FlexPod et sécurité

FlexPod

NetApp
October 30, 2025

Sommaire

FlexPod et sécurité

FlexPod, la solution aux attaques par ransomware

Tr-4802 : FlexPod, la solution vers le ransomware

Arvind Ramakrishnan, NetApp

En partenariat avec : 

Pour comprendre un ransomware, il est nécessaire de comprendre d'abord quelques points de clé sur la cryptographie. Les méthodes Cryptographiques permettent le cryptage de données avec une clé secrète partagée (cryptage de clé symétrique) ou une paire de clés (cryptage de clé asymétrique). L'une de ces clés est une clé publique largement disponible et l'autre est une clé privée non divulguée.

Les ransomwares sont un type de malware basé sur la cryptovirologie, c'est-à-dire l'utilisation de la cryptographie pour créer des logiciels malveillants. Ce programme malveillant peut utiliser à la fois le cryptage symétrique et asymétrique des clés pour verrouiller les données d'une victime et exiger une rançon afin de fournir la clé pour décrypter les données de la victime.

Comment les attaques par ransomware fonctionnent-elles ?

Les étapes suivantes décrivent la façon dont les ransomware utilisent la cryptographie pour chiffrer les données de la victime sans recourir au décryptage ou à la restauration par la victime :

1. L'attaquant génère une paire de clés comme dans le chiffrement de clé asymétrique. La clé publique générée est placée dans le programme malveillant et le programme malveillant est ensuite libéré.
2. Une fois le programme malveillant entré dans l'ordinateur ou le système de la victime, il génère une clé symétrique aléatoire à l'aide d'un générateur de nombres pseudorandom (PRNG) ou de tout autre algorithme aléatoire viable.
3. Le programme malveillant utilise cette clé symétrique pour crypter les données de la victime. Il crypte finalement la clé symétrique en utilisant la clé publique de l'attaquant qui était intégrée dans le programme malveillant. La sortie de cette étape est un texte chiffré asymétrique de la clé symétrique chiffrée et du texte chiffré des données de la victime.
4. Le programme malveillant met à zéro (efface) les données de la victime et la clé symétrique qui a été utilisée pour crypter les données, ne laissant ainsi aucune portée pour la récupération.
5. La victime est maintenant affichée le texte chiffré asymétrique de la clé symétrique et une valeur de rançon qui doit être payée afin d'obtenir la clé symétrique qui a été utilisée pour crypter les données.
6. La victime paie la rançon et partage le texte chiffré asymétrique avec l'attaquant. L'attaquant décrypte le texte du corps avec sa clé privée, ce qui donne une clé symétrique.
7. L'attaquant partage cette clé symétrique avec la victime, qui peut être utilisée pour décrypter toutes les données et ainsi récupérer de l'attaque.

À relever

Les individus et les organisations sont confrontés aux challenges suivants lorsqu'ils sont attaqués par des ransomware :

- Le défi le plus important est qu'il a un impact immédiat sur la productivité de l'organisation ou de l'individu. Il faut du temps pour revenir à un état de normalité, car tous les fichiers importants doivent être retrouvés et les systèmes sécurisés.
- Cela pourrait mener à une violation des données qui contient des informations sensibles et confidentielles appartenant à des clients ou clients et entraîner une situation de crise qu'une entreprise veut clairement éviter.
- Il y a de très bonnes chances que les données se trouvent entre de mauvaises mains ou soient effacées complètement, ce qui engendre un point de non-retour qui pourrait être désastreux pour les entreprises et les particuliers.
- Après avoir payé la rançon, il n'y a aucune garantie que l'attaquant fournira la clé pour restaurer les données.
- Il n'y a aucune assurance que l'attaquant s'abstiendra de diffuser les données sensibles malgré le paiement de la rançon.
- Dans les grandes entreprises, l'identification des failles qui ont conduit à une attaque par ransomware est une tâche fastidieuse et la sécurisation de tous les systèmes implique beaucoup d'efforts.

Qui est à risque ?

N'importe qui peut être attaqué par certaines personnes, y compris par des personnes et des grandes entreprises. Les entreprises qui ne mettent pas en œuvre de mesures et de pratiques de sécurité bien définies sont encore plus vulnérables à de telles attaques. L'effet de l'attaque sur une grande organisation peut être plusieurs fois plus important que ce qu'un individu peut supporter.

Les attaques par ransomware représentent environ 28 % de toutes les attaques de malware. En d'autres termes, plus d'un incident sur quatre est un ransomware. Les ransomwares peuvent se propager automatiquement et de manière discriminatoire à travers Internet, et lorsqu'il y a un retard de sécurité, ils peuvent entrer dans les systèmes de la victime et continuer de se propager à d'autres systèmes connectés. Les pirates informatiques ont tendance à cibler des personnes ou des entreprises qui effectuent énormément de partages de fichiers, à disposer de données sensibles ou essentielles, ou à conserver une protection inadéquate contre les attaques.

Les attaquants ont tendance à se concentrer sur les cibles potentielles suivantes :

- Universités et communautés d'étudiants
- Administrations et agences gouvernementales
- Hôpitaux
- Banques

Il ne s'agit pas d'une liste exhaustive des cibles. Vous ne pouvez pas vous protéger des attaques si vous vous trouvez en dehors de l'une de ces catégories.

Comment les ransomwares entrent-ils dans un système ou se propagent-ils ?

Il existe plusieurs façons dont les ransomwares peuvent entrer un système ou se propager à d'autres systèmes. Dans le monde d'aujourd'hui, presque tous les systèmes sont reliés les uns aux autres par l'intermédiaire d'Internet, de réseaux locaux, de réseaux WAN, etc. La quantité de données générées et

échangées entre ces systèmes ne cesse d'augmenter.

Parmi les méthodes les plus courantes par lesquelles les ransomwares peuvent être répartis, elles peuvent être utilisées quotidiennement pour partager ou accéder aux données :

- E-mail
- Réseaux P2P
- Téléchargements de fichiers
- Réseaux sociaux
- Appareils mobiles
- Connexion à des réseaux publics non sécurisés
- Accéder aux URL Web

Conséquences de la perte de données

Les conséquences ou les effets d'une perte de données peuvent se faire plus largement que ce que pourrait prévoir les entreprises. Les effets peuvent varier en fonction de la durée des temps d'arrêt ou de la période pendant laquelle une entreprise n'a pas accès à ses données. Plus l'attaque perdure longtemps, plus l'effet sur le chiffre d'affaires, la marque et la réputation de l'organisation est important. Une organisation peut aussi faire face à des problèmes juridiques et à un déclin important de la productivité.

Alors que ces questions persistent au fil du temps, elles commencent à s'agrandir et peuvent finir par changer la culture d'une organisation, selon la manière dont elle répond à l'attaque. Dans le monde d'aujourd'hui, l'information se répand rapidement et les nouvelles négatives sur une organisation pourraient causer des dommages permanents à sa réputation. Une entreprise peut être confrontée à de lourdes pénalités en cas de perte de données, ce qui pourrait éventuellement mener à la clôture de ses activités.

Effets financiers

Selon un récent "Rapport McAfee", Les coûts globaux encourus en raison de la cybercriminalité représentent environ 600 milliards de dollars, soit environ 0.8% du PIB mondial. Lorsque ce montant est comparé à la croissance mondiale de l'économie Internet de 4.2 billions de dollars, il équivaut à une taxe de 14% sur la croissance.

Une attaque par ransomware prend une part importante de ce coût financier. En 2018, les coûts encourus en raison d'attaques par ransomware étaient de l'ordre de 8 milliards—, un montant prévu pour atteindre 11.5 milliards de dollars en 2019.

Quelle est la solution ?

La récupération suite à une attaque par ransomware avec un temps d'indisponibilité minimal est uniquement possible grâce à la mise en œuvre d'un plan de reprise après incident proactif. Avoir la capacité de récupérer après une attaque est bon, mais la prévention d'une attaque est tout à fait idéale.

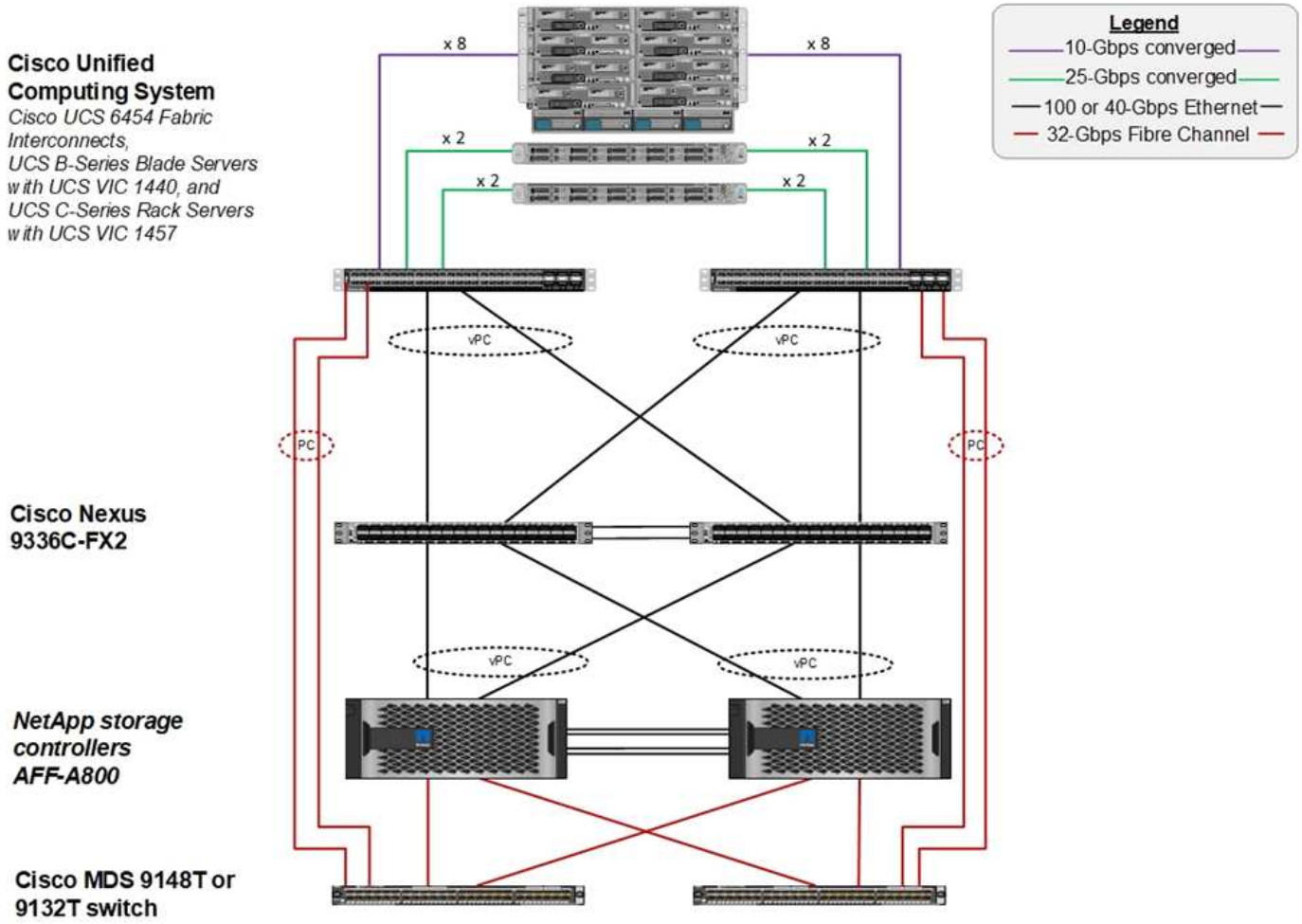
Bien que vous deviez examiner plusieurs fronts et corriger pour prévenir une attaque, le centre de données est le composant principal qui vous permet d'éviter ou de récupérer après une attaque.

La conception du data Center et les fonctionnalités fournies pour sécuriser les terminaux de réseau, de calcul et de stockage jouent un rôle essentiel dans la mise en place d'un environnement sécurisé pour les opérations quotidiennes. Ce document explique comment les fonctions d'une infrastructure de cloud hybride FlexPod peuvent vous aider à restaurer rapidement vos données en cas d'attaque et à éviter les attaques.

Présentation de FlexPod

FlexPod est une architecture préconçue, intégrée et validée qui combine les serveurs Cisco Unified Computing System (Cisco UCS), la gamme de commutateurs Cisco Nexus, les commutateurs Cisco MDS Fabric et les baies de stockage NetApp dans une architecture unique et flexible. Les solutions FlexPod sont conçues pour la haute disponibilité sans points de défaillance uniques, tout en garantissant à moindre coût et flexibilité de conception afin de prendre en charge un large éventail de charges de travail. Une conception FlexPod peut prendre en charge plusieurs hyperviseurs et serveurs sans système d'exploitation. Elle peut également être dimensionnée et optimisée en fonction des exigences des charges de travail des clients.

La figure ci-dessous illustre l'architecture FlexPod et met en évidence la haute disponibilité sur l'ensemble des couches de la pile. Les composants d'infrastructure du stockage, du réseau et du calcul sont configurés de telle sorte que les opérations puissent basculer instantanément vers le partenaire survivant en cas de panne de l'un des composants.



L'un des principaux avantages d'un système FlexPod est qu'il est prédéfini, intégré et validé pour plusieurs charges de travail. Des guides détaillés de conception et de déploiement sont publiés pour chaque validation des solutions. Ces documents comprennent les bonnes pratiques à suivre pour exécuter des charges de travail de façon transparente sur FlexPod. Ces solutions sont construites avec les meilleurs produits de calcul, de réseau et de stockage, ainsi qu'avec un ensemble de fonctionnalités dédiées à la sécurité et au renforcement de l'ensemble de l'infrastructure.

"Indice X-Force Threat Intelligence d'IBM" états-unis, « l'erreur humaine responsable des deux tiers des enregistrements compromis, y compris l'historique 424 % des erreurs de configuration dans l'infrastructure cloud ».

Avec un système FlexPod, vous pouvez éviter toute erreur de configuration de votre infrastructure grâce à l'automatisation, via des playbooks Ansible qui réalisent une configuration de bout en bout de l'infrastructure selon les meilleures pratiques décrites dans les conceptions validées de Cisco (CVD) et les architectures vérifiées NetApp (NVA).

Mesures de protection par ransomware

Cette section présente les principales fonctionnalités du logiciel de gestion des données NetApp ONTAP, ainsi que les outils pour Cisco UCS et Cisco Nexus que vous pouvez utiliser pour protéger et récupérer efficacement contre les attaques par ransomware.

Stockage : NetApp ONTAP

Le logiciel ONTAP offre de nombreuses fonctionnalités utiles pour la protection des données, dont la plupart sont gratuites pour les clients qui disposent d'un système ONTAP. Vous pouvez à tout moment utiliser les fonctions suivantes pour protéger les données d'attaques :

- **Technologie NetApp Snapshot.** Une copie Snapshot est une image en lecture seule d'un volume qui capture l'état d'un système de fichiers à un moment donné. Ces copies aident à protéger les données sans affecter les performances du système et elles n'occupent pas autant d'espace de stockage important. NetApp vous recommande de créer un calendrier pour la création de copies Snapshot. Vous devez également maintenir un temps de rétention long car certains programmes malveillants peuvent rester inactifs puis réactiver des semaines ou des mois après une infection. En cas d'attaque, le volume peut être restauré à l'aide d'une copie Snapshot prise avant l'infection.
- **Technologie NetApp SnapRestore.** le logiciel de restauration des données SnapRestore est extrêmement utile pour restaurer les données en cas de corruption ou pour restaurer uniquement le contenu des fichiers. SnapRestore ne rétablit pas les attributs d'un volume. Elle est bien plus rapide que ce que peut obtenir un administrateur en copiant les fichiers à partir de la copie Snapshot vers le système de fichiers actif. La vitesse à laquelle les données peuvent être restaurées est utile lorsque de nombreux fichiers doivent être restaurés aussi rapidement que possible. En cas d'attaque, ce processus de restauration hautement efficace permet de remettre rapidement les activités en ligne.
- **Technologie NetApp SnapCenter**.* le logiciel SnapCenter utilise des fonctions de sauvegarde et de réplication basées sur le stockage NetApp pour assurer une protection des données cohérente au niveau des applications. Ce logiciel s'intègre aux applications d'entreprise et fournit des flux de production spécifiques aux applications et aux bases de données afin de répondre aux besoins des administrateurs d'applications, de bases de données et d'infrastructure virtuelle. SnapCenter fournit une plateforme qui permet de coordonner et de gérer facilement et en toute sécurité la protection de vos données sur l'ensemble des applications, bases de données et systèmes de fichiers. La capacité à fournir une protection des données cohérente au niveau des applications est primordiale lors de la restauration des données, car elle permet de restaurer facilement les applications dans un état cohérent plus rapidement.
- **Technologie NetApp SnapLock.** SnapLock fournit un volume spécial dans lequel les fichiers peuvent être stockés dans un état non réinscriptibles et non effaçables. Les données de production de l'utilisateur résidant dans un volume FlexVol peuvent être mises en miroir ou archivées sur un volume SnapLock grâce respectivement à la technologie NetApp SnapMirror ou SnapVault. Les fichiers du volume SnapLock, le volume lui-même et son agrégat d'hébergement ne peuvent pas être supprimés avant la fin de la période de conservation.
- **Technologie NetApp FPolicy.** utilisez le logiciel FPolicy pour éviter les attaques en désautorisant des opérations sur des fichiers avec des extensions spécifiques. Un événement FPolicy peut être déclenché

pour des opérations de fichiers spécifiques. L'événement est lié à une politique, qui appelle le moteur qu'il doit utiliser. Vous pouvez configurer une règle avec un ensemble d'extensions de fichiers qui pourraient éventuellement contenir un ransomware. Lorsqu'un fichier doté d'une extension non autorisée tente d'effectuer une opération non autorisée, FPolicy empêche cette opération.

Réseau : Cisco Nexus

Le logiciel Cisco NX OS prend en charge la fonctionnalité NetFlow qui permet une détection améliorée des anomalies et de la sécurité du réseau. NetFlow capture les métadonnées de chaque conversation sur le réseau, les parties impliquées dans la communication, le protocole utilisé et la durée de la transaction. Une fois les informations agrégées et analysées, elles permettent de mieux comprendre le comportement normal.

Les données collectées permettent également d'identifier des modèles d'activité douteux, tels que les programmes malveillants, qui s'étendent sur le réseau, qui peuvent autrement passer inaperçues.

NetFlow utilise des flux pour fournir des statistiques sur la surveillance du réseau. Un flux est un flux unidirectionnel de paquets arrivant sur une interface source (ou VLAN) et possède les mêmes valeurs pour les clés. Une clé est une valeur identifiée pour un champ dans le paquet. Vous créez un flux à l'aide d'un enregistrement de flux pour définir les clés uniques de votre flux. Vous pouvez exporter les données collectées par NetFlow pour vos flux à l'aide d'un exportateur de flux vers un collecteur NetFlow distant, tel que Cisco StealthWatch. StealthWatch exploite ces informations pour assurer une surveillance continue du réseau et fournit une détection en temps réel des menaces et une analyse des réponses aux incidents en cas d'attaque par ransomware.

Calcul : Cisco UCS

Cisco UCS est le terminal de calcul d'une architecture FlexPod. Vous pouvez utiliser plusieurs produits Cisco qui contribuent à sécuriser cette couche de la pile au niveau du système d'exploitation.

Vous pouvez implémenter les produits clés suivants dans la couche de calcul ou d'application :

- **Cisco Advanced Malware protection (AMP) pour les noeuds finaux.** pris en charge sur les systèmes d'exploitation Microsoft Windows et Linux, cette solution intègre des capacités de prévention, de détection et de réponse. Ce logiciel de sécurité évite les failles de sécurité, bloque les programmes malveillants au point d'entrée et surveille et analyse en continu les activités des fichiers et des processus afin de détecter, de contenir et de corriger rapidement les menaces qui peuvent échapper aux défenses en première ligne.

  Le composant de protection contre les activités malveillantes (MAP) de l'AMP surveille en permanence toute l'activité des points finaux et assure la détection des temps d'exécution et le blocage du comportement anormal d'un programme en cours d'exécution sur le point final. Par exemple, lorsque le comportement de terminal indique un ransomware, les processus incriminés se terminent, ce qui empêche le chiffrement du terminal et arrête l'attaque.

- **Cisco Advanced Malware protection for Email Security.** les e-mails sont devenus le véhicule de premier choix pour la propagation des programmes malveillants et l'exécution des cyber-attaques. En moyenne, environ 100 milliards d'e-mails sont échangés en une seule journée, ce qui fournit aux pirates un excellent vecteur de pénétration dans les systèmes des utilisateurs. Par conséquent, il est absolument essentiel de se défendre contre cette ligne d'attaque.

  AMP analyse les e-mails contre les menaces, telles que les attaques sans jour et les logiciels malveillants furtifs cachés dans des pièces jointes malveillantes. Il utilise également des informations URL de pointe pour lutter contre les liens malveillants. Elle offre aux utilisateurs une protection avancée contre le phishing ciblé, les attaques par ransomware et d'autres attaques sophistiquées.

- **Système de prévention des intrusions nouvelle génération (NGIPS).** Cisco FirePOWER NGIPS peut

être déployé en tant qu'appliance physique dans le centre de données ou en tant qu'appliance virtuelle sur VMware (NGIPSv pour VMware). Ce système hautement efficace de prévention des intrusions offre des performances fiables et un faible coût total de possession. La protection contre les menaces peut être étendue avec des licences d'abonnement facultatives pour fournir AMP, visibilité et contrôle des applications, ainsi que des fonctionnalités de filtrage des URL. Le système NGIPS virtualisé inspecte le trafic entre les machines virtuelles et facilite le déploiement et la gestion des solutions NGIPS sur des sites disposant de ressources limitées, ce qui renforce la protection des ressources physiques et virtuelles.

Protégez et restaurez les données sur FlexPod

Cette section décrit comment les données d'un utilisateur final peuvent être récupérées en cas d'attaque et comment empêcher les attaques à l'aide d'un système FlexPod.

Présentation du banc d'essai

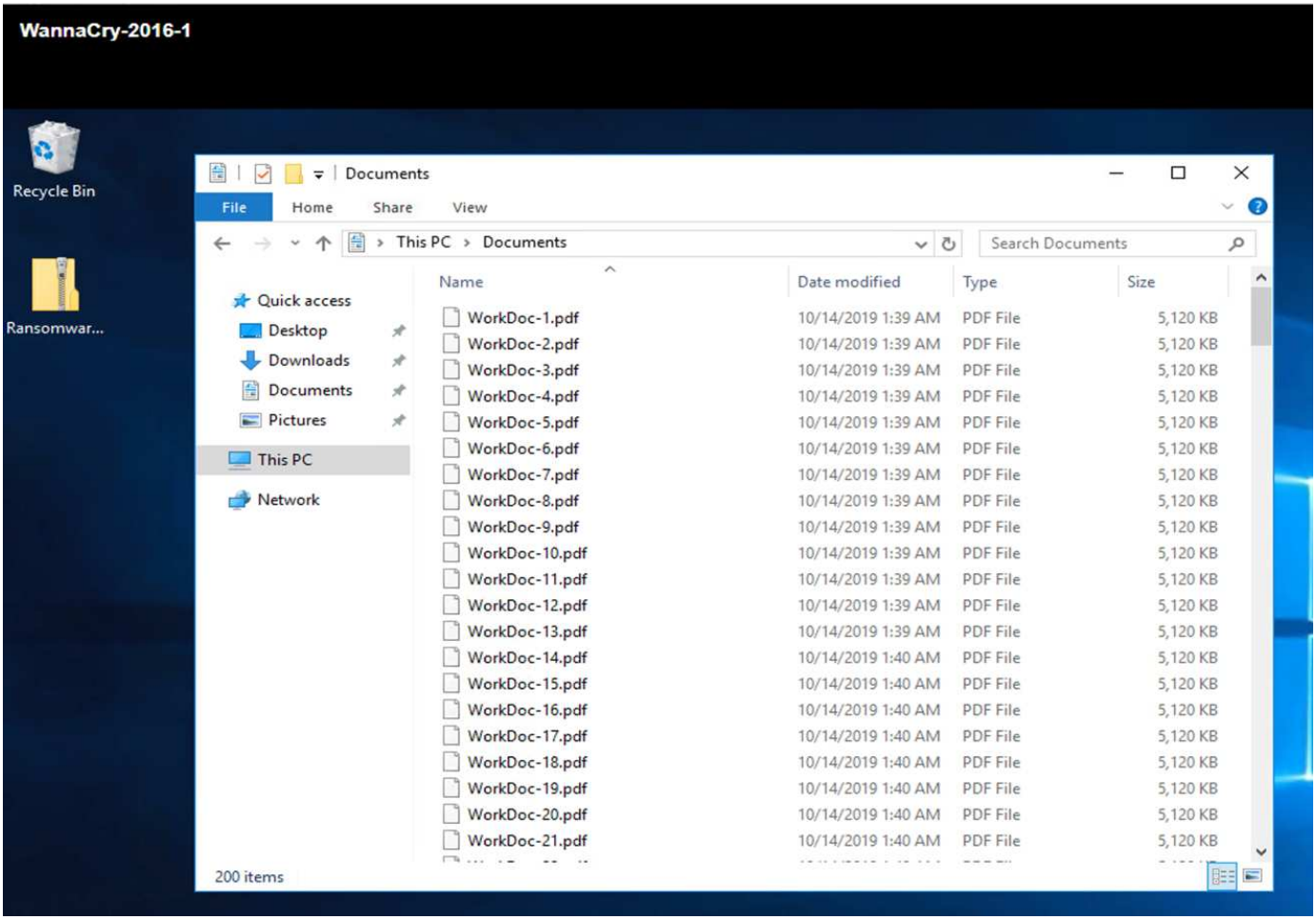
Pour mettre en avant la détection, la résolution et la prévention des problèmes liés à FlexPod, un banc d'essai a été créé à partir des directives spécifiées dans les guides CVD de la dernière plateforme disponibles au moment de l'élaboration de ce document : "CVD FlexPod Datacenter avec VMware vSphere 6.7 U1, Cisco UCS de 4e génération et NetApp AFF A-Series".

Une machine virtuelle Windows 2016, qui fournissait un partage CIFS à partir du logiciel NetApp ONTAP, a été déployée dans l'infrastructure VMware vSphere. Ensuite, NetApp FPolicy a été configuré sur le partage CIFS pour éviter l'exécution de fichiers avec certains types d'extensions. Le logiciel NetApp SnapCenter a également été déployé pour gérer les copies Snapshot des serveurs virtuels au sein de l'infrastructure afin d'offrir des copies Snapshot cohérentes au niveau des applications.

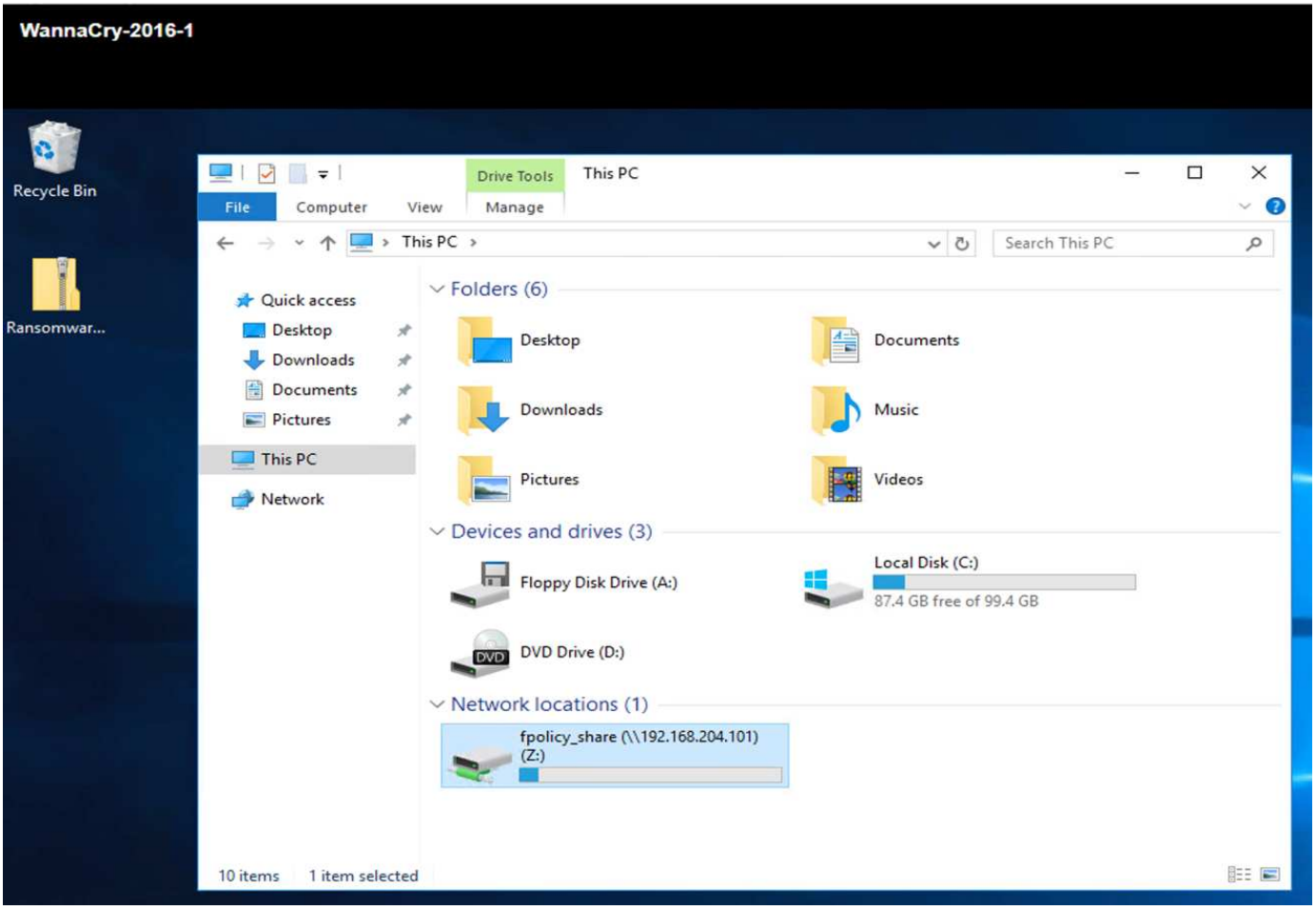
État du serveur virtuel et de ses fichiers avant une attaque

Cette section décrit l'état des fichiers avant une attaque sur la machine virtuelle et le partage CIFS qui lui a été mappé.

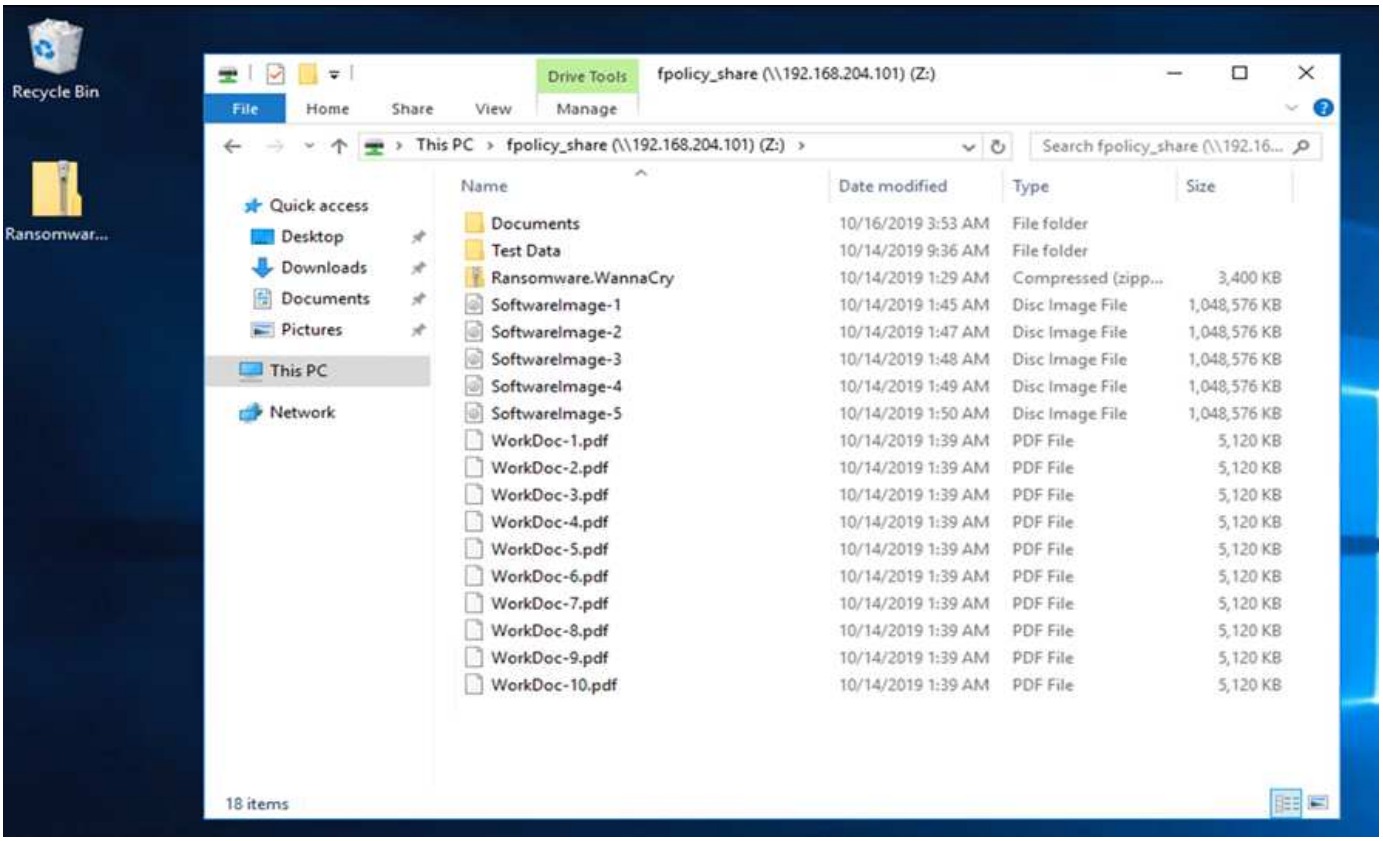
Le dossier documents de la machine virtuelle contient un ensemble de fichiers PDF qui n'ont pas encore été cryptés par le programme malveillant WannaCry.



La capture d’écran suivante montre le partage CIFS qui a été mappé sur la machine virtuelle.



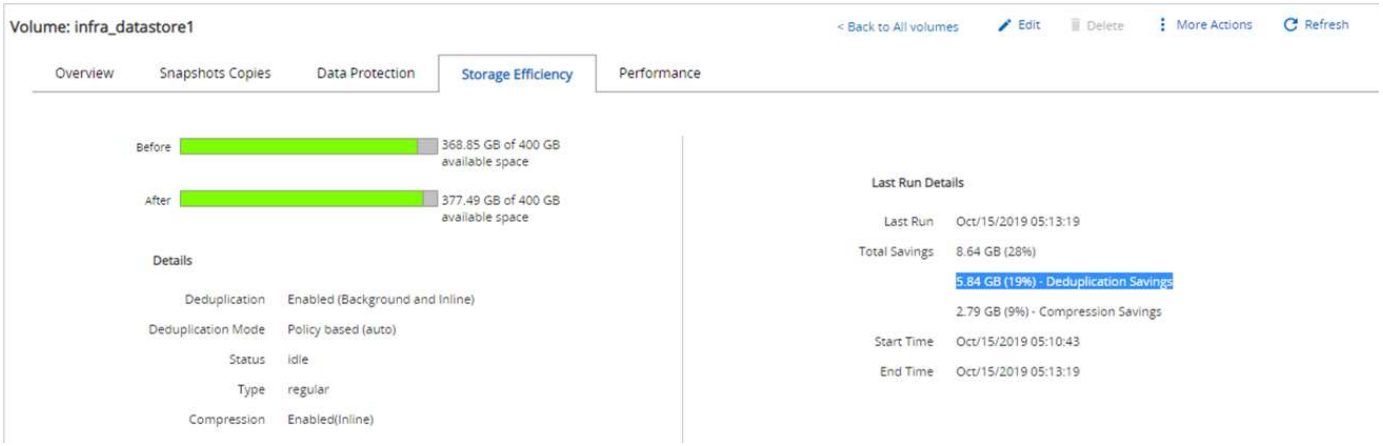
La capture d’écran suivante présente les fichiers du partage CIFS `fpolicy_share` Cela n’a pas encore été chiffré par le programme malveillant de WannaCry.



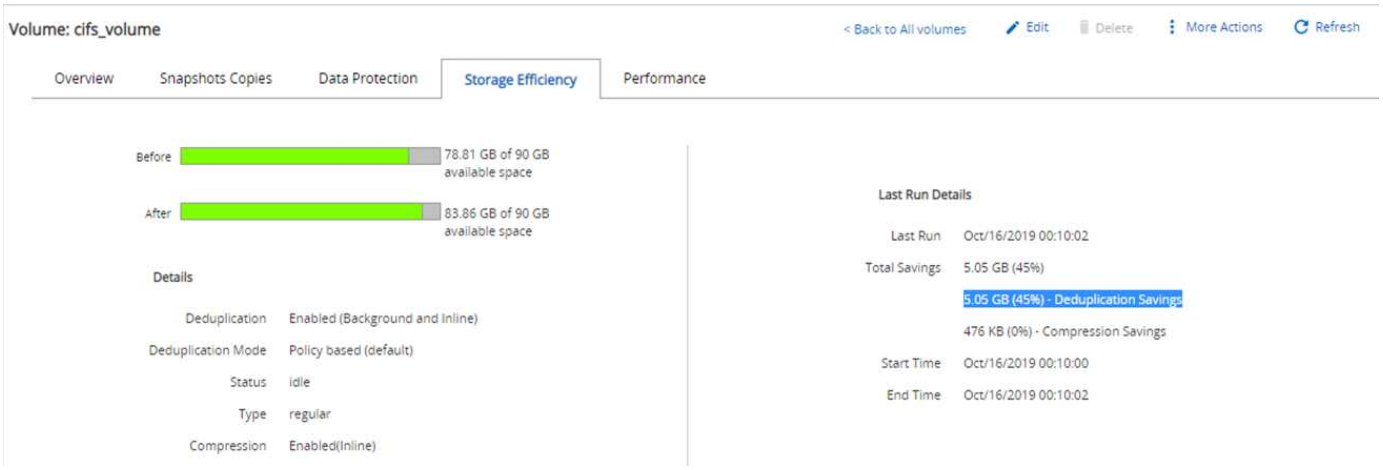
Informations relatives à la déduplication et aux snapshots avant la crise

Les détails sur l'efficacité du stockage et la taille de la copie Snapshot avant une attaque sont indiqués et utilisés comme référence lors de la phase de détection.

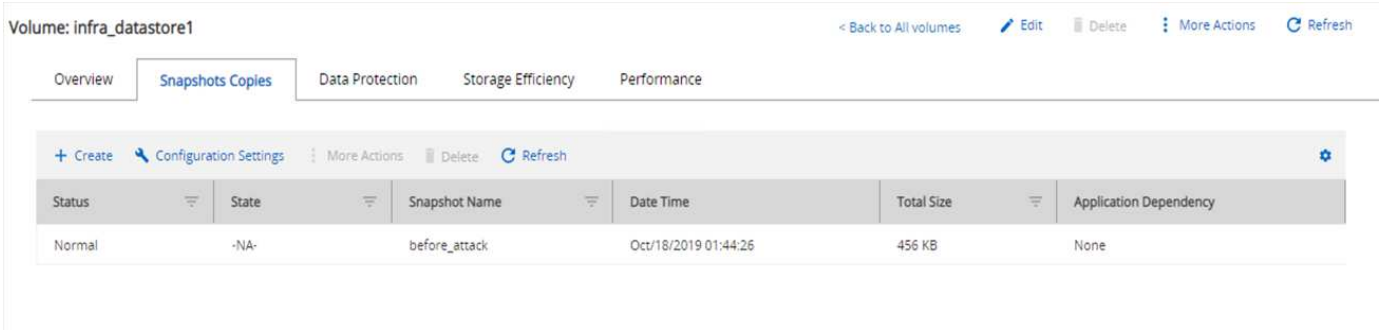
Des économies de stockage de 19 % ont été réalisées grâce à la déduplication sur le volume hébergeant la machine virtuelle.



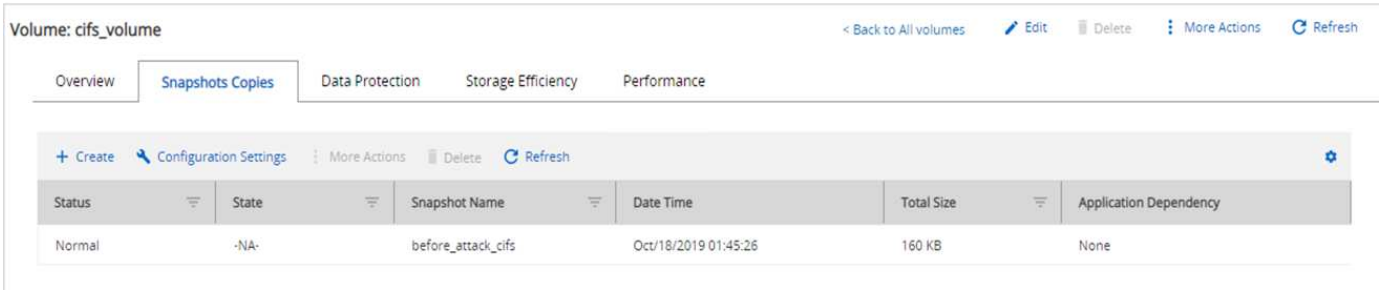
Des économies de stockage de 45 % ont été réalisées grâce à la déduplication sur le partage CIFS `fpolicy_share`.



Une taille de copie Snapshot de 456 Ko a été observée pour le volume hébergeant la machine virtuelle.



Une taille de copie Snapshot de 160 Ko a été observée pour le partage CIFS `fpolicy_share`.



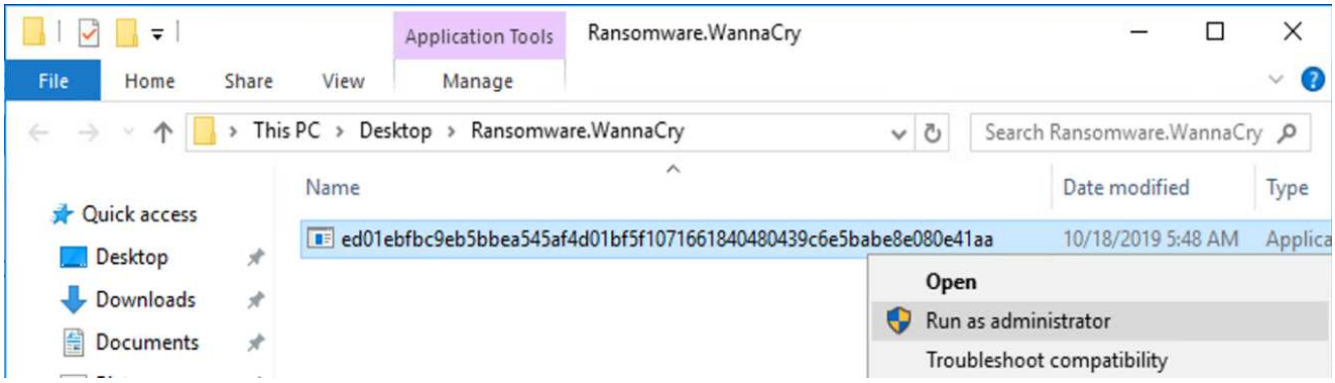
Infection de WannaCry sur VM et partage CIFS

Dans cette section, nous montrons comment le programme malveillant WannaCry a été introduit dans l'environnement FlexPod et les changements ultérieurs au système observés.

Les étapes suivantes montrent comment le binaire du programme malveillant WannaCry a été introduit dans la VM :

1. Le programme malveillant sécurisé a été extrait.

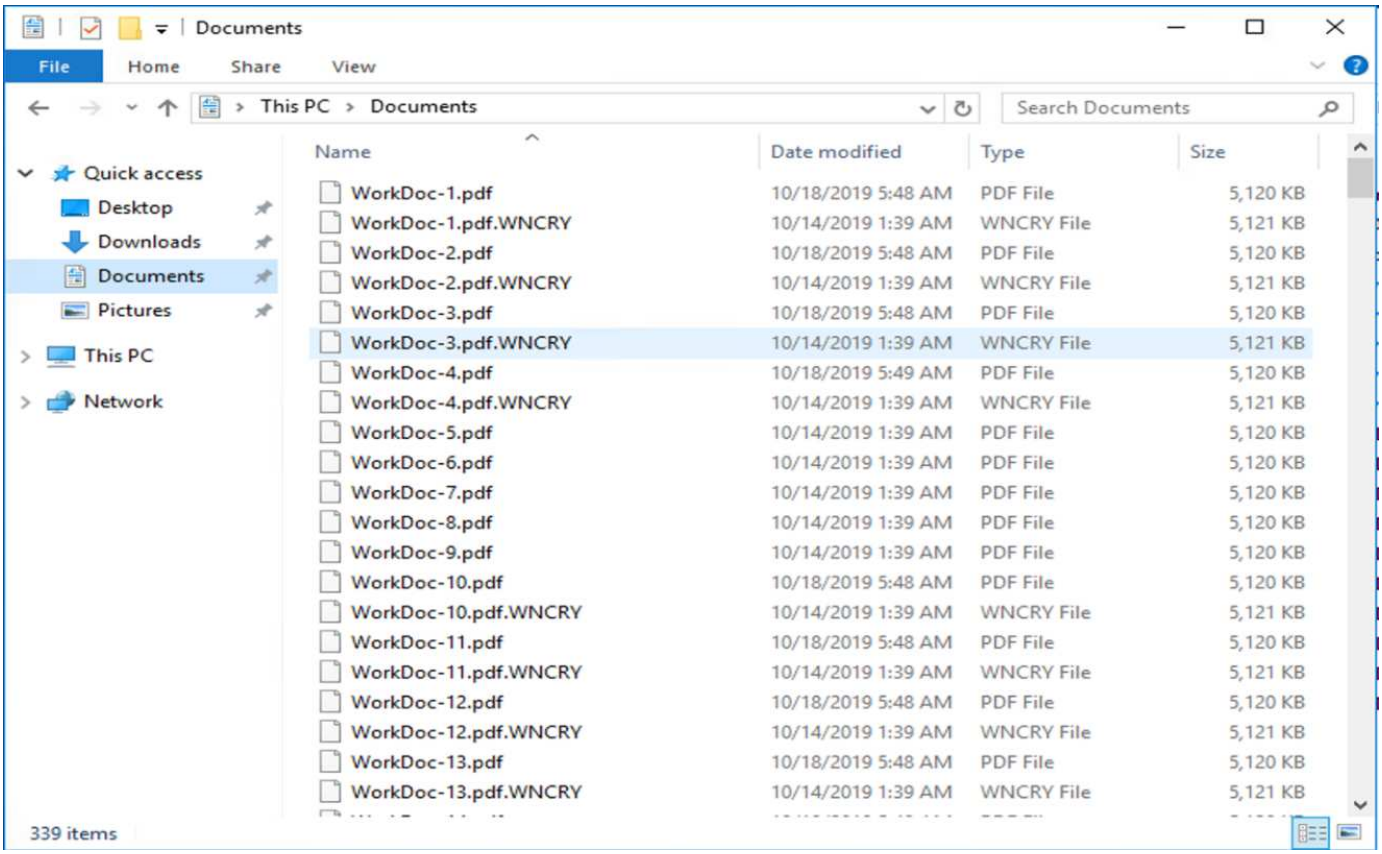
2. Le binaire a été exécuté.



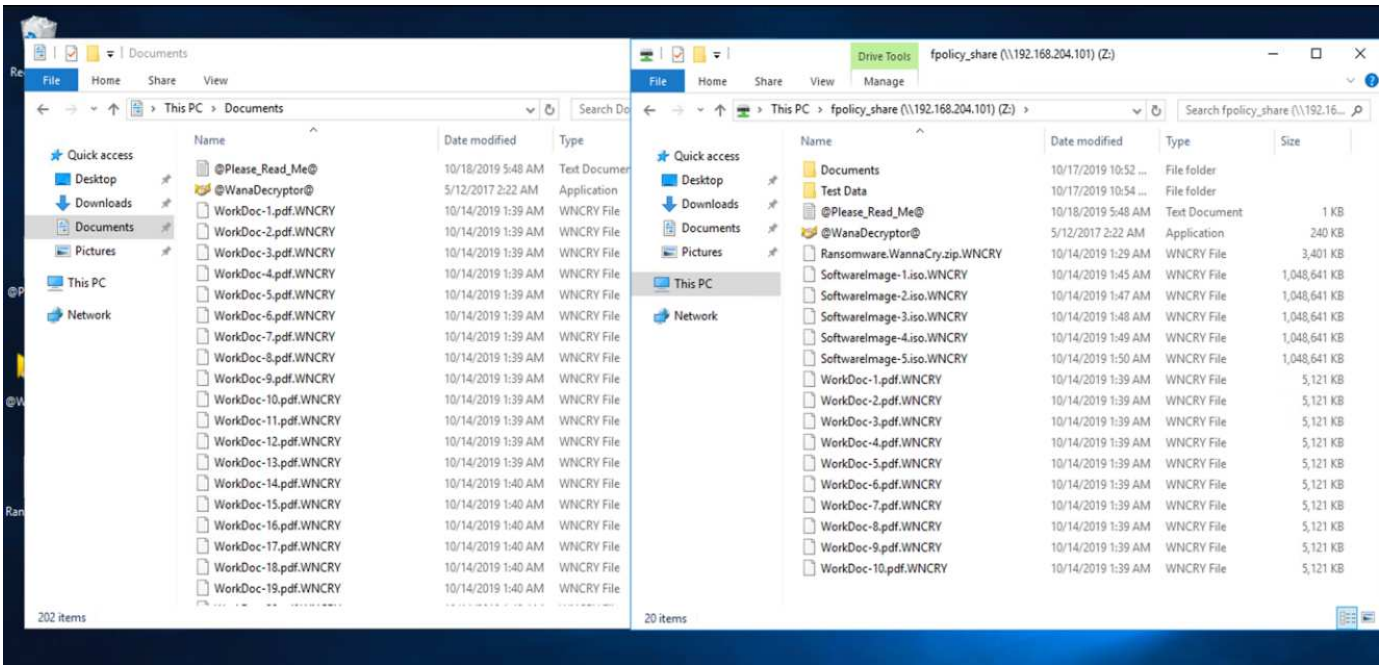
Cas 1 : WannaCry crypte le système de fichiers au sein de la machine virtuelle et le partage CIFS mappé

Le système de fichiers local et le partage CIFS mappé ont été cryptés par le programme malveillant WannaCry.

Le programme malveillant commence à crypter des fichiers avec des extensions WNCRY.



Le programme malveillant crypte tous les fichiers de la machine virtuelle locale et le partage mappé.

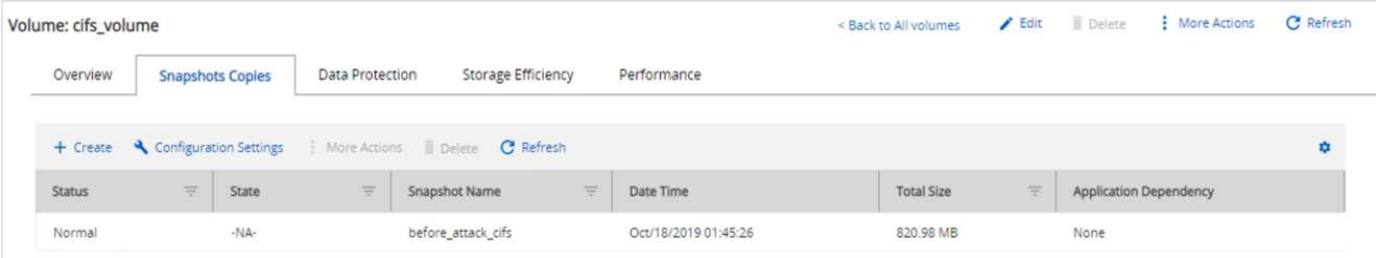


Détection

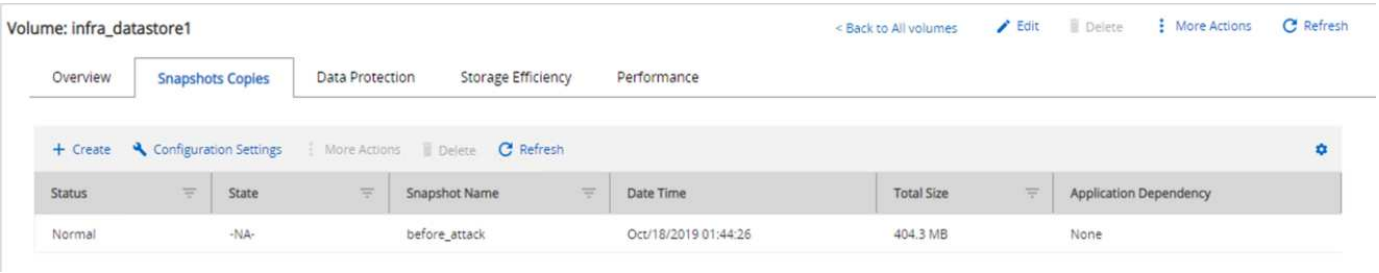
Au moment où le programme malveillant a commencé à chiffrer les fichiers, il a déclenché une augmentation exponentielle de la taille des copies Snapshot et une diminution exponentielle du pourcentage d'efficacité du stockage.

Nous avons détecté une augmentation spectaculaire de la taille de l'instantané à 820.98MB pour le volume

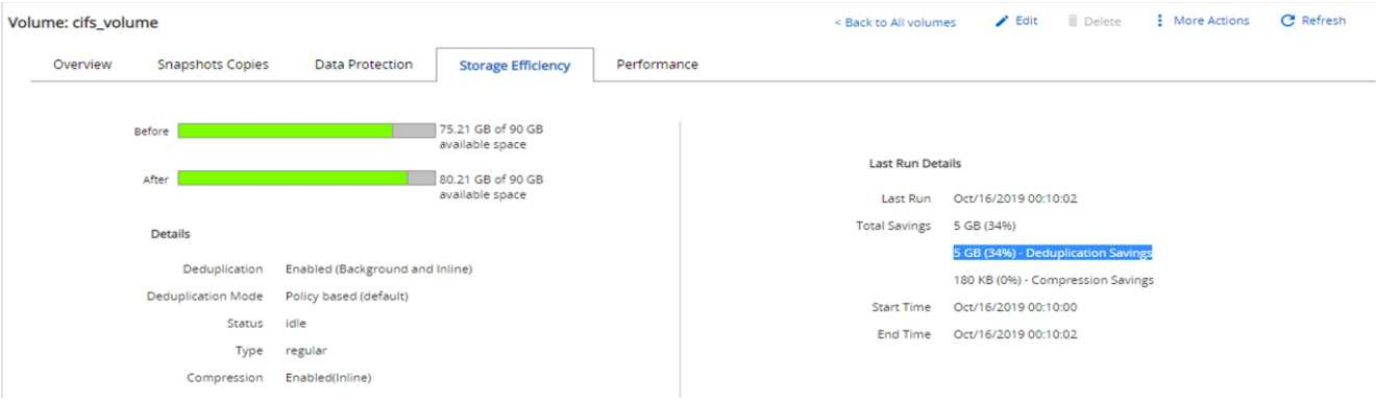
hébergeant le partage CIFS pendant l'attaque.



Nous avons détecté une augmentation de la taille de la copie Snapshot à 404,3 Mo pour le volume hébergeant la machine virtuelle.



L'efficacité du stockage pour le volume hébergeant le partage CIFS a été réduite à 34 %.



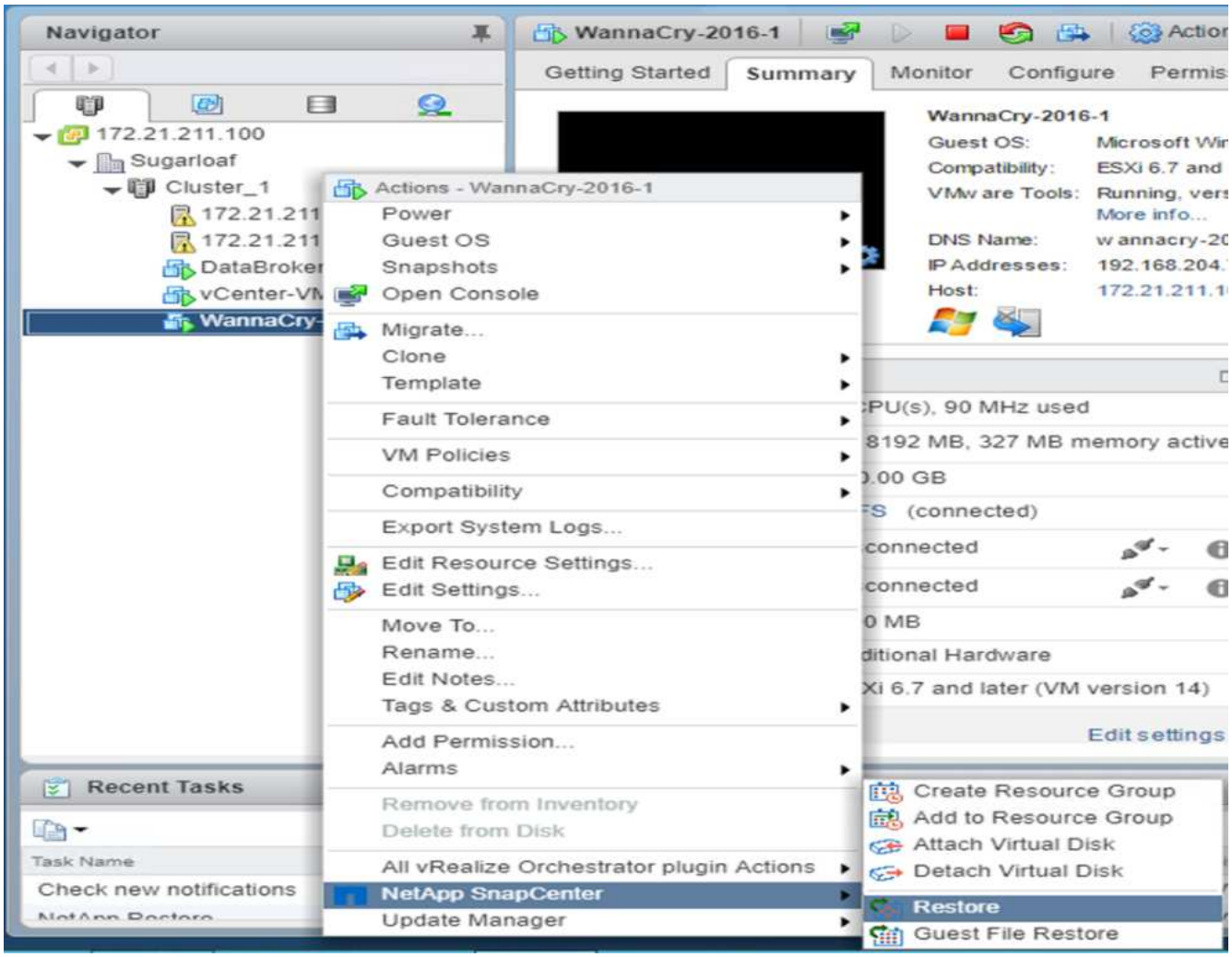
Résolution

Restaurez la machine virtuelle et le partage CIFS mappé à l'aide d'une copie Snapshot complète avant l'attaque.

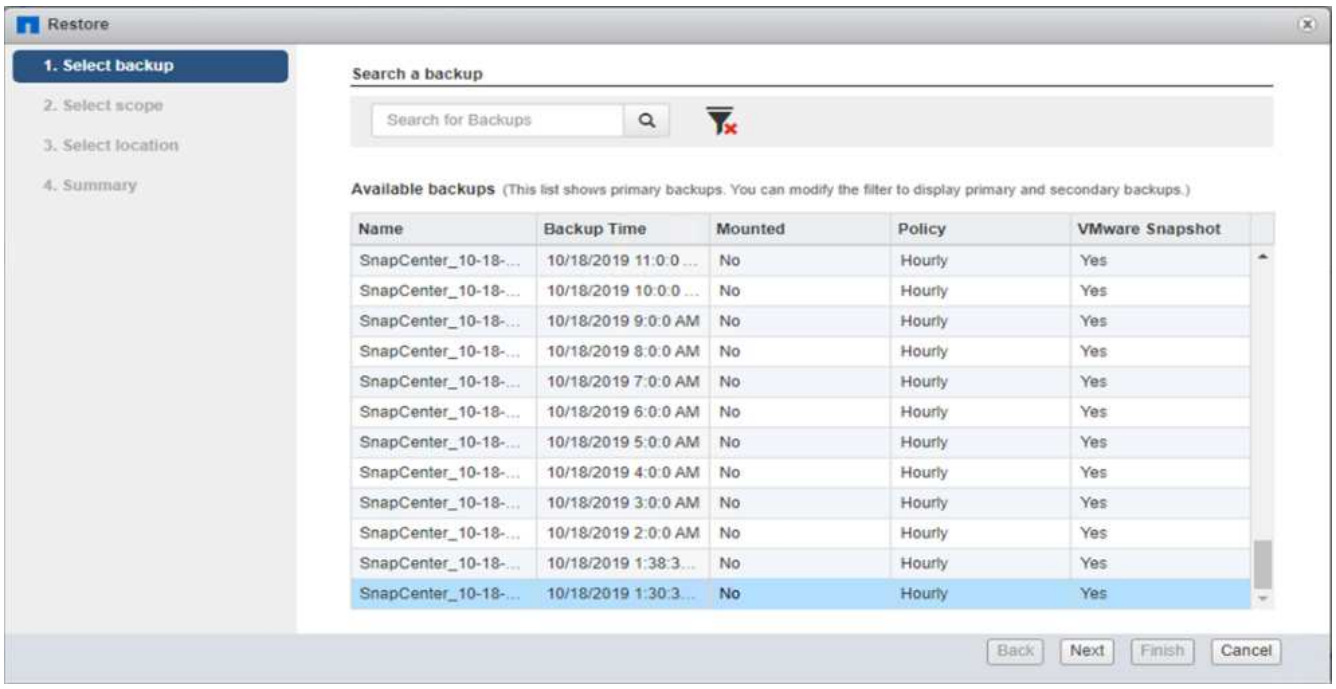
Restaurer VM

Pour restaurer la machine virtuelle, procédez comme suit :

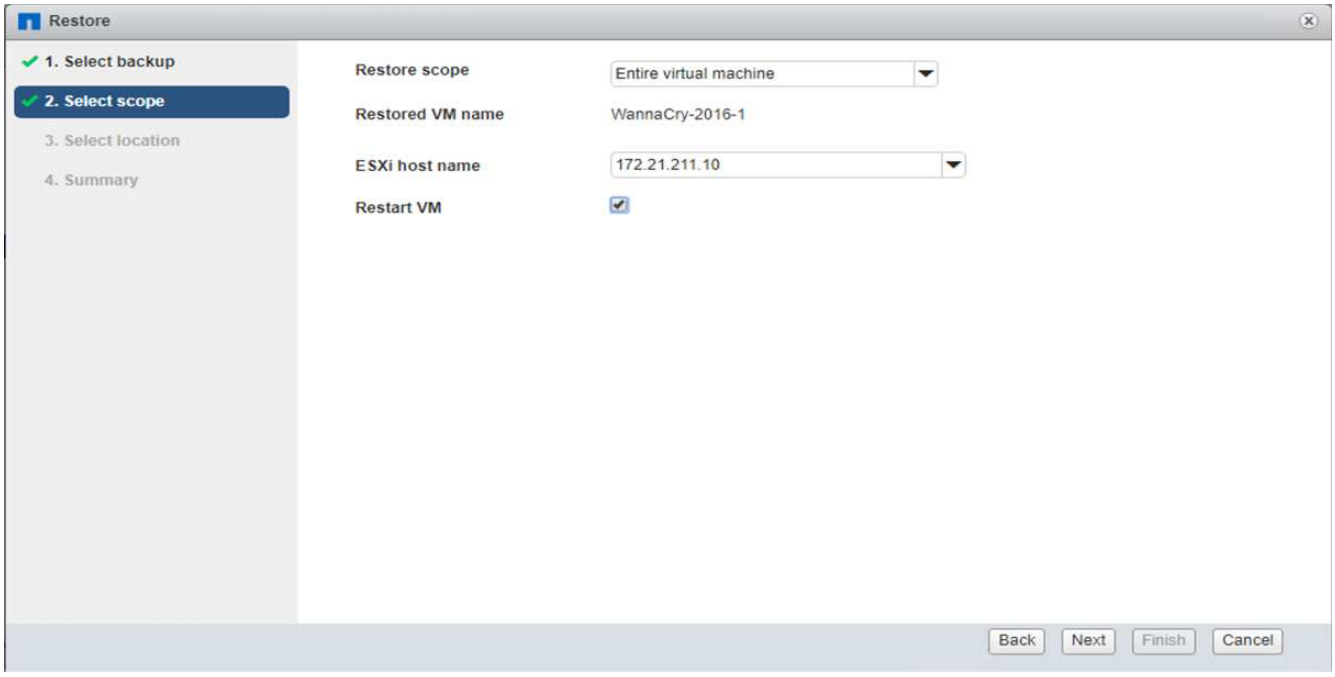
1. Utiliser la copie Snapshot que vous avez créée avec SnapCenter pour restaurer la machine virtuelle.



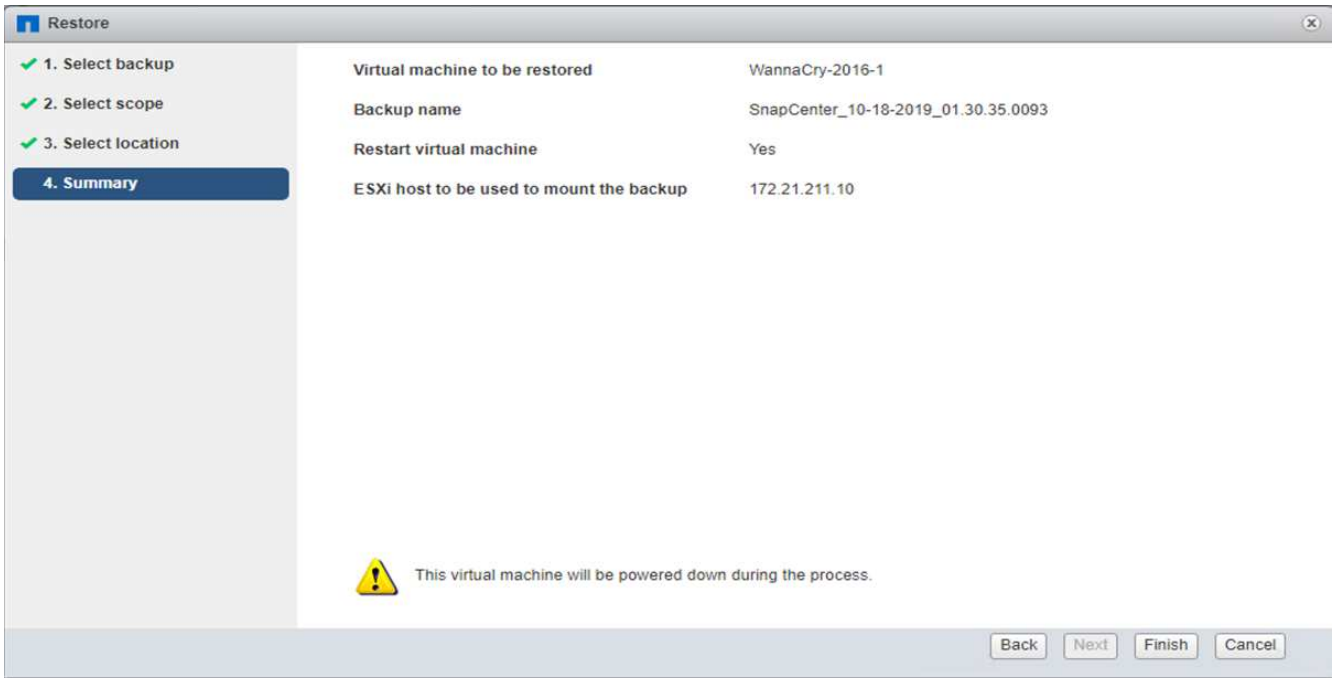
2. Sélectionnez la copie Snapshot cohérente avec VMware souhaitée pour la restauration.



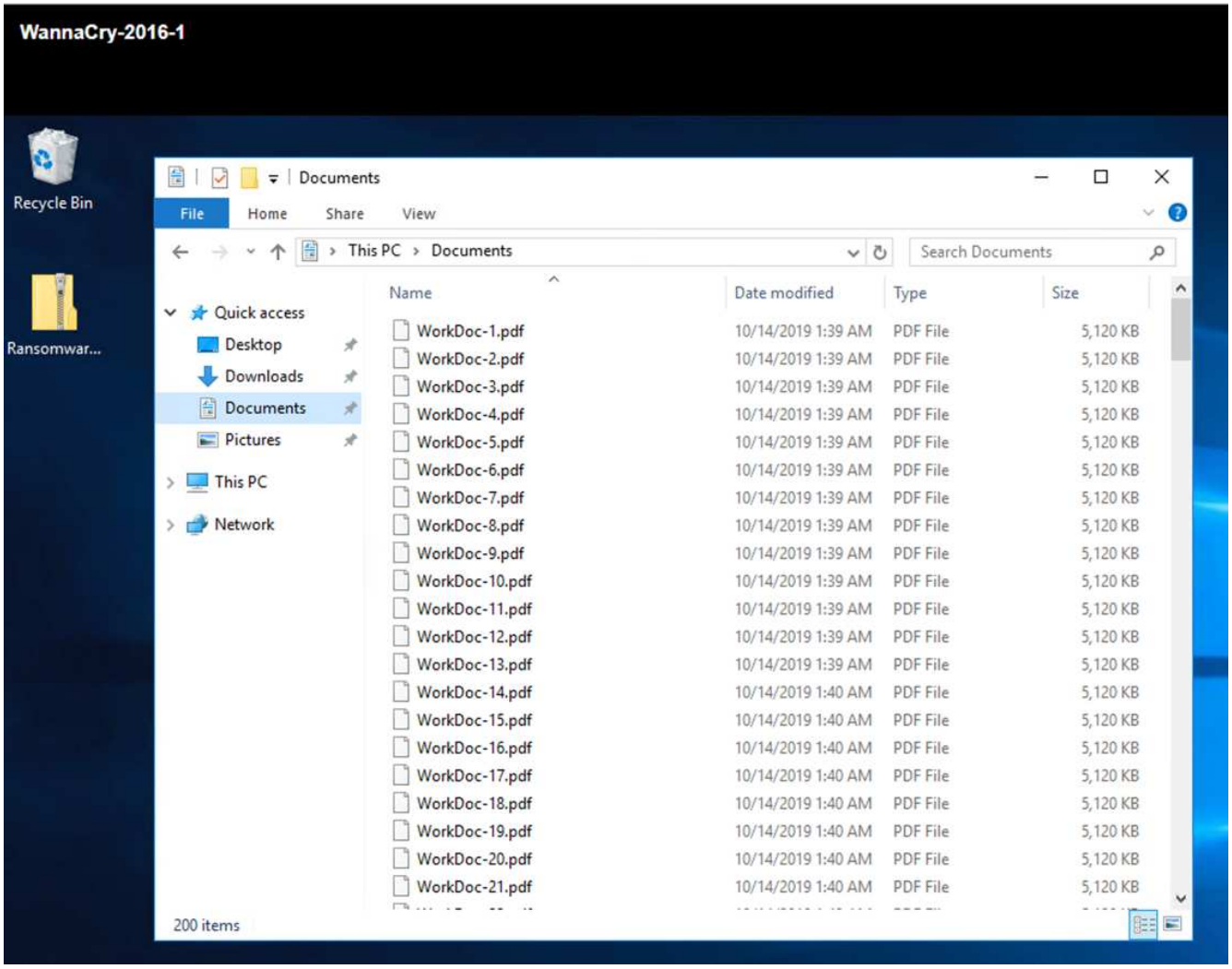
3. L’intégralité du serveur virtuel est restaurée et redémarrée.



4. Cliquez sur Terminer pour lancer le processus de restauration.



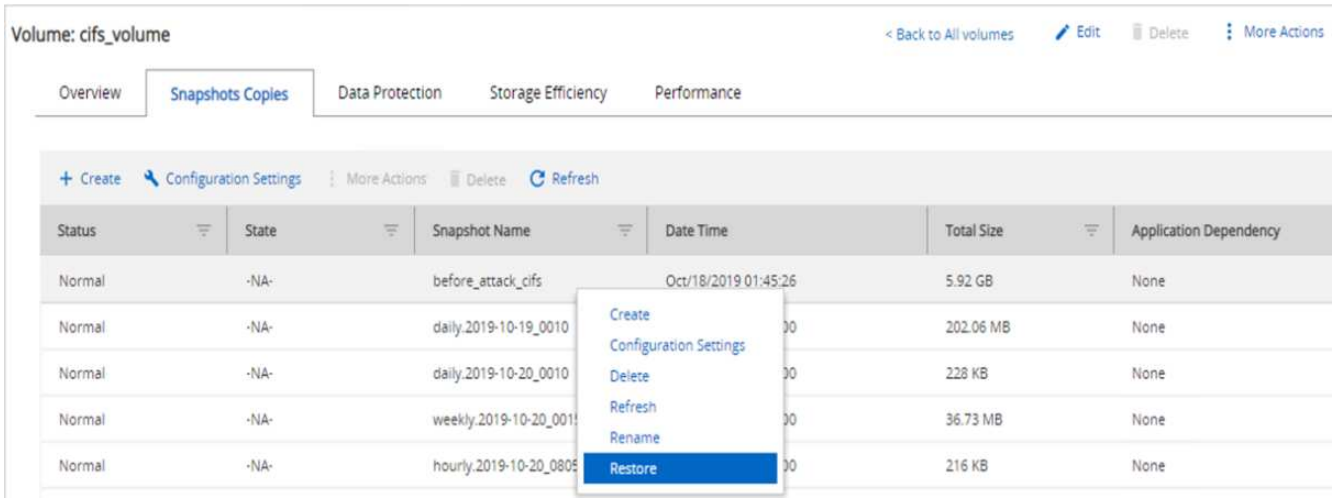
5. La machine virtuelle et ses fichiers sont restaurés.



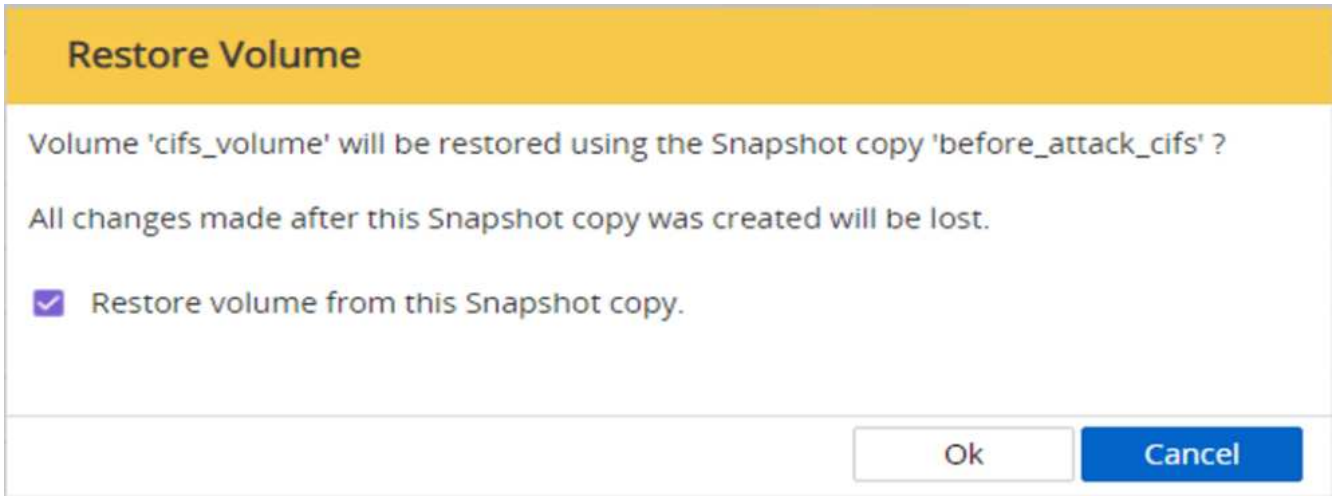
Restaurer le partage CIFS

Pour restaurer le partage CIFS, procédez comme suit :

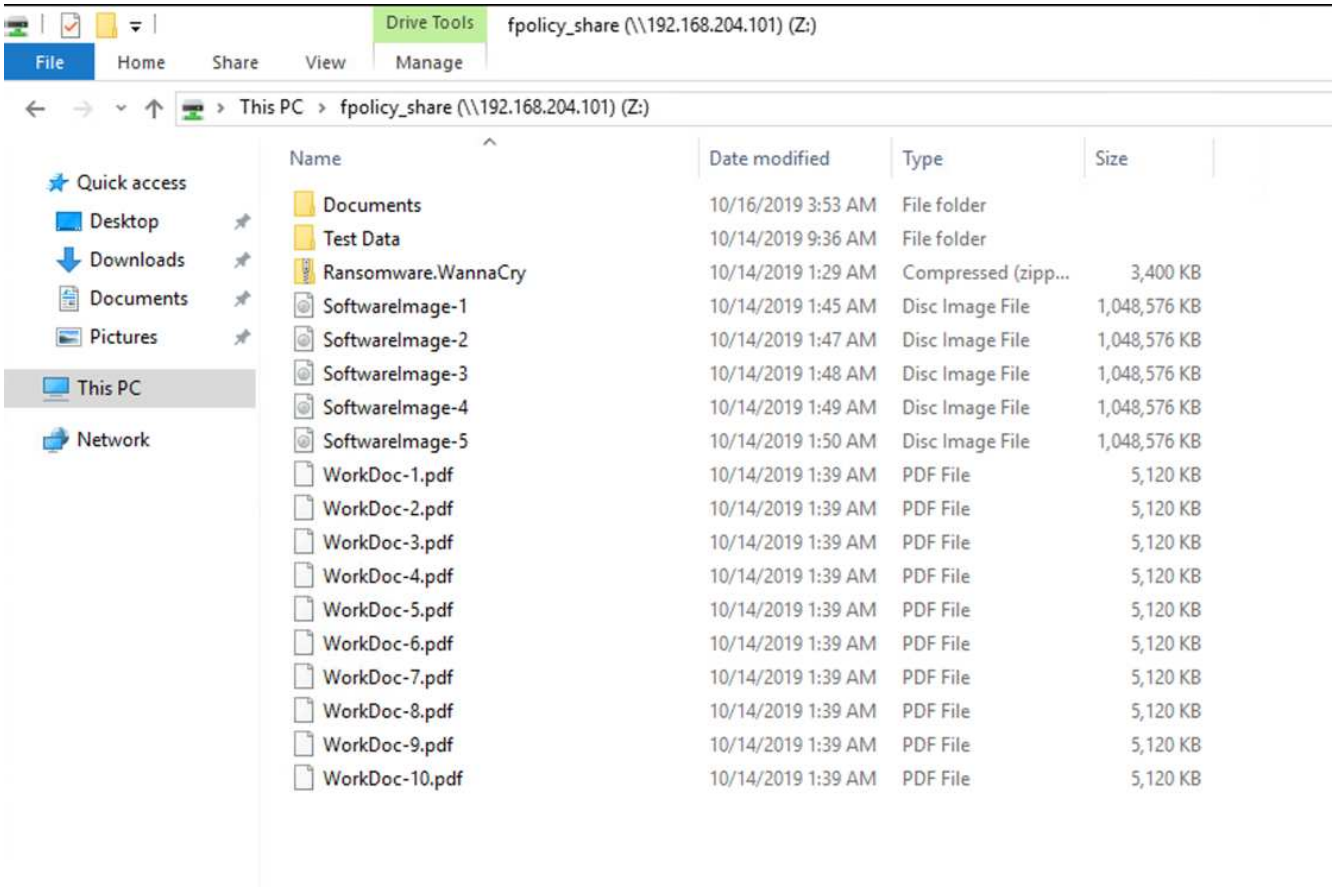
1. Utilisez la copie Snapshot du volume prise avant l'attaque pour restaurer le partage.



2. Cliquez sur OK pour lancer l'opération de restauration.



3. Afficher le partage CIFS après la restauration.



Cas 2 : WannaCry chiffre le système de fichiers au sein de la machine virtuelle et tente de chiffrer le partage CIFS mappé protégé par FPolicy

Prévention

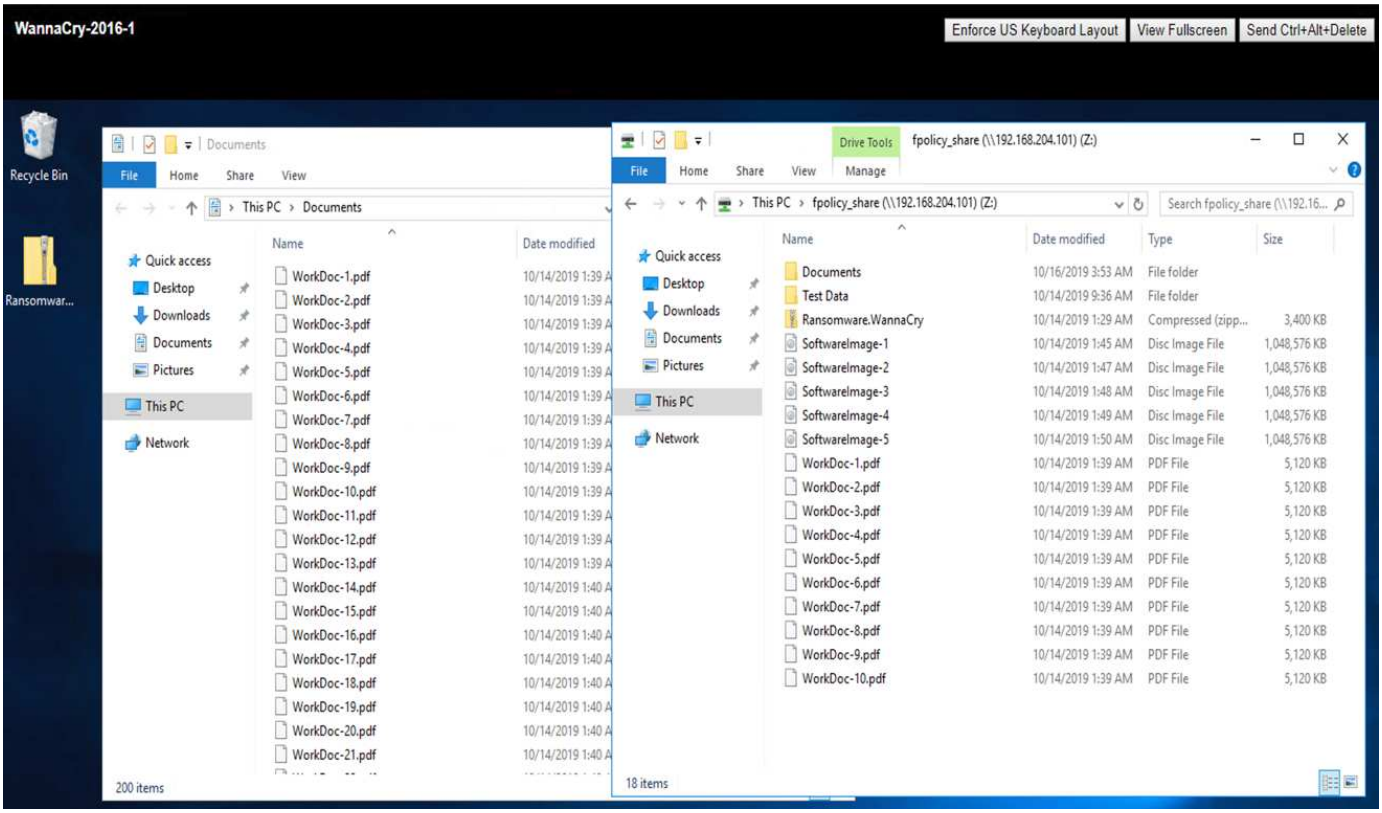
Configurer FPolicy

Pour configurer FPolicy sur le partage CIFS, exécutez les commandes suivantes sur le cluster ONTAP :

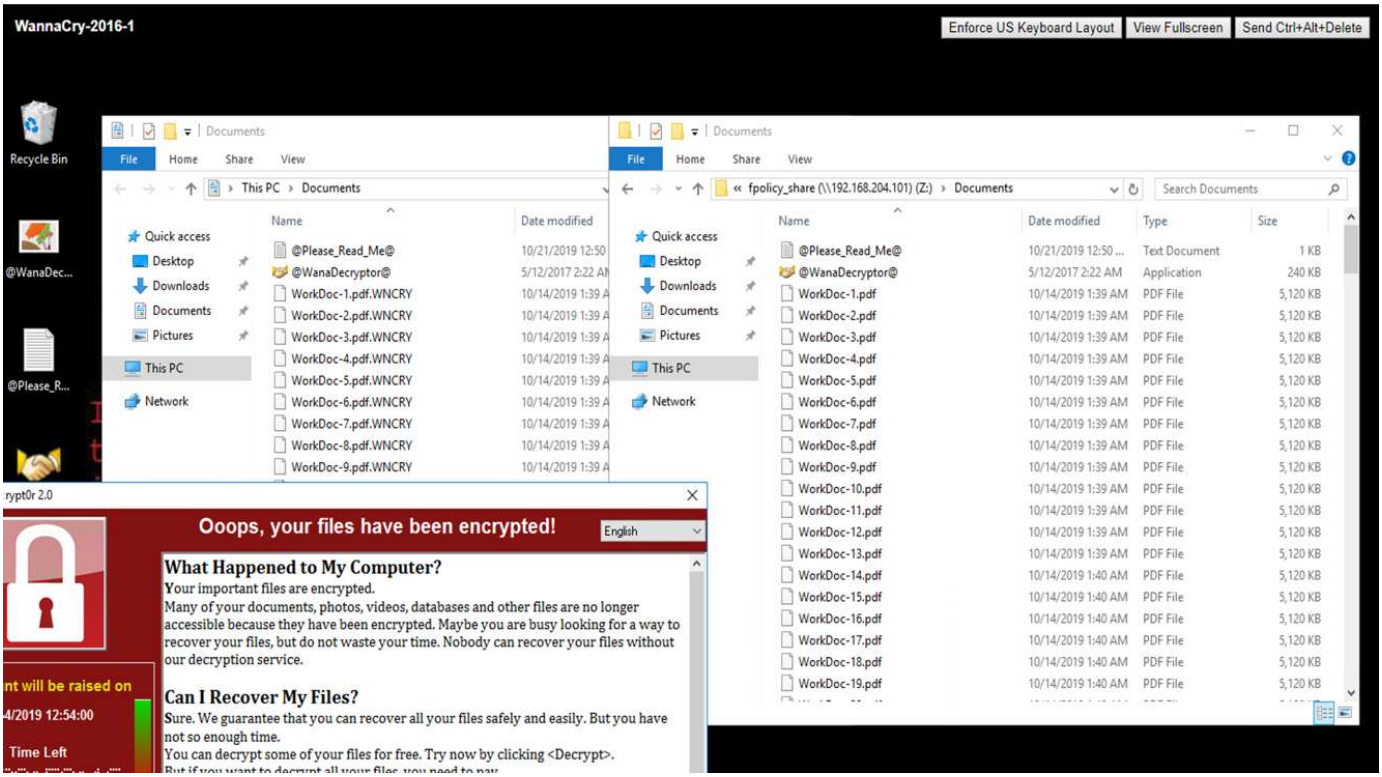
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create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

Avec cette stratégie, les fichiers avec les extensions WNCRY, Locky et ad4c ne sont pas autorisés à effectuer les opérations de création, de renommage, d'écriture ou d'ouverture de fichiers.

Afficher l'état des fichiers avant d'attaquer, ils sont non cryptés et dans un système propre.



Les fichiers de la machine virtuelle sont chiffrés. Le programme malveillant WannaCry tente de crypter les fichiers du partage CIFS, mais FPolicy l'empêche de modifier les fichiers.



Continuez vos activités sans payer de rançon

Les fonctionnalités NetApp décrites dans ce document vous aident à restaurer les données en quelques minutes après une attaque et à éviter les attaques en premier lieu, afin de pouvoir continuer l'activité sans faire l'obstacle.

Un planning de copies Snapshot peut être défini pour atteindre l'objectif de point de récupération souhaité. Les opérations de restauration basées sur des copies Snapshot sont très rapides. Par conséquent, il est possible d'atteindre un objectif de durée de restauration (RTO) très faible.

Par-dessus tout, vous n'avez pas à payer de rançon suite à une attaque, et vous pouvez rapidement revenir à la normale.

Conclusion

Les ransomwares sont un produit de la criminalité organisée et ils n'ont pas d'ordre éthique. Ils peuvent s'abstenir de fournir la clé pour le décryptage même après avoir reçu la rançon. La victime perd non seulement ses données mais aussi une quantité importante d'argent et devra faire face à des conséquences liées à la perte de données de production.

Selon un "Article Forbes", seuls 19 % des victimes d'attaques par ransomware récupèrent leurs données pour autant. Par conséquent, les auteurs recommandent de ne pas payer une rançon en cas d'attaque, car cela renforce la foi de l'attaquant dans leur modèle d'entreprise.

Les opérations de sauvegarde et de restauration de données jouent un rôle important dans la restauration par ransomware. Par conséquent, ils doivent être inclus dans la planification des activités. La mise en œuvre de ces opérations doit être budgétisée de sorte à ce que les capacités de restauration ne puissent faire l'objet d'aucun compromis en cas d'attaque.

Il est important de choisir le partenaire technologique adéquat pour cette transition, et FlexPod propose la plupart des fonctionnalités de manière native, sans frais supplémentaires dans un système FAS 100 % Flash.

Remerciements

L'auteur tient à remercier les personnes suivantes pour leur soutien à la création de ce document :

- Jorge Gomez Navarret, NetApp
- Ganesh Kamath, NetApp

Informations supplémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Logiciel NetApp Snapshot

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

- Gestion des sauvegardes SnapCenter

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

- Conformité des données SnapLock

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

- Documentation produit NetApp

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

- Protection avancée contre les programmes malveillants Cisco (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"

Solution FlexPod conforme à la norme FIPS 140-2 pour le secteur de la sécurité dans le secteur de la santé

Tr-4892 : solution FlexPod conforme à la norme FIPS 140-2 pour le secteur de la santé

JayaKishore Esanakula, NetApp John McAbel, Cisco

La loi HITECH (Health information Technology for Economic and Clinical Health Act) requiert le cryptage certifié FIPS (Federal information Processing Standard) 140-2 des informations de santé électroniques protégées (ePHI). Les applications et logiciels HIT

(Health information Technology) doivent être conformes à la norme FIPS 140-2 pour obtenir la certification « promotion Interoperability Program » (anciennement « Gsignificative Use Incentive Program »). Les prestataires admissibles et les hôpitaux sont tenus d'utiliser un RÉSULTAT conforme à la norme FIPS 140-2 (niveau 1) pour bénéficier d'incentives Medicare et Medicaid et pour éviter les pénalités de remboursement du Centre for Medicare and Medicaid (CMS). Les algorithmes de chiffrement certifiés FIPS 140-2 sont éligibles en tant que dispositifs de sécurité techniques requis conformément au "Règle de sécurité" De la loi américaine sur la transférabilité et la responsabilité en matière d'information médicale (HIPAA).

FIPS 140-2 est une loi américaine norme gouvernementale qui définit les exigences de sécurité pour les modules cryptographiques dans les matériels, les logiciels et les firmwares afin de protéger les informations sensibles. La conformité à la norme est obligatoire pour toute utilisation par les États-Unis les administrations publiques, et elles sont aussi souvent utilisées dans des secteurs réglementés tels que les services financiers et les soins de santé. Ce rapport technique aide le lecteur à comprendre à un niveau élevé la norme de sécurité FIPS 140-2-2. Il aide également le public à comprendre les diverses menaces auxquelles les organismes de santé sont confrontés. Enfin, le rapport technique permet de comprendre comment un système FlexPod conforme à la norme FIPS 140-2 permet de sécuriser les ressources de santé lorsqu'il est déployé sur une infrastructure convergée FlexPod.

Portée

Ce document présente une présentation technique des infrastructures Cisco Unified Computing System (Cisco UCS), Cisco Nexus, Cisco MDS et FlexPod basées sur NetApp ONTAP pour héberger une ou plusieurs applications OU solutions INFORMATIQUES de santé conformes à la norme FIPS 140-2-2.

Public

Ce document est destiné aux leaders techniques du secteur de la santé, aux ingénieurs solutions partenaires Cisco et NetApp et aux équipes des services professionnels. NetApp suppose que le lecteur connaît bien les concepts de dimensionnement du stockage et du calcul, ainsi que la connaissance technique des menaces médicales, de la sécurité sanitaire, des systèmes IT de santé, de Cisco UCS et des systèmes de stockage NetApp.

"Suivant : les menaces de cybersécurité dans le domaine de la santé."

Cyber-menaces dans le secteur de la santé

"Précédent : introduction."

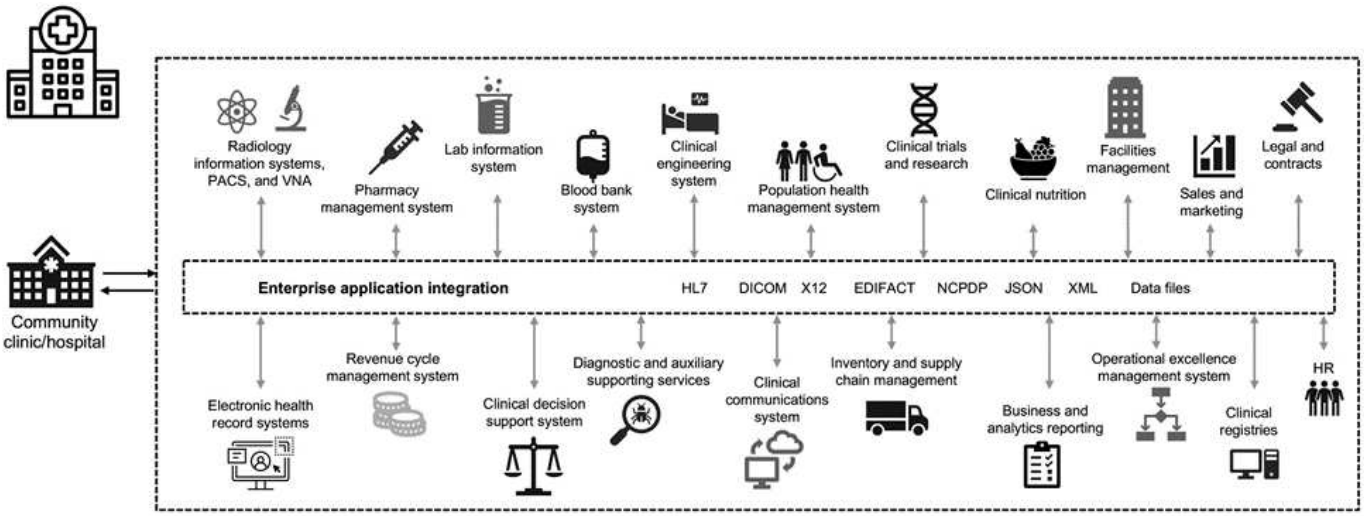
Chaque problème représente une nouvelle opportunité : la pandémie de COVID donne un exemple. Selon un "rapport" Par le programme de cybersécurité du ministère de la Santé et des Services sociaux (HHS), la réponse de la COVID a entraîné l'augmentation du nombre d'attaques par ransomware. Il y avait 6,000 nouveaux domaines Internet enregistrés juste au cours de la troisième semaine de mars 2020. Plus de 50 % des domaines ont hébergé des programmes malveillants. Les attaques par ransomware étaient responsables de près de 50 % de l'ensemble des violations de données de santé en 2020 et touchent plus de 630 organismes de santé et environ 29 millions de dossiers médicaux. Dix-neuf béchers/sites ont doublé l'extorsion. Avec un taux de 24.5 %, le secteur de la santé a été considéré comme la plus forte violation de données en 2020.

Les agents malveillants ont tenté de violer la sécurité et la confidentialité des informations médicales protégées (PHI) en vendant ces informations ou en menaçant de les détruire ou de les exposer. Des tentatives ciblées et de diffusion en masse sont fréquemment effectuées pour obtenir un accès non autorisé à l'ePHI. Environ 75 % des dossiers patient exposés au cours de la seconde moitié de 2020 étaient dus à des relations professionnelles compromises.

La liste suivante des organismes de soins de santé était ciblée par les agents malveillants :

- Systèmes hospitaliers
- Laboratoires de sciences de la vie
- Laboratoires de recherche
- Installations de réhabilitation
- Hôpitaux et cliniques communautaires

La diversité des applications qui constituent une organisation de soins de santé est indéniable et de plus en plus complexe. Les bureaux de la sécurité de l'information doivent assurer la gouvernance d'une grande variété de systèmes ET ressources IT. La figure suivante illustre les capacités cliniques d'un système hospitalier type.



Les données patient sont au cœur de cette image. La perte de données sur les patients et la stigmatisation associée aux affections médicales sensibles sont très réelles. Parmi les autres questions sensibles figurent le risque d'exclusion sociale, le chantage, le profilage, la vulnérabilité au marketing ciblé, l'exploitation et la responsabilité financière potentielle envers les payeurs à propos de l'information médicale au-delà des privilèges du payeur.

Les menaces pour les soins de santé sont multidimensionnelles dans la nature et dans l'impact. Les gouvernements du monde entier ont adopté diverses dispositions pour sécuriser les renseignements médicaux personnels. Les effets néfastes et la nature évolutive des menaces qui pèsent sur les soins de santé rendent difficile la défense de toutes les menaces.

Voici une liste de menaces courantes identifiées dans le domaine de la santé :

- Attaques par ransomware
- Perte ou vol d'équipement ou de données contenant des informations sensibles
- Attaques de phishing

- Attaques contre des dispositifs médicaux connectés pouvant affecter la sécurité du patient
- Envoyez un e-mail aux attaques de phishing
- Perte ou vol d'équipement ou de données
- Compromis sur le protocole des postes de travail à distance
- Vulnérabilité logicielle

Les établissements de santé opèrent dans un environnement juridique et réglementaire aussi complexe que leurs écosystèmes numériques. Cet environnement inclut, sans s'y limiter, les éléments suivants :

- Bureau du coordonnateur national (pour la technologie des soins de santé) normes d'interopérabilité des technologies de l'information en santé électroniques certifiées ONC
- Accès à l'assurance-santé et Loi sur la réautorisation du Programme d'assurance-santé pour enfants (MACRA)/utilisation significative
- Obligations multiples en vertu de la Food and Drug Administration (FDA)
- Les processus d'accréditation de la Commission mixte
- Exigences HIPAA
- Exigences HITECH
- Normes de risque minimales acceptables pour les payeurs
- Règles de confidentialité et de sécurité
- Loi fédérale sur la modernisation de la sécurité de l'information exigences intégrées aux contrats fédéraux et aux subventions de recherche par l'intermédiaire d'organismes comme les National Institutes of Health
- Norme de sécurité de l'industrie des cartes de paiement (PCI-DSS)
- Exigences relatives à la gestion des services de santé mentale et de toxicomanie (SAMHSA)
- Loi Gramm-Leach-Bliley pour le traitement financier
- La loi Stark en ce qui concerne la prestation de services aux organisations affiliées
- Loi sur les droits à l'éducation familiale et la protection des renseignements personnels (FERPA) pour les institutions qui participent à l'enseignement supérieur
- Loi sur la non-discrimination en matière d'information génétique (GINA)
- Le nouveau Règlement général sur la protection des données (RGPD) dans l'Union européenne

Les normes d'architecture de sécurité évoluent rapidement pour empêcher les acteurs malveillants d'affecter les systèmes d'information de santé. L'une de ces normes est la norme FIPS 140-2, définie par l'Institut national des normes et de la technologie (NIST). La publication FIPS 140-2 détaille le niveau américain exigences gouvernementales pour un module cryptographique. Les exigences de sécurité couvrent les domaines liés à la conception et à l'implémentation sécurisées d'un module cryptographique et peuvent être appliqués à HIT. Les frontières cryptographiques bien définies facilitent la gestion de la sécurité tout en restant à jour avec les modules cryptographiques. Ces limites permettent d'éviter les faibles modules de cryptage qui peuvent être facilement exploités par des acteurs malveillants. Ils permettent également d'éviter les erreurs humaines lors de la gestion de modules cryptographiques standard.

Le NIST, de concert avec le Centre de sécurité des communications (CSE), a mis en place le Programme de validation du module cryptographique (CMVP) pour certifier les modules cryptographiques des niveaux de validation FIPS 140-2. Grâce à un module certifié FIPS 140-2-2, les organismes fédéraux doivent protéger leurs données sensibles ou précieuses tout en transit. En raison de sa réussite dans la protection des informations sensibles ou précieuses, de nombreux systèmes de santé ont choisi de crypter les informations médicales confidentielles à l'aide de modules cryptographiques FIPS 140-2 au-delà du niveau de sécurité

minimum requis par la loi.

L'exploitation et la mise en œuvre des fonctionnalités FlexPod FIPS 140-2 ne prennent que des heures (et non plusieurs jours). La plupart des organismes de santé, quelle que soit leur taille, sont à la portée de la conformité avec la norme FIPS. Avec des limites de chiffrement clairement définies et des étapes de mise en œuvre simples et bien documentées, une architecture FlexPod conforme à la norme FIPS 140-2 peut constituer une base de sécurité solide pour l'infrastructure. De plus, des améliorations simples permettent d'améliorer encore la protection contre les menaces de sécurité.

"Présentation de la norme FIPS 140-2."

Présentation de la norme FIPS 140-2

"Précédent : cyber-menaces dans le domaine de la santé."

"FIPS 140-2" spécifie les exigences de sécurité pour un module cryptographique utilisé dans un système de sécurité qui protège les informations sensibles dans les systèmes informatiques et de télécommunication. Un module cryptographique doit être un ensemble de matériel, de logiciels, de micrologiciels ou une combinaison. FIPS s'applique aux algorithmes cryptographiques, à la génération de clés et aux gestionnaires de clés contenus dans une limite cryptographique. Il est important de comprendre que la norme FIPS 140-2 s'applique spécifiquement au module cryptographique et non au produit, à l'architecture, aux données ou à l'écosystème. Le module cryptographique, qui est défini dans les termes clés plus loin dans ce document, est le composant spécifique (qu'il s'agisse du matériel, du logiciel et/ou du micrologiciel) qui implémente des fonctions de sécurité approuvées. La norme FIPS 140-2 spécifie également quatre niveaux. Les algorithmes cryptographiques approuvés sont communs à tous les niveaux. Voici les éléments clés et exigences de chaque niveau de sécurité :

- **Niveau de sécurité 1**
  - Spécifie les exigences de sécurité de base pour un module cryptographique (au moins un algorithme ou une fonction de sécurité approuvé est nécessaire).
  - Aucun mécanisme de sécurité physique spécifique n'est requis pour le niveau 1 au-delà des exigences de base pour les composants de qualité de production.
- **Niveau de sécurité 2**
  - Améliore les mécanismes de sécurité physique en ajoutant la nécessité de preuves d'inviolabilité en utilisant des solutions inviolables telles que des revêtements ou des joints, des verrous sur des capots ou portes amovibles des modules cryptographiques.
  - Exige, au minimum, que le contrôle d'accès basé sur des rôles (RBAC) dans lequel le module cryptographique authentifie l'autorisation d'un opérateur ou d'un administrateur d'assumer un rôle spécifique et exécute un ensemble de fonctions correspondant.
- **Niveau de sécurité 3**
  - S'appuie sur les exigences inviolables du niveau 2 et tente d'empêcher un accès plus poussé aux paramètres de sécurité critiques (CSP) au sein du module cryptographique.
  - Les mécanismes de sécurité physique requis au niveau 3 sont destinés à avoir une forte probabilité de détecter et de répondre aux tentatives d'accès physique ou à toute utilisation ou modification du module cryptographique. Il peut s'agir, par exemple, de boîtiers forts, d'une détection d'autosurveillance et de circuits de réponse qui zéros tous les CSP en texte clair lorsqu'un capot

amovible sur le module cryptographique est ouvert.

- Nécessite des mécanismes d'authentification basés sur les identités pour renforcer la sécurité des mécanismes RBAC spécifiés au niveau 2. Un module cryptographique authentifie l'identité d'un opérateur et vérifie que celui-ci est autorisé à utiliser un rôle et à exécuter les fonctions du rôle.

- **Niveau de sécurité 4**
  - Le plus haut niveau de sécurité de la norme FIPS 140-2.
  - Le niveau le plus utile pour les opérations dans les environnements physiquement non protégés.
  - À ce niveau, les mécanismes de sécurité physique sont conçus pour fournir une protection complète autour du module cryptographique, qui est responsable de détecter et de répondre à toute tentative non autorisée d'accès physique.
  - La pénétration ou l'exposition du module cryptographique devrait avoir une forte probabilité de détection et entraîner la mise à zéro immédiate de tous les CSP non sécurisés ou en texte clair.

"Ensuite, plan de contrôle et plan de données."

Plan de contrôle et plan de données

"Précédent : présentation de la norme FIPS 140-2."

Lors de la mise en œuvre d'une stratégie FIPS 140-2-2, il est important de comprendre ce qui est protégé. Elle peut facilement être divisée en deux zones : le plan de contrôle et le plan de données. Un plan de contrôle se réfère aux aspects ayant un impact sur le contrôle et le fonctionnement des composants au sein du système FlexPod : par exemple, accès administratif aux contrôleurs de stockage NetApp, commutateurs Cisco Nexus et serveurs Cisco UCS. La protection à cette couche est assurée par la limitation des protocoles et des gestionnaires cryptographiques que les administrateurs peuvent utiliser pour se connecter aux périphériques et apporter des modifications. Un plan de données fait référence aux informations réelles, telles que les informations médicales personnelles, dans le système FlexPod. Ces données sont protégées par chiffrement des données au repos, puis à nouveau pour la norme FIPS, garantissant ainsi que les modules de chiffrement utilisés respectent les normes.

"Nœuds de calcul FlexPod Cisco UCS et FIPS 140-2"

Les ressources de calcul FlexPod Cisco UCS et FIPS 140-2

"Précédent : plan de contrôle par rapport au plan de données."

Une architecture FlexPod peut être conçue avec un serveur Cisco UCS conforme à la norme FIPS 140-2-2. Conformément à la norme U. S. Le serveur Cisco UCS, NIST, peut fonctionner en mode de conformité FIPS 140-2 de niveau 1. Pour obtenir la liste complète des composants Cisco compatibles FIPS, reportez-vous à la section "La page FIPS 140 de Cisco". Cisco UCS Manager est certifié FIPS 140-2-2.

Cisco UCS et Fabric Interconnect

Cisco UCS Manager est déployé et s'exécute à partir des interconnexions de fabric Cisco (IF).

Pour plus d'informations sur Cisco UCS et sur l'activation de FIPS, reportez-vous au "Documentation Cisco UCS Manager".

Pour activer le mode FIPS sur le Cisco Fabric Interconnect sur chaque structure A et B, exécutez les commandes suivantes :

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

Pour remplacer un SYSTÈME DE CLUSTER sur Cisco UCS Manager version 3.2(3) par UN FI disponible dans une version antérieure à Cisco UCS Manager version 3.2(3), désactivez le mode FIPS (désactivez-les `fips-mode`) Sur le FI existant avant d'ajouter le FI de remplacement au cluster. Une fois le cluster formé, dans le cadre du démarrage de Cisco UCS Manager, le mode FIPS est automatiquement activé.

Cisco propose les produits clés suivants pouvant être implémentés au niveau de la couche de calcul ou d'application :

- **Cisco Advanced Malware protection (AMP) pour les noeuds finaux.** pris en charge sur les systèmes d'exploitation Microsoft Windows et Linux, cette solution intègre des capacités de prévention, de détection et de réponse. Ce logiciel de sécurité évite les failles de sécurité, bloque les programmes malveillants au point d'entrée et surveille et analyse en continu les activités des fichiers et des processus afin de détecter, de contenir et de corriger rapidement les menaces qui peuvent échapper aux défenses en première ligne. Le composant de protection contre les activités malveillantes (MAP) de l'AMP surveille en permanence toute l'activité des points finaux et assure la détection des temps d'exécution et le blocage du comportement anormal d'un programme en cours d'exécution sur le point final. Par exemple, lorsque le comportement de terminal indique un ransomware, les processus incriminés se terminent, ce qui empêche le chiffrement du terminal et arrête l'attaque.
- **AMP pour la sécurité des e-mails** les e-mails sont devenus le véhicule principal pour propager des programmes malveillants et mener à bien des cyberattaques. En moyenne, environ 100 milliards d'e-mails sont échangés en une seule journée, ce qui fournit aux pirates un excellent vecteur de pénétration dans les systèmes des utilisateurs. Par conséquent, il est absolument essentiel de se défendre contre cette ligne d'attaque. AMP analyse les e-mails contre les menaces, telles que les attaques sans jour et les logiciels malveillants furtifs cachés dans des pièces jointes malveillantes. Il utilise également des informations URL de pointe pour lutter contre les liens malveillants. Elle offre aux utilisateurs une protection avancée contre le phishing ciblé, les attaques par ransomware et d'autres attaques sophistiquées.
- **Système de prévention des intrusions nouvelle génération (NGIPS).** Cisco FirePOWER NGIPS peut être déployé en tant qu'appliance physique dans le centre de données ou en tant qu'appliance virtuelle sur VMware (NGIPSv pour VMware). Ce système hautement efficace de prévention des intrusions offre des performances fiables et un faible coût total de possession. La protection contre les menaces peut être étendue avec des licences d'abonnement facultatives pour fournir AMP, visibilité et contrôle des applications, ainsi que des fonctionnalités de filtrage des URL. Le système NGIPS virtualisé inspecte le trafic entre les machines virtuelles et facilite le déploiement et la gestion des solutions NGIPS sur des sites disposant de ressources limitées, ce qui renforce la protection des ressources physiques et virtuelles.

"FlexPod : connectivité réseau Cisco et FIPS 140-2."

Les réseaux FlexPod Cisco et FIPS 140-2

"Précédent : calcul FlexPod Cisco UCS et FIPS 140-2."

Cisco MDS

La plateforme Cisco MDS 9000 avec logiciel 8.4.x est "Conforme à la norme FIPS 140-2". Cisco MDS implémente des modules cryptographiques et les services suivants pour SNMPv3 et SSH.

- Établissement de session prenant en charge chaque service
- Tous les algorithmes cryptographiques sous-jacents prenant en charge les fonctions de dérivation des clés de service
- Hachage pour chaque service
- Chiffrement symétrique pour chaque service

Avant d'activer le mode FIPS, effectuez les tâches suivantes sur le commutateur MDS :

1. Faites de vos mots de passe un minimum de huit caractères.
2. Désactivez Telnet. Les utilisateurs doivent se connecter à l'aide de SSH uniquement.
3. Désactivez l'authentification à distance via RADIUS/TACACS+. Seuls les utilisateurs locaux du commutateur peuvent être authentifiés.
4. Désactivez SNMP v1 et v2. Tout compte utilisateur existant sur le commutateur qui a été configuré pour SNMPv3 doit être configuré uniquement avec SHA pour l'authentification et AES/3DES pour la confidentialité.
5. Désactivez VRRP.
6. Supprimez toutes les règles IKE qui ont soit MD5 pour l'authentification, soit DES pour le cryptage. Modifiez les règles de sorte qu'elles utilisent SHA pour l'authentification et 3DES/AES pour le cryptage.
7. Supprimez tous les types de clés RSA1 du serveur SSH.

Pour activer le mode FIPS et afficher l'état FIPS sur le commutateur MDS, procédez comme suit :

1. Affiche le statut FIPS.

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

2. Configurez la clé SSH 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. Activez le mode 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. Affiche le statut FIPS.

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

5. Enregistrez la configuration dans la configuration en cours d’exécution.

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

6. Redémarrez le commutateur MDS

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

7. Affiche le statut FIPS.

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

Pour plus d'informations, voir "Activation du mode FIPS".

Commutateurs Cisco Nexus

Les commutateurs de la gamme Cisco Nexus 9000 (version 9.3) sont "Conforme à la norme FIPS 140-2". Cisco Nexus implémente des modules cryptographiques et les services suivants pour SNMPv3 et SSH.

- Établissement de session prenant en charge chaque service
- Tous les algorithmes cryptographiques sous-jacents prenant en charge les fonctions de dérivation des clés de service
- Hachage pour chaque service
- Chiffrement symétrique pour chaque service

Avant d'activer le mode FIPS, effectuez les tâches suivantes sur le commutateur Cisco Nexus :

1. Désactivez Telnet. Les utilisateurs doivent se connecter à l'aide de Secure Shell (SSH) uniquement.
2. Désactivez SNMPv1 et v2. Tout compte utilisateur existant sur le périphérique qui a été configuré pour SNMPv3 doit être configuré uniquement avec SHA pour l'authentification et AES/3DES pour la confidentialité.
3. Supprimez toutes les paires de clés RSA1 du serveur SSH.
4. Activez le contrôle d'intégrité des messages (MIC) HMAC-SHA1 à utiliser lors de la négociation du protocole SAP (Security Association Protocol) de Cisco TrustSec. Pour ce faire, entrez l'algorithme de hachage sap `HMAC-SHA-1` de la commande `cts-manual` ou `cts-dot1x` mode.

Pour activer le mode FIPS sur le commutateur Nexus, effectuez les opérations suivantes :

1. Configurez la clé SSH 2048 bits.

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

2. Configurez la clé SSH 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. Activez le mode 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. Redémarrez le commutateur Nexus.

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

5. Affiche le statut FIPS.

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

De plus, le logiciel Cisco NX OS prend en charge la fonctionnalité NetFlow qui permet une détection améliorée des anomalies et de la sécurité du réseau. NetFlow capture les métadonnées de chaque conversation sur le réseau, les parties impliquées dans la communication, le protocole utilisé et la durée de la transaction. Une fois les informations agrégées et analysées, elles permettent de mieux comprendre le comportement normal. Les données collectées permettent également d'identifier des modèles d'activité douteux, tels que les programmes malveillants, qui s'étendent sur le réseau, qui peuvent autrement passer inaperçues. NetFlow utilise des flux pour fournir des statistiques sur la surveillance du réseau. Un flux est un flux unidirectionnel de paquets arrivant sur une interface source (ou VLAN) et possède les mêmes valeurs pour les clés. Une clé est une valeur identifiée pour un champ dans le paquet. Vous créez un flux à l'aide d'un enregistrement de flux pour définir les clés uniques de votre flux. Vous pouvez exporter les données collectées par NetFlow pour vos flux à l'aide d'un exportateur de flux vers un collecteur NetFlow distant, tel que Cisco StealthWatch. StealthWatch exploite ces informations pour assurer une surveillance continue du réseau et fournit une détection en temps réel des menaces et une analyse des réponses aux incidents en cas d'attaque par ransomware.

"FlexPod : stockage NetApp ONTAP et FIPS 140-2."

Stockage FlexPod ONTAP et FIPS 140-2

"Précédent : réseau FlexPod Cisco et FIPS 140-2."

NetApp propose toute une gamme de matériel, de logiciels et de services, qui peuvent inclure divers composants des modules cryptographiques validés selon la norme. NetApp a donc recours à diverses approches de conformité à la norme FIPS 140-2 pour le plan de contrôle et le plan de données :

- NetApp inclut des modules cryptographiques qui ont obtenu une validation de niveau 1 pour les données en transit et le chiffrement des données au repos.
- NetApp acquiert à la fois des modules matériels et logiciels ayant été validés par la norme FIPS 140-2 par les fournisseurs de ces composants. Par exemple, la solution NetApp Storage Encryption exploite des disques validés conformes à la norme FIPS de niveau 2.
- Les produits NetApp peuvent utiliser un module validé conformément à la norme, même si le produit ou la fonctionnalité ne se trouve pas aux limites de la validation. Par exemple, NetApp Volume Encryption (NVE) est conforme à la norme FIPS 140-2-2. Bien qu'il ne soit pas validé séparément, il exploite le module cryptographique de NetApp, qui est validé au niveau 1. Pour comprendre les spécificités de la conformité de votre version de ONTAP, contactez votre expert technique FlexPod.

Les modules cryptographiques NetApp sont certifiés conformes à la norme FIPS 140-2 de niveau 1

- NetApp Cryptographic Security module (NCSM) est certifié conforme à la norme FIPS 140-2 de niveau 1.

Les disques à autochiffrement de NetApp sont validés par la norme FIPS 140-2 de niveau 2

NetApp achète des disques à autocryptage (SED) qui ont été validés par la norme FIPS 140-2 par le fabricant d'équipement d'origine ; les clients qui les recherchent doivent les spécifier lors de la commande. Les disques sont validés au niveau 2. Les produits NetApp suivants peuvent utiliser les disques SED validés :

- AFF A-Series et les systèmes de stockage FAS
- Systèmes de stockage E-Series et EF-Series

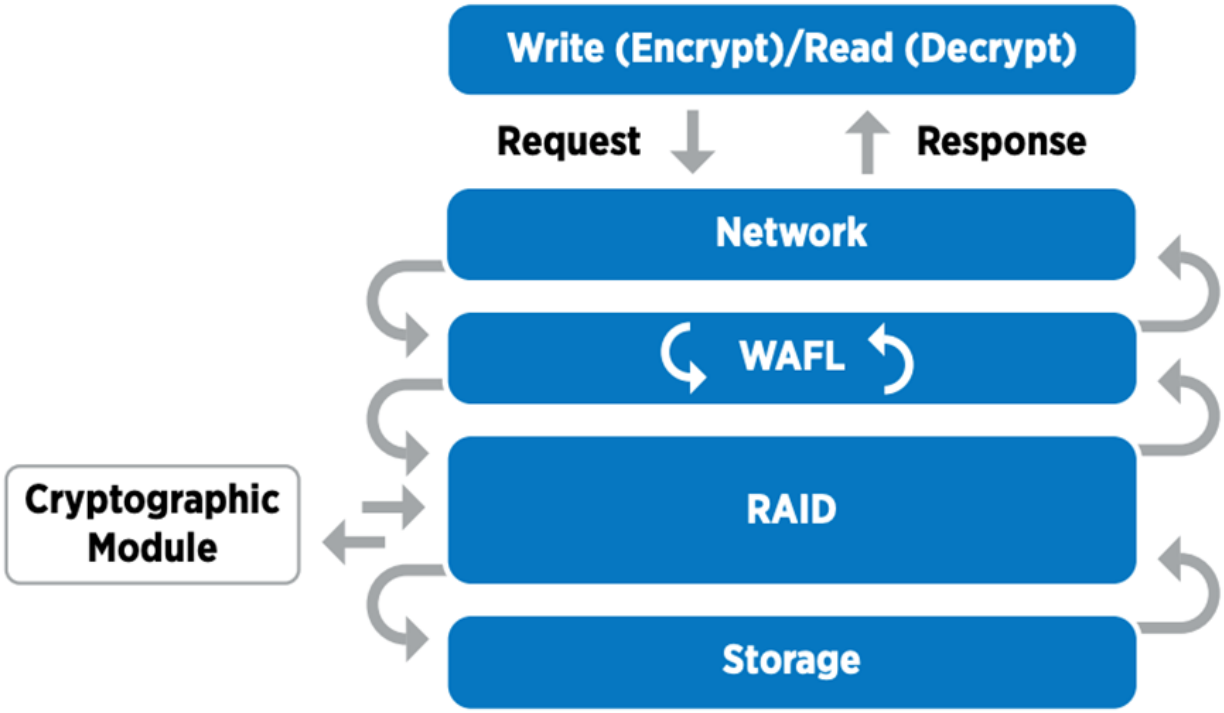
NetApp Aggregate Encryption et NetApp Volume Encryption

Les technologies NVE et NetApp Aggregate Encryption (NAE) permettent de chiffrer les données au niveau des volumes et des agrégats, de manière à ce qu'elles soient indépendantes du disque physique.

Mécanisme de chiffrement logiciel des données au repos, disponible à partir de ONTAP 9.1, conforme à la norme FIPS 140-2-2 depuis ONTAP 9.2. NVE permet à ONTAP de chiffrer les données pour chaque volume pour la granularité. NAE, disponible avec ONTAP 9.6, est une solution de plus en plus croissante de NVE. Il permet au ONTAP de chiffrer les données pour chaque volume et aux volumes de partager les clés dans l'ensemble de l'agrégat. NVE et NAE utilisent tous deux le chiffrement AES 256 bits. Les données peuvent également être stockées sur disque sans disques SED. Avec NVE et NAE, vous pouvez utiliser des fonctionnalités d'efficacité du stockage même lorsque le chiffrement est activé. Un chiffrement au niveau des applications uniquement résout tous les avantages de l'efficacité du stockage. Avec NVE et NAE, les fonctionnalités d'efficacité du stockage sont maintenues, car les données proviennent du réseau via NetApp WAFL et de la couche RAID qui détermine si les données doivent être chiffrées. Pour une meilleure efficacité du stockage, il est possible d'utiliser la déduplication globale avec NAE. Les volumes NVE et NAE peuvent coexister sur un même agrégat NAE. Les agrégats NAE ne prennent pas en charge les volumes non chiffrés.

Voici comment fonctionne le processus : lorsque les données sont cryptées, elles sont envoyées au module cryptographique validé FIPS 140-2 de niveau 1. Le module cryptographique crypte les données et les renvoie

à la couche RAID. Les données cryptées sont alors envoyées au disque. Par conséquent, avec la combinaison de NVE et de NAE, les données sont déjà chiffrées sur le disque. Les lectures suivent la trajectoire inverse. En d'autres termes, les données quittent le disque chiffré, sont envoyées au RAID, elles sont déchiffrées par le module cryptographique et sont ensuite envoyées le reste de la pile, comme illustré dans la figure suivante.



NVE utilise un module cryptographique logiciel conforme à la norme FIPS 140-2 de niveau 1.

Pour plus d'informations sur NVE, consultez le "Fiche technique NVE".

NVE protège les données dans le cloud. Cloud Volumes ONTAP et Azure NetApp Files peuvent assurer le chiffrement des données au repos conforme à la norme FIPS 140-2-2.

Depuis ONTAP 9.7, les volumes et les agrégats nouvellement créés sont chiffrés par défaut lorsque vous disposez d'une licence NVE et d'une gestion des clés intégrée ou externe. Depuis ONTAP 9.6, vous pouvez utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de chiffrer les volumes. Les volumes que vous créez dans l'agrégat sont chiffrés par défaut. Vous pouvez remplacer la valeur par défaut lorsque vous chiffrez le volume.

COMMANDES CLI ONTAP NAE

Avant d'exécuter les commandes CLI suivantes, vérifiez que le cluster possède la licence NVE requise.

Pour créer un agrégat et le chiffrer, exécutez la commande suivante (lorsqu'elle s'exécute sur ONTAP 9.6 et version ultérieure de l'interface de ligne de commandes du cluster) :

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

Pour convertir un agrégat non-NAE en agrégat, exécutez la commande suivante (lorsqu'il s'exécute sur un ONTAP 9.6 et une interface de ligne de commande de cluster ultérieure) :

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

Pour convertir un agrégat NAE en agrégat non-NAE, exécutez la commande suivante (lorsqu'il s'exécute sur un ONTAP 9.6 et l'interface de ligne de commande du cluster par la suite) :

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

COMMANDES CLI ONTAP NVE

Depuis ONTAP 9.6, vous pouvez utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de chiffrer les volumes. Les volumes que vous créez dans l'agrégat sont chiffrés par défaut.

Pour créer un volume sur un agrégat NAE activé, exécutez la commande suivante (lorsqu'elle s'exécute sur ONTAP 9.6 et versions ultérieures de l'interface de ligne de commande du cluster) :

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

Pour activer le chiffrement d'un volume existant « inplace » sans déplacement du volume, exécutez la commande suivante (lorsqu'elle est exécutée sur un ONTAP 9.6 et version ultérieure de l'interface de ligne de commande du cluster) :

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

Pour vérifier que les volumes sont activés pour le chiffrement, exécutez la commande CLI suivante :

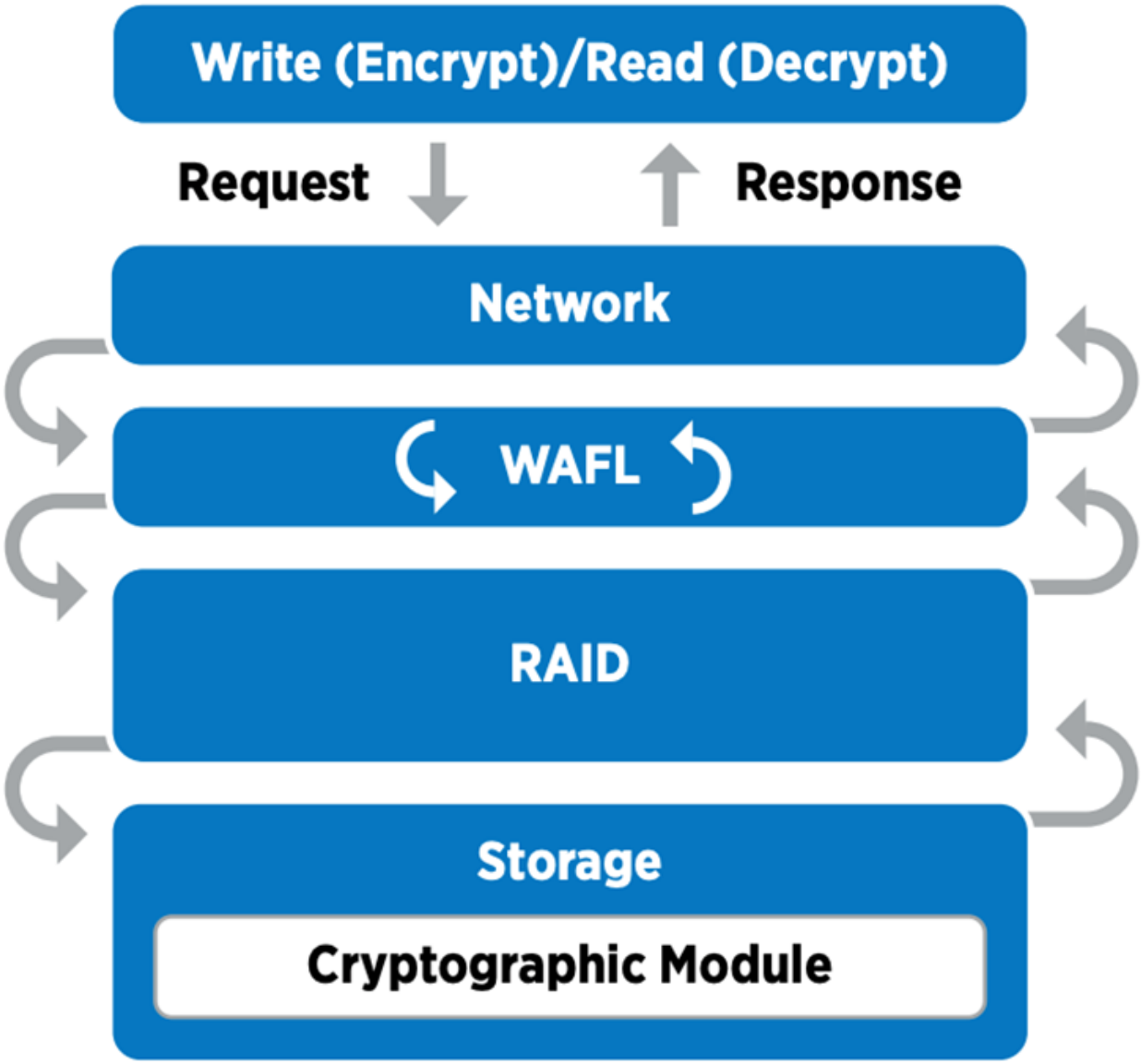
```
fp-health::> volume show -is-encrypted true
```

NSE

NSE utilise les disques SED pour effectuer le chiffrement des données à l'aide d'un mécanisme à accélération matérielle.

NSE est configuré pour utiliser des disques à autochiffrement FIPS 140-2 de niveau 2 pour faciliter la conformité et les retours de disques de secours, en assurant la protection des données au repos via le chiffrement de disque transparent AES 256 bits. Ces disques effectuent toutes les opérations de chiffrement des données en interne, comme illustré dans la figure ci-dessous, notamment la génération de clés de chiffrement. Pour empêcher tout accès non autorisé aux données, le système de stockage doit s'authentifier

auprès du disque à l'aide d'une clé d'authentification établie lors de la première utilisation du disque.



NSE utilise un chiffrement matériel sur chaque disque certifié conforme à la norme FIPS 140-2 de niveau 2.

Pour plus d'informations sur NSE, reportez-vous au "Fiche technique NSE".

Gestion des clés

La norme FIPS 140-2 s'applique au module cryptographique, tel que défini par la limite, comme illustré dans la figure suivante.

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.

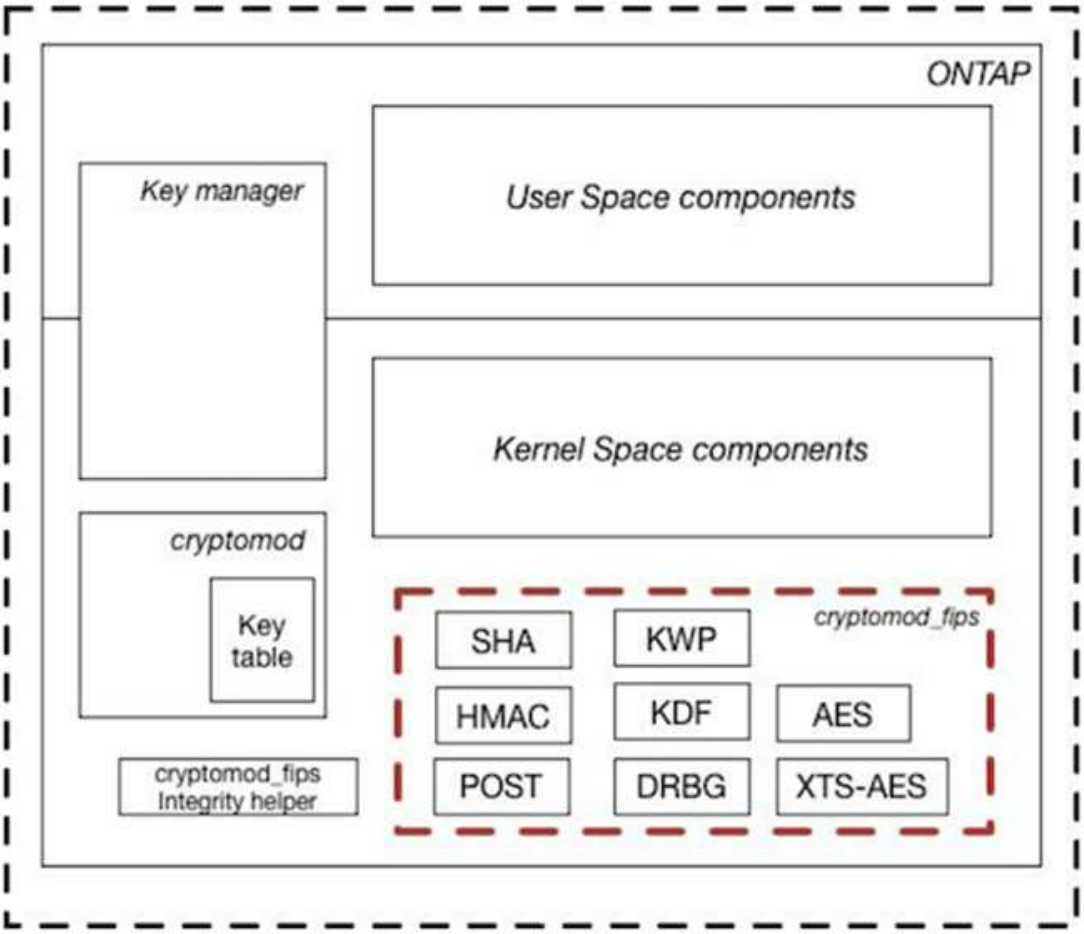


Figure 1 - Block Diagram

Le gestionnaire de clés assure le suivi de toutes les clés de cryptage utilisées par ONTAP. Les disques SED NSE utilisent le gestionnaire de clés pour définir les clés d'authentification pour les disques SED NSE. Avec le gestionnaire de clés, la solution combinée NVE et NAE est composée d'un module cryptographique logiciel, de clés de chiffrement et d'un gestionnaire de clés. Pour chaque volume, NVE utilise une clé de chiffrement des données XTS-AES 256 unique, qui stocke le gestionnaire de clés. La clé utilisée pour un volume de données est unique pour le volume de données du cluster et est générée lors de la création du volume chiffré. De même, un volume NAE utilise des clés de chiffrement des données XTS-AES 256 uniques par agrégat, ce que le gestionnaire de clés stocke également. Les clés NAE sont générées lors de la création de l'agrégat chiffré. ONTAP ne prégénère pas de clés, ne les réutilisez pas ou ne les affiche pas en texte clair : elles sont stockées et protégées par le gestionnaire de clés.

Prise en charge d'un gestionnaire de clés externe

Depuis la version ONTAP 9.3, les gestionnaires de clés externes sont pris en charge dans les solutions NVE et NSE. La norme FIPS 140-2 s'applique au module cryptographique utilisé dans la mise en œuvre du fournisseur spécifique. Le plus souvent, les clients FlexPod et ONTAP utilisent l'une des solutions suivantes validées (selon le "Matrice d'interopérabilité NetApp") gestionnaires clés :

- Gemalto ou SafeNet À L'ADRESSE
- Vormetric (Thales)
- IBM SKLM
- Utimaco (anciennement Microfocus, HPE)

La clé d'authentification NSE et NVMe SED est sauvegardée dans un gestionnaire de clés externe à l'aide du protocole KMIP (OASIS Key Management Interoperability Protocol), une norme du secteur. Seuls le système de stockage, le disque et le gestionnaire de clés ont accès à la clé et le disque ne peut pas être déverrouillé s'il est déplacé en dehors du domaine de sécurité, empêchant ainsi les fuites de données. Le gestionnaire de clés externe stocke également des clés de chiffrement de volume NVE et des clés de chiffrement d'agrégat NAE. Si le contrôleur et les disques sont déplacés et qu'ils n'ont plus accès au gestionnaire de clés externe, les volumes NVE et NAE ne sont plus accessibles et ne peuvent pas être déchiffrés.

L'exemple de commande suivant ajoute deux serveurs de gestion des clés à la liste des serveurs utilisés par le gestionnaire de clés externe pour stocker une machine virtuelle (SVM) `svmname1`.

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

Dans le FlexPod cas d'une colocation, ONTAP permet aux utilisateurs d'utiliser la colocation pour des raisons de sécurité au niveau de la SVM.

Pour vérifier la liste des gestionnaires de clés externes, exécutez la commande CLI suivante :

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

Combinaison du cryptage pour le double cryptage (protection en couches)

Si vous devez isoler l'accès aux données et veiller à ce qu'elles soient protégées en permanence, les disques SED NSE peuvent être combinés avec un cryptage au niveau du réseau ou de la structure. Les disques SED NSE agissent comme un backstop si un administrateur oublie de configurer ou de configurer un cryptage de niveau supérieur. Pour deux couches de chiffrement distinctes, vous pouvez combiner les disques SED NSE avec NVE et NAE.

Plan de contrôle NetApp ONTAP en mode FIPS au niveau du cluster

Le logiciel de gestion de données NetApp ONTAP est doté d'une configuration FIPS-mode qui instancie un niveau de sécurité supplémentaire pour le client. Ce mode FIPS s'applique uniquement au plan de contrôle. Lorsque le mode FIPS est activé, conformément aux éléments clés de FIPS 140-2, transport Layer Security v1 (TLSv1) et SSLv3 sont désactivés et seuls TLS v1.1 et TLS v1.2 restent activés.

> Le panneau de contrôle ONTAP en mode FIPS est conforme à la norme FIPS 140-2 de niveau 1. Le mode FIPS sur l'ensemble du cluster utilise un module cryptographique logiciel fourni par NCSM.

Le mode de conformité FIPS 140-2 pour le plan de contrôle à l'échelle du cluster sécurise toutes les interfaces de contrôle de ONTAP. Par défaut, le mode FIPS 140-2 uniquement est désactivé. Cependant, vous pouvez activer ce mode en configurant le `is- fips-enabled` paramètre à `true` pour le `security config modify` commande.

Pour activer le mode FIPS sur le cluster ONTAP, exécutez la commande suivante :

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

Lorsque le mode SSL FIPS est activé, la communication SSL de ONTAP vers les composants client ou serveur externes en dehors de ONTAP utilise le chiffrement des plaintes FIPS pour SSL.

Pour afficher le statut FIPS pour l'ensemble du cluster, exécutez les commandes suivantes :

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

"Ensuite, les avantages de l'infrastructure convergée FlexPod."

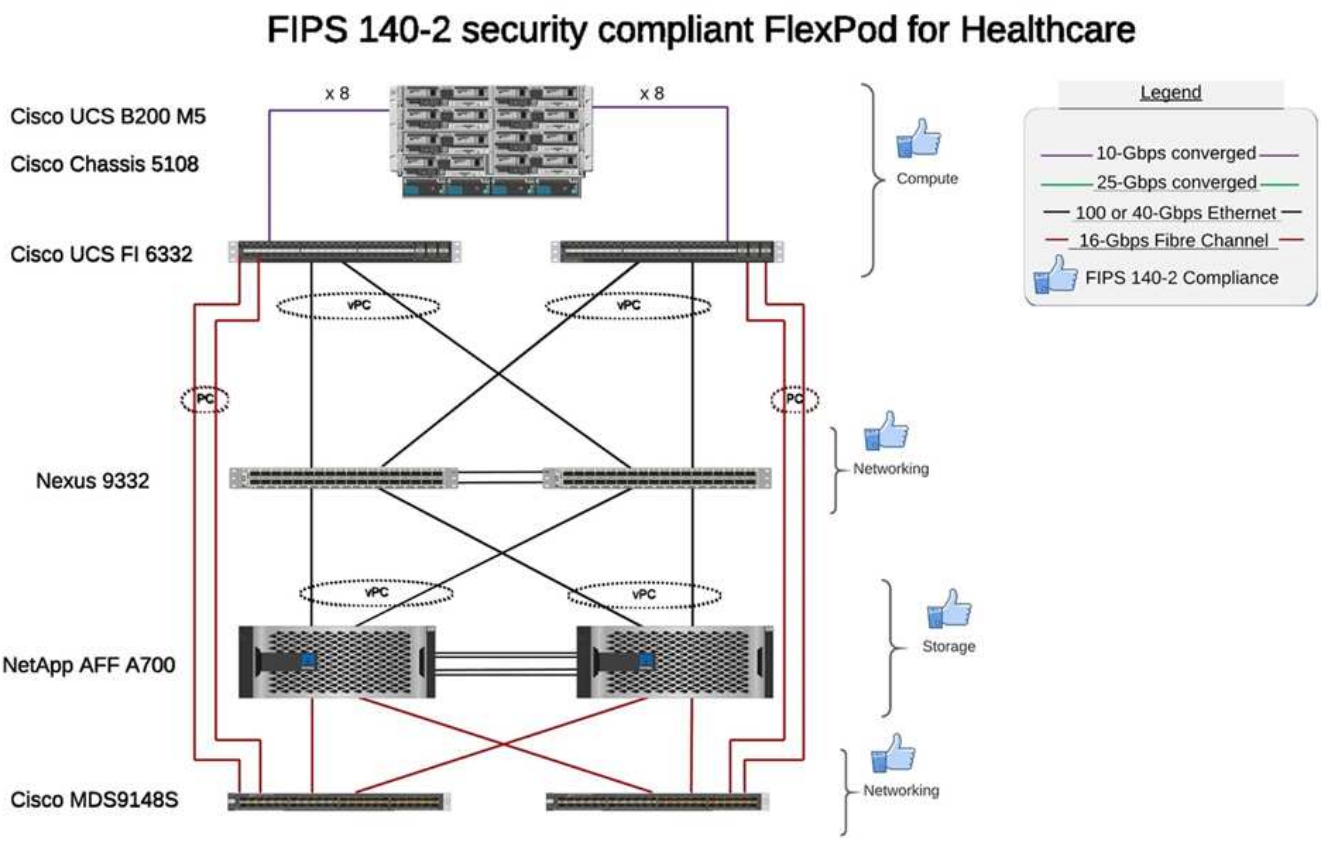
Avantages de la solution de l'infrastructure convergée FlexPod

"Précédent : stockage NetApp ONTAP de FlexPod et FIPS 140-2."

Les organismes de santé disposent de plusieurs systèmes stratégiques. Deux des systèmes les plus critiques sont les systèmes de dossiers médicaux électroniques (DME) et les systèmes d'imagerie médicale. Pour démontrer la configuration FIPS sur un système FlexPod, nous avons utilisé un système de DME open source et un système de communication et d'archivage des images open source pour la configuration en laboratoire et la validation des charges de travail sur le système FlexPod. Pour obtenir la liste complète des fonctionnalités EHR, des composants d'application logique EHR et les avantages des systèmes EHR lorsqu'ils sont implémentés sur un système FlexPod, consultez la section "Tr-4881 : FlexPod pour les systèmes de dossiers de santé électroniques". Pour obtenir la liste complète des fonctionnalités d'un système d'imagerie médicale, des composants d'application logique et des avantages des systèmes d'imagerie médicale lorsqu'ils sont implémentés sur FlexPod, consultez la section "Tr-4865 : FlexPod pour l'imagerie médicale".

Lors de la configuration de FIPS et de la validation des charges de travail, nous avons exercé les caractéristiques de workloads représentatives d'un organisme de santé typique. Par exemple, nous avons exercé un système open source EHR afin d'inclure des scénarios réalistes d'accès aux données des patients et de changement. Par ailleurs, nous avons exercé les charges de travail d'imagerie médicale incluant l'imagerie numérique et les communications dans des objets médicaux (DICOM) dans un `*. dcm` format de fichier. Les objets DICOM avec métadonnées étaient stockés dans le stockage de fichiers et en blocs. De plus, nous avons mis en œuvre des fonctionnalités de chemins d'accès multiples à partir d'un serveur virtualisé RedHat Enterprise Linux (RHEL). Nous stockons des objets DICOM sur un système NFS, des LUN montées à l'aide d'iSCSI et des LUN montées à l'aide de FC. Lors de la configuration et de la validation FIPS, nous avons observé que l'infrastructure convergée FlexPod dépassait nos attentes.

La figure suivante décrit le système FlexPod utilisé pour la configuration et la validation de FIPS. Nous avons utilisé "FlexPod Datacenter avec VMware vSphere 7.0 et NetApp ONTAP 9.7 conception validée par Cisco (CVD)" pendant le processus de configuration.



Composants matériels et logiciels de l’infrastructure de la solution

Les deux figures suivantes illustrent respectivement les composants matériels et logiciels utilisés lors du test FIPS lors de l’activation sur un FlexPod. Les recommandations présentées dans ces tableaux sont des exemples. Vous devez collaborer avec votre expert technique NetApp pour vous assurer que les composants sont adaptés à votre entreprise. Assurez-vous également que les composants et versions sont pris en charge dans le "Matrice d’interopérabilité NetApp" (IMT) et "Liste de compatibilité matérielle Cisco (HCL)".

Calque	Famille de produits	Quantité et modèle	Détails
Calcul	Châssis Cisco UCS 5108	1 ou 2	
	Les serveurs lames Cisco UCS	3 B200 M5	Chacun doté de 2 20 cœurs ou plus, de 2,7 GHz et de 128 Go de RAM
	Carte d’interface virtuelle Cisco UCS (VIC)	Cisco UCS 1440	Voir la
	2 interconnexions de fabric Cisco UCS	6332	-
Le réseau	Commutateurs Cisco Nexus	2 x Cisco Nexus 9332	-

Calque	Famille de produits	Quantité et modèle	Détails
Réseau de stockage	Réseau IP pour l'accès au stockage via les protocoles SMB/CIFS, NFS ou iSCSI	Mêmes commutateurs réseau que ci-dessus	-
	Accès au stockage via FC	2 x Cisco MDS 9148S	-
Stockage	Système de stockage 100 % Flash NetApp AFF A700	1 Cluster	Cluster à deux nœuds
	Tiroir disque	Un tiroir disque DS224C ou NS224	Plein avec 24 disques
	SSD	Pour 24, 1,2 To ou plus	-

Logiciel	Famille de produits	Version ou version	Détails
Divers	Linux	RHEL 7.X.	-
	Répertoires de base	Windows Server 2012 R2 (64 bits)	-
	NetApp ONTAP	ONTAP 9.7 ou version ultérieure	-
	Fabric Interconnect Cisco UCS	Cisco UCS Manager 4.1 ou version ultérieure	-
	Switchs Cisco Ethernet 3000 ou 9000	Pour la série 9000, 7.0(3)I7(7) ou ultérieure pour la série 3000, 9.2(4) ou ultérieure	-
	Cisco FC : Cisco MDS 9132T	8.4(1a) ou ultérieure	-
	Hyperviseur	VMware vSphere ESXi 6.7 U2 ou version ultérieure	-
Stockage	Système de gestion de l'hyperviseur	VMware vCenter Server 6.7 U3 (vCSA) ou version ultérieure	-
Le réseau	NetApp Virtual Storage Console (VSC)	VSC 9.7 ou version ultérieure	-
	NetApp SnapCenter	SnapCenter 4.3 ou version ultérieure	-
	Cisco UCS Manager	4.1(1c) ou ultérieure	
Hyperviseur	VMware ESXi		

Logiciel	Famille de produits	Version ou version	Détails
Gestion	Système de gestion de l'hyperviseur VMware vCenter Server 6.7 U3 (vCSA) ou version ultérieure		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 ou version ultérieure	
	NetApp SnapCenter	SnapCenter 4.3 ou version ultérieure	
	Cisco UCS Manager	4.1(1c) ou ultérieure	

"Ensuite, d'autres considérations relatives à la sécurité FlexPod."

Autres considérations relatives à la sécurité FlexPod

"Précédent : avantages de la solution pour l'infrastructure convergée FlexPod."

L'infrastructure FlexPod est une plateforme modulaire, convergée, évolutive (scale-out et scale-up) et économique. Avec la plateforme FlexPod, vous pouvez faire évoluer indépendamment les ressources de calcul, de réseau et de stockage pour accélérer le déploiement de vos applications. En outre, l'architecture modulaire garantit la continuité de l'activité, même lors des activités de mise à niveau et d'évolutivité horizontale de votre système.

Les différents composants d'un système HIT nécessitent que les données soient stockées dans des systèmes de fichiers SMB/CIFS, NFS, Ext4 et NTFS. Par conséquent, l'infrastructure doit fournir un accès aux données via les protocoles NFS, CIFS et SAN. Un système de stockage NetApp unique peut prendre en charge tous ces protocoles, ce qui évite la pratique existante de systèmes de stockage spécifiques au protocole. Un système de stockage NetApp unique peut également prendre en charge plusieurs charges DE travail HIT (DME, PACS ou VNA), génomique, VDI, etc. avec des niveaux de performance garantis et configurables.

Lorsqu'elle est déployée dans un système FlexPod, HIT offre plusieurs avantages spécifiques au secteur de la santé. La liste suivante fournit une description générale de ces avantages :

- **Sécurité FlexPod**. La sécurité est à la base même d'un système FlexPod. Ces dernières années, les attaques par ransomware sont devenues une menace. Les ransomwares sont un type de malware basé sur la cryptovirologie, l'utilisation de la cryptographie pour créer des logiciels malveillants. Ce programme malveillant peut utiliser à la fois un cryptage symétrique et asymétrique pour verrouiller les données d'une victime et exiger une rançon afin de fournir la clé de chiffrement des données. Pour découvrir comment la solution FlexPod permet de réduire les menaces telles que les ransomware, rendez "Tr-4802 : la solution aux attaques par ransomware"-vous sur . Les composants de l'infrastructure FlexPod sont également "Conforme à la norme FIPS 140-2".
- **Cisco Intersight** Cisco Intersight est une plateforme de gestion à la demande basée sur le cloud et innovante, qui offre une fenêtre unique pour la gestion et l'orchestration FlexPod de la pile complète. La plateforme Intersight utilise des modules cryptographiques conformes à la norme FIPS 140-2. L'architecture de gestion hors bande de la plate-forme la rend hors de portée pour certaines normes ou certains audits comme HIPAA. Aucune information d'intégrité identifiable sur le réseau n'est envoyée au portail Intersight.

- **Technologie NetApp FPolicy.** NetApp FPolicy (une évolution de l'politique de fichiers de noms) est un framework de notification d'accès aux fichiers permettant de surveiller et de gérer l'accès aux fichiers via les protocoles NFS ou SMB/CIFS. Depuis plus de dix ans, cette technologie fait partie du logiciel de gestion des données ONTAP. Elle aide à détecter les attaques par ransomware. Ce moteur Zero Trust fournit des mesures de sécurité supplémentaires au-delà des autorisations dans les listes de contrôle d'accès (ACL). FPolicy possède deux modes de fonctionnement : natif et externe :
  - Le mode natif fournit à la fois la liste noire et la liste blanche des extensions de fichiers.
  - Le mode externe offre les mêmes fonctionnalités que le mode natif, mais il s'intègre également à un serveur FPolicy qui s'exécute en externe au système ONTAP ainsi qu'à un système de gestion des informations de sécurité et des événements (SIEM). Pour plus d'informations sur la lutte contre les ransomwares, consultez le "Lutte contre les attaques par ransomware : troisième partie : ONTAP FPolicy, un autre outil natif puissant (ou gratuit)" blog.
- **Données au repos**. Avec ONTAP 9 et les versions ultérieures, les données au repos sont chiffrées conformes à la norme FIPS 140-2 :
  - NSE est une solution matérielle qui utilise des disques à chiffrement automatique.
  - NVE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque où il est activé avec une clé unique pour chaque volume.
  - NAE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque grâce à des clés uniques pour chaque agrégat.

> Depuis ONTAP 9.7, NAE et NVE sont activés par défaut si le package de licence NetApp NVE dont le nom est VE est en place.

- **Données en vol**. Depuis ONTAP 9.8, la sécurité IPSec (Internet Protocol Security) fournit une prise en charge de cryptage de bout en bout pour tout le trafic IP entre un client et un SVM ONTAP. Le cryptage de données IPSec pour tout le trafic IP inclut les protocoles NFS, iSCSI et SMB/CIFS. IPSec fournit la seule option de cryptage en vol pour le trafic iSCSI.
- **Chiffrement des données de bout en bout dans une Data Fabric hybride et multicloud**. Les clients qui utilisent des technologies de chiffrement des données au repos comme NSE ou NVE et Cluster peering Encryption (CPE) pour le trafic de réplication des données peuvent désormais utiliser le chiffrement de bout en bout entre les clients et le stockage dans leur structure de données multicloud hybride en effectuant une mise à niveau vers ONTAP 9.8 ou version ultérieure et en utilisant IPSec. À partir de ONTAP 9, vous pouvez activer le mode de conformité FIPS 140-2 pour les interfaces du plan de contrôle au niveau du cluster. Par défaut, le mode FIPS 140-2 uniquement est désactivé. À partir de ONTAP 9.6, CPE assure la prise en charge du cryptage TLS 1.2 AES-256 GCM pour les fonctionnalités de réplication des données ONTAP telles que les technologies NetApp SnapMirror, NetApp SnapVault et NetApp FlexCache. Le chiffrement est configuré au moyen d'une clé pré-partagée (PSK) entre deux pairs de cluster.
- **Colocation sécurisée**. Prend en charge les besoins accrus de l'infrastructure partagée de serveurs et de stockage virtualisés, ce qui permet une colocation sécurisée des informations spécifiques aux sites, notamment si vous hébergez plusieurs instances de bases de données et de logiciels.

"Suivant: Conclusion."

Conclusion

"Précédent : autres considérations de sécurité FlexPod."

En exécutant votre application médicale sur une plateforme FlexPod, votre organisme de santé est mieux protégé par une plateforme compatible FIPS 140-2. FlexPod propose

une protection à plusieurs couches pour chaque composant : calcul, réseau et stockage. Les fonctionnalités de protection des données de FlexPod protègent les données au repos ou à la volée. Les sauvegardes restent sécurisées et prêtes à l'emploi, selon les besoins.

Évitez les erreurs humaines en tirant parti des designs prévalidés de FlexPod soumis à des tests rigoureux d'infrastructures convergées issues du partenariat stratégique de Cisco et de NetApp. Un système FlexPod conçu et conçu pour fournir des performances prévisibles avec une faible latence des systèmes et une haute disponibilité avec un impact minimal, même lorsque la norme FIPS 140-2 est activée dans les couches de calcul, de réseau et de stockage. Cette approche permet d'améliorer l'expérience utilisateur et de bénéficier d'un temps de réponse optimal pour les utilisateurs de votre système HIT.

"Suivant : Remerciements, historique des versions, et où trouver des informations supplémentaires."

Remerciements, historique des versions et où trouver des informations supplémentaires

"Précédent: Conclusion."

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et sites web :

- Guide de configuration de la sécurité de la gamme 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

- Guide de configuration de la sécurité Cisco Nexus série 9000 NX-OS, version 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

- Publication NetApp and Federal information Processing Standard (FIPS) 140-2

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

- FIPS 140-2

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

- Guide NetApp ONTAP 9 sur le renforcement du partenariat

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

- Guide d'alimentation du cryptage NetApp

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

- Fiche produit NVE et NAE

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

- Fiche technique NSE

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

- Centre de documentation ONTAP 9

  http://docs.netapp.com

- Publication NetApp and Federal information Processing Standard (FIPS) 140-2

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

- Conformité Cisco et FIPS 140-2

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

- Module de chiffrement NetApp

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

- Cybersécurité pour les moyennes et grandes organisations dans le domaine de la santé

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

- Programme de validation Cisco et module cryptographique (CMVP)

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

- NetApp Storage Encryption, disques avec autocryptage NVMe, NetApp Volume Encryption et NetApp Aggregate Encryption

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

- NetApp Volume Encryption et chiffrement d'agrégat NetApp

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

- NetApp Storage Encryption

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

- FlexPod pour les systèmes de dossiers médicaux électroniques

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

- Disponibilité immédiate des données : améliorer les performances dans les environnements de DME EPIC grâce à la technologie Flash connectée au cloud

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

- FlexPod Datacenter pour infrastructure EHR Epic

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

- Guide de déploiement de FlexPod Datacenter pour Epic EHR

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

- Infrastructure de data Center FlexPod pour le logiciel MEDITECH

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

- La norme FlexPod s'étend au logiciel MEDITECH

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

- FlexPod pour MEDITECH : Guide de dimensionnement

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

- FlexPod pour l'imagerie médicale

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

- L'IA dans le domaine de la santé

  https://www.netapp.com/pdf.html?item=/media/7393-na-369pdf.pdf

- FlexPod pour le secteur de la santé facilite votre transformation

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

- FlexPod de Cisco et NetApp

  https://flexpod.com/

Remerciements

- Abhinav Singh, Ingénieur marketing et technique, NetApp
- Brian O'Mehony, architecte de solutions au sein du secteur de la santé (Epic), NetApp
- Brian Pruitt, responsable du développement commercial chez NetApp
- Arvind Ramakrishnan, architecte de solutions senior, NetApp
- Michael Hommer, Directeur technique mondial chez FlexPod, NetApp

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Avril 2021	Version initiale