FlexPod，《勒索软件解决方案》

FlexPod

NetApp

October 30, 2025

目录

FlexPod ，《勒索软件解决方案》

TR-4802： FlexPod ，《勒索软件解决方案》

NetApp 公司 Arvind Ramakrishnan

与以下合作伙伴： 

要了解勒索软件，必须首先了解有关加密的几个要点。加密方法可以使用共享密钥（对称密钥加密）或一对密钥（非对称密钥加密）对数据进行加密。其中一个密钥是广泛可用的公有密钥，另一个密钥是未公开的私钥。

勒索软件是一种基于密码学的恶意软件，即使用加密技术构建恶意软件。此恶意软件可以使用对称密钥加密和非对称密钥加密来锁定受影响的数据，并要求勒索以提供密钥来对受影响的数据进行解密。

勒索软件的工作原理是什么？

以下步骤介绍勒索软件如何使用加密技术对受害者的数据进行加密，而不会为受害者提供任何解密或恢复范围：

1. 与非对称密钥加密一样，攻击者会生成密钥对。生成的公有密钥将放置在该恶意软件中，然后释放该恶意软件。
2. 恶意软件进入受影响用户的计算机或系统后，它会使用伪数字生成器（ Pseudorandom Number Generator ， PRG ）或任何其他可行的随机数字生成算法生成一个随机对称密钥。
3. 恶意软件使用此对称密钥对受影响的数据进行加密。它最终会使用恶意软件中嵌入的攻击者的公有密钥对对称密钥进行加密。此步骤的输出是加密对称密钥的非对称密文和受影响数据的对称密文。
4. 恶意软件会将受害者的数据以及用于加密数据的对称密钥置零（擦除），从而无法进行恢复。
5. 现在，系统会向受影响的用户显示对称密钥的非对称密钥文本以及为获取用于加密数据的对称密钥而必须支付的勒索金额。
6. 受害者支付勒索费用，并与攻击者共享非对称密码短文。攻击者使用其私钥对密码短文进行解密，从而导致出现对称密钥。
7. 攻击者与受影响的用户共享此对称密钥，此密钥可用于对所有数据进行解密，从而从攻击中恢复。

挑战

个人和组织在遭受勒索软件攻击时面临以下挑战：

- 最重要的挑战是， IT 会立即影响组织或个人的工作效率。恢复正常状态需要一些时间，因为所有重要文件都必须重新获取，并且系统必须安全。
- 它可能会导致数据泄露，其中包含属于客户或客户的敏感机密信息，并导致组织显然希望避免的危机情况。
- 数据很有可能落入不当之手或被彻底擦除，从而导致无法返回，可能对组织和个人造成灾难性后果。
- 支付完勒索后，无法保证攻击者将提供密钥来还原数据。

- 目前无法保证攻击者在支付了勒索之后仍不会广播敏感数据。
- 在大型企业中，识别导致勒索软件攻击的漏洞是一项繁琐的任务，确保所有系统的安全需要付出大量的努力。

谁面临风险?

任何人都可能受到勒索软件的攻击，包括个人和大型组织。如果组织未实施定义明确的安全措施和实践，则更容易受到此类攻击。攻击对大型组织的影响可能比个人承受的影响要大几倍。

勒索软件大约占所有恶意软件攻击的 28% 。换言之，每四个恶意软件事件中就有一个以上是勒索软件攻击。勒索软件可以自动和不分青红皂白地通过互联网传播，一旦发生安全问题，它就可以进入受影响的系统并继续传播到其他已连接的系统。攻击者往往会将目标锁定在执行大量文件共享，拥有大量敏感和关键数据或未充分防范攻击的人员或组织。

攻击者往往关注以下潜在目标：

- 大学和学生社区
- 政府部门和机构
- 医院
- 银行

这并不是详尽的目标列表。如果您不属于这些类别之一，则您将无法认为自己不会受到攻击。

勒索软件如何进入系统或传播?

勒索软件可以通过多种方式进入系统或传播到其他系统。在当今世界，几乎所有系统都通过互联网， LAN ， WAN 等相互连接。在这些系统之间生成和交换的数据量只会增加。

勒索软件的一些最常见传播方式包括我们每天用于共享或访问数据的方法：

- email
- P2P 网络
- 文件下载
- 社交网络
- 移动设备
- 连接到不安全的公有网络
- 访问 Web URL

数据丢失的后果

数据丢失的后果或影响可能会比企业预期的范围更广。根据停机持续时间或组织无法访问其数据的时间段，这些影响可能会有所不同。攻击持续时间越长，对组织收入，品牌和声誉的影响就越大。企业还可能面临法律问题和生产率急剧下降。

随着这些问题持续存在，它们开始放大，并可能最终改变组织的文化，具体取决于组织如何应对攻击。在当今世界，信息迅速传播，有关组织的负面新闻可能会对其声誉造成发生原因永久损害。企业可能会因数据丢失而面临巨大的处罚，最终可能导致业务关闭。

财务影响

据最近的一份报告称 "McAfee 报告"网络犯罪造成的全球成本约为 6000 亿美元，约占全球 GDP 的 0.8% 。与全球互联网经济增长 4.2 万亿美元相比，这一金额相当于对增长征收 14% 的税。

勒索软件在这一财务成本中占很大比例。2018 年，勒索软件攻击所产生的成本约为 80 亿美元—预计 2019 年将达到 115 亿美元。

什么是解决方案?

只有通过实施主动式灾难恢复计划，才能在最短停机时间内从勒索软件攻击中恢复。拥有从攻击中恢复的能力是不错的，但完全防止攻击是理想之选。

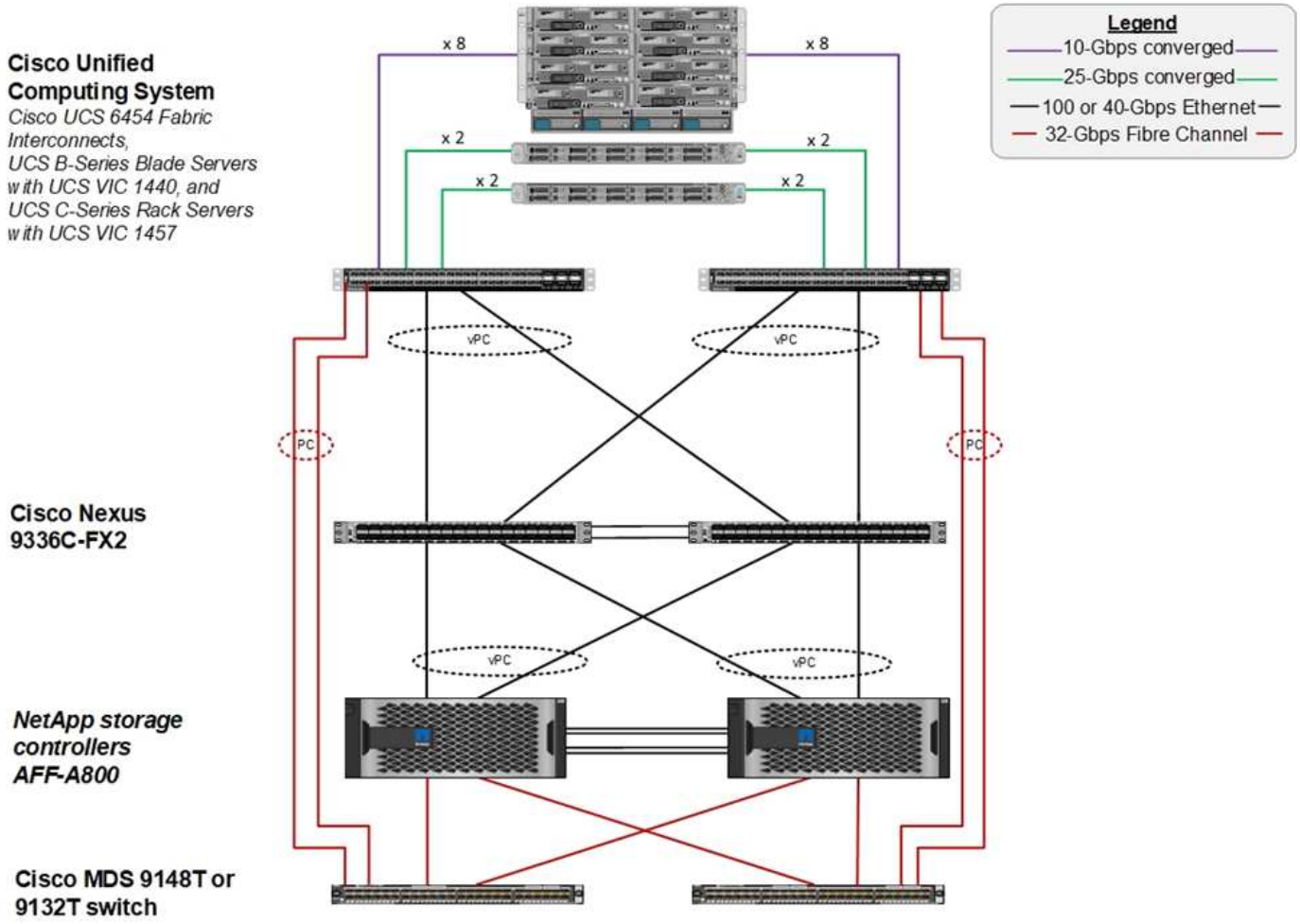
尽管为了防止攻击，您必须查看和修复几个方面，但允许您防止或从攻击中恢复的核心组件是数据中心。

数据中心的设计及其为保护网络，计算和存储端点提供的功能对于构建安全的日常运营环境起着至关重要的作用。本文档介绍了 FlexPod 混合云基础架构的功能如何帮助在发生攻击时快速恢复数据，以及如何帮助全面防止攻击。

FlexPod 概述

FlexPod 是一种经过预先设计，集成和验证的架构，可将 Cisco 统一计算系统（ Cisco UCS ）服务器， Cisco Nexus 系列交换机， Cisco MDS 光纤交换机和 NetApp 存储阵列组合到一个灵活的架构中。FlexPod 解决方案旨在实现高可用性，不会出现单点故障，同时保持成本效益和设计灵活性，以支持各种工作负载。FlexPod 设计可以支持不同的虚拟机管理程序和裸机服务器，也可以根据客户工作负载要求进行规模估算和优化。

下图展示了 FlexPod 架构，并清楚地突出了堆栈所有层的高可用性。存储，网络和计算等基础架构组件的配置方式使操作可以在其中一个组件发生故障时瞬时故障转移到正常运行的配对节点。



FlexPod 系统的一个主要优势是，它经过预先设计，集成和验证，可用于多个工作负载。每项解决方案验证都会发布详细的设计和部署指南。这些文档介绍了工作负载要在 FlexPod 上无缝运行所必须采用的最佳实践。这些解决方案采用同类最佳的计算，网络和存储产品以及一系列侧重于整个基础架构安全性和强化的功能。

"IBM 的 X-Force 威胁情报索引" 声明： " 由于人类错误，三分之二的记录受到破坏，包括配置不当的云基础架构在历史上的 424%" 。

借助 FlexPod 系统，您可以通过 Ansible 攻略手册使用自动化来避免配置不当基础架构，这些攻略手册会根据 Cisco 验证设计（ CVD ）和 NetApp 验证架构（ NVA ）中介绍的最佳实践对基础架构执行端到端设置。

勒索软件保护措施

本节介绍 NetApp ONTAP 数据管理软件以及适用于 Cisco UCS 和 Cisco Nexus 的工具的主要功能，您可以使用这些功能有效地保护和抵御勒索软件攻击。

存储： **NetApp ONTAP**

ONTAP 软件提供了许多对数据保护有用的功能，其中大多数功能对于拥有 ONTAP 系统的客户是免费的。您可以随时使用以下功能来保护数据免受攻击：

- * NetApp Snapshot 技术。 * Snapshot 副本是卷的只读映像，用于捕获文件系统在某一时间点的状态。这些副本有助于保护数据，而不会影响系统性能，同时也不会占用大量存储空间。NetApp 建议您创建 Snapshot 副本创建计划。您还应保持较长的保留时间，因为某些恶意软件可能会休眠，然后在感染后数周或数月重新

激活。发生攻击时，可以使用感染前创建的 Snapshot 副本回滚卷。

- * NetApp SnapRestore 技术。 * SnapRestore 数据恢复软件对于从数据损坏中恢复或仅还原文件内容非常有用。SnapRestore 不会还原卷的属性；它比管理员通过将文件从 Snapshot 副本复制到活动文件系统来实现的速度快得多。如果必须尽快恢复多个文件，则恢复数据的速度会很有用。在发生攻击时，这种高效的恢复过程有助于快速恢复业务联机。
- * NetApp SnapCenter 技术。 * SnapCenter 软件使用基于 NetApp 存储的备份和复制功能来提供应用程序一致的数据保护。该软件可与企业级应用程序集成，并提供特定于应用程序和数据库的工作流，以满足应用程序，数据库和虚拟基础架构管理员的需求。SnapCenter 提供了一个易于使用的企业平台，用于在应用程序，数据库和文件系统之间安全地协调和管理数据保护。它能够提供应用程序一致的数据保护，这在数据恢复期间至关重要，因为它可以轻松地将应用程序更快地还原到一致的状态。
- * NetApp SnapLock 技术。 * SnapLock 提供了一个特殊用途卷，可在其中存储文件并将其提交到不可擦除，不可重写的状态。驻留在 FlexVol 卷中的用户生产数据可以分别通过 NetApp SnapMirror 或 SnapVault 技术镜像或存储到 SnapLock 卷。在保留期限结束之前，无法删除 SnapLock 卷，卷本身及其托管聚合中的文件。
- * NetApp FPolicy 技术。 * 使用 FPolicy 软件禁止对具有特定扩展名的文件执行操作，以防止受到攻击。可以为特定文件操作触发 FPolicy 事件。此事件与策略相关联，策略将调用需要使用的引擎。您可以为策略配置一组可能包含勒索软件的文件扩展名。如果具有不允许扩展名的文件尝试执行未经授权的操作，则 FPolicy 会阻止执行该操作。

网络： **Cisco Nexus**

Cisco NX OS 软件支持可增强网络异常检测和安全性的网络流功能。网络流可捕获网络上每个对话的元数据，通信所涉及的各方，正在使用的协议以及事务持续时间。对信息进行汇总和分析后，可以深入了解正常行为。

通过收集的数据，还可以确定可疑的活动模式，例如恶意软件在网络中传播，否则可能会被忽视。

网络流使用流为网络监控提供统计信息。流量是指到达源接口（或 VLAN ）且密钥值相同的单向数据包流。密钥是指数据包中某个字段的标识值。您可以使用流记录创建流，以便为流定义唯一密钥。您可以使用流量导出器将网络流为流收集的数据导出到远程网络流收集器，例如 Cisco Stealthwatch 。Stealthwatch 使用此信息持续监控网络，并在发生勒索软件爆发时提供实时威胁检测和意外事件响应取证。

计算： **Cisco UCS**

Cisco UCS 是 FlexPod 架构中的计算端点。您可以使用多种 Cisco 产品来帮助在操作系统级别保护堆栈的这一层。

您可以在计算或应用程序层实施以下关键产品：

- * 适用于端点的 Cisco 高级恶意软件保护（ AMP ）。 * 此解决方案在 Microsoft Windows 和 Linux 操作系统上受支持，集成了预防，检测和响应功能。此安全软件可防止违规行为，在入口点阻止恶意软件，并持续监控和分析文件和流程活动，以快速检测，控制和修复可能规避前线防护的威胁。

  AMP 的恶意活动保护（ MAP ）组件持续监控所有端点活动，并提供运行时检测和阻止端点上正在运行的程序的异常行为。例如，如果端点行为表明存在勒索软件，则会终止违规流程，从而阻止端点加密并阻止攻击。

- * 通过 Cisco 高级恶意软件保护实现电子邮件安全。 * 电子邮件已成为传播恶意软件和实施网络攻击的主要工具。平均而言，一天内会交换大约 1000 亿封电子邮件，这为攻击者提供了一个极好的渗透载体，可以渗透到用户的系统中。因此，抵御这种攻击是绝对必要的。

  AMP 可分析电子邮件中隐藏在恶意附件中的威胁，例如零日攻击和窃取恶意软件。此外，它还利用行业领

先的 URL 智能来打击恶意链路。它可以为用户提供高级保护，防止他们遭受鱼叉式网络攻击，勒索软件和其他复杂攻击。

- * 下一代入侵防护系统（ NGIP ）。 * Cisco Firepower NGIP 可以部署为数据中心中的物理设备，也可以部署为 VMware 上的虚拟设备（ NGIPSv for VMware ）。这种高效的入侵防护系统可提供可靠的性能和较低的总拥有成本。威胁保护可以通过可选的订阅许可证进行扩展，以提供 AMP ，应用程序可见性和控制以及 URL 筛选功能。虚拟化的 NGIP 可检查虚拟机（ VM ）之间的流量，并在资源有限的站点上更轻松地部署和管理 NGIP 解决方案，从而增强对物理和虚拟资产的保护。

保护和恢复 FlexPod 上的数据

本节介绍在发生攻击时如何恢复最终用户的数据，以及如何使用 FlexPod 系统防止攻击。

测试台概述

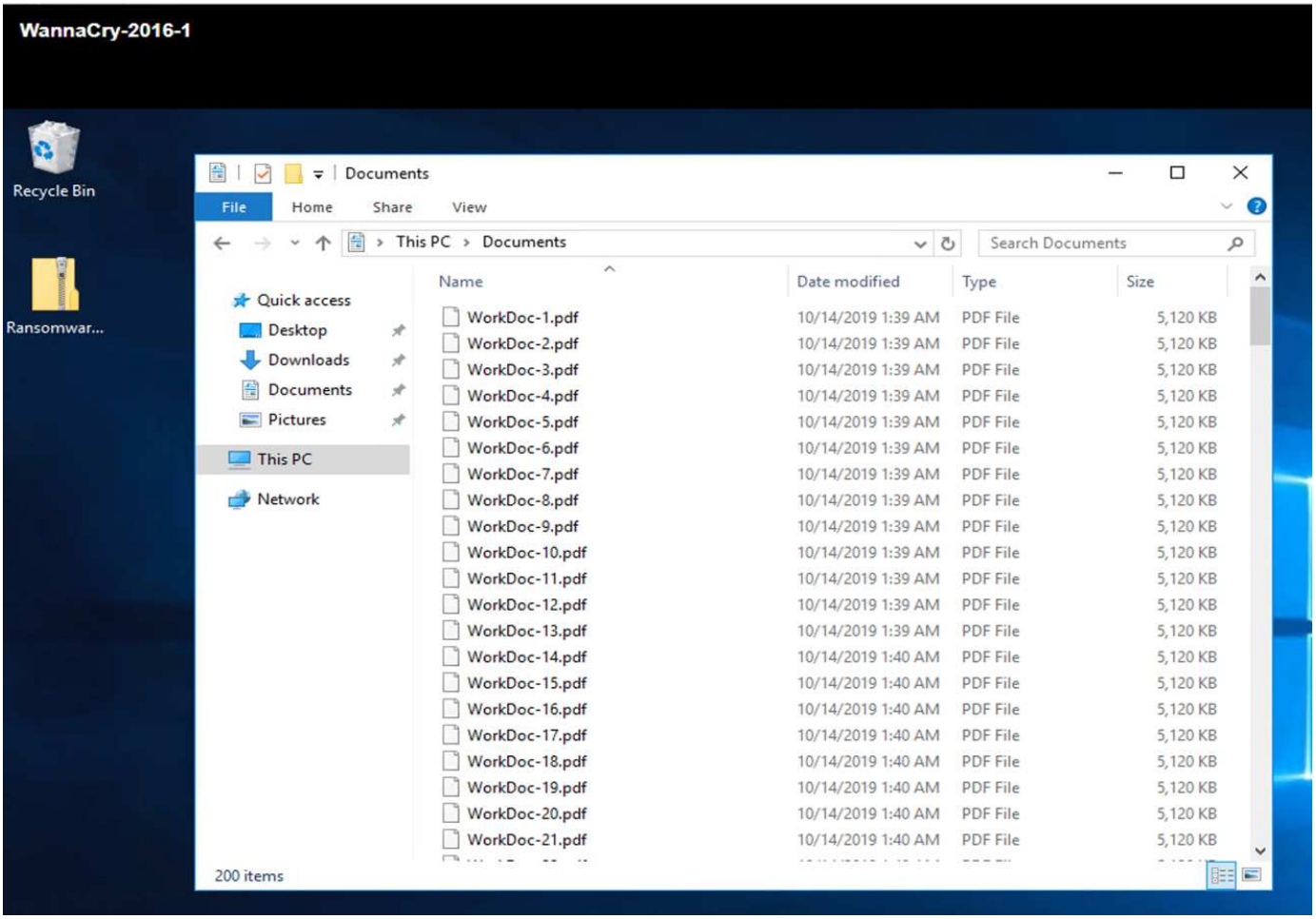
为了展示 FlexPod 的检测，修复和预防，我们根据编写本文档时提供的最新平台 CVD 中指定的准则构建了一个测试台： "采用 VMware vSphere 6.7 U1 ， Cisco UCS 第四代和 NetApp AFF A 系列 CVD 的 FlexPod 数据中心"。

在 VMware vSphere 基础架构中部署了一个 Windows 2016 VM ，该 VM 通过 NetApp ONTAP 软件提供 CIFS 共享。然后，在 CIFS 共享上配置了 NetApp FPolicy ，以防止执行具有特定扩展类型的文件。此外，还部署了 NetApp SnapCenter 软件来管理基础架构中 VM 的 Snapshot 副本，以提供应用程序一致的 Snapshot 副本。

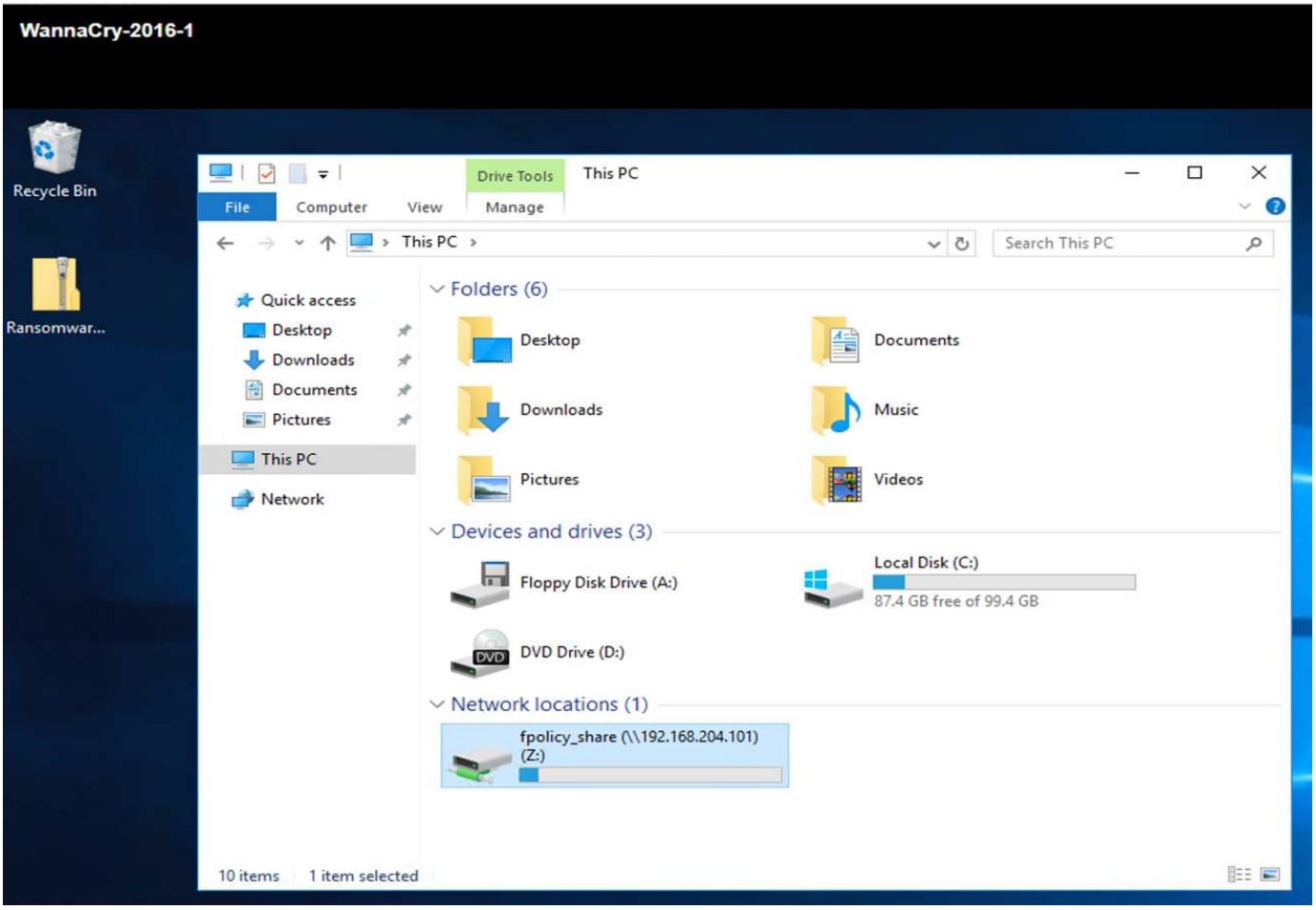
发生攻击前的虚拟机状态及其文件

本节显示了在对虚拟机进行攻击之前文件的状态以及映射到该虚拟机的 CIFS 共享。

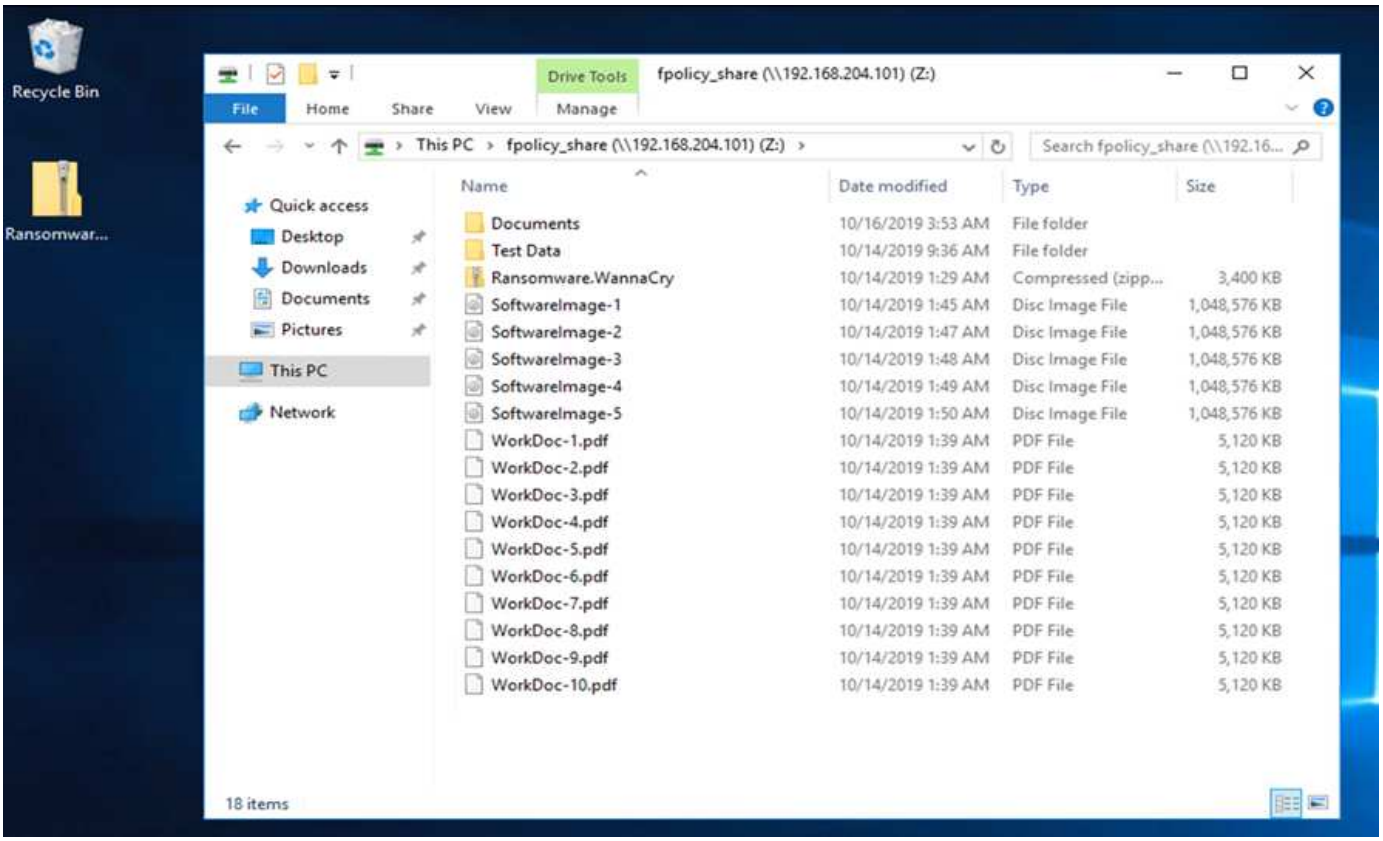
VM 的 Documents 文件夹包含一组 PDF 文件，这些文件尚未被 WannaCry 恶意软件加密。



以下屏幕截图显示了映射到虚拟机的 CIFS 共享。



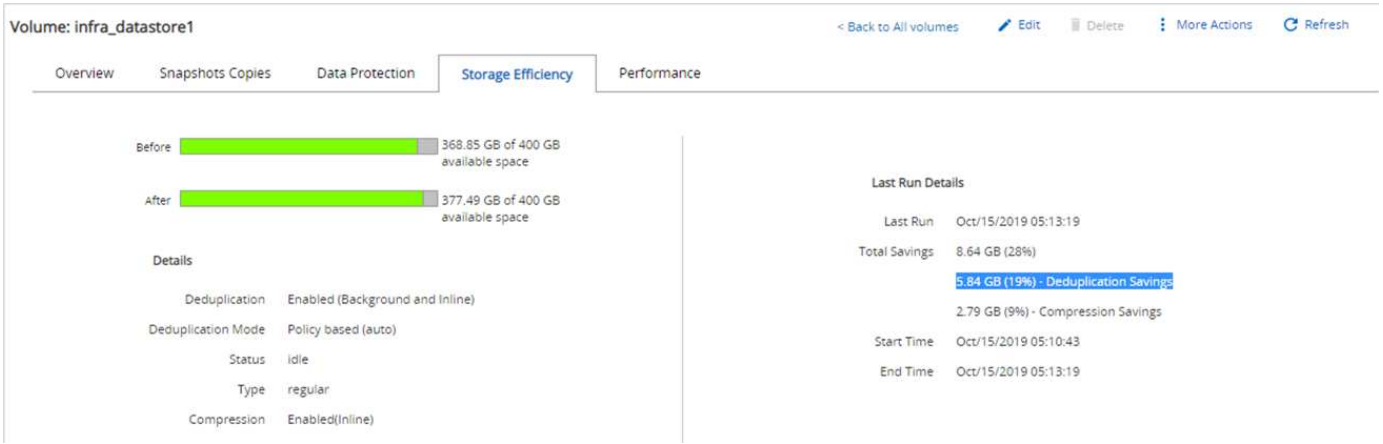
以下屏幕截图显示了 CIFS 共享 `fpolicy_share` 上尚未被 WannaCry 恶意软件加密的文件。



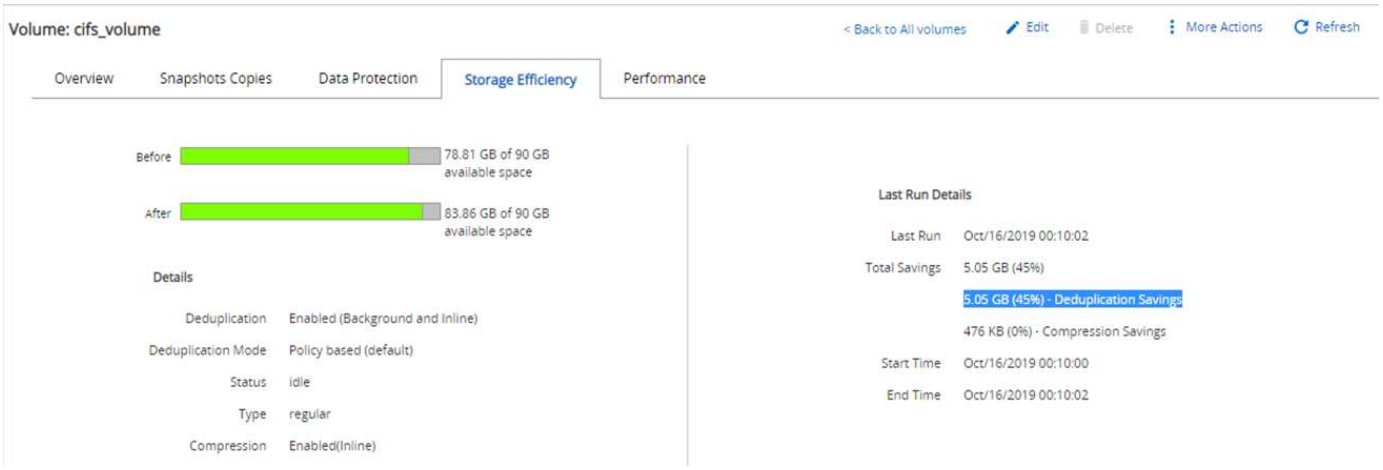
攻击前的重复数据删除和 **Snapshot** 信息

在检测阶段，系统会指示并参考 Snapshot 副本在攻击之前的存储效率详细信息和大小。

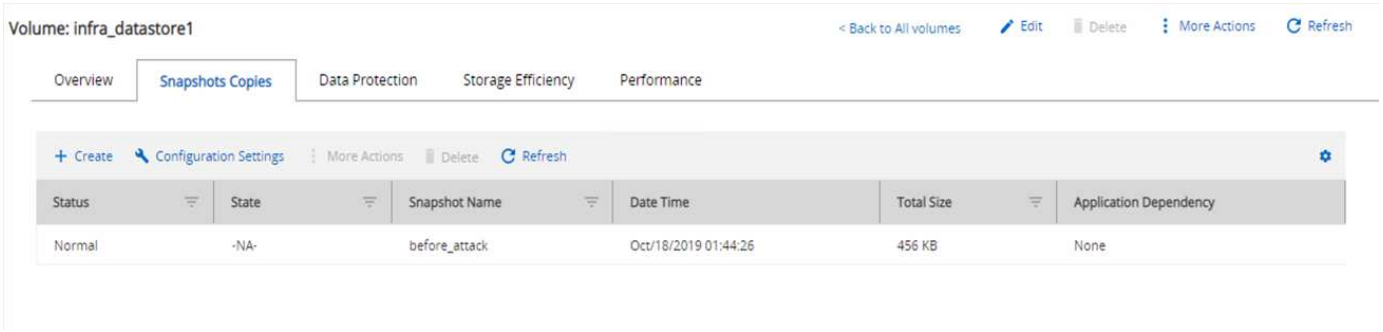
通过对托管 VM 的卷执行重复数据删除，存储节省了 19% 。



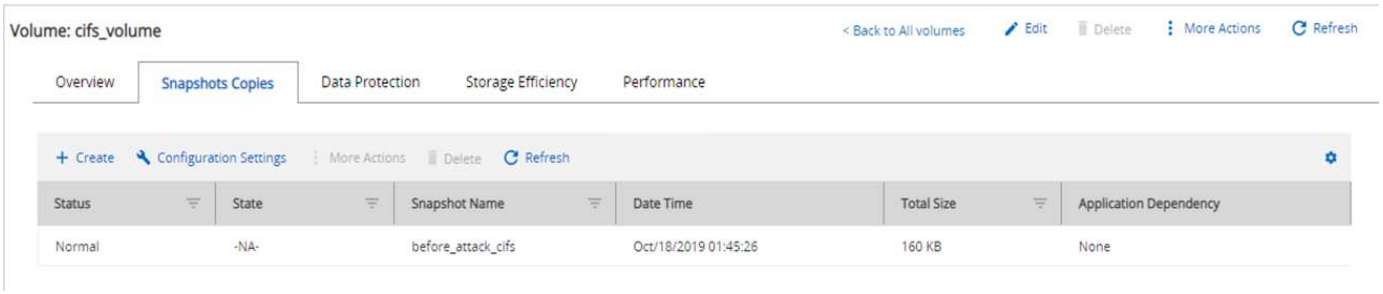
通过对 CIFS 共享 `fpolicy_share` 执行重复数据删除，存储节省了 45% 。



对于托管 VM 的卷，观察到 Snapshot 副本大小为 456 KB 。



对于 CIFS 共享 `fpolicy_share` ，观察到的 Snapshot 副本大小为 160 KB 。



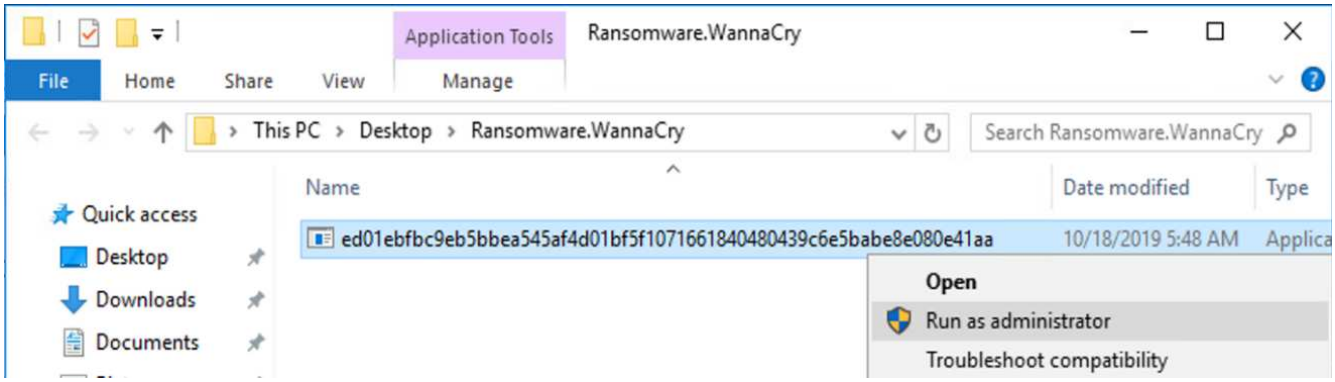
VM 和 CIFS 共享上的 WannaCry 感染

在本节中，我们将介绍 WannaCry 恶意软件是如何引入 FlexPod 环境的，以及随后观察到的系统更改。

以下步骤说明了 WannaCry 恶意软件二进制文件是如何引入 VM 的：

1. 已提取受保护的恶意软件。

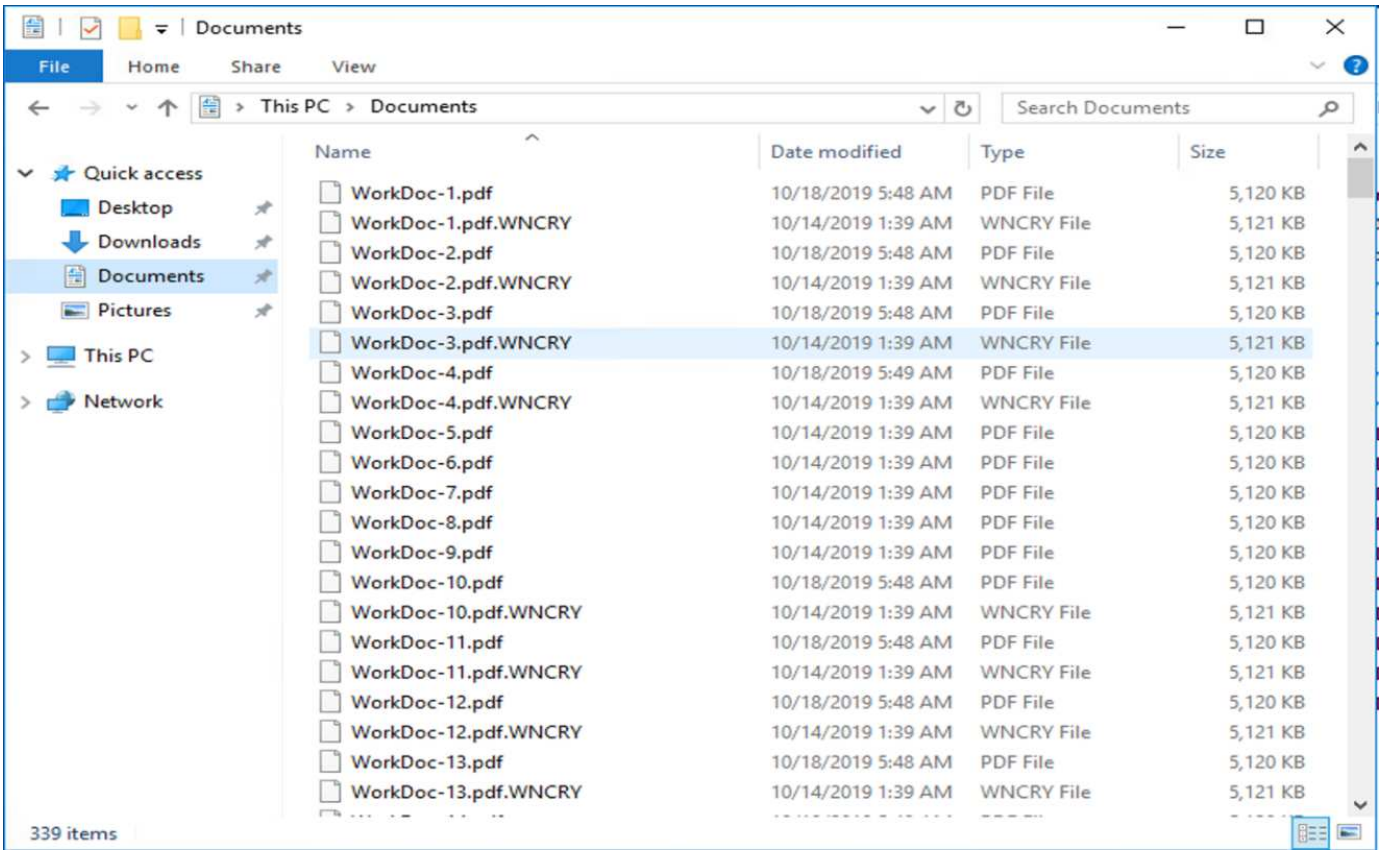
2. 已执行二进制文件。



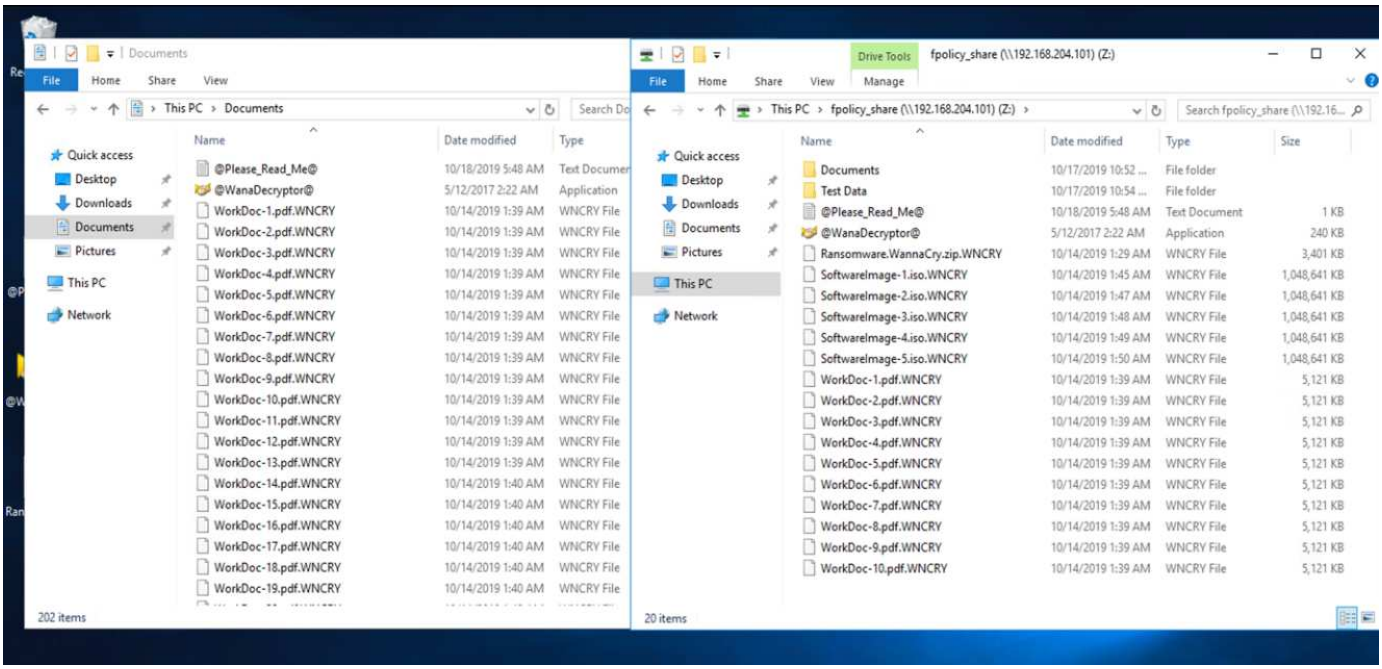
案例 **1**： **WannaCry** 对 **VM** 和映射的 **CIFS** 共享中的文件系统进行加密

本地文件系统和映射的 CIFS 共享已被 WannaCry 恶意软件加密。

恶意软件开始对具有 WNCRY 扩展名的文件进行加密。



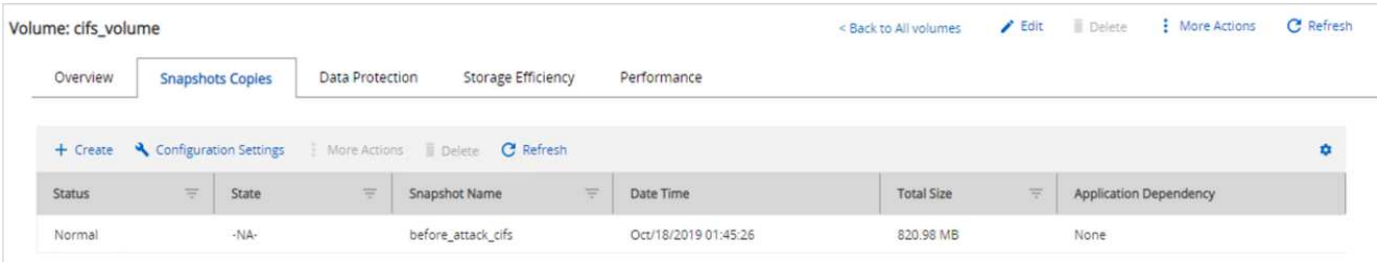
恶意软件会对本地 VM 和映射共享中的所有文件进行加密。



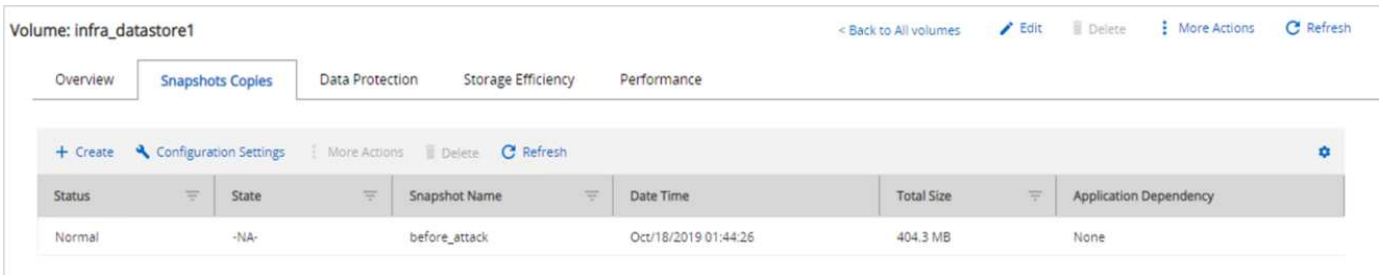
检测

从恶意软件开始对文件进行加密的那一刻起，它就触发了 Snapshot 副本大小的指数级增长以及存储效率百分比的指数级下降。

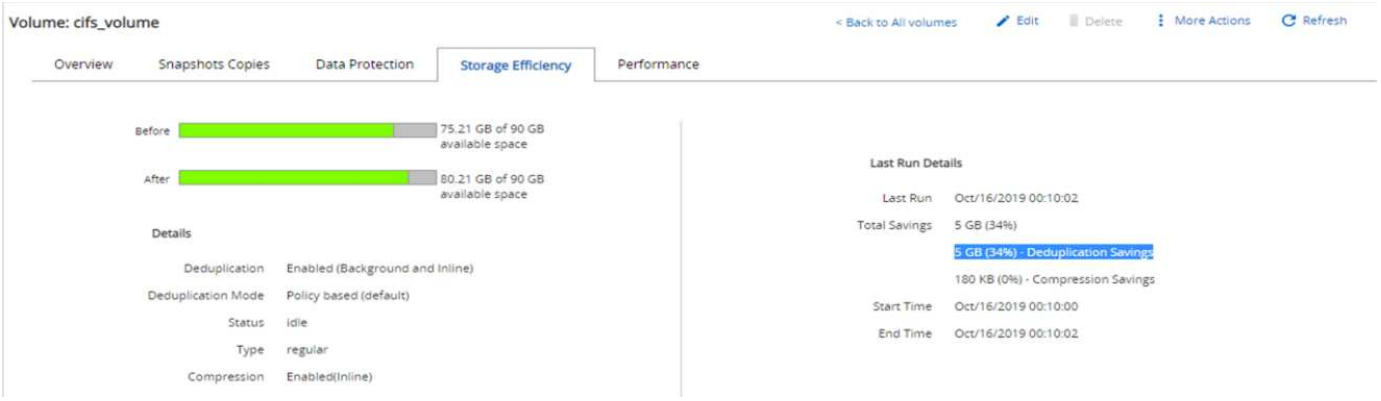
我们检测到，在攻击期间，托管 CIFS 共享的卷的 Snapshot 大小大幅增加到 820.98MB 。



我们检测到托管 VM 的卷的 Snapshot 副本大小增加到了 404.3MB 。



托管 CIFS 共享的卷的存储效率降低到 34% 。



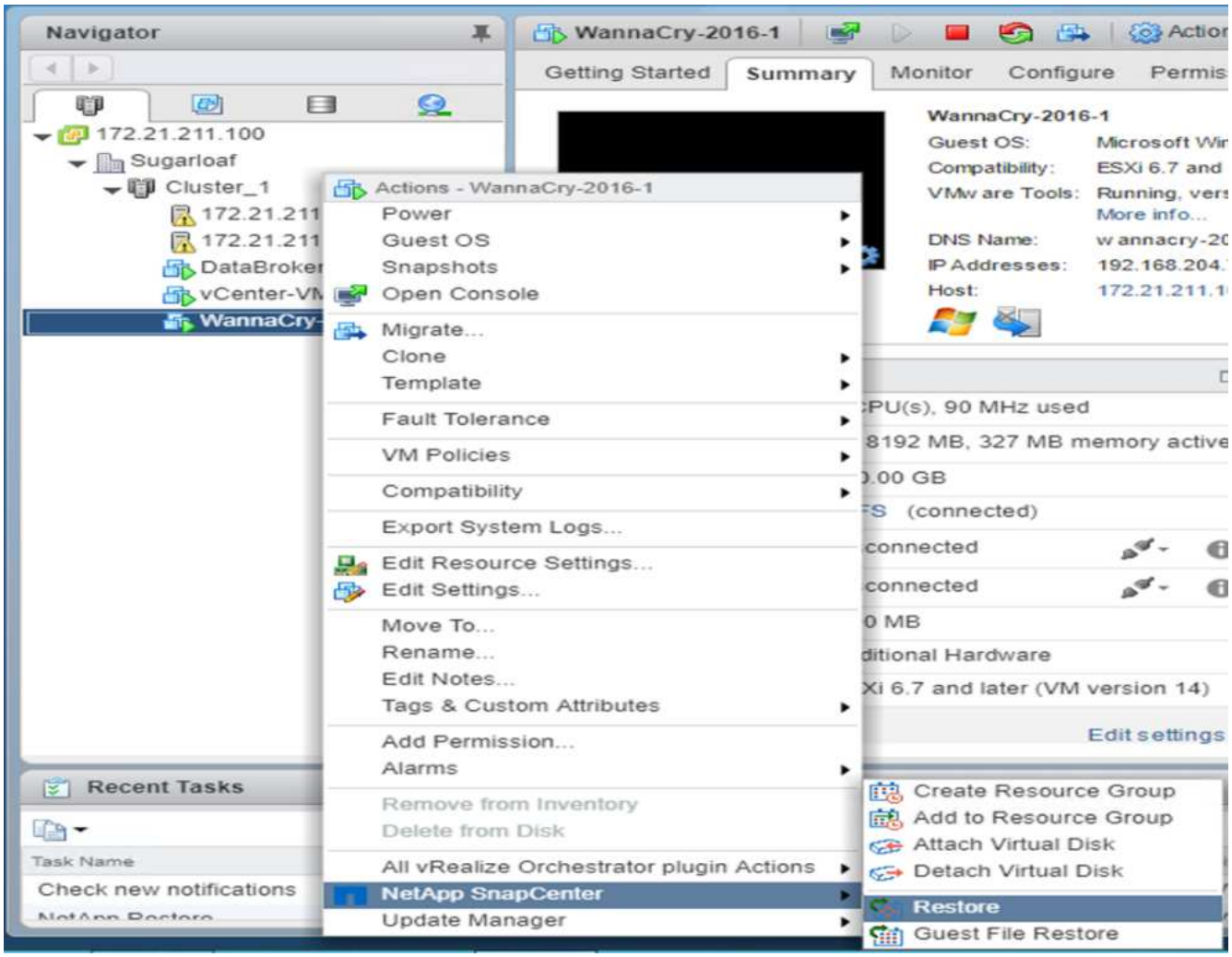
修复

在受到攻击之前使用全新 Snapshot 副本创建功能还原虚拟机和映射的 CIFS 共享。

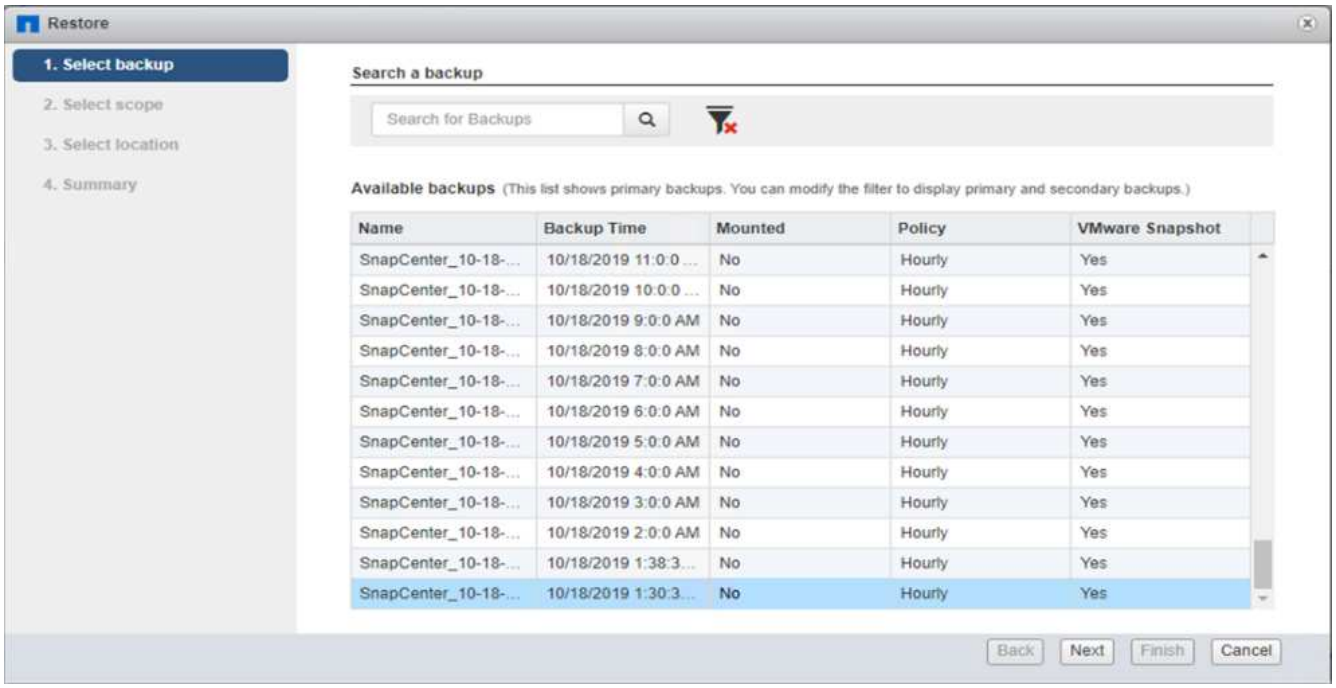
- 还原 VM*

要还原虚拟机，请完成以下步骤：

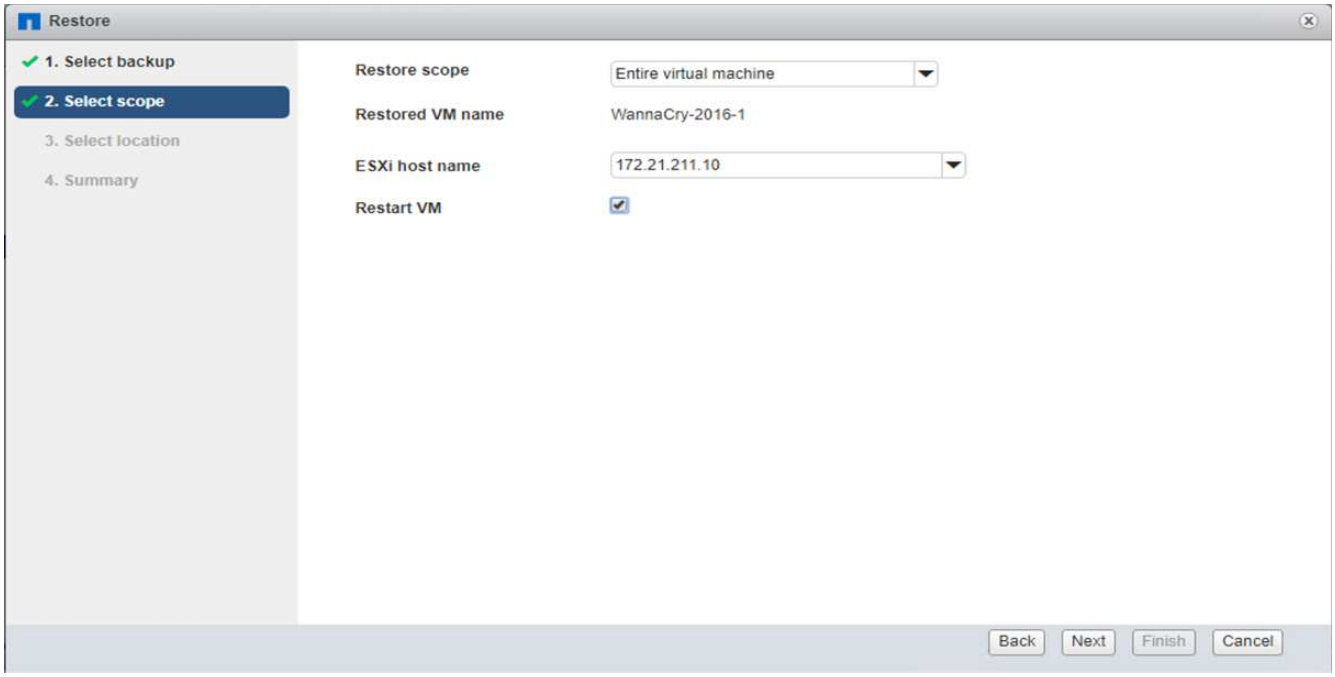
1. 使用您使用 SnapCenter 创建的 Snapshot 副本还原虚拟机。



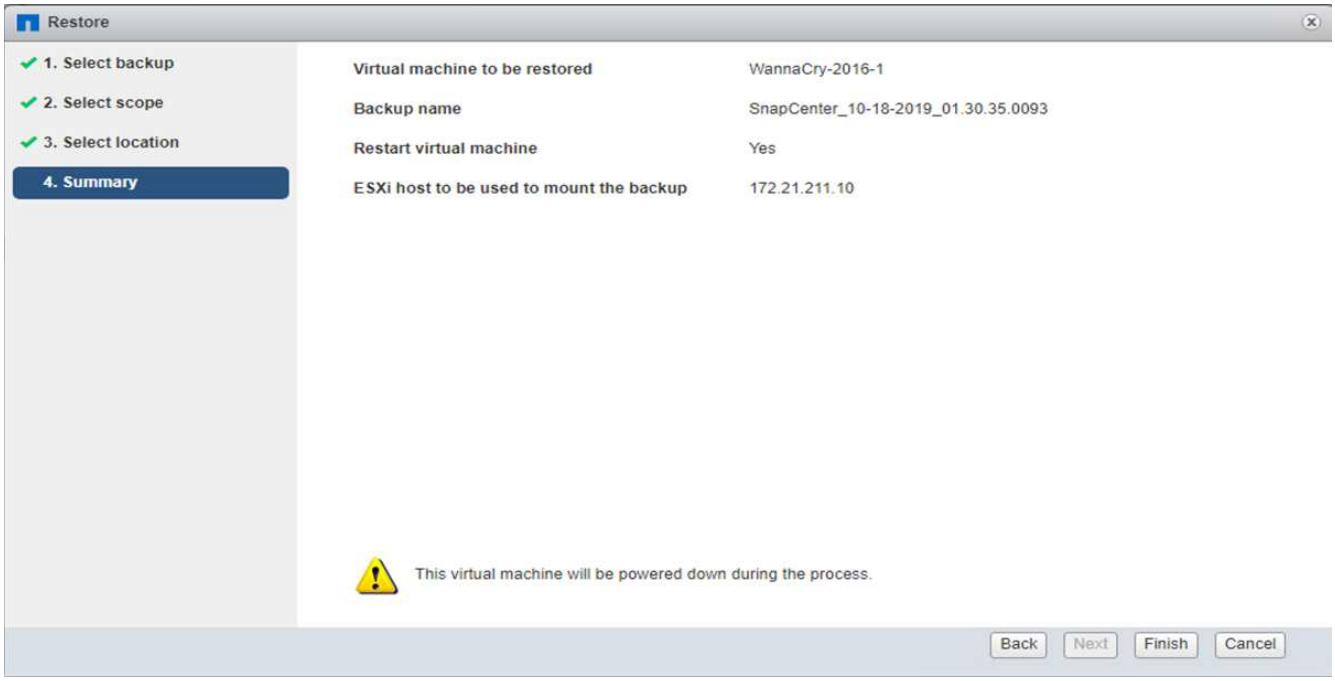
2. 选择所需的 VMware 一致 Snapshot 副本进行还原。



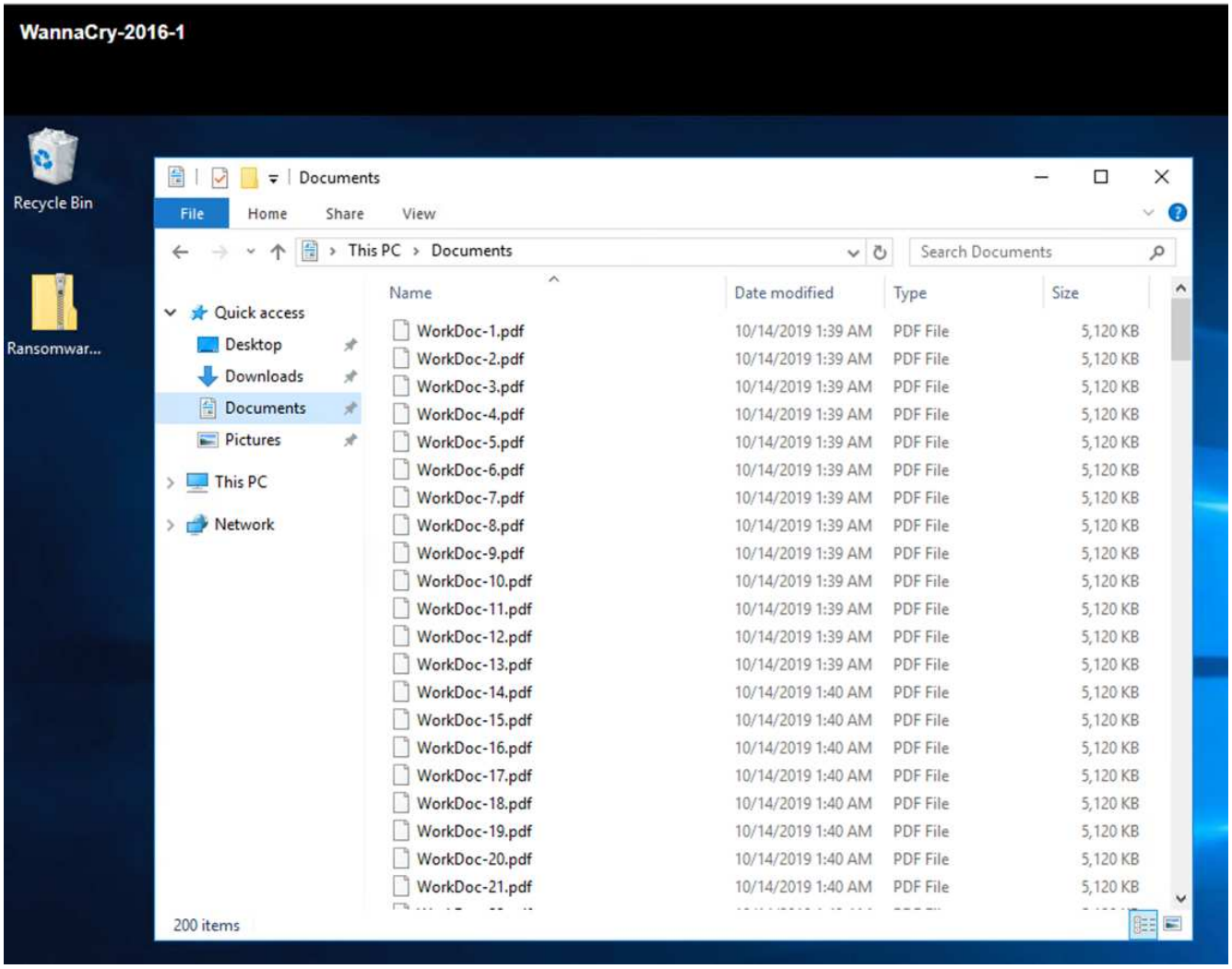
3. 此时将还原并重新启动整个 VM 。



4. 单击完成以启动还原过程。



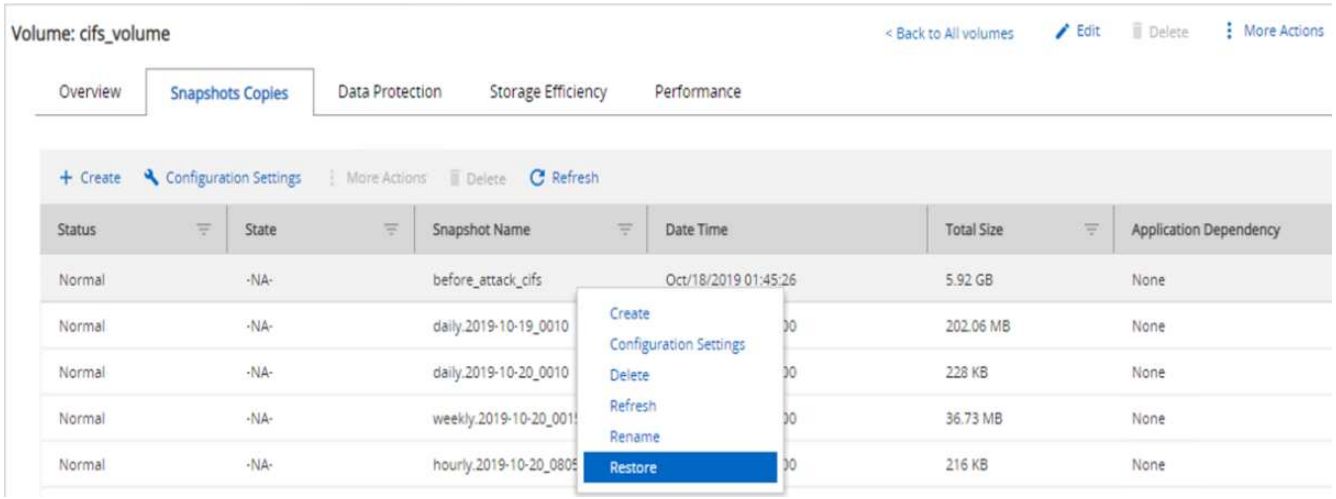
5. 虚拟机及其文件将会还原。



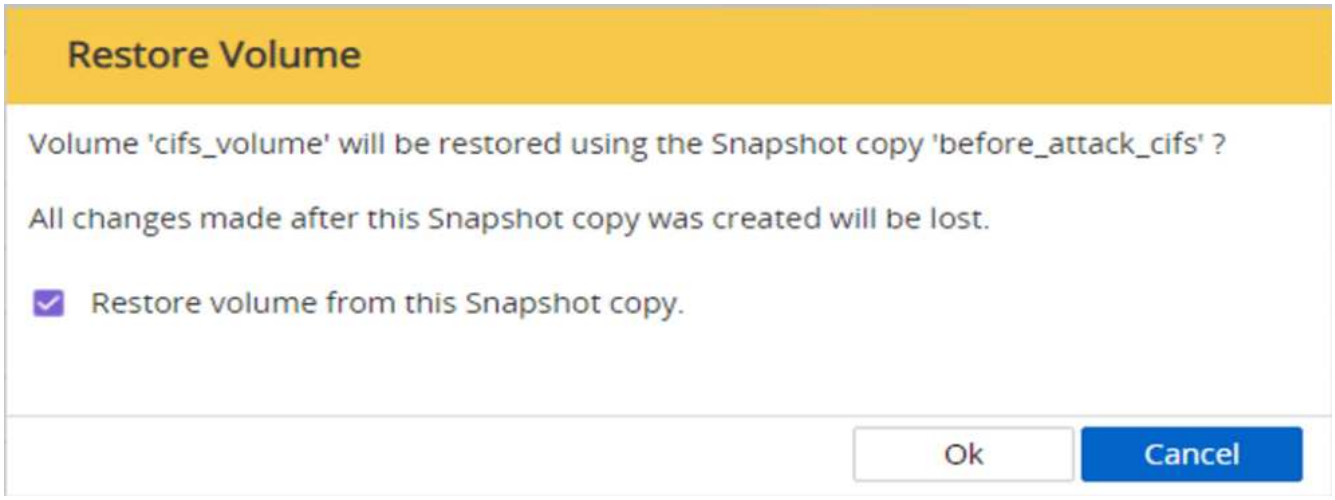
◦ 还原 CIFS 共享 *

要还原 CIFS 共享，请完成以下步骤：

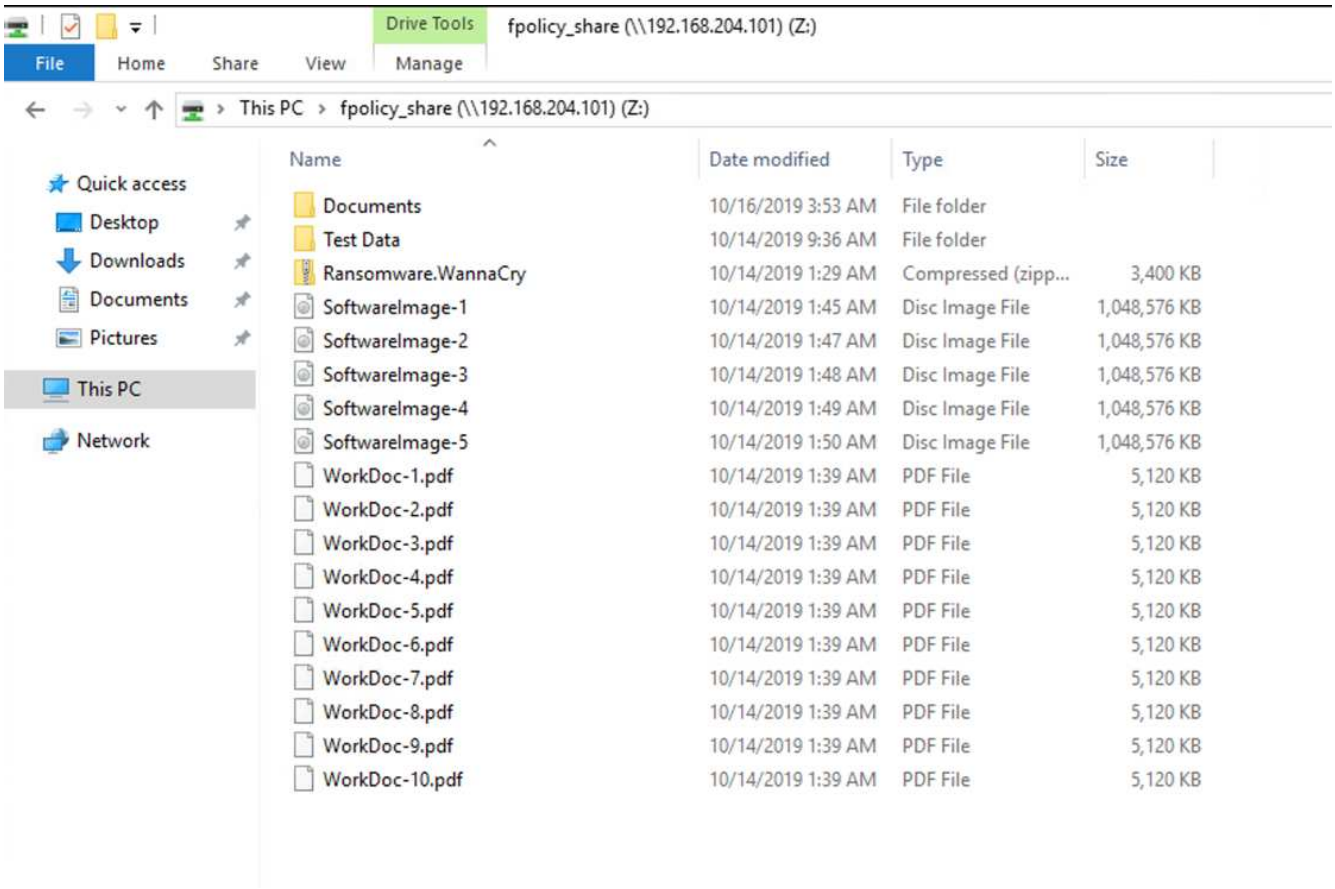
1. 使用攻击前创建的卷的 Snapshot 副本还原共享。



2. 单击确定以启动还原操作。



3. 还原后查看 CIFS 共享。



案例 **2**： **WannaCry** 对虚拟机中的文件系统进行加密，并尝试对通过 **FPolicy** 保护的映射 **CIFS** 共享进行加密

预防

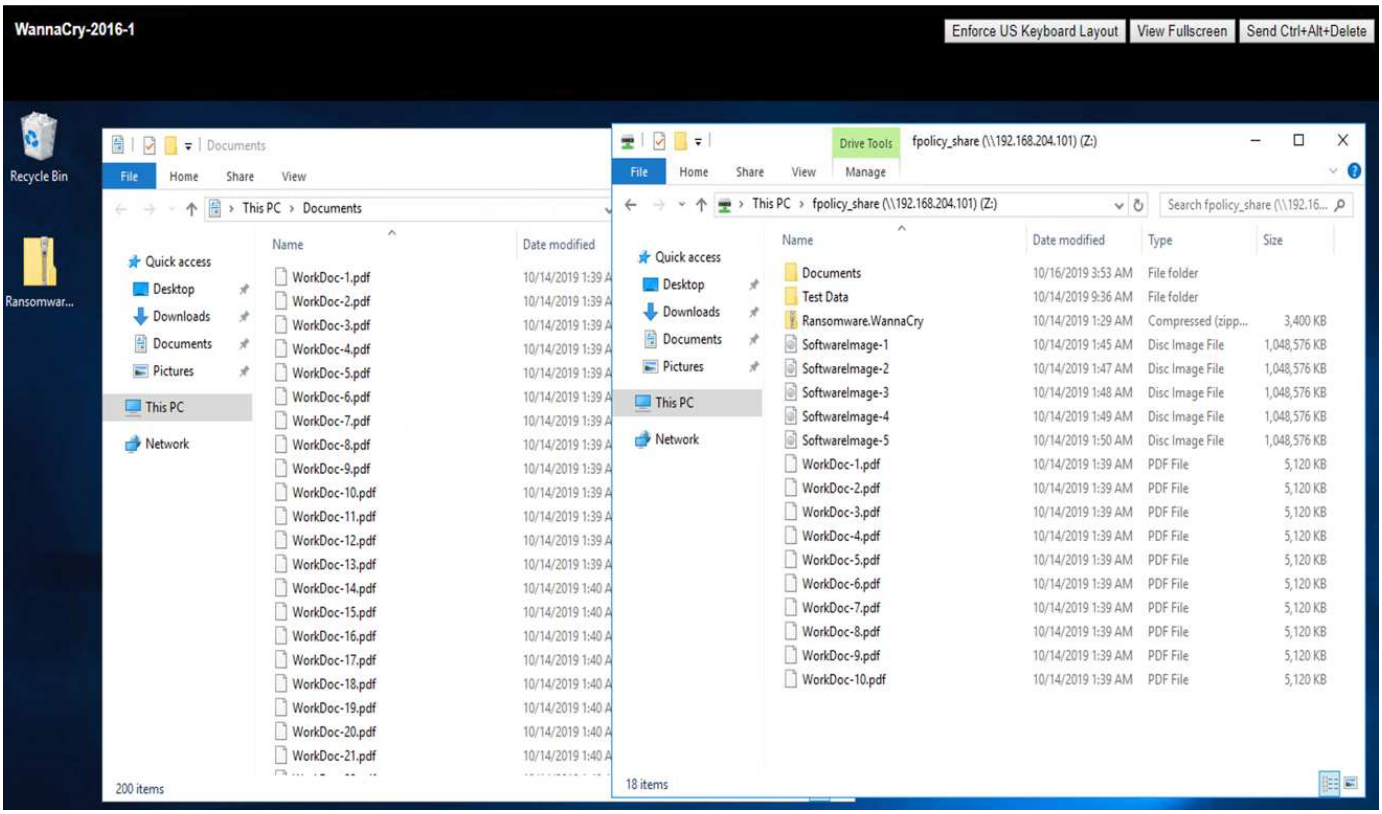
- 配置 FPolicy*

要在 CIFS 共享上配置 FPolicy ，请在 ONTAP 集群上运行以下命令：

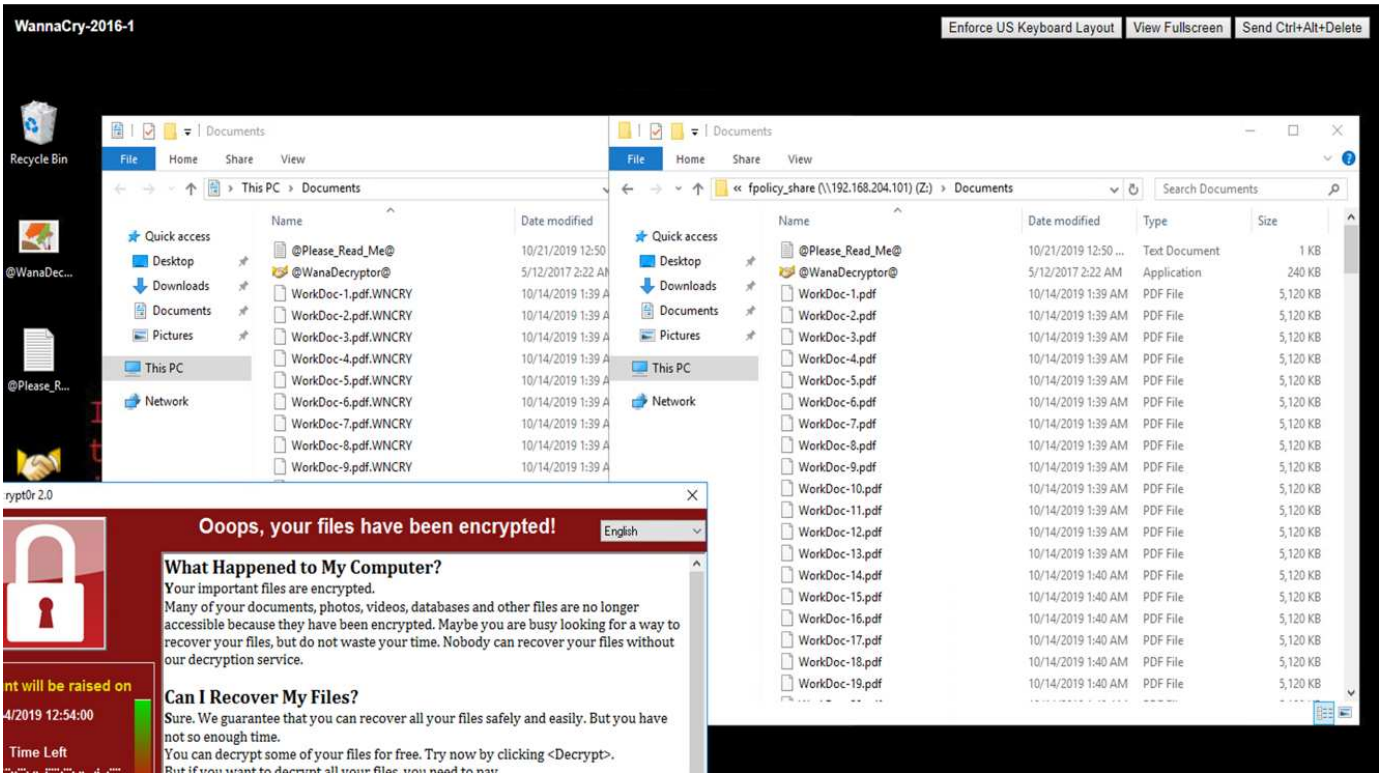
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create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

使用此策略时，不允许使用扩展名为 WNCRY ， Locky 和 ad4c 的文件执行文件操作 create ， rename ， write 或 open 。

查看文件在攻击前的状态—它们未加密且位于一个干净的系统中。



虚拟机上的文件已加密。WannaCry 恶意软件会尝试对 CIFS 共享中的文件进行加密，但 FPolicy 会防止其影响这些文件。



继续开展业务运营，无需支付任何费用

本文档中介绍的 NetApp 功能可帮助您在攻击发生后几分钟内还原数据，并从一开始就防止攻击，以便您可以无阻碍地继续开展业务运营。

可以设置 Snapshot 副本计划以满足所需的恢复点目标（ RPO ）。基于 Snapshot 副本的还原操作非常快速；因此，可以实现极低的恢复时间目标（ RTO ）。

最重要的是，您不必因攻击而支付任何勒索，您可以快速恢复正常运营。

结论

勒索软件是有组织犯罪的产物，攻击者不会按照道德标准行事。即使在收到勒索之后，他们也可以避免提供解密密钥。受害者不仅会丢失数据，还会损失大量资金，并将面临与生产数据丢失相关的后果。

根据 A "《福布斯》文章"只有 19% 的勒索软件受害者在支付了勒索之后才会获得数据。因此，作者建议在发生攻击时不要支付勒索，因为这样做会增强攻击者对其业务模式的信心。

数据备份和还原操作是勒索软件恢复的重要组成部分。因此，必须将它们作为业务规划的一个组成部分。实施这些操作的预算应用于，以便在发生攻击时恢复功能不会受到任何影响。

关键在于在此过程中选择正确的技术合作伙伴， FlexPod 可在纯闪存 FAS 系统中提供本机所需的大多数功能，而无需额外费用。

致谢

作者谨感谢以下人员为编写本文档提供的支持：

- NetApp 公司的 JORGE Gomez Navarrete
- NetApp 公司 Ganesh Kamath

追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- NetApp Snapshot 软件

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

- SnapCenter 备份管理

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

- SnapLock 数据合规性

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

- NetApp 产品文档

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

- Cisco 高级恶意软件保护（ 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"