解決策、 FlexPod によるランサムウェア対策

FlexPod

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/flexpod/security/security-ransomware_what_is_ransomware.html on March 25, 2024. Always check docs.netapp.com for the latest.

目次

解決策、 FlexPod によるランサムウェア対策 . . . 1
TR-4802 ：『 FlexPod 、 the 解決策 to Ransomware 』 . . . 1
FlexPod の概要 . . . 3
ランサムウェアからの保護対策 . . . 4
FlexPod でデータを保護し、リカバリできます . . . 6
身代金を支払うことなく業務を継続 . . . 19
まとめ . . . 19
謝辞 . . . 20
追加情報 . . . 20

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。

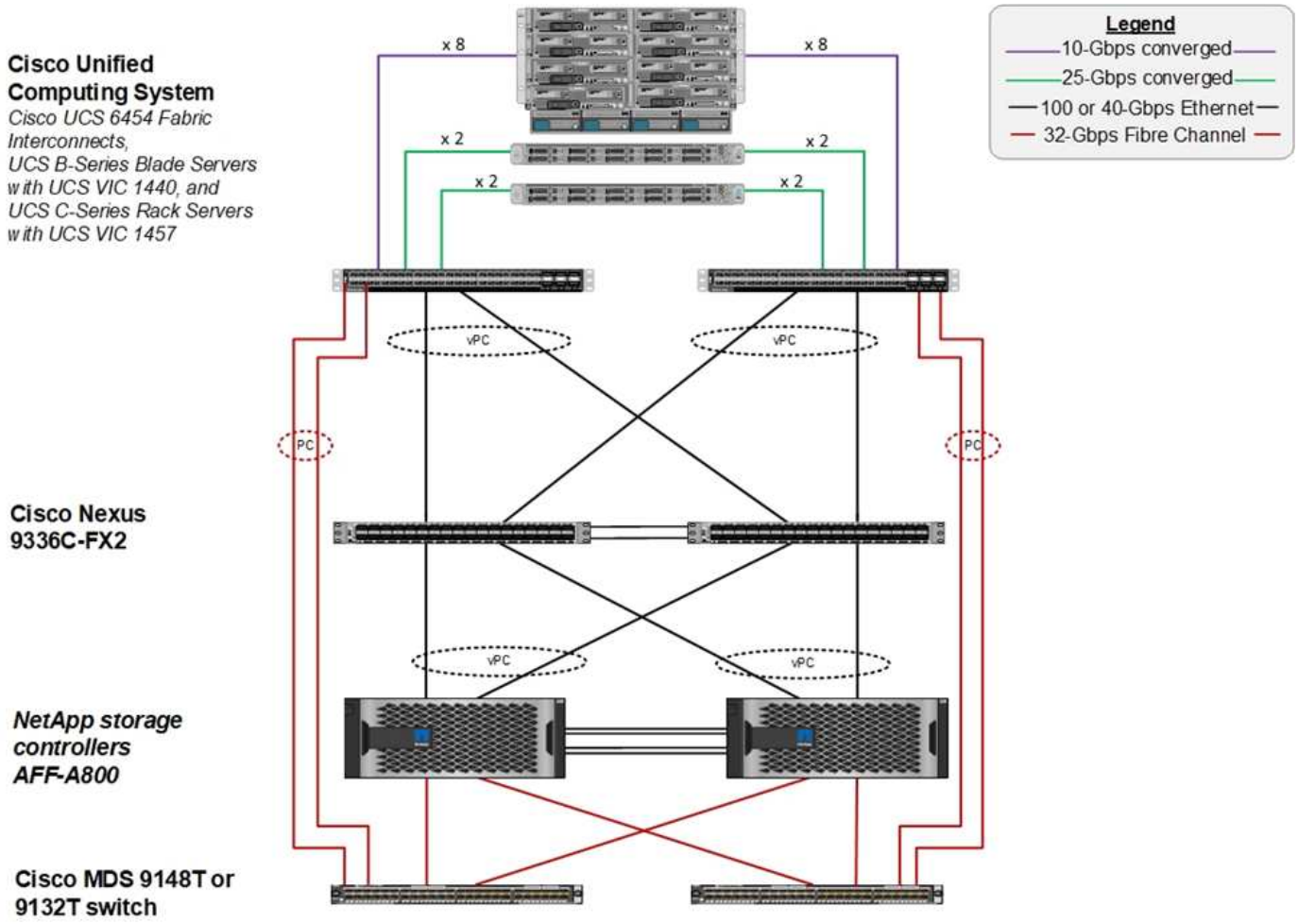
ネットワーク、コンピューティング、ストレージのエンドポイントを保護するデータセンターの設計と機能は、日常業務の安全な環境を構築する上で重要な役割を果たします。このドキュメントでは、 FlexPod ハイブリッドクラウドインフラストラクチャの機能が、攻撃の発生時に迅速にデータをリカバリするのにどのように役立つか、また攻撃を防御するのにどのように役立つかを説明します。

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

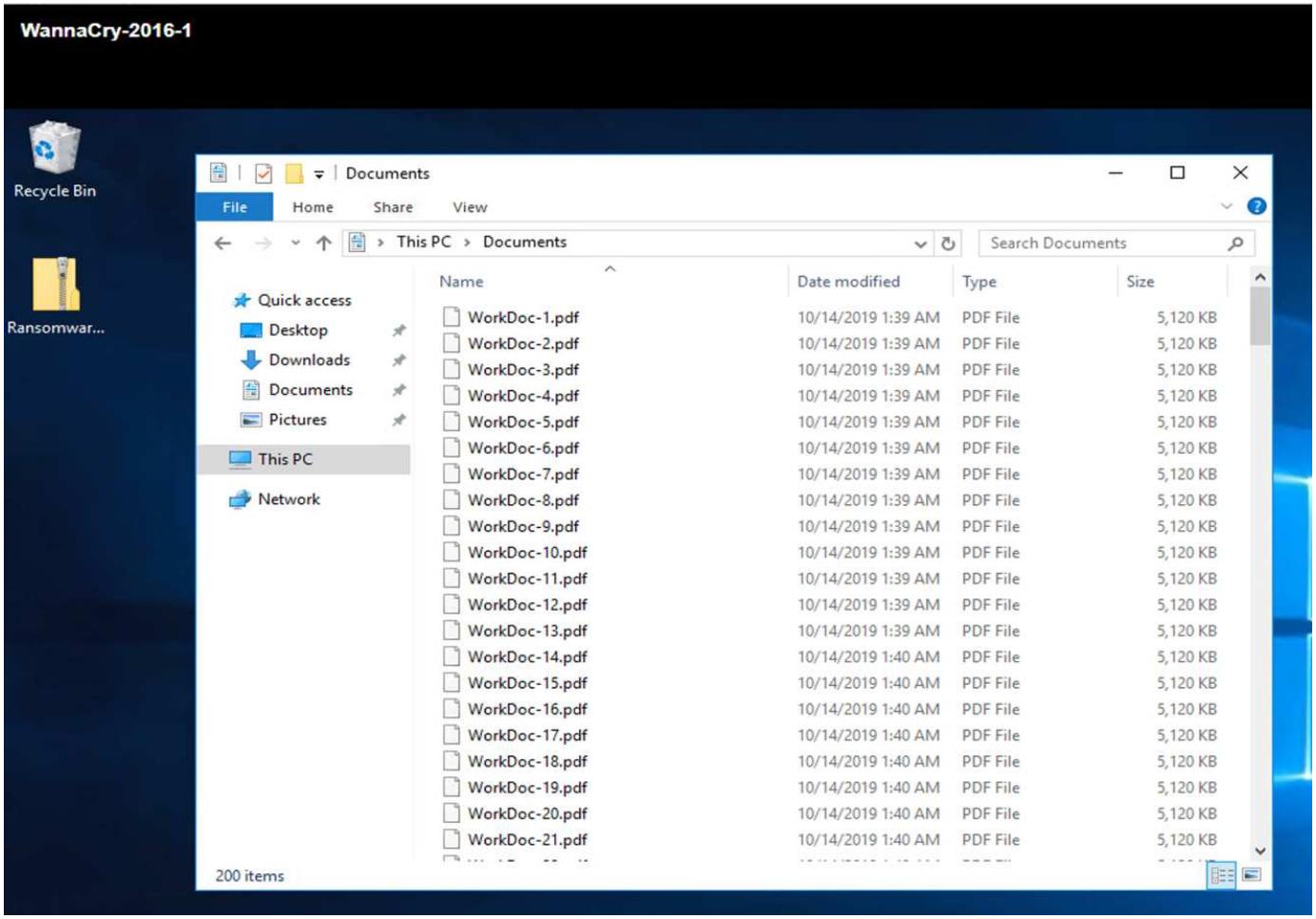
テストベッドは、 FlexPod の検出、修復、および防止を示すために、本ドキュメントの作成時点で使用可能な最新のプラットフォーム CVD で指定されているガイドラインに基づいて構築されています。 "FlexPod データセンターと VMware vSphere 6.7 U1 、 Cisco UCS 第 4 世代、および NetApp AFF A シリーズに関する CVD"。

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。

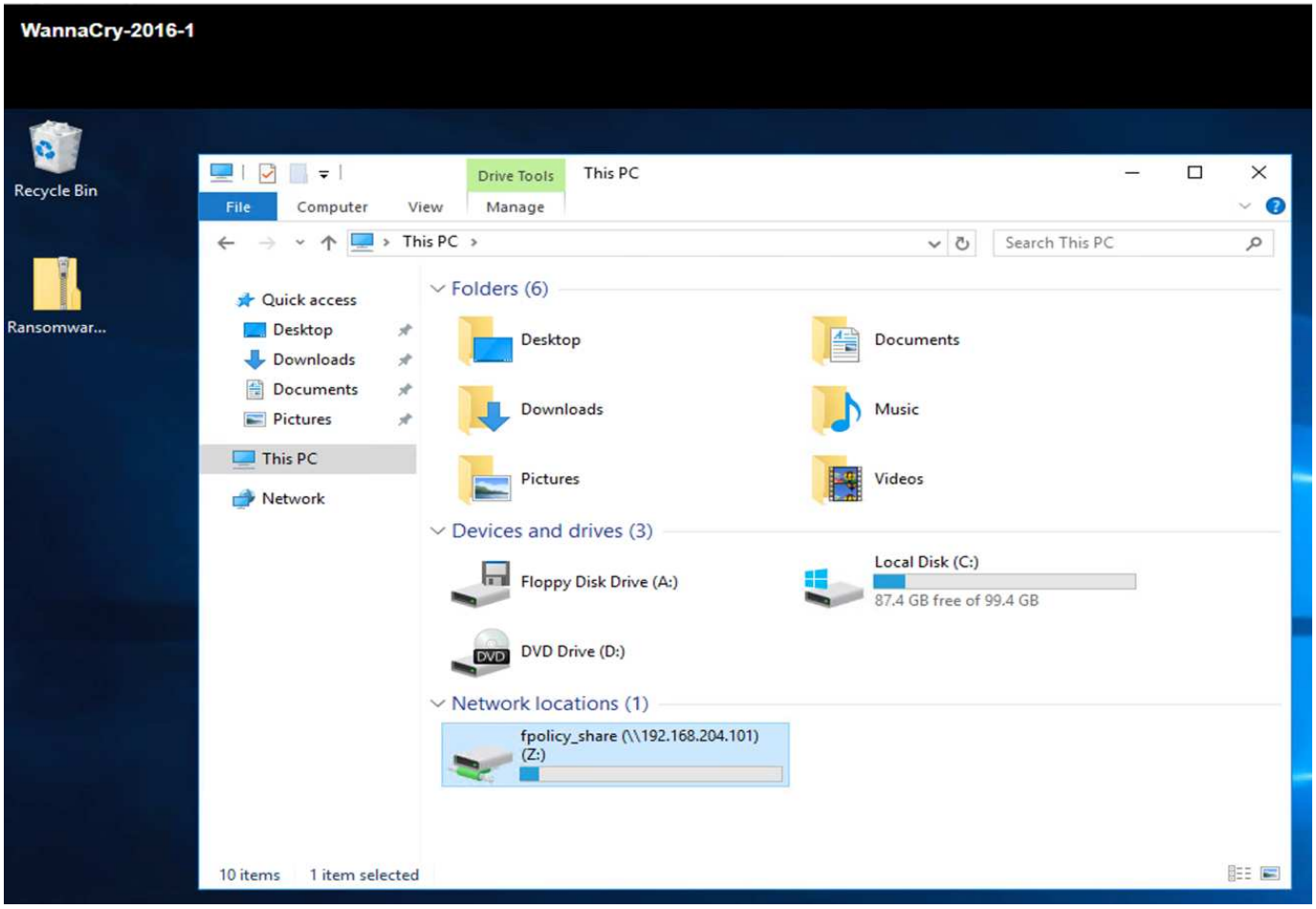
攻撃前の **VM** とそのファイルの状態

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。

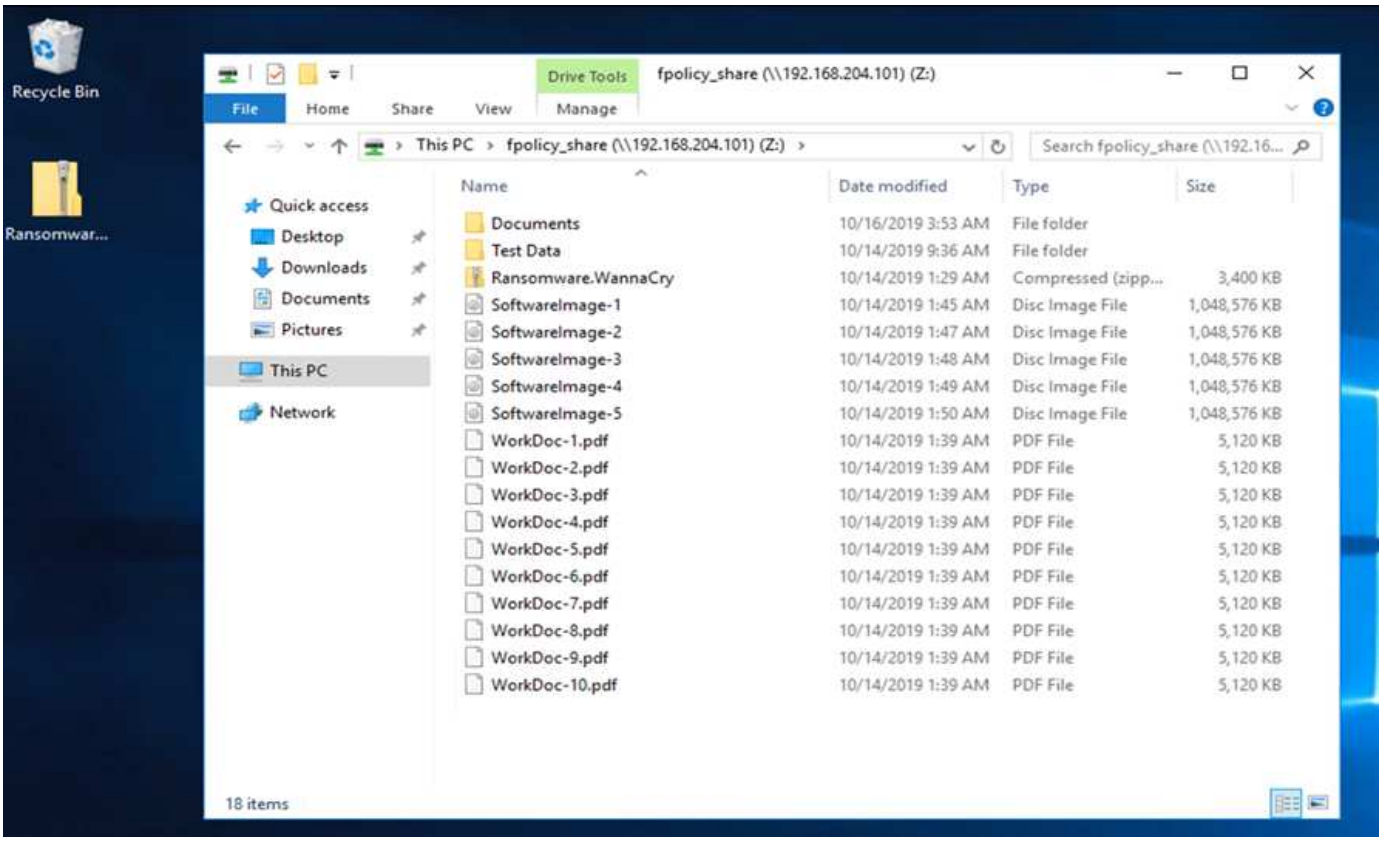
VM の Documents フォルダには、 WannaCry マルウェアによってまだ暗号化されていない PDF ファイルのセットがありました。



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。



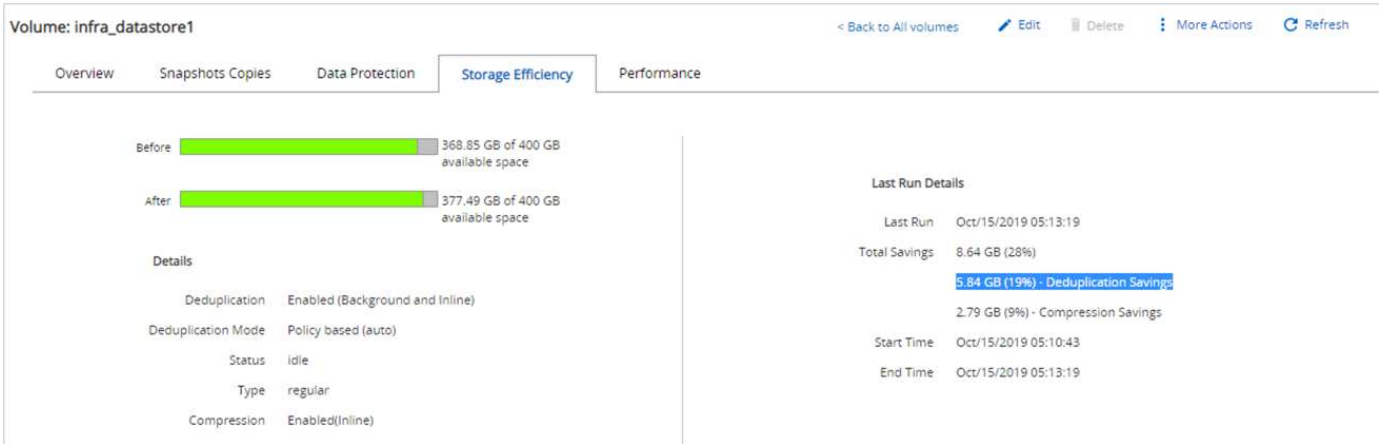
次のスクリーンショットは、 WannaCry マルウェアによってまだ暗号化されていない CIFS 共有 'fpolicy_share' 上のファイルを示しています。



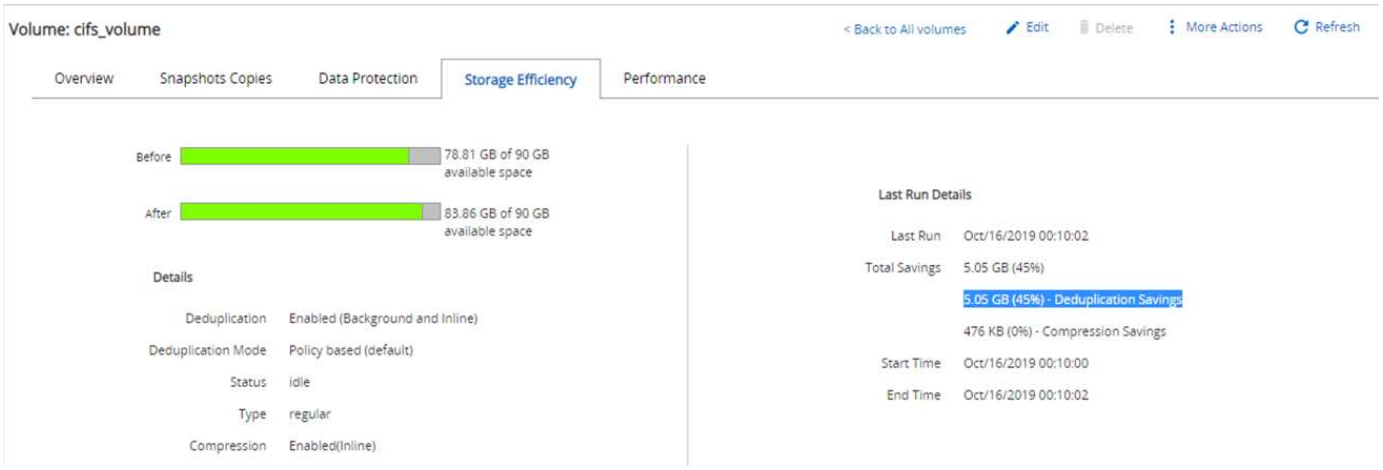
攻撃前の重複排除およびスナップショット情報

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。

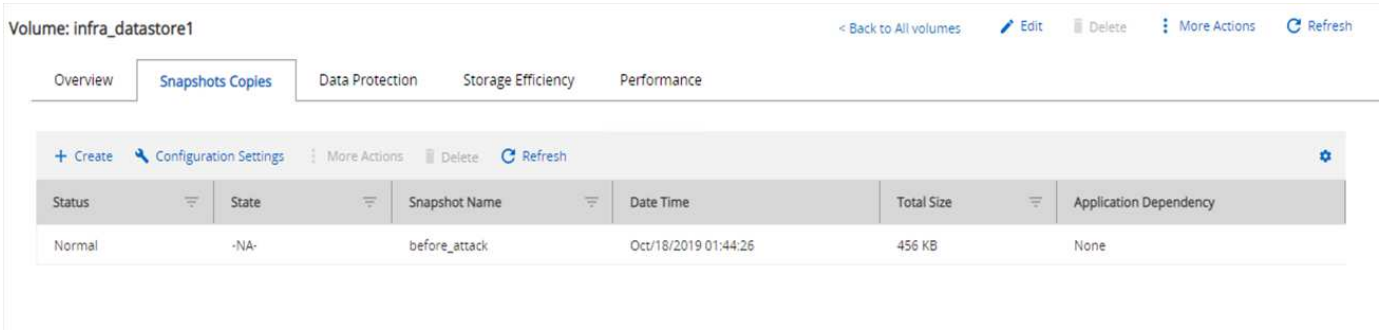
VM をホストするボリュームで重複排除を実行すると、ストレージを 19% 削減できました。



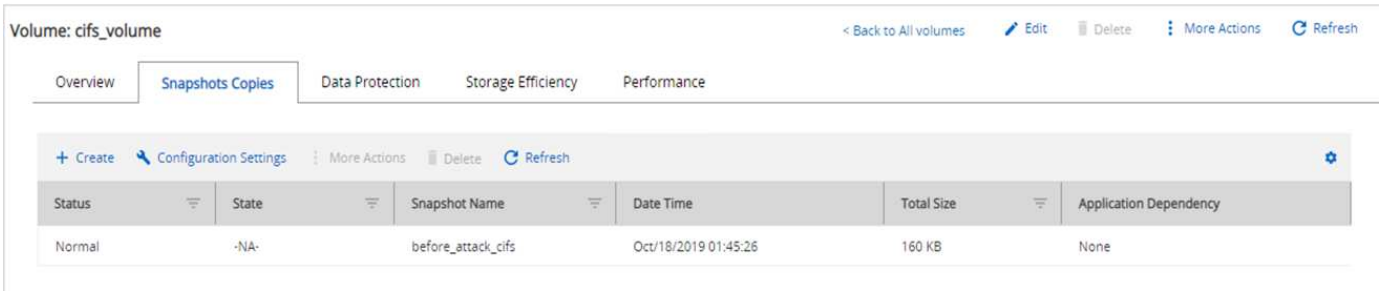
CIFS 共有「 fpolicy_share 」の重複排除により、 45% のストレージ節約を達成しました。



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。



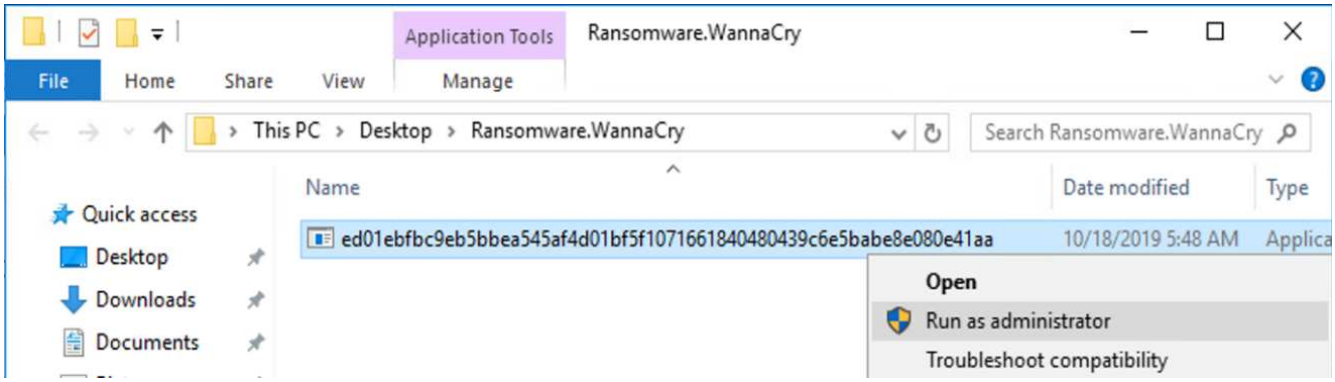
VM および CIFS 共有での WannaCry 感染

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。

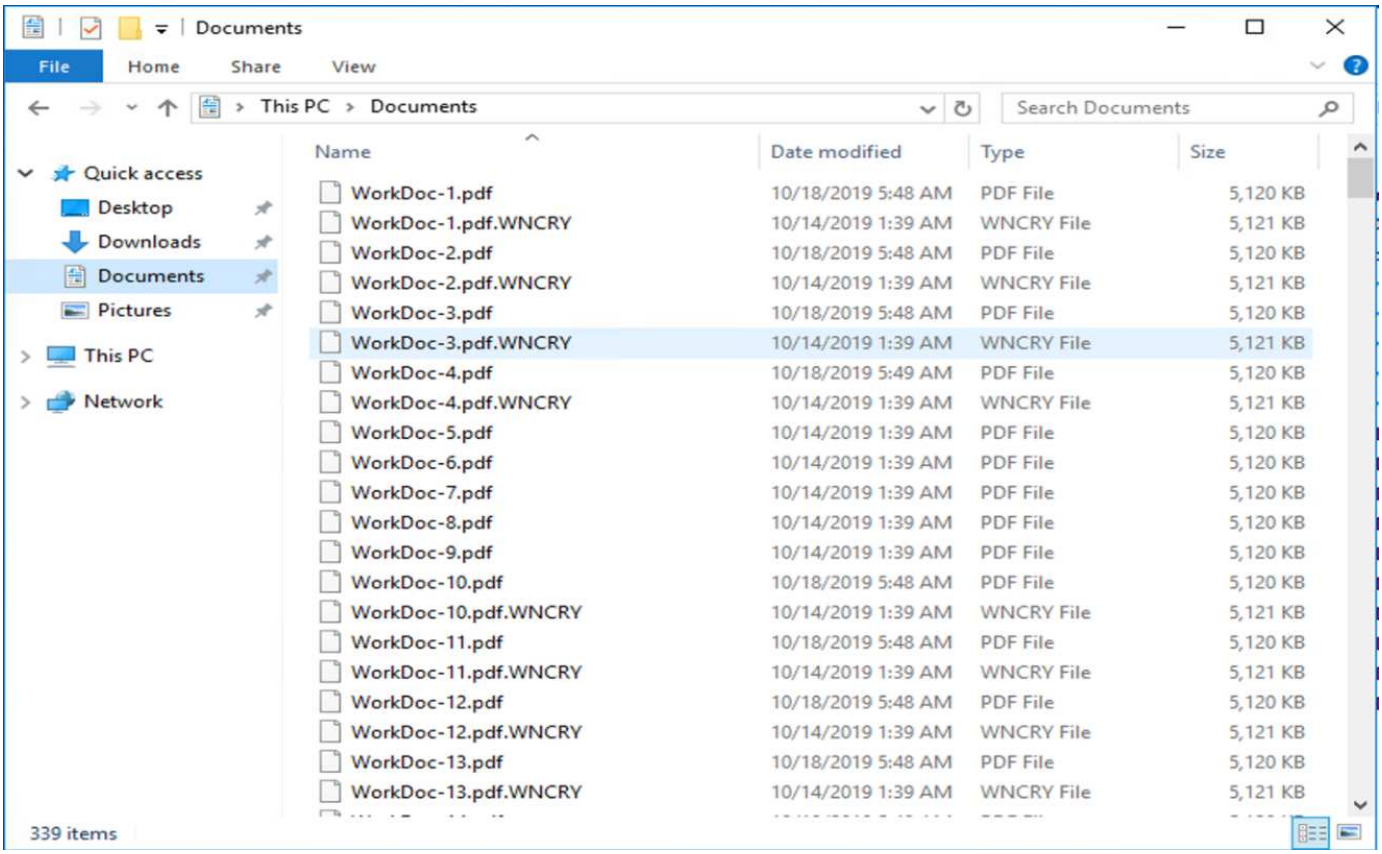
2. バイナリが実行されました。



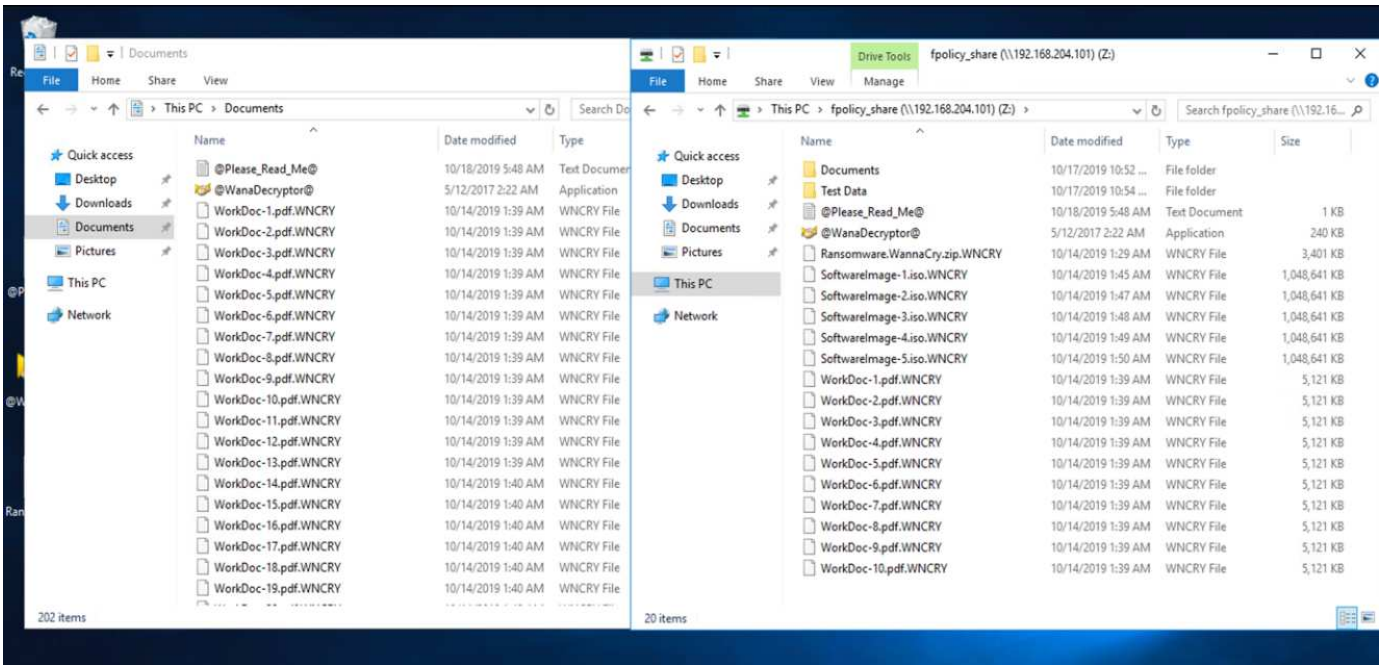
ケース 1 ： **WannaCry** は **VM** 内のファイルシステムを暗号化し、マッピングされた **CIFS** 共有を暗号化します

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。

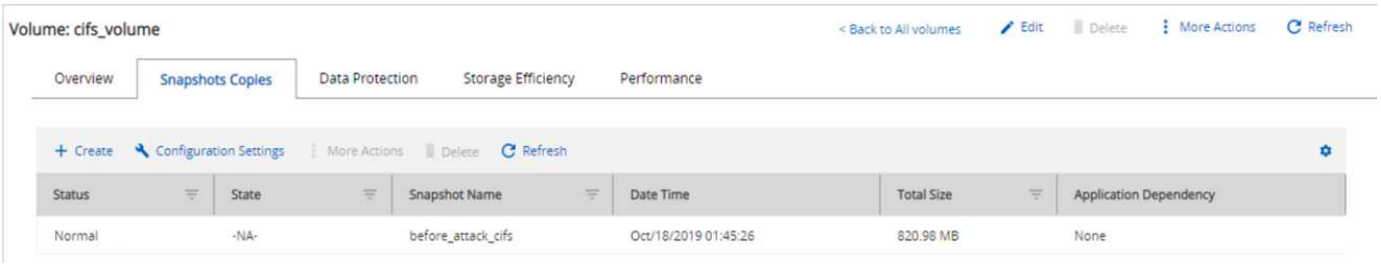


検出

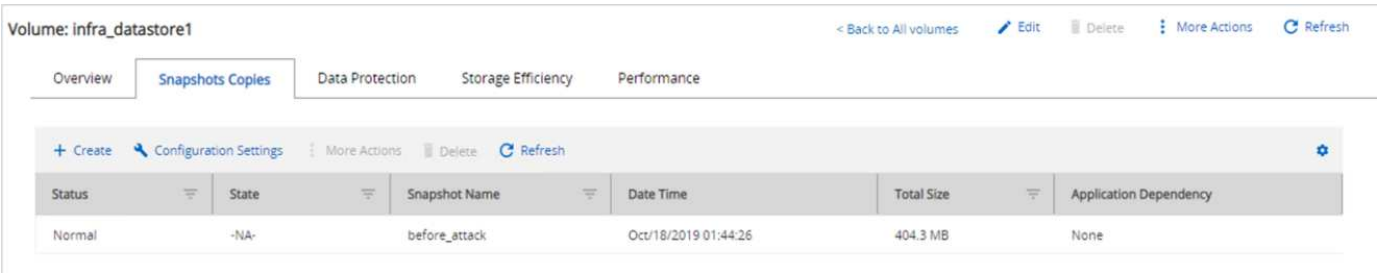
マルウェアがファイルの暗号化を開始した瞬間から、 Snapshot コピーのサイズが急激に増加し、ストレージ効率が急激に低下しました。

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

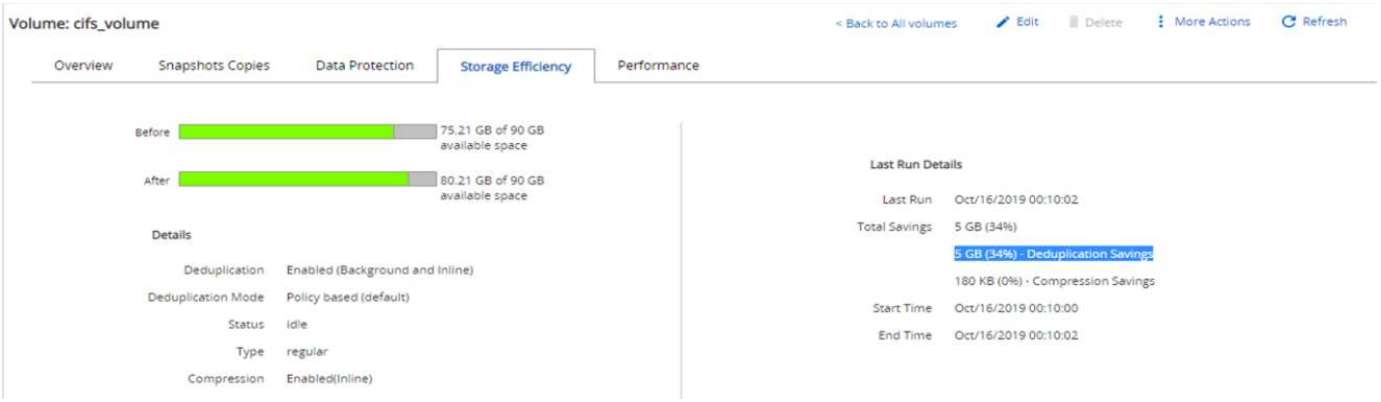
されました。



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。



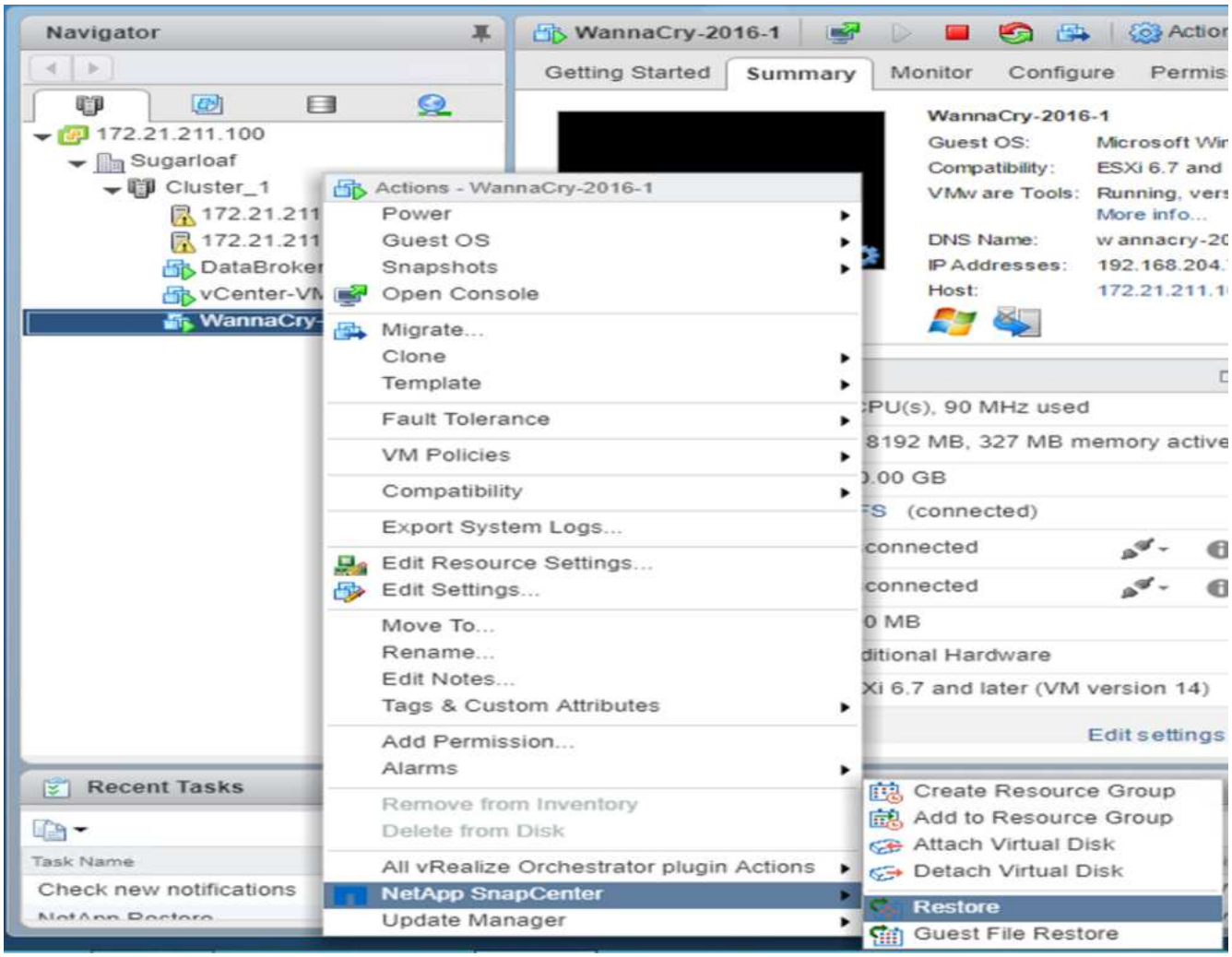
修正

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。

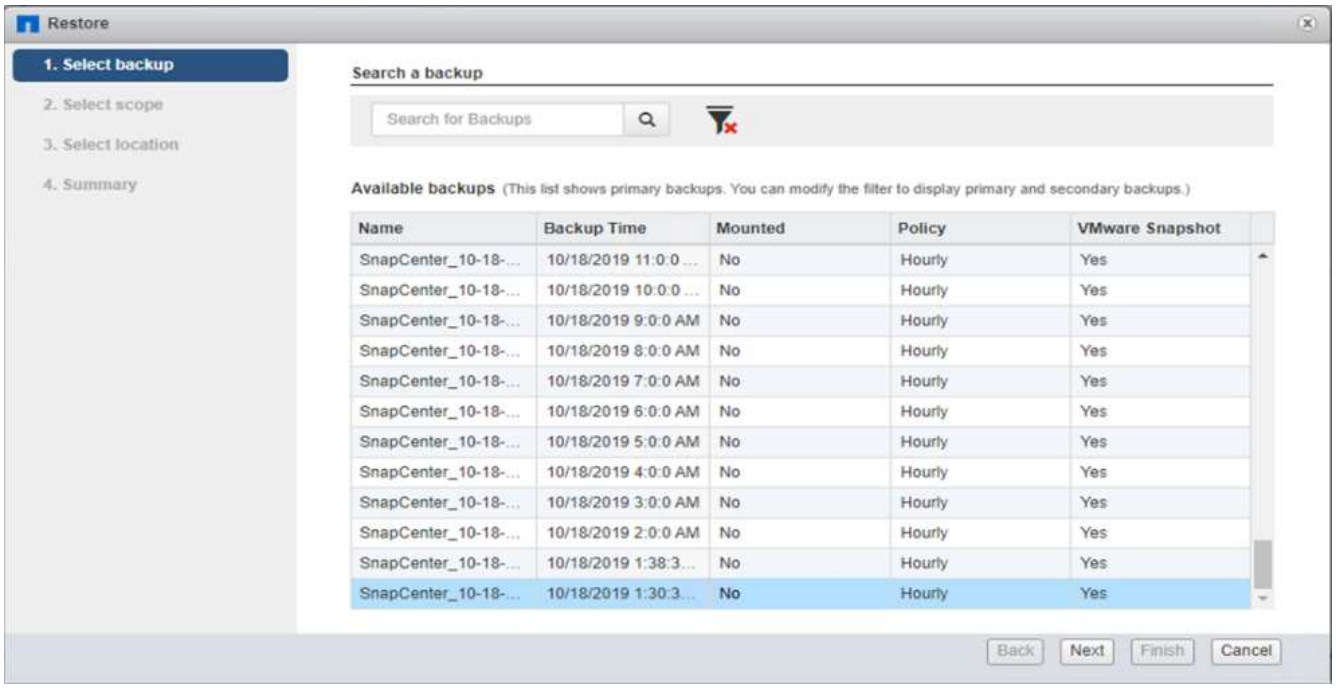
- リストア VM *

VM をリストアするには、次の手順を実行します。

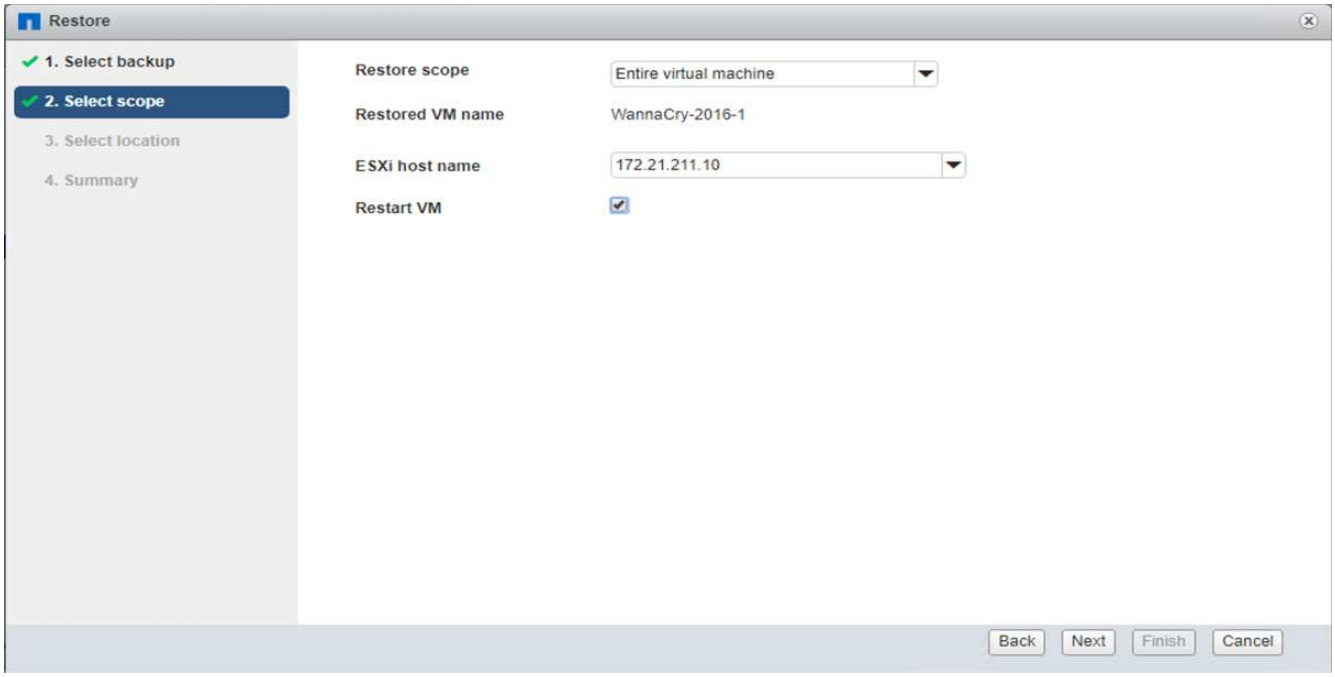
1. SnapCenter で作成した Snapshot コピーを使用して、 VM をリストアします。



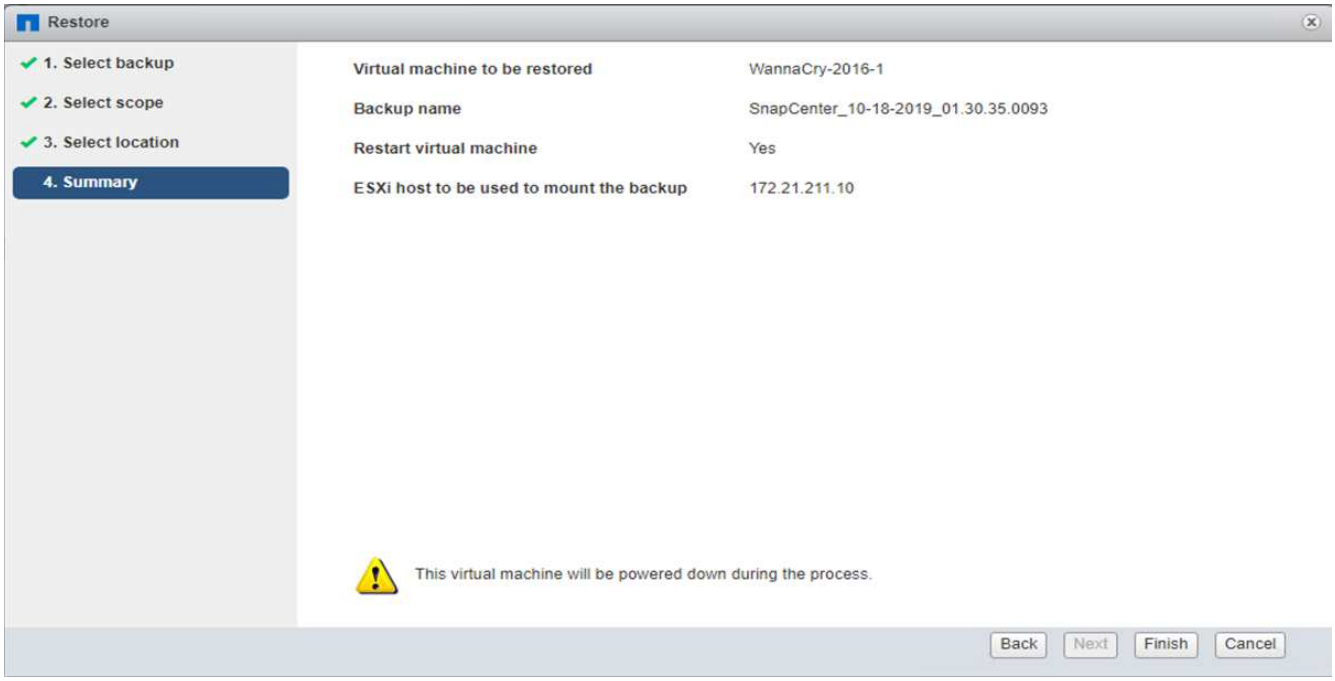
2. リストアに使用する VMware 整合性のある Snapshot コピーを選択します。



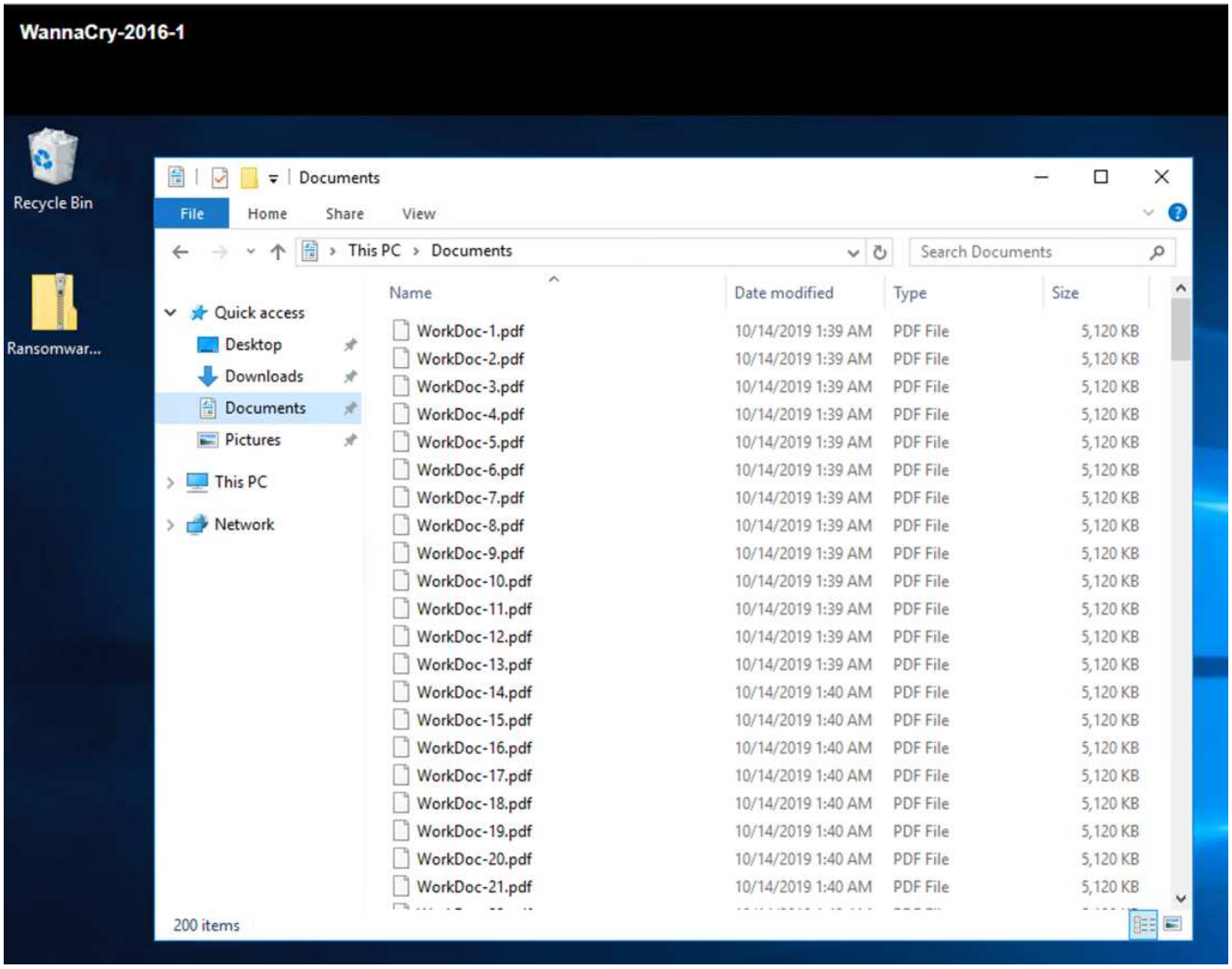
3. VM 全体がリストアされて再起動されます。



4. [完了] をクリックして、復元プロセスを開始します。



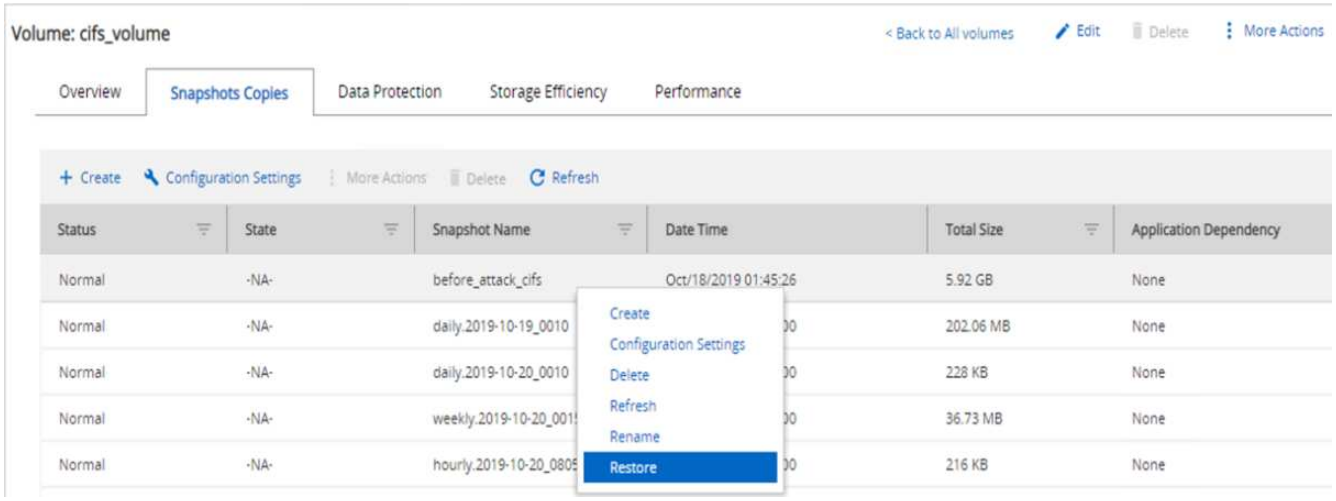
5. VM とそのファイルがリストアされます。



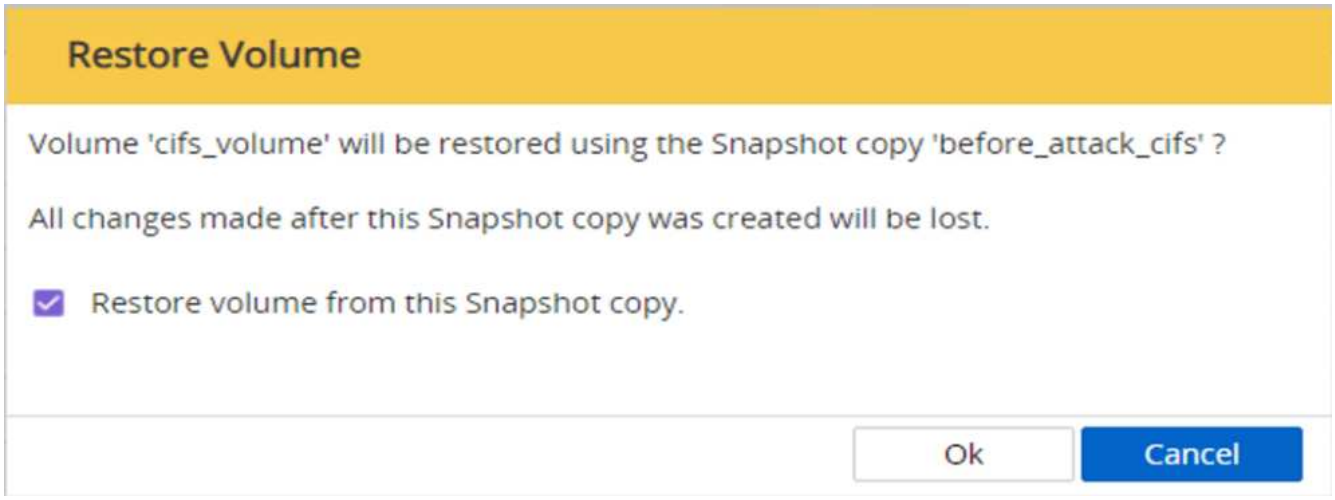
◦ CIFS 共有の復元 *

CIFS 共有をリストアするには、次の手順を実行します。

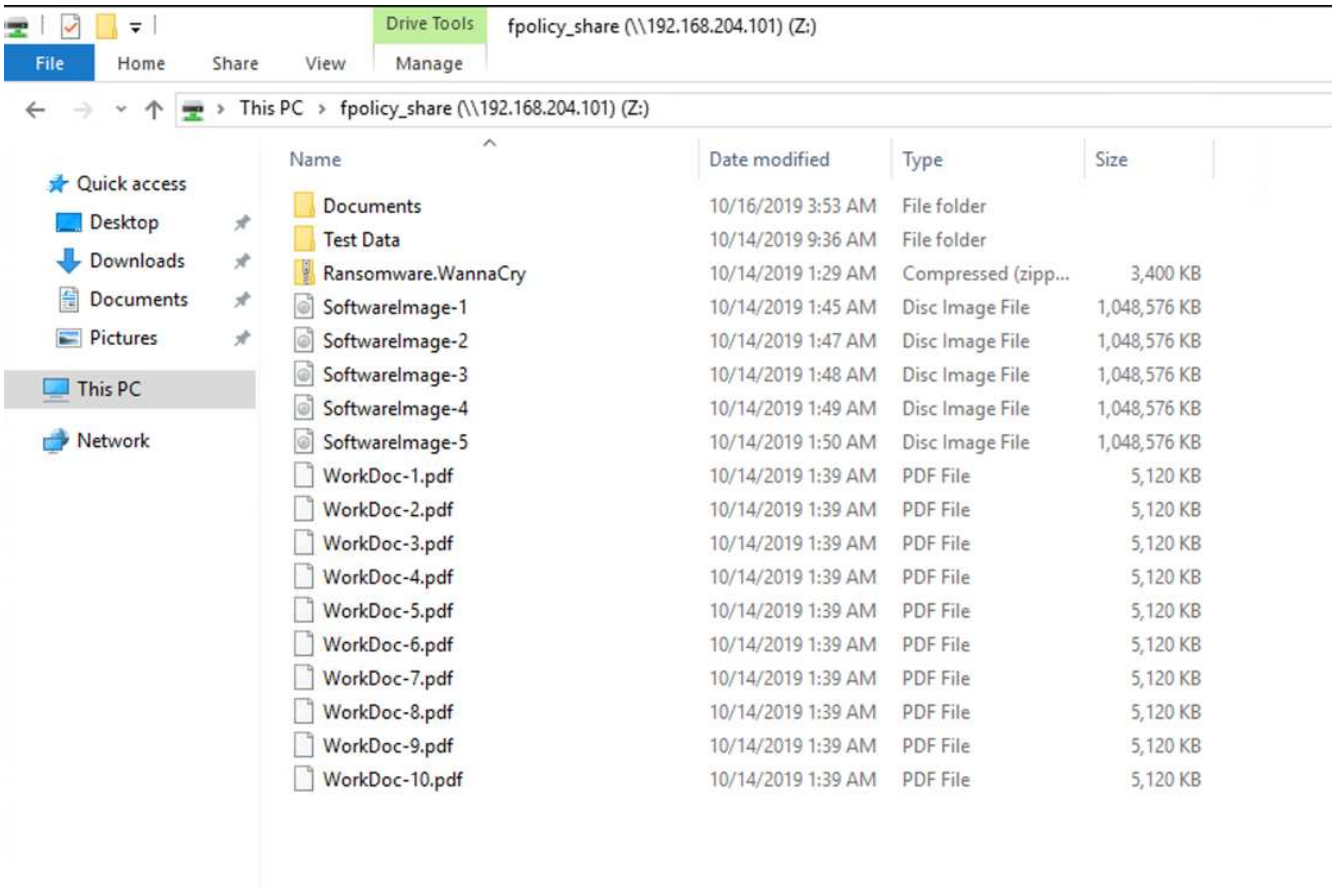
1. 攻撃の前に作成されたボリュームの Snapshot コピーを使用して、共有をリストアします。



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

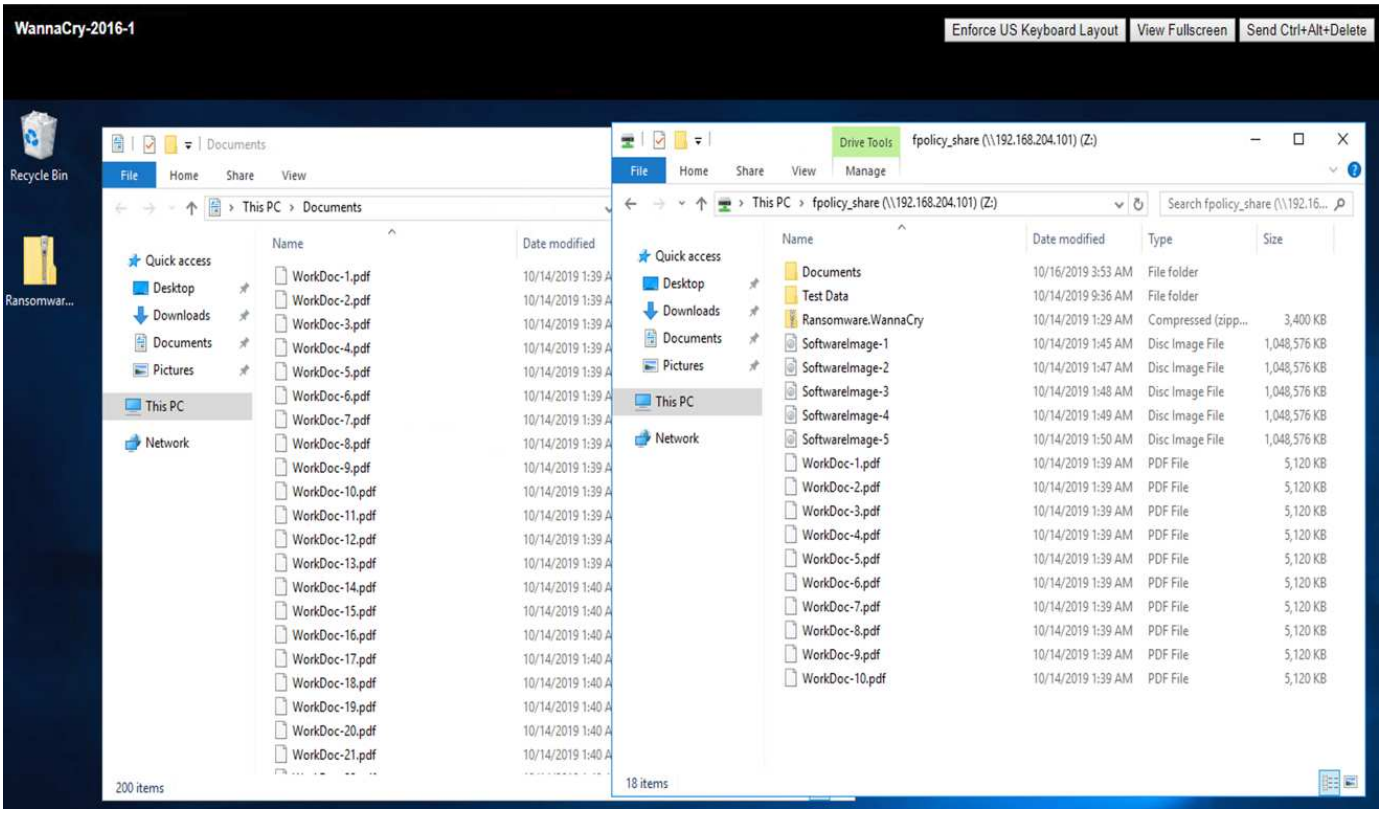
- FPolicy を設定 *

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。

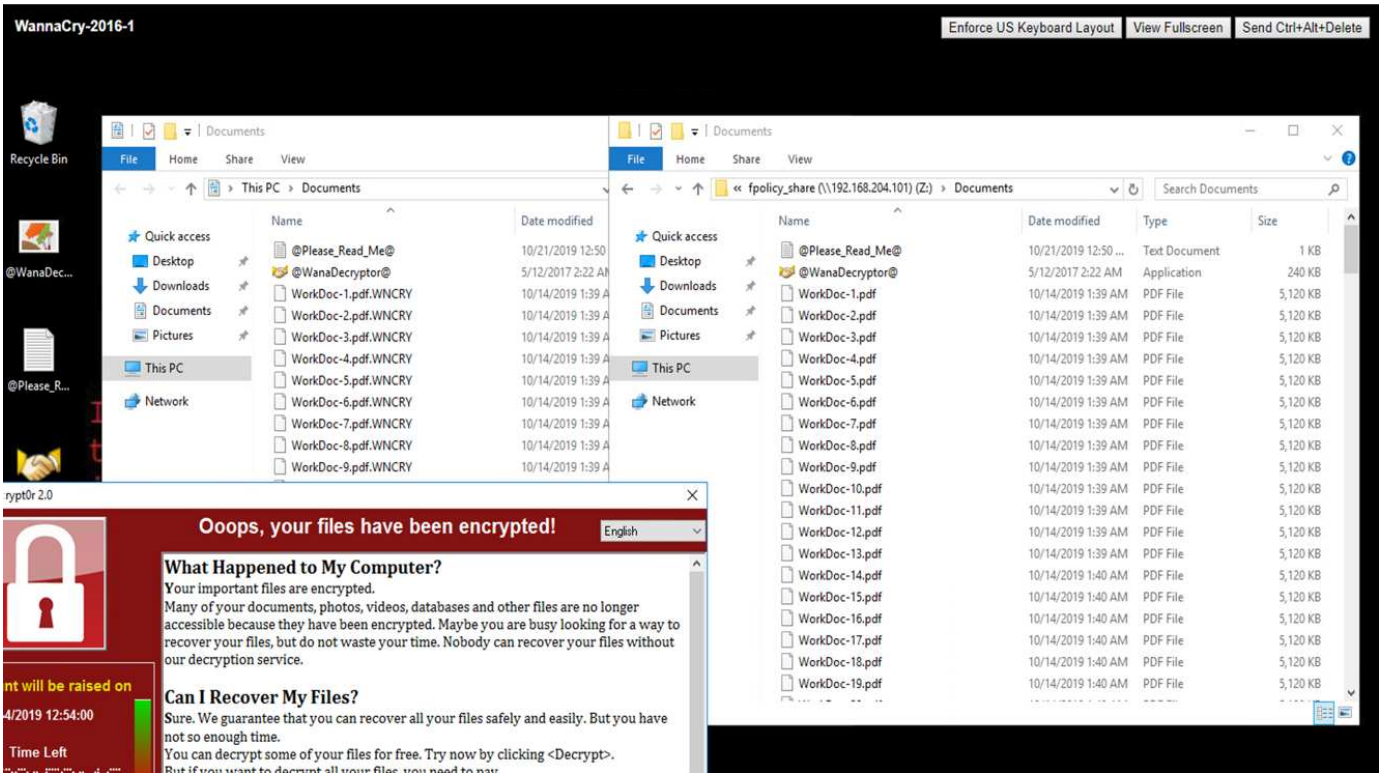
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -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"

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。