FlexPod 和安全性

FlexPod

NetApp

October 30, 2025

目录

FlexPod 和安全性

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。

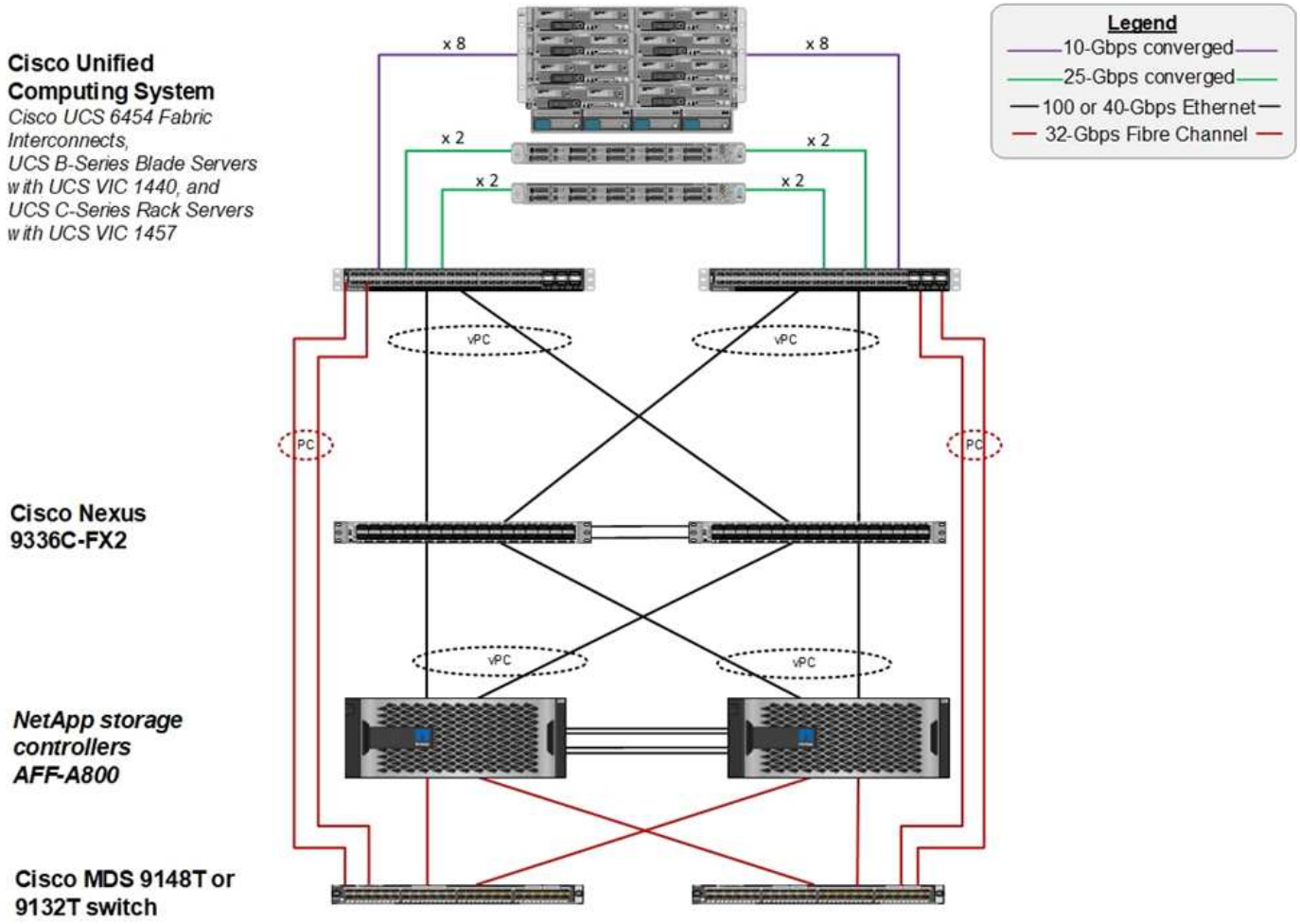
尽管为了防止攻击，您必须查看和修复几个方面，但允许您防止或从攻击中恢复的核心组件是数据中心。

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

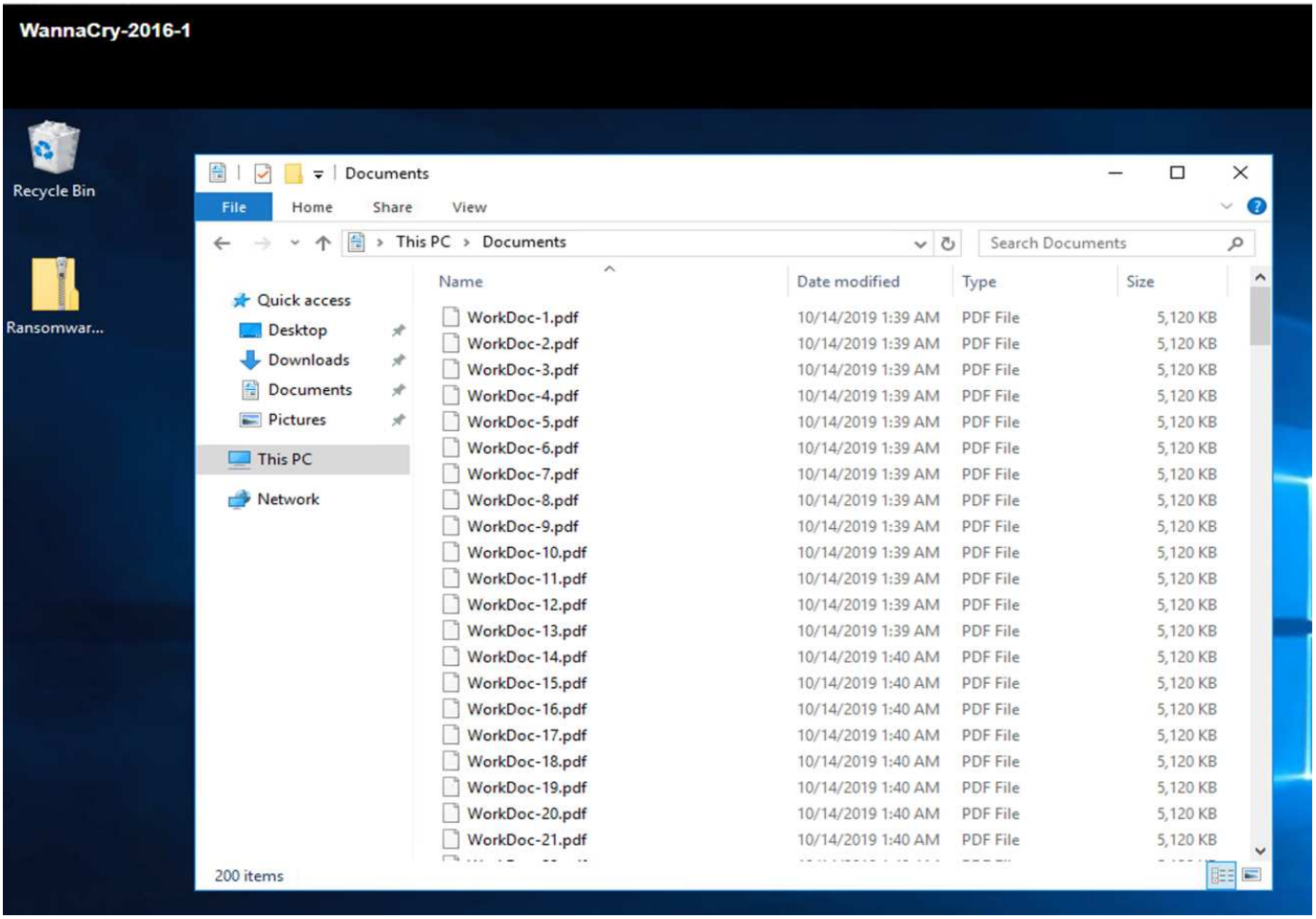
为了展示 FlexPod 的检测，修复和预防，我们根据编写本文档时提供的最新平台 CVD 中指定的准则构建了一个测试台： "采用 VMware vSphere 6.7 U1 ， Cisco UCS 第四代和 NetApp AFF A 系列 CVD 的 FlexPod 数据中心"。

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。

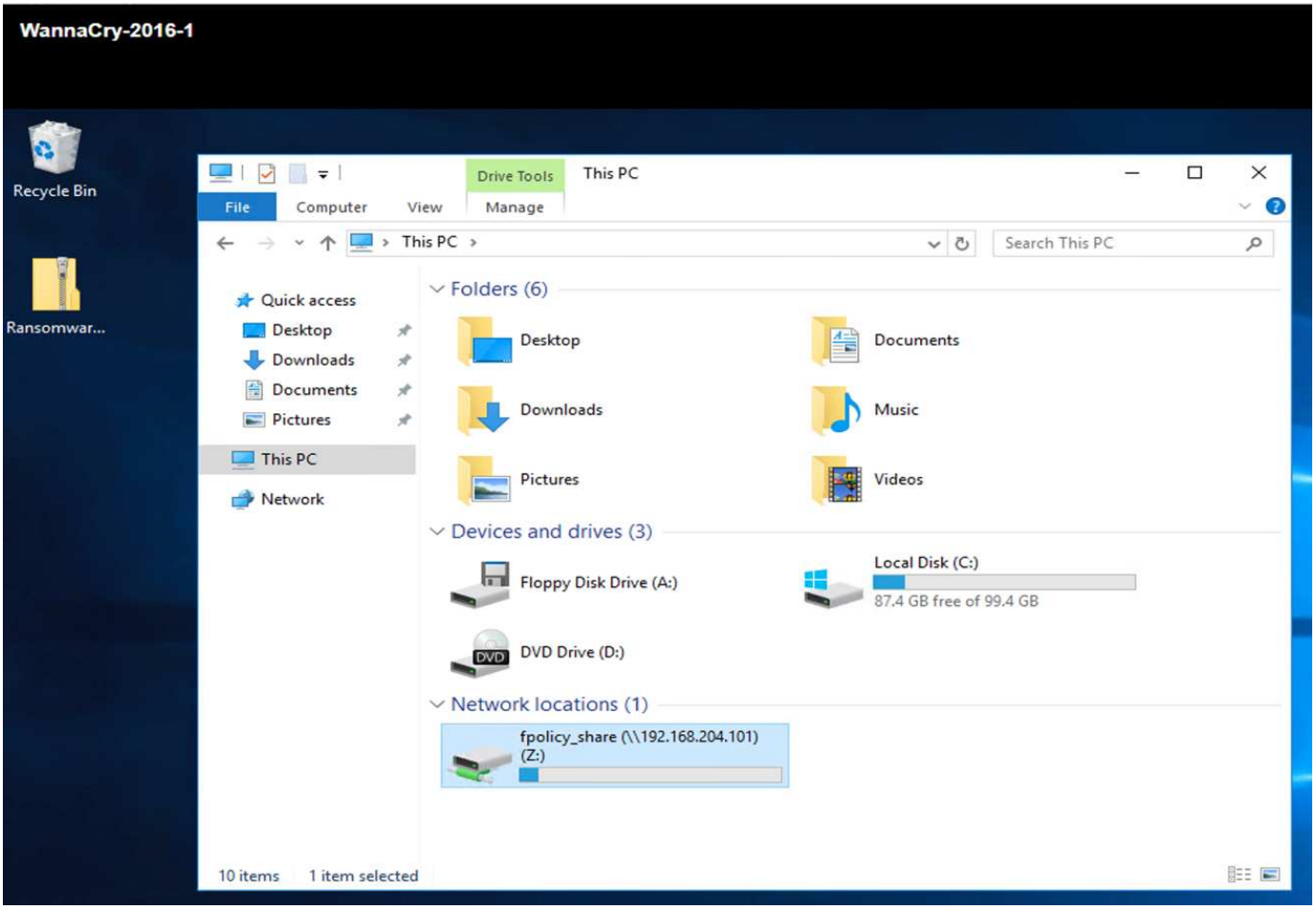
发生攻击前的虚拟机状态及其文件

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。

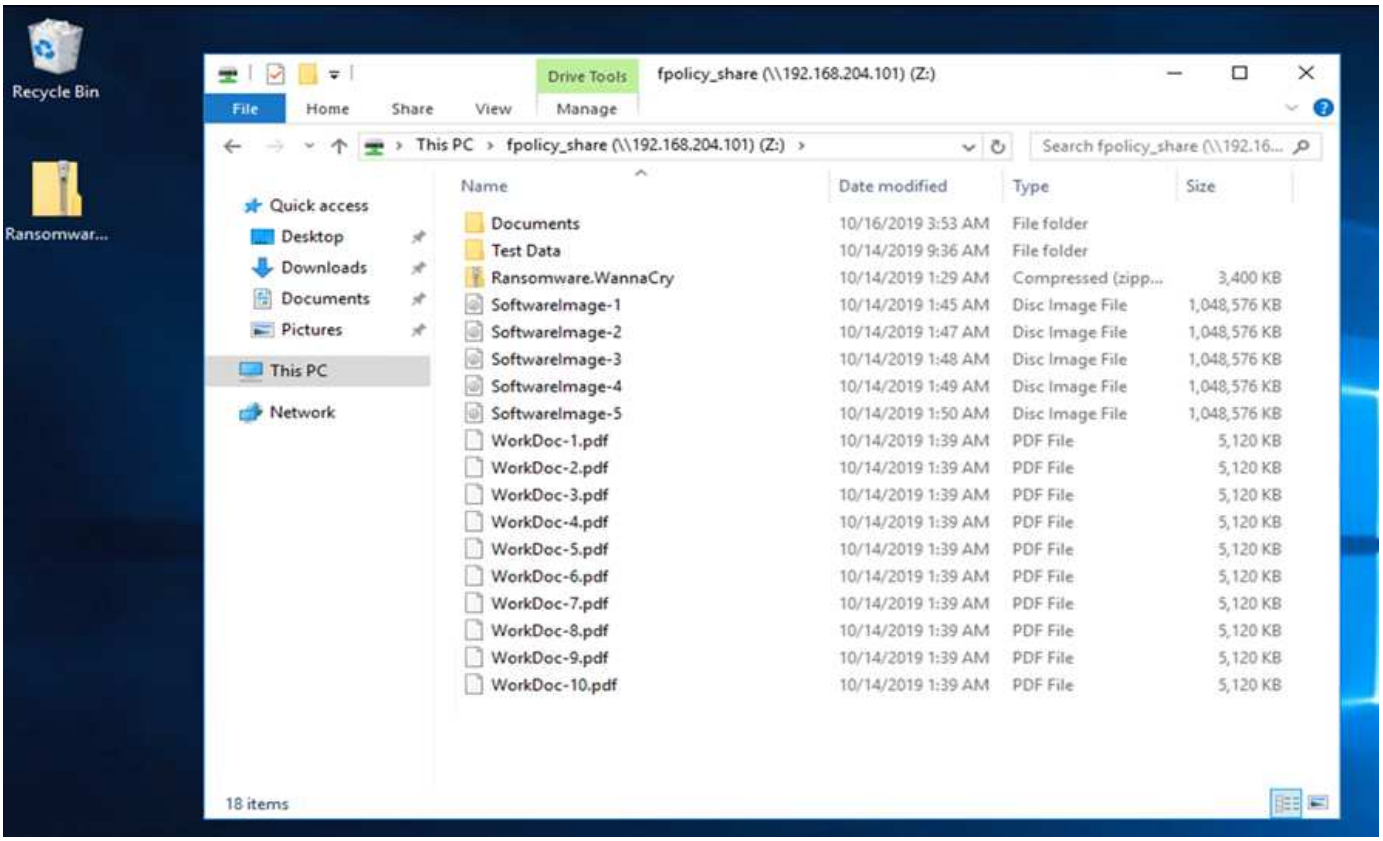
VM 的 Documents 文件夹包含一组 PDF 文件，这些文件尚未被 WannaCry 恶意软件加密。



以下屏幕截图显示了映射到虚拟机的 CIFS 共享。



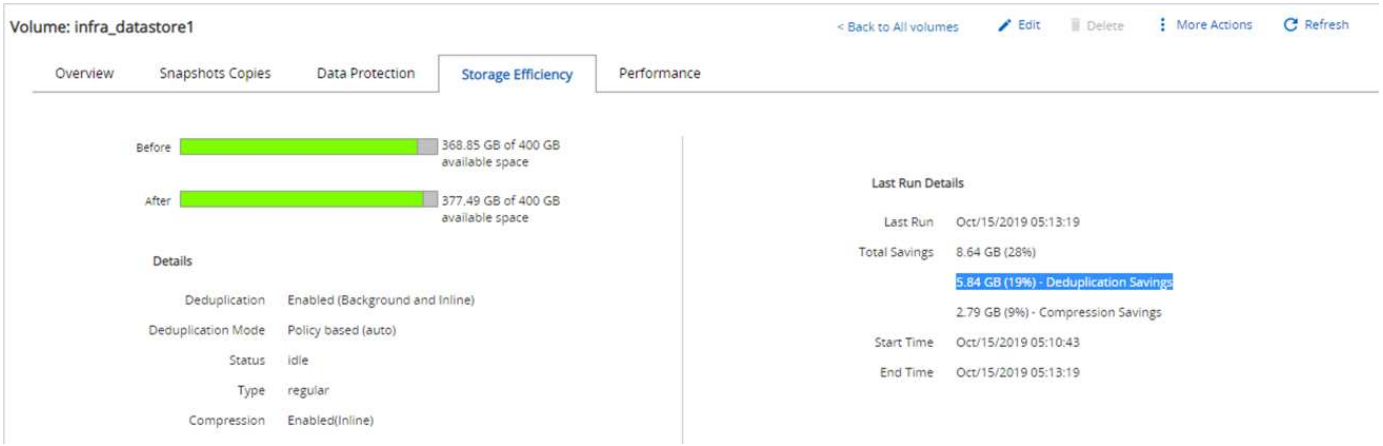
以下屏幕截图显示了 CIFS 共享 `fpolicy_share` 上尚未被 WannaCry 恶意软件加密的文件。



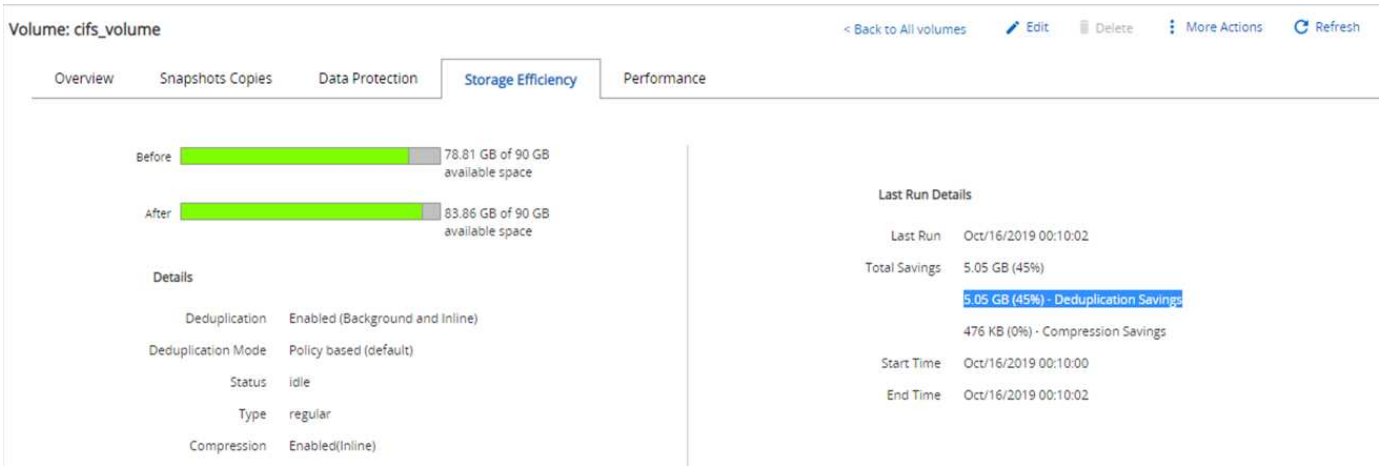
攻击前的重复数据删除和 **Snapshot** 信息

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。

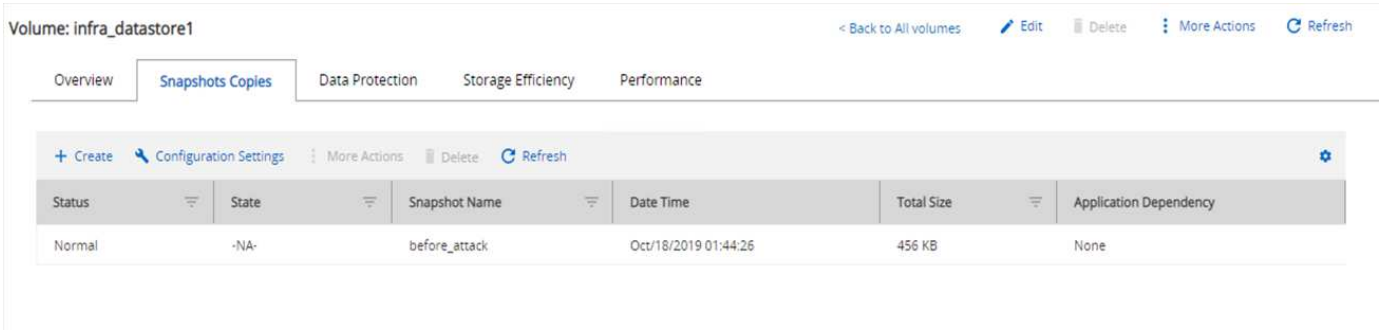
通过对托管 VM 的卷执行重复数据删除，存储节省了 19% 。



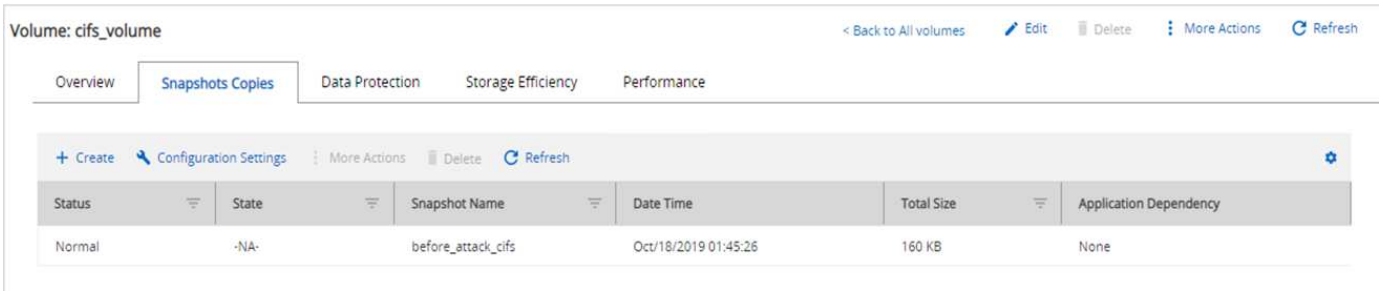
通过对 CIFS 共享 `fpolicy_share` 执行重复数据删除，存储节省了 45% 。



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 。



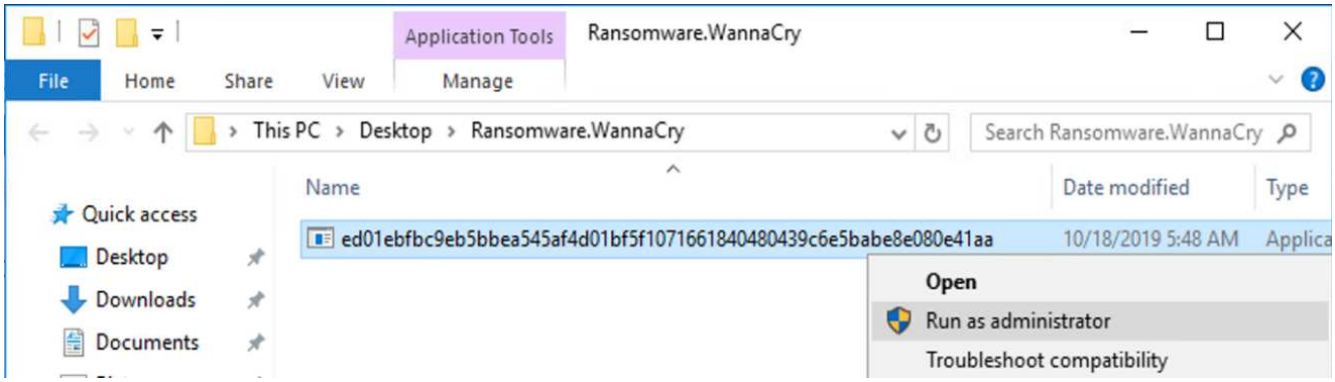
VM 和 **CIFS** 共享上的 **WannaCry** 感染

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。

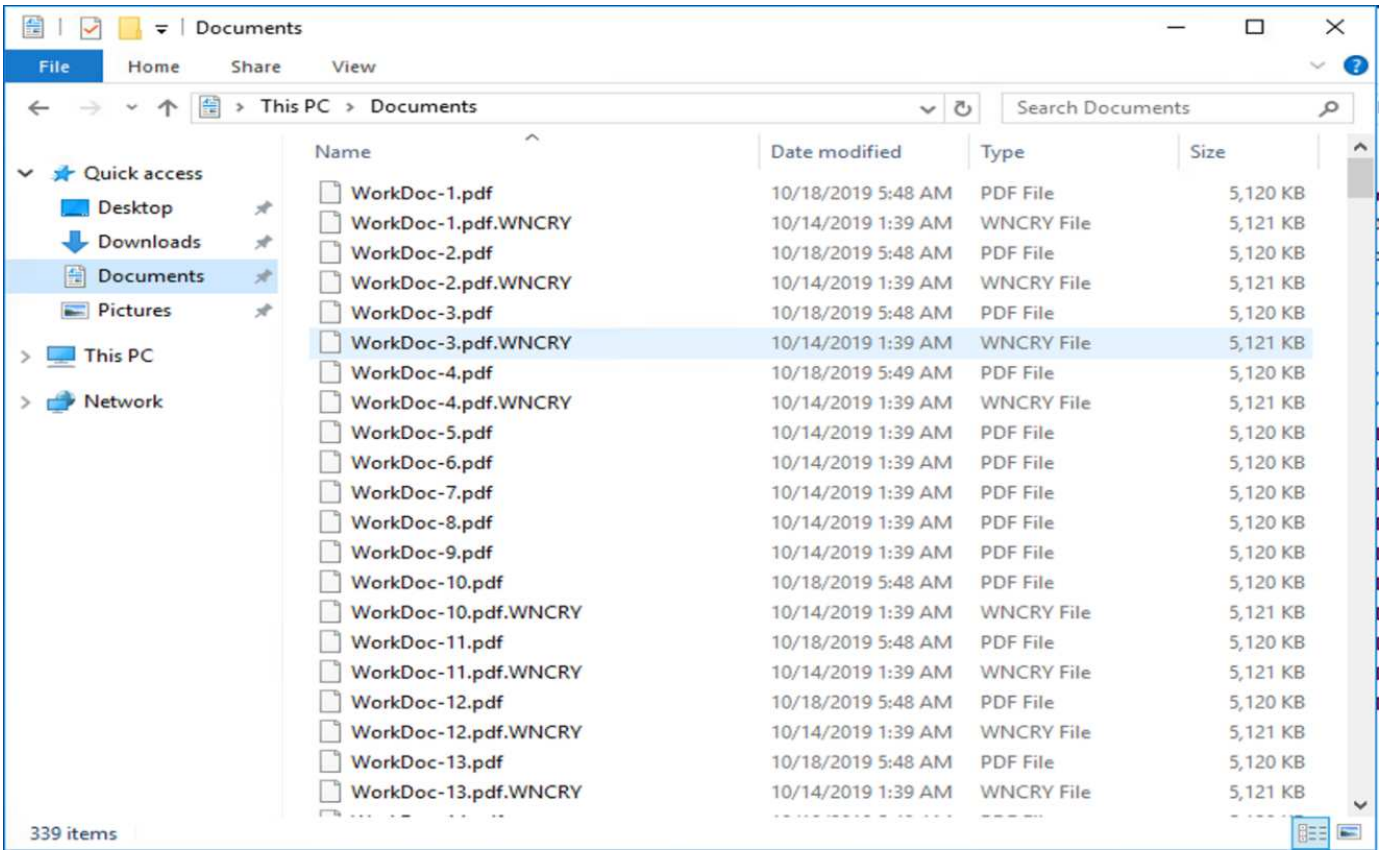
2. 已执行二进制文件。



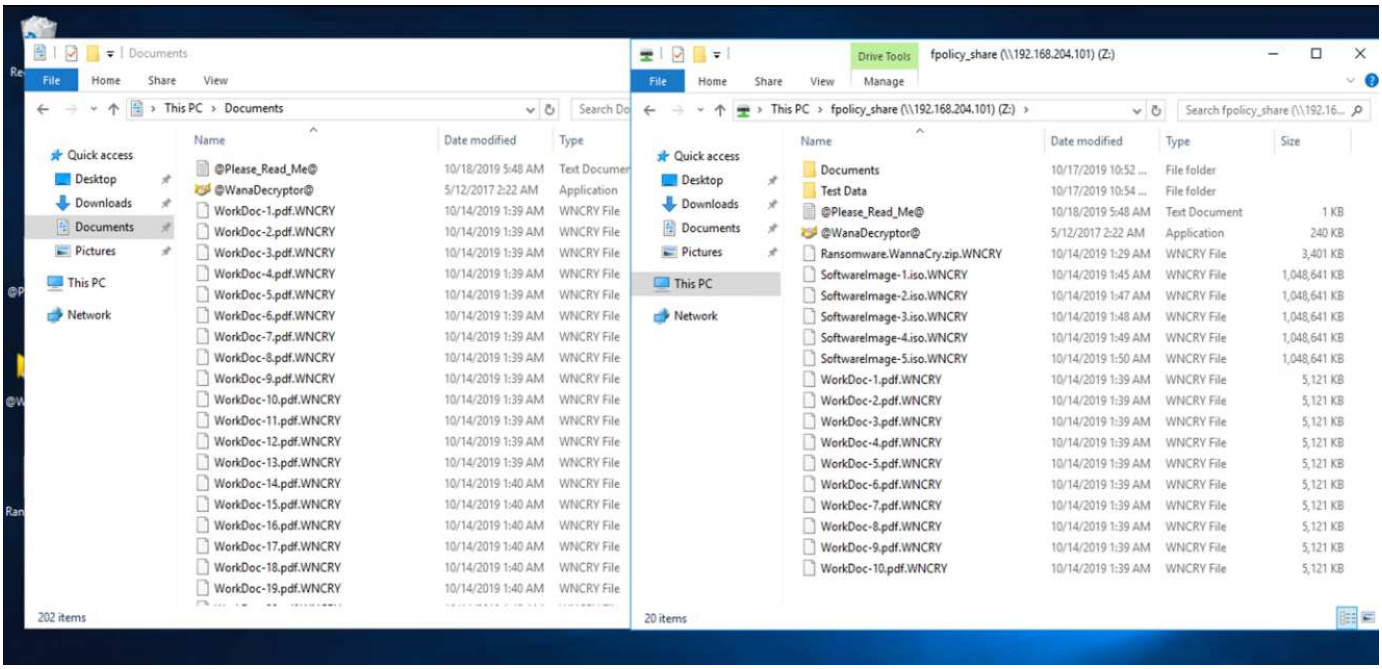
案例 **1**： **WannaCry** 对 **VM** 和映射的 **CIFS** 共享中的文件系统进行加密

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。



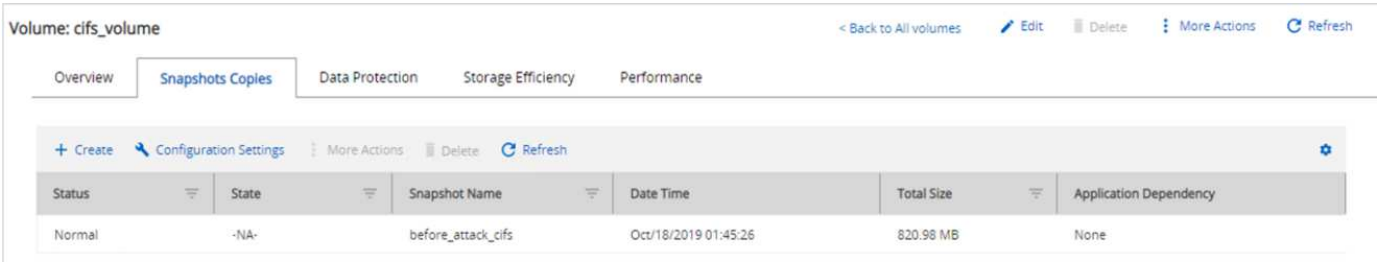
恶意软件会对本地 VM 和映射共享中的所有文件进行加密。



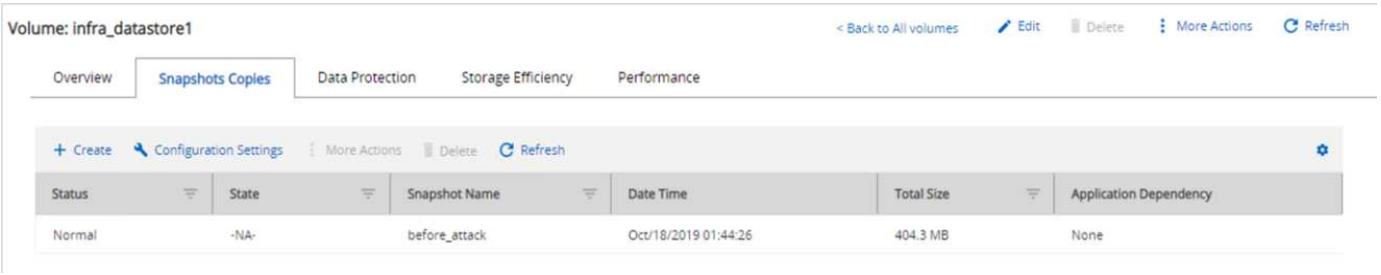
检测

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。

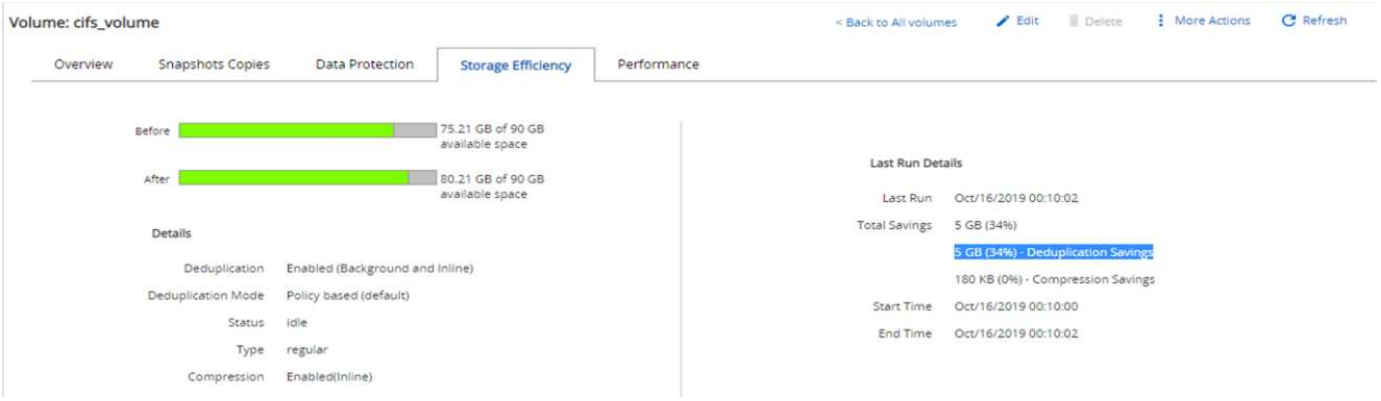
我们检测到，在攻击期间，托管 CIFS 共享的卷的 Snapshot 大小大幅增加到 820.98MB 。



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% 。



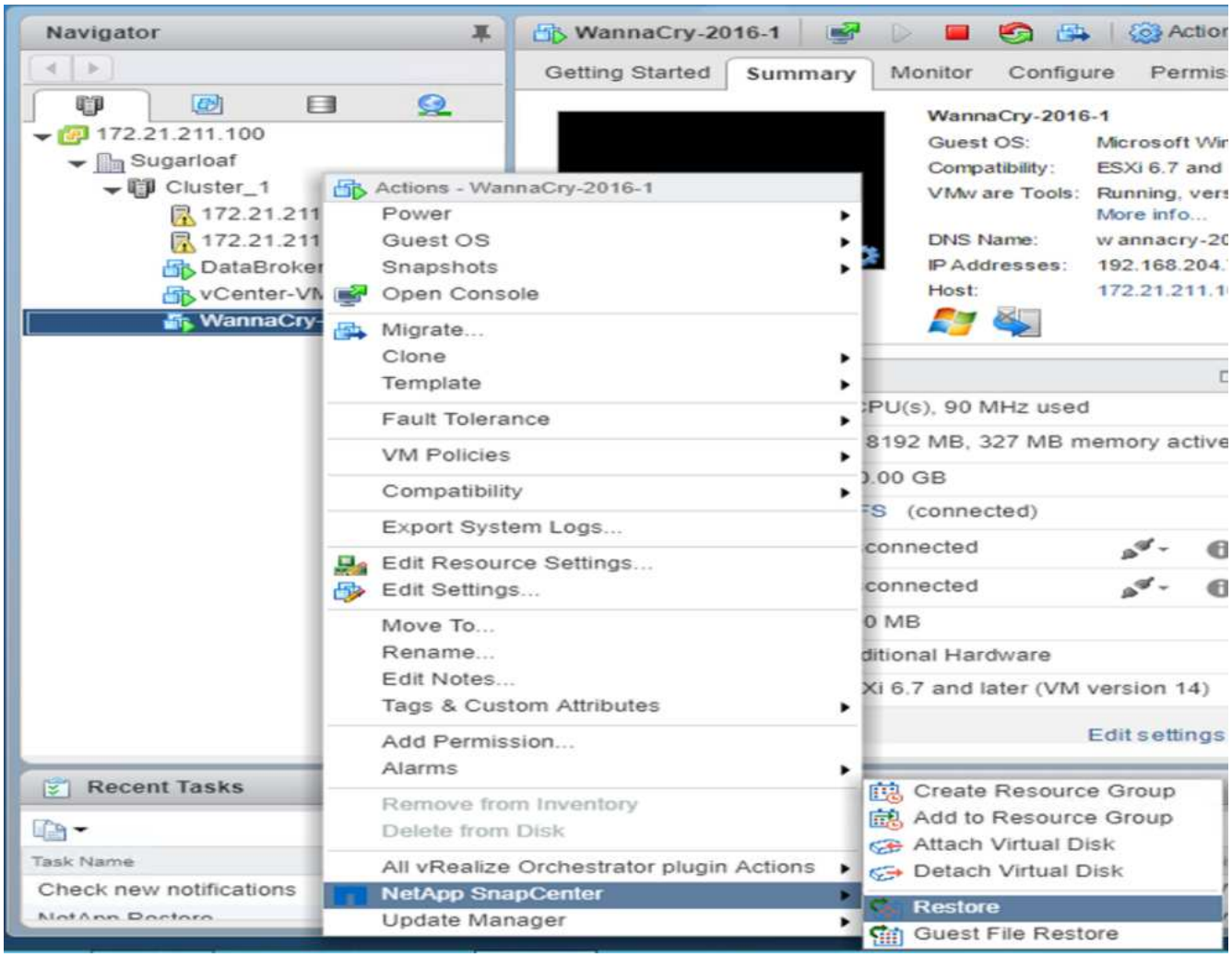
修复

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。

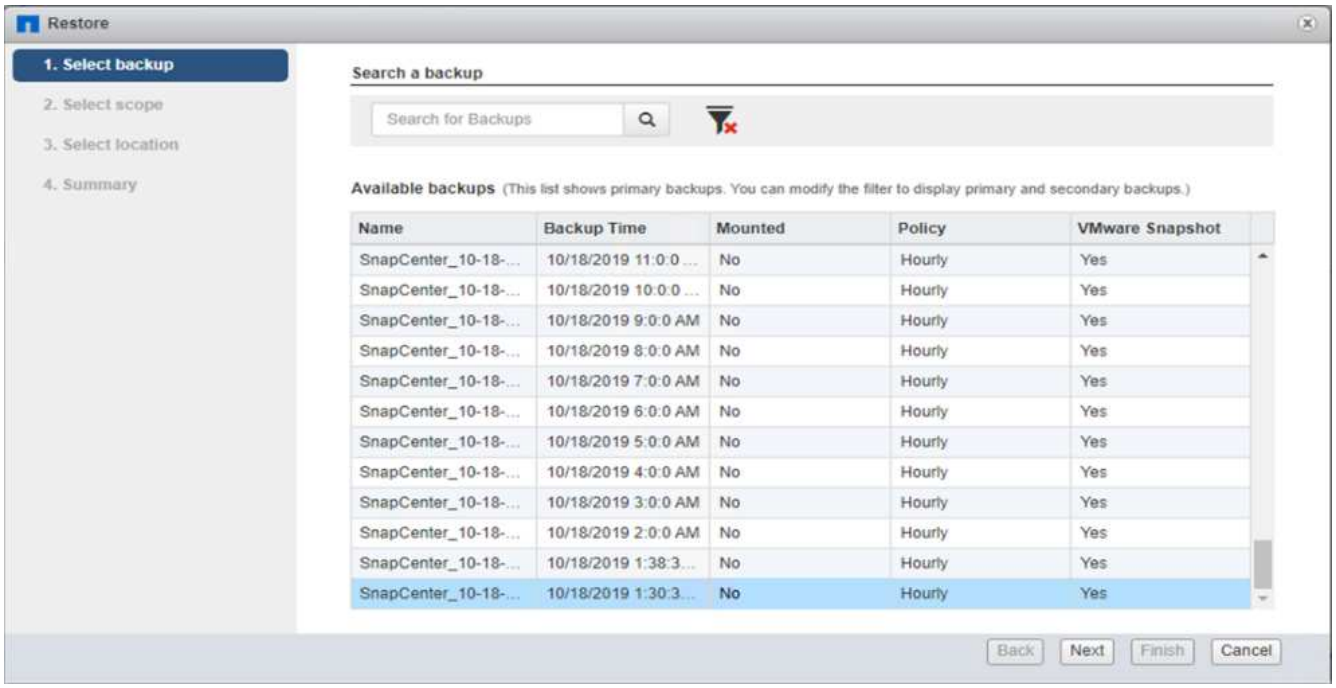
- 还原 VM*

要还原虚拟机，请完成以下步骤：

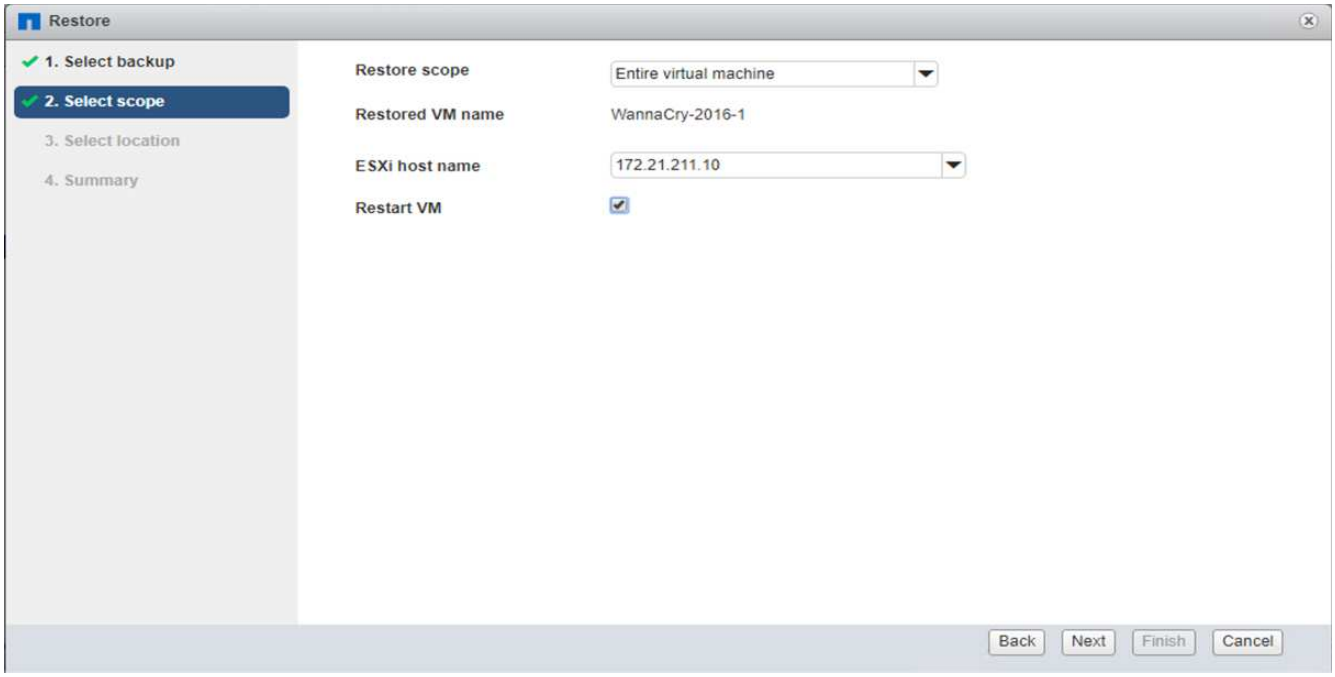
1. 使用您使用 SnapCenter 创建的 Snapshot 副本还原虚拟机。



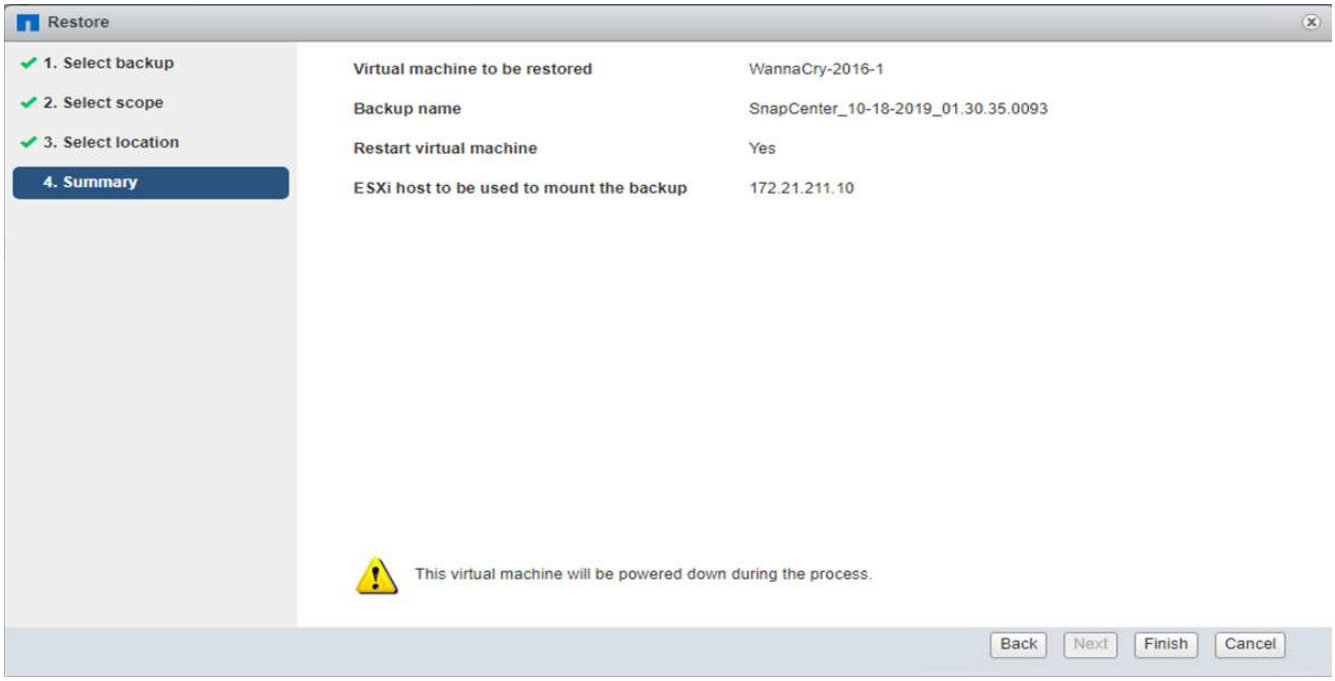
2. 选择所需的 VMware 一致 Snapshot 副本进行还原。



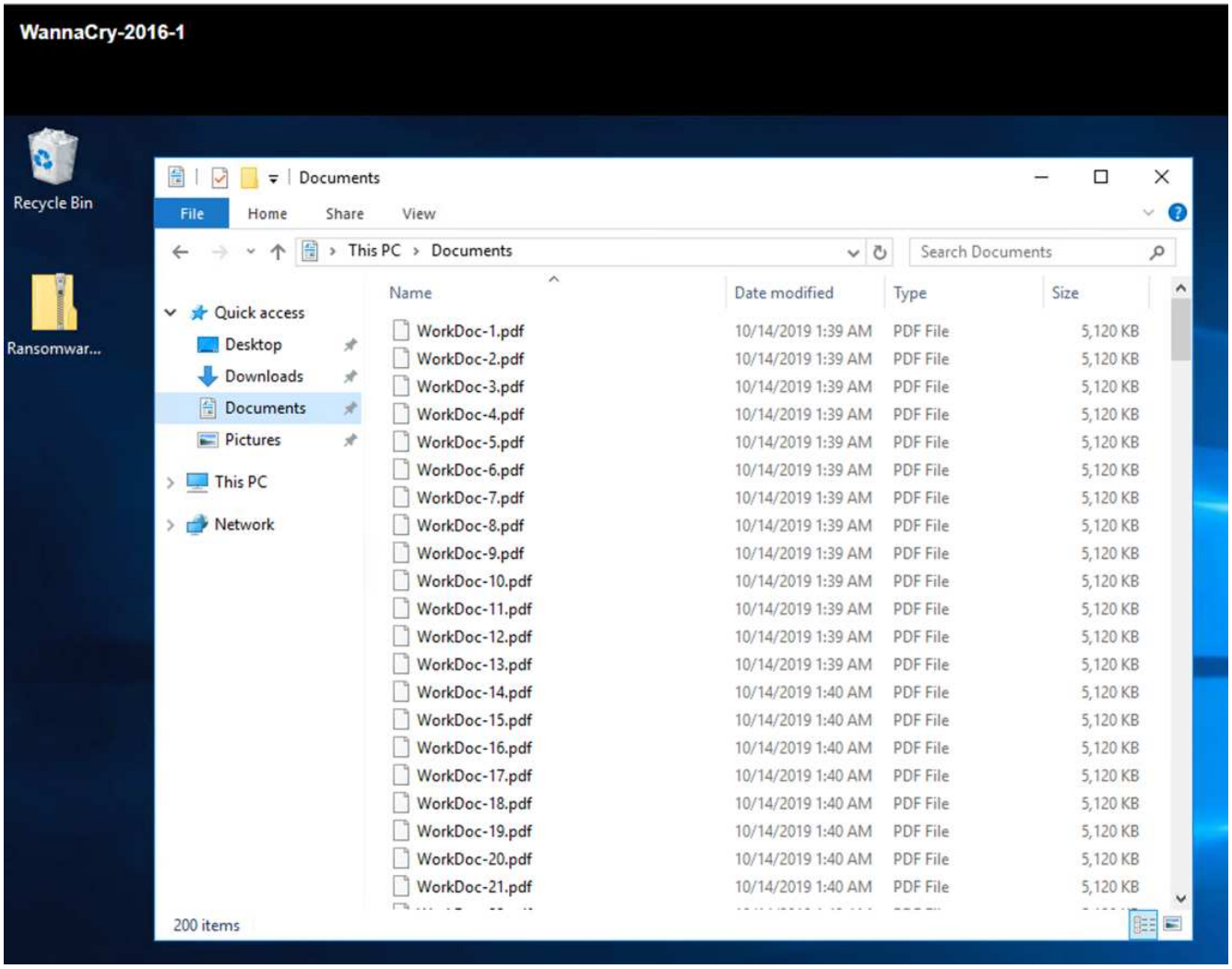
3. 此时将还原并重新启动整个 VM 。



4. 单击完成以启动还原过程。



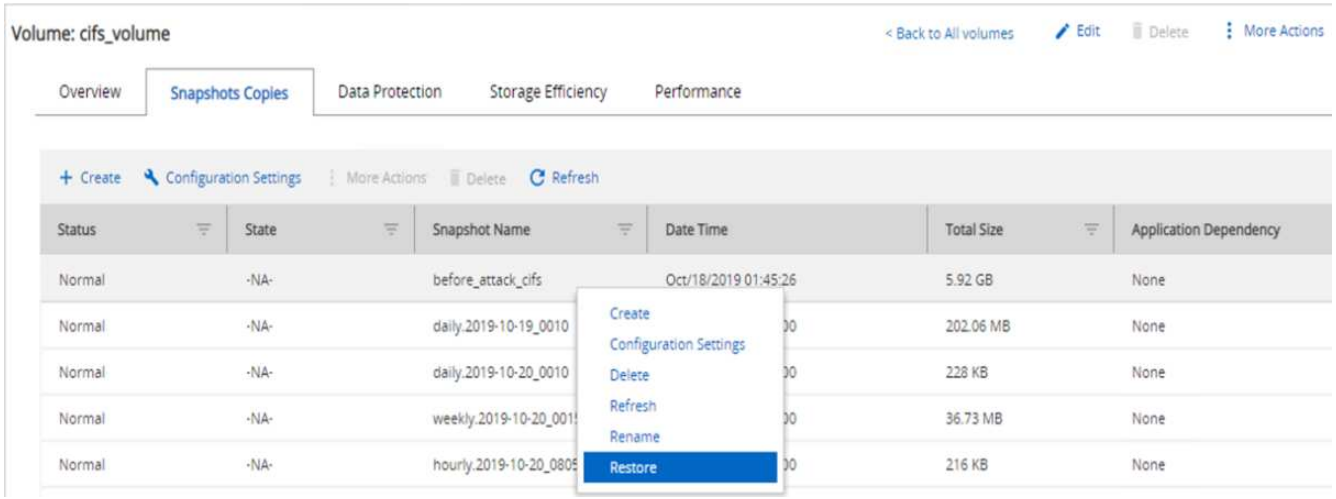
5. 虚拟机及其文件将会还原。



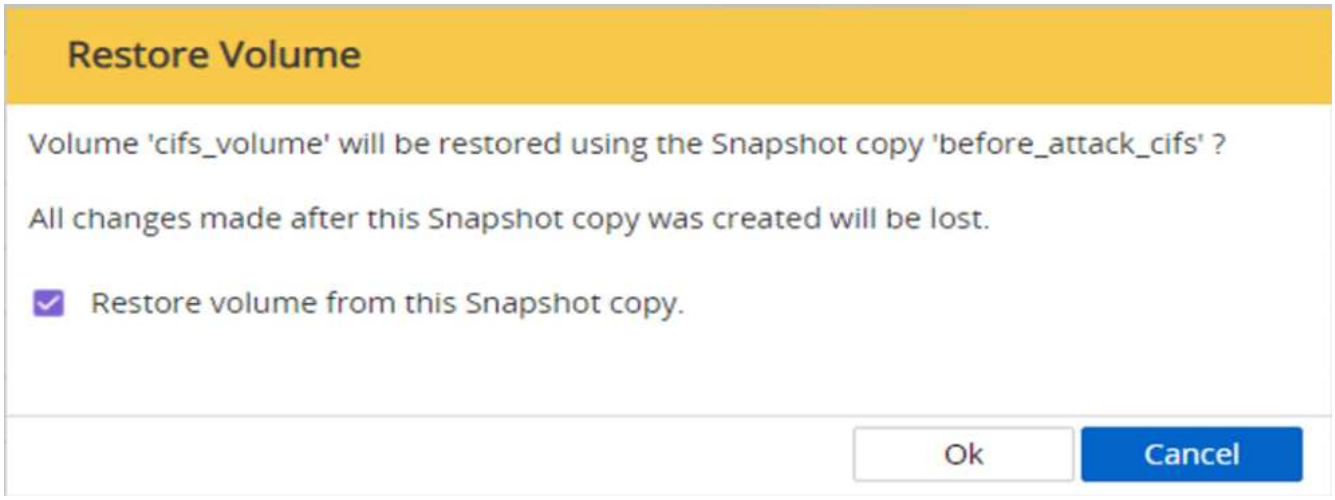
◦ 还原 CIFS 共享 *

要还原 CIFS 共享，请完成以下步骤：

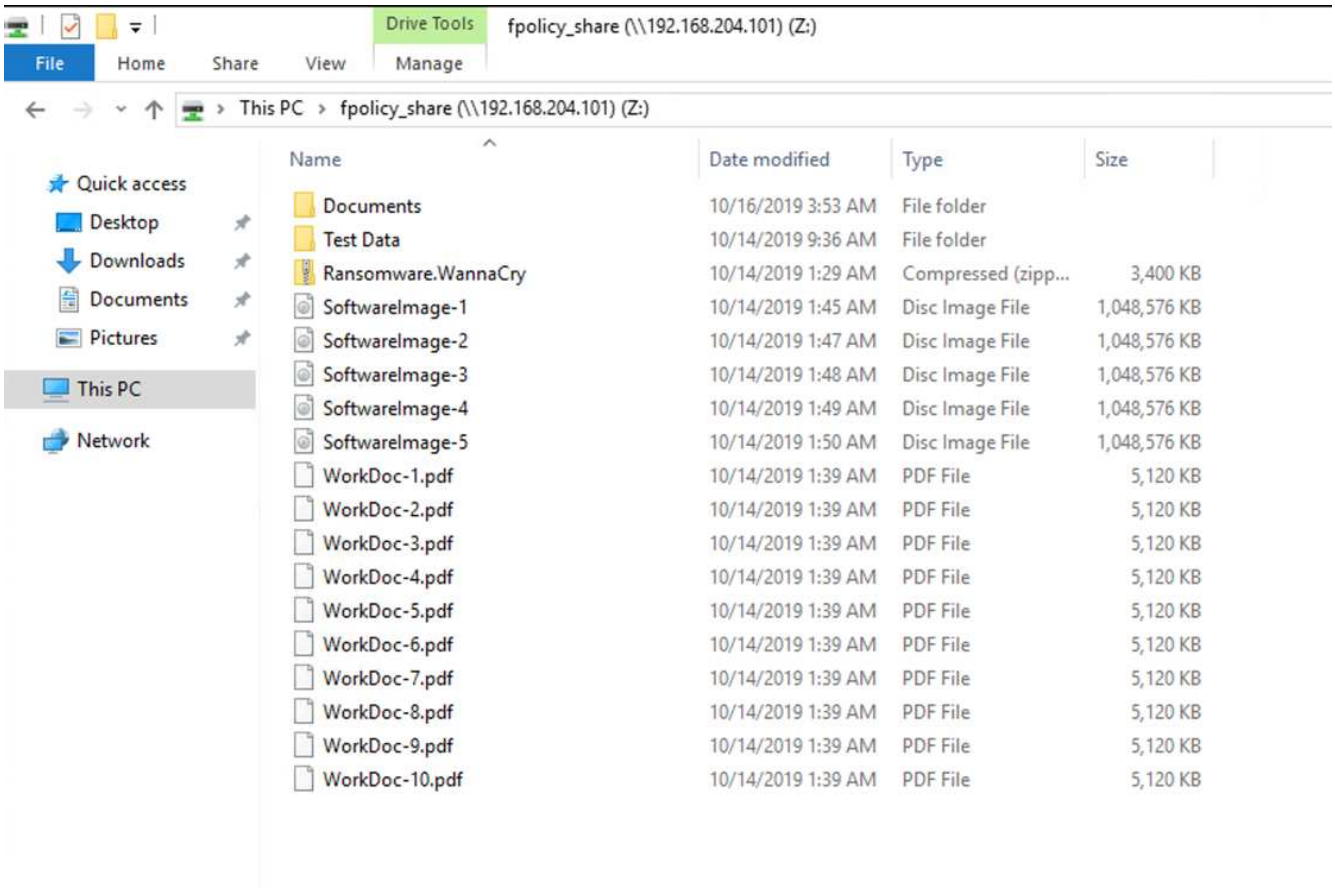
1. 使用攻击前创建的卷的 Snapshot 副本还原共享。



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

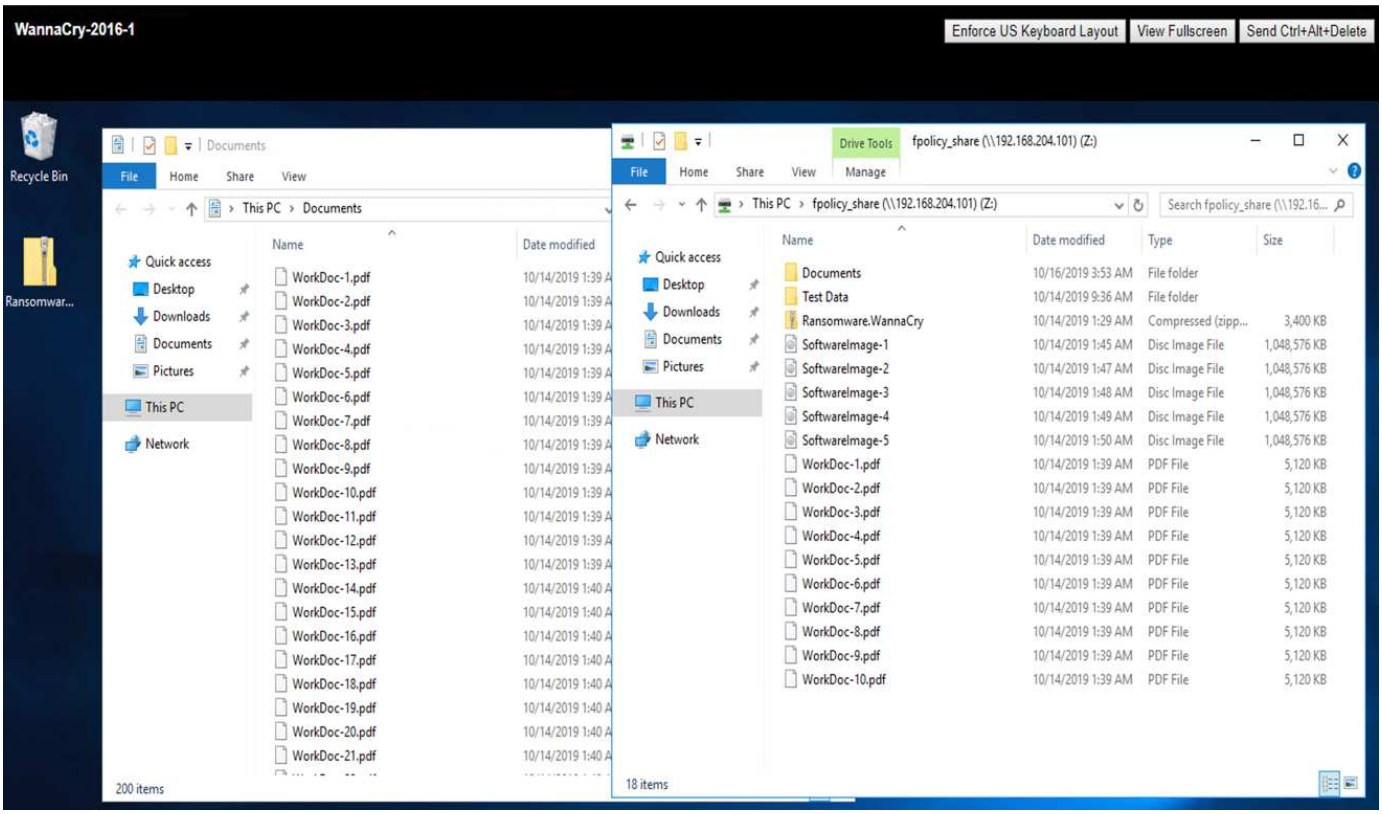
- 配置 FPolicy*

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

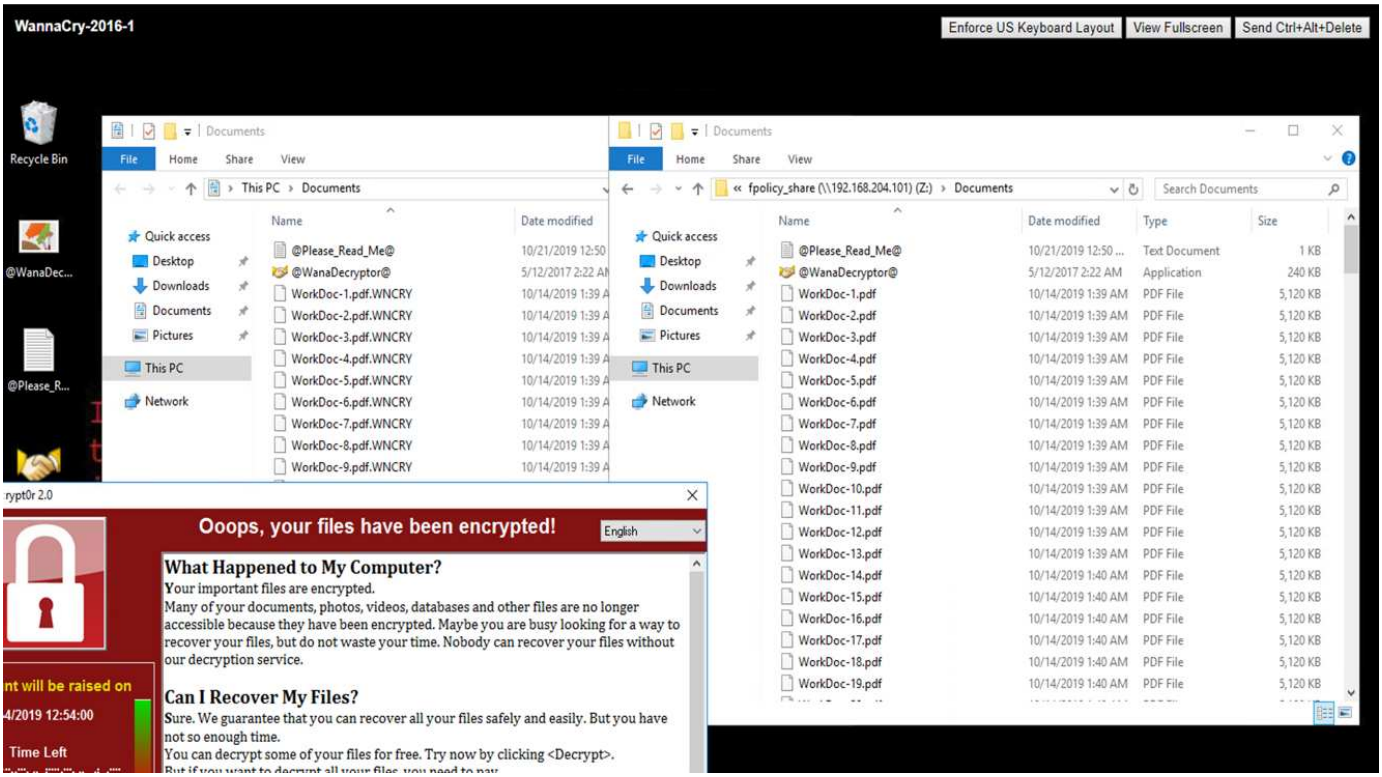
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create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

适用于医疗保健的 FIPS 140-2 安全合规 FlexPod 解决方案

TR-4892 ： 适用于医疗保健的 FIPS 140-2 安全合规 FlexPod 解决方案

NetApp Cisco 公司 John McAbel 的 JayaKishore Esanakula

《经济和临床健康健康信息技术法案》（ HITECH ）要求对经联邦信息处理标准（ FIPS ） 140-2 验证的电子受保护健康信息（ ePHI ）进行加密。要获得 " 提升互操作性计划 "（以前称为 " 有意义的使用奖励计划 " ）认证，运行状况信息技术（ HIT ）应用程序和软件必须符合 FIPS 140-2 的要求。符合条件的提供商和医院必须使用符合 FIPS 140-2 （ 1 级）标准的命中率来获得医疗保健和医疗辅助奖励，并避免从医疗保健和医疗辅助中心（ CMS ）获得报销处罚。FIPS 140-2 认证加密算法符合作为技术保障的要求 "安全规则" 《健康信息可移植性和责任法案》（ HIPAA ）。

FIPS 140-2 属于美国为硬件，软件和固件中的加密模块设置安全要求以保护敏感信息的政府标准。美国要求遵守本标准政府机构， IT 也经常用于金融服务和医疗保健等受监管行业。本技术报告有助于读者深入了解 FIPS 140-2 安全标准。它还有助于受众了解医疗保健组织面临的各种威胁。最后，该技术报告有助于了解在 FlexPod 融合基础架构上部署符合 FIPS 140-2 标准的 FlexPod 系统如何帮助保护医疗保健资产的安全。

范围

本文档对基于 Cisco Unified Computing System （ Cisco UCS ）， Cisco Nexus ， Cisco MDS 和 NetApp ONTAP 的 FlexPod 基础架构进行了技术概述，用于托管一个或多个需要 FIPS 140-2 安全合规性的医疗保健 IT 应用程序或解决方案。

audience

本文档面向医疗保健行业的技术主管以及 Cisco 和 NetApp 合作伙伴解决方案工程师和专业服务人员。NetApp 假定读者已很好地了解计算和存储规模估算概念，并在技术上熟悉医疗保健威胁，医疗保健安全，医疗保健 IT 系统， Cisco UCS 和 NetApp 存储系统。

"接下来：医疗保健领域的网络安全威胁。"

医疗保健领域的网络安全威胁

"上一页：简介。"

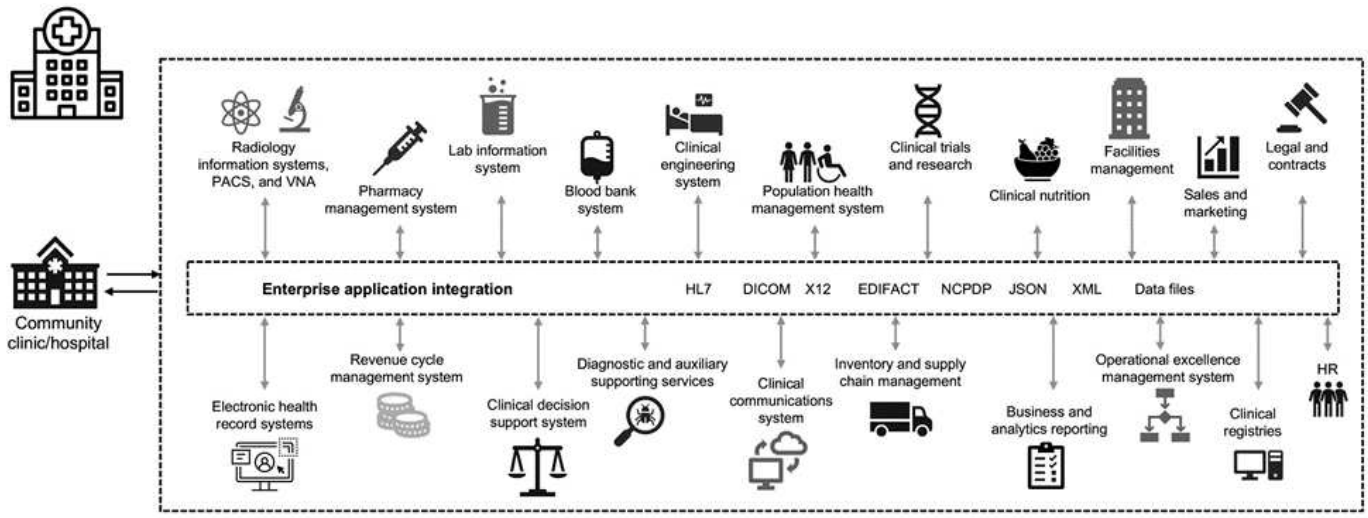
每一个问题都带来了新的机会， COVID 大流行病就是一个例子。根据 A "report" 根据健康和人类服务部门（ HHS ）网络安全计划， COVID 的响应导致勒索软件攻击数量增加。截至 2020 年 3 月第三周，注册的新互联网域有 6 ， 000 个。超过 50% 的域托管恶意软件。2020 年，勒索软件攻击造成了近 50% 的医疗保健数据违规，影响到超过 630 家医疗保健组织和大约 2 ， 900 万份医疗保健记录。19 个泄漏点 / 站点的勒索行为增加了一倍。在 2020 年，医疗保健行业的数据泄露次数高达 24.5% 。

恶意代理通过销售受保护健康信息（ Phi ）或威胁销毁或公开该信息，试图破坏该信息的安全性和隐私。通常会进行有针对性的大规模广播尝试，以获取对 ePHI 的未授权访问。在 2020 年下半年，大约 75% 的公开患者记录是由于业务伙伴受到影响。

以下医疗保健组织被恶意代理作为目标：

- 医院系统
- 生命科学实验室
- 研究实验室
- 恢复设施
- 社区医院和诊所

构成医疗保健组织的应用程序的多样性是不可否认的，并且日益复杂。信息安全办公室面临着为大量 IT 系统和资产提供监管的挑战。下图显示了典型医院系统的临床功能。



患者数据是此图的核心。患者数据的丢失以及与敏感医疗状况相关的侮辱是非常真实的。其他敏感问题包括社会排斥，勒索，特征描述，容易受到有针对性的营销，被利用的风险，以及在支付者的特权之外对医疗信息可能承担的财务责任。

医疗保健面临的威胁具有多层面性质，而且具有多种影响。全球政府已制定各种条款来确保 ePHI 的安全。医疗保健所面临的不利影响和不断变化的性质使医疗保健组织难以抵御所有威胁。

下面列出了医疗保健领域中发现的常见威胁：

- 勒索软件攻击
- 丢失或被盗包含敏感信息的设备或数据
- 网络钓鱼攻击
- 攻击连接的医疗设备，可能会影响患者安全
- 电子邮件网络钓鱼攻击
- 设备或数据丢失或被盗
- 远程桌面协议损坏
- 软件漏洞

医疗保健组织在法律和监管环境中运营，这种环境与数字生态系统一样复杂。此环境包括但不限于以下内容：

- 美国国家医疗保健技术协调办公室（美国国家协调办公室） ONC 认证电子医疗保健信息技术互操作性标准
- 享受医疗保健和儿童健康保险计划重新授权法案（ MACRA ） / 有意义的使用
- 根据食品和药物管理局（ FDA ）承担的多项义务
- 联合委员会的资格鉴定过程
- HIPAA 要求
- 高科技要求
- 付款人可接受的最低风险标准
- 规定隐私和安全规则
- 通过国家卫生机构等机构将联邦信息安全现代化法案要求纳入联邦合同和研究拨款中

- 支付卡行业数据安全标准（ PCI-DSS ）
- 《药物滥用和精神健康服务管理（ SAMHSA ）要求》
- 用于财务处理的《格雷姆 - 里奇 - 比利雷法案》
- 与向附属组织提供服务相关的《 Stark 法律》
- 《家庭教育权利和隐私法》（ FERPA ）适用于参与高等教育的机构
- 《遗传信息不歧视法》（ GINA-GINESE ）
- 欧盟新的《一般数据保护条例》（ GDPR ）

安全架构标准正在快速发展，以防止恶意行为者影响医疗保健信息系统。其中一项标准是 FIPS 140-2 ，该标准由美国国家标准与技术协会（ NIST ）定义。FIPS 出版物 140-2 详细介绍了美国加密模块的政府要求。安全要求涵盖与安全设计和实施加密模块相关的区域，可应用于命中。定义完善的加密边界可以简化安全管理，同时保持最新的加密模块。这些边界有助于防止恶意攻击者容易利用弱密码模块。它们还有助于防止在管理标准加密模块时出现人为错误。

NIST 与通信安全机构（ CSE ）共同制定了加密模块验证计划（ CMVP ），用于对 FIPS 140-2 验证级别的加密模块进行认证。联邦组织需要使用 FIPS 140-2 认证模块在空闲和移动时保护敏感或有价值的数据。由于 ePHI 能够成功保护敏感或有价值的信息，因此许多医疗保健系统都选择使用 FIPS 140-2 加密模块对 ePHI 进行加密，这超出了法律规定的最低安全级别。

利用和实施 FlexPod FIPS 140-2 功能只需数小时（而不是数天）。无论规模大小，大多数医疗保健组织都可以获得 FIPS 合规性。通过明确定义的加密边界以及详细记录的简单实施步骤，符合 FIPS 140-2 的 FlexPod 架构可以为基础架构奠定坚实的安全基础，并可通过简单的增强功能进一步增强对安全威胁的保护。

"接下来： FIPS 140-2 概述。"

FIPS 140-2 概述

"上一篇：医疗保健领域的网络安全威胁。"

"FIPS 140-2" 指定在保护计算机和电信系统中敏感信息的安全系统中使用的加密模块的安全要求。加密模块应为一组硬件，软件，固件或两者的组合。FIPS 适用场景 加密边界内包含的加密算法，密钥生成和密钥管理器。请务必了解， FIPS 140-2 专门适用于加密模块，而不是产品，架构，数据或生态系统。本文档后面的关键术语中定义的加密模块是实施批准的安全功能的特定组件（无论是硬件，软件和 / 或固件）。此外， FIPS 140-2 还指定了四个级别。经过批准的加密算法适用于所有级别。每个安全级别的关键要素和要求包括：

- * 安全级别 1*
  - 指定加密模块的基本安全要求（至少需要一个经过批准的算法或安全功能）。
  - 除了生产级组件的基本要求之外， 1 级不需要任何指定的物理安全机制。
- * 安全级别 2*
  - 通过使用不受篡改的解决方案（例如，覆盖层或密封，可拆卸盖板或加密模块的门锁）添加篡改证据要求，增强了物理安全机制。
  - 至少需要基于角色的访问控制（ Role-Based Access Control ， RBAC ），在此控制中，加密模块对操作员或管理员的授权进行身份验证，以承担特定角色并执行一组相应的功能。

- * 安全级别 3*
  - 基于 2 级的防篡改要求构建，并尝试防止进一步访问加密模块中的关键安全参数（ CSP ）。
  - 第 3 级所需的物理安全机制旨在检测和响应物理访问尝试或对加密模块的任何使用或修改的可能性较高。示例可能包括：打开加密模块上的可拆卸盖时，强磁盘机箱，防拆检测以及将所有纯文本 CSP 置零的响应电路。
  - 需要基于身份的身份验证机制来增强级别 2 中指定的 RBAC 机制的安全性。加密模块对操作员身份进行身份验证，并验证操作员是否有权使用某个角色并执行该角色的功能。
- * 安全级别 4*
  - FIPS 140-2 中最高级别的安全性。
  - 在物理上不受保护的环境中执行操作的最有用级别。
  - 在这一级别，物理安全机制旨在为加密模块提供全面保护，并负责检测和响应任何未经授权的物理访问尝试。
  - 加密模块的渗透或暴露应具有很高的检测概率，并导致所有不安全或纯文本 CSP 立即置零。

"下一步：控制平面与数据平面。"

控制平面与数据平面

"先前版本： FIPS 140-2 概述。"

在实施 FIPS 140-2 策略时，了解要保护的内容非常重要。这可以轻松细分为两个区域：控制平面和数据平面。控制面板是指影响 FlexPod 系统中组件的控制和操作的方面：例如，对 NetApp 存储控制器， Cisco Nexus 交换机和 Cisco UCS 服务器的管理访问。通过限制管理员可用于连接到设备和进行更改的协议和加密网络算法，可以在这一层提供保护。数据平面是指 FlexPod 系统中的实际信息，例如 PHI 。通过对空闲数据进行加密以及对 FIPS 再次进行加密来保护此数据，从而确保使用的加密模块符合标准。

"接下来： FlexPod Cisco UCS 计算和 FIPS 140-2 。"

FlexPod Cisco UCS 计算和 FIPS 140-2

"上一步：控制平面与数据平面。"

FlexPod 架构可以使用符合 FIPS 140-2 的 Cisco UCS 服务器进行设计。根据美国SNIST ， Cisco UCS 服务器可以在 FIPS 140-2 1 级合规模式下运行。有关符合 FIPS 的 Cisco 组件的完整列表，请参见 "Cisco 的 FIPS 140 页面"。Cisco UCS Manager 已通过 FIPS 140-2 验证。

Cisco UCS 和互联阵列

Cisco UCS Manager 可通过 Cisco 互联阵列（ Fabric Interconnects ， FI ）进行部署和运行。

有关 Cisco UCS 以及如何启用 FIPS 的详细信息，请参见 "Cisco UCS Manager 文档"。

要在每个网络结构 A 和 B 上的 Cisco 互联阵列上启用 FIPS 模式，请运行以下命令：

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

要在 Cisco UCS Manager 3.2 （ 3 ）版之前的版本上将集群中的 FI 替换为 FI ，请在将替代 FI 添加到集群之前，先在现有 FI 上禁用 FIPS 模式（ disable `FIPS-mode` ）。集群形成后，在 Cisco UCS Manager 启动过程中， FIPS 模式将自动启用。

Cisco 提供了可在计算或应用程序层实施的以下关键产品：

- * 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。
- * 电子邮件安全性的 AMP 。 * 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的物理设备，也可以部署为 VMware 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，并使在资源有限的站点上部署和管理 NGIP 解决方案变得更加轻松，从而增强对物理和虚拟资产的保护。

"接下来： FlexPod Cisco 网络和 FIPS 140-2 。"

FlexPod Cisco 网络和 FIPS 140-2

"先前版本： FlexPod Cisco UCS 计算和 FIPS 140-2 。"

Cisco MDS

使用软件 8.4.x 的 Cisco MDS 9000 系列平台为 "符合 FIPS 140-2"。Cisco MDS 可为 SNMPv3 和 SSH 实施加密模块和以下服务。

- 支持每个服务的会话建立
- 支持每个服务密钥派生功能的所有底层加密算法
- 每个服务的哈希
- 为每个服务提供对称加密

在启用 FIPS 模式之前，请在 MDS 交换机上完成以下任务：

1. 使密码长度至少为八个字符。
2. 禁用 Telnet 。用户应仅使用 SSH 登录。

3. 禁用通过 RADIUS/TACACS+ 进行远程身份验证。只能对交换机本地的用户进行身份验证。
4. 禁用 SNMP v1 和 v2 。交换机上为 SNMPv3 配置的任何现有用户帐户只能配置 SHA 以进行身份验证，并配置 AES/3DES 以保证隐私。
5. 禁用 VRRP 。
6. 删除具有用于身份验证的 MD5 或用于加密的 DES 的所有 ike 策略。修改策略，使其使用 SHA 进行身份验证，并使用 3DES/AES 进行加密。
7. 删除所有 SSH 服务器 RSA1 密钥对。

要启用 FIPS 模式并在 MDS 交换机上显示 FIPS 状态，请完成以下步骤：

1. 显示 FIPS 状态。

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

2. 设置 2048 位 SSH 密钥。

```
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. 启用 FIPS 模式。

```
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. 显示 FIPS 状态。

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

5. 将配置保存到正在运行的配置中。

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

6. 重新启动 MDS 交换机

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

7. 显示 FIPS 状态。

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

有关详细信息，请参见 "启用 FIPS 模式"。

Cisco Nexus

Cisco Nexus 9000 系列交换机（ 9.3 版） "符合 FIPS 140-2"。Cisco Nexus 为 SNMPv3 和 SSH 实施加密模块和以下服务。

- 支持每个服务的会话建立
- 支持每个服务密钥派生功能的所有底层加密算法

- 每个服务的哈希
- 为每个服务提供对称加密

在启用 FIPS 模式之前，请在 Cisco Nexus 交换机上完成以下任务：

1. 禁用 Telnet 。用户应仅使用安全 Shell （ SSH ）登录。
2. 禁用 SNMPv1 和 v2 。设备上已配置 SNMPv3 的任何现有用户帐户只能配置 SHA 进行身份验证，并配置 AES/3DES 以保证隐私。
3. 删除所有 SSH 服务器 RSA1 密钥对。
4. 启用 HMAC-SHA1 消息完整性检查（ Message Integrity Checking ，麦克风），以便在 Cisco TrustSec 安全关联协议（ SAP ）协商期间使用。要执行此操作，请在 `CTS-manual` 或 `CTS-dot1x` 模式中输入 SAP hash-orolor `HMAC-SHA-1` 命令。

要在 Nexus 交换机上启用 FIPS 模式，请完成以下步骤：

1. 设置 2048 位 SSH 密钥。

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

2. 设置 2048 位 SSH 密钥。

```
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. 启用 FIPS 模式。

```
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. 重新启动 Nexus 交换机。

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

5. 显示 FIPS 状态。

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

此外， Cisco NX OS 软件还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。

"接下来： FlexPod NetApp ONTAP 存储和 FIPS 140-2 。"

FlexPod NetApp ONTAP 存储和 FIPS 140-2

"先前版本： FlexPod Cisco 网络和 FIPS 140-2 。"

NetApp 提供各种硬件，软件和服务，其中可以包括根据标准验证的加密模块的各种组件。因此， NetApp 使用多种方法在控制平面和数据平面上实现 FIPS 140-2 合规性：

- NetApp 提供的加密模块已通过传输中数据加密和空闲数据加密的 1 级验证。
- NetApp 收购的硬件和软件模块均已通过这些组件供应商的 FIPS 140-2 验证。例如， NetApp 存储加密解决方案 利用经过 FIPS 级别 2 验证的驱动器。
- NetApp 产品可以使用符合标准的经验证模块，即使该产品或功能不在验证范围内也是如此。例如， NetApp 卷加密（ NVE ）符合 FIPS 140-2 标准。虽然未单独进行验证，但它会利用经过 1 级验证的 NetApp 加密模块。要了解您的 ONTAP 版本的合规性详情，请联系您的 FlexPod SME 。
- NetApp 加密模块已通过 FIPS 140-2 1 级验证 *
- NetApp 加密安全模块（ NetApp Cryptographic Security Module ， NCSM ）已通过 FIPS 140-2 1 级验证。
- NetApp 自加密驱动器已通过 FIPS 140-2 2 级认证 *

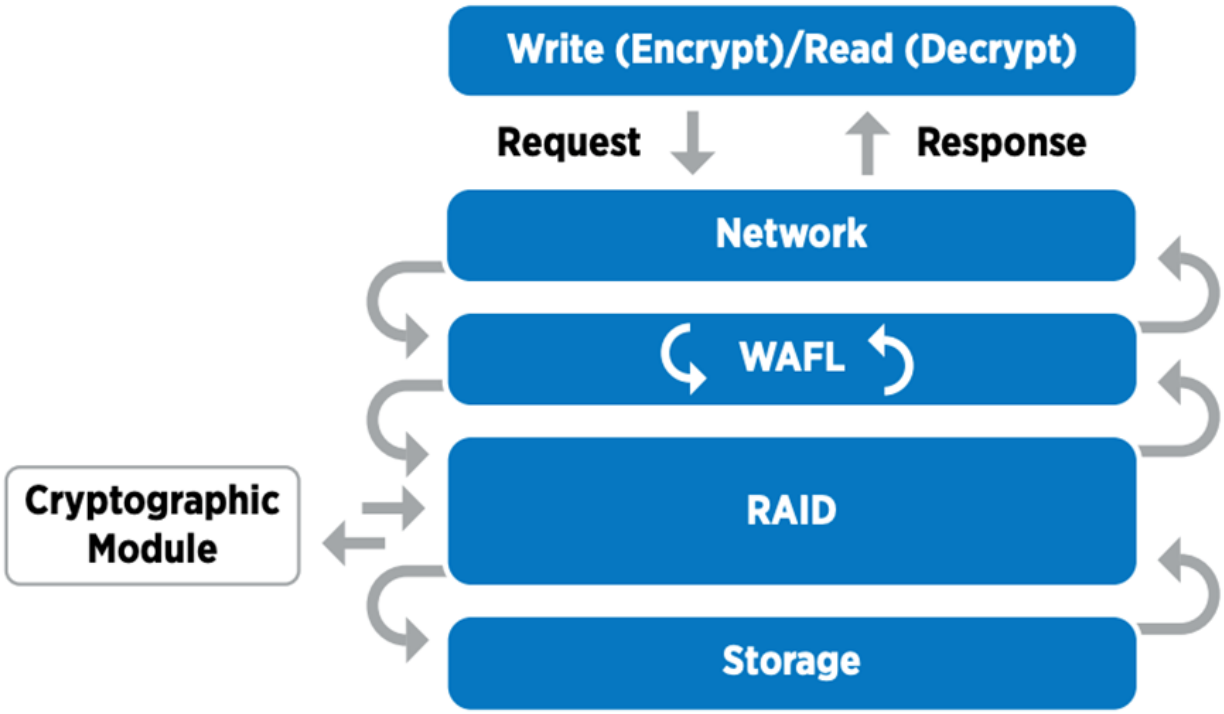
NetApp 购买的自加密驱动器（ SED ）已经过原始设备制造商（ OEM ）的 FIPS 140-2 验证；需要这些驱动器的客户必须在订购时指定这些驱动器。驱动器在级别 2 进行验证。以下 NetApp 产品可以利用经验证的 SED ：

- AFF A 系列和 FAS 存储系统
- E 系列和 EF 系列存储系统
- NetApp 聚合加密和 NetApp 卷加密 *

NVE 和 NetApp 聚合加密（聚合加密， NAE ）技术分别在卷和聚合级别加密数据，使解决方案 与物理驱动器无关。

NVE 是一种基于软件的空闲数据加密解决方案 ，从 ONTAP 9.1 开始提供，自 ONTAP 9.2 起已符合 FIPS 140-2 标准。通过 NVE ， ONTAP 可以对每个卷的数据进行精细加密。ONTAP 9.6 附带的 NAE 是 NVE 的一种增长；它允许 ONTAP 对每个卷的数据进行加密，并且这些卷可以在聚合中共享密钥。NVE 和 NAE 都使用 AES 256 位加密。数据也可以存储在没有 SED 的磁盘上。通过 NVE 和 NAE ，即使启用了加密，您也可以使用存储效率功能。纯应用程序层加密会使存储效率的所有优势失败。使用 NVE 和 NAE 可以保持存储效率，因为数据通过 NetApp WAFL 从网络传入 RAID 层，而 RAID 层决定了数据是否应加密。为了提高存储效率，您可以将聚合重复数据删除与 NAE 结合使用。NVE 卷和 NAE 卷可以同时位于同一 NAE 聚合上。NAE 聚合不支持未加密的卷。

此过程的工作原理如下：对数据进行加密后，它会发送到经过 FIPS 140-2 1 级验证的加密模块。加密模块对数据进行加密并将其发送回 RAID 层。然后，加密数据将发送到磁盘。因此，结合使用 NVE 和 NAE 时，数据在传输到磁盘的过程中已加密。读取操作遵循反向路径。换言之，数据离开磁盘时会进行加密，发送到 RAID ，并通过加密模块进行解密，然后再发送到堆栈的其余部分，如下图所示。



NVE 使用经过 FIPS 140-2 1 级验证的软件加密模块。

有关NVE的详细信息，请参见 "NVE 产品规格"。

NVE 可保护云中的数据。Cloud Volumes ONTAP 和 Azure NetApp Files 能够提供 FIPS 140-2 合规的空闲数据加密。

从 ONTAP 9.7 开始，如果您拥有 NVE 许可证以及板载或外部密钥管理，则新创建的聚合和卷会默认加密。从 ONTAP 9.6 开始，您可以使用聚合级别的加密为要加密的卷的所属聚合分配密钥。默认情况下，您在聚合中创建的卷会进行加密。对卷进行加密时，您可以覆盖默认值。

ONTAP NAE 命令行界面命令

在运行以下命令行界面命令之前，请确保集群具有所需的 NVE 许可证。

要创建聚合并对其进行加密，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

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

要将非 NAE 聚合转换为 NAE 聚合，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

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

要将 NAE 聚合转换为非 NAE 聚合，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

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

ONTAP NVE 命令行界面命令

从 ONTAP 9.6 开始，您可以使用聚合级别的加密为要加密的卷的所属聚合分配密钥。默认情况下，您在聚合中创建的卷会进行加密。

要在启用了 NAE 的聚合上创建卷，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

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

要在不移动卷的情况下对现有卷进行 " 原位 " 加密，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

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

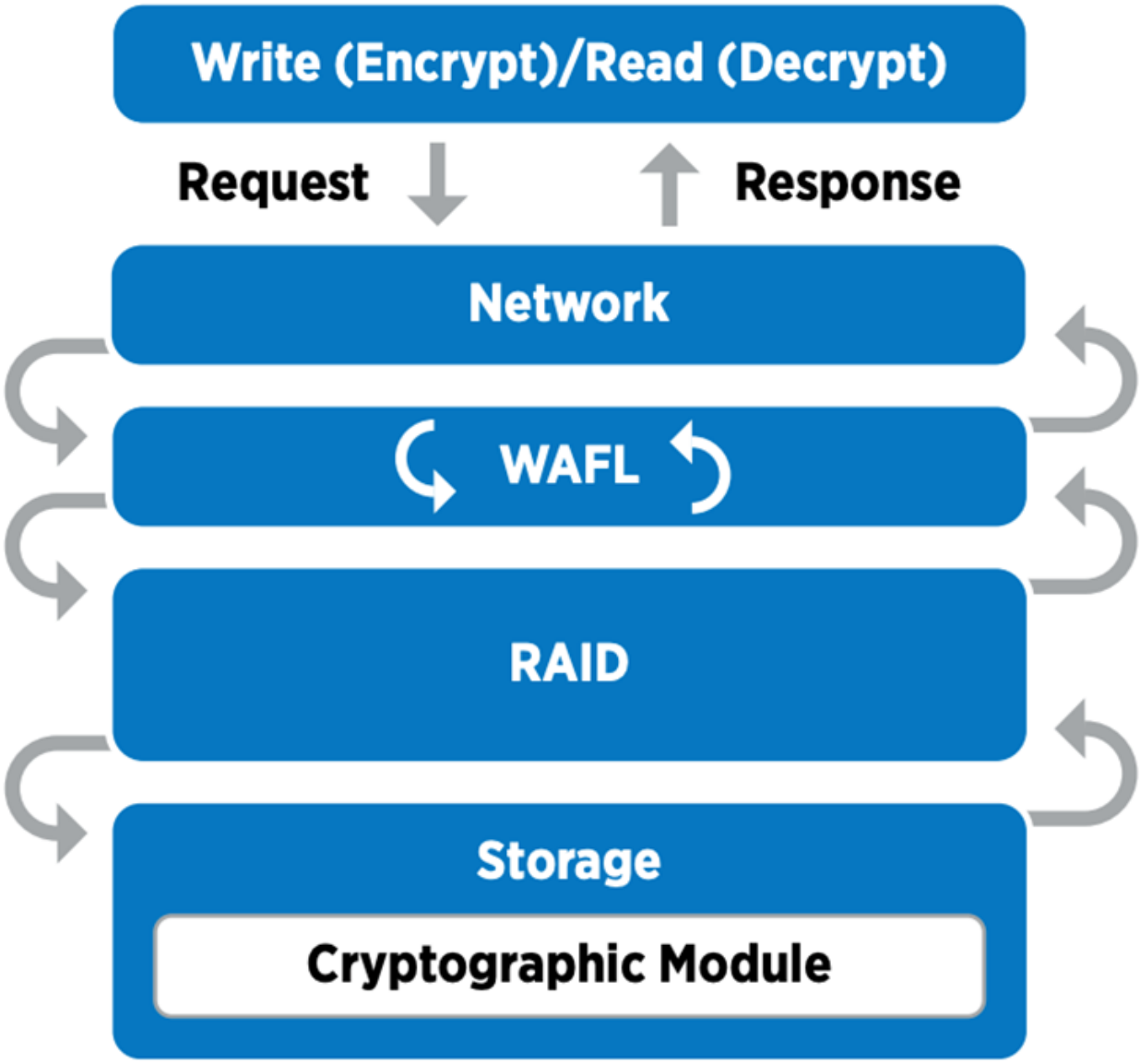
要验证是否已为卷启用加密，请运行以下命令行界面命令：

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

NSE

NSE 使用 SED 通过硬件加速机制执行数据加密。

NSE 配置为使用 FIPS 140-2 2 级自加密驱动器，通过 AES 256 位透明磁盘加密来保护空闲数据，从而有利于合规性和备用磁盘返回。驱动器在内部执行所有数据加密操作，如下图所示，包括生成加密密钥。为了防止未经授权访问数据，存储系统必须使用首次使用驱动器时建立的身份验证密钥向驱动器进行身份验证。



NSE 会在每个驱动器上使用硬件加密，此加密已通过 FIPS 140-2 2 级别 2 验证。

有关NSE的详细信息，请参见 "NSE 产品规格"。

密钥管理

FIPS 140-2 标准适用场景 边界定义的加密模块，如下图所示。

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.

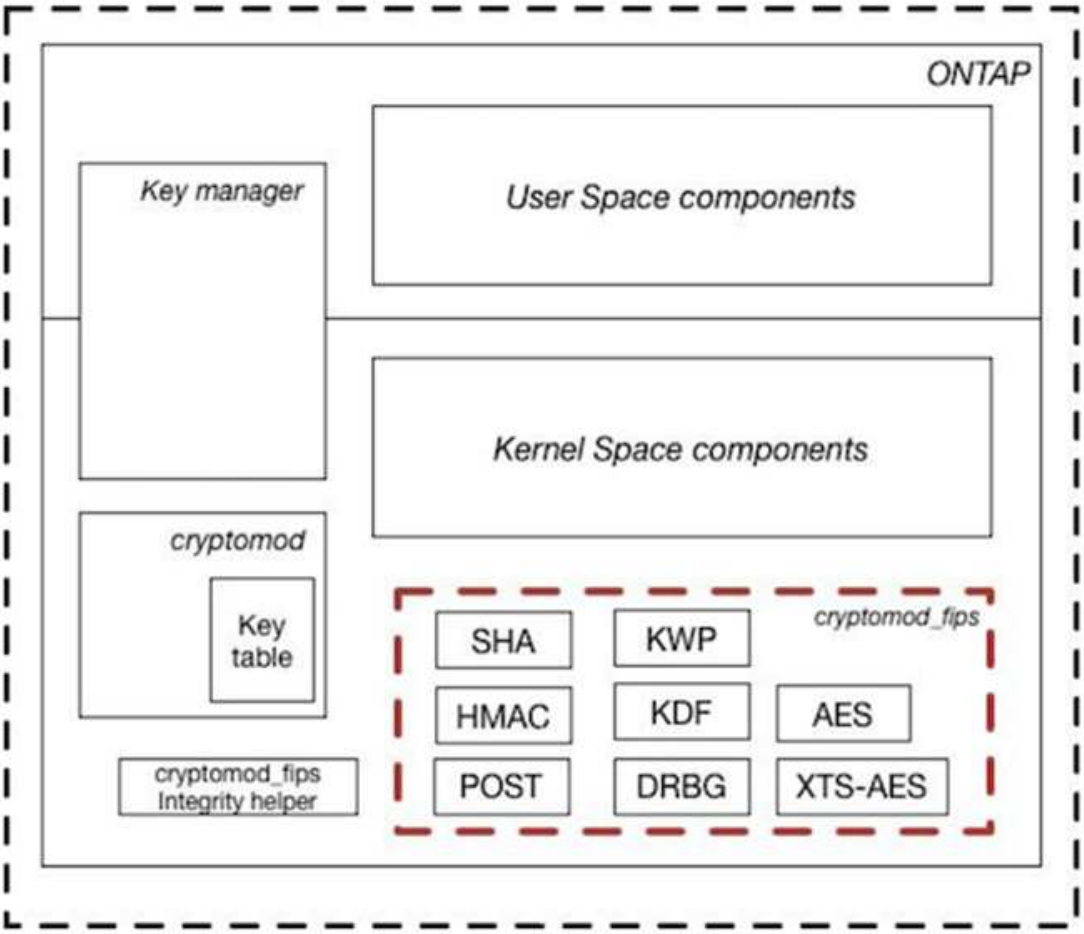


Figure 1 - Block Diagram

密钥管理器会跟踪 ONTAP 使用的所有加密密钥。NSE SED 使用密钥管理器为 NSE SED 设置身份验证密钥。使用密钥管理器时， NVE 和 NAE 解决方案 的组合由软件加密模块，加密密钥和密钥管理器组成。对于每个卷， NVE 使用唯一的 XTS-AES 256 数据加密密钥，该密钥由密钥管理器存储。用于数据卷的密钥对于该集群中的数据卷是唯一的，它是在创建加密卷时生成的。同样， NAE 卷在每个聚合中使用唯一的 XTS-AES 256 数据加密密钥，密钥管理器也会存储这些密钥。创建加密聚合时会生成 NAE 密钥。ONTAP 不会对密钥执行重新生成，重复使用或以纯文本格式显示—它们由密钥管理器存储和保护。

支持外部密钥管理器

从 ONTAP 9.3 开始， NVE 和 NSE 解决方案均支持外部密钥管理器。FIPS 140-2 标准适用场景 —特定供应商实施中使用的加密模块。大多数情况下， FlexPod 和 ONTAP 客户会使用以下经过验证（根据 "NetApp 互操作性表"）密钥管理器：

- Gemalto 或 SafeNet ，网址为
- Vormetric （ Thales ）
- IBM SKLM

- Utimaco （原 MicroFocus ， HPE ）

NSE 和 NVMe SED 身份验证密钥可使用行业标准 OASIS 密钥管理互操作性协议（ KMIP ）备份到外部密钥管理器。只有存储系统，驱动器和密钥管理器才能访问此密钥，如果将此驱动器移至安全域之外，则无法解锁，从而防止数据泄露。外部密钥管理器还存储 NVE 卷加密密钥和 NAE 聚合加密密钥。如果控制器和磁盘已移动，并且无法再访问外部密钥管理器，则 NVE 和 NAE 卷将无法访问，并且无法解密。

以下示例命令会将两个密钥管理服务器添加到 Storage Virtual Machine （ SVM ） `svmname1` 的外部密钥管理器所使用的服务器列表中。

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

在多租户情形中使用 FlexPod 数据中心时， ONTAP 会在 SVM 级别为用户提供租户隔离，以确保安全。

要验证外部密钥管理器列表，请运行以下命令行界面命令：

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

将加密结合使用实现双重加密（分层防护）

如果您需要隔离对数据的访问并确保数据始终受到保护，则 NSE SED 可以与网络或网络结构级加密结合使用。如果管理员忘记配置或错误配置更高级别的加密，则 NSE SED 就像一个后备站。对于两个不同的加密层，您可以将 NSE SED 与 NVE 和 NAE 结合使用。

NetApp ONTAP 集群范围控制面板 **FIPS** 模式

NetApp ONTAP 数据管理软件具有 FIPS 模式配置，可为客户实例化更高的安全性级别。此 FIPS 模式仅对控制平面进行适用场景 。根据 FIPS 140-2 的关键要素启用 FIPS 模式后，传输层安全 v1 （ Transport Layer Security v1 ， TLSv1 ）和 SSLv3 将被禁用，只有 TLS v1.1 和 TLS v1.2 保持启用状态。

> FIPS 模式下的 ONTAP 集群范围控制窗格符合 FIPS 140-2 1 级标准。集群范围的 FIPS 模式使用 NCSM 提供的基于软件的加密模块。

集群范围控制平面的 FIPS 140-2 合规模式可保护 ONTAP 的所有控制接口。默认情况下，仅 FIPS 140-2 模式处于禁用状态；但是，您可以通过将 `security config modify` 命令的 `is-fips-enabled` 参数设置为 `true` 来启用此模式。

要在 ONTAP 集群上启用 FIPS 模式，请运行以下命令：

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

启用 SSL FIPS 模式后，从 ONTAP 到外部客户端或 ONTAP 外部服务器组件的 SSL 通信将对 SSL 使用 FIPS 兼容加密。

要显示整个集群的 FIPS 状态，请运行以下命令：

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

"接下来： FlexPod 融合基础架构的解决方案 优势。"

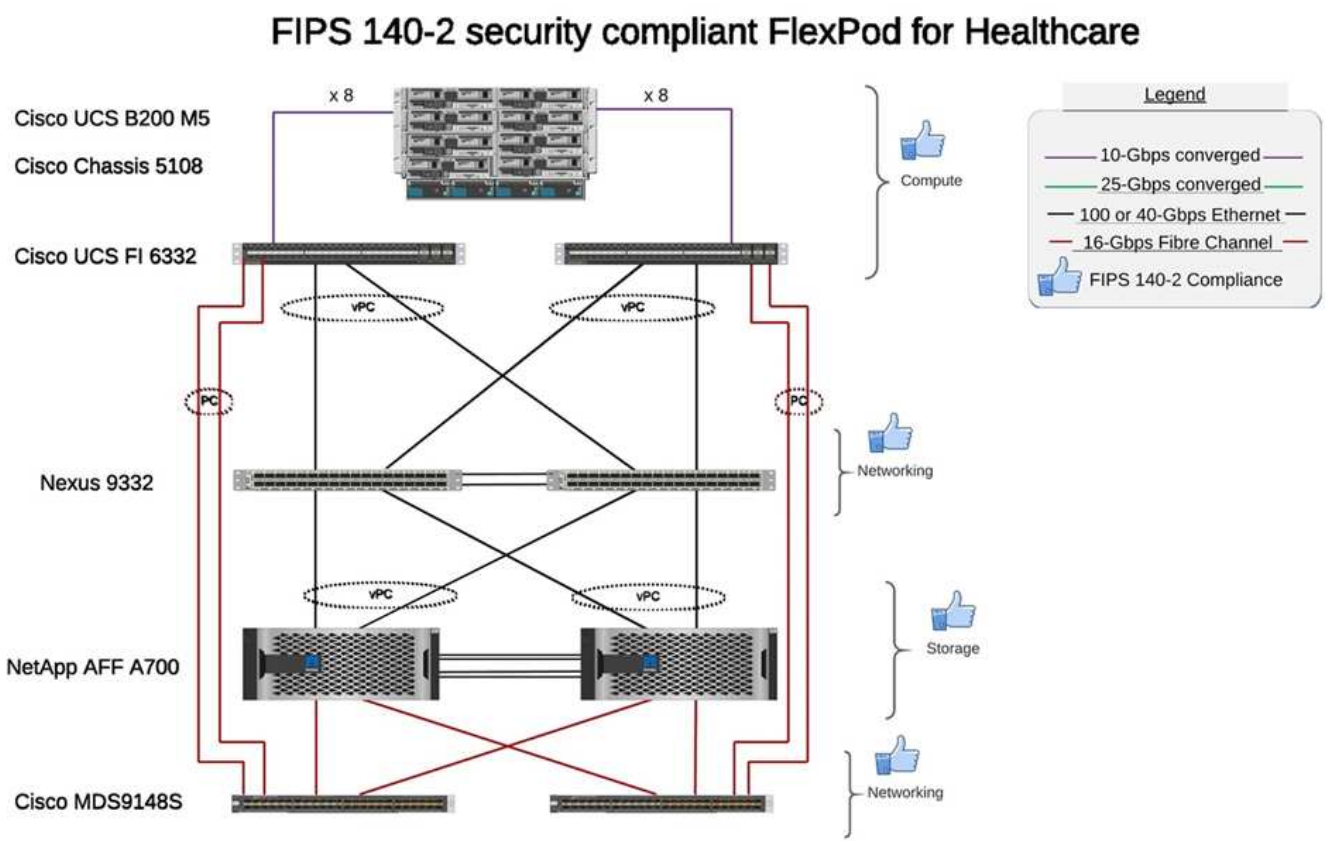
FlexPod 融合基础架构的解决方案 优势

"先前版本： FlexPod NetApp ONTAP 存储和 FIPS 140-2 。"

医疗保健组织拥有多个任务关键型系统。其中两个最关键的系统是电子健康记录（ EHR ）系统和医学影像系统。为了演示 FlexPod 系统上的 FIPS 设置，我们在 FlexPod 系统上使用了开源 EHR 和开源图片归档和通信系统（ PACS ）系统进行实验室设置和工作负载验证。有关 EHR 功能， EHR 逻辑应用程序组件以及在 FlexPod 系统上实施 EHR 系统时如何获益的完整列表，请参见 "TR-4881： 适用于电子健康记录系统的 FlexPod"。有关医疗成像系统功能，逻辑应用程序组件以及在 FlexPod 上实施医疗成像系统时如何受益的完整列表，请参见 "TR-4865： 适用于医疗成像的 FlexPod"。

在 FIPS 设置和工作负载验证期间，我们会运用典型医疗保健组织的工作负载特征。例如，我们采用了开源 EHR 系统，其中包括真实的患者数据访问和更改场景。此外，我们还在 ` * 中执行了医疗成像工作负载，其中包括医学数字成像和通信（ Dicom ）对象。dcm` 文件格式。包含元数据的 Dicom 对象存储在文件和块存储中。此外，我们还从虚拟化 RedHat Enterprise Linux （ RHEL ）服务器中实施了多路径功能。我们会将 Dicom 对象存储在 NFS 上，使用 iSCSI 挂载 LUN 以及使用 FC 挂载 LUN 。在 FIPS 设置和验证期间，我们发现 FlexPod 融合基础架构超出了我们的预期，并且性能无缝。

下图显示了用于 FIPS 设置和验证的 FlexPod 系统。我们利用了 "采用 VMware vSphere 7.0 和 NetApp ONTAP 9.7 的 FlexPod Datacenter Cisco 验证设计（ CVD ）" 在设置过程中。



解决方案基础架构硬件和软件组件

以下两个图分别列出了在 FlexPod 上启用 FIPS 测试期间使用的硬件和软件组件。这些表中的建议仅为示例；您应与 NetApp SME 合作，确保这些组件适合您的组织。此外，请确保中支持这些组件和版本 "NetApp 互操作性表工具" （ IMT ）和 "Cisco 硬件兼容性列表（ HCL ）"。

层	产品系列	数量和型号	详细信息
计算	Cisco UCS 5108 机箱	1 或 2	
	Cisco UCS 刀片式服务器	3 个 B200 M5	每个都具有 2 个 20 或更多核心， 2.7 GHz 和 128-384 GB RAM
	Cisco UCS 虚拟接口卡（ VIC ）	Cisco UCS 1440	请参见
	2 个 Cisco UCS 互联阵列	6332	-
网络	Cisco Nexus 交换机	2 个 Cisco Nexus 9332	-
存储网络	用于通过 SMB/CIFS ， NFS 或 iSCSI 协议进行存储访问的 IP 网络	与上述相同的网络交换机	-
	通过 FC 进行存储访问	2 个 Cisco MDS 9148S	-
存储	NetApp AFF A700 全闪存存储系统	1 个集群	具有两个节点的集群

层	产品系列	数量和型号	详细信息
	磁盘架	一个 DS224C 或 NS224 磁盘架	已完全填充 24 个驱动器
	SSD	大于 24 ， 1.2 TB 或更大的容量	-

软件	产品系列	版本或版本	详细信息
各种	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 （ 64 位）	-
	NetApp ONTAP	ONTAP 9.7 或更高版本	-
	Cisco UCS 互联阵列	Cisco UCS Manager 4.1 或更高版本	-
	Cisco 以太网 3000 或 9000 系列交换机	对于 9000 系列，对于 3000 系列，则为 7.0 （ 3 ） i7 （ 7 ）或更高版本，对于 9.2 （ 4 ）或更高版本	-
	Cisco FC： Cisco MDS 9132T	8.4 （ 1a ）或更高版本	-
	虚拟机管理程序	VMware vSphere ESXi 6.7 U2 或更高版本	-
存储	虚拟机管理程序管理系统	VMware vCenter Server 6.7 U3 （ vCSA ）或更高版本	-
网络	NetApp 虚拟存储控制台（ VSC ）	VSC 9.7 或更高版本	-
	NetApp SnapCenter	SnapCenter 4.3 或更高版本	-
	Cisco UCS Manager	4.1 （ 1c ）或更高版本	
虚拟机管理程序	ESXi		
管理	虚拟机管理程序管理系统 VMware vCenter Server 6.7 U3 （ vCSA ）或更高版本		
	NetApp 虚拟存储控制台（ VSC ）	VSC 9.7 或更高版本	
	NetApp SnapCenter	SnapCenter 4.3 或更高版本	
	Cisco UCS Manager	4.1 （ 1c ）或更高版本	

"接下来：其他 FlexPod 安全注意事项。"

其他 FlexPod 安全注意事项

"上一篇： FlexPod 融合基础架构的解决方案 优势。"

FlexPod 基础架构是一个模块化，融合，可选择虚拟化，可扩展（横向扩展和纵向扩展）以及经济高效的平台。借助 FlexPod 平台，您可以独立横向扩展计算，网络和存储，加快应用程序部署速度。模块化架构支持无中断运行，即使在系统横向扩展和升级活动期间也是如此。

HIT 系统的不同组件要求将数据存储在 SMB/CIFS ， NFS ， ext4 和 NTFS 文件系统中。这一要求意味着基础架构必须通过 NFS ， CIFS 和 SAN 协议提供数据访问。一个 NetApp 存储系统可以支持所有这些协议，因此不再需要采用传统的协议专用存储系统。此外，一个 NetApp 存储系统还可以支持多个命中工作负载，例如 EHRs ， PACS 或 VNA ，基因组学， VDI 等。 具有有保障且可配置的性能级别。

在 FlexPod 系统中部署时， Hit 可提供医疗保健行业特有的多项优势。下面列出了这些优势的高级问题描述：

- * FlexPod 安全性 * 。安全性是 FlexPod 系统的基础。在过去几年中，勒索软件已成为一种威胁。勒索软件是一种基于密码学的恶意软件，它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数据进行解密。要了解FlexPod解决方案如何帮助缓解勒索软件等威胁，请参见 "TR-4802： 《从解决方案 到勒索软件》"。FlexPod基础架构组件也是 "符合 FIPS 140-2"。
- * Cisco Intersight 。 * Cisco Intersight 是一款基于云的创新型管理即服务平台，可为全堆栈 FlexPod 管理和编排提供单一管理平台。Intersight 平台使用符合 FIPS 140-2 安全标准的加密模块。该平台的带外管理架构使其超出了某些标准或审计范围，例如 HIPAA 。网络上任何可识别的个人运行状况信息都不会发送到 Intersight 门户。
- * NetApp FPolicy 技术。 * NetApp FPolicy （名称文件策略的演变）是一个文件访问通知框架，用于通过 NFS 或 SMB/CIFS 协议监控和管理文件访问。这项技术已成为 ONTAP 数据管理软件的一部分已有十多年来的发展，它有助于检测勒索软件。此零信任引擎提供的安全措施超出了访问控制列表（ ACL ）中的权限范围。FPolicy 有两种操作模式：原生 和外部：
  - 原生 模式同时提供了文件扩展名的黑名单和白名单功能。
  - 外部模式与原生 模式具有相同的功能，但它还与在 ONTAP 系统外部运行的 FPolicy 服务器以及安全信息和事件管理（ Security Information and Event Management ，）系统集成。有关如何打击勒索软件的详细信息，请参见 "《与勒索软件作斗争》： 第三部分— ONTAP FPolicy ，另一款功能强大的原生 （也称为免费）工具" 博客
- * 空闲数据 * 。ONTAP 9 及更高版本提供了三种符合 FIPS 140-2 标准的空闲数据加密解决方案：
  - NSE 是一种使用自加密驱动器的硬件解决方案 。
  - NVE 是一种软件解决方案，用于对任何驱动器类型上的任何数据卷进行加密，其中每个卷都有一个唯一的密钥。
  - NAE 是一种软件解决方案，用于对任何驱动器类型上的任何数据卷进行加密，其中每个聚合都使用唯一的密钥启用数据卷。

> 从 ONTAP 9.7 开始，如果已安装名为 VE 的 NetApp NVE 许可证包，则默认情况下会启用 NAE 和 NVE 。

- * 数据正在传输 * 。从 ONTAP 9.8 开始，互联网协议安全（ Internet Protocol Security ， IPsec ）为客户端与 ONTAP SVM 之间的所有 IP 流量提供端到端加密支持。所有 IP 流量的 IPsec 数据加密包括 NFS ， iSCSI 和 SMB/CIFS 协议。IPsec 为 iSCSI 流量提供了唯一的传输加密选项。

- * 跨混合多云数据网络结构的端到端数据加密 * 。现在，使用 NSE 或 NVE 等空闲数据加密技术以及集群对等加密（ Cluster peering Encryption ， CPE ）传输数据复制流量的客户可以通过升级到 ONTAP 9.8 或更高版本并使用 IPsec 在混合多云数据网络结构中的客户端和存储之间使用端到端加密。从 ONTAP 9 开始，您可以为集群范围的控制面板接口启用 FIPS 140-2 合规模式。默认情况下，仅 FIPS 140-2 模式处于禁用状态。从 ONTAP 9.6 开始， CPe 为 ONTAP 数据复制功能（例如 NetApp SnapMirror ， NetApp SnapVault 和 NetApp FlexCache 技术）提供 TLS 1.2 AES-256 GCM 加密支持。加密可通过两个集群对等方之间的预共享密钥（ PSk ）进行设置。
- * 安全多租户 * 。支持日益增长的虚拟化服务器和存储共享基础架构需求，从而可以安全地多租户特定于设施的信息，尤其是在托管多个数据库和软件实例时。

"接下来：总结。"

结论

"先前版本：其他 FlexPod 安全注意事项。"

通过在 FlexPod 平台上运行医疗保健应用程序，支持 FIPS 140-2 的平台可以更好地保护您的医疗保健组织。FlexPod 可为计算，网络和存储等每个组件提供多层保护。FlexPod 数据保护功能可保护空闲或传输中的数据，并在需要时确保备份安全，随时准备就绪。

利用 FlexPod 预先验证的设计避免人为错误，这些设计经过 Cisco 和 NetApp 战略合作伙伴关系严格测试的融合基础架构。FlexPod 系统经过精心设计和设计，即使在计算，网络和存储层启用了 FIPS 140-2 ，也能以极低的影响提供可预测的低延迟系统性能和高可用性。这种方法可为您的 HIT 系统用户提供卓越的用户体验和最佳的响应时间。

"下一步：确认，版本历史记录以及在何处查找追加信息 。"

声明，版本历史记录以及在何处查找追加信息

"上一篇：结论。"

要了解有关本文档所述信息的更多信息，请查看以下文档和网站：

- 《 Cisco MDS 9000 系列 NX-OS 安全配置指南》

  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 系列 NX-OS 安全配置指南 9.3 （ x ）版

  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 和联邦信息处理标准（ FIPS ）出版物 140-2

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

- FIPS 140-2

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

- 《 NetApp ONTAP 9 加固指南》

  https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf

- 《 NetApp 加密高级指南》

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

- NVE 和 NAE 产品规格

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

- NSE 产品规格

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

- ONTAP 9 文档中心

  http://docs.netapp.com

- NetApp 和联邦信息处理标准（ FIPS ）出版物 140-2

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

- Cisco 和 FIPS 140-2 合规性

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

- NetApp 加密安全模块

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

- 适用于大中型医疗保健组织的网络安全实践

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

- Cisco 和加密模块验证计划（ CMVP ）

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

- NetApp 存储加密， NVMe 自加密驱动器， NetApp 卷加密和 NetApp 聚合加密

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

- NetApp 卷加密和 NetApp 聚合加密

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

- NetApp 存储加密

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

- 适用于电子健康记录系统的 FlexPod

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf
- Data Now ： 利用云互联闪存技术提高 Epic EHR 环境的性能

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf
- 适用于 Epic EHR 基础架构的 FlexPod 数据中心

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf
- 《适用于 Epic EHR 的 FlexPod 数据中心部署指南》

  https://www.netapp.com/media/10658-tr-4693.pdf
- 适用于 MEDITECH 软件的 FlexPod 数据中心基础架构

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf
- FlexPod 标准扩展到了 MEDITECH 软件

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/
- 《适用于 MEDITECH 的 FlexPod 方向性规模估算指南》

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf
- 用于医学影像的 FlexPod

  https://www.netapp.com/media/19793-tr-4865.pdf
- 医疗保健领域的人工智能

  https://www.netapp.com/pdf.html?item=/media/7393-na-369pdf.pdf
- FlexPod for HealthCare 可帮助您轻松实现转型

  https://flexpod.com/solutions/verticals/healthcare/
- Cisco 和 NetApp 的 FlexPod

  https://flexpod.com/

致谢

- NetApp 技术营销工程师 Abhinav Singh
- NetApp 解决方案 医疗保健（ Epic ）架构师 Brian O ' Marhony
- NetApp 追求业务开发经理 Brian Pruitt
- NetApp 高级解决方案架构师 Arvind Ramakrishnan
- NetApp 公司 FlexPod 全球现场首席技术官 Michael Hommer

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2021年4月	初始版本。