FlexPod y Seguridad

FlexPod

NetApp
March 25, 2024

Tabla de contenidos

FlexPod y Seguridad 1
FlexPod, la solución a ransomware 1
Solución FlexPod para el sector sanitario conforme a la seguridad FIPS 140-2-2 21

FlexPod y Seguridad

FlexPod, la solución a ransomware

TR-4802: FlexPod, la solución para ransomware

Arvind Ramakrishnan, NetApp

En colaboración con: 

Para comprender el ransomware, es necesario en primer lugar comprender algunos puntos clave sobre la criptografía. Los métodos criptográficos permiten el cifrado de datos con una clave secreta compartida (cifrado de clave simétrica) o un par de claves (cifrado de claves asimétrico). Una de estas claves es una clave pública ampliamente disponible y la otra es una clave privada no revelada.

El ransomware es un tipo de malware basado en la criptovirología, que es el uso de criptografía para crear software malicioso. Este malware puede utilizar tanto el cifrado simétrico como el cifrado de claves asimétricas para bloquear los datos de una víctima y exigir un rescate para proporcionar la clave para descifrar los datos de la víctima.

¿Cómo funciona el ransomware?

Los siguientes pasos describen cómo el ransomware utiliza la criptografía para cifrar los datos de la víctima sin ningún ámbito para su descifrado o recuperación por parte de la víctima:

1. El atacante genera un par de claves como en el cifrado de claves asimétricas. La clave pública generada se coloca dentro del malware y el malware se libera.
2. Después de que el malware haya entrado en el equipo o sistema de la víctima, genera una clave simétrica aleatoria utilizando un generador de números pseudoorandom (PRNG) o cualquier otro algoritmo viable de generación de números aleatorios.
3. El malware utiliza esta clave simétrica para cifrar los datos de la víctima. Finalmente, cifra la clave simétrica mediante el uso de la clave pública del atacante que se incrustó en el malware. El resultado de este paso es un cifrado asimétrico de la clave simétrica cifrada y el texto cifrado simétrico de los datos de la víctima.
4. El malware borra los datos de la víctima y la clave simétrica que se utilizó para cifrar los datos, sin así dejar margen para la recuperación.
5. La víctima se muestra ahora el texto cifrado asimétrico de la clave simétrica y un valor de rescate que debe pagarse para obtener la clave simétrica que se utilizó para cifrar los datos.
6. La víctima paga el rescate y comparte el cifrado asimétrico con el atacante. El atacante descifra el cifrado con su clave privada, lo que da como resultado la clave simétrica.
7. El atacante comparte esta clave simétrica con la víctima, que se puede utilizar para descifrar todos los datos y, por tanto, recuperarse del ataque.

Retos

Individuos y organizaciones se enfrentan a los siguientes retos cuando son atacados por ransomware:

- El desafío más importante es que se cobra un costo inmediato en la productividad de la organización o del individuo. Toma tiempo para volver a un estado de normalidad, porque todos los archivos importantes deben ser recuperados, y los sistemas deben ser asegurados.
- Podría llevar a una filtración de datos que contenga información confidencial y confidencial de clientes o clientes, y provocar una situación de crisis que una organización querría evitar claramente.
- Existe una gran posibilidad de que los datos entren en las manos equivocadas o se eliminen por completo, lo que conduce a un punto de retorno nulo que podría ser desastroso para las organizaciones y los individuos.
- Después de pagar el rescate, no hay garantía de que el atacante proporcionará la clave para restaurar los datos.
- No hay garantías de que el atacante se abstenga de transmitir los datos delicados a pesar de pagar el rescate.
- En las grandes empresas, identificar la laguna que llevó a un ataque de ransomware es una tarea tediosa, y asegurar todos los sistemas implica un gran esfuerzo.

¿Quién está en riesgo?

Cualquiera puede ser atacado por ransomware, incluidos individuos y organizaciones grandes. Las organizaciones que no aplican medidas y prácticas de seguridad bien definidas son aún más vulnerables a esos ataques. El efecto del ataque en una organización grande puede ser varias veces mayor de lo que un individuo podría soportar.

El ransomware representa aproximadamente el 28 % de todos los ataques de malware. En otras palabras, más de uno de cada cuatro incidentes de malware es un ataque de ransomware. El ransomware puede propagarse automática e indiscriminadamente a través de Internet y, cuando hay un lapso de seguridad, puede entrar en los sistemas de la víctima y continuar extendiéndose a otros sistemas conectados. Los atacantes tienden a dirigirse a personas u organizaciones que realizan un gran uso compartido de archivos, tienen una gran cantidad de datos confidenciales y críticos o a mantener una protección inadecuada frente a ataques.

Los atacantes tienden a centrarse en los siguientes objetivos potenciales:

- Universidades y comunidades estudiantiles
- Oficinas y organismos gubernamentales
- Hospitales
- De Estados Unidos

Esta no es una lista exhaustiva de objetivos. Usted no puede considerarse seguro de los ataques si se encuentra fuera de una de estas categorías.

¿Cómo se introduce el ransomware en un sistema o se distribuye?

Existen varias formas en las que el ransomware puede entrar en un sistema o propagarse a otros sistemas. En el mundo actual, casi todos los sistemas están conectados entre sí a través de Internet, LAN, WAN, etc. La cantidad de datos que se generan e intercambian entre estos sistemas no hace más que aumentar.

Algunos de los métodos más comunes mediante los que se puede distribuir el ransomware incluyen métodos

que utilizamos diariamente para compartir o acceder a los datos:

- Correo electrónico
- Redes P2P
- Descargas de archivos
- Redes sociales
- Dispositivos móviles
- Conectarse a redes públicas no seguras
- Acceso a direcciones URL Web

Consecuencias de la pérdida de datos

Las consecuencias o los efectos de la pérdida de datos pueden ser más amplios de lo que las organizaciones podrían anticipar. Los efectos pueden variar en función de la duración del tiempo de inactividad o del período de tiempo durante el cual una organización no tiene acceso a sus datos. Cuanto más dure el ataque, mayor será el efecto sobre los ingresos, la Marca y la reputación de la organización. Una organización también puede enfrentarse a problemas legales y a una fuerte disminución de la productividad.

A medida que estas cuestiones continúan persistiéndose con el tiempo, comienzan a magnificar y podrían terminar cambiando la cultura de una organización, dependiendo de cómo responda al ataque. En el mundo actual, la información se propaga rápidamente y las noticias negativas sobre una organización podrían causar un daño permanente a su reputación. Una organización podría enfrentarse a enormes sanciones por pérdida de datos, lo que podría desembocar en el cierre de un negocio.

Efectos financieros

Según un informe reciente "Informe de McAfee", Los costos globales incurridos por el crimen cibernético son aproximadamente 600 mil millones de dólares, lo que representa aproximadamente el 0.8% del PIB global. Cuando esta cantidad se compara con la creciente economía mundial de internet de 4.2 billones de dólares, equivale a un impuesto del 14% sobre el crecimiento.

El ransomware asume una parte importante de este coste financiero. En 2018, los costos incurridos debido a los ataques de ransomware fueron aproximadamente de $8 mil millones—una cantidad que se prevé que alcanzará los $11.5 mil millones en 2019.

¿Cuál es la solución?

La recuperación a partir de un ataque de ransomware con un tiempo de inactividad mínimo solo es posible gracias a la implementación de un plan de recuperación ante desastres proactivo. Tener la capacidad para recuperarse de un ataque es bueno, pero evitar un ataque es ideal.

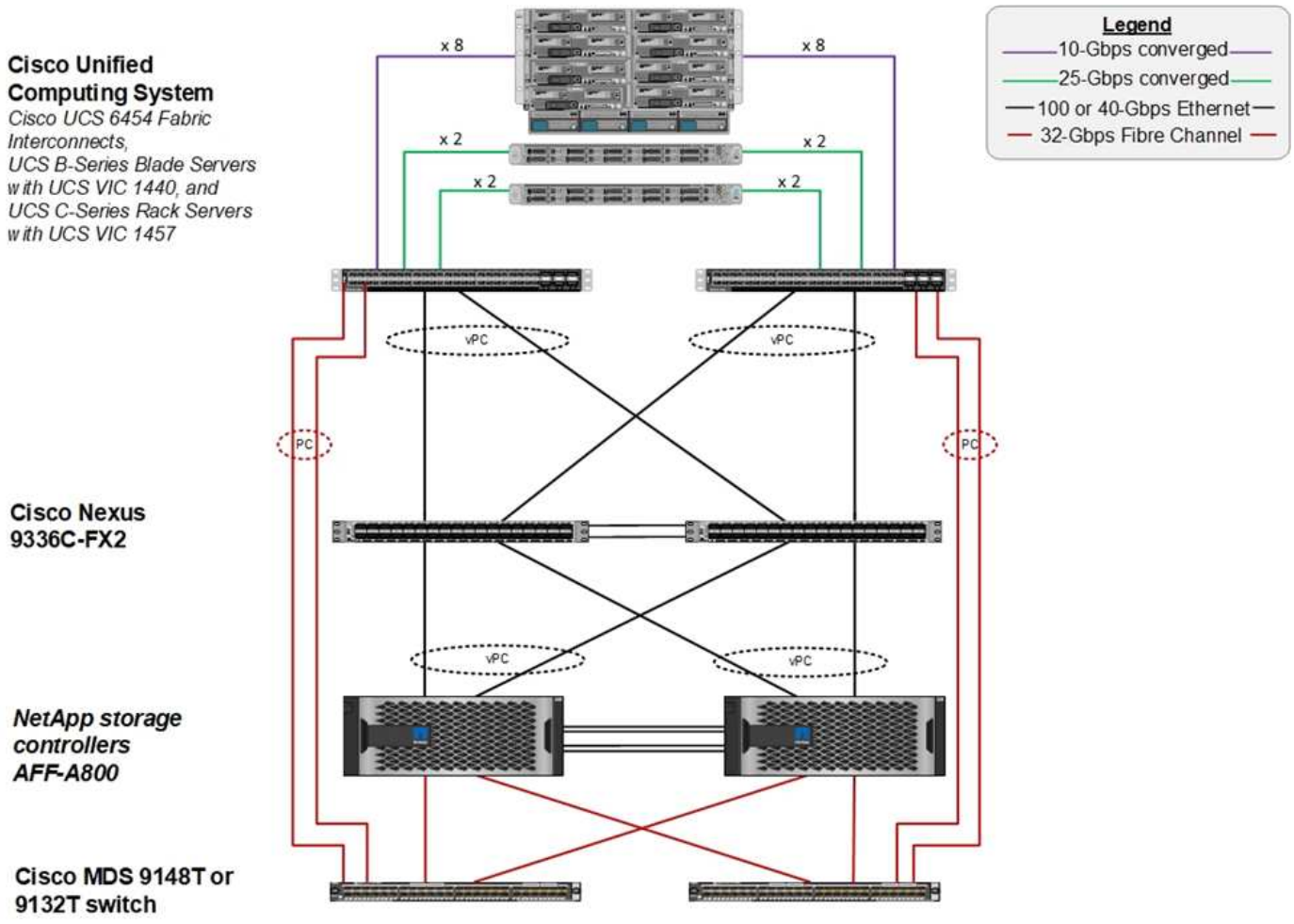
Aunque hay varios frentes que se deben revisar y reparar para evitar un ataque, el componente central que permite prevenir o recuperar de un ataque es el centro de datos.

El diseño del centro de datos y las funciones que proporciona para proteger los puntos finales de red, informática y almacenamiento tienen un papel fundamental a la hora de crear un entorno seguro para las operaciones cotidianas. Este documento muestra cómo las funciones de una infraestructura de cloud híbrido de FlexPod pueden ayudar a lograr una recuperación de datos rápida en caso de ataque, y también pueden ayudar a evitar ataques.

Información general de FlexPod

FlexPod es una arquitectura prediseñada, integrada y validada que combina servidores Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus, switches estructurales Cisco MDS y cabinas de almacenamiento de NetApp en una sola arquitectura flexible. Las soluciones FlexPod están diseñadas para ofrecer alta disponibilidad sin puntos únicos de error, a la vez que mantienen la rentabilidad y la flexibilidad del diseño necesarias para acomodar una amplia variedad de cargas de trabajo. Un diseño de FlexPod puede admitir diferentes hipervisores y servidores con configuración básica, y también puede dimensionarse y optimizarse según los requisitos de carga de trabajo de los clientes.

La siguiente figura muestra la arquitectura de FlexPod y destaca claramente la alta disponibilidad en todas las capas de la pila. Los componentes de la infraestructura de almacenamiento, red y computación se configuran de forma que las operaciones se pueden conmutar al respaldo instantáneamente al partner superviviente en caso de que uno de los componentes falle.



Una ventaja importante para un sistema FlexPod es que está diseñado, integrado y validado para varias cargas de trabajo. Se publican guías detalladas de diseño e instalación para cada validación de soluciones. Estos documentos incluyen las prácticas recomendadas que debe emplear para que las cargas de trabajo se ejecuten sin problemas en FlexPod. Estas soluciones se han creado con los mejores productos de informática, red y almacenamiento de su clase y con una gran cantidad de funciones centradas en la seguridad y el endurecimiento de toda la infraestructura.

"El índice de inteligencia de amenazas X-Force de IBM" estados, “error humano responsable de dos tercios de los registros comprometidos, incluido un aumento histórico del 424% en infraestructura de nube mal configurada”.

Con un sistema FlexPod, puede evitar una configuración incorrecta de su infraestructura mediante los libros de estrategia de Ansible que realizan una configuración integral de la infraestructura de acuerdo con las mejores prácticas descritas en los diseños validados por Cisco (CVD) y las arquitecturas verificadas de NetApp (NVA).

Medidas de protección contra ransomware

En esta sección se describen las funciones clave del software de gestión de datos ONTAP de NetApp y las herramientas para Cisco UCS y Cisco Nexus que puede usar para proteger y recuperar datos de forma efectiva de ataques de ransomware.

Almacenamiento: ONTAP de NetApp

El software ONTAP ofrece muchas funciones útiles para la protección de datos, la mayoría de las cuales son gratuitas para los clientes que tienen un sistema ONTAP. Puede utilizar las siguientes funciones en todo momento para proteger los datos de los ataques:

- **Tecnología Snapshot de NetApp.** una copia snapshot es una imagen de solo lectura de un volumen que captura el estado de un sistema de archivos en un momento dado. Estas copias ayudan a proteger los datos sin afectar el rendimiento del sistema y, al mismo tiempo, no ocupan mucho espacio de almacenamiento. NetApp recomienda crear un programa para la creación de copias Snapshot. Usted también debe mantener un largo período de retención porque algunos malware pueden permanecer inactivos y luego reactivar semanas o meses después de una infección. En caso de ataque, es posible revertir el volumen utilizando una copia snapshot que se había realizado antes de la infección.
- **Tecnología SnapRestore de NetApp.** el software de recuperación de datos SnapRestore es extremadamente útil para la recuperación de datos dañados o para revertir únicamente el contenido del archivo. SnapRestore no revierte los atributos de un volumen; es mucho más rápido de lo que puede conseguir un administrador al copiar los archivos de la copia snapshot al sistema de archivos activo. La velocidad a la que se pueden recuperar los datos resulta útil cuando se deben recuperar muchos archivos lo antes posible. En caso de ataque, este eficiente proceso de recuperación ayuda a que el negocio vuelva a estar online rápidamente.
- **La tecnología SnapCenter de NetApp.** el software SnapCenter utiliza funciones de backup y replicación basadas en almacenamiento de NetApp para proporcionar una protección de datos coherente con las aplicaciones. Este software se integra con aplicaciones empresariales y proporciona flujos de trabajo específicos para aplicaciones y bases de datos para satisfacer las necesidades de los administradores de aplicaciones, bases de datos e infraestructuras virtuales. SnapCenter proporciona una plataforma empresarial fácil de usar para coordinar y administrar de un modo seguro la protección de datos en aplicaciones, bases de datos y sistemas de archivos. Su capacidad de proporcionar protección de datos coherente con las aplicaciones es fundamental durante la recuperación de datos, ya que facilita la restauración de las aplicaciones a un estado coherente con mayor rapidez.
- **La tecnología SnapLock de NetApp.** SnapLock proporciona un volumen para finalidades especiales en el que los archivos se pueden almacenar y poner en un estado en el que no se pueden borrar ni sobrescribir. Los datos de producción del usuario que se encuentran en un volumen FlexVol se pueden duplicar o realizar copias vault en un volumen SnapLock mediante la tecnología SnapMirror o SnapVault de NetApp, respectivamente. Los archivos del volumen de SnapLock, el volumen en sí y su agregado de alojamiento no se pueden eliminar hasta que finalice el período de retención.
- **Tecnología FPolicy de NetApp.** Utilice el software FPolicy para evitar ataques al desactivar las operaciones en archivos con extensiones específicas. Es posible activar un evento de FPolicy para

operaciones de archivos específicas. El evento está ligado a una política, que llama al motor que necesita utilizar. Puede configurar una política con un conjunto de extensiones de archivo que potencialmente puedan contener ransomware. Cuando un archivo con una extensión no permitida intenta realizar una operación no autorizada, FPolicy impide que esa operación se ejecute.

Red: Cisco Nexus

El software Cisco NX OS admite la función NetFlow que permite una detección mejorada de anomalías y seguridad de la red. NetFlow captura los metadatos de cada conversación de la red, las partes implicadas en la comunicación, el protocolo utilizado y la duración de la transacción. Una vez agregada y analizado la información, puede proporcionar una visión del comportamiento normal.

Los datos recopilados también permiten la identificación de patrones de actividad cuestionables, como el malware que se propaga a través de la red, lo que de otra manera puede pasar desapercibida.

NetFlow utiliza flujos para proporcionar estadísticas para la supervisión de la red. Un flujo es un flujo unidireccional de paquetes que llega a una interfaz de origen (o VLAN) y tiene los mismos valores para las claves. Una clave es un valor identificado para un campo dentro del paquete. Puede crear un flujo utilizando un registro de flujo para definir las claves únicas para su flujo. Puede exportar los datos que NetFlow recopila para sus flujos utilizando un exportador de flujo a un colector NetFlow remoto, como Cisco StealtWatch. StealtWatch utiliza esta información para la supervisión continua de la red y proporciona información forense de respuesta a incidentes y detección de amenazas en tiempo real si se produce un brote de ransomware.

Computación: Cisco UCS

Cisco UCS es el extremo de computación en una arquitectura de FlexPod. Puede usar varios productos de Cisco que pueden ayudar a proteger esta capa de la pila en el nivel del sistema operativo.

Puede implementar los siguientes productos clave en la capa informática o de aplicación:

- **Cisco Advanced Malware Protection (AMP) para endpoints.** compatible con los sistemas operativos Microsoft Windows y Linux, esta solución integra capacidades de prevención, detección y respuesta. Este software de seguridad evita infracciones, bloquea el malware en el punto de entrada y supervisa y analiza continuamente la actividad de los archivos y procesos para detectar, contener y resolver rápidamente amenazas que puedan evadir las defensas de primera línea.

  El componente de Protección de actividad maliciosa (MAP) de AMP supervisa continuamente todas las actividades de los extremos y proporciona detección en tiempo de ejecución y bloqueo del comportamiento anormal de un programa en ejecución en el punto final. Por ejemplo, cuando el comportamiento del punto final indica ransomware, los procesos ofensor se terminan, lo que impide el cifrado del punto final y detiene el ataque.

- **Cisco Advanced Malware Protection for Email Security.** los correos electrónicos se han convertido en el vehículo principal para propagar malware y llevar a cabo ciberataques. En promedio, aproximadamente 100 mil millones de correos electrónicos se intercambian en un solo día, lo que proporciona a los atacantes un excelente vector de penetración en los sistemas de los usuarios. Por lo tanto, es absolutamente esencial defender contra esta línea de ataque.

  AMP analiza correos electrónicos para amenazas tales como exploits de día cero y malware sigiloso ocultos en archivos adjuntos maliciosos. También utiliza la inteligencia de URL líder en el sector para combatir enlaces maliciosos. Proporciona a los usuarios protección avanzada contra el phishing espear, el ransomware y otros ataques sofisticados.

- **Sistema de prevención de intrusiones de próxima generación (NGIPS).** Cisco Firepower NGIPS se puede implementar como un dispositivo físico en el centro de datos o como un dispositivo virtual en

VMware (NGIPSv para VMware). Este sistema altamente eficaz de prevención de intrusiones proporciona un rendimiento fiable y un costo total de propiedad bajo. La protección contra amenazas se puede ampliar con licencias de suscripción opcionales para proporcionar funciones de AMP, visibilidad y control de aplicaciones y filtrado de URL. La virtualización de NGIPS inspecciona el tráfico entre equipos virtuales (VM) y facilita la implementación y gestión de soluciones de NGIPS en sitios con recursos limitados, lo que aumenta la protección tanto para activos físicos como virtuales.

Proteja y recupere datos en FlexPod

En esta sección se describe cómo se pueden recuperar los datos de un usuario final en caso de un ataque y cómo se pueden prevenir los ataques mediante un sistema FlexPod.

Resumen de banco

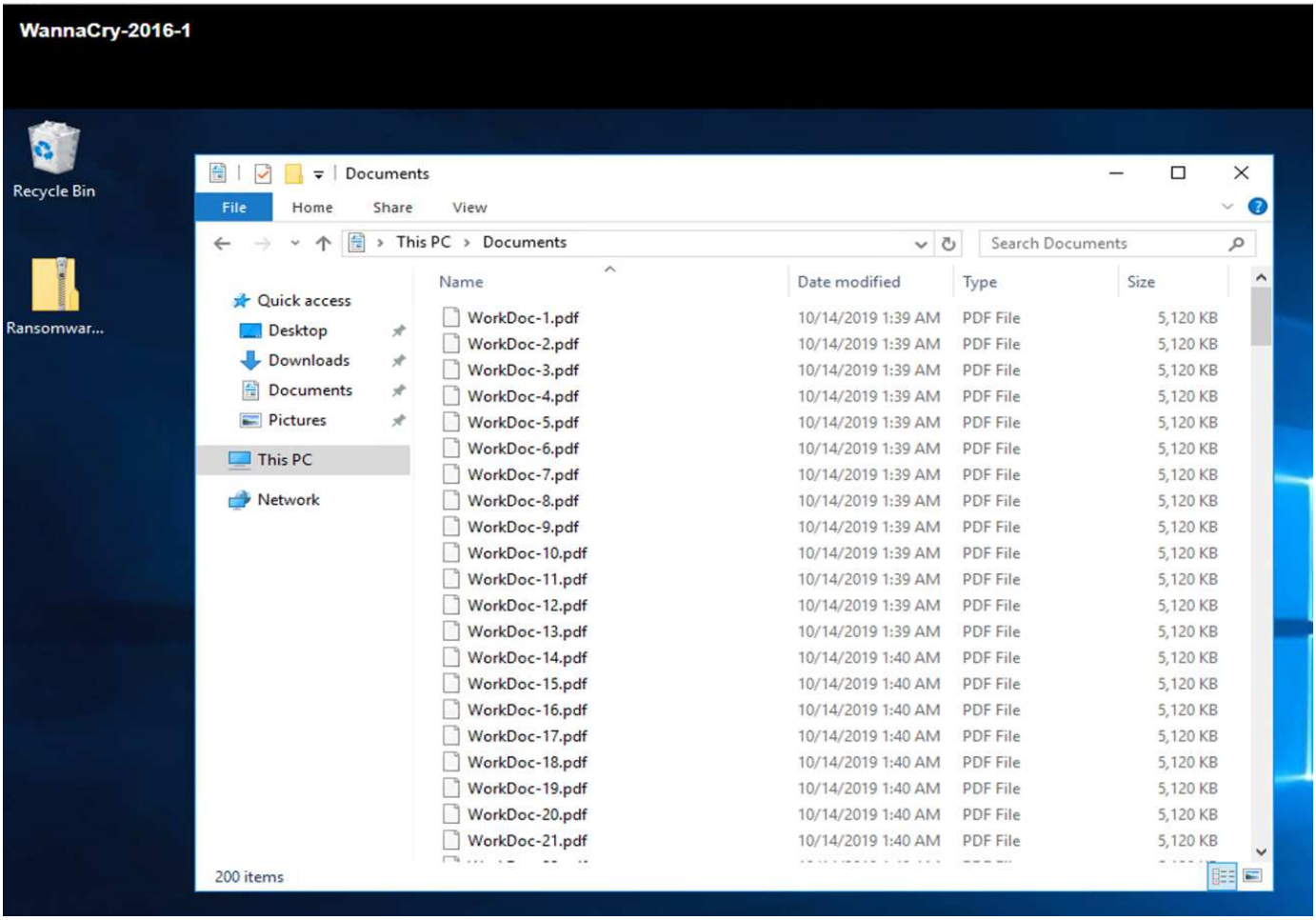
Para presentar la detección, la corrección y la prevención de FlexPod, se creó un banco de pruebas basado en las directrices especificadas en el último CVD de plataforma disponible en el momento en el que se escribió este documento: "FlexPod Datacenter con VMware vSphere 6.7 U1, Cisco UCS de cuarta generación y NetApp AFF A-Series CVD".

Se puso en marcha un equipo virtual con Windows 2016, que proporcionaba un recurso compartido CIFS del software ONTAP de NetApp, en la infraestructura de VMware vSphere. A continuación, se configuró FPolicy de NetApp en el recurso compartido de CIFS para evitar la ejecución de archivos con ciertos tipos de extensiones. El software SnapCenter de NetApp también se puso en marcha para gestionar las copias Snapshot de los equipos virtuales de la infraestructura para proporcionar copias Snapshot coherentes con las aplicaciones.

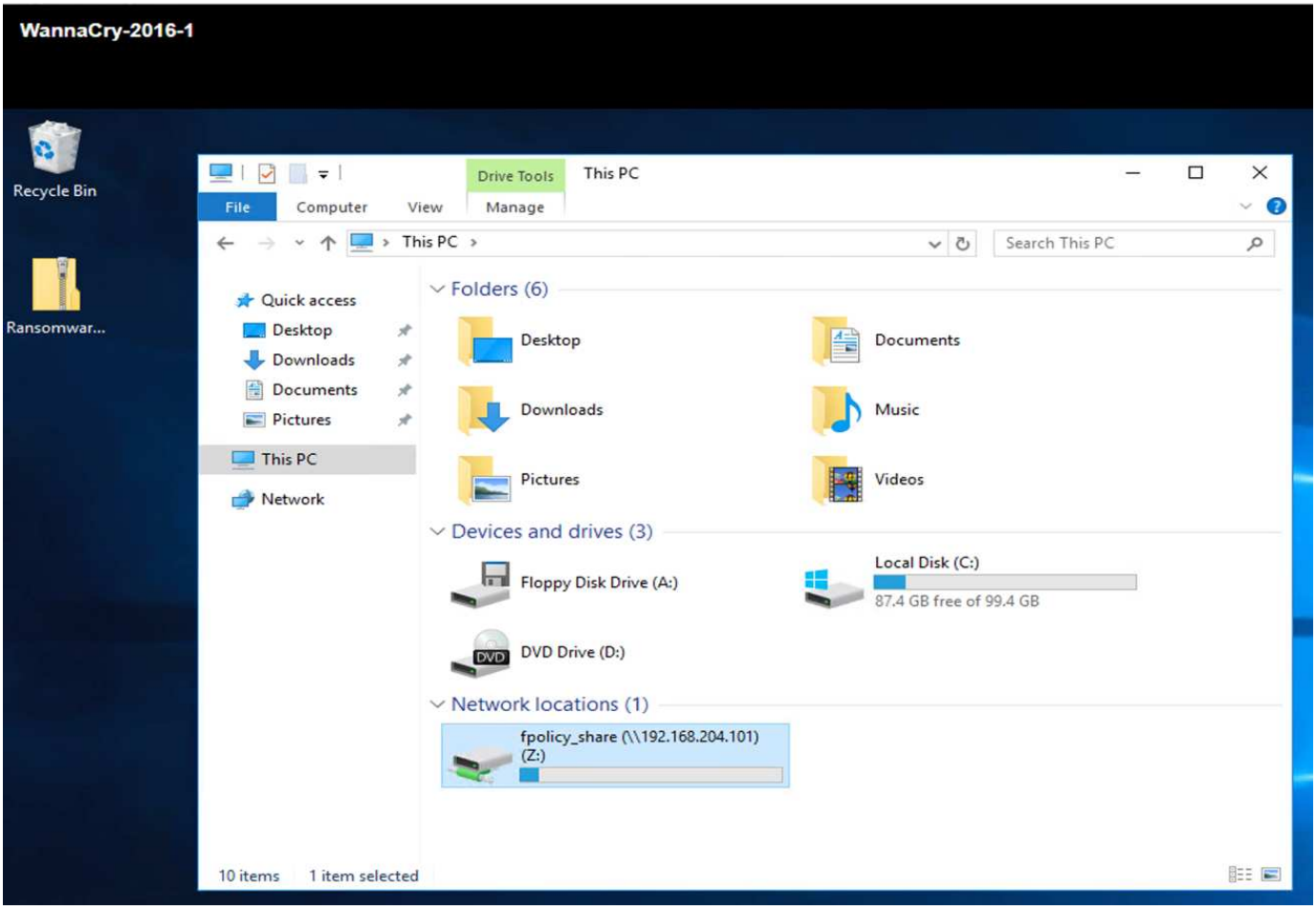
Estado del equipo virtual y sus archivos antes de un ataque

En esta sección se muestra el estado de los archivos antes de un ataque a la máquina virtual y al recurso compartido CIFS que se le ha asignado.

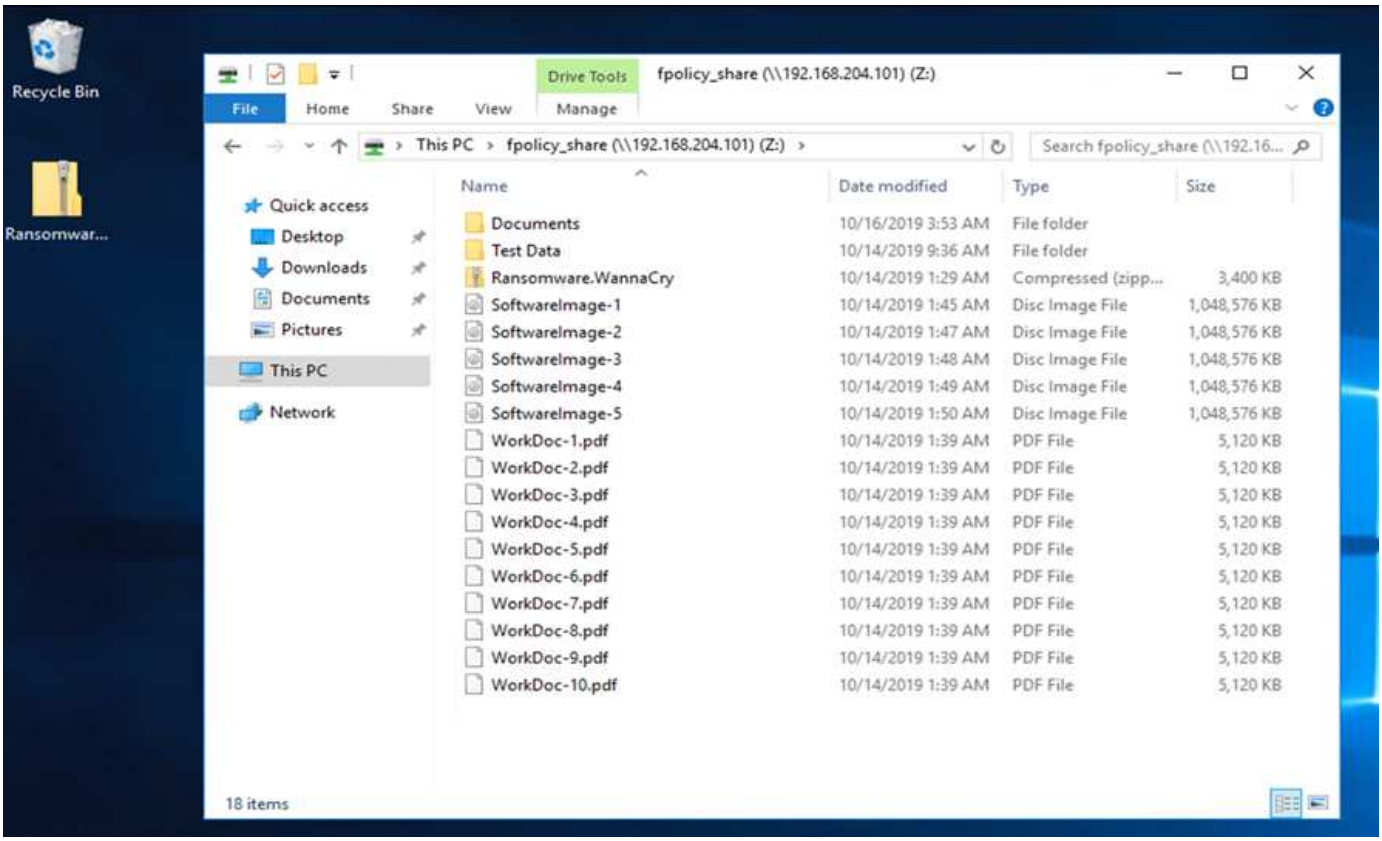
La carpeta Documentos del equipo virtual tenía un conjunto de archivos PDF que todavía no han sido cifrados por el malware WannaCry.



La siguiente captura de pantalla muestra el recurso compartido de CIFS asignado a la máquina virtual.



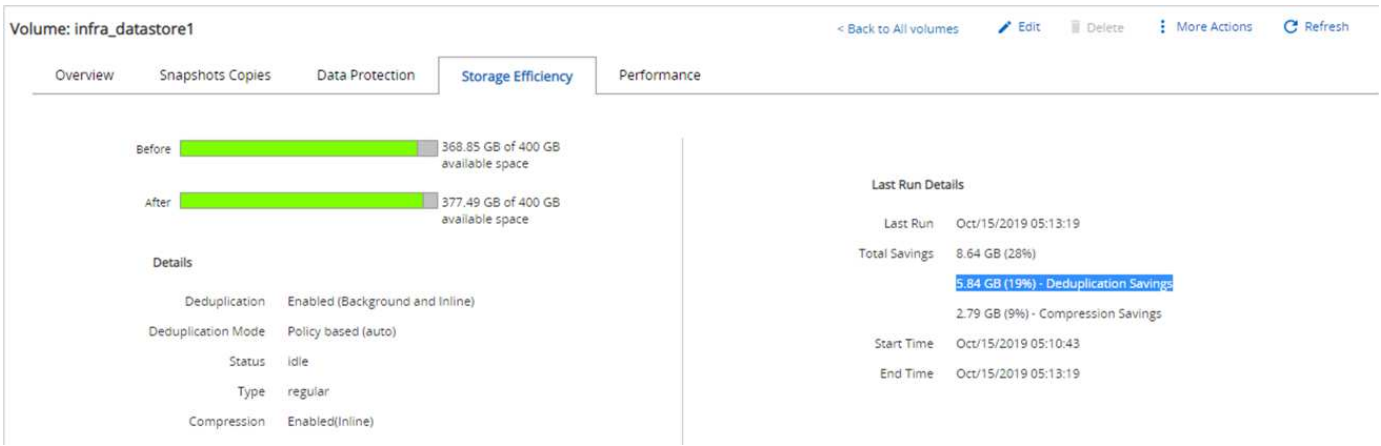
La siguiente captura de pantalla muestra los archivos del recurso compartido CIFS `fpolicy_share` Que todavía no han sido cifrados por el malware WannaCry.



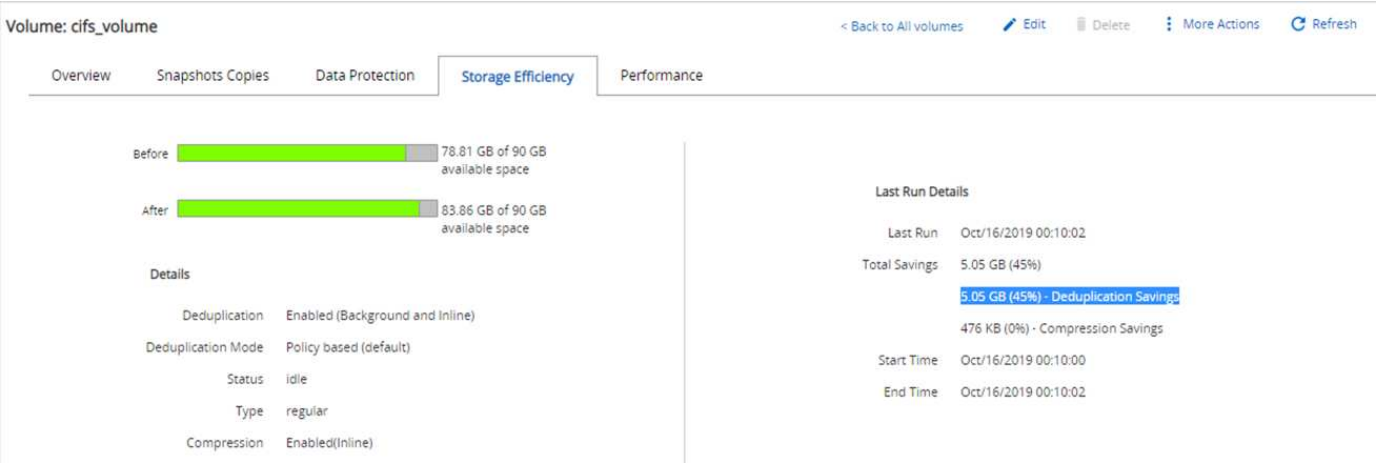
Información sobre deduplicación y copias snapshot antes de un ataque

Los detalles de la eficiencia del almacenamiento y el tamaño de la copia Snapshot antes de un ataque se indican y se utilizan como referencia durante la fase de detección.

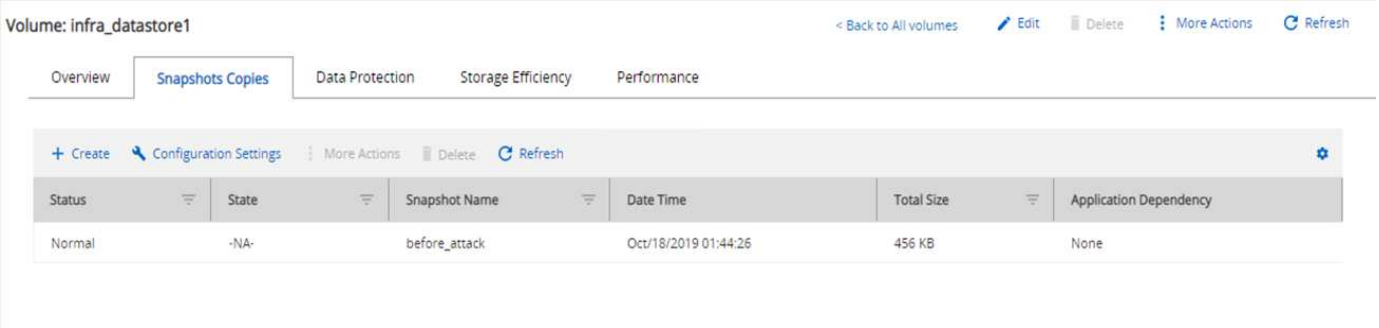
Se obtuvo un ahorro del 19% en el almacenamiento, gracias a la deduplicación en el volumen que alojaba el equipo virtual.



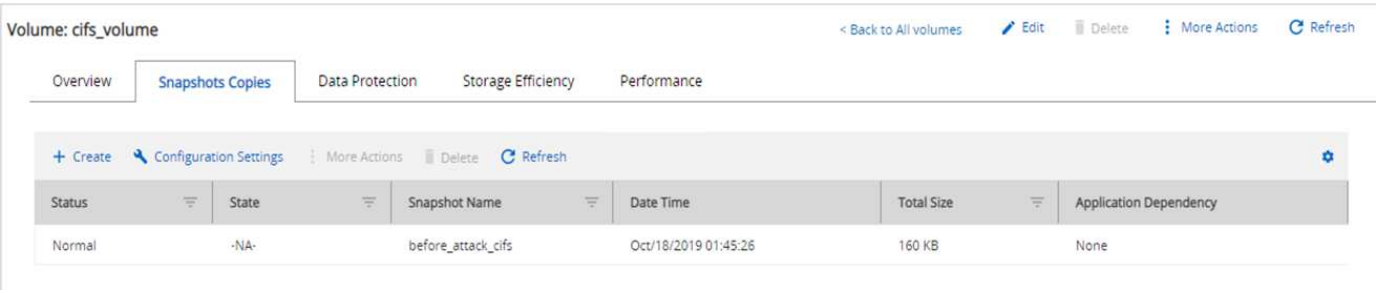
Se obtuvo un ahorro del 45% gracias a la deduplicación en la unidad CIFS `fpolicy_share`.



Se observó un tamaño de copia snapshot de 456 KB para el volumen donde se alojaba el equipo virtual.



Se observó un tamaño de copia Snapshot de 160 KB para el recurso compartido de CIFS `fpolicy_share`.



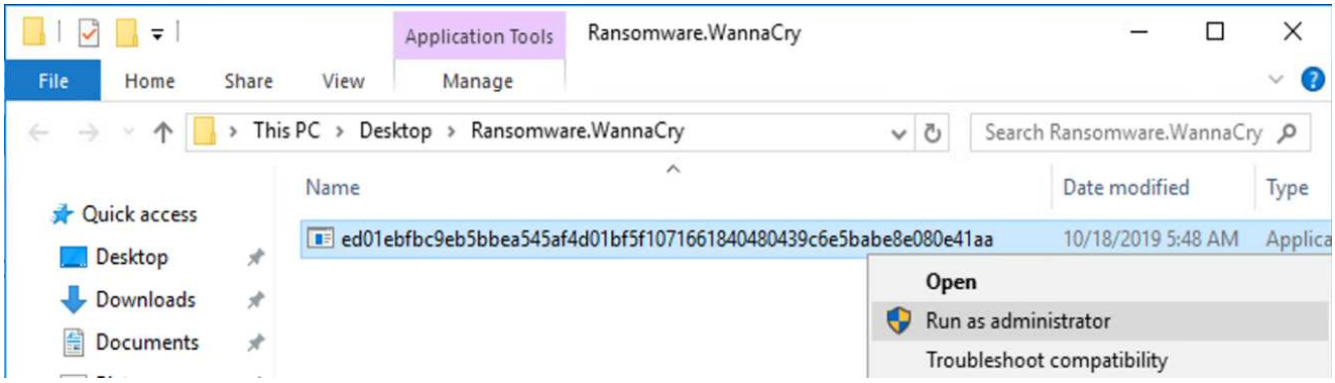
Infección de WannaCry en VM y recursos compartidos de CIFS

En esta sección, mostramos cómo se introdujo el malware de WannaCry en el entorno de FlexPod y los posteriores cambios en el sistema que se observaron.

Los pasos siguientes muestran cómo se introdujo el binario de malware WannaCry en el equipo virtual:

1. Se extrajo el malware protegido.

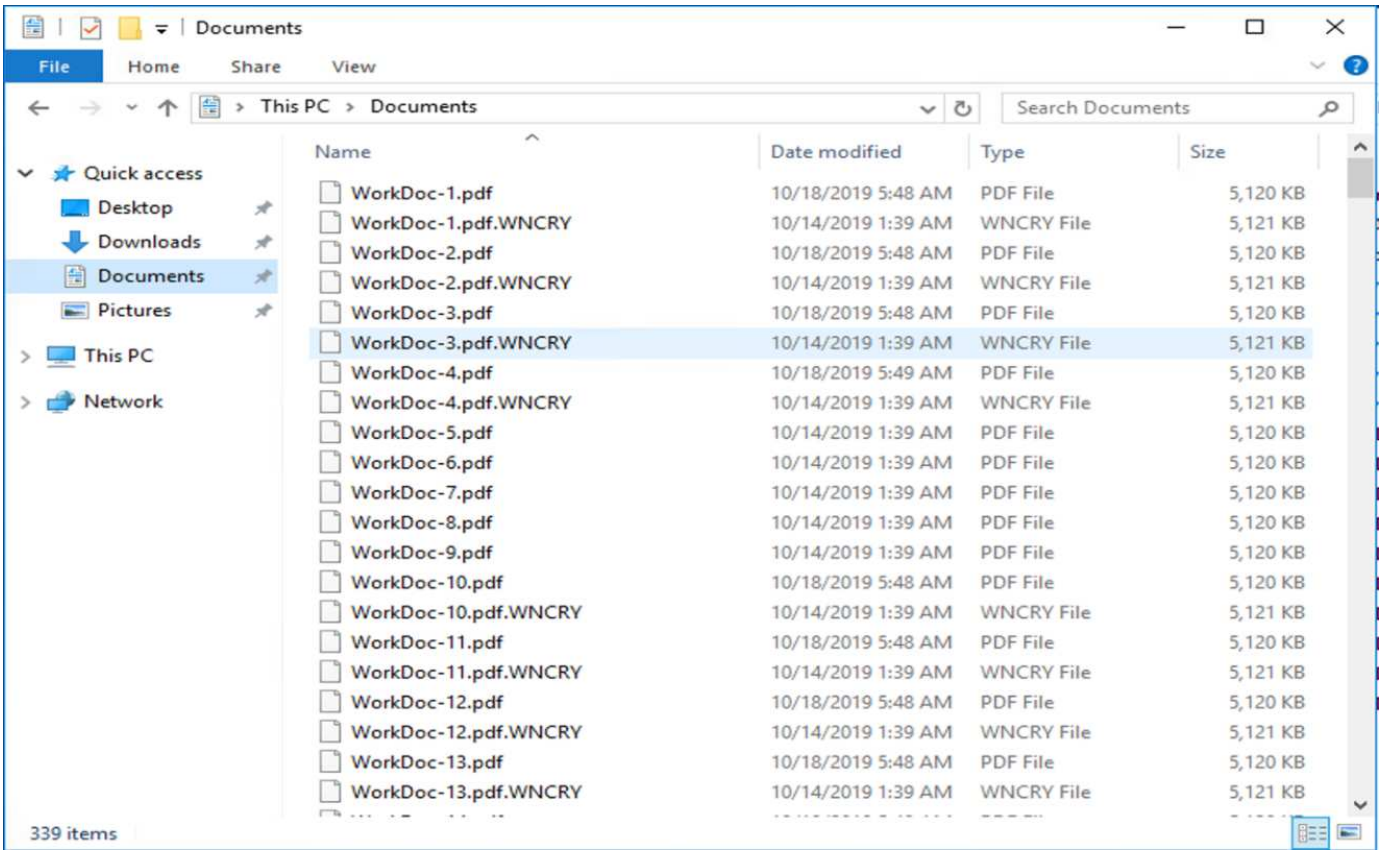
2. Se ejecutó el binario.



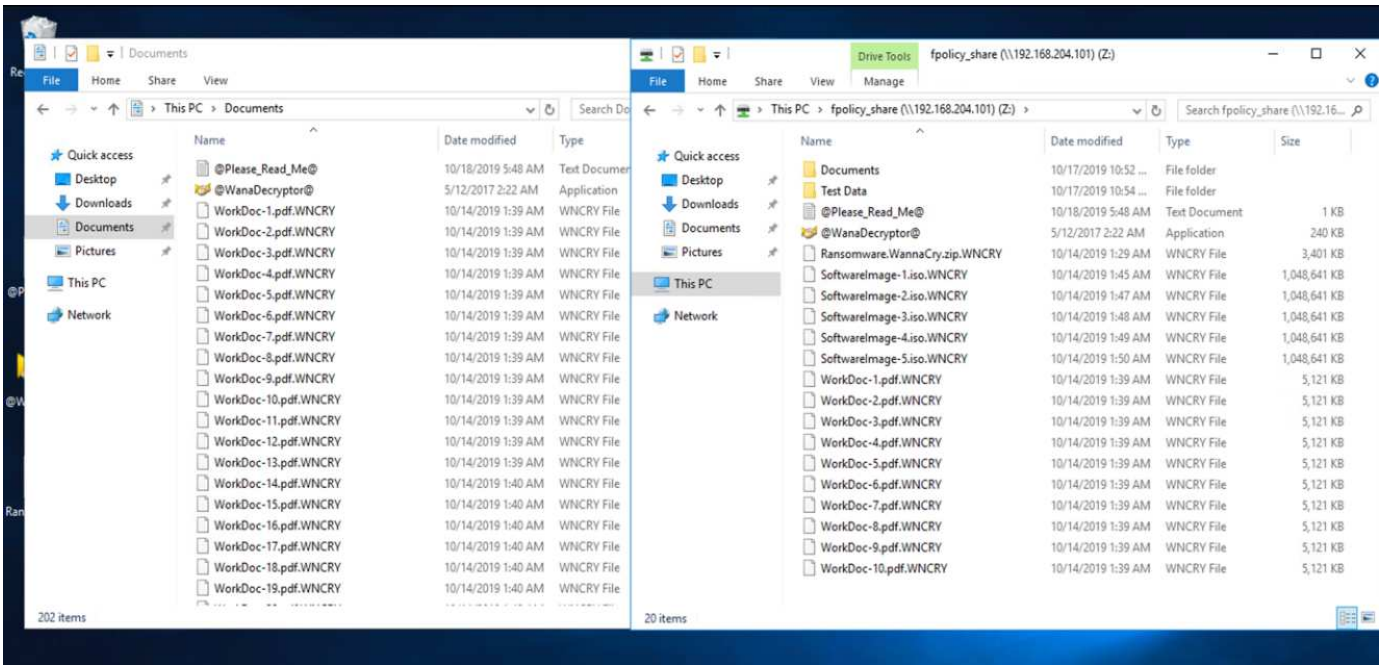
Caso 1: WannaCry cifra el sistema de archivos dentro del equipo virtual y el recurso compartido CIFS asignado

El sistema de archivos local y el recurso compartido CIFS asignado fueron cifrados por el malware WannaCry.

El malware comienza a cifrar archivos con extensiones WNCRY.



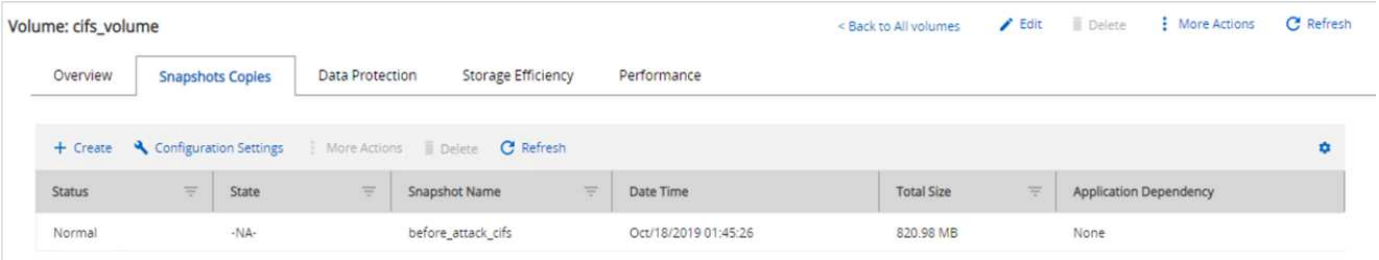
El malware cifra todos los archivos del equipo virtual local y del recurso compartido asignado.



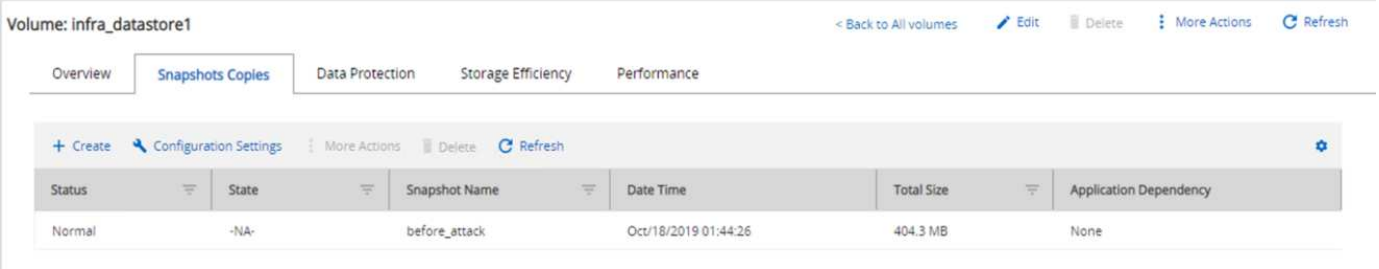
Detección

Desde el momento en que el malware comenzó a cifrar los archivos, se activó un aumento exponencial del tamaño de las copias snapshot y una reducción exponencial del porcentaje de eficiencia del almacenamiento.

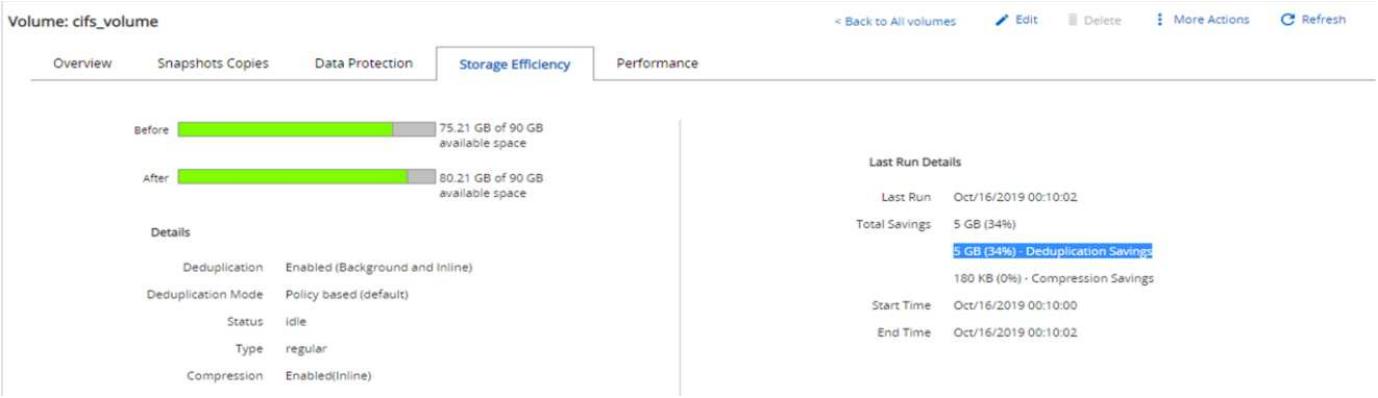
Se detectó un aumento espectacular del tamaño de snapshot a 820,98 MB para el volumen que aloja la unidad CIFS durante el ataque.



Hemos detectado un aumento en el tamaño de la copia snapshot a 404,3 MB para el volumen donde se aloja la máquina virtual.



La eficiencia de almacenamiento para el volumen que aloja la unidad CIFS se redujo a un 34 %.



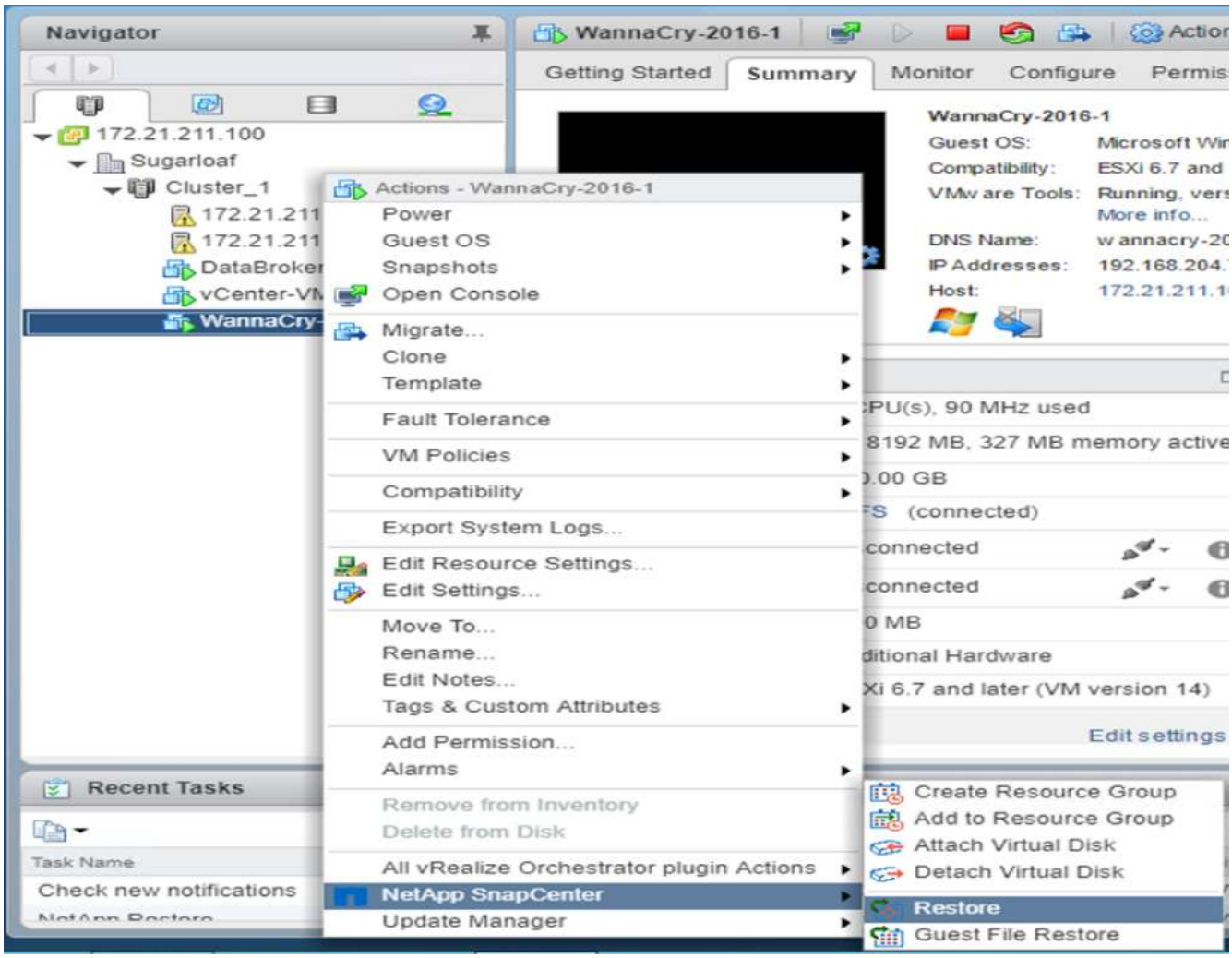
Reparación

Restaurar el equipo virtual y el recurso compartido CIFS asignado mediante una copia Snapshot limpia creada antes del ataque

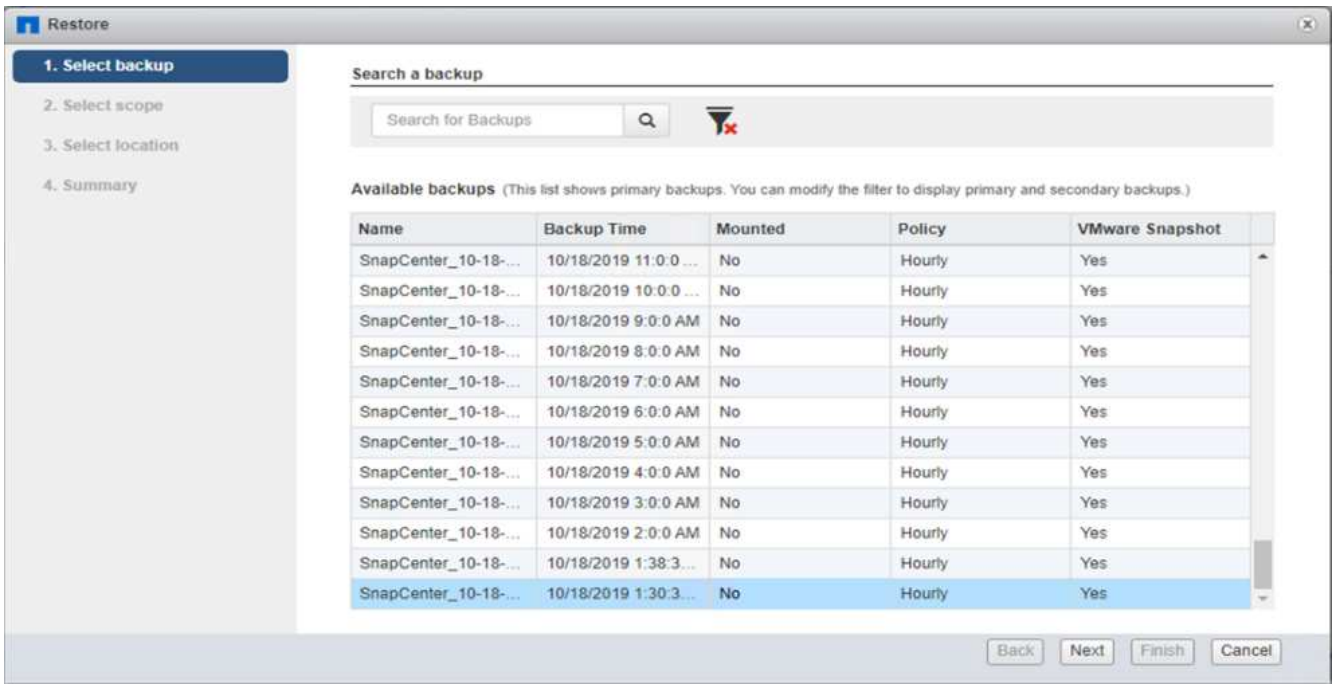
Restaurar VM

Para restaurar el equipo virtual, complete los siguientes pasos:

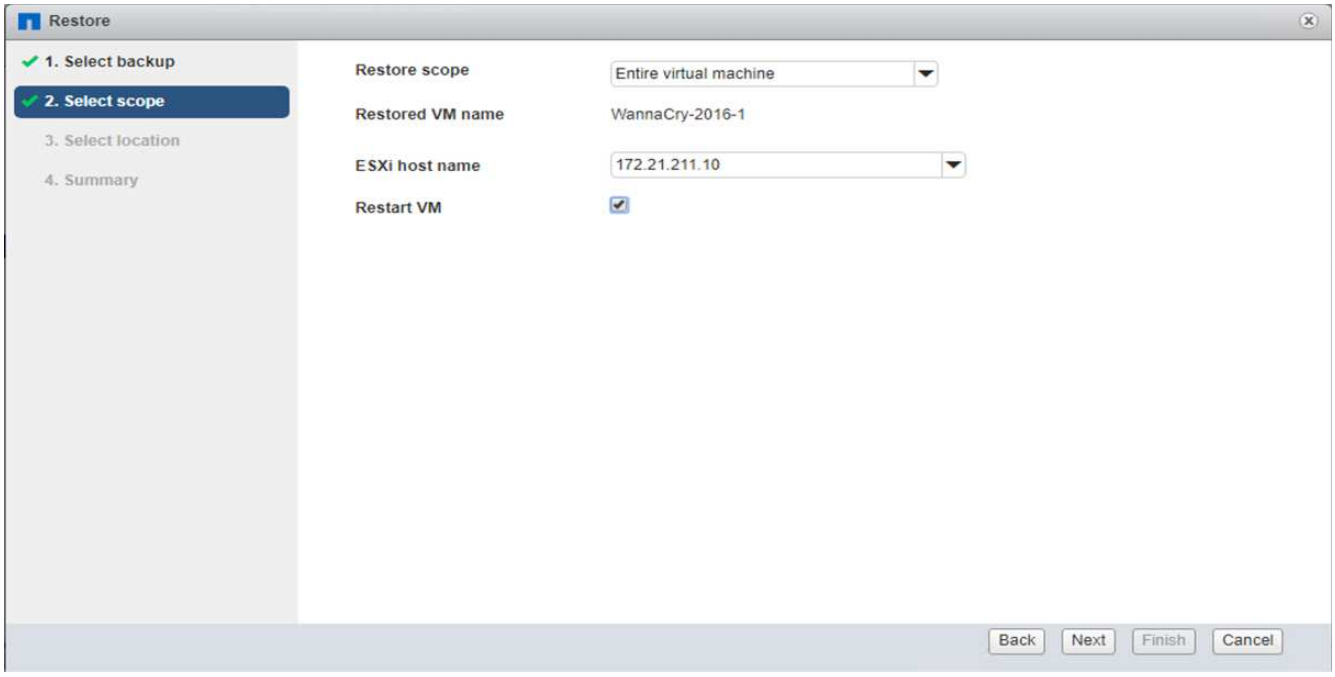
1. Use la copia Snapshot que creó con SnapCenter para restaurar la máquina virtual.



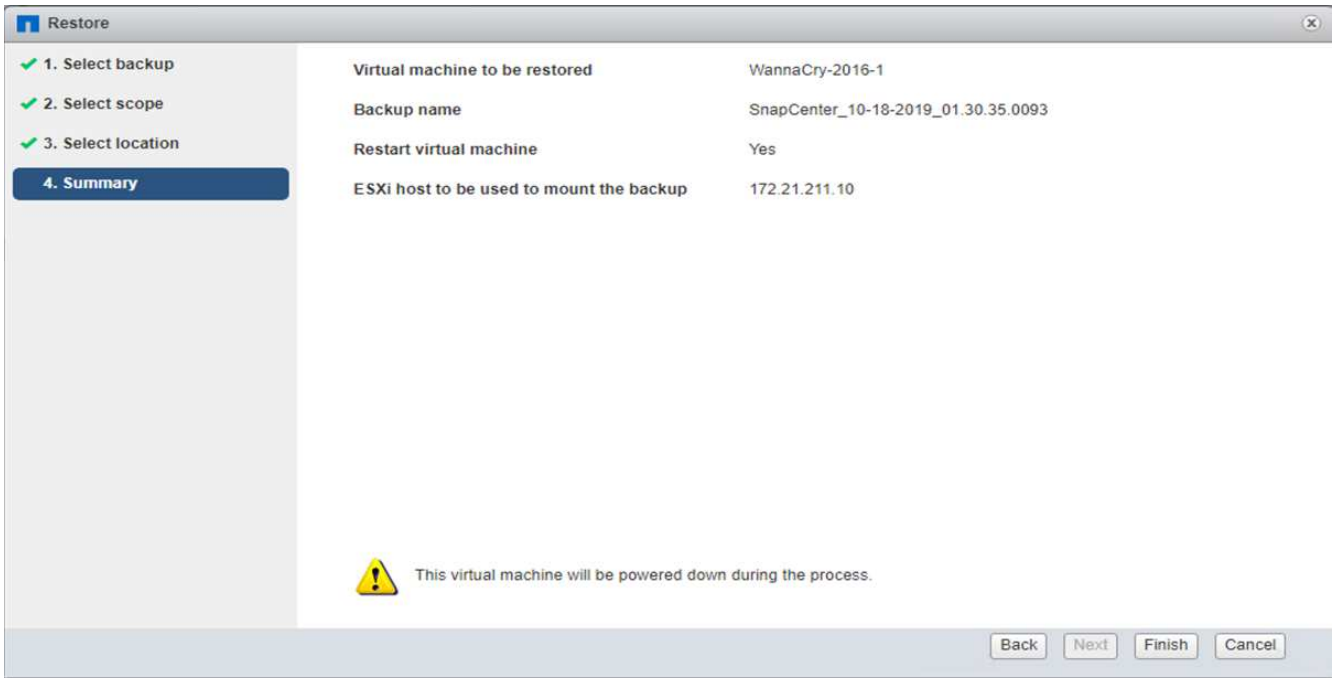
2. Seleccione la copia de Snapshot coherente con VMware que desee restaurar.



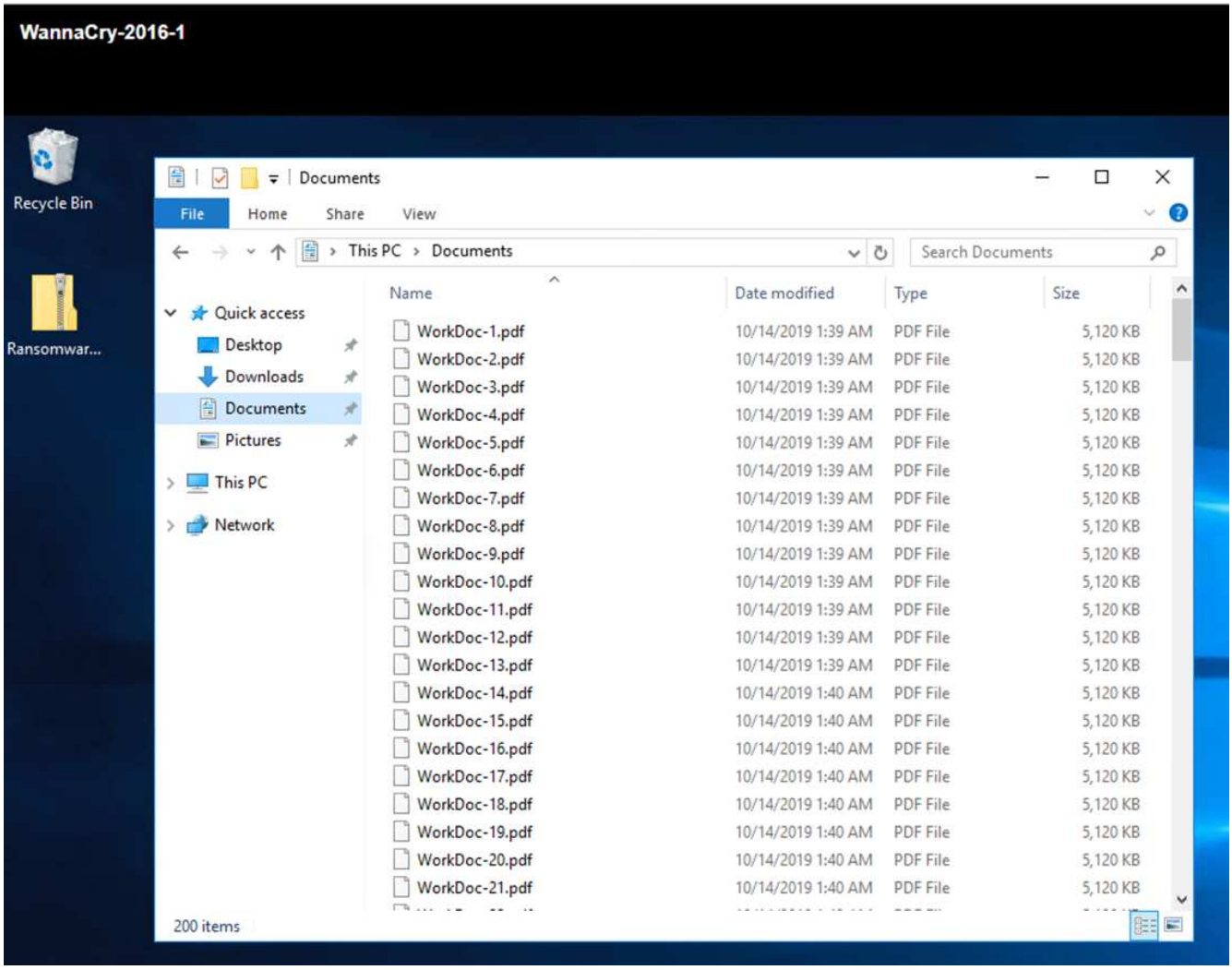
3. Toda la máquina virtual se restaura y se reinicia.



4. Haga clic en Finalizar para iniciar el proceso de restauración.



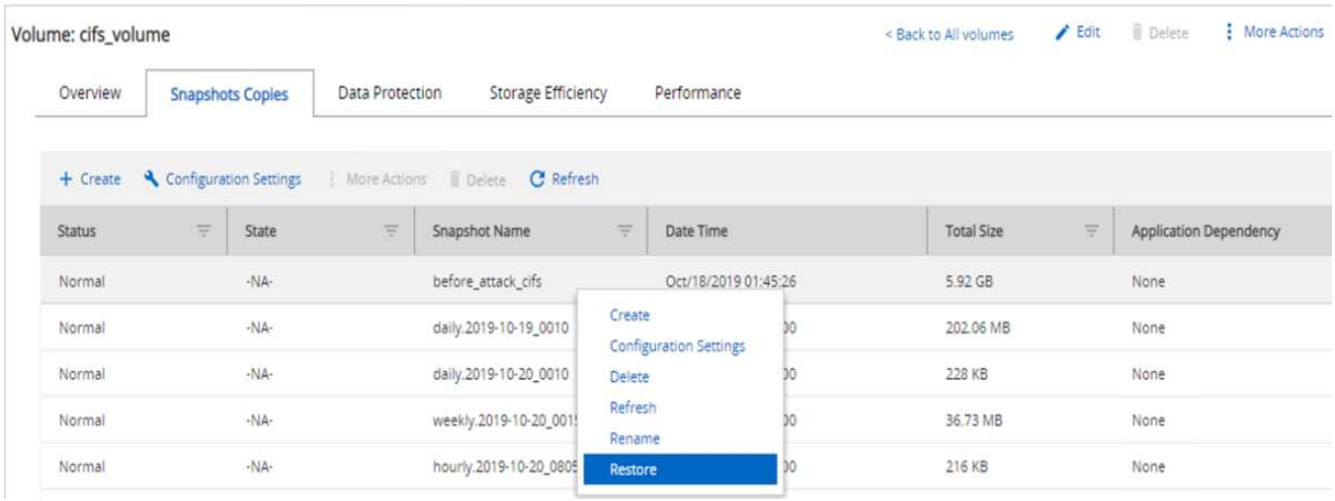
5. Se restauran el equipo virtual y sus archivos.



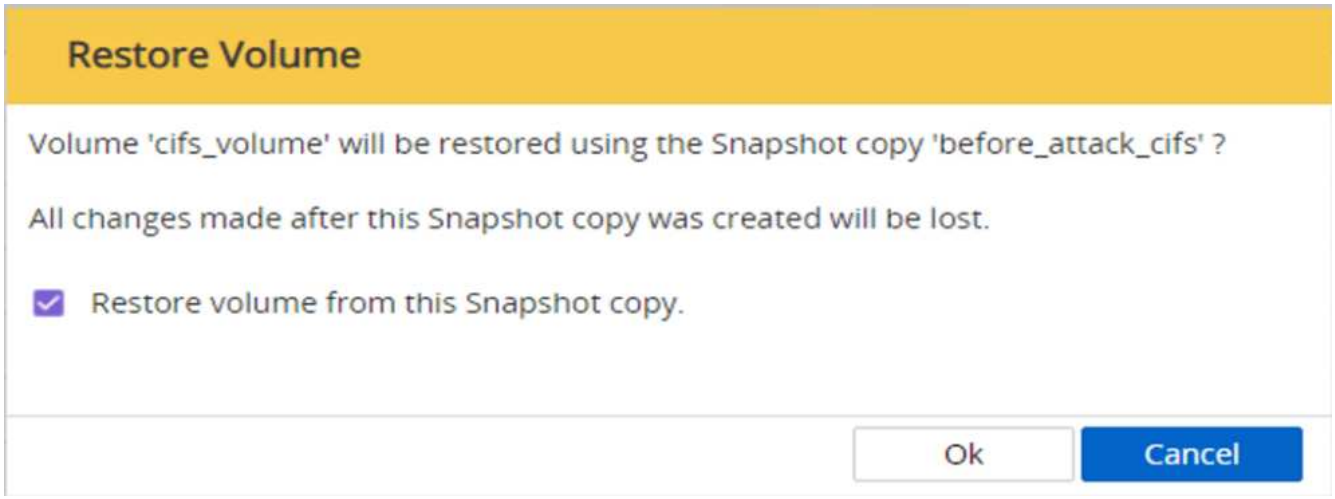
Restaurar recurso compartido CIFS

Para restaurar el recurso compartido CIFS, realice los siguientes pasos:

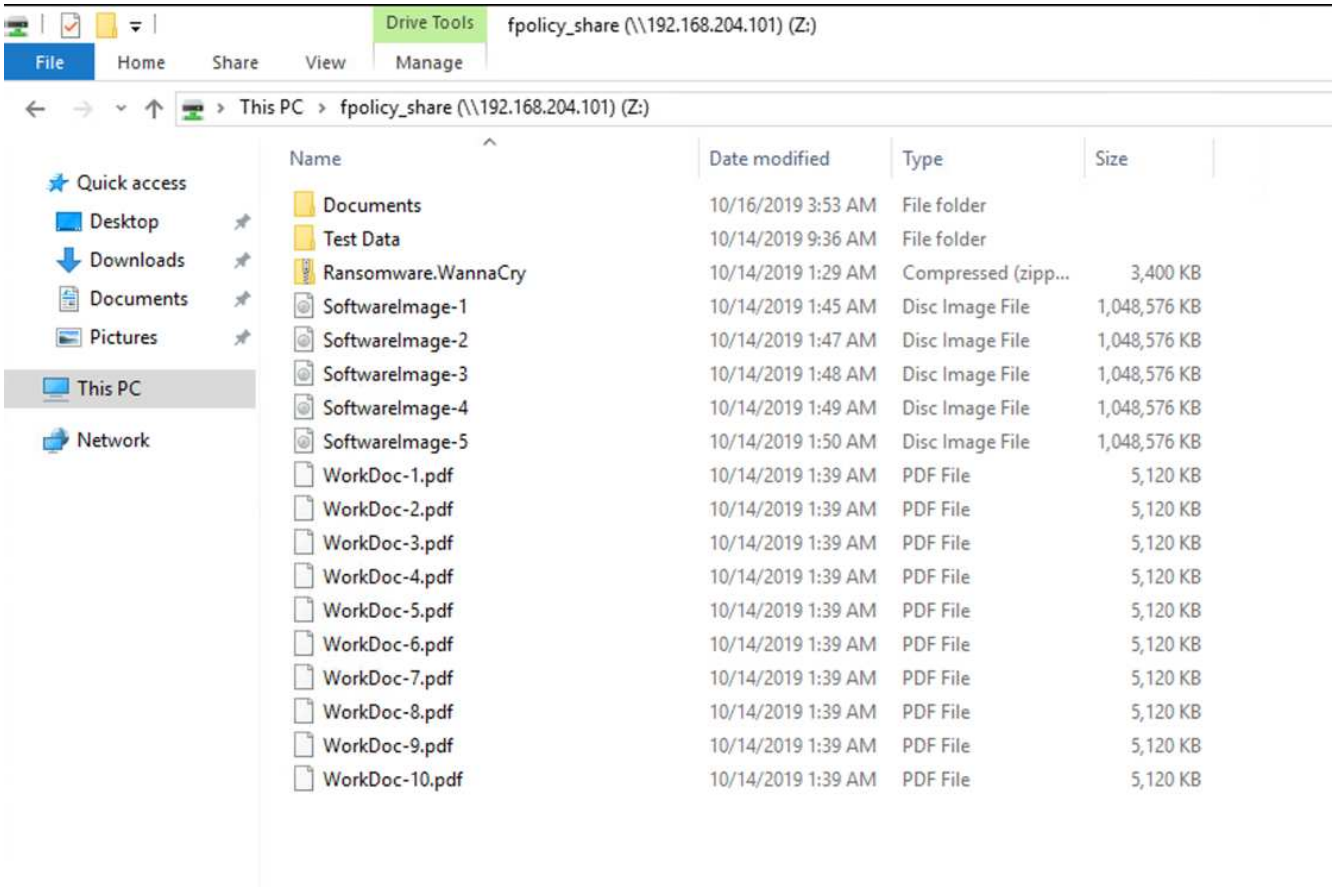
1. Utilice la copia snapshot del volumen que haya tomado antes del ataque para restaurar el recurso compartido.



2. Haga clic en OK para iniciar la operación de restauración.



3. Vea el recurso compartido CIFS después de la restauración.



Caso 2: WannaCry cifra el sistema de archivos dentro del equipo virtual e intenta cifrar el recurso compartido CIFS asignado que está protegido mediante FPolicy

Prevención

Configurar FPolicy

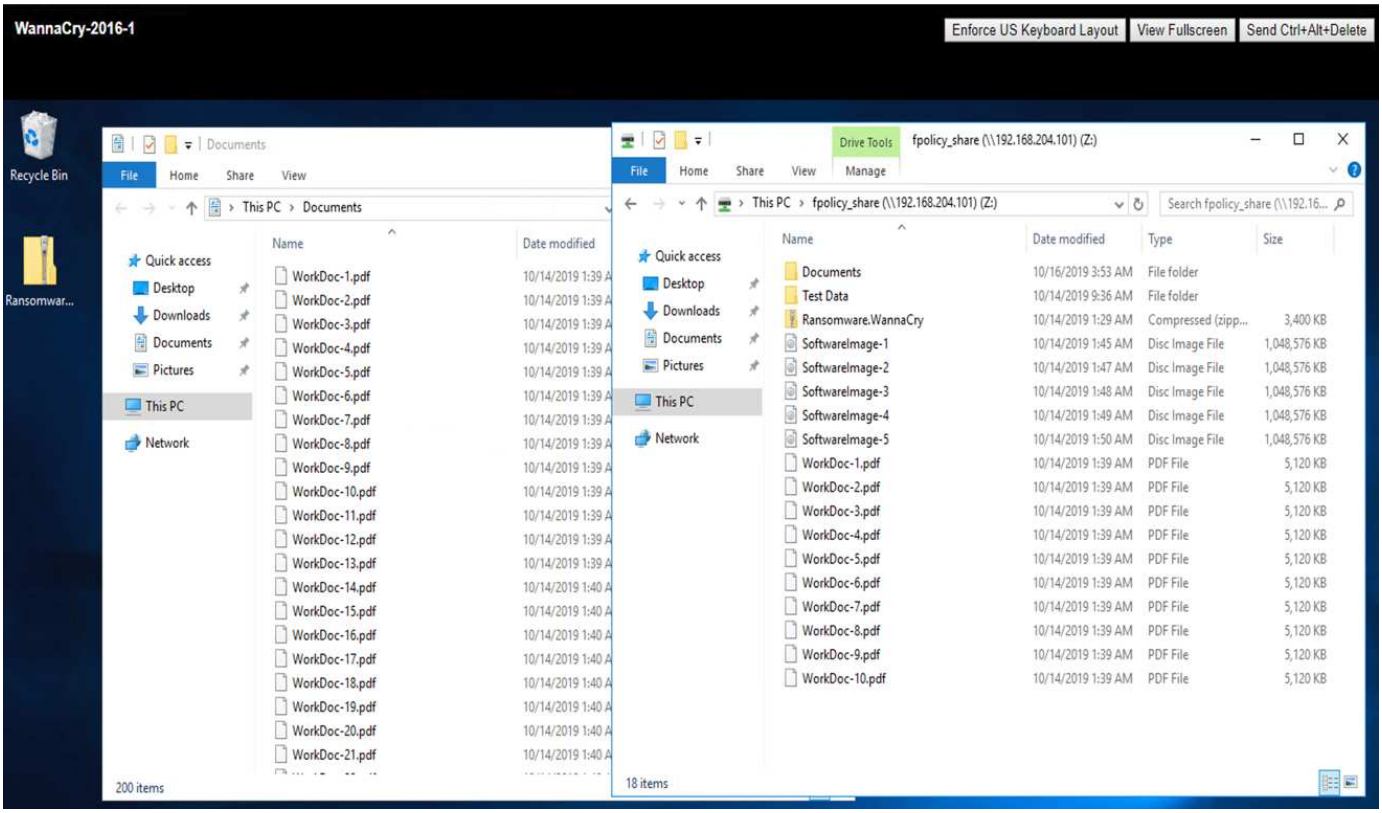
Para configurar FPolicy en el recurso compartido de CIFS, ejecute los siguientes comandos en el clúster de

ONTAP:

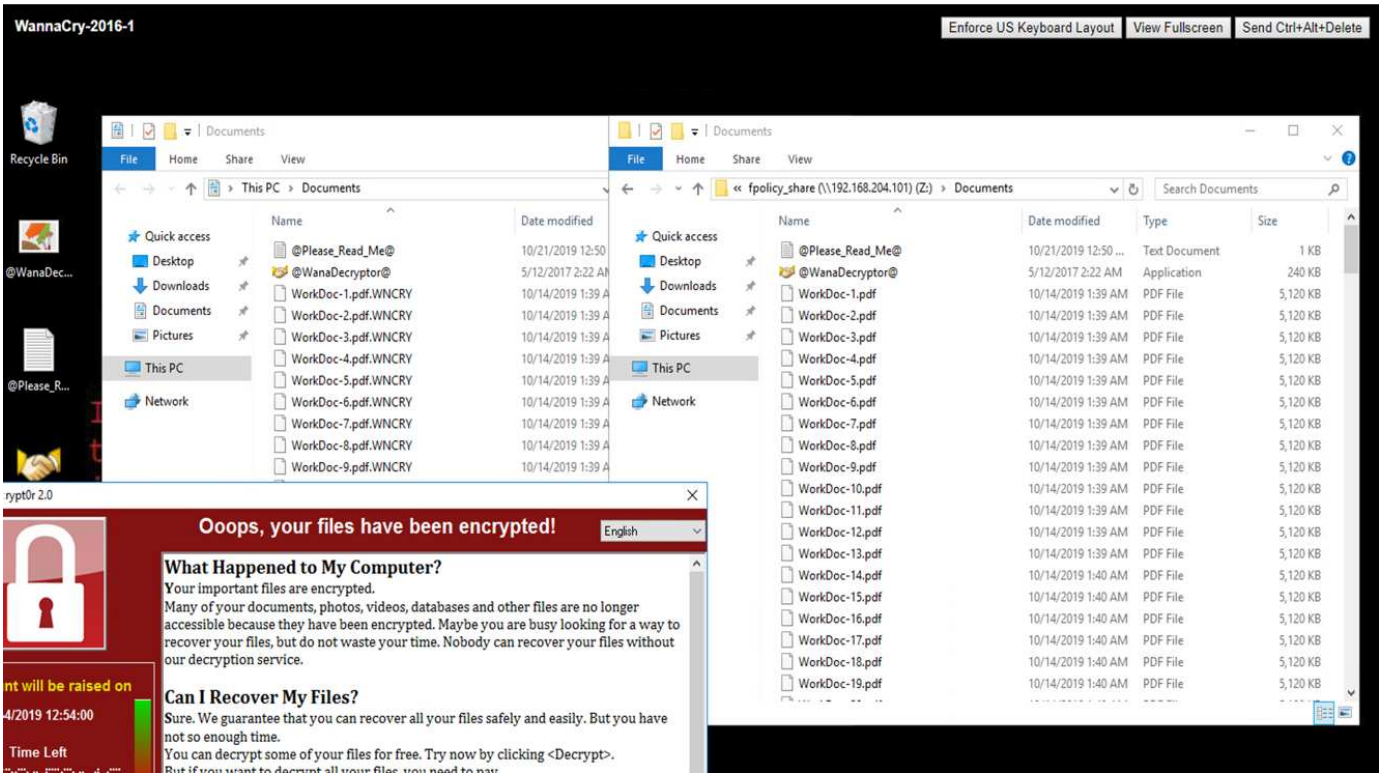
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create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

Con esta directiva, los archivos con extensiones WNCRY, Locky y ad4c no pueden realizar las operaciones de archivo crear, cambiar el nombre, escribir o abrir.

Ver el estado de los archivos antes del ataque: Están sin cifrar y en un sistema limpio.



Los archivos del equipo virtual están cifrados. El malware WannaCry intenta cifrar los archivos en el recurso compartido de CIFS, pero FPolicy evita que afecten a los archivos.



Continuar las operaciones de negocios sin pagar el rescate

Las funcionalidades de NetApp descritas en este documento le ayudan a restaurar los datos en cuestión de minutos después de un ataque y a evitar ataques en primer lugar, de tal modo que pueda continuar con sus operaciones empresariales sin impedimentos.

Es posible establecer una programación de copias Snapshot para cumplir el objetivo de punto de recuperación (RPO) deseado. Las operaciones de restauración basadas en copias de Snapshot son muy rápidas; por lo tanto, se puede lograr un objetivo de tiempo de recuperación (RTO) muy bajo.

Por encima de todo, usted no tiene que pagar cualquier rescate como resultado de un ataque, y usted puede rápidamente volver a las operaciones regulares.

Conclusión

El ransomware es un producto de la delincuencia organizada, y los atacantes no operan con la ética. Pueden abstenerse de proporcionar la clave para el descifrado incluso después de recibir el rescate. La víctima no solo pierde sus datos, sino también una cantidad importante de dinero, y se enfrenta a las consecuencias asociadas con la pérdida de datos de producción.

Según a "Artículo de Forbes", sólo el 19% de las víctimas de ransomware obtienen sus datos después de pagar el rescate. Por lo tanto, los autores recomiendan no pagar un rescate en caso de un ataque porque hacerlo refuerza la fe del atacante en su modelo de negocios.

Las operaciones de backup y restauración de datos juegan un papel importante de la recuperación de ransomware. Por lo tanto, deben incluirse como parte integral de la planificación empresarial. La implementación de estas operaciones se debe presupuestar para que no exista ningún compromiso en las funcionalidades de recuperación en caso de ataque.

La clave está en seleccionar el partner tecnológico correcto en este viaje. FlexPod proporciona la mayoría de las funcionalidades necesarias de forma nativa sin coste adicional en un sistema FAS all-flash.

Reconocimientos

El autor desea agradecer a las siguientes personas su apoyo en la creación de este documento:

- Jorge Gómez Navarrete, NetApp
- Ganesh Kamath, NetApp

Información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Software Snapshot de NetApp

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

- Gestión de backups de SnapCenter

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

- Cumplimiento de normativas para datos de SnapLock

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

- Documentación de productos de NetApp

  "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 StealtWatch

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

Solución FlexPod para el sector sanitario conforme a la seguridad FIPS 140-2-2

TR-4892: Solución FlexPod para el sector sanitario conforme a la seguridad FIPS 140-2-2

JayaKishore Esanakula, NetApp John McAbel, Cisco

La Ley de Tecnología de la Información sanitaria para la Salud Económica y Clínica (HITECH) requiere el cifrado validado de la Norma Federal de procesamiento de Información (FIPS) 140-2 de la Información médica protegida electrónica (ePHI). Las

aplicaciones y el software de tecnología de la información sanitaria (HIT) deben cumplir los requisitos de FIPS 140-2 para obtener la certificación del Programa de interoperabilidad de promoción (anteriormente, significativo programa de incentivos para uso). Los proveedores y hospitales elegibles deben usar UN GOLPE conforme a FIPS 140-2 (nivel 1) para recibir los incentivos de Medicare y Medicaid y para evitar las sanciones de reembolso del Centro para Medicare y Medicaid (CMS). Los algoritmos de cifrado certificados FIPS 140-2-2, cumplen los requisitos técnicos de protección "Regla de seguridad" De la Ley de Portabilidad y responsabilidad de la Información de Salud (HIPAA).

FIPS 140-2 es un territorio estadounidense estándar gubernamental que establece los requisitos de seguridad de los módulos criptográficos en hardware, software y firmware que protegen la información confidencial. El cumplimiento del estándar es obligatorio para su uso por parte de EE. UU también se utilizan a menudo en sectores regulados como los servicios financieros y la asistencia sanitaria. Este informe técnico ayuda al lector a comprender la norma de seguridad FIPS 140-2 de alto nivel. También ayuda a la audiencia a comprender las diversas amenazas a las que se enfrentan las organizaciones sanitarias. Por último, el informe técnico nos ayuda a comprender cómo puede ayudarle un sistema FlexPod conforme a FIPS 140-2 a proteger los activos sanitarios cuando se implementa en una infraestructura convergente de FlexPod.

Ámbito

Este documento es una descripción general técnica de un sistema Cisco Unified Computing System (Cisco UCS), Cisco Nexus, Cisco MDS y la infraestructura FlexPod basada en ONTAP de NetApp para alojar una o más aplicaciones o soluciones DE TI para el sector sanitario que requieren cumplimiento de normativas de seguridad FIPS 140-2-2.

Destinatarios

Este documento está dirigido a líderes técnicos del sector sanitario y a ingenieros de soluciones de partners de Cisco y NetApp y personal de servicios profesionales. NetApp asume que el lector tiene un buen conocimiento de los conceptos de configuración de la computación y el almacenamiento, así como una familiaridad técnica con las amenazas para la salud, la seguridad sanitaria, los sistemas TECNOLÓGICOS para el sector sanitario, Cisco UCS y los sistemas de almacenamiento de NetApp.

"Siguiente: Amenazas de ciberseguridad en sanidad."

Amenazas de ciberseguridad en sanidad

"Anterior: Introducción."

En cada uno de los problemas se presenta una nueva oportunidad, un ejemplo de esta oportunidad dado por la pandemia del COVID. Según a "informes" Por el Programa de ciberseguridad del Departamento de Salud y Servicios Humanos (HHS), la respuesta del COVID ha dado lugar a un mayor número de ataques de ransomware. Había 6,000 nuevos dominios de Internet registrados apenas en la tercera semana de marzo de 2020. Más del 50% de los dominios hospedados de malware. Los ataques de ransomware fueron responsables de casi el 50 % de todas las infracciones de datos en la atención sanitaria en 2020, lo que afectó a más de 630 organizaciones sanitarias y a aproximadamente 29 millones de registros sanitarios. Diecinueve leakers/sitios duplicaron la extorsión. Con un 24.5%, el sector sanitario registró el mayor número de

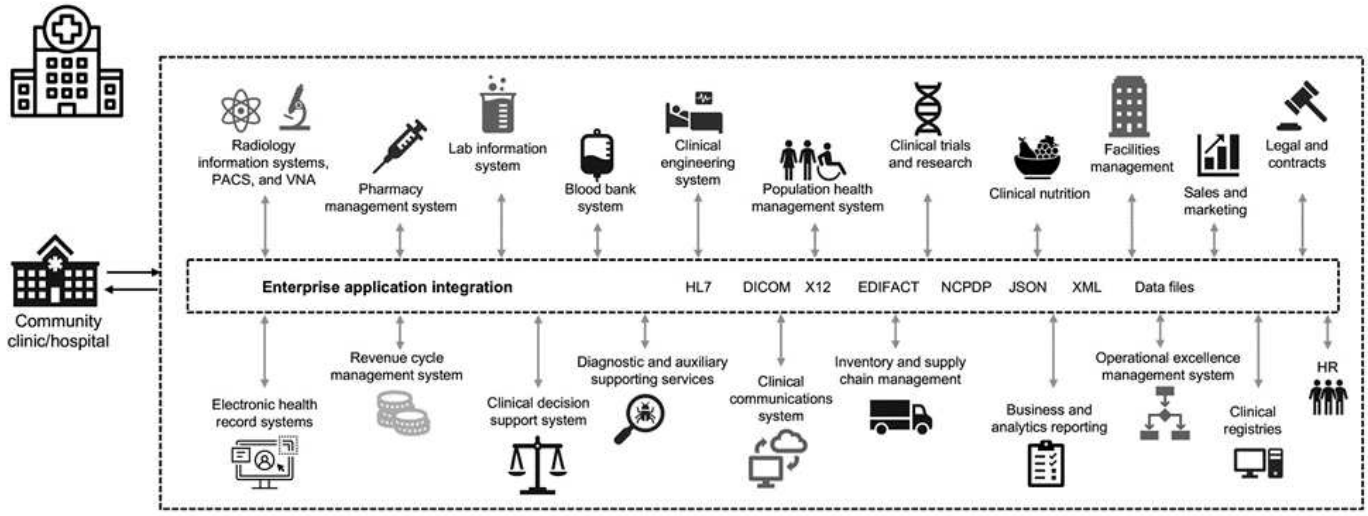
infracciones de datos en 2020.

Agentes malintencionados intentaron violar la seguridad y privacidad de la información médica protegida (PHI) vendiendo la información o amenazando con destruirla o exponerla. Con frecuencia se realizan intentos de difusión en masa y objetivo para obtener acceso no autorizado a ePHI. Aproximadamente el 75% de los registros de pacientes expuestos en el segundo semestre de 2020 se debieron a socios comerciales comprometidos.

La siguiente lista de organizaciones de atención médica fue dirigida por los agentes maliciosos:

- Los sistemas hospitalarios
- Laboratorios de ciencias de la vida
- Laboratorios de investigación
- Instalaciones de rehabilitación
- Hospitales y clínicas comunitarias

La diversidad de aplicaciones que constituyen una organización sanitaria es innegable y cada vez más compleja. Las oficinas de seguridad de la información se enfrentan al reto de proporcionar gobierno a la gran variedad de sistemas Y activos TECNOLÓGICOS. La figura siguiente muestra las capacidades clínicas de un sistema hospitalario típico.



Los datos del paciente se encuentran en el centro de esta imagen. La pérdida de datos de pacientes y el estigma asociado con condiciones médicas sensibles es muy real. Otras cuestiones sensibles incluyen el riesgo de exclusión social, chantaje, perfilado, vulnerabilidad a la comercialización dirigida, explotación y posible responsabilidad financiera hacia los pagadores sobre la información médica más allá de los privilegios del pagador.

Las amenazas a la salud son multidimensionales en la naturaleza y en el impacto. Los gobiernos de todo el mundo han promulgado diversas disposiciones para asegurar la ePHI. Los efectos perjudiciales y la naturaleza en evolución de las amenazas a la atención sanitaria hacen que a las organizaciones sanitarias les resulte difícil defender todas las amenazas.

A continuación se presenta una lista de amenazas comunes identificadas en la atención sanitaria:

- Ataques de ransomware
- Pérdida o robo de equipo o datos con información confidencial

- Ataques de phishing
- Ataques contra dispositivos médicos conectados que pueden afectar la seguridad del paciente
- Ataques de phishing por correo electrónico
- Pérdida o robo de equipo o datos
- Protocolo de puesto de trabajo remoto sacrifica
- Vulnerabilidad del software

Las organizaciones sanitarias trabajan en un entorno legal y regulatorio que es tan complicado como sus ecosistemas digitales. Este entorno incluye, entre otros, lo siguiente:

- Oficina del Coordinador Nacional (para Tecnología sanitaria) normas de interoperabilidad de Tecnología Electrónica de la Información de Salud con certificación ONC
- Acceso a Medicare y Ley de reautorización del Programa de Seguro médico para niños (MACRA)/uso significativo
- Múltiples obligaciones bajo la Administración de Alimentos y medicamentos (FDA)
- Los procesos de acreditación de la Comisión conjunta
- Requisitos de HIPAA
- Requisitos DE HITECH
- Normas de riesgo mínimas aceptables para los pagadores
- Normas de privacidad y seguridad del Estado
- Requisitos de la Ley Federal de modernización de la Seguridad de la Información tal como están incorporados a contratos federales y subvenciones de investigación a través de agencias como los Institutos nacionales de la Salud
- Estándar de seguridad de datos del sector de tarjetas de pago (PCI-DSS)
- Requisitos de la Administración de Servicios de abuso de sustancias y Salud Mental (SAMHSA)
- La ley Gramm-Leach-Bliley relativa al procesamiento financiero
- La Ley Stark en su relación con la prestación de servicios a organizaciones afiliadas
- Ley de Derechos educativos y Privacidad de la Familia (FERPA) para instituciones que participan en la educación superior
- Información genética Ley de no discriminación (GINA)
- El nuevo Reglamento general de protección de datos (GDPR) en la Unión Europea

Los estándares de la arquitectura de seguridad están evolucionando rápidamente para impedir que los actores malintencionados afecten a los sistemas de información sanitaria. Uno de estos estándares es FIPS 140-2, definido por el Instituto Nacional de estándares y Tecnología (NIST). La publicación FIPS 140-2 detalla el territorio de EE. UU requisitos gubernamentales de un módulo criptográfico. Los requisitos de seguridad cubren las áreas relacionadas con un diseño seguro y la implementación de un módulo criptográfico y se pueden aplicar para GOLPEAR. Los límites criptográficos bien definidos permiten una gestión de la seguridad más sencilla al tiempo que se mantienen al día con los módulos criptográficos. Estos límites ayudan a prevenir módulos criptográfico débiles que pueden ser explotados fácilmente por actores malintencionados. También pueden ayudar a prevenir errores humanos al gestionar módulos criptográficos estándar.

NIST junto con el establecimiento de seguridad de comunicaciones (CSE) han establecido el programa de validación de módulos criptográficos (CMVP) para certificar módulos criptográficos para niveles de validación FIPS 140-2-2. Mediante el uso de un módulo certificado FIPS 140-2-2, las organizaciones federales deben

proteger tanto los datos confidenciales como los valiosos mientras están en movimiento. Debido a su éxito en la protección de información sensible o valiosa, muchos sistemas de atención médica han decidido cifrar la ePHI mediante el uso de módulos criptográficos FIPS 140-2 más allá del nivel mínimo de seguridad legalmente requerido.

El aprovechamiento e implementación de las funcionalidades de FIPS 140-2 de FlexPod solo lleva horas (no días). Cumplir con FIPS está al alcance de la mayoría de las organizaciones sanitarias, independientemente del tamaño. Con límites criptográficos claramente definidos y pasos de implementación sencillos y bien documentados, una arquitectura de FlexPod conforme a FIPS 140-2 puede establecer una base de seguridad sólida para la infraestructura y permitir mejoras sencillas que incrementen aún más la protección frente a amenazas de seguridad.

"Siguiente: Descripción general de FIPS 140-2."

Información general de FIPS 140-2

"Anterior: Amenazas de ciberseguridad en sanidad."

"FIPS 140-2" especifica los requisitos de seguridad de un módulo criptográfico utilizado en un sistema de seguridad que protege la información confidencial en los sistemas informáticos y de telecomunicaciones. Un módulo criptográfico debe ser un conjunto de hardware, software, firmware o una combinación. FIPS se aplica a los algoritmos criptográficos, la generación de claves y los gestores de claves contenidos en un ámbito criptográfico. Es importante entender que FIPS 140-2 se aplica específicamente al módulo criptográfico, no al producto, la arquitectura, los datos o el ecosistema. El módulo criptográfico, que se define en los términos clave más adelante en este documento, es el componente específico (ya sea hardware, software o firmware) que implementa funciones de seguridad aprobadas. Además, FIPS 140-2 especifica cuatro niveles. Los algoritmos criptográficos aprobados son comunes a todos los niveles. Algunos de los elementos clave y requisitos de cada nivel de seguridad son:

- **Nivel de seguridad 1**
  - Especifica los requisitos básicos de seguridad de un módulo criptográfico (se requiere al menos un algoritmo aprobado o una función de seguridad).
  - No se requieren mecanismos de seguridad física especificados para el nivel 1 más allá de los requisitos básicos para los componentes de nivel de producción.
- **Nivel de seguridad 2**
  - Mejora los mecanismos de seguridad física al añadir el requisito de prueba de manipulación mediante el uso de soluciones a prueba de manipulación como revestimientos o sellos, bloqueos de cubiertas extraíbles o puertas de los módulos criptográficos.
  - Requiere, como mínimo, el control de acceso basado en funciones (RBAC) en el que el módulo criptográfico autentica la autorización de un operador o administrador para asumir una función específica y realizar un conjunto de funciones correspondiente.
- **Nivel de seguridad 3**
  - Se basa en los requisitos de seguridad a prueba de manipulaciones del nivel 2 e intenta evitar un mayor acceso a los parámetros de seguridad críticos (CSP) del módulo criptográfico.
  - Los mecanismos de seguridad física necesarios en el nivel 3 tienen la intención de tener una alta probabilidad de detectar y responder a los intentos de acceso físico, o cualquier uso o modificación del

módulo criptográfico. Los ejemplos pueden incluir carcasas fuertes, detección de manipulación y circuitos de respuesta que se ceros a todos los CSPs de texto sin formato cuando se abre una cubierta extraíble en el módulo criptográfico.

  - Requiere mecanismos de autenticación basados en identidades para mejorar la seguridad de los mecanismos RBAC especificados en el nivel 2. Un módulo criptográfico autentica la identidad de un operador y verifica que el operador está autorizado a utilizar una función y realizar las funciones de la función.

- **Nivel de seguridad 4**
  - El nivel más alto de seguridad en FIPS 140-2.
  - El nivel más útil para operaciones en entornos físicamente sin protección.
  - En este nivel, los mecanismos de seguridad física tienen por objeto proporcionar una protección completa alrededor del módulo criptográfico, con la responsabilidad de detectar y responder a cualquier intento no autorizado de acceso físico.
  - La penetración o exposición del módulo criptográfico debe tener una alta probabilidad de detección y dar como resultado la zeroización inmediata de todos los CSPs no seguros o de texto sin formato.

"Siguiente: Plano de control frente al plano de datos."

Plano de control frente al plano de datos

"Anterior: Descripción general de FIPS 140-2."

Al implementar una estrategia FIPS 140-2-2, es importante comprender qué se está protegiendo. Esto se puede dividir fácilmente en dos áreas: Plano de control y plano de datos. Un plano de control se refiere a los aspectos que afectan al control y al funcionamiento de los componentes del sistema FlexPod; por ejemplo, acceso administrativo a las controladoras de almacenamiento de NetApp, los switches Cisco Nexus y los servidores Cisco UCS. La protección en esta capa se proporciona limitando los protocolos y los cyphers criptográficos que los administradores pueden utilizar para conectar a dispositivos y realizar cambios. Un plano de datos hace referencia a la información real, como la PHI, dentro del sistema FlexPod. Esto se protege mediante el cifrado de datos en reposo y de nuevo en FIPS, lo que garantiza que los módulos criptográficos en uso cumplen los estándares.

"Siguiente: Computación Cisco UCS de FlexPod y FIPS 140-2."

Computación Cisco UCS de FlexPod y FIPS 140-2

"Anterior: Plano de control frente al plano de datos."

La arquitectura de FlexPod se puede diseñar con un servidor Cisco UCS compatible con FIPS 140-2-2. De acuerdo con la U. S. El servidor Cisco UCS puede funcionar en modo de cumplimiento de normativas FIPS 140-2 nivel 1. Si desea obtener una lista completa de los componentes de Cisco conformes con FIPS, consulte "Página FIPS 140 de Cisco". Cisco UCS Manager está validado según FIPS 140-2.

Cisco UCS y Fabric Interconnect

Cisco UCS Manager se pone en marcha y se ejecuta desde las interconexiones de estructura de Cisco (FIS).

Para obtener más información sobre Cisco UCS y cómo habilitar FIPS, consulte "Documentación de Cisco UCS Manager".

Para habilitar el modo FIPS en la interconexión de estructura Cisco en cada estructura A y B, ejecute los siguientes comandos:

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

> Para sustituir UNA FI de un clúster en Cisco UCS Manager versión 3.2(3) por UNA FI en una versión anterior a Cisco UCS Manager versión 3.2(3), deshabilite el modo FIPS (disable `fips-mode`) En LA RED EXISTENTE antes de agregar LA RED FI de repuesto al clúster. Después de formar el clúster, como parte del arranque de Cisco UCS Manager, se habilita el modo FIPS automáticamente.

Cisco ofrece los siguientes productos clave que se pueden implementar en la capa informática o de aplicación:

- **Cisco Advanced Malware Protection (AMP) para endpoints.** compatible con los sistemas operativos Microsoft Windows y Linux, esta solución integra capacidades de prevención, detección y respuesta. Este software de seguridad evita infracciones, bloquea el malware en el punto de entrada y supervisa y analiza continuamente la actividad de los archivos y procesos para detectar, contener y resolver rápidamente amenazas que puedan evadir las defensas de primera línea. El componente de Protección de actividad maliciosa (MAP) de AMP supervisa continuamente todas las actividades de los extremos y proporciona detección en tiempo de ejecución y bloqueo del comportamiento anormal de un programa en ejecución en el punto final. Por ejemplo, cuando el comportamiento del punto final indica ransomware, los procesos ofensor se terminan, lo que impide el cifrado del punto final y detiene el ataque.
- **AMP para seguridad de correo electrónico.** los correos electrónicos se han convertido en el vehículo principal para difundir malware y llevar a cabo ciberataques. En promedio, aproximadamente 100 mil millones de correos electrónicos se intercambian en un solo día, lo que proporciona a los atacantes un excelente vector de penetración en los sistemas de los usuarios. Por lo tanto, es absolutamente esencial defender contra esta línea de ataque. AMP analiza correos electrónicos para amenazas tales como exploits de día cero y malware sigiloso ocultos en archivos adjuntos maliciosos. También utiliza la inteligencia de URL líder en el sector para combatir enlaces maliciosos. Proporciona a los usuarios protección avanzada contra el phishing espear, el ransomware y otros ataques sofisticados.
- **Sistema de prevención de intrusiones de próxima generación (NGIPS).** Cisco Firepower NGIPS se puede implementar como un dispositivo físico en el centro de datos o como un dispositivo virtual en VMware (NGIPSv para VMware). Este sistema altamente eficaz de prevención de intrusiones proporciona un rendimiento fiable y un costo total de propiedad bajo. La protección contra amenazas se puede ampliar con licencias de suscripción opcionales para proporcionar funciones de AMP, visibilidad y control de aplicaciones y filtrado de URL. La virtualización de NGIPS inspecciona el tráfico entre equipos virtuales (VM) y facilita la implementación y gestión de soluciones de NGIPS en sitios con recursos limitados, lo que aumenta la protección tanto para activos físicos como virtuales.

"Siguiente: Redes Cisco de FlexPod y FIPS 140-2."

Redes Cisco de FlexPod y FIPS 140-2

"Anterior: Computación Cisco UCS de FlexPod y FIPS 140-2."

MDS de Cisco

Plataforma Cisco MDS 9000 con software 8.4.x. "Conforme a FIPS 140-2-2". Cisco MDS implementa módulos criptográficos y los siguientes servicios para SNMPv3 y SSH.

- Establecimiento de sesiones en apoyo de cada servicio
- Todos los algoritmos criptográficos subyacentes admiten las funciones de derivación de cada clave de servicios
- Hash para cada servicio
- Cifrado simétrico para cada servicio

Antes de activar el modo FIPS, complete las siguientes tareas en el conmutador MDS:

1. Convierta las contraseñas en un mínimo de ocho caracteres.
2. Desactivar Telnet. Los usuarios deben iniciar sesión solo con SSH.
3. Desactive la autenticación remota mediante RADIUS/TACACS+. Sólo se pueden autenticar los usuarios locales del conmutador.
4. Deshabilite SNMP v1 y v2. Cualquier cuenta de usuario existente en el conmutador que se haya configurado para SNMPv3 debe configurarse sólo con SHA para autenticación y AES/3DES para privacidad.
5. Desactive VRRP.
6. Elimine todas las directivas IKE que tengan MD5 para autenticación o DES para cifrado. Modifique las directivas para que utilicen SHA para la autenticación y 3DES/AES para el cifrado.
7. Elimine todos los teclados RSA1 del servidor SSH.

Para activar el modo FIPS y mostrar el estado FIPS en el conmutador MDS, lleve a cabo los pasos siguientes:

1. Muestra el estado de FIPS.

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

2. Configure la clave SSH de 2048 bits.

```
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. Habilite el modo FIPS.

```
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. Muestra el estado de FIPS.

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

5. Guarde la configuración en la configuración en ejecución.

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

6. Reinicie el conmutador MDS

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

7. Muestra el estado de FIPS.

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

Para obtener más información, consulte "Habilitar el modo FIPS".

Cisco Nexus

Los switches de la serie Cisco Nexus 9000 (versión 9.3) son "Conforme a FIPS 140-2-2". Cisco Nexus implementa módulos criptográficos y los siguientes servicios para SNMPv3 y SSH.

- Establecimiento de sesiones en apoyo de cada servicio
- Todos los algoritmos criptográficos subyacentes admiten las funciones de derivación de cada clave de servicios
- Hash para cada servicio
- Cifrado simétrico para cada servicio

Antes de habilitar el modo FIPS, complete las siguientes tareas en el switch Cisco Nexus:

1. Desactivar Telnet. Los usuarios deben iniciar sesión solo con Secure Shell (SSH).
2. Desactive SNMPv1 y v2. Cualquier cuenta de usuario existente en el dispositivo que se haya configurado para SNMPv3 debe configurarse sólo con SHA para autenticación y AES/3DES para privacidad.
3. Elimine todos los pares de claves RSA1 del servidor SSH.
4. Habilite la comprobación de integridad de mensajes (MIC) HMAC-SHA1 para que se utilice durante la negociación del protocolo de asociación de seguridad (SAP) de Cisco TrustSec. Para ello, introduzca el algoritmo hash de SAP `HMAC-SHA-1` desde el `cts-manual` o. `cts-dot1x` modo.

Para activar el modo FIPS en el switch Nexus, realice los pasos siguientes:

1. Configure una clave SSH de 2048 bits.

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

2. Configure la clave SSH de 2048 bits.

```
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. Habilite el modo FIPS.

```
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. Reinicie el switch Nexus.

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

5. Muestra el estado de FIPS.

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

Además, el software Cisco NX OS admite la función NetFlow que permite una detección mejorada de anomalías y seguridad de la red. NetFlow captura los metadatos de cada conversación de la red, las partes implicadas en la comunicación, el protocolo utilizado y la duración de la transacción. Una vez agregada y analizado la información, puede proporcionar una visión del comportamiento normal. Los datos recopilados también permiten la identificación de patrones de actividad cuestionables, como el malware que se propaga a través de la red, lo que de otra manera puede pasar desapercibida. NetFlow utiliza flujos para proporcionar estadísticas para la supervisión de la red. Un flujo es un flujo unidireccional de paquetes que llega a una interfaz de origen (o VLAN) y tiene los mismos valores para las claves. Una clave es un valor identificado para un campo dentro del paquete. Puede crear un flujo utilizando un registro de flujo para definir las claves únicas para su flujo. Puede exportar los datos que NetFlow recopila para sus flujos utilizando un exportador de flujo a un colector NetFlow remoto, como Cisco StealtWatch. StealtWatch utiliza esta información para la supervisión continua de la red y proporciona información forense de respuesta a incidentes y detección de amenazas en tiempo real si se produce un brote de ransomware.

"Siguiente: Almacenamiento ONTAP de FlexPod y FIPS 140-2."

Almacenamiento ONTAP de FlexPod y FIPS 140-2

"Anterior: Redes Cisco de FlexPod y FIPS 140-2."

NetApp ofrece una amplia gama de hardware, software y servicios que pueden incluir varios componentes de los módulos criptográficos validados bajo el estándar. Por lo tanto, NetApp utiliza diferentes enfoques para el cumplimiento de normativas FIPS 140-2 para el plano de control y el plano de datos:

- NetApp incluye módulos criptográficos que han logrado una validación de nivel 1 para cifrado de datos en tránsito y de datos en reposo.
- NetApp adquiere módulos de hardware y software que han sido validados por FIPS 140-2-2 por los proveedores de dichos componentes. Por ejemplo, la solución de cifrado del almacenamiento de NetApp aprovecha las unidades validadas con el nivel 2 de FIPS.
- Los productos de NetApp pueden utilizar un módulo validado de manera que se cumpla con la norma aunque el producto o la función no estén dentro del límite de la validación. Por ejemplo, el cifrado de volúmenes de NetApp (NVE) cumple con FIPS 140-2-2. Aunque no se valida por separado, aprovecha el módulo criptográfico de NetApp, que se valida en el nivel 1. Para comprender cuáles son las características específicas del cumplimiento de su versión de ONTAP, póngase en contacto con su SME de FlexPod.

Los módulos criptográficos de NetApp están validados con FIPS 140-2 nivel 1

- El módulo de seguridad criptográfica de NetApp (NCSM) tiene la validación FIPS 140-2 nivel 1.

Las unidades de autocifrado de NetApp cuentan con la validación FIPS 140-2 nivel 2

NetApp adquiere unidades de autocifrado (SED) 140-2 que han sido validadas por el fabricante del equipo original (OEM); los clientes que buscan estas unidades deben especificarlas al realizar el pedido. Las unidades se validan en el nivel 2. Los siguientes productos de NetApp pueden aprovechar SED validados:

- Sistemas de almacenamiento A-Series y FAS de AFF
- Sistemas de almacenamiento E-Series y EF-Series

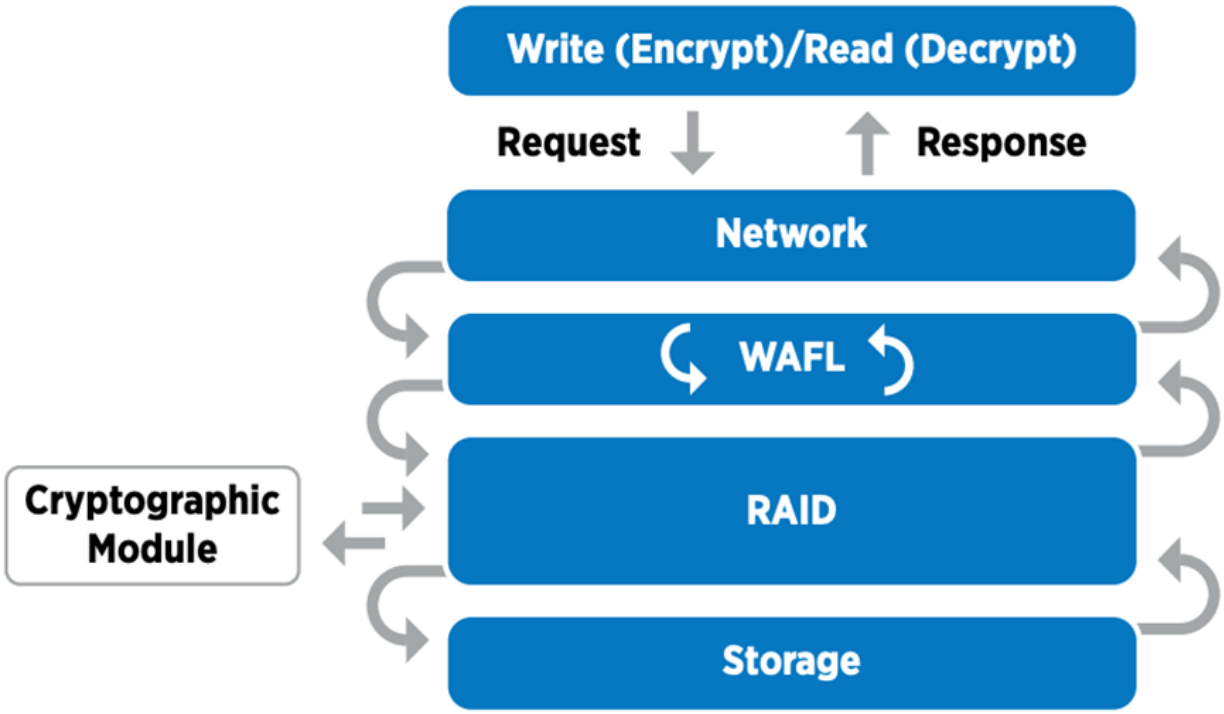
Cifrado de agregados de NetApp y cifrado de volúmenes de NetApp

Las tecnologías NVE y NetApp Aggregate Encryption (NAE) permiten el cifrado de datos a nivel de volumen y agregado respectivamente, lo que convierte la solución en independiente de la unidad física.

NVE es una solución de cifrado de datos en reposo basada en software disponible a partir de ONTAP 9.1. Desde ONTAP 9.2 es compatible con FIPS 140-2-2. NVE permite a ONTAP cifrar los datos por cada volumen para obtener granularidad. NAE, disponible con ONTAP 9.6, es una consecuencia del crecimiento de NVE; permite a ONTAP cifrar datos en cada volumen y los volúmenes pueden compartir claves en el agregado. Tanto NVE como NAE utilizan el cifrado AES de 256 bits. Los datos también se pueden almacenar en disco sin SED. NVE y NAE le permiten utilizar las funciones de eficiencia del almacenamiento incluso cuando el cifrado está habilitado. Un cifrado de solo capa de aplicaciones vence a todas las ventajas de la eficiencia del almacenamiento. Con NVE y NAE se mantienen las eficiencias del almacenamiento porque los datos entran desde la red a través de WAFL de NetApp hasta la capa RAID, que determina si los datos deben ser cifrados. Con el fin de mejorar la eficiencia del almacenamiento, puede utilizar la deduplicación de agregados con NAE. Los volúmenes NVE y NAE pueden coexistir en el mismo agregado NAE. Los agregados NAE no admiten volúmenes no cifrados.

Aquí está cómo funciona el proceso: Cuando se cifran los datos, se envían al módulo criptográfico que está

validado FIPS 140-2 nivel 1. El módulo criptográfico cifra los datos y los envía de nuevo a la capa RAID. A continuación, los datos cifrados se envían al disco. Por lo tanto, con la combinación de NVE y NAE, los datos ya se cifran en el camino al disco. Las lecturas siguen la ruta inversa. En otras palabras, los datos salen del disco cifrado, se envían a RAID, se descifran por el módulo criptográfico y, a continuación, se envían por el resto de la pila, como se muestra en la siguiente figura.



NVE utiliza un módulo criptográfico de software validado por FIPS 140-2 nivel 1.

Para obtener más información sobre NVE, consulte "Especificaciones técnicas de NVE".

NVE protege los datos en el cloud. Cloud Volumes ONTAP y Azure NetApp Files pueden proporcionar cifrado de datos en reposo conforme a la normativa FIPS 140-2-2.

A partir de ONTAP 9.7, los agregados y los volúmenes recién creados se cifran de forma predeterminada cuando tiene la licencia de NVE y la gestión de claves incorporada o externa. A partir de ONTAP 9.6, se puede utilizar el cifrado a nivel de agregado para asignar claves al agregado que contiene para los volúmenes que se van a cifrar. Los volúmenes que se crean en el agregado están cifrados de manera predeterminada. Puede anular el valor predeterminado al cifrar el volumen.

Comandos de la CLI de NAE de ONTAP

Antes de ejecutar los siguientes comandos de la CLI, asegúrese de que el clúster tenga la licencia de NVE requerida.

Para crear un agregado y cifrarlo, ejecute el siguiente comando (cuando se ejecuta en ONTAP 9.6 y una CLI de clúster posterior):

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

Para convertir un agregado que no sea NAE en un agregado de NAE, ejecute el siguiente comando (cuando se ejecute en ONTAP 9.6 y versiones posteriores de CLI de clústeres):

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

Para convertir un agregado de NAE en un agregado que no sea NAE, ejecute el siguiente comando (cuando se ejecute en ONTAP 9.6 y versiones posteriores de CLI de clústeres):

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

Comandos de la CLI de NVE de ONTAP

A partir de ONTAP 9.6, se puede utilizar el cifrado a nivel de agregado para asignar claves al agregado que contiene para los volúmenes que se van a cifrar. Los volúmenes que se crean en el agregado están cifrados de manera predeterminada.

Para crear un volumen en un agregado que NAE esté habilitado, ejecute el siguiente comando (cuando se ejecute en ONTAP 9.6 y versiones posteriores de CLI de clústeres):

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

Para habilitar el cifrado de un volumen existente “en posición” sin mover un volumen, ejecute el siguiente comando (cuando se ejecute en ONTAP 9.6 y versiones posteriores de CLI de clústeres):

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

Para verificar que los volúmenes estén habilitados para el cifrado, ejecute el siguiente comando de la CLI:

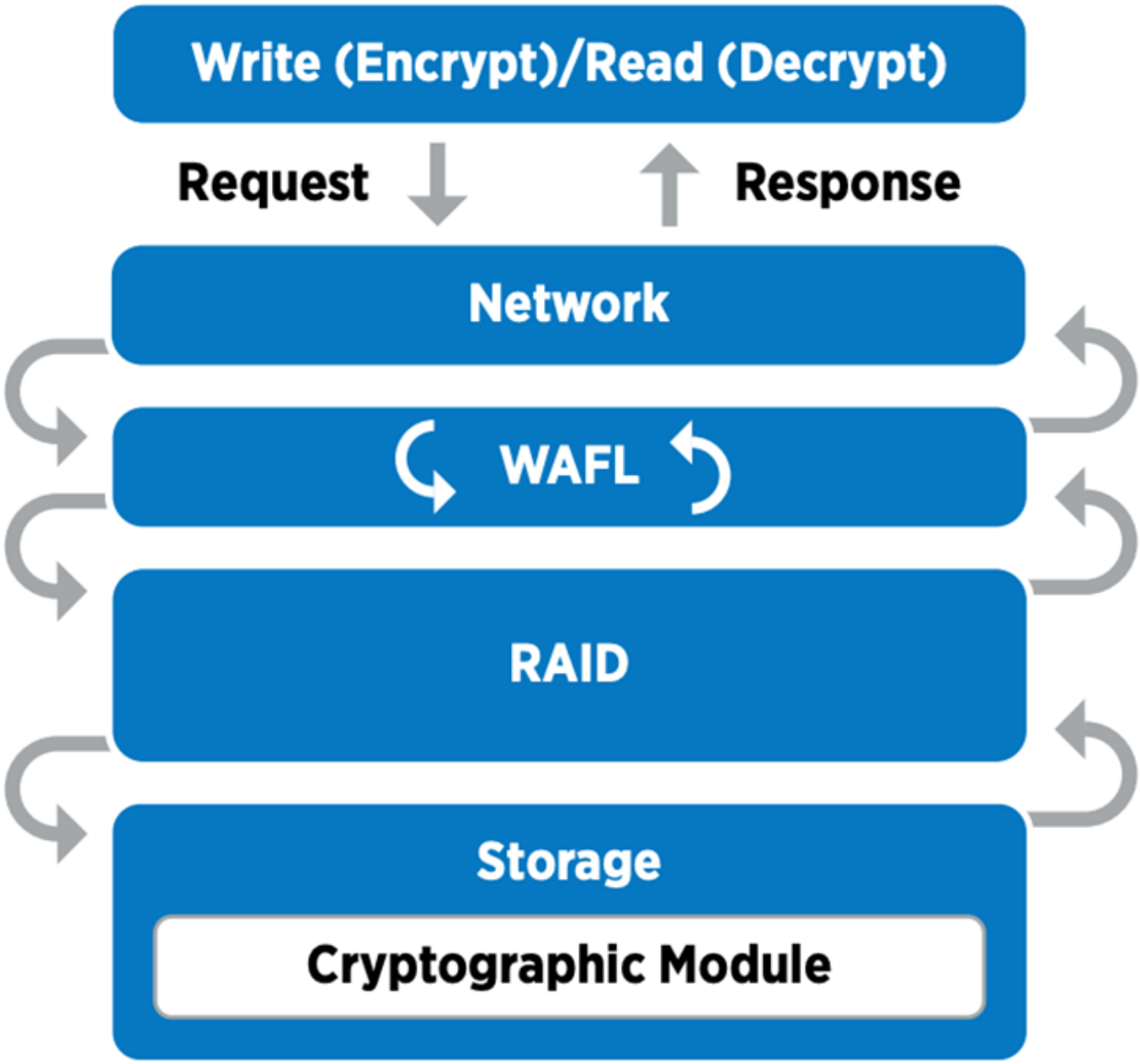
```
fp-health::> volume show -is-encrypted true
```

NSE

NSe utiliza SED para realizar el cifrado de datos a través de un mecanismo acelerado por hardware.

NSe está configurado para utilizar unidades de autocifrado FIPS 140-2 de nivel 2 para facilitar el cumplimiento de normativas y el retorno de reserva al permitir la protección de los datos en reposo mediante el cifrado de

disco transparente AES de 256 bits. Las unidades realizan todas las operaciones de cifrado de datos internamente, como se muestra en la siguiente figura, incluida la generación de claves de cifrado. Para evitar el acceso no autorizado a los datos, el sistema de almacenamiento debe autenticarse con la unidad mediante una clave de autenticación que se establezca la primera vez que se utilice la unidad.



NSe utiliza el cifrado de hardware en cada unidad, que se valida con FIPS 140-2 nivel 2.

Para obtener más información sobre NSE, consulte "Especificaciones técnicas de NSE".

Gestión de claves

El estándar FIPS 140-2 se aplica al módulo criptográfico según lo definido por el límite, como se muestra en la siguiente figura.

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.

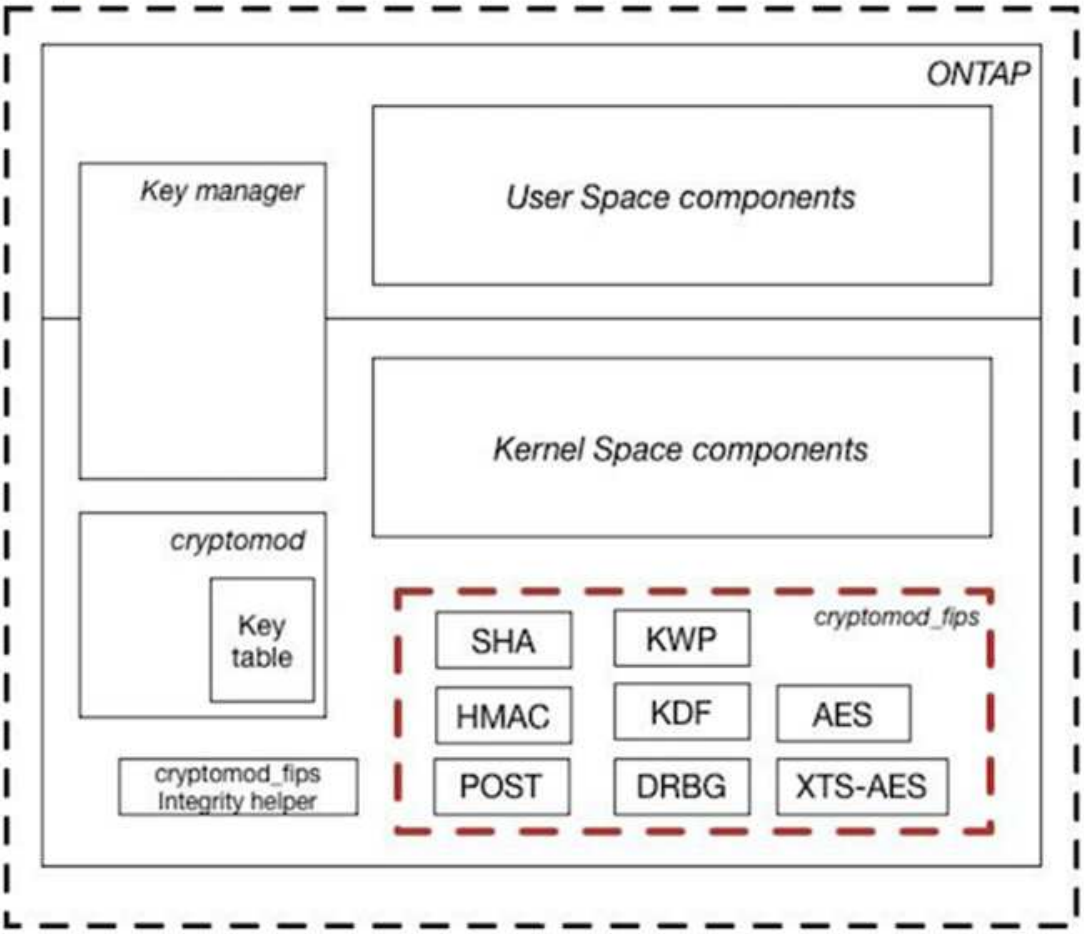


Figure 1 - Block Diagram

Key Manager realiza un seguimiento de todas las claves de cifrado utilizadas por ONTAP. NSe SED utiliza el gestor de claves para establecer las claves de autenticación de NSE SED. Cuando se utiliza el gestor de claves, la solución combinada NVE y NAE está compuesta por un módulo criptográfico de software, claves de cifrado y un gestor de claves. Para cada volumen, NVE utiliza una clave de cifrado de datos XTS-AES 256 única que almacena el gestor de claves. La clave utilizada para un volumen de datos es única para el volumen de datos de ese clúster y se genera cuando se crea el volumen cifrado. De forma similar, un volumen NAE utiliza claves de cifrado de datos XTS-AES 256 exclusivas por agregado, que también almacena el gestor de claves. Las claves NAE se generan cuando se crea el agregado cifrado. ONTAP no pregenera claves, las reutiliza o las muestra en texto sin formato; el administrador de claves las almacena y protege.

Compatibilidad con gestor de claves externo

A partir de ONTAP 9.3, los gestores de claves externos son compatibles con las soluciones NVE y NSE. El estándar FIPS 140-2 se aplica al módulo criptográfico utilizado en la implementación del proveedor específico. Con mayor frecuencia, los clientes de FlexPod y ONTAP utilizan una de las siguientes opciones validadas (según el "Matriz de interoperabilidad de NetApp") gestores de claves:

- Gemalto o SafeNet EN

- Vormétrico (Thales)
- SKLM DE IBM
- Utimaco (anteriormente Microfocus, HPE)

Se realiza un backup de la clave de autenticación SED de NSE y NVMe en un gestor de claves externo mediante el protocolo de interoperabilidad de gestión de claves (KMIP) DE OASIS estándar del sector. Solo el sistema de almacenamiento, la unidad y el administrador de claves tienen acceso a la clave y no es posible desbloquear la unidad si se mueve fuera del dominio de seguridad, para evitar la fuga de datos. El gestor de claves externo también almacena claves de cifrado de volúmenes NVE y claves de cifrado de agregados de NAE. Si el controlador y los discos se mueven y ya no tienen acceso al gestor de claves externo, no se podrá acceder a los volúmenes NVE y NAE ni se podrán descifrar.

El siguiente comando de ejemplo añade dos servidores de gestión de claves a la lista de servidores usados por el administrador de claves externo para almacenar máquinas virtuales (SVM) `svmname1`.

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

Cuando se utiliza un centro de datos de FlexPod en una situación de multi-tenancy, ONTAP permite a los usuarios al proporcionar separación de tenancy por motivos de seguridad en el nivel de SVM.

Para verificar la lista de gestores de claves externos, ejecute el siguiente comando de la CLI:

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

Combine el cifrado para obtener el doble cifrado (defensa por capas).

Si necesita segregar el acceso a los datos y asegurarse de que los datos estén protegidos todo el tiempo, NSE SED puede combinarse con cifrado a nivel de red o estructura. NSe SED actúa como una backstop si un administrador se olvida de configurar o configurar incorrectamente el cifrado de nivel superior. Para dos capas distintas de cifrado, puede combinar NSE SED con NVE y NAE.

Plano de control ONTAP de NetApp modo FIPS para todo el clúster

El software de gestión de datos ONTAP de NetApp tiene una configuración de modo FIPS que instancia un nivel de seguridad añadido para el cliente. Este modo FIPS sólo se aplica al plano de control. Cuando se habilita el modo FIPS, de acuerdo con los elementos clave de FIPS 140-2, se deshabilitan Transport Layer Security v1 (TLSv1) y SSLv3, y sólo se mantienen habilitadas TLS v1.1 y TLS v1.2.

> El panel de control de todo el clúster ONTAP del modo FIPS es compatible con FIPS 140-2 de nivel 1. El modo FIPS de todo el clúster utiliza un módulo criptográfico basado en software proporcionado por NCSM.

El modo de cumplimiento de normativas FIPS 140-2 para el plano de control de todo el clúster protege todas las interfaces de control de ONTAP. De forma predeterminada, el modo solo FIPS 140-2 está deshabilitado; sin embargo, puede habilitar este modo mediante la configuración del `is- fips-enabled` parámetro a. `true` para la `security config modify` comando.

Para habilitar el modo FIPS en el clúster ONTAP, ejecute el siguiente comando:

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

Cuando el modo SSL FIPS está habilitado, la comunicación SSL de ONTAP con el cliente o los componentes de servidor externos a ONTAP utilizará la criptografía de quejas FIPS para SSL.

Para ver el estado FIPS del clúster completo, ejecute los siguientes comandos:

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

"Siguiente: Ventajas de la solución de la infraestructura convergente de FlexPod."

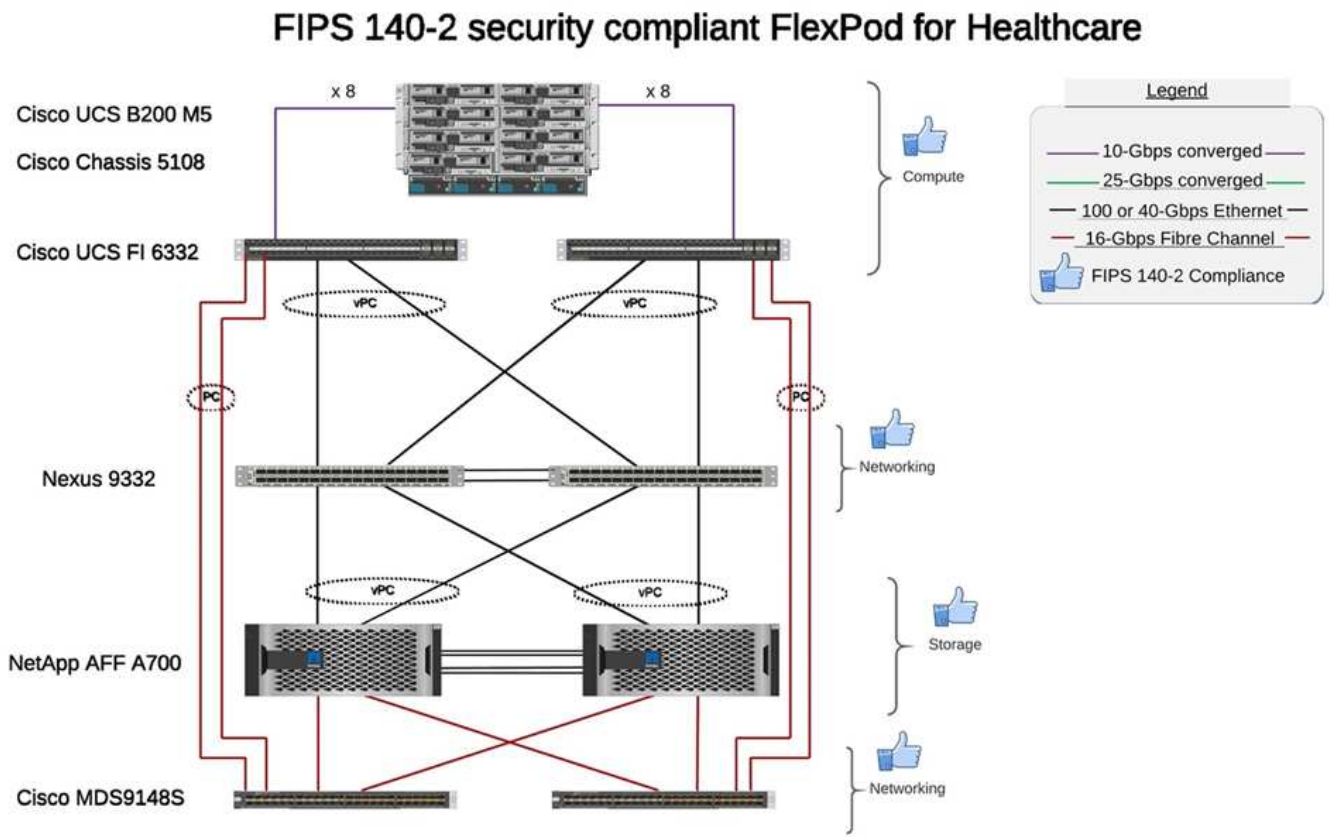
Ventajas para las soluciones de la infraestructura convergente de FlexPod

"Anterior: Almacenamiento ONTAP de FlexPod y FIPS 140-2."

Las organizaciones sanitarias cuentan con varios sistemas de misión crítica. Dos de los sistemas más críticos son los sistemas de historiales médicos electrónicos (EHR) y los sistemas de exploración médica. Para realizar una demostración de la configuración de FIPS en un sistema FlexPod, utilizamos un sistema EHR de código abierto y un sistema de archivado y comunicación de imágenes (PACS) de código abierto para la configuración de laboratorio y la validación de cargas de trabajo en el sistema FlexPod. Para obtener una lista completa de las funcionalidades de EHR, los componentes de las aplicaciones lógicas de EHR y las ventajas que se obtienen con la implantación en un sistema FlexPod, consulte "TR-4881: FlexPod para sistemas de registros sanitarios electrónicos". Para obtener una lista completa de las capacidades del sistema de imágenes médicas, los componentes de la aplicación lógica y cómo se benefician los sistemas de imágenes médicas cuando se implementan en FlexPod, consulte "TR-4865: FlexPod para imágenes médicas".

Durante la configuración de FIPS y la validación de cargas de trabajo, hemos ejercido características de carga de trabajo que eran representativas de una organización sanitaria típica. Por ejemplo, hemos ejercido un sistema EHR de código abierto para incluir un acceso realista a los datos del paciente y escenarios de cambio. Además, se realizaron cargas de trabajo de imágenes médicas que incluyeron imágenes digitales y comunicaciones en objetos médicos (DICOM) en un `*. dcm` formato de archivo. Los objetos DICOM con metadatos se almacenaban en el almacenamiento de archivos y bloques. Además, implementamos funciones multivía desde un servidor Red Hat Enterprise Linux (RHEL) virtualizado. Almacenamos objetos DICOM en un NFS, montamos LUN mediante iSCSI y montan LUN mediante FC. Durante la configuración y validación FIPS, observamos que la infraestructura convergente FlexPod superó nuestras expectativas y tuvo un rendimiento fluido.

La siguiente figura muestra el sistema FlexPod utilizado para la configuración y validación FIPS. Aprovechamos la "FlexPod Datacenter con VMware vSphere 7.0 y NetApp ONTAP 9.7 Cisco Validated Design (CVD)" durante el proceso de configuración.



Infraestructura de la solución componentes de hardware y software

En las dos figuras siguientes se enumeran los componentes de hardware y software respectivamente, que se usan durante las pruebas FIPS que se habilitan en una FlexPod. Las recomendaciones en estas tablas son ejemplos. Debe trabajar con el SME de NetApp para garantizar que los componentes se corresponden con su organización. Además, asegúrese de que los componentes y las versiones sean compatibles con el "Herramienta de matriz de interoperabilidad de NetApp" (IMT) y. "Lista de compatibilidad de hardware (HCL) de Cisco".

Capa	Familia de productos	Cantidad y modelo	Detalles
Informática	Chasis Cisco UCS 5108	1 o 2	
	Servidores blade Cisco UCS	3 B200 M5	Cada uno con 2 20 núcleos o más, 2,7 GHz y 128 GB de RAM
	Tarjeta de interfaz virtual (VIC) de Cisco UCS	Cisco UCS 1440	Consulte
	2 interconexiones de estructura Cisco UCS	6332	-
Red	Switches Cisco Nexus	2 switches Cisco Nexus 9332	-

Capa	Familia de productos	Cantidad y modelo	Detalles
Red de almacenamiento	Red IP para el acceso de almacenamiento mediante protocolos SMB/CIFS, NFS o iSCSI	Los mismos switches de red que se han descrito anteriormente	-
	Acceso a almacenamiento mediante FC	2 Cisco MDS 9148S	-
Reducida	Sistema de almacenamiento all-flash AFF A700 de NetApp	Clúster 1	Clúster con dos nodos
	Bandeja de discos	Una bandeja de discos DS224C o NS224	Totalmente lleno con 24 unidades
	SSD	>24, 1,2 TB o mayor capacidad	-

De NetApp	Familia de productos	Versión o versión	Detalles
Varios	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 (64 bits)	-
	ONTAP de NetApp	ONTAP 9.7 o posterior	-
	Interconexión de estructura Cisco UCS	Cisco UCS Manager 4.1 o posterior	-
	Switches de las series Cisco Ethernet 3000 o 9000	Para la serie 9000, 7.0(3)I7(7) o posterior para la serie 3000, 9.2(4) o posterior	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) o posterior	-
	Hipervisor	VMware vSphere ESXi 6.7 U2 o posterior	-
Reducida	Sistema de gestión de hipervisores	VMware vCenter Server 6.7 U3 (vcsa) o posterior	-
Red	Virtual Storage Console (VSC) de NetApp	VSC 9.7 o posterior	-
	SnapCenter de NetApp	SnapCenter 4.3 o posterior	-
	Administrador de Cisco UCS	4.1(1c) o posterior	
Hipervisor	ESXi		
Gestión	Sistema de gestión de hipervisores VMware vCenter Server 6.7 U3 (vcsa) o posterior		

De NetApp	Familia de productos	Versión o versión	Detalles
	Virtual Storage Console (VSC) de NetApp	VSC 9.7 o posterior	
	SnapCenter de NetApp	SnapCenter 4.3 o posterior	
	Administrador de Cisco UCS	4.1(1c) o posterior	

"Siguiente: Consideraciones adicionales sobre seguridad de FlexPod."

Otras consideraciones de seguridad de FlexPod

"Anterior: Ventajas de la solución de la infraestructura convergente de FlexPod."

La infraestructura FlexPod es una plataforma modular, convergente, opcionalmente virtualizada, escalable (escalado horizontal y vertical) y rentable. Con la plataforma FlexPod, puede escalar horizontalmente de forma independiente la computación, la red y el almacenamiento para acelerar la puesta en marcha de las aplicaciones. Además, la arquitectura modular posibilita operaciones no disruptivas incluso durante las actividades de escalado horizontal y actualización del sistema.

Los diferentes componentes de un sistema HIT requieren que los datos se almacenen en sistemas de archivos SMB/CIFS, NFS, Ext4 y NTFS. Este requisito implica que la infraestructura debe proporcionar acceso a datos a través de los protocolos NFS, CIFS y SAN. Un único sistema de almacenamiento de NetApp es compatible con todos estos protocolos, lo que elimina la necesidad de utilizar sistemas de almacenamiento específicos de protocolos existentes. Además, un único sistema de almacenamiento de NetApp es compatible CON múltiples CARGAS de trabajo DE HIT, como EHR, PACS o VNA, genómica, VDI, etc. con niveles de rendimiento garantizados y configurables.

CUANDO se implementa en un sistema FlexPod, HIT ofrece varias ventajas específicas para el sector sanitario. La siguiente lista es una descripción de alto nivel de estas ventajas:

- **Seguridad FlexPod**. La seguridad es la base misma de un sistema FlexPod. En los últimos años, el ransomware se ha convertido en una amenaza. El ransomware es un tipo de malware basado en la criptovirología, el uso de criptografía para crear software malicioso. Este malware puede utilizar cifrado de clave simétrica y asimétrica para bloquear los datos de una víctima y exigir un rescate para proporcionar la clave para descifrar los datos. Para descubrir cómo la solución FlexPod ayuda a mitigar amenazas como el ransomware, consulte "TR-4802: La solución para el ransomware". Los componentes de infraestructura de FlexPod también lo son "Conforme a FIPS 140-2".
- * Cisco Intersight.* Cisco Intersight es una plataforma innovadora basada en la nube y de gestión como servicio que proporciona un único panel para la gestión y orquestación de FlexPod en toda la pila. La plataforma InterSight utiliza módulos criptográficos compatibles con la seguridad FIPS 140-2. La arquitectura de gestión fuera de banda de la plataforma lo hace fuera del alcance de algunos estándares o auditorías como HIPAA. Nunca se envía al portal Intersight ningún tipo de información de salud identificable de la red.
- **La tecnología FPolicy de NetApp.** FPolicy de NetApp (una evolución de la política de archivos de nombres) es un marco de notificaciones de acceso a archivos para supervisar y gestionar el acceso a archivos a través de los protocolos NFS o SMB/CIFS. Esta tecnología forma parte del software de gestión de datos ONTAP desde hace más de una década, lo cual resulta útil para detectar ransomware. Este motor Zero Trust proporciona medidas de seguridad adicionales más allá de los permisos en las listas de

control de acceso (ACL). FPolicy tiene dos modos de funcionamiento: Nativo y externo:

  - El modo nativo proporciona tanto la lista negra como la lista blanca de extensiones de archivo.
  - El modo externo tiene las mismas funcionalidades que el modo nativo, pero también se integra con un servidor FPolicy que se ejecuta externamente al sistema ONTAP así como un sistema SIEM (información de seguridad y gestión de eventos). Para obtener más información sobre cómo combatir el ransomware, consulte la "Lucha contra el ransomware: Parte tres – FPolicy de ONTAP, otra potente herramienta nativa (también conocida como gratuita)" blog.

- **Datos en reposo**. ONTAP 9 y versiones posteriores tienen tres soluciones de cifrado de datos en reposo conformes con la normativa FIPS 140-2:
  - NSe es una solución de hardware que utiliza unidades de autocifrado.
  - NVE es una solución de software que permite el cifrado de cualquier volumen de datos en cualquier tipo de unidad donde se habilita con una clave única para cada volumen.
  - NAE es una solución de software que permite el cifrado de cualquier volumen de datos en cualquier tipo de unidad en la que se habilita con claves únicas para cada agregado.

> A partir de ONTAP 9.7, NAE y NVE están habilitados por defecto si el paquete de licencia NetApp NVE con el nombre ve está en su lugar.

- **Datos en vuelo**. A partir de ONTAP 9.8, IPsec (el protocolo de seguridad de Internet) proporciona compatibilidad con cifrado de extremo a extremo para todo el tráfico de IP entre un cliente y una SVM de ONTAP. El cifrado de datos IPSec para todo el tráfico IP incluye protocolos NFS, iSCSI y SMB/CIFS. IPSec proporciona la única opción de cifrado en vuelo para el tráfico iSCSI.
- **Cifrado de datos integral en una estructura de datos multicloud híbrida**. Los clientes que usan tecnologías de cifrado de datos en reposo como NSE, NVE y el cifrado de paridad de clúster (CPE) para el tráfico de replicación de datos pueden ahora usar el cifrado integral entre el cliente y el almacenamiento en su estructura de datos multicloud híbrido mediante la actualización a ONTAP 9.8 o una versión posterior y mediante IPsec. A partir de ONTAP 9, puede habilitar el modo de cumplimiento normativo FIPS 140-2 para las interfaces en el plano de control de todo el clúster. De manera predeterminada, se deshabilita el modo FIPS 140-2-only. A partir de ONTAP 9.6, CPE proporciona compatibilidad del cifrado TLS 1.2 AES-256 GCM para las funciones de replicación de datos de ONTAP como las tecnologías SnapMirror, NetApp SnapVault y NetApp FlexCache. El cifrado se configura mediante una clave precompartida (PSK) entre dos pares de clústeres.
- **Multitenancy seguro**. Admite el aumento de las necesidades de la infraestructura compartida de servidores virtualizados y almacenamiento, lo que permite una multi-tenancy seguro de información específica del centro, en particular cuando se alojan varias instancias de bases de datos y software.

"Siguiente: Conclusión."

Conclusión

"Anterior: Consideraciones adicionales sobre seguridad de FlexPod."

Al ejecutar su aplicación de atención médica en una plataforma FlexPod, su organización de atención médica estará mejor protegida por una plataforma habilitada para FIPS 140-2. FlexPod ofrece protección con varias capas en cada componente único: Informática, redes y almacenamiento. Las funcionalidades de protección de datos de FlexPod protegen los datos en reposo o en movimiento y conservan los backups seguros y listos cuando sea necesario.

Evite errores humanos aprovechando los diseños prevalidados de FlexPod recientemente probados e infraestructuras convergentes de la alianza estratégica de Cisco y NetApp. Un sistema FlexPod ha diseñado y diseñado para proporcionar un rendimiento del sistema previsible y de baja latencia, y una alta disponibilidad con un impacto mínimo, incluso si se habilita FIPS 140-2 en las capas de computación, redes y almacenamiento. Este enfoque da como resultado una experiencia de usuario superior y un tiempo de respuesta óptimo para los usuarios del sistema HIT.

"Siguiente: Reconocimientos, historial de versiones y dónde encontrar información adicional."

Agradecimientos, historial de versiones y dónde encontrar información adicional

"Anterior: Conclusión."

Si quiere obtener más información sobre el contenido de este documento, consulte los siguientes documentos y sitios web:

- Guía de configuración de seguridad de la familia Cisco MDS 9000 NX-OS

  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

- Guía de configuración de seguridad de NX-OS con Cisco Nexus serie 9000, versión 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

- Publicación 140-2 de NetApp y del estándar de procesamiento de información federal (FIPS)

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

- FIPS 140-2

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

- Guía de fortalecimiento de NetApp ONTAP 9

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

- Guía completa de cifrado de NetApp

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

- Especificaciones técnicas de NVE y NAE

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

- Especificaciones técnicas de NSE

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

- Centro de documentación de ONTAP 9

  http://docs.netapp.com

- Publicación 140-2 de NetApp y del estándar de procesamiento de información federal (FIPS)

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

- Cumplimiento de normativas Cisco y FIPS 140-2-2

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

- Módulo de seguridad de criptografía de NetApp

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

- Prácticas de ciberseguridad para medianas y grandes organizaciones sanitarias

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

- Programa de validación de módulos de criptografía y Cisco (CMVP)

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

- Cifrado del almacenamiento de NetApp, unidades de autocifrado NVMe, cifrado de volúmenes de NetApp y cifrado agregado de NetApp

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

- Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp

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

- Cifrado del almacenamiento de NetApp

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

- FlexPod para sistemas de registros médicos electrónicos

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

- Datos ahora: Mejora de rendimiento en entornos EHR de Epic con la tecnología flash conectada al cloud

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

- Centro de datos FlexPod para infraestructura EHR de Epic

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

- Guía de puesta en marcha del centro de datos FlexPod para EHR de Epic

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

- Infraestructura de centro de datos FlexPod para el software MEDITECH

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

- El estándar FlexPod se extiende al software MEDITECH

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

- Guía de tamaños direccionales de FlexPod para MEDITECH

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

- FlexPod para imágenes médicas

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

- IA en la sanidad

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

- FlexPod para el sector sanitario facilita su transformación

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

- FlexPod de Cisco y NetApp

  https://flexpod.com/

Reconocimientos

- Abhinav Singh, Ingeniero Técnico de Marketing de NetApp
- Brian o'Mahony, arquitecto de soluciones Healthcare (Epic), NetApp
- Brian Pruitt, director de desarrollo comercial de NetApp
- Arvind Ramakrishnan, arquitecto sénior de soluciones de NetApp
- Michael Hommer, Director técnico de FlexPod Global Field, NetApp

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Abril de 2021	Versión inicial