サービスの対称暗号化

FIPS モードをイネーブルにする前に、 MDS スイッチで次の作業を実行します。

1. パスワードは 8 文字以上にする必要があります。
2. Telnet を無効にします。ユーザは SSH のみを使用してログインする必要があります。
3. RADIUS/TACACS+ によるリモート認証をディセーブルにします。認証できるのは、スイッチに対してローカルなユーザだけです。
4. SNMP v1 および v2 を無効にします。SNMPv3 用に設定されたスイッチ上の既存のユーザアカウントは、認証に SHA 、プライバシーには AES/3DES だけを設定する必要があります。

5. VRRP を無効にします。
6. 認証用の MD5 または暗号化用の DES を持つすべての IKE ポリシーを削除します。認証に SHA を使用し、暗号化に 3DES/AES を使用するようにポリシーを変更します。
7. すべての SSH Server RSA1 キーペアを削除します。

MDS スイッチで FIPS モードを有効にして FIPS ステータスを表示するには、次の手順を実行します。

1. FIPS のステータスを表示します。

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 2048 ビットの SSH キーを設定します。

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. FIPS モードを有効にする。

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. FIPS のステータスを表示します。

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. コンフィギュレーションを実行コンフィギュレーションに保存します。

```
MDSSwitch(config)# copy ru st
[##########################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. MDS スイッチを再起動します

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. FIPS のステータスを表示します。

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

詳細については、を参照してください "FIPS モードの有効化"。

Cisco Nexus の場合

Cisco Nexus 9000 シリーズスイッチ（バージョン 9.3 ）はです "FIPS 140-2 に準拠しています"。Cisco Nexus は、 SNMPv3 および SSH の暗号モジュールと次のサービスを実装します。

- 各サービスをサポートするセッション確立
- 各サービスの主要な派生機能をサポートする、基盤となるすべての暗号化アルゴリズム

- 各サービスのハッシュ化
- 各サービスの対称暗号化

FIPS モードを有効にする前に、 Cisco Nexus スイッチで次の作業を実行します。

1. Telnet を無効にします。ユーザは Secure Shell （ SSH ）のみを使用してログインする必要があります。
2. SNMPv1 および v2 を無効にします。SNMPv3 用に設定されたデバイス上の既存のユーザアカウントは、認証に SHA 、プライバシーには AES/3DES だけを設定する必要があります。
3. すべての SSH サーバ RSA1 キー・ペアを削除します
4. Cisco TrustSec セキュリティアソシエーションプロトコル（ SAP ）ネゴシエーション中に使用する HMAC-SHA1 メッセージ整合性チェック（ MIC ）をイネーブルにします。これを行うには、「 cts-manual' 」または「 cts-dot1x' 」モードから sap hash-calgorithm「 HMAC-sha-1 」コマンドを入力します。

Nexus スイッチで FIPS モードを有効にするには、次の手順を実行します。

1. 2048 ビットの SSH 鍵を設定します。

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 2048 ビットの SSH キーを設定します。

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. FIPS モードを有効にする。

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Nexus スイッチを再起動します。

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. FIPS のステータスを表示します。

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

さらに、 Cisco NX-OS ソフトウェアは、ネットワーク異常およびセキュリティの検出を強化する NetFlow 機能をサポートしています。NetFlow は、ネットワーク上のすべてのカンバセーション、通信に関係する側、使用されているプロトコル、およびトランザクションの期間のメタデータをキャプチャします。情報を集約して分析すると、正常な動作に関する洞察を得ることができます。収集されたデータを使用すると、疑わしいアクティビティのパターンを識別することもできます。たとえば、マルウェアがネットワーク全体に拡散し、これが気付かない場合があります。NetFlow では、フローを使用してネットワークモニタリングの統計情報を提供します。フローは、送信元インターフェイス（または VLAN ）に着信し、キーの値が同じパケットの単方向ストリームです。キーは、パケット内のフィールドの識別された値です。フローレコードを使用してフローを作成し、フローに固有のキーを定義します。フローエクスポータを使用して、 Cisco StealthWatch などのリモート NetFlow コレクタに NetFlow が収集するデータをエクスポートできます。StealthWatch では、この情報を使用してネットワークを継続的に監視し、ランサムウェアの発生が発生した場合にリアルタイムの脅威検出およびインシデント応答フォレンジックを提供します。

"次のセクションでは、 FlexPod の ONTAP ストレージと FIPS 140-2 について説明します。"

FlexPod の NetApp ONTAP ストレージと FIPS 140-2

"前のリリース： FlexPod のシスコネットワークと FIPS 140-2"

ネットアップは、さまざまなハードウェア、ソフトウェア、サービスを提供しています。これらのサービスには、この標準で検証済みの暗号モジュールのさまざまなコンポーネントを含めることができます。そのため、ネットアップでは、コントロールプレーンとデータプレーンに関して、 FIPS 140-2 への準拠にさまざまなアプローチを採用しています。

- ネットアップが提供する暗号モジュールには、転送中のデータと保管中のデータの暗号化についてレベル 1 の検証を実施した暗号モジュールが含まれています。
- ネットアップは、これらのコンポーネントのサプライヤによって FIPS 140-2 認定を受けたハードウェアモジュールとソフトウェアモジュールの両方を取得します。たとえば、 NetApp Storage Encryption 解決策 は、 FIPS レベル 2 の検証済みドライブを利用します。
- ネットアップ製品では、製品や機能が検証の範囲外であっても、標準に準拠した検証済みモジュールを使用できます。たとえば、 NetApp Volume Encryption （ NVE ）は FIPS 140-2 に準拠しています。別途検証されるわけではありませんが、レベル 1 で検証済みの NetApp 暗号化モジュールが使用されます。ご使用のバージョンの ONTAP に対する準拠の詳細については、 FlexPod SME にお問い合わせください。
- NetApp Cryptographic モジュールは FIPS 140-2 レベル 1 に準拠しています *
- NetApp Cryptographic Security Module （ NCSM ）は FIPS 140-2 レベル 1 に準拠しています。
- ネットアップの自己暗号化ドライブは FIPS 140-2 レベル 2 に準拠しています *

ネットアップは、元の機器メーカー（ OEM ）が FIPS 140-2 認定を取得した自己暗号化ドライブ（ SED ）を購入しています。これらのドライブを求めるお客様は、注文時に SED を指定する必要があります。ドライブはレベル 2 で検証されます。次のネットアップ製品では、検証済み SED を利用できます。

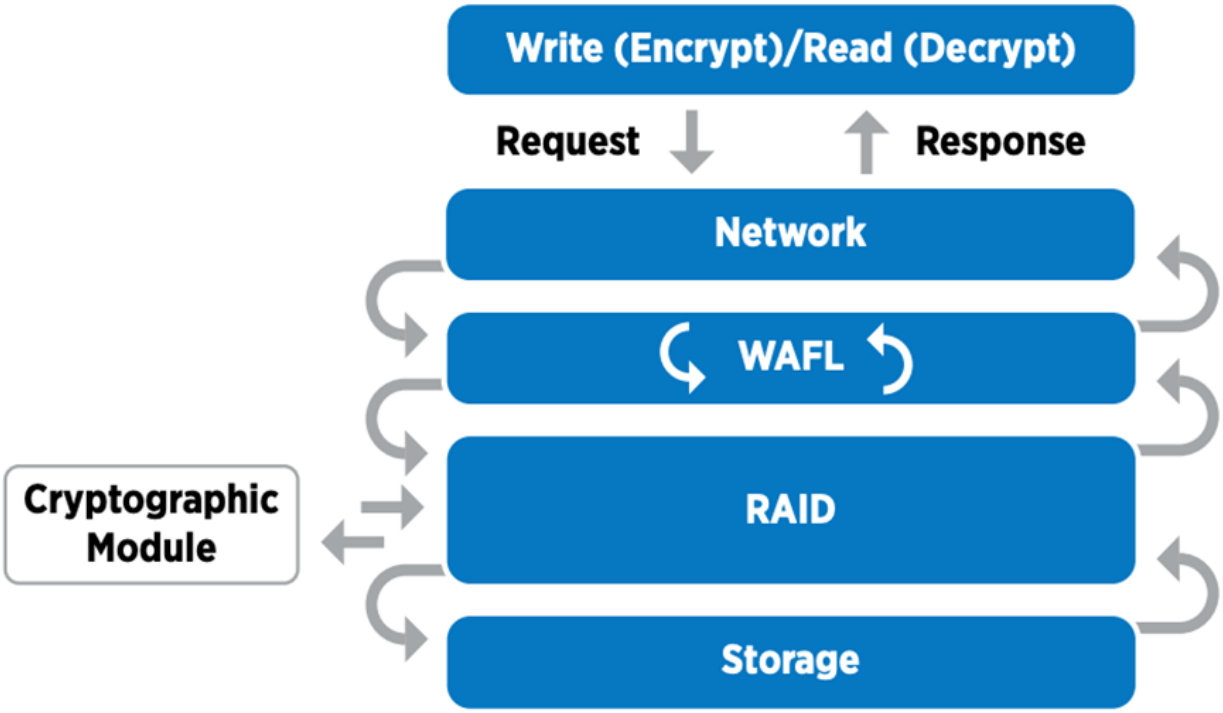
- AFF A シリーズおよび FAS ストレージシステム
- E シリーズおよび EF シリーズストレージシステム
- NetApp Aggregate Encryption および NetApp Volume Encryption *

NVE テクノロジと NetApp Aggregate Encryption （ NAE ）テクノロジを使用すると、ボリュームレベルとアグリゲートレベルでそれぞれデータを暗号化できるため、解決策 は物理ドライブに依存しません。

NVE は、 ONTAP 9.1 以降で使用可能なソフトウェアベースの保管データ暗号化解決策 で、 ONTAP 9.2 以降で FIPS 140-2 に準拠しています。NVE を使用すると、 ONTAP でボリュームごとにデータを暗号化して詳細に指定できます。NAE は ONTAP 9.6 で利用でき、 NVE の急成長です。 ONTAP は各ボリュームのデータを暗号化でき、ボリュームはアグリゲート全体でキーを共有できます。NVE と NAE はいずれも AES 256 ビット暗号化を使用します。データは、 SED を使用せずにディスクに保存することもできます。NVE および NAE を使用すると、暗号化が有効になっている場合でも Storage Efficiency 機能を使用できます。アプリケーションレイヤのみの暗号化では、 Storage Efficiency のすべてのメリットが損なわれています。NVE および NAE では、データがネットワークから NetApp WAFL を介して RAID レイヤに到着するため、ストレージ効率が維持されます。これにより、データを暗号化するかどうかが決まります。NAE では、ストレージ効率を高めるためにアグリゲート重複排除を使用できます。NVE ボリュームと NAE ボリュームは同じ NAE アグリゲート内で共存できます。NAE アグリゲートでは、暗号化されていないボリュームはサポートさ

プロセスの仕組みは次のとおりです。データが暗号化されると、 FIPS 140-2 レベル 1 認定の暗号化モジュールに送信されます。暗号モジュールはデータを暗号化して RAID レイヤに戻します。暗号化されたデータがデ

ィスクに送信されます。そのため、 NVE と NAE を組み合わせることで、データがディスクに転送される途中ですでに暗号化されています。読み取りは、逆のパスに従います。つまり、ディスクからのデータは暗号化された状態で RAID に送信され、暗号化モジュールによって復号化され、次の図に示すように、スタックの残りの部分が送信されます。



NVE は、 FIPS 140-2 レベル 1 に準拠したソフトウェア暗号化モジュールを使用します。

NVE の詳細については、を参照してください "NVE のデータシート"。

NVE でクラウド内のデータを保護する。Cloud Volumes ONTAP と Azure NetApp Files は、 FIPS 140-2 準拠の保存データ暗号化機能を提供できます。

ONTAP 9.7 以降では、 NVE ライセンスでオンボードまたは外部キー管理を使用すれば、新しく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。ONTAP 9.6 以降では、アグリゲートレベルの暗号化を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。アグリゲートに作成するボリュームはデフォルトで暗号化されます。このデフォルトの設定は、ボリュームを暗号化するときに無効にすることができます。

ONTAP NAE CLI コマンド

次の CLI コマンドを実行する前に、クラスタに必要な NVE ライセンスがあることを確認してください。

アグリゲートを作成して暗号化するには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行した場合）。

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

非 NAE アグリゲートを NAE アグリゲートに変換するには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行した場合）。

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

NAE アグリゲートを非 NAE アグリゲートに変換するには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行している場合）。

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

ONTAP NVE CLI コマンド

ONTAP 9.6 以降では、アグリゲートレベルの暗号化を使用して、暗号化するボリュームの包含アグリゲートにキーを割り当てることができます。アグリゲートに作成するボリュームはデフォルトで暗号化されます。

NAE が有効になっているアグリゲートでボリュームを作成するには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行した場合）。

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

ボリューム移動を行わずに既存ボリュームの「インプレース」暗号化を有効にするには、次のコマンドを実行します（ ONTAP 9.6 以降のクラスタ CLI で実行している場合）。

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

ボリュームで暗号化が有効になっていることを確認するには、次の CLI コマンドを実行します。

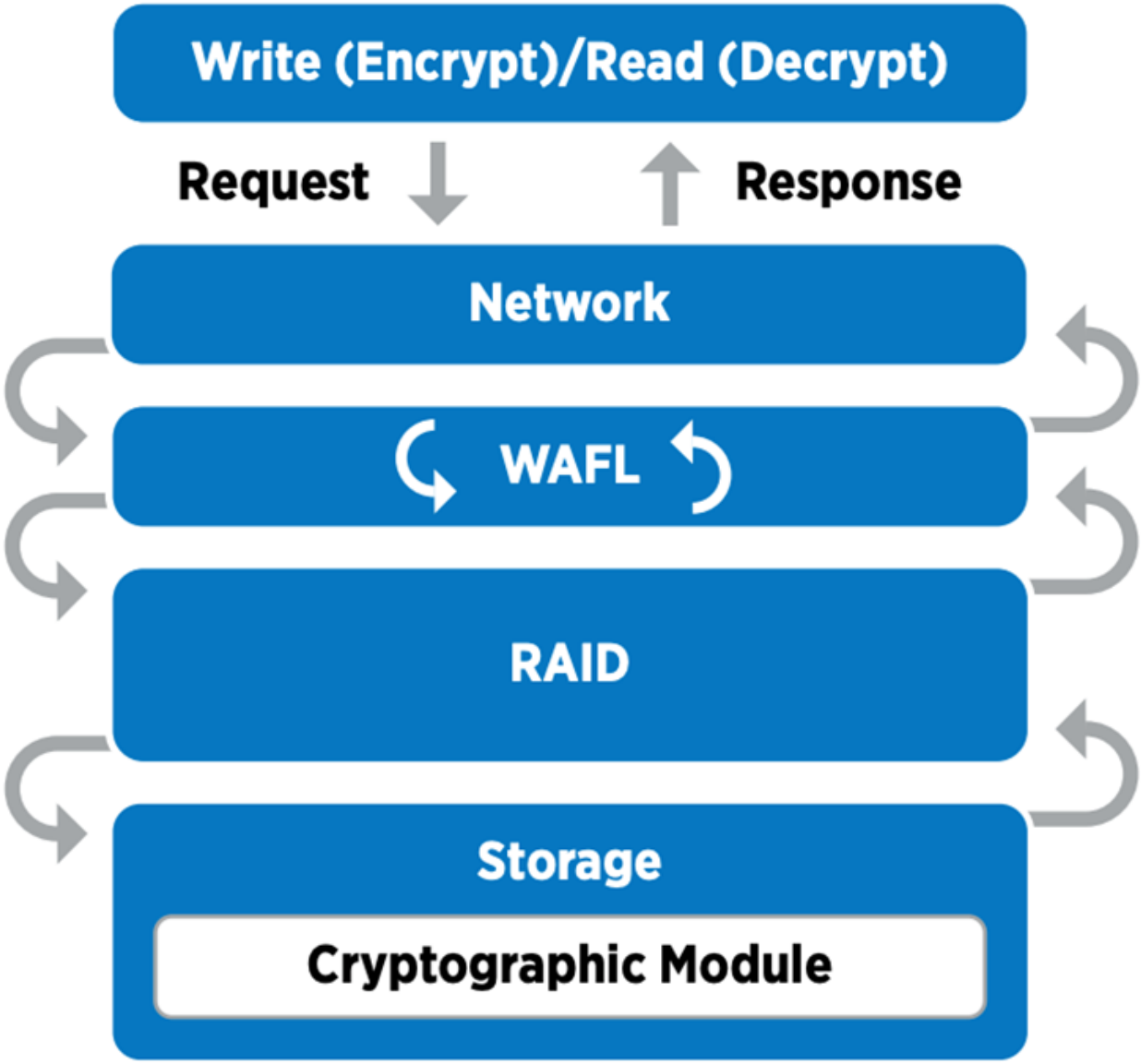
```
fp-health::> volume show -is-encrypted true
```

NSE の場合

NSE は、 SED を使用して、ハードウェアアクセラレーションメカニズムでデータ暗号化を実行します。

NSE は、 FIPS 140-2 レベル 2 自己暗号化ドライブを使用し、 AES 256 ビット透過的ディスク暗号化によって保存データを保護できるため、コンプライアンスの確保とスペアの返却が容易になります。ドライブは、暗

号化キーの生成を含め、次の図に示すように、すべてのデータ暗号化処理を内部的に実行します。データへの不正アクセスを防止するために、ストレージシステムは、ドライブの初回使用時に確立された認証キーを使用して、ドライブ自体を認証する必要があります。



NSE は、各ドライブでハードウェア暗号化を使用します。 FIPS 140-2 レベル 2 認定済みです。

NSE の詳細については、を参照してください "NSE のデータシート"。

キー管理

FIPS 140-2 規格は、次の図に示すように、境界によって定義された暗号モジュールを環境 にします。

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

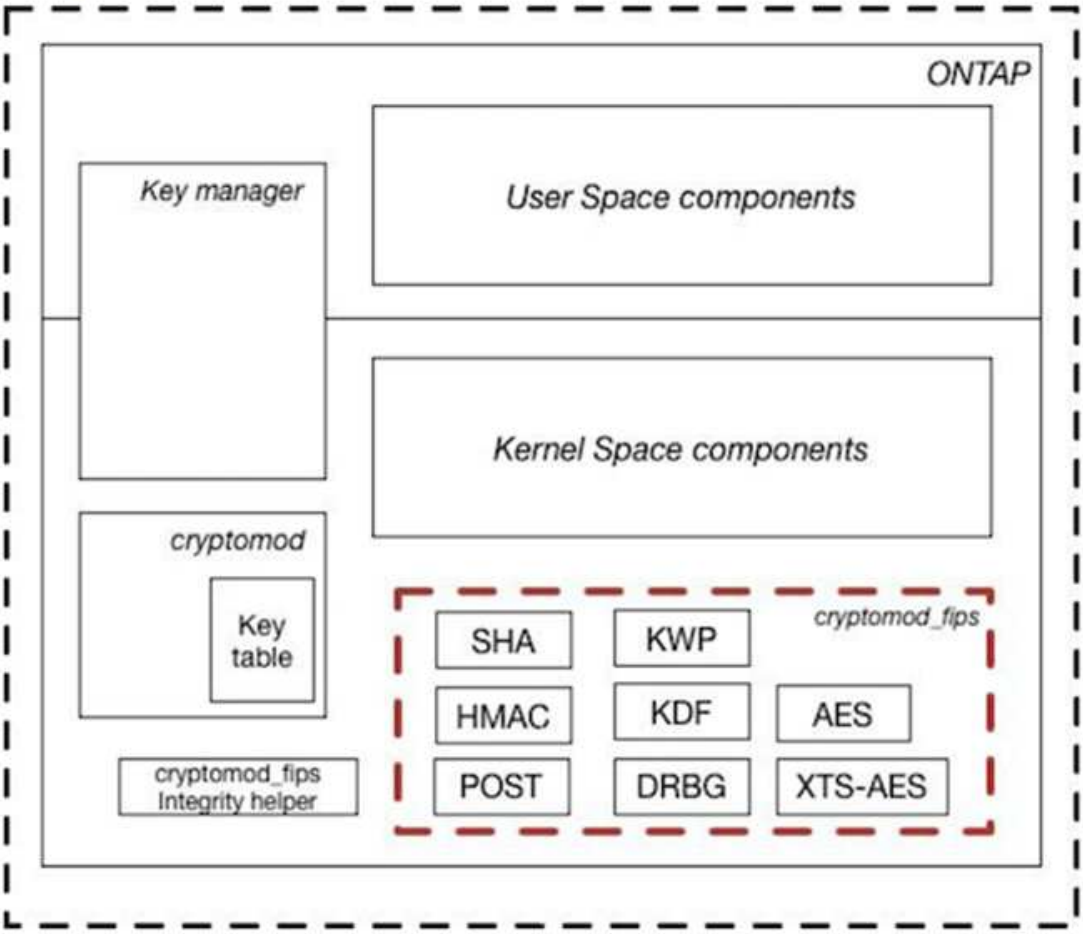


Figure 1 - Block Diagram

キー管理ツールは、 ONTAP で使用されるすべての暗号化キーを追跡します。NSE SED は、キー管理ツールを使用して NSE SED の認証キーを設定します。キー管理ツールを使用する場合は、 NVE と NAE 解決策 が組み合わされ、ソフトウェア暗号化モジュール、暗号化キー、およびキー管理ツールで構成されます。NVE は、ボリュームごとに、キー管理ツールが格納する一意の XTS-AES 256 データ暗号化キーを使用します。データボリュームに使用するキーは、そのクラスタ内のデータボリュームに一意のキーで、暗号化されたボリュームの作成時に生成されます。同様に、 NAE ボリュームはアグリゲートごとに一意の XTS-AES 256 データ暗号化キーを使用します。このキー管理ツールにも保存されます。NAE キーは、暗号化されたアグリゲートが作成されると生成されます。ONTAP は、キーをあらかじめ再生したり、再利用したり、プレーンテキストで表示したりすることはなく、キー管理ツールによって保存および保護されます。

外部キー管理ツールのサポート

ONTAP 9.3 以降では、 NVE ソリューションと NSE ソリューションの両方で外部キー管理機能がサポートされます。FIPS 140-2 規格の環境 特定のベンダーの実装で使用される暗号モジュール。ほとんどの場合、FlexPod と ONTAP のお客様は、（の）次のいずれかの検証済みソリューションを使用しています "NetApp Interoperability Matrix を参照してください") キー管理ツール：

- Gemalto または SafeNet AT のいずれかを指定します

- Vormetric （ Thales ）
- IBM SKLM
- Utimaco （旧称 Microfocus 、 HPE ）

NSE と NVMe SED の認証キーは、業界標準の OASIS Key Management Interoperability Protocol （ KMIP ）を使用して外部キーマネージャにバックアップされます。ストレージシステム、ドライブ、およびキー管理ツールのみがキーにアクセスでき、セキュリティドメイン外に移動してデータ漏洩を防止する場合は、ドライブのロックを解除できません。外部キー管理ツールでは、 NVE ボリュームの暗号化キーおよび NAE アグリゲートの暗号化キーも保存されます。コントローラとディスクを移動して外部キー管理ツールにアクセスできなくなった場合は、 NVE ボリュームと NAE ボリュームにアクセスできず、復号化できません。

次の例では、 store virtual machine （ SVM ）「 svmname1 」の外部キー管理ツールで使用されるサーバのリストに、 2 つのキー管理サーバを追加します。

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

FlexPod データセンターをマルチテナンシーシナリオで使用している場合、 ONTAP では、セキュリティ上の理由から SVM レベルでデータセンターをテナンシー環境から分離できます。

外部キー管理ツールのリストを確認するには、次の CLI コマンドを実行します。

```
fp-health::> security key-manager external show
```

暗号化を組み合わせることで二重暗号化（多層防御）を実現

データへのアクセスを分離し、データが常に保護されるようにする必要がある場合は、 NSE SED をネットワークレベルまたはファブリックレベルの暗号化と組み合わせることができます。NSE SED は、管理者が高レベルの暗号化を設定または設定ミスを忘れてしまった場合に、バックストップのように機能します。2 つの異なるレイヤの暗号化では、 NSE SED を NVE および NAE と組み合わせることができます。

NetApp ONTAP クラスタ全体のコントロールプレーン **FIPS** モード

NetApp ONTAP データ管理ソフトウェアには、お客様向けに高度なセキュリティをインスタンス化する、FIPS モードの構成が用意されています。この FIPS モードでは、コントロールプレーンの環境 のみが実行されます。FIPS モードを有効にすると、 FIPS 140-2 の主要な要素に基づいて、 Transport Layer Security v1 （ TLSv1 ）と SSLv3 は無効になり、 TLS v1.1 と TLS v1.2 のみが有効なままになります。

> FIPS モードの ONTAP クラスタ全体のコントロールペインは、 FIPS 140-2 レベル 1 に準拠しています。クラスタ全体の FIPS モードでは、 NCSM が提供するソフトウェアベースの暗号化モジュールを使用します。

クラスタ全体のコントロールプレーンの FIPS 140-2 準拠モードは、 ONTAP のすべての制御インターフェイスを保護します。デフォルトでは、 FIPS 140-2 のみのモードは無効になっていますが、 security config modify コマンドの 'is-fips-enabled ' パラメータを 'true' に設定すると、このモードを有効にできます。

ONTAP クラスタで FIPS モードを有効にするには、次のコマンドを実行します。

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

SSL FIPS モードが有効な場合は、 ONTAP から ONTAP 外部のクライアントまたはサーバコンポーネントへの SSL 通信に、 FIPS 準拠の SSL 暗号化が使用されます。

クラスタ全体の FIPS ステータスを表示するには、次のコマンドを実行します。

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"次のスライド：解決策 が FlexPod 統合インフラのメリットを提供"

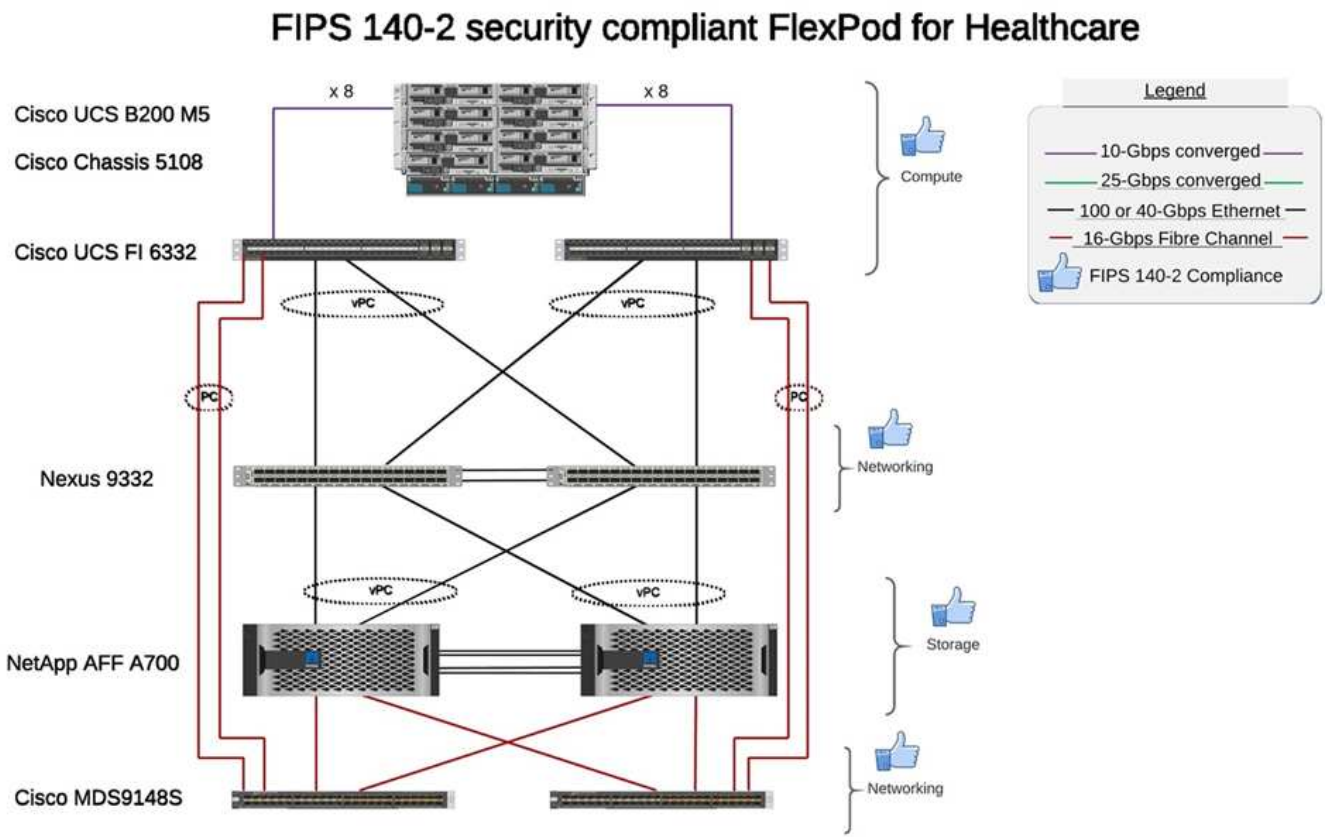
FlexPod コンバージドインフラの解決策 のメリット

"以前のリリース： FlexPod NetApp ONTAP ストレージおよび FIPS 140-2 。"

医療機関には、いくつかのミッションクリティカルなシステムがあります。最も重要なシステムの 2 つは、電子カルテ（ EHR ）システムと医療画像システムです。FlexPod システムにおける FIPS の設定を実証するために、オープンソースの EHR およびオープンソースの画像アーカイブおよび通信システム（ PACS ）システムを使用して、FlexPod システムのラボセットアップとワークロード検証を実施しました。EHR 機能、EHR 論理アプリケーションコンポーネント、および FlexPod システムに実装した場合の EHR システムのメリットの一覧については、を参照してください "TR-4881 ：『 FlexPod for Electronic Health Record Systems 』"。医療画像システムの機能、論理アプリケーションコンポーネント、および FlexPod に実装された医療画像システムの利点については、を参照してください "TR-4865 ： FlexPod for Medical Imaging"。

FIPS のセットアップとワークロードの検証では、典型的な医療機関の代表的なワークロード特性を行使しました。たとえば、現実的な患者データのアクセスおよび変更シナリオを含むオープンソースの EHR システムをテストしました。さらに、医療用画像ワークロードを実行しました。このワークロードには、医療用（ DICOM ）オブジェクトのデジタル画像処理と通信が含まれていました。dcm ファイル形式メタデータを含む DICOM オブジェクトは、ファイルストレージとブロックストレージの両方に保存されています。さらに、仮想化された RedHat Enterprise Linux （ RHEL ）サーバにマルチパス機能も実装しています。DICOM オブジェクトは、 NFS 、 iSCSI を使用してマウントされた LUN 、および FC を使用してマウントされた LUN に保存しました。FIPS のセットアップと検証で、 FlexPod コンバージドインフラが期待以上のパフォーマンスをシームレスに実現したことがわかりました。

次の図は、 FIPS のセットアップと検証に使用される FlexPod システムを示しています。ネットアップはを活用しました "FlexPod データセンターと VMware vSphere 7.0 および NetApp ONTAP 9.7 Cisco Validated Design （ CVD ）" セットアッププロセスの実行中です。



解決策インフラのハードウェアコンポーネントとソフトウェアコンポーネント

次の 2 つの図に、 FlexPod で FIPS を有効にする際に使用するハードウェアコンポーネントとソフトウェアコンポーネントを示します。これらの表に記載されている推奨事項は例です。 NetApp SME と連携して、コンポーネントが組織に適していることを確認する必要があります。また、コンポーネントとバージョンがでサポートされていることを確認します "NetApp Interoperability Matrix Tool で確認できます" （ IMT ）および "シスコハードウェア互換性リスト（ HCL ）"。

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
コンピューティング	Cisco UCS 5108 シャーシ	1 または 2	
	Cisco UCS ブレードサーバ	B200 M5 × 3	それぞれに、 20 コア以上、 2.7GHz 、および 128-384GB RAM を 2 個搭載しています
	Cisco UCS 仮想インターフェイスカード（ VIC ）	Cisco UCS 1440	を参照してください
	Cisco UCS ファブリックインターコネクト × 2	6332	-
ネットワーク	Cisco Nexus スイッチ	Cisco Nexus 9332 × 2	-
ストレージネットワーク	SMB / CIFS 、 NFS 、または iSCSI プロトコル経由のストレージアクセス用の IP ネットワーク	上記と同じネットワークスイッチ	-

レイヤー（ **Layer** ）	製品ファミリー	数量とモデル	詳細
	FC 経由のストレージアクセス	Cisco MDS 9148S × 2	-
ストレージ	NetApp AFF A700 オールフラッシュストレージシステム	1 クラスタ	2 ノードクラスタ
	ディスクシェルフ	DS224C または NS224 ディスクシェルフ × 1	24 本のドライブをフル装備
	SSD の場合	容量が 24 、 2TB 以上	-

ソフトウェア	製品ファミリー	バージョンまたはリリース	詳細
様々	Linux の場合	RHEL 7.x	-
	Windows の場合	Windows Server 2012 R2 （ 64 ビット）	-
	NetApp ONTAP	ONTAP 9.7 以降	-
	Cisco UCS ファブリックインターコネクト	Cisco UCS Manager 4.1 以降	-
	Cisco Ethernet 3000 または 9000 シリーズスイッチ	9000 シリーズの場合、7.0(3) i7(7) 以降（ 3000 シリーズ用）、 9.2(4) 以降	-
	Cisco FC ： Cisco MDS 9132T	8.4(1a) 以降	-
	ハイパーバイザー	VMware vSphere ESXi 6.7 U2 以降	-
ストレージ	ハイパーバイザー管理システム	VMware vCenter Server 6.7 U3 （ vCSA ）以降	-
ネットワーク	NetApp Virtual Storage Console （ VSC ）	VSC 9.7 以降	-
	NetApp SnapCenter	SnapCenter 4.3 以降	-
	Cisco UCS Manager の略	4.1 （ 1c ）以降	
ハイパーバイザー	ESXi		
管理	ハイパーバイザー管理システム VMware vCenter Server 6.7 U3 （ vCSA ）以降		
	NetApp Virtual Storage Console （ VSC ）	VSC 9.7 以降	
	NetApp SnapCenter	SnapCenter 4.3 以降	
	Cisco UCS Manager の略	4.1 （ 1c ）以降	

"次： FlexPod のセキュリティに関するその他の考慮事項。"

FlexPod のセキュリティに関するその他の考慮事項

"前のスライド：解決策 が FlexPod コンバージドインフラのメリットを提供"

FlexPod インフラは、モジュラ型の統合型で、必要に応じて仮想化と拡張性に優れた、コスト効率の高いプラットフォームです。FlexPod プラットフォームでは、コンピューティング、ネットワーク、ストレージを個別にスケールアウトできるため、アプリケーションの導入時間が短縮されます。また、モジュラアーキテクチャにより、システムのスケールアウトやアップグレード時にもノンストップオペレーションが実現します。

HIT システムのさまざまなコンポーネントは、データを SMB/CIFS 、 NFS 、 ext4 、および NTFS ファイルシステムに格納する必要があります。つまり、この要件のインフラでは、 NFS 、 CIFS 、 SAN の各プロトコル経由でデータアクセスを提供する必要があります。1 つのネットアップストレージシステムでこれらのプロトコルをすべてサポートできるため、プロトコル固有のストレージシステムという従来の手法は必要ありません。さらに、 1 つのネットアップストレージシステムで複数の HIT ワークロード（ EHR 、 PACS 、 VNA 、ゲノム、 VDI など）をサポートし、 パフォーマンスレベルが保証され、設定も可能です。

HIT は、 FlexPod システムに導入されると、医療業界に固有の利点をいくつか提供します。次に、これらの利点の概要概要 を示します。

- * FlexPod セキュリティ * 。セキュリティは、 FlexPod システムの基盤にあります。ここ数年、ランサムウェアは脅威になっています。ランサムウェアは、暗号化を使用して悪意のあるソフトウェアを構築する暗号技術に基づいたマルウェアの一種です。このマルウェアは、対称キー暗号と非対称キー暗号の両方を使用して、被害者のデータをロックし、データを復号化するための鍵を提供するために身代金を要求できます。FlexPod 解決策 がランサムウェアなどの脅威を軽減する方法については、を参照してください "TR-4802 ：『 The 解決策 to Ransomware 』"。FlexPod インフラコンポーネントもあります "FIPS 140-2 に準拠しています"。
- * Cisco Intersight * Cisco Intersight は、クラウドベースの革新的な管理サービスプラットフォームであり、単一のコンソールでフルスタックの FlexPod 管理とオーケストレーションを実現します。Intersight プラットフォームでは、 FIPS 140-2 セキュリティ準拠の暗号モジュールが使用されています。このプラットフォームのアウトオブバンド管理アーキテクチャは、 HIPAA などの一部の標準や監査の範囲外になります。ネットワーク上の個々の識別可能なヘルス情報が、サイト間ポータルに送信されることはありません。
- * NetApp FPolicy テクノロジ。 * NetApp FPolicy （名前ファイルポリシーの変更）は、 NFS または SMB / CIFS プロトコル経由のファイルアクセスを監視および管理するための、ファイルアクセス通知フレームワークです。このテクノロジは、 ONTAP データ管理ソフトウェアに 10 年以上にわたって組み込まれており、ランサムウェアの検出に役立ちます。このゼロトラストエンジンは、アクセスコントロールリスト（ ACL ）の権限を超えた追加のセキュリティ対策を提供します。FPolicy の処理モードには、ネイティブと外部の 2 つがあります。
  - ネイティブモードでは、ファイル拡張子のブラックリストとホワイトリストの両方が提供されます。
  - 外部モードはネイティブモードと同じ機能を備えていますが、 ONTAP システムとは外部で実行される FPolicy サーバや、セキュリティ情報 / イベント管理（ SIEM ）システムと統合されています。ランサムウェアと戦う方法の詳細については、を参照してください "『 Fighting Ransomware ： Part 3 – ONTAP FPolicy 、 Another powerful Native （別名 Free ） Tool 』" ブログ
- * 保存データ * 。ONTAP 9 以降には、 FIPS 140-2 準拠の保管データ暗号化ソリューションが 3 つあります。
  - NSE は、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。

- 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。
- 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。

> ONTAP 9.7 以降では、 VE という名前の NetApp NVE ライセンスパッケージがある場合、NAE および NVE がデフォルトで有効になります。

- * 転送中のデータ * 。ONTAP 9.8 以降では、 Internet Protocol security （ IPSec ；インターネットプロトコルセキュリティ）により、クライアントと ONTAP SVM の間のすべての IP トラフィックをエンドツーエンドで暗号化できます。すべての IP トラフィックの IPSec データ暗号化には、 NFS 、 iSCSI 、 SMB/CIFS の各プロトコルが含まれます。IPSec では、 iSCSI トラフィックに対して転送中の暗号化オプションのみが提供されます。
- * ハイブリッドマルチクラウドデータファブリック全体でエンドツーエンドのデータ暗号化を実現 * 。データレプリケーショントラフィックに NSE や NVE およびクラスタピアリング暗号化（ CPE ）などの保管データ暗号化テクノロジを使用しているお客様は、 ONTAP 9.8 以降にアップグレードして IPsec を使用することで、ハイブリッドマルチクラウドデータファブリック全体でクライアントとストレージの間のエンドツーエンドの暗号化を使用できるようになりました。ONTAP 9 以降では、クラスタ全体のコントロールプレーンインターフェイスに対して、 FIPS 140-2 準拠モードを有効にできます。FIPS 140-2 専用モードは、デフォルトでは無効になっています。ONTAP 9.6 以降では、 CPE によって、 NetApp SnapMirror 、 NetApp SnapVault 、 NetApp FlexCache テクノロジなどの ONTAP データレプリケーション機能に対する TLS 1.2 AES-256 GCM 暗号化がサポートされます。暗号化は、 2 つのクラスタピア間での Pre-Shared Key （ PSK ；事前共有キー）を使用して設定されます。
- * セキュアマルチテナンシー * 。仮想化されたサーバとストレージ共有インフラのニーズの増大に対応し、特にデータベースとソフトウェアの複数のインスタンスをホストする場合に、施設固有の情報のセキュアマルチテナンシーを実現します。

"次は終わりです"

まとめ

"Previous ： FlexPod のセキュリティに関するその他の考慮事項。"

医療アプリケーションを FlexPod プラットフォームで実行することで、医療機関は FIPS 140-2 対応プラットフォームでより適切に保護されます。FlexPod は、コンピューティング、ネットワーク、ストレージのすべてのコンポーネントでマルチレイヤ保護を提供します。FlexPod のデータ保護機能は、保管中または転送中のデータを保護し、必要に応じてバックアップを安全に実行し、準備を整えます。

Cisco とネットアップの戦略的パートナーシップによって厳格にテストされた統合インフラである FlexPod 検証済み設計を活用することで、人為的ミスを回避できます。コンピューティング、ネットワーク、ストレージの各レイヤで FIPS 140-2 が有効な場合でも、予測可能な低レイテンシのシステムパフォーマンスと高可用性を提供するように設計された FlexPod システム。影響はほとんどありません。このアプローチにより、 HIT システムのユーザーに優れたユーザー体験と最適な応答時間が実現します。

"次：謝辞、バージョン履歴、および追加情報 の検索場所"

確認応答、バージョン履歴、および追加情報 の参照先

"前へ：終わりに。"

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。

- 『 Cisco MDS 9000 Family NX-OS Security Configuration Guide 』

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000 Series NX-OS Security Configuration Guide 、 Release 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- NetApp and Federal Information Processing Standard （ FIPS ） 140-2 』を参照できます

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- 『 NetApp ONTAP 9 Hardening Guide 』

  https://www.netapp.com/us/media/tr-4569.pdf

- NetApp Encryption パワーガイド』を参照してください

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- NVE および NAE のデータシート

  https://www.netapp.com/us/media/ds-3899.pdf

- NSE のデータシート

  https://www.netapp.com/us/media/ds-3213-en.pdf

- ONTAP 9 ドキュメンテーション・センター

  http://docs.netapp.com

- NetApp and Federal Information Processing Standard （ FIPS ） 140-2 』を参照できます

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Cisco および FIPS 140-2 への準拠

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- NetApp Cryptographic Security Module の略

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- 中規模および大規模な医療機関向けのサイバーセキュリティの実践

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Cisco and Cryptographic Module Validation Program （ CMVP ）

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp ストレージ暗号化、 NVMe 自己暗号化ドライブ、 NetApp Volume Encryption 、 NetApp Aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp Volume Encryption および NetApp Aggregate Encryption の略

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NetApp Storage Encryption の略

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- 電子医療記録システム用 FlexPod

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- 現在のデータ：クラウド対応フラッシュテクノロジを使用した Epic EHR 環境でパフォーマンスを向上

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- Epic EHR インフラ向け FlexPod データセンター

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- Epic EHR 向け FlexPod データセンター導入ガイド

  https://www.netapp.com/media/10658-tr-4693.pdf

- MEDITECH ソフトウェア対応 FlexPod データセンターインフラ

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- FlexPod 規格は MEDITECH ソフトウェアにも対応しています

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- FlexPod for MEDITECH の指向性サイジングガイド

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- 医療用画像処理用の FlexPod

  https://www.netapp.com/media/19793-tr-4865.pdf

- 医療業界の AI

  https://www.netapp.com/us/media/na-369.pdf

- ヘルスケア向けの FlexPod で変革を促進

  https://flexpod.com/solutions/verticals/healthcare/

- Cisco とネットアップが提供する FlexPod

  https://flexpod.com/

謝辞

- ネットアップ、テクニカルマーケティングエンジニア、 Abhinav Singh 氏
- ネットアップ、解決策 Architect Healthcare （ Epic ）、 Brian O'Menahony 氏
- ネットアップ、 Pursuit Business Development Manager 、 Brian Pruitt 氏
- ネットアップシニアソリューションアーキテクト、 Arvind Ramakrinan 氏
- ネットアップ、 FlexPod グローバルフィールド CTO 、 Michael Hommer 氏

バージョン履歴

バージョン	日付	ドキュメントのバージョン履歴
バージョン 1.0 以降	2021年4月	初版リリース