FlexPod e sicurezza

FlexPod

NetApp
March 25, 2024

Sommario

FlexPod e sicurezza

FlexPod, la soluzione per il ransomware

TR-4802: FlexPod, la soluzione per il ransomware

Arvind Ramakrishnan, NetApp

In collaborazione con: 

Per comprendere il ransomware, è necessario prima comprendere alcuni punti chiave sulla crittografia. I metodi crittografici consentono la crittografia dei dati con una chiave segreta condivisa (crittografia a chiave simmetrica) o con una coppia di chiavi (crittografia a chiave asimmetrica). Una di queste chiavi è una chiave pubblica ampiamente disponibile e l'altra è una chiave privata non divulgata.

Ransomware è un tipo di malware basato sulla crittografia, ovvero l'utilizzo della crittografia per la creazione di software dannoso. Questo malware può utilizzare la crittografia a chiave simmetrica e asimmetrica per bloccare i dati della vittima e richiedere un riscatto per fornire la chiave per decrittare i dati della vittima.

Come funziona il ransomware?

I seguenti passaggi descrivono come ransomware utilizza la crittografia per crittografare i dati della vittima senza alcun scopo per la decifratura o il ripristino da parte della vittima:

1. L'utente malintenzionato genera una coppia di chiavi come nella crittografia a chiave asimmetrica. La chiave pubblica generata viene inserita nel malware e il malware viene quindi rilasciato.
2. Una volta che il malware è entrato nel computer o nel sistema della vittima, genera una chiave simmetrica casuale utilizzando un generatore di numeri pseudocasuali (PRNG) o qualsiasi altro algoritmo di generazione di numeri casuali.
3. Il malware utilizza questa chiave simmetrica per crittografare i dati della vittima. Infine, crittografa la chiave simmetrica utilizzando la chiave pubblica dell'utente malintenzionato incorporata nel malware. L'output di questo passo è un testo cifrato asimmetrico della chiave simmetrica crittografata e il testo cifrato simmetrico dei dati della vittima.
4. Il malware azzera (cancella) i dati della vittima e la chiave simmetrica utilizzata per crittografare i dati, senza lasciare spazio per il ripristino.
5. La vittima ora mostra il testo cifrato asimmetrico della chiave simmetrica e un valore di riscatto che deve essere pagato per ottenere la chiave simmetrica utilizzata per crittografare i dati.
6. La vittima paga il riscatto e condivide il testo cifrato asimmetrico con l'autore dell'attacco. L'utente malintenzionato decrittografa il testo crittografato con la propria chiave privata, che determina la chiave simmetrica.
7. L'utente malintenzionato condivide questa chiave simmetrica con la vittima, che può essere utilizzata per decrittare tutti i dati e quindi per ripristinarli dall'attacco.

Sfide

Individui e organizzazioni devono affrontare le seguenti sfide quando vengono attaccati dal ransomware:

- La sfida più importante è che richiede un costo immediato sulla produttività dell'organizzazione o dell'individuo. Ci vuole tempo per tornare a uno stato di normalità, perché tutti i file importanti devono essere riconquistati e i sistemi devono essere protetti.
- Potrebbe portare a una violazione dei dati che contiene informazioni riservate e riservate che appartengono a clienti o clienti e che porta a una situazione di crisi che un'organizzazione vorrebbe chiaramente evitare.
- Esiste un'ottima probabilità che i dati entrino nelle mani sbagliate o vengano cancellati completamente, il che porta a un punto di non ritorno che potrebbe essere disastroso per le organizzazioni e gli individui.
- Dopo aver pagato il riscatto, non vi è alcuna garanzia che l'utente malintenzionato fornisca la chiave per ripristinare i dati.
- Non vi è alcuna garanzia che l'utente malintenzionato si asterrà dalla trasmissione dei dati sensibili nonostante il pagamento del riscatto.
- Nelle grandi imprese, identificare la lacuna che ha portato a un attacco ransomware è un compito noioso e la protezione di tutti i sistemi richiede un notevole impegno.

Chi è a rischio?

Chiunque può essere attaccato da ransomware, inclusi individui e grandi organizzazioni. Le organizzazioni che non implementano procedure e misure di sicurezza ben definite sono ancora più vulnerabili a tali attacchi. L'effetto dell'attacco su un'organizzazione di grandi dimensioni può essere più grande di quanto un individuo potrebbe sopportare.

Ransomware rappresenta circa il 28% di tutti gli attacchi di malware. In altre parole, più di un malware su quattro è un attacco ransomware. Il ransomware può diffondersi automaticamente e indiscriminatamente attraverso Internet e, in caso di mancanza di sicurezza, può entrare nei sistemi della vittima e continuare a diffondersi ad altri sistemi connessi. Gli autori degli attacchi tendono a rivolgersi a persone o organizzazioni che eseguono una grande quantità di file sharing, dispongono di molti dati sensibili e critici o mantengono una protezione inadeguata contro gli attacchi.

Gli autori degli attacchi tendono a concentrarsi sui seguenti potenziali obiettivi:

- Università e comunità studentesche
- Uffici governativi e agenzie
- Ospedali
- Banche

Questo non è un elenco completo di obiettivi. Non puoi considerarti al sicuro dagli attacchi se ti trovi al di fuori di una di queste categorie.

In che modo il ransomware entra in un sistema o si diffonde?

Esistono diversi modi in cui il ransomware può entrare in un sistema o diffondersi in altri sistemi. Nel mondo odierno, quasi tutti i sistemi sono connessi tra loro tramite Internet, LAN, WAN e così via. La quantità di dati che vengono generati e scambiati tra questi sistemi è solo in aumento.

Alcuni dei modi più comuni con cui il ransomware può diffondersi includono metodi che utilizziamo quotidianamente per condividere o accedere ai dati:

- E-mail
- Reti P2P
- Download di file
- Social network
- Dispositivi mobili
- Connessione a reti pubbliche non sicure
- Accesso agli URL Web

Conseguenze della perdita di dati

Le conseguenze o gli effetti della perdita di dati possono arrivare più ampiamente di quanto le organizzazioni potrebbero prevedere. Gli effetti possono variare a seconda della durata del downtime o del periodo di tempo durante il quale un'organizzazione non ha accesso ai propri dati. Quanto più dura l'attacco, tanto maggiore sarà l'effetto sui ricavi, sul marchio e sulla reputazione dell'organizzazione. Un'organizzazione può anche affrontare problemi legali e un drastico calo della produttività.

Poiché questi problemi continuano a persistere nel tempo, iniziano ad ingrandirsi e potrebbero finire per cambiare la cultura di un'organizzazione, a seconda di come risponde all'attacco. Nel mondo di oggi, le informazioni si diffondono rapidamente e le notizie negative su un'organizzazione potrebbero causare danni permanenti alla sua reputazione. Un'organizzazione potrebbe affrontare enormi sanzioni per la perdita di dati, che potrebbe portare alla chiusura di un'azienda.

Effetti finanziari

Secondo un recente "Report McAfee", I costi globali sostenuti a causa della criminalità informatica sono pari a circa 600 miliardi di dollari, pari a circa il 0.8% del PIL globale. Quando questo importo viene confrontato con la crescente economia mondiale di Internet di 4.2 trilioni di dollari, equivale a una tassa del 14% sulla crescita.

Ransomware prende una quota significativa di questo costo finanziario. Nel 2018, i costi sostenuti per gli attacchi ransomware sono stati di circa 8 miliardi di dollari—, un importo previsto per raggiungere i 11.5 miliardi di dollari nel 2019.

Qual è la soluzione?

Il ripristino da un attacco ransomware con downtime minimo è possibile solo implementando un piano di disaster recovery proattivo. Avere la capacità di recuperare da un attacco è un bene, ma prevenire un attacco è l'ideale.

Sebbene vi siano diversi fronti che è necessario rivedere e correggere per prevenire un attacco, il componente principale che consente di prevenire o ripristinare da un attacco è il data center.

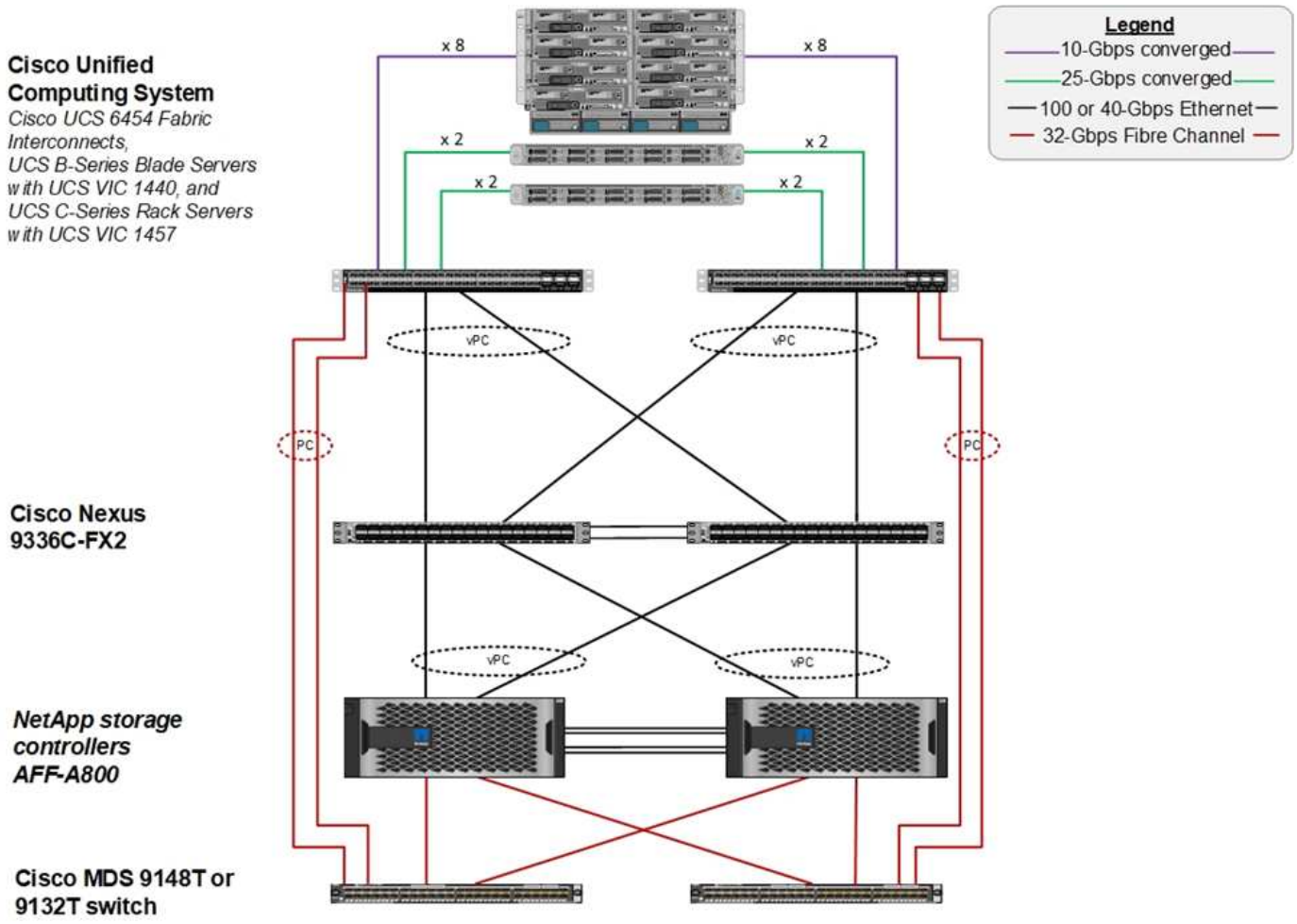
Il design del data center e le funzionalità che offre per proteggere gli end-point di rete, calcolo e storage svolgono un ruolo fondamentale nella creazione di un ambiente sicuro per le operazioni quotidiane. Questo documento mostra in che modo le funzionalità di un'infrastruttura di cloud ibrido FlexPod possono contribuire al rapido ripristino dei dati in caso di attacco e possono anche contribuire a prevenire del tutto gli attacchi.

Panoramica di FlexPod

FlexPod è un'architettura pre-progettata, integrata e validata che combina i server Cisco Unified Computing System (Cisco UCS), la famiglia di switch Cisco Nexus, gli switch Cisco MDS Fabric e gli storage array NetApp in un'unica architettura flessibile. Le

soluzioni FlexPod sono progettate per l'alta disponibilità senza singoli punti di errore, mantenendo al contempo convenienza e flessibilità di progettazione per supportare un'ampia varietà di carichi di lavoro. Un design FlexPod può supportare diversi hypervisor e server bare metal e può anche essere dimensionato e ottimizzato in base ai requisiti dei carichi di lavoro del cliente.

La figura seguente illustra l'architettura FlexPod e evidenzia chiaramente l'alta disponibilità in tutti i livelli dello stack. I componenti dell'infrastruttura di storage, rete e calcolo sono configurati in modo che le operazioni possano eseguire il failover istantaneo al partner sopravvissuto in caso di guasto di uno dei componenti.



Un vantaggio importante per un sistema FlexPod è la sua pre-progettazione, integrazione e validazione per diversi carichi di lavoro. Vengono pubblicate guide dettagliate di progettazione e implementazione per ogni convalida della soluzione. Questi documenti includono le Best practice da adottare per consentire ai carichi di lavoro di essere eseguiti senza problemi su FlexPod. Queste soluzioni sono costruite con i migliori prodotti di calcolo, rete e storage e una serie di funzionalità che si concentrano sulla sicurezza e la protezione avanzata dell'intera infrastruttura.

"L'X-Force Threat Intelligence Index di IBM" afferma: "Errore umano responsabile di due terzi dei record compromessi, compreso un salto storico del 424% nell'infrastruttura cloud non configurata correttamente".

Con un sistema FlexPod, è possibile evitare di configurare in modo errato l'infrastruttura utilizzando l'automazione attraverso i playbook Ansible che eseguono una configurazione end-to-end dell'infrastruttura in base alle Best practice descritte in Cisco Validated Designs (CVD) e NetApp Verified Architectures (NVA).

Misure di protezione ransomware

In questa sezione vengono descritte le funzionalità principali del software di gestione dei dati NetApp ONTAP e gli strumenti per Cisco UCS e Cisco Nexus che è possibile utilizzare per proteggere e ripristinare in modo efficace dagli attacchi ransomware.

Storage: NetApp ONTAP

Il software ONTAP offre molte funzionalità utili per la protezione dei dati, la maggior parte delle quali è gratuita per i clienti che dispongono di un sistema ONTAP. È possibile utilizzare le seguenti funzionalità in qualsiasi momento per proteggere i dati dagli attacchi:

- **Tecnologia NetApp Snapshot.** Una copia Snapshot è un'immagine di sola lettura di un volume che acquisisce lo stato di un file system in un momento specifico. Queste copie aiutano a proteggere i dati senza alcun effetto sulle prestazioni del sistema e, allo stesso tempo, non occupano molto spazio di storage. NetApp consiglia di creare una pianificazione per la creazione di copie Snapshot. È inoltre necessario mantenere un lungo periodo di conservazione, in quanto alcuni malware possono andare in stato di inattività e quindi riattivarsi settimane o mesi dopo un'infezione. In caso di attacco, è possibile eseguire il rollback del volume utilizzando una copia Snapshot acquisita prima dell'infezione.
- **La tecnologia NetApp SnapRestore.** il software di ripristino dei dati SnapRestore è estremamente utile per eseguire il ripristino dalla corruzione dei dati o per ripristinare solo il contenuto del file. SnapRestore non ripristina gli attributi di un volume, ma è molto più veloce di quanto un amministratore possa ottenere copiando i file dalla copia Snapshot al file system attivo. La velocità con cui è possibile recuperare i dati è utile quando molti file devono essere ripristinati il più rapidamente possibile. In caso di attacco, questo processo di recovery altamente efficiente consente di ripristinare rapidamente il business online.
- **Tecnologia NetApp SnapCenter.** il software SnapCenter utilizza le funzioni di backup e replica basate su storage NetApp per fornire una protezione dei dati coerente con l'applicazione. Questo software si integra con le applicazioni aziendali e fornisce flussi di lavoro specifici per applicazioni e database per soddisfare le esigenze degli amministratori di applicazioni, database e infrastrutture virtuali. SnapCenter offre una piattaforma aziendale di facile utilizzo per coordinare e gestire in modo sicuro la protezione dei dati tra applicazioni, database e file system. La sua capacità di fornire una protezione dei dati coerente con l'applicazione è fondamentale durante il ripristino dei dati, perché semplifica il ripristino delle applicazioni a uno stato coerente più rapidamente.
- **Tecnologia NetApp SnapLock.** SnapLock offre un volume speciale in cui i file possono essere memorizzati e impegnati in uno stato non cancellabile e non riscrivibile. I dati di produzione dell'utente che risiedono in un volume FlexVol possono essere mirrorati o archiviati in un volume SnapLock, rispettivamente tramite NetApp SnapMirror o la tecnologia SnapVault. I file nel volume SnapLock, nel volume stesso e nel relativo aggregato di hosting non possono essere cancellati fino alla fine del periodo di conservazione.
- **Tecnologia NetApp FPolicy.** Usa il software FPolicy per prevenire gli attacchi impedendo operazioni su file con estensioni specifiche. È possibile attivare un evento FPolicy per operazioni di file specifiche. L'evento è legato a una policy, che richiama il motore che deve utilizzare. È possibile configurare un criterio con una serie di estensioni di file che potrebbero contenere ransomware. Quando un file con un'estensione non consentita tenta di eseguire un'operazione non autorizzata, FPolicy impedisce l'esecuzione di tale operazione.

Rete: Cisco Nexus

Il software Cisco NX OS supporta la funzione NetFlow che consente un rilevamento avanzato delle anomalie e della sicurezza della rete. NetFlow acquisisce i metadati di ogni conversazione sulla rete, le parti coinvolte nella comunicazione, il protocollo utilizzato e la durata della transazione. Una volta aggregate e analizzate le informazioni, possono fornire informazioni dettagliate sul comportamento normale.

I dati raccolti consentono inoltre l'identificazione di modelli di attività dubbi, come la diffusione di malware nella rete, che altrimenti potrebbero passare inosservati.

NetFlow utilizza i flussi per fornire statistiche per il monitoraggio della rete. Un flusso è un flusso unidirezionale di pacchetti che arriva su un'interfaccia di origine (o VLAN) e ha gli stessi valori per le chiavi. Una chiave è un valore identificato per un campo all'interno del pacchetto. Si crea un flusso utilizzando un record di flusso per definire le chiavi univoche per il flusso. È possibile esportare i dati raccolti da NetFlow per i flussi utilizzando un'esportazione di flusso in un NetFlow Collector remoto, ad esempio Cisco Stealthwatch. Stealthwatch utilizza queste informazioni per il monitoraggio continuo della rete e fornisce analisi forensi in tempo reale per il rilevamento delle minacce e la risposta agli incidenti in caso di scoppio di ransomware.

Calcolo: Cisco UCS

Cisco UCS è l'endpoint di calcolo in un'architettura FlexPod. È possibile utilizzare diversi prodotti Cisco per proteggere questo livello dello stack a livello di sistema operativo.

È possibile implementare i seguenti prodotti chiave a livello di elaborazione o applicazione:

- **Cisco Advanced malware Protection (AMP) per endpoint.** supportata sui sistemi operativi Microsoft Windows e Linux, questa soluzione integra funzionalità di prevenzione, rilevamento e risposta. Questo software di sicurezza previene le violazioni, blocca il malware nel punto di ingresso e monitora e analizza continuamente le attività di file e processi per rilevare, contenere e rimediare rapidamente alle minacce che possono eludere le difese front-line.

  Il componente di protezione delle attività dannose (MAP) di AMP monitora continuamente tutte le attività degli endpoint e fornisce il rilevamento in fase di esecuzione e il blocco del comportamento anomalo di un programma in esecuzione sull'endpoint. Ad esempio, quando il comportamento degli endpoint indica ransomware, i processi in errore vengono terminati, impedendo la crittografia degli endpoint e arrestando l'attacco.

- **Cisco Advanced malware Protection for Email Security.** le email sono diventate il mezzo principale per diffondere malware e per eseguire cyber-attacchi. In media, circa 100 miliardi di e-mail vengono scambiate in un solo giorno, il che fornisce agli autori degli attacchi un eccellente vettore di penetrazione nei sistemi degli utenti. Pertanto, è assolutamente essenziale difendersi da questa linea di attacco.

  AMP analizza le e-mail per individuare minacce come exploit zero-day e malware furtivo nascosto in allegati dannosi. Utilizza inoltre l'intelligence URL leader del settore per combattere i collegamenti dannosi. Offre agli utenti una protezione avanzata contro il phishing, il ransomware e altri attacchi sofisticati.

- **Next-Generation Intrusion Prevention System (NGIPS).** Cisco firepower NGIPS può essere implementato come appliance fisica nel data center o come appliance virtuale su VMware (NGIPSv per VMware). Questo sistema di prevenzione delle intrusioni altamente efficace offre performance affidabili e un basso costo totale di proprietà. La protezione dalle minacce può essere estesa con licenze di abbonamento opzionali per fornire AMP, visibilità e controllo delle applicazioni e funzionalità di filtraggio degli URL. I NGIPS virtualizzati ispezionano il traffico tra macchine virtuali (VM) e semplificano l'implementazione e la gestione delle soluzioni NGIPS in siti con risorse limitate, aumentando la protezione per risorse fisiche e virtuali.

Proteggere e ripristinare i dati su FlexPod

Questa sezione descrive come è possibile ripristinare i dati di un utente finale in caso di attacco e come è possibile prevenire gli attacchi utilizzando un sistema FlexPod.

Panoramica testbed

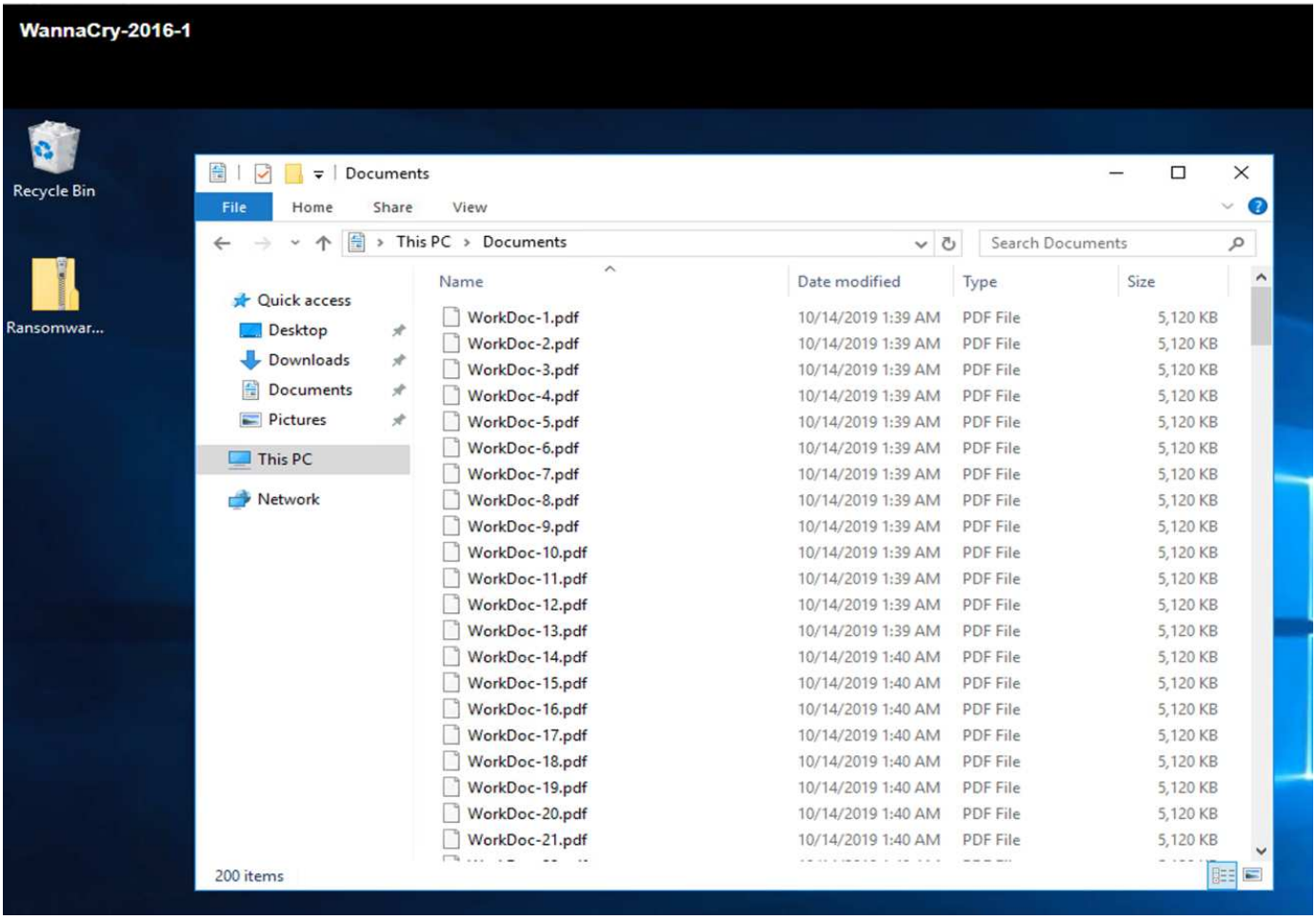
Per mostrare il rilevamento, la correzione e la prevenzione di FlexPod, è stato creato un testbed basato sulle linee guida specificate nell'ultima piattaforma CVD disponibile al momento della stesura del presente documento: "FlexPod Datacenter con VMware vSphere 6.7 U1, Cisco UCS 4a generazione e NetApp AFF A-Series CVD".

Una macchina virtuale Windows 2016, che forniva una condivisione CIFS dal software NetApp ONTAP, è stata implementata nell'infrastruttura VMware vSphere. Quindi, NetApp FPolicy è stato configurato sulla condivisione CIFS per impedire l'esecuzione di file con determinati tipi di estensione. Il software NetApp SnapCenter è stato implementato anche per gestire le copie Snapshot delle macchine virtuali nell'infrastruttura per fornire copie Snapshot coerenti con l'applicazione.

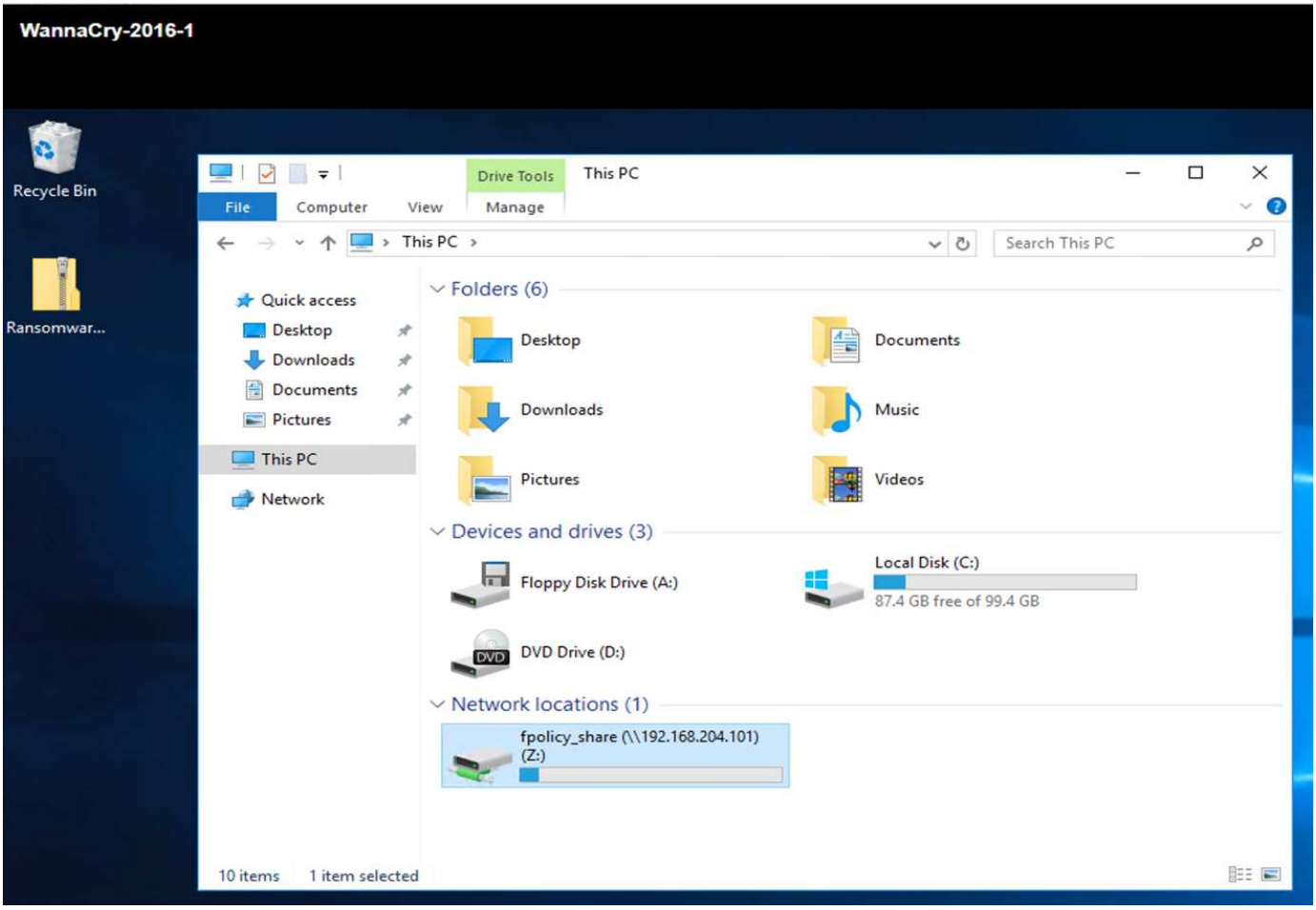
Stato della macchina virtuale e dei relativi file prima di un attacco

Questa sezione mostra lo stato dei file prima di un attacco alla macchina virtuale e la condivisione CIFS ad essa mappata.

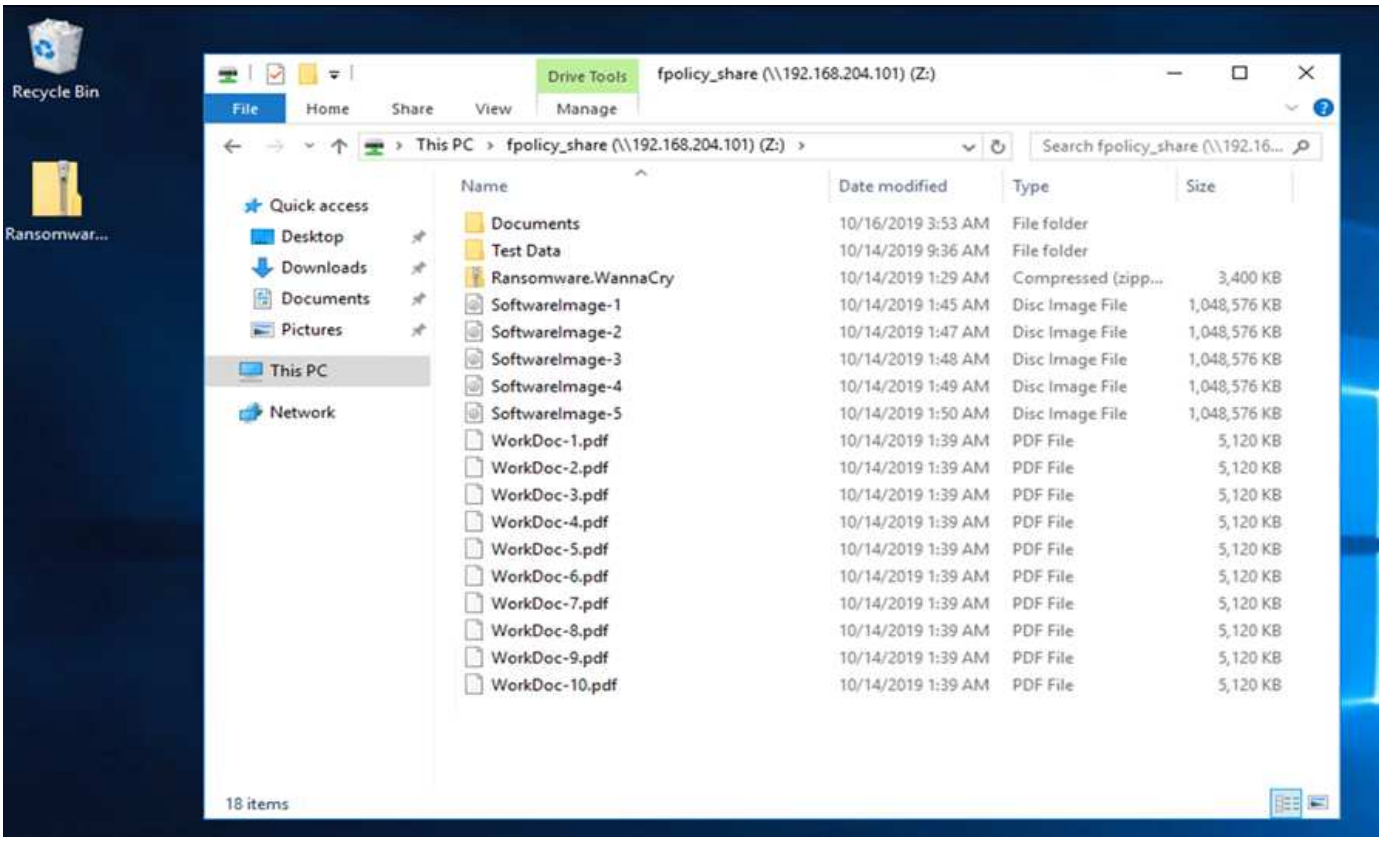
La cartella documenti della macchina virtuale aveva un set di file PDF che non sono stati ancora crittografati dal malware WannaCry.



La seguente schermata mostra la condivisione CIFS mappata alla macchina virtuale.



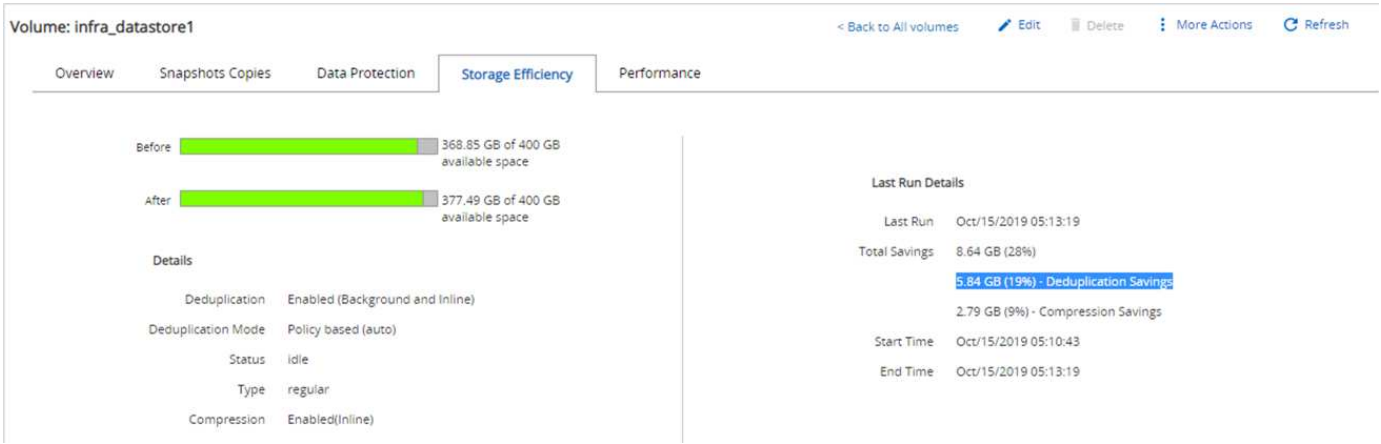
La seguente schermata mostra i file sulla condivisione CIFS `fpolicy_share` Che non sono ancora stati crittografati dal malware WannaCry.



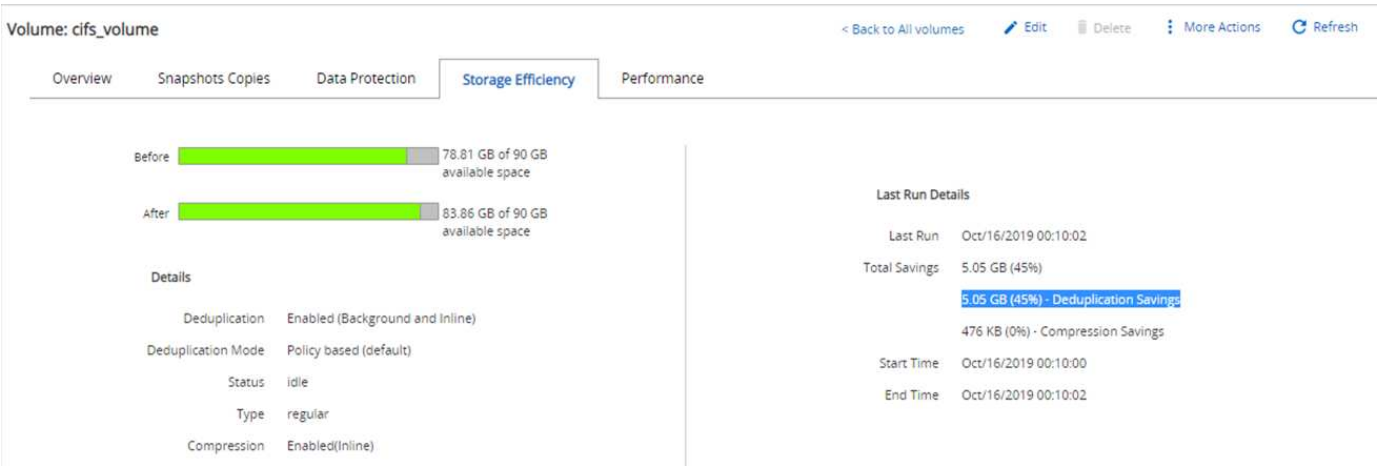
Deduplica e informazioni Snapshot prima di un attacco

I dettagli sull'efficienza dello storage e le dimensioni della copia Snapshot prima di un attacco vengono indicati e utilizzati come riferimento durante la fase di rilevamento.

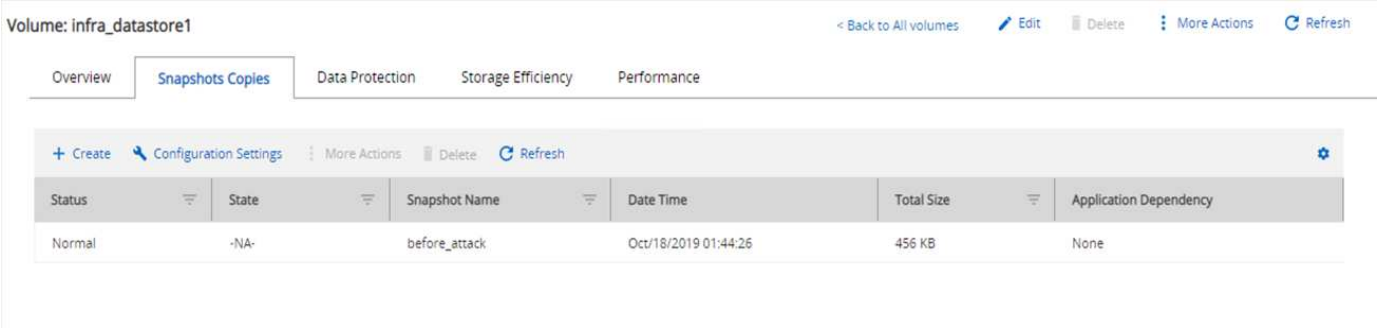
Grazie alla deduplica sul volume che ospita la macchina virtuale, sono stati ottenuti risparmi dello storage del 19%.



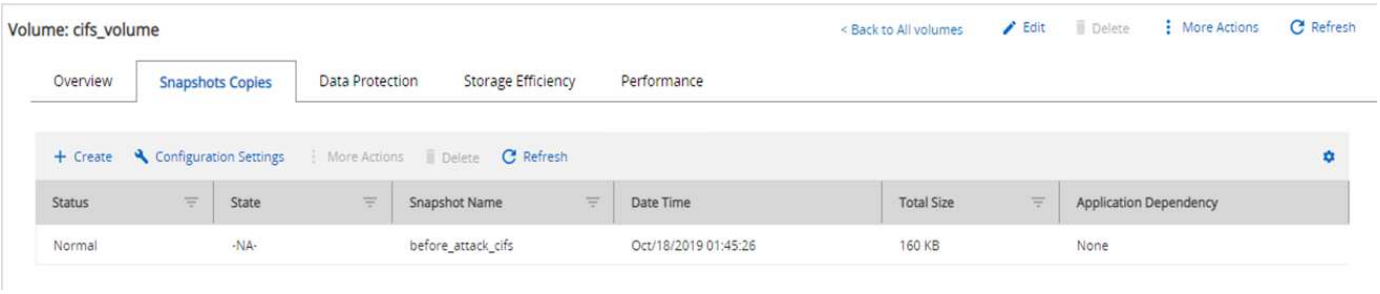
Con la deduplica sulla condivisione CIFS sono stati ottenuti risparmi dello storage del 45% `fpolicy_share`.



È stata rilevata una dimensione della copia Snapshot di 456 KB per il volume che ospita la macchina virtuale.



Per la condivisione CIFS è stata osservata una dimensione della copia Snapshot di 160 KB `fpolicy_share`.



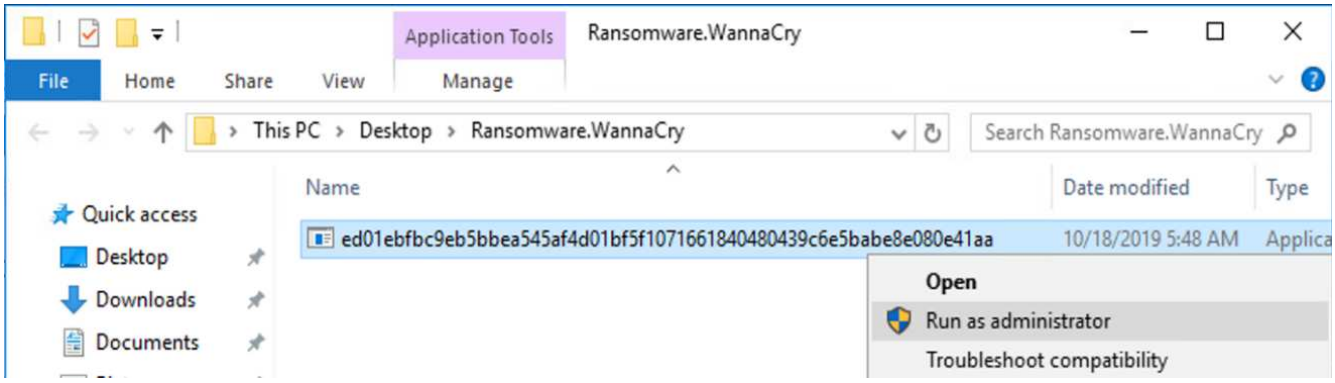
Infezione WannaCry su VM e condivisione CIFS

In questa sezione viene illustrato come il malware WannaCry è stato introdotto nell'ambiente FlexPod e le successive modifiche apportate al sistema.

I seguenti passaggi dimostrano come il malware binario WannaCry è stato introdotto nella macchina virtuale:

1. Il malware protetto è stato estratto.

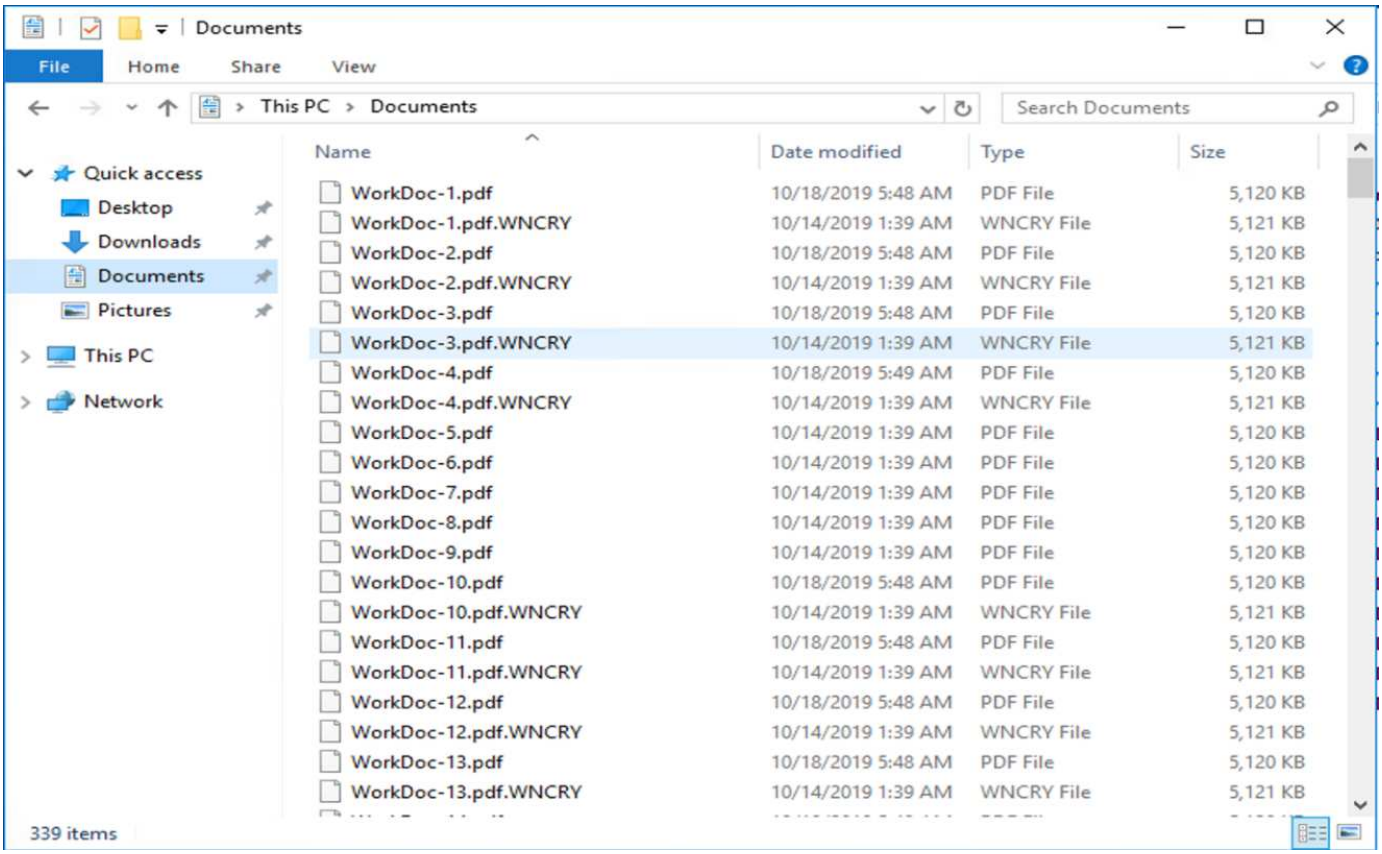
2. Il binario è stato eseguito.



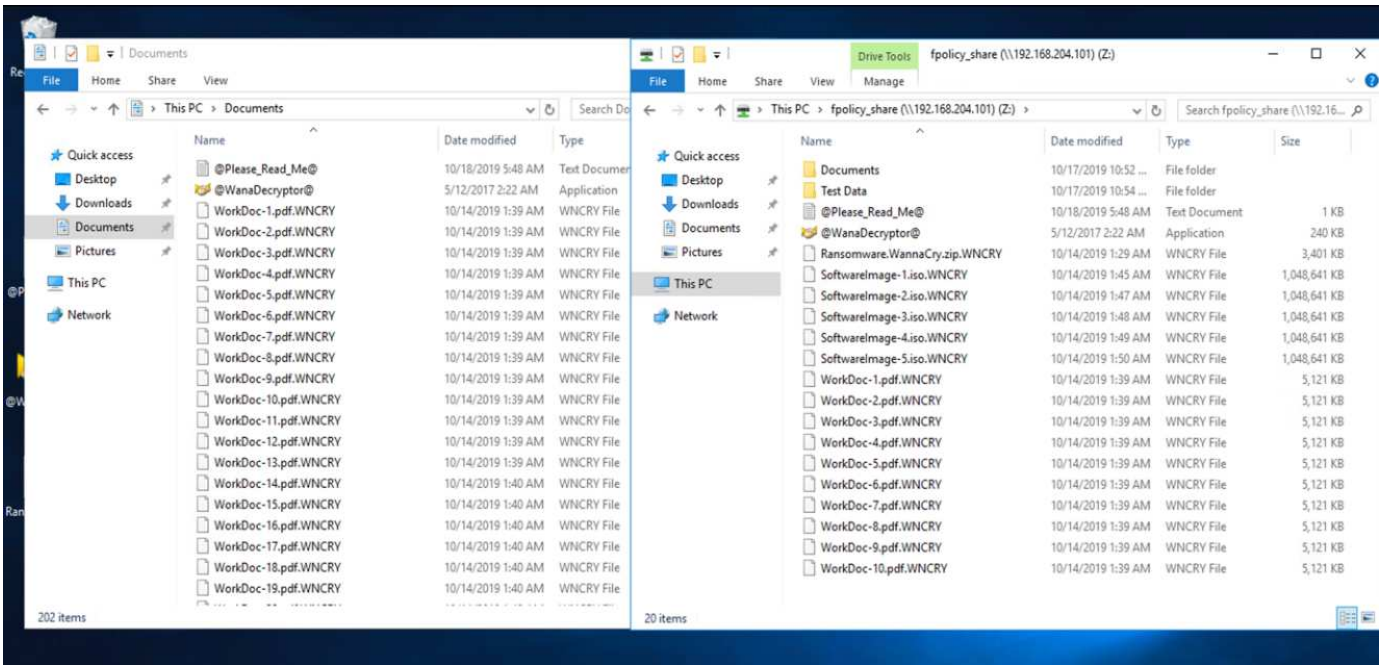
Caso 1: WannaCry crittografa il file system all'interno della VM e della condivisione CIFS mappata

Il file system locale e la condivisione CIFS mappata sono stati crittografati dal malware WannaCry.

Il malware inizia a crittografare i file con estensioni WNCRY.



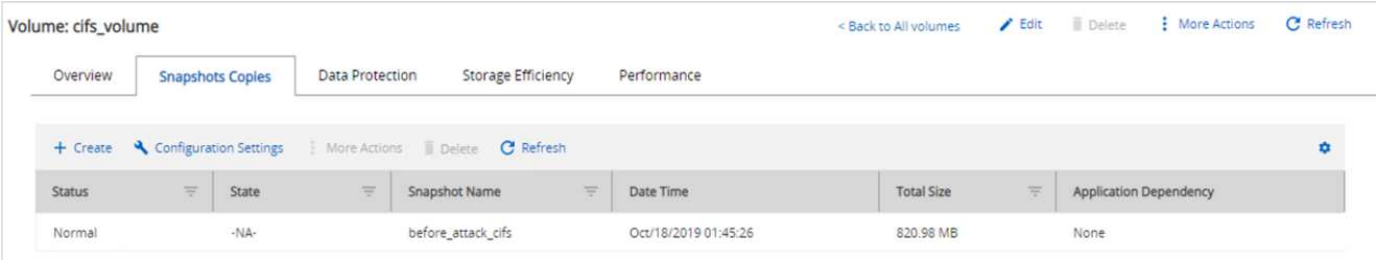
Il malware crittografa tutti i file nella VM locale e nella condivisione mappata.



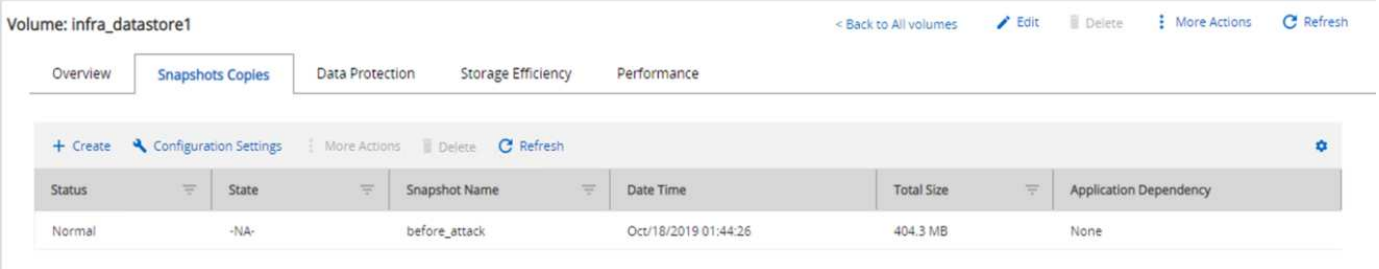
Rilevamento

Dal momento in cui il malware ha iniziato a crittografare i file, ha generato un aumento esponenziale delle dimensioni delle copie Snapshot e una diminuzione esponenziale della percentuale di efficienza dello storage.

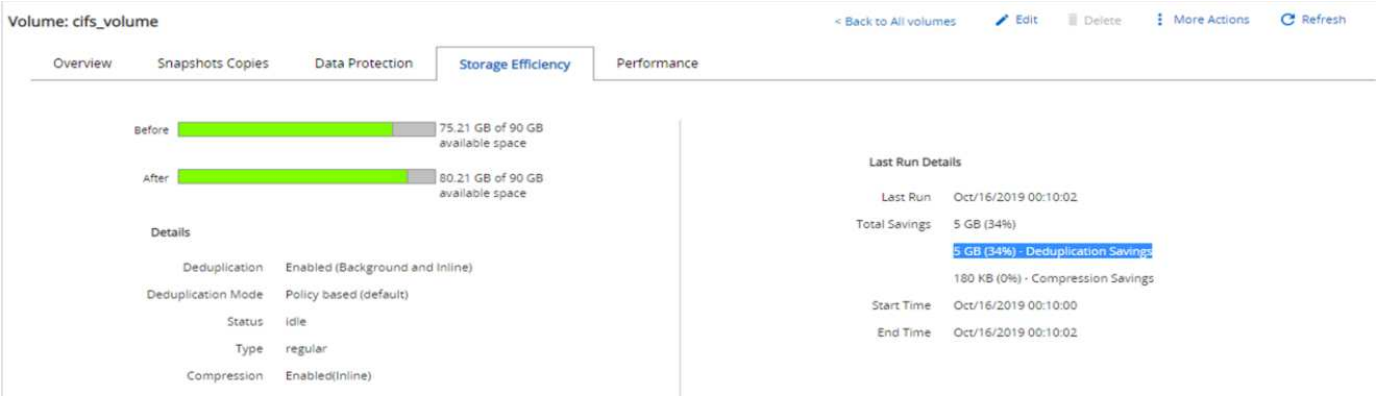
Durante l'attacco, è stato rilevato un notevole aumento delle dimensioni di Snapshot fino a 820,98 MB per il volume che ospita la condivisione CIFS.



È stato rilevato un aumento delle dimensioni della copia Snapshot fino a 404,3 MB per il volume che ospita la macchina virtuale.



L'efficienza dello storage per il volume che ospita la condivisione CIFS è scesa al 34%.



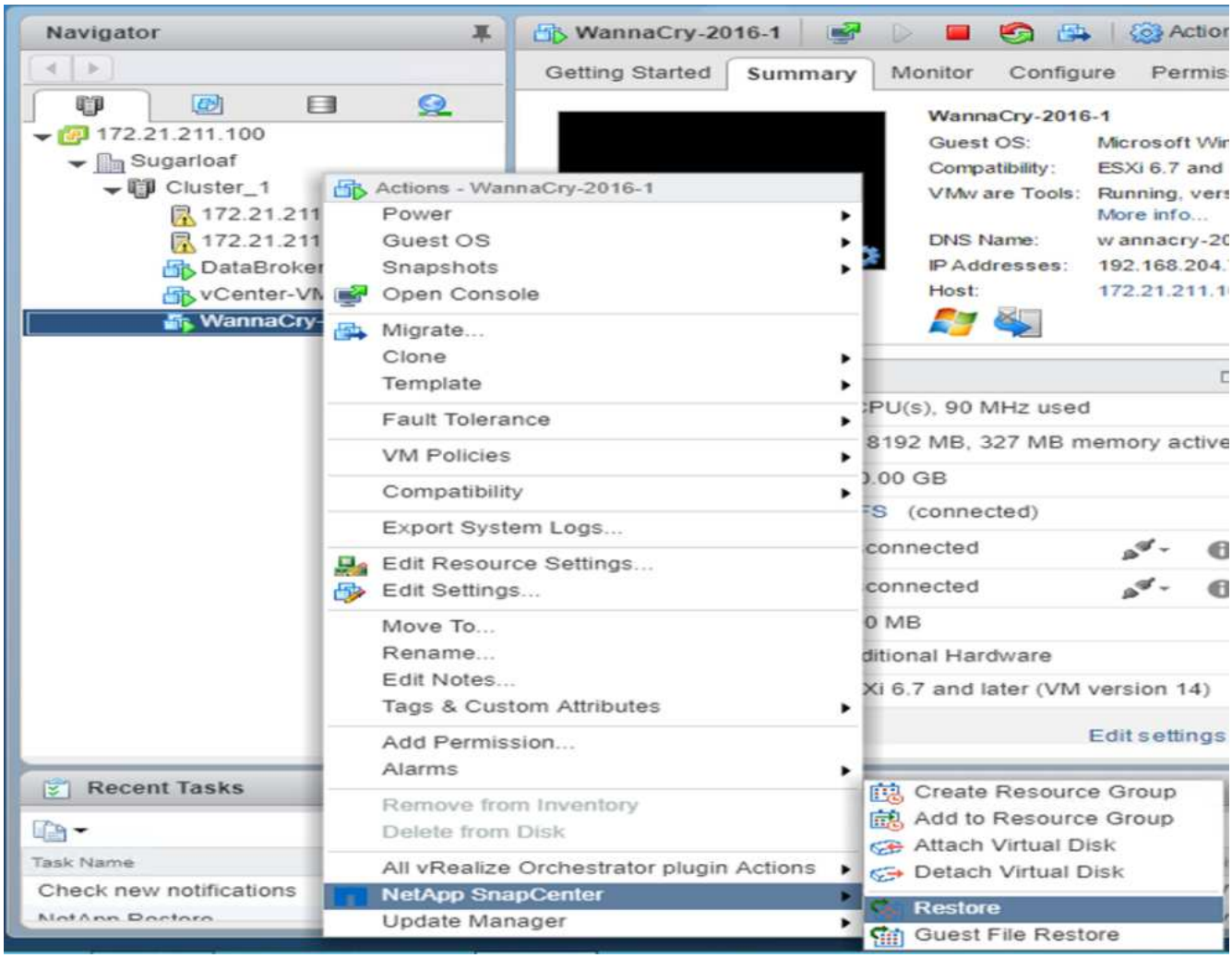
Risoluzione dei problemi

Ripristinare la VM e la condivisione CIFS mappata utilizzando una copia Snapshot pulita creata prima dell'attacco.

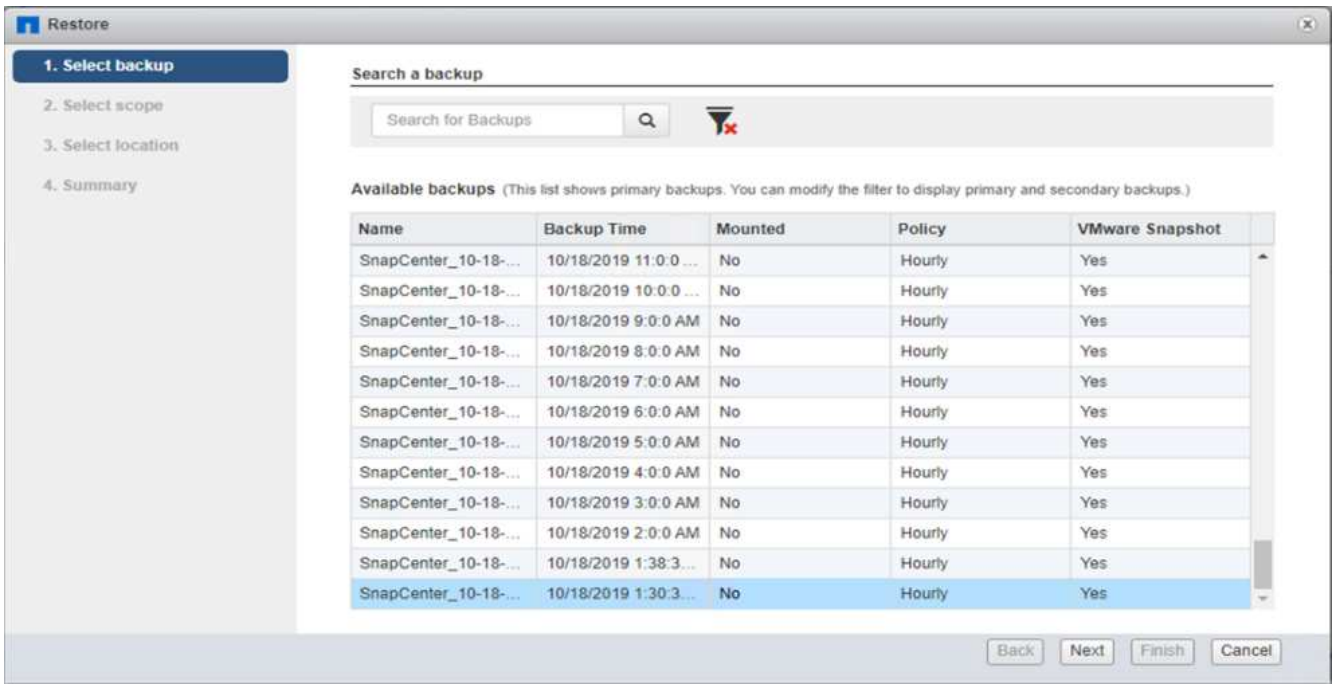
Ripristinare la macchina virtuale

Per ripristinare la macchina virtuale, attenersi alla seguente procedura:

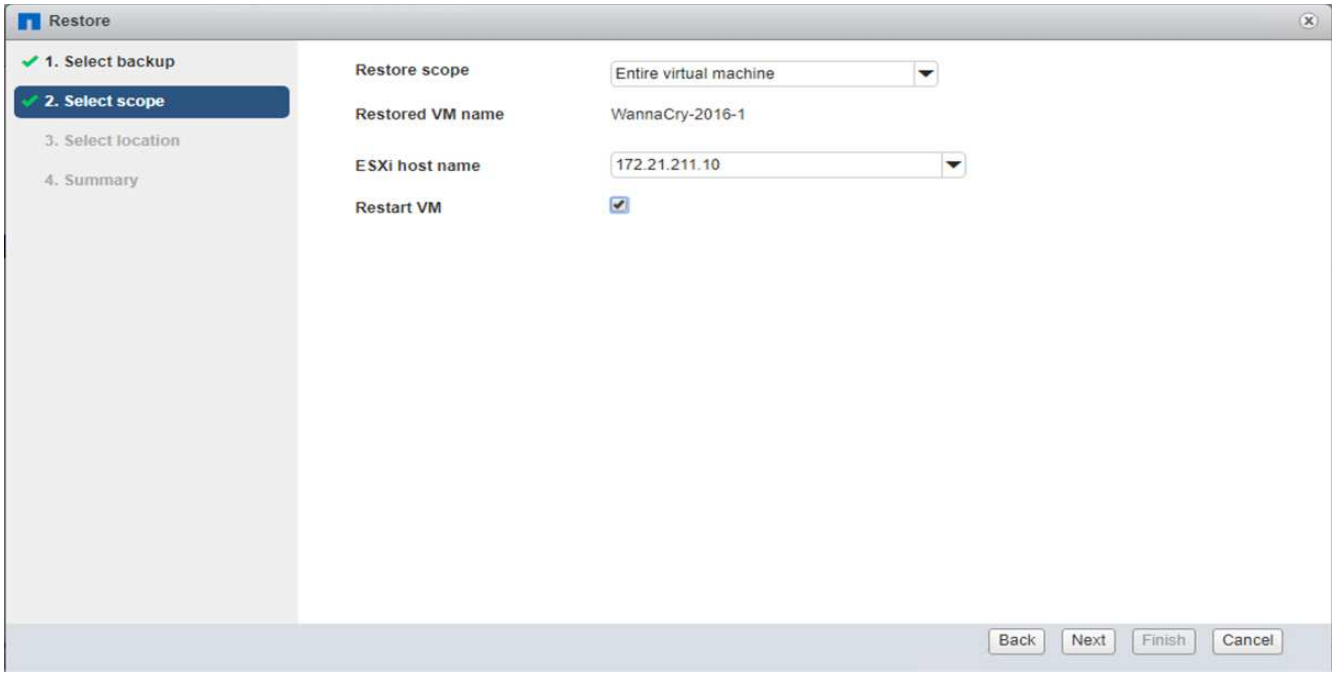
1. Utilizzare la copia Snapshot creata con SnapCenter per ripristinare la macchina virtuale.



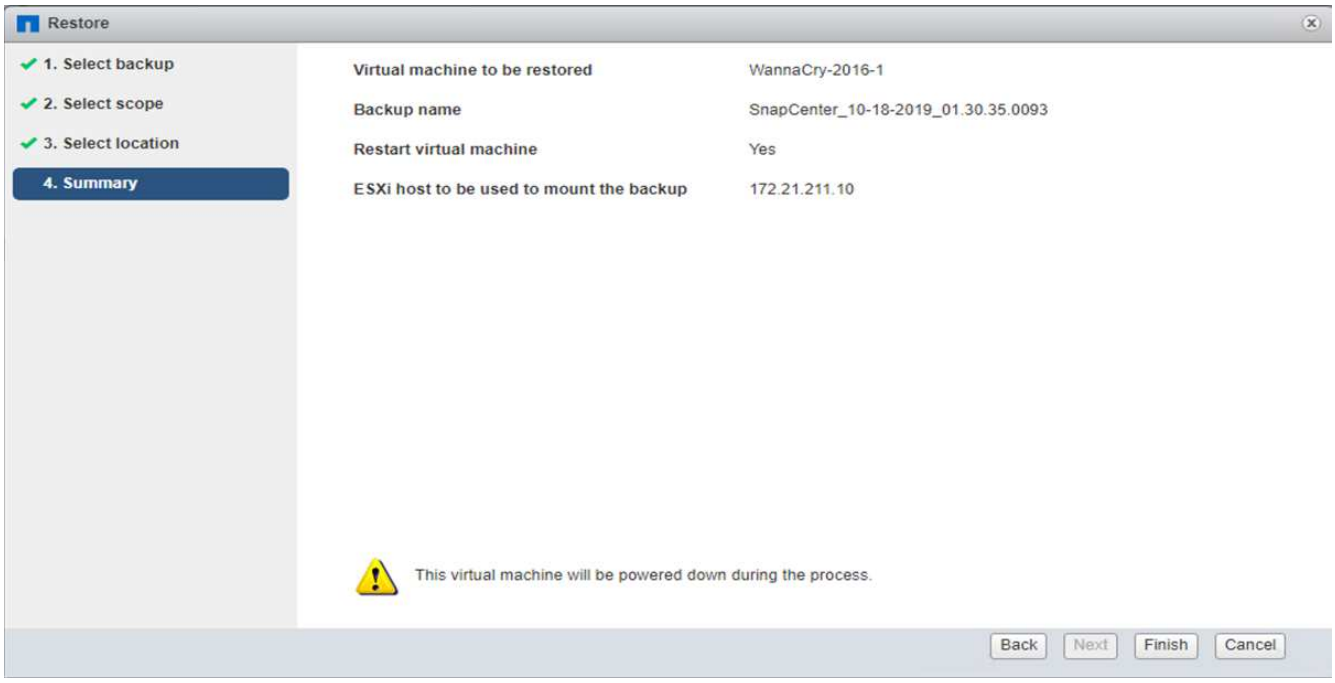
2. Selezionare la copia Snapshot coerente VMware desiderata per il ripristino.



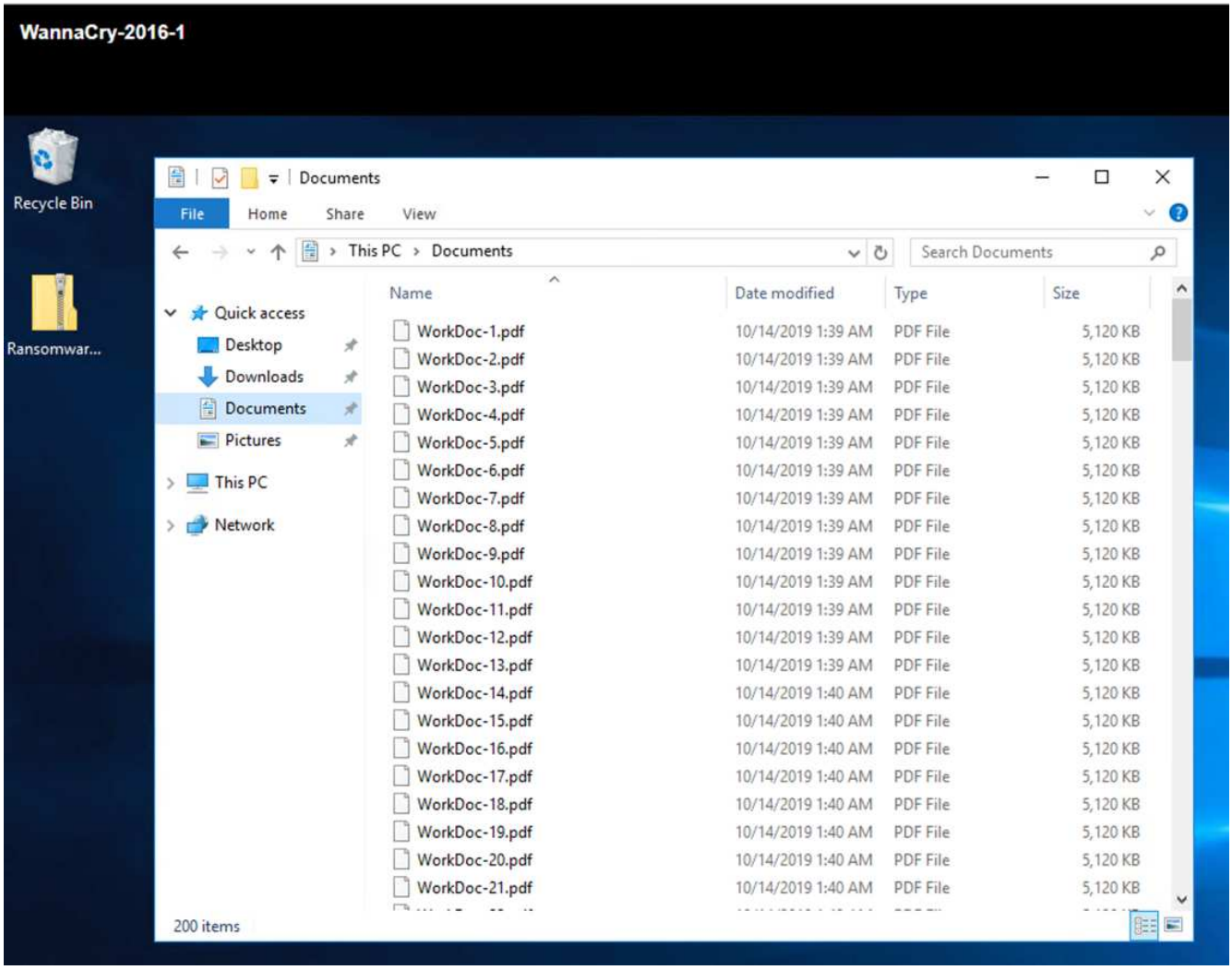
3. L'intera macchina virtuale viene ripristinata e riavviata.



4. Fare clic su Finish (fine) per avviare il processo di ripristino.



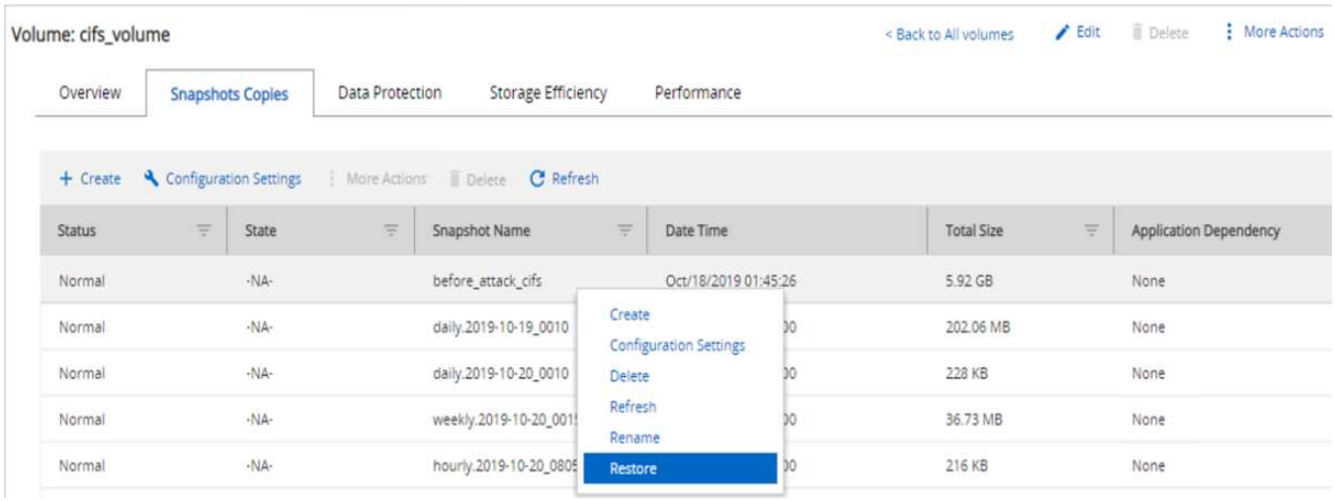
5. La macchina virtuale e i relativi file vengono ripristinati.



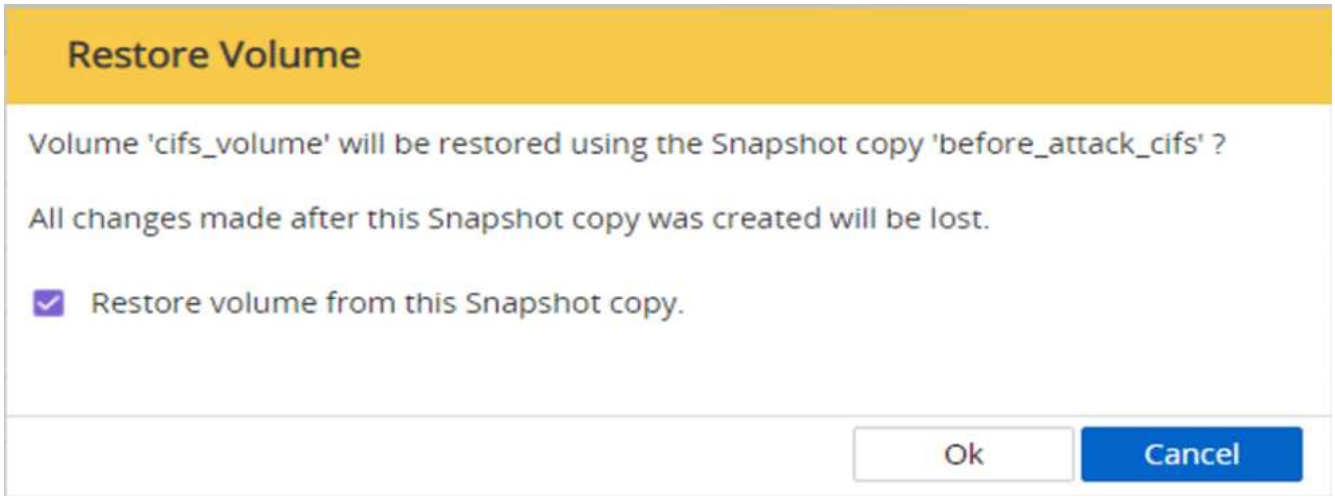
Ripristina condivisione CIFS

Per ripristinare la condivisione CIFS, attenersi alla seguente procedura:

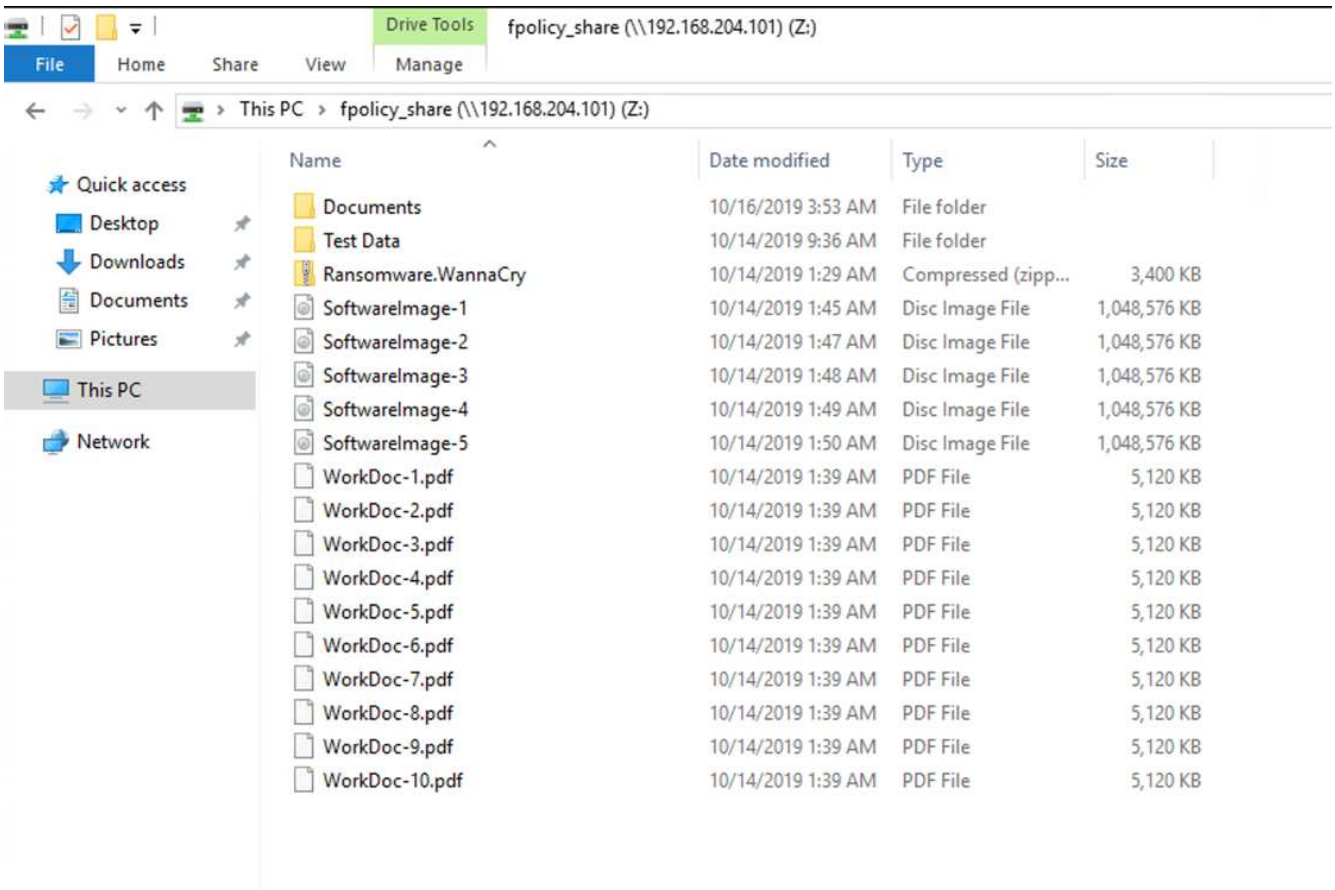
1. Utilizzare la copia Snapshot del volume preso prima dell'attacco per ripristinare la condivisione.



2. Fare clic su OK per avviare l'operazione di ripristino.



3. Visualizzare la condivisione CIFS dopo il ripristino.



Caso 2: WannaCry crittografa il file system all'interno della macchina virtuale e tenta di crittografare la condivisione CIFS mappata protetta tramite FPolicy

Prevenzione

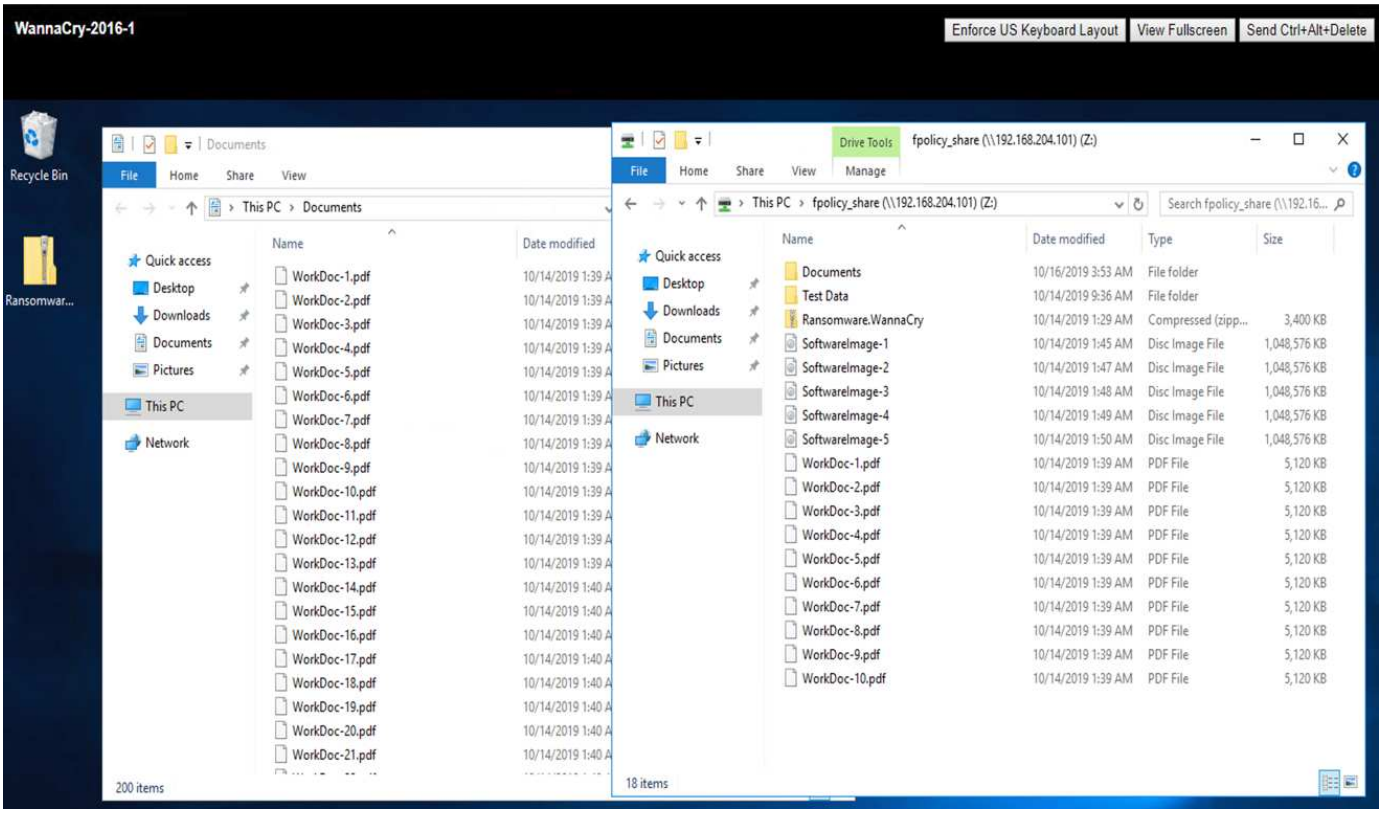
Configura FPolicy

Per configurare FPolicy sulla condivisione CIFS, eseguire i seguenti comandi sul cluster ONTAP:

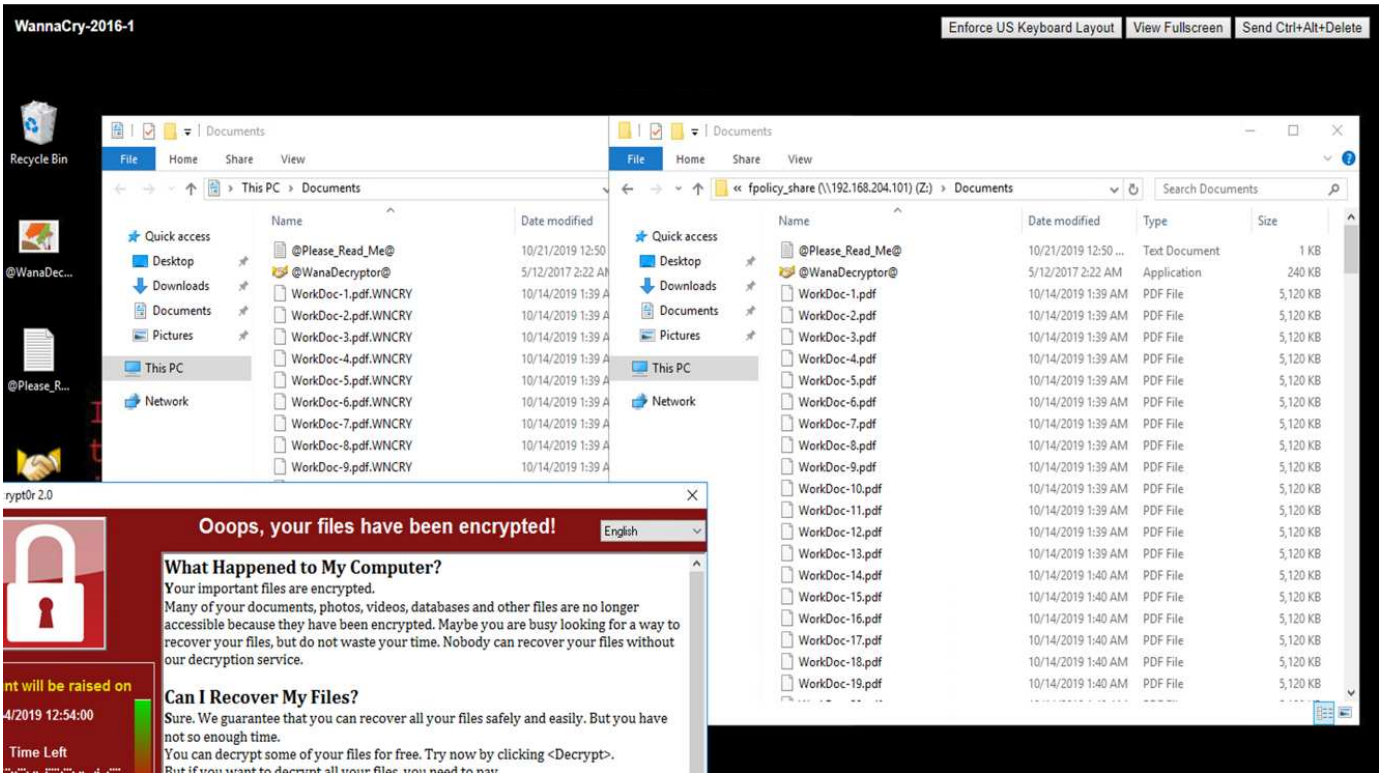
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -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 questo criterio, ai file con estensioni WNCRY, Locky e ad4c non è consentito eseguire le operazioni di creazione, ridenominazione, scrittura o apertura dei file.

Visualizzare lo stato dei file prima dell'attacco: Sono non crittografati e in un sistema pulito.



I file sulla macchina virtuale sono crittografati. Il malware WannaCry tenta di crittografare i file nella condivisione CIFS, ma FPolicy impedisce che influiscano sui file.



Continua le operazioni di business senza pagare il riscatto

Le funzionalità di NetApp descritte in questo documento consentono di ripristinare i dati entro pochi minuti dopo un attacco e prevenire gli attacchi, in modo da poter continuare le operazioni di business senza ostacoli.

È possibile impostare un programma di copia Snapshot per soddisfare l'obiettivo RPO (Recovery Point Objective) desiderato. Le operazioni di ripristino basate su copia Snapshot sono molto rapide, pertanto è possibile raggiungere un obiettivo RTO (Recovery Time Objective) molto basso.

Soprattutto, non è necessario pagare alcun riscatto a seguito di un attacco e si può tornare rapidamente alle operazioni regolari.

Conclusione

Ransomware è un prodotto di crimine organizzato e gli autori degli attacchi non operano con l'etica. Possono astenersi dal fornire la chiave per la decifratura anche dopo aver ricevuto il riscatto. La vittima non solo perde i propri dati, ma anche una notevole quantità di denaro e si trova ad affrontare le conseguenze associate alla perdita dei dati di produzione.

Secondo a. "Articolo di Forbes", solo il 19% delle vittime del ransomware ottiene i propri dati dopo aver pagato il riscatto. Pertanto, gli autori consigliano di non pagare un riscatto in caso di attacco, in quanto ciò rafforza la fiducia dell'utente malintenzionato nel proprio modello di business.

Le operazioni di backup e ripristino dei dati svolgono una parte importante del ripristino ransomware. Pertanto, devono essere inclusi come parte integrante della pianificazione aziendale. L'implementazione di queste operazioni deve essere preventivata in modo da non compromettere le funzionalità di recovery in caso di attacco.

La chiave è scegliere il partner tecnologico corretto in questo percorso e FlexPod fornisce la maggior parte delle funzionalità necessarie in modo nativo senza costi aggiuntivi in un sistema FAS all-flash.

Ringraziamenti

L'autore desidera ringraziare le seguenti persone per il loro supporto nella creazione di questo documento:

- Jorge Gomez Navarrete, NetApp
- Ganesh Kamath, NetApp

Ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Software NetApp Snapshot

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

- Gestione del backup di SnapCenter

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

- Conformità dei dati SnapLock

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

- Documentazione sui prodotti 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 Stealthwatch

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

Soluzione FlexPod conforme alla sicurezza FIPS 140-2 per il settore sanitario

TR-4892: Soluzione FlexPod conforme alla sicurezza FIPS 140-2 per il settore sanitario

JayaKishore Esanakula, NetApp John McAbel, Cisco

La Health Information Technology for Economic and Clinical Health Act (HITECH) richiede una crittografia certificata FIPS (Federal Information Processing Standard) 140-2 di ePHI (Electronic Protected Health Information). Le applicazioni e il software HIT

(Health Information Technology) devono essere conformi a FIPS 140-2 per ottenere la certificazione Promoving Interoperability Program (in precedenza significativo programma di incentivi per l'utilizzo). I fornitori e gli ospedali idonei devono utilizzare un HIT conforme a FIPS 140-2 (livello 1) per ricevere gli incentivi Medicare e Medicaid e per evitare le sanzioni per il rimborso da parte del Center for Medicare and Medicaid (CMS). Gli algoritmi di crittografia certificati FIPS 140-2 si qualificano come protezioni tecniche richieste in base a. "Regola di sicurezza" Del Health Information Portability and Accountability Act (HIPAA).

FIPS 140-2 è un standard governativo che definisce i requisiti di sicurezza per i moduli crittografici in hardware, software e firmware che proteggono le informazioni sensibili. La conformità allo standard è richiesta per l'utilizzo da parte degli Stati Uniti enti governativi, e spesso viene utilizzato anche in settori regolamentati come i servizi finanziari e l'assistenza sanitaria. Questo report tecnico aiuta il lettore a comprendere lo standard di sicurezza FIPS 140-2 ad alto livello. Inoltre, aiuta il pubblico a comprendere le varie minacce affrontate dalle organizzazioni sanitarie. Infine, il report tecnico aiuta a capire come un sistema FlexPod conforme a FIPS 140-2 può contribuire a proteggere le risorse sanitarie quando viene implementato su un'infrastruttura convergente FlexPod.

Scopo

Questo documento è una panoramica tecnica di un'infrastruttura FlexPod basata su Cisco Unified Computing System (Cisco UCS), Cisco Nexus, Cisco MDS e NetApp ONTAP per ospitare una o più applicazioni IT per il settore sanitario o soluzioni che richiedono la conformità alla sicurezza FIPS 140-2.

Pubblico

Il presente documento è destinato ai responsabili tecnici del settore sanitario, ai tecnici delle soluzioni partner Cisco e NetApp e al personale dei servizi professionali. NetApp presuppone che il lettore abbia una buona comprensione dei concetti di dimensionamento di calcolo e storage, nonché una familiarità tecnica con le minacce per il settore sanitario, la sicurezza sanitaria, i sistemi IT per il settore sanitario, Cisco UCS e i sistemi storage NetApp.

"Avanti: Minacce alla cybersicurezza nel settore sanitario."

Minacce alla cybersicurezza nel settore sanitario

"Precedente: Introduzione."

Ogni problema presenta una nuova opportunità: Un esempio di tale opportunità è rappresentato dalla pandemia di COVID. Secondo a. "report" Dal programma Cybersecurity del Department of Health and Human Services (HHS), la risposta COVID ha portato a un aumento del numero di attacchi ransomware. Ci sono stati 6,000 nuovi domini internet registrati solo nella terza settimana di marzo 2020. Oltre il 50% dei domini ospitava malware. Gli attacchi ransomware sono stati responsabili di quasi il 50% di tutte le violazioni dei dati sanitari nel 2020 che hanno colpito più di 630 organizzazioni sanitarie e circa 29 milioni di cartelle cliniche. Diciannove leakers/siti hanno raddoppiato l'estorsione. Con il 24.5%, il settore sanitario ha registrato il maggior numero di violazioni dei dati nel 2020.

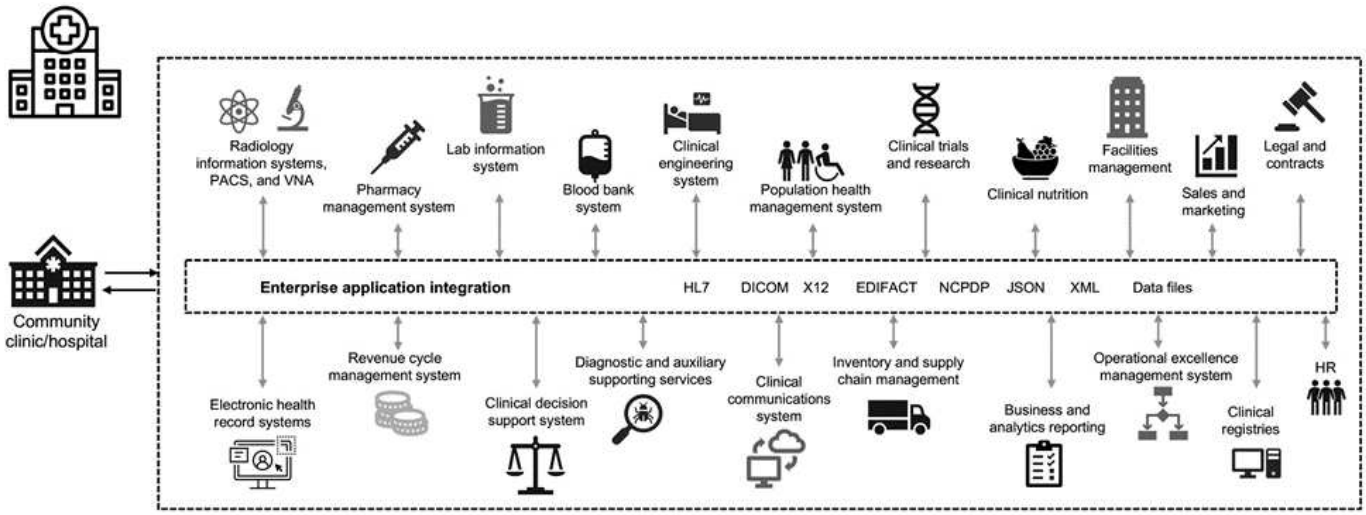
Gli agenti dannosi hanno tentato di violare la sicurezza e la privacy delle informazioni sanitarie protette (PHI)

vendendo le informazioni o minacciando di distruggerle o di esporle. Spesso vengono effettuati tentativi mirati e di trasmissione di massa per ottenere un accesso non autorizzato a ePHI. Circa il 75% delle cartelle cliniche dei pazienti esposte nella seconda metà del 2020 era dovuto a dipendenti aziendali compromessi.

Il seguente elenco di organizzazioni sanitarie è stato preso di mira dagli agenti dannosi:

- Sistemi ospedalieri
- Laboratori di life science
- Laboratori di ricerca
- Strutture di riabilitazione
- Ospedali e cliniche della comunità

La diversità delle applicazioni che costituiscono un'organizzazione sanitaria è innegabile e sempre più complessa. Gli uffici per la sicurezza delle informazioni devono fornire una governance per la vasta gamma di sistemi E risorse IT. La figura seguente illustra le funzionalità cliniche di un sistema ospedaliero tipico.



I dati dei pazienti sono al centro dell'immagine. La perdita dei dati dei pazienti e lo stigma associato a condizioni mediche sensibili sono molto reali. Altri problemi sensibili includono il rischio di esclusione sociale, ricatti, profiling, vulnerabilità al marketing mirato, sfruttamento e potenziale responsabilità finanziaria nei confronti dei pagatori in merito alle informazioni mediche al di là dei privilegi del pagatore.

Le minacce per l'assistenza sanitaria sono di natura multidimensionale e di impatto. I governi di tutto il mondo hanno adottato varie disposizioni per garantire ePHI. Gli effetti negativi e la natura in evoluzione delle minacce per l'assistenza sanitaria rendono difficile per le organizzazioni sanitarie difendere tutte le minacce.

Di seguito viene riportato un elenco delle minacce più comuni identificate nel settore sanitario:

- Attacchi ransomware
- Perdita o furto di apparecchiature o dati con informazioni sensibili
- Attacchi di phishing
- Attacchi contro i dispositivi medici collegati che possono compromettere la sicurezza del paziente
- Attacchi di phishing via e-mail
- Perdita o furto di apparecchiature o dati
- Compromissione del protocollo del desktop remoto

- Vulnerabilità del software

Le organizzazioni del settore sanitario operano in un ambiente legale e normativo complicato quanto i loro ecosistemi digitali. Questo ambiente include, a titolo esemplificativo e non esaustivo, i seguenti elementi:

- Office of the National Coordinator (for Healthcare Technology) Standard di interoperabilità con Electronic Health Information Technology con certificazione ONC
- Medicare Access e il Children's Health Insurance Program ReAuthorization Act (MACRA)/uso significativo
- Obblighi multipli ai sensi della Food and Drug Administration (FDA)
- I processi di accreditamento della Joint Commission
- Requisiti HIPAA
- Requisiti HITECH
- Standard minimi di rischio accettabili per i pagatori
- Norme di sicurezza e privacy statali
- Requisiti del Federal Information Security Modernization Act come incorporati nei contratti federali e nelle borse di ricerca attraverso agenzie come gli istituti nazionali di salute
- Payment Card Industry Data Security Standard (PCI-DSS)
- Requisiti relativi all'abuso di sostanze e all'amministrazione dei servizi di salute mentale (SAMHSA)
- Il Gramm-Leach-Bliley Act per l'elaborazione finanziaria
- La legge di Stark in relazione alla fornitura di servizi alle organizzazioni affiliate
- Family Educational Rights and Privacy Act (FERPA) per le istituzioni che partecipano all'istruzione superiore
- Genetic Information Nondiscrimination Act (GINA)
- Il nuovo regolamento generale sulla protezione dei dati (GDPR) nell'Unione europea

Gli standard dell'architettura di sicurezza sono in rapida evoluzione per impedire agli attori malintenzionati di influire sui sistemi informativi sanitari. Uno di questi standard è FIPS 140-2, definito dal National Institute of Standards and Technology (NIST). La pubblicazione FIPS 140-2 descrive in dettaglio gli Stati Uniti requisiti governativi per un modulo crittografico. I requisiti di sicurezza coprono le aree correlate a una progettazione sicura e all'implementazione di un modulo crittografico e possono essere applicati a HIT. I confini crittografici ben definiti consentono una gestione più semplice della sicurezza, mantenendo al contempo aggiornati i moduli crittografici. Questi limiti aiutano a prevenire i deboli moduli di crittografia che possono essere facilmente sfruttati da utenti malintenzionati. Inoltre, possono contribuire a prevenire gli errori umani durante la gestione dei moduli crittografici standard.

NIST insieme a Communications Security Establishment (CSE) hanno definito il programma di convalida del modulo crittografico (CMVP) per certificare i moduli crittografici per i livelli di convalida FIPS 140-2. Utilizzando un modulo certificato FIPS 140-2, le organizzazioni federali devono proteggere i dati sensibili o preziosi mentre sono a riposo e in movimento. A causa del suo successo nella protezione di informazioni sensibili o preziose, molti sistemi sanitari hanno scelto di crittografare ePHI utilizzando i moduli crittografici FIPS 140-2 oltre il livello minimo di sicurezza richiesto dalla legge.

Sfruttare e implementare le funzionalità FIPS 140-2 di FlexPod richiede solo ore (non giorni). La conformità FIPS è a portata di mano per la maggior parte delle organizzazioni sanitarie, indipendentemente dalle dimensioni. Con confini crittografici chiaramente definiti e semplici fasi di implementazione ben documentate, un'architettura FlexPod conforme a FIPS 140-2 può creare una solida base di sicurezza per l'infrastruttura e consentire semplici miglioramenti per aumentare ulteriormente la protezione per le minacce alla sicurezza.

"Pagina successiva: Panoramica di FIPS 140-2."

Panoramica di FIPS 140-2

"Precedente: Minacce alla cybersicurezza nel settore sanitario."

"FIPS 140-2" specifica i requisiti di sicurezza per un modulo crittografico utilizzato all'interno di un sistema di sicurezza che protegge le informazioni sensibili nei sistemi informatici e di telecomunicazione. Un modulo crittografico deve essere un insieme di hardware, software, firmware o una combinazione. FIPS si applica agli algoritmi di crittografia, alla generazione delle chiavi e ai gestori delle chiavi contenuti all'interno di un confine crittografico. È importante comprendere che FIPS 140-2 si applica specificamente al modulo crittografico, non al prodotto, all'architettura, ai dati o all'ecosistema. Il modulo crittografico, definito nei termini chiave più avanti in questo documento, è il componente specifico (hardware, software e/o firmware) che implementa le funzioni di sicurezza approvate. Inoltre, FIPS 140-2 specifica quattro livelli. Gli algoritmi crittografici approvati sono comuni a tutti i livelli. Gli elementi e i requisiti chiave di ciascun livello di sicurezza includono:

- **Livello di sicurezza 1**
  - Specifica i requisiti di sicurezza di base per un modulo crittografico (è richiesto almeno un algoritmo approvato o una funzione di sicurezza).
  - Per il livello 1 non sono necessari meccanismi di sicurezza fisici specifici oltre i requisiti di base per i componenti di livello di produzione.
- **Livello di sicurezza 2**
  - Migliora i meccanismi di sicurezza fisica aggiungendo il requisito per l'evidenza di manomissione utilizzando soluzioni antimanomissione come rivestimenti o sigilli, blocchi su coperture rimovibili o porte dei moduli crittografici.
  - Richiede, come minimo, il RBAC (role-based access control) in cui il modulo crittografico autentica l'autorizzazione di un operatore o amministratore ad assumere un ruolo specifico ed eseguire un set corrispondente di funzioni.
- **Livello di sicurezza 3**
  - Si basa sui requisiti di antimanomissione del livello 2 e tenta di impedire un ulteriore accesso ai parametri di sicurezza critici (CSP) all'interno del modulo crittografico.
  - I meccanismi di sicurezza fisici richiesti al livello 3 hanno un'elevata probabilità di rilevare e rispondere a tentativi di accesso fisico o a qualsiasi utilizzo o modifica del modulo crittografico. Ad esempio, enclosure potenti, rilevamento delle manomissioni e circuiti di risposta che azzerano tutti i CSP non crittografati quando viene aperto un coperchio rimovibile sul modulo crittografico.
  - Richiede meccanismi di autenticazione basati sull'identità per migliorare la sicurezza dei meccanismi RBAC specificati nel livello 2. Un modulo crittografico autentica l'identità di un operatore e verifica che l'operatore sia autorizzato a utilizzare un ruolo ed eseguire le funzioni del ruolo.
- **Livello di sicurezza 4**
  - Il massimo livello di sicurezza in FIPS 140-2.
  - Il livello più utile per le operazioni in ambienti fisicamente non protetti.
  - A questo livello, i meccanismi di sicurezza fisica sono progettati per fornire una protezione completa intorno al modulo crittografico con la responsabilità di rilevare e rispondere a qualsiasi tentativo non

autorizzato di accesso fisico.

- La penetrazione o l'esposizione del modulo crittografico deve avere un'elevata probabilità di rilevamento e determinare l'azzeramento immediato di tutti i CSP non sicuri o non crittografati.

"Avanti: Piano di controllo rispetto al piano dati."

Piano di controllo rispetto al piano dati

"Precedente: Panoramica di FIPS 140-2."

Quando si implementa una strategia FIPS 140-2, è importante comprendere cosa viene protetto. Questo può essere facilmente suddiviso in due aree: Piano di controllo e piano dati. Un piano di controllo si riferisce agli aspetti che influiscono sul controllo e sul funzionamento dei componenti all'interno del sistema FlexPod: Ad esempio, l'accesso amministrativo ai controller di storage NetApp, agli switch Cisco Nexus e ai server Cisco UCS. La protezione a questo livello viene fornita limitando i protocolli e i crittografia che gli amministratori possono utilizzare per connettersi ai dispositivi e apportare modifiche. Un piano di dati si riferisce alle informazioni effettive, come il PHI, all'interno del sistema FlexPod. Questo è protetto crittografando i dati a riposo e di nuovo per FIPS, garantendo che i moduli crittografici in uso soddisfino gli standard.

"Avanti: Calcolo Cisco UCS e FIPS 140-2 di FlexPod."

Cisco UCS Compute e FIPS 140-2 di FlexPod

"Precedente: Piano di controllo rispetto al piano dati."

Un'architettura FlexPod può essere progettata con un server Cisco UCS conforme a FIPS 140-2. In conformità con il brevetto U. S. NIST, il server Cisco UCS può funzionare in modalità di conformità FIPS 140-2 livello 1. Per un elenco completo dei componenti Cisco conformi a FIPS, vedere "Pagina FIPS 140 di Cisco". Cisco UCS Manager è validato FIPS 140-2.

Cisco UCS e Fabric Interconnect

Cisco UCS Manager viene implementato ed eseguito da Cisco Fabric Interconnects (IF).

Per ulteriori informazioni su Cisco UCS e su come attivare FIPS, consultare "Documentazione di Cisco UCS Manager".

Per attivare la modalità FIPS sull'interconnessione fabric Cisco su ciascun fabric A e B, eseguire i seguenti comandi:

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

> Per sostituire un Fi in un cluster su Cisco UCS Manager versione 3.2(3) con un Fi su una release precedente a Cisco UCS Manager versione 3.2(3), disattivare la modalità FIPS (disattivare `fips-mode`) Sul Fi esistente prima di aggiungere il Fi sostitutivo al cluster. Una volta creato il cluster, durante l'avvio di Cisco UCS Manager, la modalità FIPS viene attivata automaticamente.

Cisco offre i seguenti prodotti chiave che possono essere implementati a livello di elaborazione o applicazione:

- **Cisco Advanced malware Protection (AMP) per endpoint.** supportata sui sistemi operativi Microsoft Windows e Linux, questa soluzione integra funzionalità di prevenzione, rilevamento e risposta. Questo software di sicurezza previene le violazioni, blocca il malware nel punto di ingresso e monitora e analizza continuamente le attività di file e processi per rilevare, contenere e rimediare rapidamente alle minacce che possono eludere le difese front-line. Il componente di protezione delle attività dannose (MAP) di AMP monitora continuamente tutte le attività degli endpoint e fornisce il rilevamento in fase di esecuzione e il blocco del comportamento anomalo di un programma in esecuzione sull'endpoint. Ad esempio, quando il comportamento degli endpoint indica ransomware, i processi in errore vengono terminati, impedendo la crittografia degli endpoint e arrestando l'attacco.
- **AMP per la sicurezza della posta elettronica.** le e-mail sono diventate il mezzo principale per diffondere malware e per eseguire cyberattacchi. In media, circa 100 miliardi di e-mail vengono scambiate in un solo giorno, il che fornisce agli autori degli attacchi un eccellente vettore di penetrazione nei sistemi degli utenti. Pertanto, è assolutamente essenziale difendersi da questa linea di attacco. AMP analizza le e-mail per individuare minacce come exploit zero-day e malware furtivo nascosto in allegati dannosi. Utilizza inoltre l'intelligence URL leader del settore per combattere i collegamenti dannosi. Offre agli utenti una protezione avanzata contro il phishing, il ransomware e altri attacchi sofisticati.
- **Next- Generation Intrusion Prevention System (NGIPS).** Cisco firepower NGIPS può essere implementato come appliance fisica nel data center o come appliance virtuale su VMware (NGIPSv per VMware). Questo sistema di prevenzione delle intrusioni altamente efficace offre performance affidabili e un basso costo totale di proprietà. La protezione dalle minacce può essere estesa con licenze di abbonamento opzionali per fornire AMP, visibilità e controllo delle applicazioni e funzionalità di filtraggio degli URL. I NGIPS virtualizzati ispezionano il traffico tra macchine virtuali (VM) e semplificano l'implementazione e la gestione delle soluzioni NGIPS in siti con risorse limitate, aumentando la protezione per risorse fisiche e virtuali.

"Avanti: Rete Cisco FlexPod e FIPS 140-2."

Rete Cisco FlexPod e FIPS 140-2

"Precedente: Calcolo Cisco UCS FlexPod e FIPS 140-2."

Cisco MDS

Piattaforma Cisco MDS serie 9000 con software 8.4.x IS "Conforme a FIPS 140-2". Cisco MDS implementa moduli crittografici e i seguenti servizi per SNMPv3 e SSH.

- Creazione di una sessione a supporto di ciascun servizio
- Tutti gli algoritmi crittografici sottostanti che supportano le funzioni di derivazione delle chiavi di ciascun servizio
- Hashing per ogni servizio
- Crittografia simmetrica per ciascun servizio

Prima di attivare la modalità FIPS, completare le seguenti attività sullo switch MDS:

1. Impostare le password su una lunghezza minima di otto caratteri.
2. Disattiva Telnet. Gli utenti devono effettuare l'accesso solo tramite SSH.
3. Disattiva l'autenticazione remota tramite RADIUS/TACACS+. È possibile autenticare solo gli utenti locali dello switch.
4. Disattivare SNMP v1 e v2. Tutti gli account utente esistenti sullo switch configurati per SNMPv3 devono essere configurati solo con SHA per l'autenticazione e AES/3DES per la privacy.
5. Disattiva VRRP.
6. Eliminare tutti i criteri IKE che dispongono di MD5 per l'autenticazione o DES per la crittografia. Modificare i criteri in modo che utilizzino SHA per l'autenticazione e 3DES/AES per la crittografia.
7. Eliminare tutte le coppie di chiavi RSA1 di SSH Server.

Per attivare la modalità FIPS e visualizzare lo stato FIPS sullo switch MDS, attenersi alla seguente procedura:

1. Mostra lo stato FIPS.

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

2. Impostare la chiave SSH a 2048 bit.

```
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. Attivare la modalità 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. Mostra lo stato FIPS.

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

5. Salvare la configurazione nella configurazione in esecuzione.

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

6. Riavviare lo switch MDS

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

7. Mostra lo stato FIPS.

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

Per ulteriori informazioni, vedere "Attivazione della modalità FIPS".

Cisco Nexus

Gli switch Cisco Nexus serie 9000 (versione 9.3) sono "Conforme a FIPS 140-2". Cisco Nexus implementa moduli crittografici e i seguenti servizi per SNMPv3 e SSH.

- Creazione di una sessione a supporto di ciascun servizio
- Tutti gli algoritmi crittografici sottostanti che supportano le funzioni di derivazione delle chiavi di ciascun servizio

- Hashing per ogni servizio
- Crittografia simmetrica per ciascun servizio

Prima di attivare la modalità FIPS, completare le seguenti attività sullo switch Cisco Nexus:

1. Disattiva Telnet. Gli utenti devono effettuare l'accesso solo con Secure Shell (SSH).
2. Disattivare SNMPv1 e v2. Tutti gli account utente esistenti sul dispositivo configurati per SNMPv3 devono essere configurati solo con SHA per l'autenticazione e AES/3DES per la privacy.
3. Eliminare tutte le coppie di chiavi RSA1 del server SSH.
4. Abilitare il controllo dell'integrità del messaggio (MIC) HMAC-SHA1 da utilizzare durante la negoziazione del protocollo SAP (Security Association Protocol) Cisco TrustSec. A tale scopo, immettere l'algoritmo hash sap `HMAC-SHA-1` dal `cts-manual` oppure `cts-dot1x` modalità.

Per attivare la modalità FIPS sullo switch Nexus, attenersi alla seguente procedura:

1. Impostare una chiave SSH a 2048 bit.

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

2. Impostare la chiave SSH a 2048 bit.

```
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. Attivare la modalità 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. Riavviare lo switch Nexus.

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

5. Mostra lo stato FIPS.

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

Inoltre, il software Cisco NX OS supporta la funzione NetFlow che consente un rilevamento avanzato delle anomalie di rete e della sicurezza. NetFlow acquisisce i metadati di ogni conversazione sulla rete, le parti coinvolte nella comunicazione, il protocollo utilizzato e la durata della transazione. Una volta aggregate e analizzate le informazioni, possono fornire informazioni dettagliate sul comportamento normale. I dati raccolti consentono inoltre l'identificazione di modelli di attività dubbi, come la diffusione di malware nella rete, che altrimenti potrebbero passare inosservati. NetFlow utilizza i flussi per fornire statistiche per il monitoraggio della rete. Un flusso è un flusso unidirezionale di pacchetti che arriva su un'interfaccia di origine (o VLAN) e ha gli stessi valori per le chiavi. Una chiave è un valore identificato per un campo all'interno del pacchetto. Si crea un flusso utilizzando un record di flusso per definire le chiavi univoche per il flusso. È possibile esportare i dati raccolti da NetFlow per i flussi utilizzando un'esportazione di flusso in un NetFlow Collector remoto, ad esempio Cisco Stealthwatch. Stealthwatch utilizza queste informazioni per il monitoraggio continuo della rete e fornisce analisi forensi in tempo reale per il rilevamento delle minacce e la risposta agli incidenti in caso di scoppio di ransomware.

"Pagina successiva: Storage NetApp ONTAP e FIPS 140-2 di FlexPod."

Storage NetApp ONTAP e FIPS 140-2 di FlexPod

"Precedente: Rete Cisco FlexPod e FIPS 140-2."

NetApp offre una vasta gamma di hardware, software e servizi, che possono includere vari componenti dei moduli crittografici validati in base allo standard. Pertanto, NetApp utilizza una serie di approcci per la conformità FIPS 140-2 per il piano di controllo e il piano dati:

- NetApp include moduli crittografici che hanno ottenuto la convalida di livello 1 per la crittografia dei dati in transito e dei dati a riposo.
- NetApp acquisisce moduli hardware e software che sono stati convalidati FIPS 140-2 dai fornitori di tali componenti. Ad esempio, la soluzione NetApp Storage Encryption sfrutta dischi convalidati FIPS livello 2.
- I prodotti NetApp possono utilizzare un modulo validato in modo conforme allo standard anche se il prodotto o la funzionalità non rientra nei limiti della convalida. Ad esempio, NetApp Volume Encryption (NVE) è conforme a FIPS 140-2. Anche se non convalidato separatamente, sfrutta il modulo crittografico NetApp, validato al livello 1. Per conoscere le specifiche di conformità per la versione di ONTAP in uso, contatta il tuo SME FlexPod.

I moduli NetApp Cryptographic sono validati FIPS 140-2 livello 1

- NetApp Cryptographic Security Module (NCSM) è validato FIPS 140-2 livello 1.

I dischi con crittografia automatica NetApp sono convalidati FIPS 140-2 livello 2

NetApp acquista dischi con crittografia automatica (SED) che sono stati convalidati FIPS 140-2 dall'OEM (Original Equipment Manufacturer); i clienti che cercano questi dischi devono specificarli al momento dell'ordine. I dischi sono validati al livello 2. I seguenti prodotti NetApp possono sfruttare i SED validati:

- Sistemi storage AFF A-Series e FAS
- Sistemi storage e-Series ed EF-Series

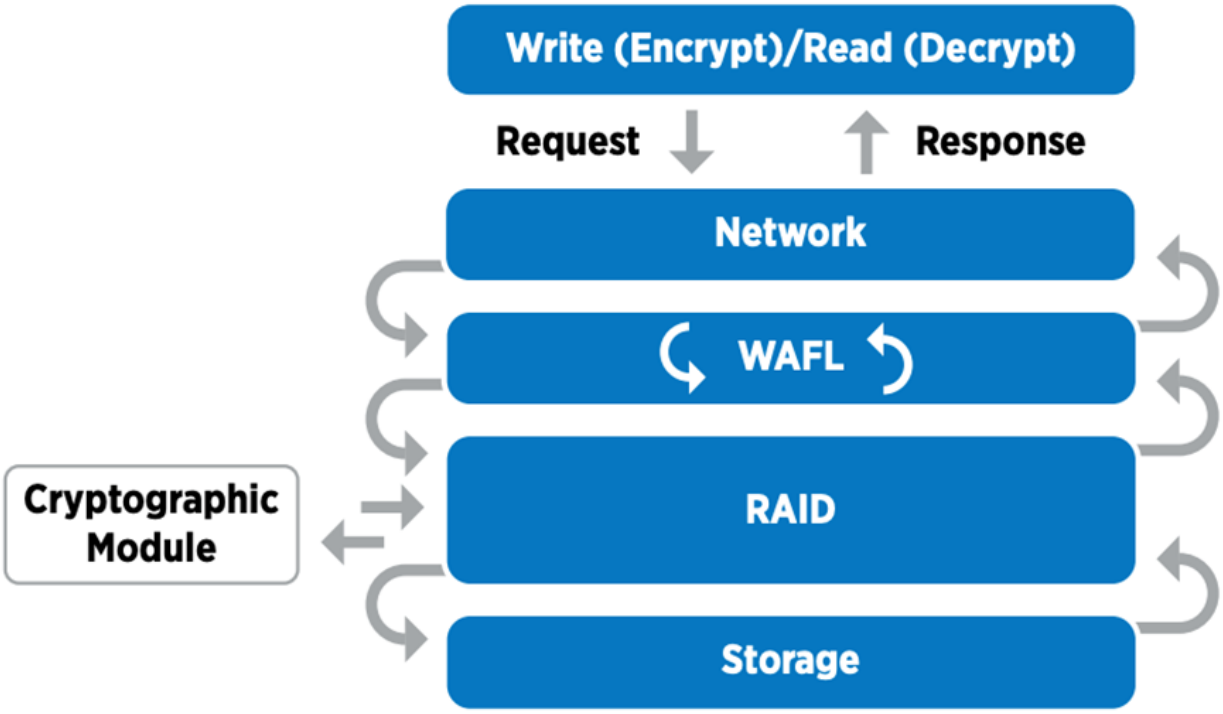
NetApp aggregate Encryption e NetApp Volume Encryption

Le tecnologie NVE e NetApp aggregate Encryption (NAE) consentono la crittografia dei dati rispettivamente a livello di volume e aggregato, rendendo la soluzione indipendente dal disco fisico.

NVE è una soluzione di crittografia dei dati a riposo basata su software disponibile a partire da ONTAP 9.1 ed è conforme a FIPS 140-2 a partire da ONTAP 9.2. NVE consente a ONTAP di crittografare i dati per ogni volume per la granularità. NAE, disponibile con ONTAP 9.6, è un'espansione di NVE; consente a ONTAP di crittografare i dati per ogni volume e i volumi possono condividere le chiavi nell'aggregato. Sia NVE che NAE utilizzano la crittografia AES a 256 bit. I dati possono anche essere memorizzati su disco senza SED. NVE e NAE consentono di utilizzare le funzionalità di efficienza dello storage anche quando la crittografia è attivata. La crittografia solo a livello di applicazione consente di ridurre tutti i vantaggi dell'efficienza dello storage. Con NVE e NAE, l'efficienza dello storage viene mantenuta perché i dati provengono dalla rete attraverso NetApp WAFL al livello RAID, che determina se i dati devono essere crittografati. Per una maggiore efficienza dello storage, è possibile utilizzare la deduplica aggregata con NAE. I volumi NVE e NAE possono coesistere sullo stesso aggregato NAE. Gli aggregati NAE non supportano volumi non crittografati.

Ecco come funziona il processo: Quando i dati vengono crittografati, vengono inviati al modulo crittografico convalidato FIPS 140-2 livello 1. Il modulo crittografico crittografa i dati e li invia di nuovo al livello RAID. I dati crittografati vengono quindi inviati al disco. Pertanto, con la combinazione di NVE e NAE, i dati sono già crittografati durante il percorso verso il disco. Le letture seguono il percorso inverso. In altre parole, i dati

lasciano il disco crittografato, vengono inviati a RAID, vengono decifrati dal modulo crittografico e quindi inviati al resto dello stack, come mostrato nella figura seguente.



NVE utilizza un modulo di crittografia software validato FIPS 140-2 livello 1.

Per ulteriori informazioni su NVE, vedere "Scheda informativa di NVE".

NVE protegge i dati nel cloud. Cloud Volumes ONTAP e Azure NetApp Files sono in grado di fornire la crittografia dei dati conforme a FIPS 140-2 a riposo.

A partire da ONTAP 9.7, gli aggregati e i volumi appena creati vengono crittografati per impostazione predefinita quando si dispone della licenza NVE e della gestione delle chiavi integrata o esterna. A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da crittografare. I volumi creati nell'aggregato vengono crittografati per impostazione predefinita. È possibile ignorare l'impostazione predefinita quando si crittografa il volume.

Comandi ONTAP NAE CLI

Prima di eseguire i seguenti comandi CLI, assicurarsi che il cluster disponga della licenza NVE richiesta.

Per creare un aggregato e crittografarlo, eseguire il seguente comando (quando viene eseguito su un'interfaccia CLI del cluster ONTAP 9.6 e versioni successive):

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

Per convertire un aggregato non NAE in un aggregato NAE An, eseguire il seguente comando (se eseguito su

una CLI cluster ONTAP 9.6 e versioni successive):

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

Per convertire un aggregato NAE in un aggregato non NAE, eseguire il seguente comando (quando viene eseguito su una CLI cluster ONTAP 9.6 e versioni successive):

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

Comandi CLI NVE di ONTAP

A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da crittografare. I volumi creati nell'aggregato vengono crittografati per impostazione predefinita.

Per creare un volume su un aggregato abilitato NAE, eseguire il seguente comando (se eseguito su una CLI cluster ONTAP 9.6 e versioni successive):

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

Per abilitare la crittografia di un volume esistente "inplace" senza uno spostamento del volume, eseguire il seguente comando (se eseguito su un'interfaccia CLI del cluster ONTAP 9.6 e versioni successive):

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

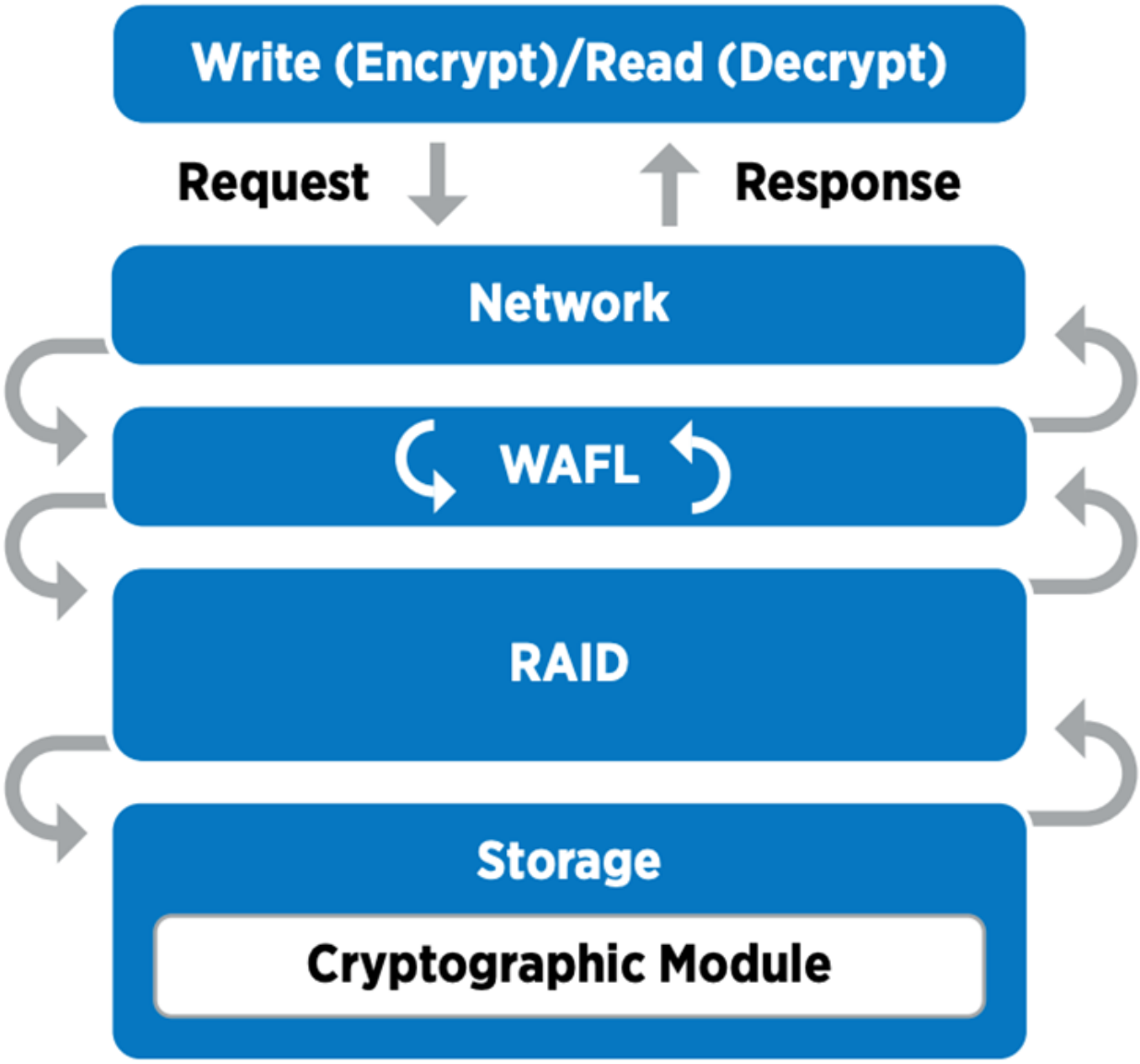
Per verificare che i volumi siano abilitati per la crittografia, eseguire il seguente comando CLI:

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

NSE

NSE utilizza i SED per eseguire la crittografia dei dati attraverso un meccanismo con accelerazione hardware.

NSE è configurato per utilizzare dischi con crittografia automatica FIPS 140-2 livello 2 per facilitare la conformità e il ritorno delle parti di ricambio, consentendo la protezione dei dati inattivi tramite crittografia trasparente dei dischi AES a 256 bit. I dischi eseguono tutte le operazioni di crittografia dei dati internamente, come illustrato nella figura seguente, inclusa la generazione della chiave di crittografia. Per impedire l'accesso non autorizzato ai dati, il sistema di storage deve autenticarsi con il disco utilizzando una chiave di autenticazione stabilita al primo utilizzo del disco.



NSE utilizza la crittografia hardware su ogni disco, convalidata FIPS 140-2 livello 2.

Per ulteriori informazioni su NSE, consultare "Scheda tecnica NSE".

Gestione delle chiavi

Lo standard FIPS 140-2 si applica al modulo crittografico come definito dal confine, come mostrato nella figura seguente.

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.

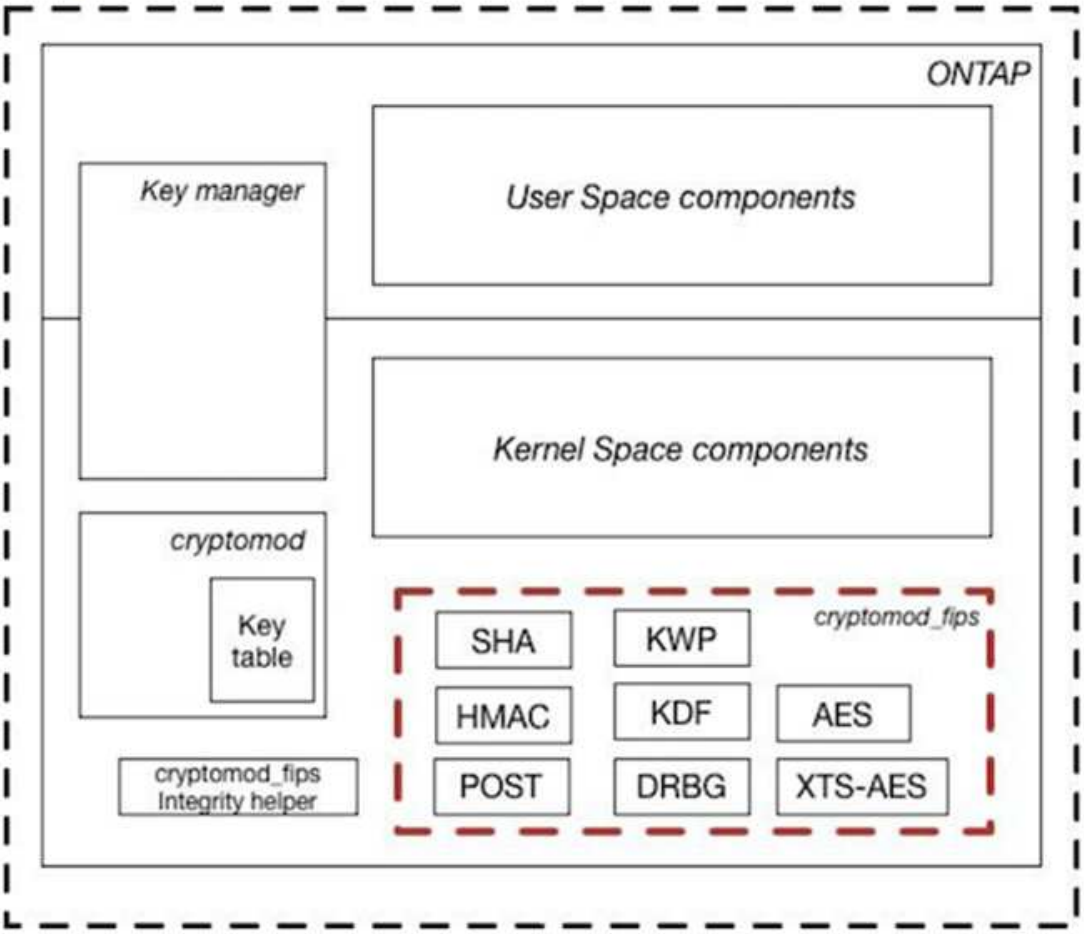


Figure 1 - Block Diagram

Key Manager tiene traccia di tutte le chiavi di crittografia utilizzate da ONTAP. I SED NSE utilizzano il gestore delle chiavi per impostare le chiavi di autenticazione per i SED NSE. Quando si utilizza il gestore delle chiavi, la soluzione combinata NVE e NAE è composta da un modulo di crittografia software, chiavi di crittografia e un gestore delle chiavi. Per ciascun volume, NVE utilizza una chiave di crittografia dati XTS-AES 256 univoca, archiviata dal gestore delle chiavi. La chiave utilizzata per un volume di dati è univoca per il volume di dati in quel cluster e viene generata quando viene creato il volume crittografato. Allo stesso modo, un volume NAE utilizza chiavi di crittografia dati XTS-AES 256 univoche per aggregato, memorizzate anche dal gestore delle chiavi. Le chiavi NAE vengono generate quando viene creato l'aggregato crittografato. ONTAP non genera in anticipo le chiavi, le riutilizza o le visualizza in testo normale, ma vengono memorizzate e protette dal gestore delle chiavi.

Supporto per gestore chiavi esterno

A partire da ONTAP 9.3, i key manager esterni sono supportati sia nelle soluzioni NVE che NSE. Lo standard FIPS 140-2 si applica al modulo crittografico utilizzato nell'implementazione del vendor specifico. Nella maggior parte dei casi, i clienti FlexPod e ONTAP utilizzano una delle seguenti soluzioni validate (in base al "Matrice di interoperabilità NetApp") responsabili chiave:

- Gemalto o SafeNet ALL'INDIRIZZO
- Vormetric (Thales)
- IBM SKLM
- Utimaco (in precedenza Microfous, HPE)

Il backup delle chiavi di autenticazione NSE e NVMe SED viene eseguito su un gestore di chiavi esterno utilizzando LO standard di settore OASIS Key Management Interoperability Protocol (KMIP). Solo il sistema di storage, il disco e il gestore delle chiavi hanno accesso alla chiave e l'unità non può essere sbloccata se viene spostata all'esterno del dominio di sicurezza, impedendo così la perdita di dati. Il gestore delle chiavi esterno memorizza anche le chiavi di crittografia del volume NVE e le chiavi di crittografia aggregate NAE. Se il controller e i dischi vengono spostati e non hanno più accesso al gestore delle chiavi esterno, i volumi NVE e NAE non saranno accessibili e non potranno essere decifrati.

Il seguente comando di esempio aggiunge due server di gestione delle chiavi all'elenco di server utilizzati dal gestore delle chiavi esterno per la macchina virtuale dello store (SVM) `svmname1`.

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

Quando un data center FlexPod viene utilizzato in uno scenario di multi-tenancy, ONTAP consente agli utenti di fornire una separazione di tenancy per motivi di sicurezza a livello di SVM.

Per verificare l'elenco dei key manager esterni, eseguire il seguente comando CLI:

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

Combinazione della crittografia per la doppia crittografia (difesa a più livelli)

Se è necessario separare l'accesso ai dati e assicurarsi che i dati siano sempre protetti, i SED NSE possono essere combinati con la crittografia a livello di rete o fabric. I SED NSE agiscono come un backstop se un amministratore dimentica di configurare o configurare in modo errato la crittografia di livello superiore. Per due diversi livelli di crittografia, è possibile combinare i SED NSE con NVE e NAE.

Modalità FIPS del piano di controllo a livello di cluster NetApp ONTAP

Il software per la gestione dei dati NetApp ONTAP dispone di una configurazione in modalità FIPS che crea un'istanza di un livello di sicurezza aggiunto per il cliente. Questa modalità FIPS si applica solo al piano di controllo. Quando la modalità FIPS è attivata, in conformità con gli elementi chiave di FIPS 140-2, Transport Layer Security v1 (TLSv1) e SSLv3 sono disattivati e solo TLS v1.1 e TLS v1.2 rimangono attivati.

> Il pannello di controllo a livello di cluster ONTAP in modalità FIPS è conforme a FIPS 140-2 livello 1. La modalità FIPS a livello di cluster utilizza un modulo crittografico basato su software fornito da NCSM.

La modalità di conformità FIPS 140-2 per il piano di controllo a livello di cluster protegge tutte le interfacce di controllo di ONTAP. Per impostazione predefinita, la modalità solo FIPS 140-2 è disattivata; tuttavia, è possibile abilitarla impostando `is- fips-enabled` parametro a. `true` per `security config modify` comando.

Per attivare la modalità FIPS sul cluster ONTAP, eseguire il seguente comando:

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

Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP al client esterno o ai componenti server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.

Per visualizzare lo stato FIPS dell'intero cluster, eseguire i seguenti comandi:

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

"Avanti: Vantaggi della soluzione dell'infrastruttura convergente FlexPod."

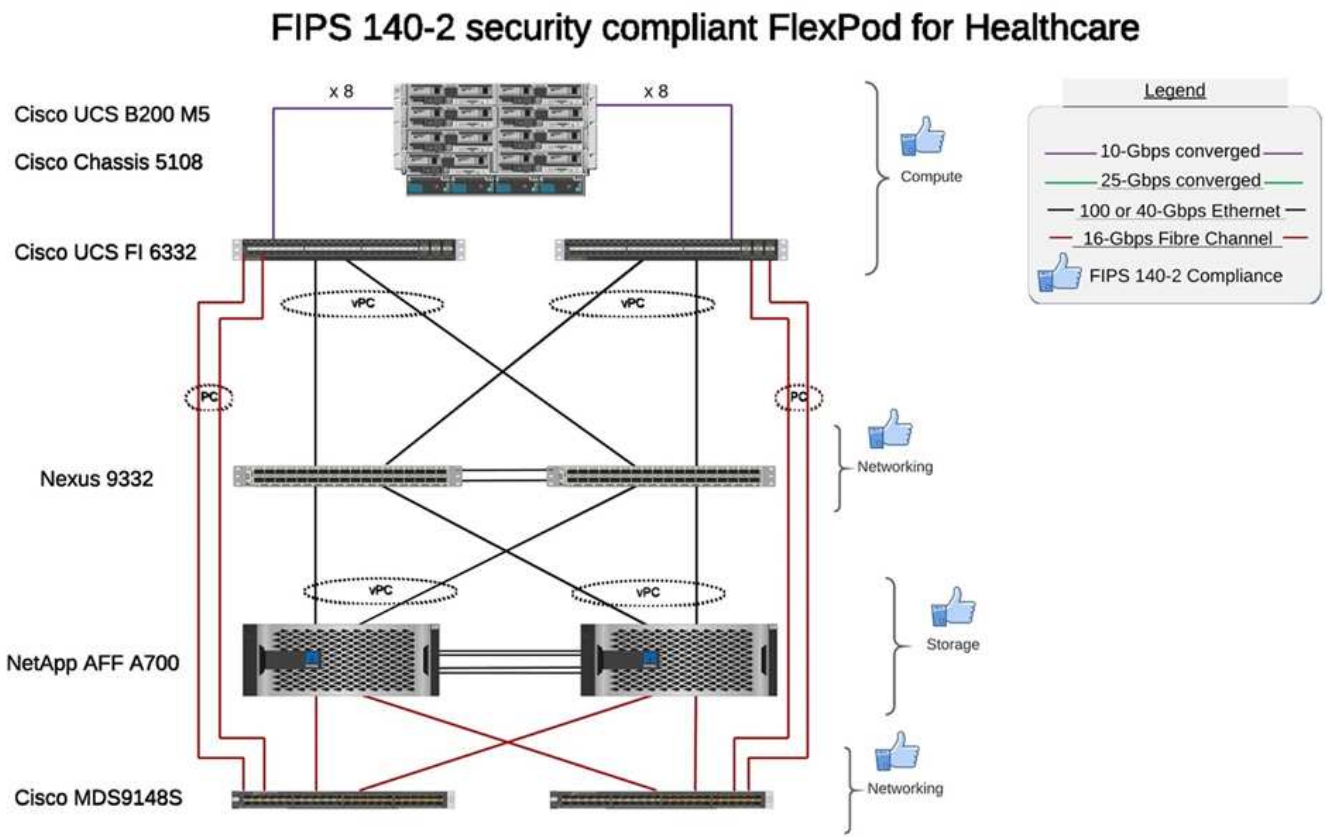
Vantaggi della soluzione dell'infrastruttura convergente FlexPod

"Precedente: Storage NetApp ONTAP FlexPod e FIPS 140-2."

Le organizzazioni del settore sanitario dispongono di diversi sistemi mission-critical. Due dei sistemi più critici sono i sistemi di cartelle cliniche elettroniche (EHR) e i sistemi di imaging medicale. Per dimostrare la configurazione FIPS su un sistema FlexPod, abbiamo utilizzato un EHR open-source e un sistema di archiviazione e comunicazione delle immagini open-source (PACS) per la configurazione del laboratorio e la convalida del carico di lavoro sul sistema FlexPod. Per un elenco completo delle funzionalità EHR, dei componenti dell'applicazione logica EHR e dei vantaggi dei sistemi EHR implementati su un sistema FlexPod, vedere "TR-4881: FlexPod per i sistemi di cartella clinica elettronica". Per un elenco completo delle funzionalità di un sistema di imaging medicale, dei componenti applicativi logici e dei vantaggi offerti dai sistemi di imaging medicale implementati su FlexPod, vedere "TR-4865: FlexPod per l'imaging medicale".

Durante la configurazione FIPS e la convalida del carico di lavoro, abbiamo esercitato caratteristiche di carico di lavoro che erano rappresentative di una tipica organizzazione sanitaria. Ad esempio, abbiamo utilizzato un sistema EHR open-source per includere scenari di modifica e accesso ai dati dei pazienti realistici. Inoltre, abbiamo esercitato carichi di lavoro di imaging medico che includevano imaging digitale e oggetti di comunicazione in medicina (DICOM) in un `*. dcm` formato del file. Gli oggetti DICOM con metadati sono stati memorizzati sia nel file che nello storage a blocchi. Inoltre, abbiamo implementato funzionalità di multipathing all'interno di un server RedHat Enterprise Linux (RHEL) virtualizzato. Abbiamo memorizzato oggetti DICOM su NFS, montato LUN utilizzando iSCSI e montato LUN utilizzando FC. Durante la configurazione e la convalida FIPS, abbiamo osservato che l'infrastruttura convergente FlexPod ha superato le nostre aspettative e ha ottenuto risultati senza problemi.

La figura seguente mostra il sistema FlexPod utilizzato per la configurazione e la convalida FIPS. Abbiamo sfruttato "Data center FlexPod con VMware vSphere 7.0 e NetApp ONTAP 9.7 Cisco Validated Design (CVD)" durante il processo di configurazione.



Componenti hardware e software dell'infrastruttura della soluzione

Le due figure seguenti elencano i componenti hardware e software rispettivamente utilizzati durante il test FIPS di abilitazione su un FlexPod. I consigli riportati in queste tabelle sono esempi; è necessario collaborare con il proprio SME NetApp per assicurarsi che i componenti siano adatti alla propria organizzazione. Inoltre, assicurarsi che i componenti e le versioni siano supportati in "Tool di matrice di interoperabilità NetApp" (IMT) e. "Cisco hardware Compatibility List (HCL) (elenco compatibilità hardware Cisco)".

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Calcolo	Chassis Cisco UCS 5108	1 o 2	
	Blade server Cisco UCS	3 B200 M5	Ciascuno con 2 core da 20 o più, 2,7 GHz e 128 GB di RAM
	Cisco UCS Virtual Interface Card (VIC)	Cisco UCS 1440	Vedere
	2 interconnessioni fabric Cisco UCS	6332	-
Rete	Switch Cisco Nexus	2 Cisco Nexus 9332	-
Rete di storage	Rete IP per l'accesso allo storage su protocolli SMB/CIFS, NFS o iSCSI	Stessi switch di rete come sopra	-
	Accesso allo storage tramite FC	2 Cisco MDS 9148S	-

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Storage	Sistema storage all-flash NetApp AFF A700	1 cluster	Cluster con due nodi
	Shelf di dischi	Uno shelf di dischi DS224C o NS224	Completamente popolato con 24 dischi
	SSD	Capacità superiore a 24, 1,2 TB	-

Software	Famiglia di prodotti	Versione o release	Dettagli
Vari	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 (64 bit)	-
	NetApp ONTAP	ONTAP 9.7 o versione successiva	-
	Cisco UCS Fabric Interconnect	Cisco UCS Manager 4.1 o versione successiva	-
	Switch Cisco Ethernet serie 3000 o 9000	Per la serie 9000, 7.0(3)I7(7) o versioni successive per la serie 3000, 9.2(4) o versioni successive	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) o successiva	-
	Hypervisor	VMware vSphere ESXi 6.7 U2 o versione successiva	-
Storage	Sistema di gestione dell'hypervisor	VMware vCenter Server 6.7 U3 (vCSA) o versione successiva	-
Rete	NetApp Virtual Storage Console (VSC)	VSC 9.7 o versione successiva	-
	NetApp SnapCenter	SnapCenter 4.3 o versione successiva	-
	Cisco UCS Manager	4.1(1c) o versione successiva	
Hypervisor	ESXi		
Gestione	Sistema di gestione dell'hypervisor VMware vCenter Server 6.7 U3 (vCSA) o versione successiva		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 o versione successiva	

Software	Famiglia di prodotti	Versione o release	Dettagli
	NetApp SnapCenter	SnapCenter 4.3 o versione successiva	
	Cisco UCS Manager	4.1(1c) o versione successiva	

"Avanti: Ulteriori considerazioni sulla sicurezza di FlexPod."

Ulteriori considerazioni sulla sicurezza di FlexPod

"Precedente: Vantaggi della soluzione dell'infrastruttura convergente FlexPod."

L'infrastruttura FlexPod è una piattaforma modulare, convergente, facoltativamente virtualizzata, scalabile (scale-out e scale-up) e conveniente. Con la piattaforma FlexPod, puoi scalare in modo indipendente calcolo, rete e storage per accelerare l'implementazione delle applicazioni. Inoltre, l'architettura modulare consente operazioni senza interruzioni anche durante le attività di scale-out e upgrade del sistema.

I diversi componenti di un sistema HIT richiedono l'archiviazione dei dati nei file system SMB/CIFS, NFS, Ext4 e NTFS. Questo requisito significa che l'infrastruttura deve fornire l'accesso ai dati sui protocolli NFS, CIFS e SAN. Un singolo sistema storage NetApp è in grado di supportare tutti questi protocolli, eliminando la necessità di una pratica legacy di sistemi storage specifici del protocollo. Inoltre, un singolo sistema storage NetApp può supportare carichi di lavoro HIT multipli come EHR, PACS o VNA, genomica, VDI e altro ancora, con livelli di performance garantiti e configurabili.

Se implementato in un sistema FlexPod, HIT offre diversi vantaggi specifici per il settore sanitario. Il seguente elenco contiene una descrizione di alto livello di questi vantaggi:

- **Sicurezza FlexPod**. La sicurezza è alla base di un sistema FlexPod. Negli ultimi anni, il ransomware è diventato una minaccia. Ransomware è un tipo di malware basato sulla crittografia, l'utilizzo della crittografia per creare software dannoso. Questo malware può utilizzare la crittografia a chiave simmetrica e asimmetrica per bloccare i dati della vittima e richiedere un riscatto per fornire la chiave per decrittare i dati. Per scoprire come la soluzione FlexPod aiuta a mitigare minacce come ransomware, consulta "TR-4802: La soluzione per il ransomware". Lo sono anche i componenti dell'infrastruttura FlexPod "Conforme a FIPS 140-2".
- * Cisco Intersight.* Cisco Intersight è una piattaforma innovativa, basata sul cloud e di gestione come servizio che offre un singolo pannello di controllo per la gestione e l'orchestrazione di FlexPod full-stack. La piattaforma Intersight utilizza moduli crittografici conformi alla sicurezza FIPS 140-2. L'architettura di gestione out-of-band della piattaforma lo rende fuori ambito per alcuni standard o audit come HIPAA. Nessuna informazione personale identificabile sulla salute sulla rete viene mai inviata al portale Intersight.
- **Tecnologia NetApp FPolicy.** NetApp FPolicy (un'evoluzione della policy del file dei nomi) è un framework di notifica di accesso ai file per il monitoraggio e la gestione dell'accesso ai file tramite i protocolli NFS o SMB/CIFS. Questa tecnologia fa parte del software per la gestione dei dati ONTAP da oltre un decennio ed è utile per rilevare ransomware. Questo motore Zero Trust offre misure di sicurezza aggiuntive oltre alle autorizzazioni negli elenchi di controllo degli accessi (ACL). FPolicy prevede due modalità operative: Nativa ed esterna:
    - La modalità nativa offre sia la blacklist che la whitelisting delle estensioni di file.
    - La modalità esterna ha le stesse funzionalità della modalità nativa, ma si integra anche con un server FPolicy che viene eseguito esternamente al sistema ONTAP e con un sistema SIEM (Security Information and Event Management). Per ulteriori informazioni su come combattere il ransomware,

consultare "Combattere il ransomware: Terza parte – ONTAP FPolicy, un altro potente strumento nativo (alias gratuito)" blog.

- **Dati inattivi**. ONTAP 9 e versioni successive dispongono di tre soluzioni di crittografia dei dati a riposo conformi a FIPS 140-2:
  - NSE è una soluzione hardware che utilizza dischi con crittografia automatica.
  - NVE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con una chiave univoca per ciascun volume.
  - NAE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con chiavi univoche per ciascun aggregato.

> A partire da ONTAP 9.7, NAE e NVE sono attivati per impostazione predefinita se è attivo il pacchetto di licenza NVE di NetApp con il nome VE.

- **Dati in volo**. A partire da ONTAP 9.8, IPSec (Internet Protocol Security) fornisce il supporto della crittografia end-to-end per tutto il traffico IP tra un client e una SVM ONTAP. La crittografia dei dati IPSec per tutto il traffico IP include i protocolli NFS, iSCSI e SMB/CIFS. IPSec fornisce l'unica opzione di crittografia in volo per il traffico iSCSI.
- **Crittografia dei dati end-to-end su un data fabric ibrido multicloud**. I clienti che utilizzano tecnologie di crittografia dei dati a riposo come NSE o NVE e la crittografia del peering dei cluster (CPE) per il traffico di replica dei dati possono ora utilizzare la crittografia end-to-end tra client e storage nel data fabric multicloud ibrido eseguendo l'aggiornamento a ONTAP 9.8 o versione successiva e utilizzando IPSec. A partire da ONTAP 9, è possibile attivare la modalità di conformità FIPS 140-2 per le interfacce del piano di controllo a livello di cluster. Per impostazione predefinita, la modalità solo FIPS 140-2 è disattivata. A partire da ONTAP 9.6, CPE fornisce il supporto della crittografia TLS 1.2 AES-256 GCM per le funzionalità di replica dei dati ONTAP, come NetApp SnapMirror, NetApp SnapVault e le tecnologie NetApp FlexCache. La crittografia viene impostata tramite una chiave precondivisa (PSK) tra due peer del cluster.
- **Multitenancy sicura**. Supporta le crescenti esigenze di infrastruttura condivisa di storage e server virtualizzati, consentendo la multi-tenancy sicura di informazioni specifiche della struttura, in particolare quando si ospitano più istanze di database e software.

"Prossimo: Conclusione."

Conclusione

"Precedente: Ulteriori considerazioni sulla sicurezza di FlexPod."

Eseguendo la tua applicazione per il settore sanitario su una piattaforma FlexPod, la tua organizzazione sanitaria è meglio protetta da una piattaforma abilitata per FIPS 140-2. FlexPod offre una protezione multilivello per ogni singolo componente: Calcolo, rete e storage. Le funzionalità di protezione dei dati di FlexPod proteggono i dati a riposo o in volo e mantengono i backup sicuri e pronti quando necessario.

Evita gli errori umani sfruttando i design pre-validati di FlexPod che sono infrastrutture convergenti rigorosamente testate dalla partnership strategica di Cisco e NetApp. Un sistema FlexPod progettato e progettato per offrire performance di sistema prevedibili e a bassa latenza e alta disponibilità con un impatto minimo, anche quando FIPS 140-2 è abilitato nei livelli di calcolo, networking e storage. Questo approccio offre un'esperienza utente superiore e tempi di risposta ottimali per gli utenti del sistema HIT.

"Pagina successiva: Riconoscimenti, cronologia delle versioni e informazioni aggiuntive."

Riconoscimenti, cronologia delle versioni e dove trovare ulteriori informazioni

"Precedente: Conclusione."

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e siti Web:

- Guida alla configurazione della sicurezza NX-OS della famiglia Cisco MDS 9000

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

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

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

- NetApp e la pubblicazione FIPS (Federal Information Processing Standard) 140-2

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

- FIPS 140-2

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

- Guida al rafforzamento di NetApp ONTAP 9

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

- NetApp Encryption Power Guide

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

- Scheda informativa su NVE e NAE

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

- Scheda informativa NSE

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

- Centro documentazione di ONTAP 9

  http://docs.netapp.com

- NetApp e la pubblicazione FIPS (Federal Information Processing Standard) 140-2

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

- Conformità Cisco e FIPS 140-2

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

- NetApp Cryptographic Security Module

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

- Procedure di cybersecuryper le organizzazioni sanitarie di medie e grandi dimensioni

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

- Cisco e il programma CMVP (Cryptographic Module Validation Program)

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

- NetApp Storage Encryption, NVMe Self-Encrypting Drive, NetApp Volume Encryption e NetApp aggregate Encryption

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

- NetApp Volume Encryption e NetApp aggregate Encryption

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

- Crittografia dello storage NetApp

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

- FlexPod per sistemi di cartella clinica elettronica

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

- Data Now: Miglioramento delle performance negli ambienti Epic EHR con la tecnologia flash connessa al cloud

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

- Data center FlexPod per l'infrastruttura EHR Epic

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

- Guida all'implementazione di FlexPod Datacenter per Epic EHR

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

- Infrastruttura del data center FlexPod per il software MEDITECH

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

- Lo standard FlexPod si estende al software MEDITECH

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

- Guida al dimensionamento direzionale di FlexPod per MEDITECH

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

- FlexPod per imaging medicale

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

- Ai nel settore sanitario

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

- FlexPod per il settore sanitario semplifica la tua trasformazione

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

- FlexPod di Cisco e NetApp

  https://flexpod.com/

Ringraziamenti

- Abhinav Singh, Technical Marketing Engineer, NetApp
- Brian o'Mahony, Solution Architect Healthcare (Epic), NetApp
- Brian Pruitt, Pursuit Business Development Manager, NetApp
- Arvind Ramakrishnan, Senior Solutions Architect, NetApp
- Michael Hommer, FlexPod Global Field CTO, NetApp

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Aprile 2021	Release iniziale