FlexPod, la solution aux attaques par ransomware

FlexPod

NetApp
January 21, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/flexpod/security/security-ransomware_what_is_ransomware.html on January 21, 2025. Always check docs.netapp.com for the latest.

Sommaire

FlexPod, la solution aux attaques par ransomware . . . 1
Tr-4802 : FlexPod, la solution vers le ransomware . . . 1
Présentation de FlexPod . . . 4
Mesures de protection par ransomware . . . 5
Protégez et restaurez les données sur FlexPod . . . 7
Continuez vos activités sans payer de rançon . . . 20
Conclusion . . . 20
Remerciements . . . 21
Informations supplémentaires . . . 21

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.

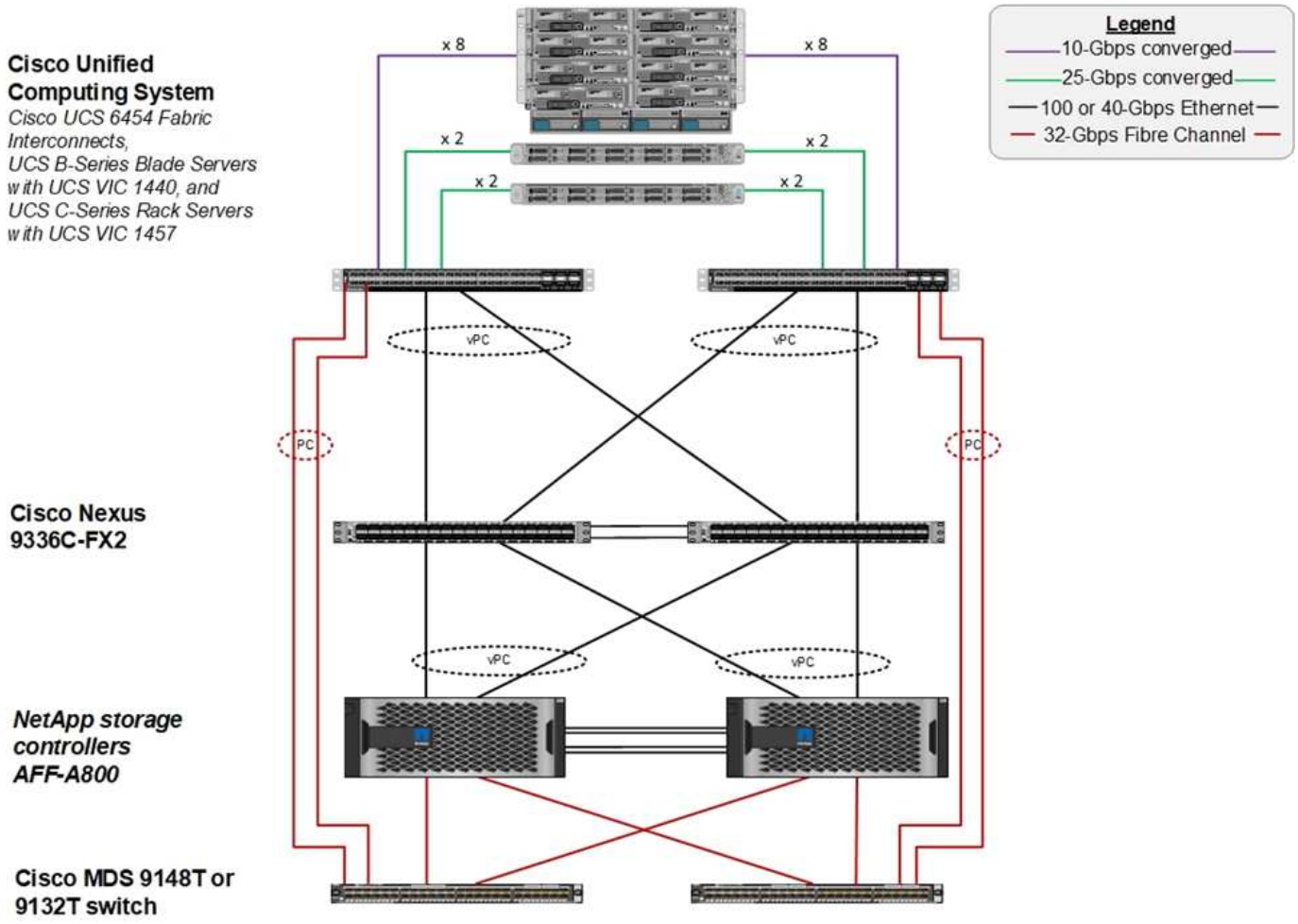
Bien que vous deviez examiner plusieurs fronts et corriger pour prévenir une attaque, le centre de données est le composant principal qui vous permet d'éviter ou de récupérer après une attaque.

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

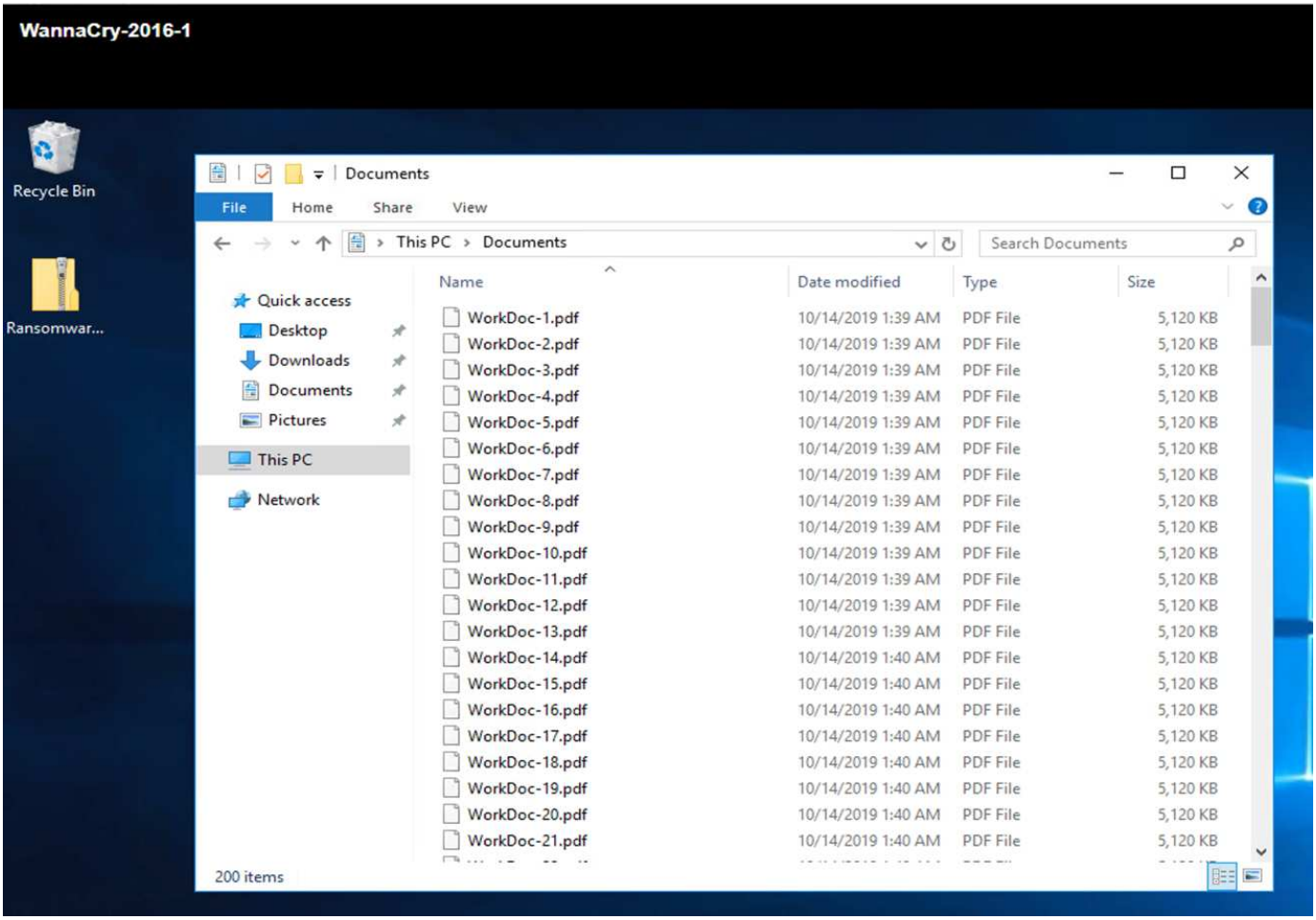
Pour mettre en avant la détection, la résolution et la prévention des problèmes liés à FlexPod, un banc d'essai a été créé à partir des directives spécifiées dans les guides CVD de la dernière plateforme disponibles au moment de l'élaboration de ce document : "CVD FlexPod Datacenter avec VMware vSphere 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.

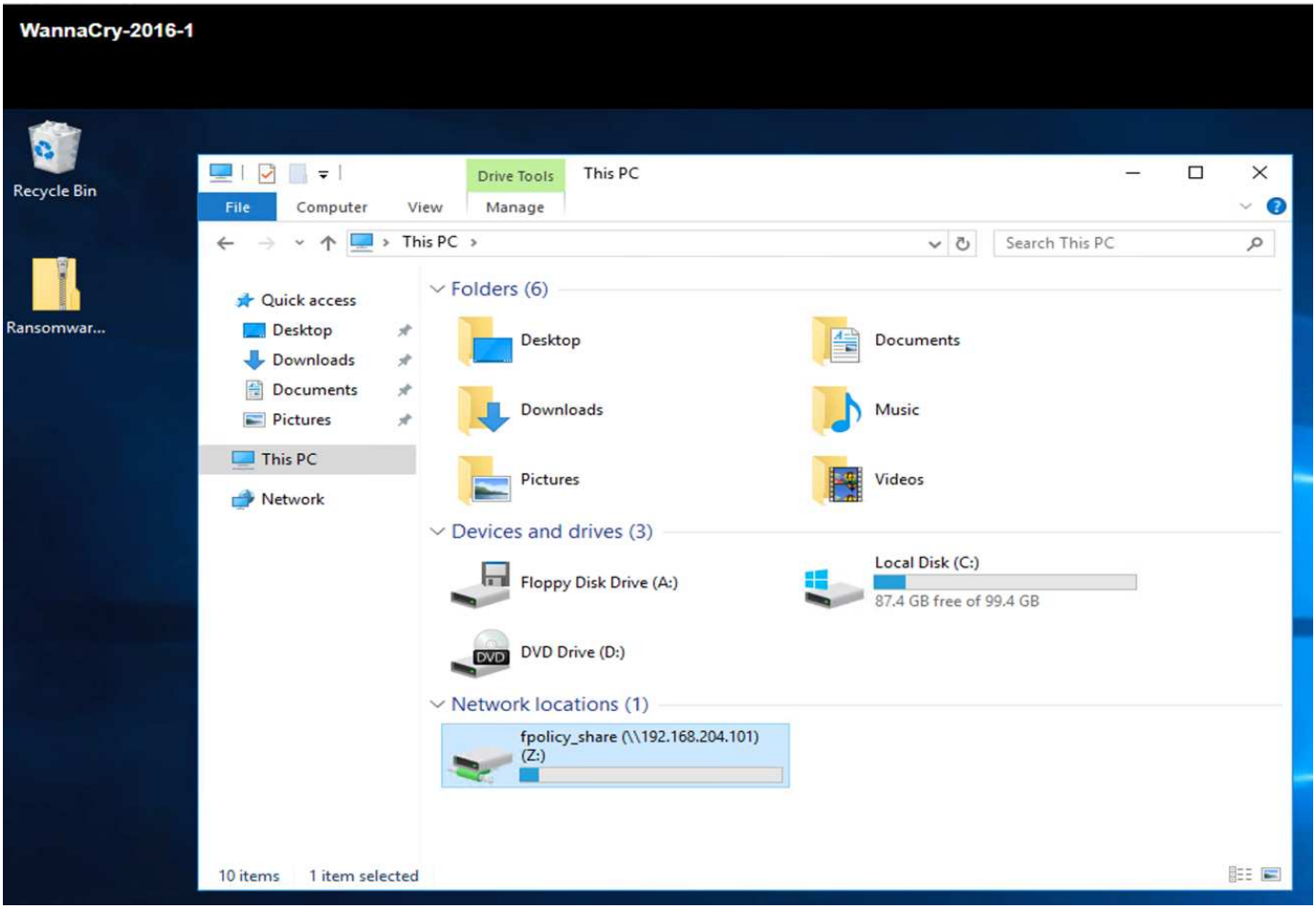
État du serveur virtuel et de ses fichiers avant une attaque

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

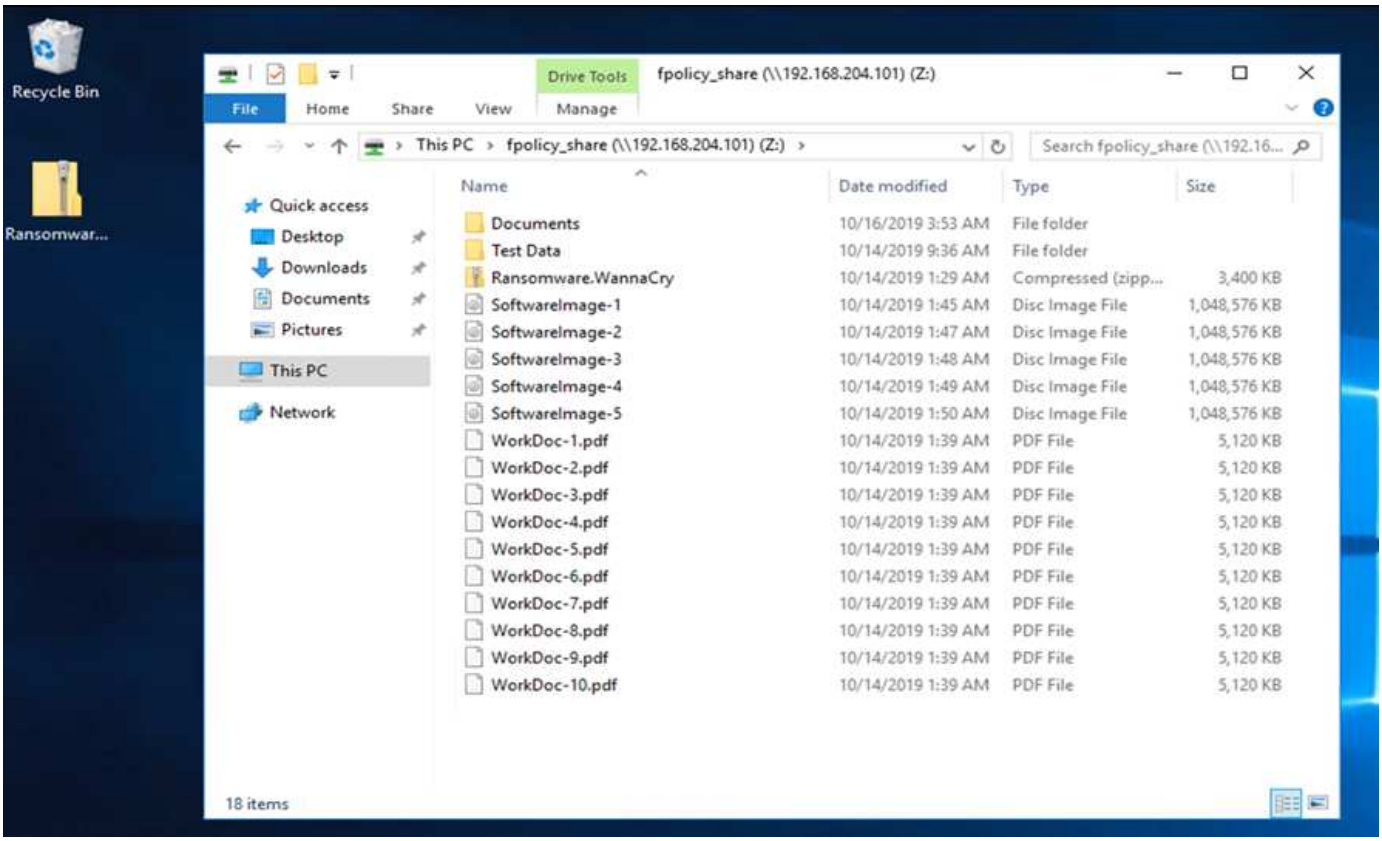
Le dossier documents de la machine virtuelle contient un ensemble de fichiers PDF qui n'ont pas encore été cryptés par le programme malveillant WannaCry.



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



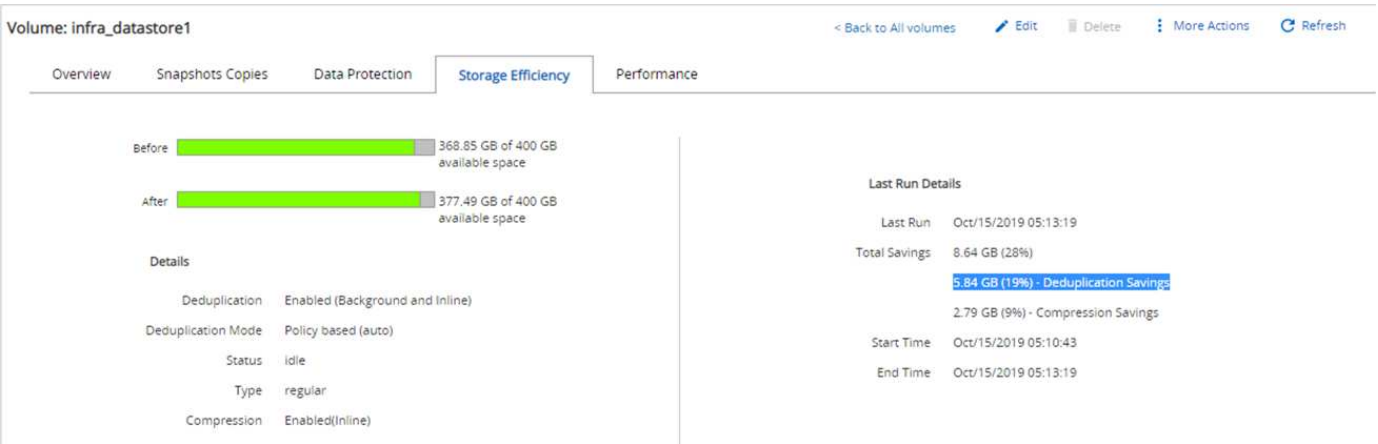
La capture d'écran suivante présente les fichiers du partage CIFS `fpolicy_share` Cela n'a pas encore été chiffré par le programme malveillant de WannaCry.



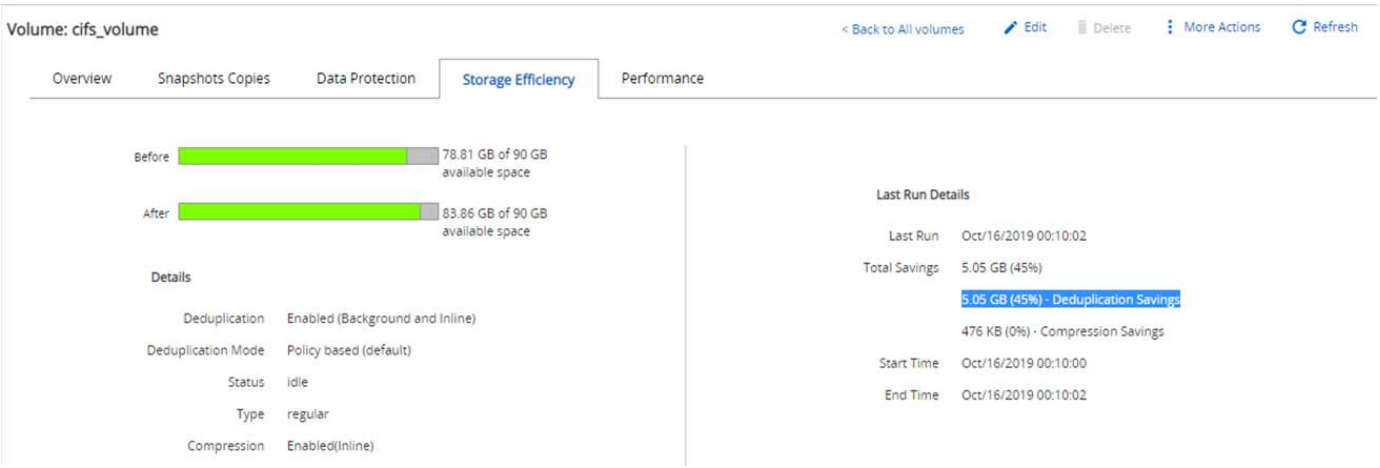
Informations relatives à la déduplication et aux snapshots avant la crise

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.

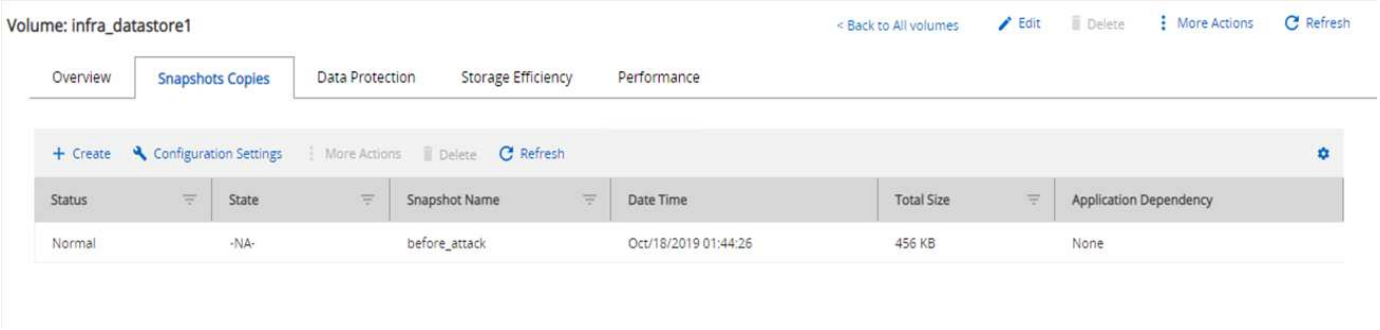
Des économies de stockage de 19 % ont été réalisées grâce à la déduplication sur le volume hébergeant la machine virtuelle.



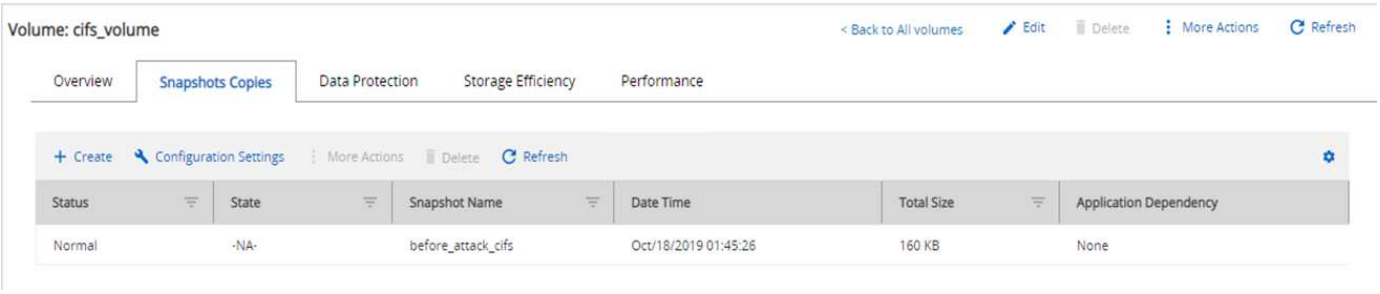
Des économies de stockage de 45 % ont été réalisées grâce à la déduplication sur le partage CIFS `fpolicy_share`.



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`.



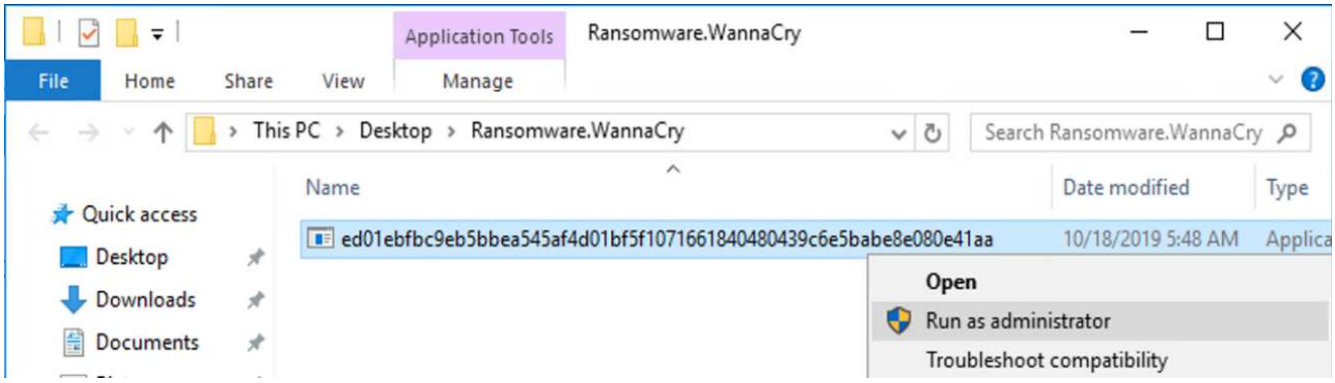
Infection de WannaCry sur VM et partage CIFS

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.

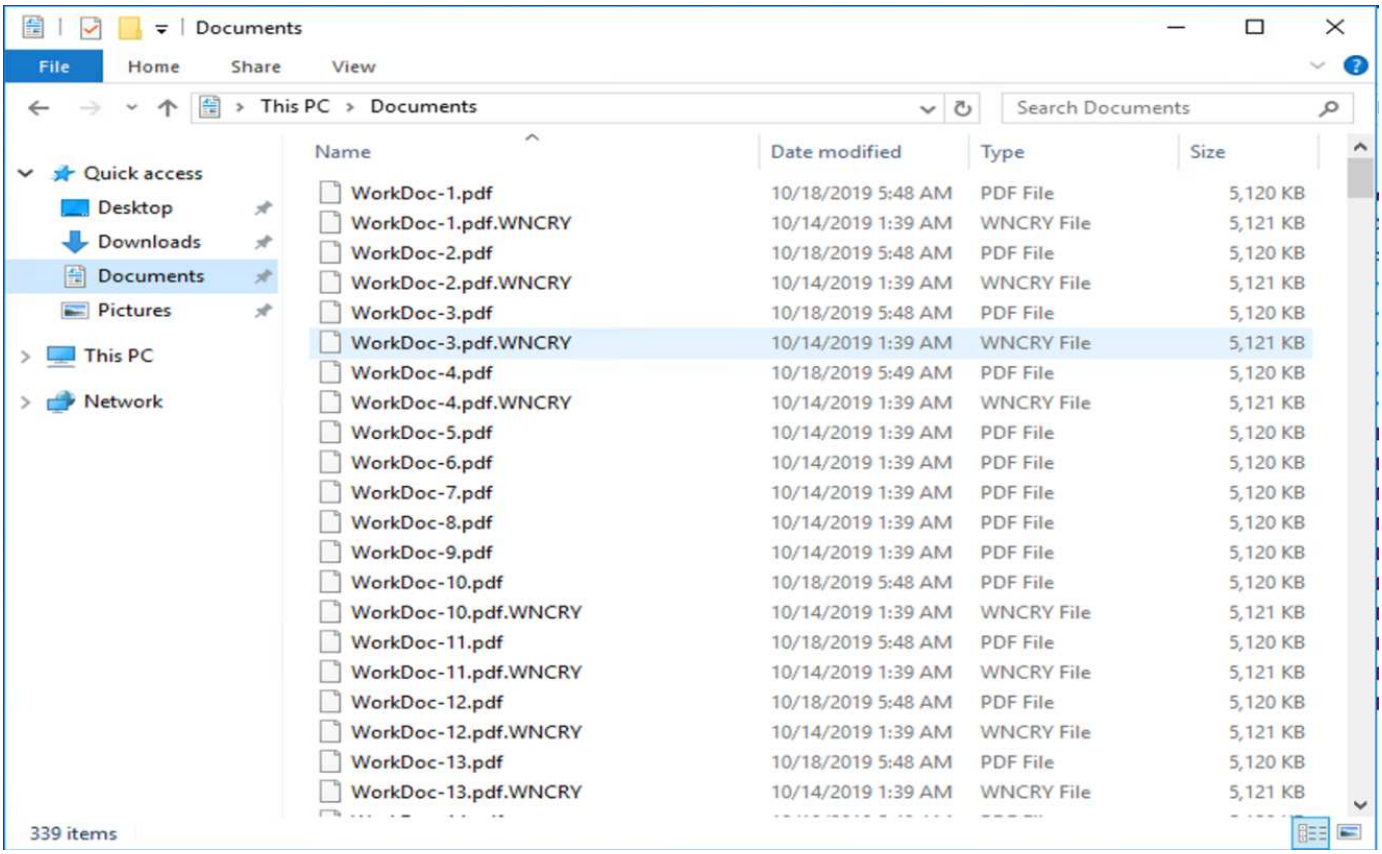
2. Le binaire a été exécuté.



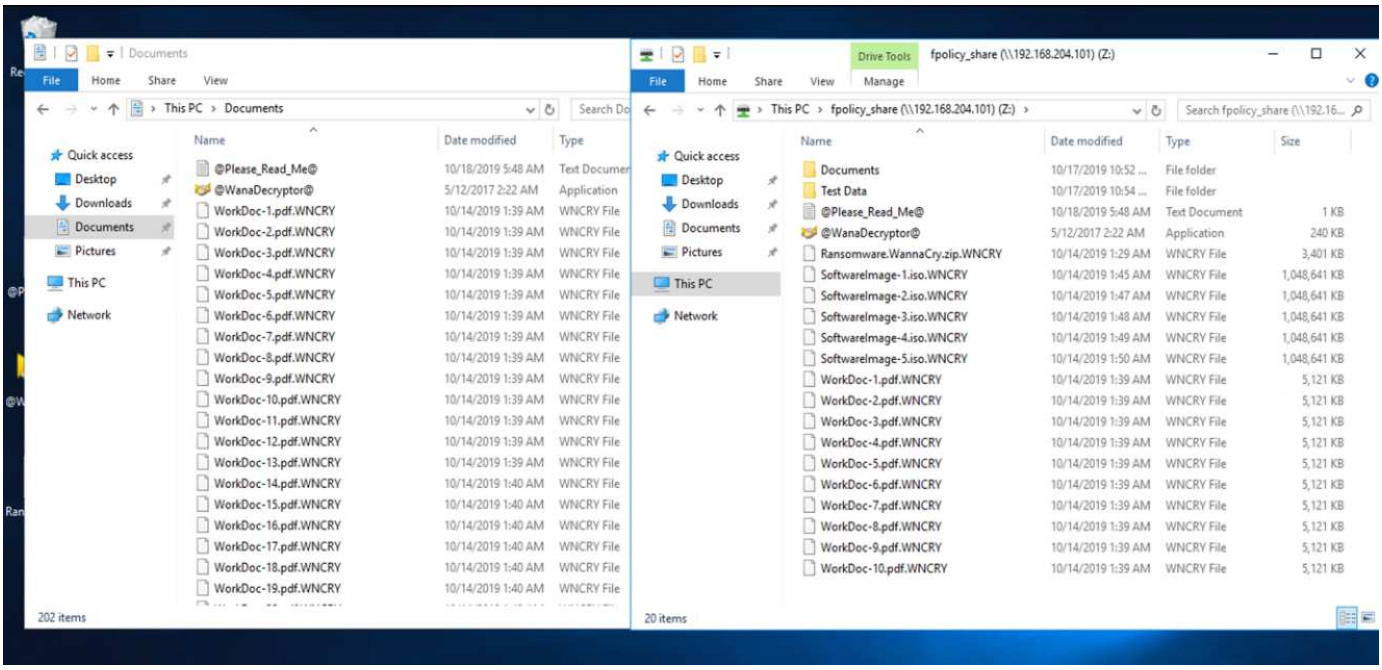
Cas 1 : WannaCry crypte le système de fichiers au sein de la machine virtuelle et le partage CIFS mappé

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.

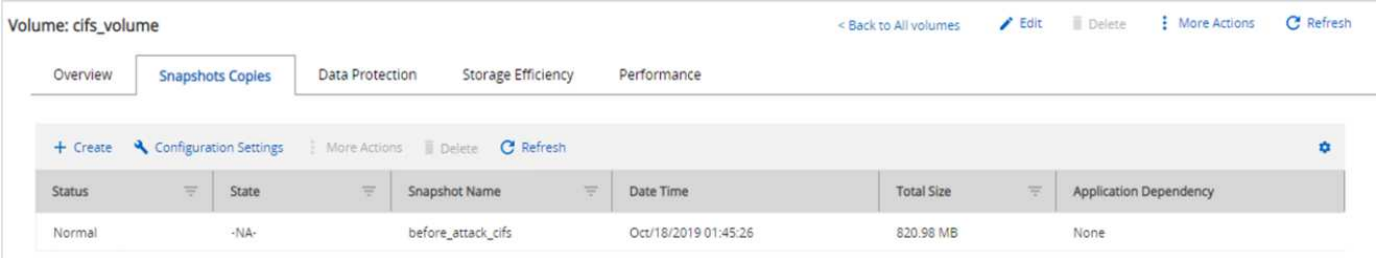


Détection

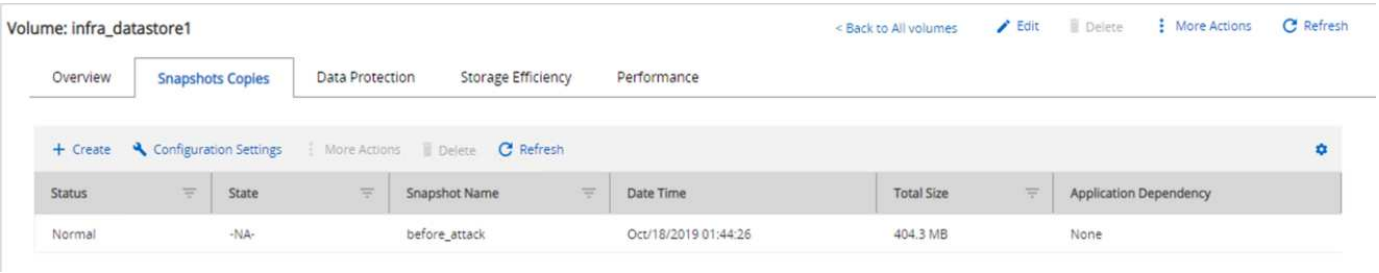
Au moment où le programme malveillant a commencé à chiffrer les fichiers, il a déclenché une augmentation exponentielle de la taille des copies Snapshot et une diminution exponentielle du pourcentage d'efficacité du stockage.

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

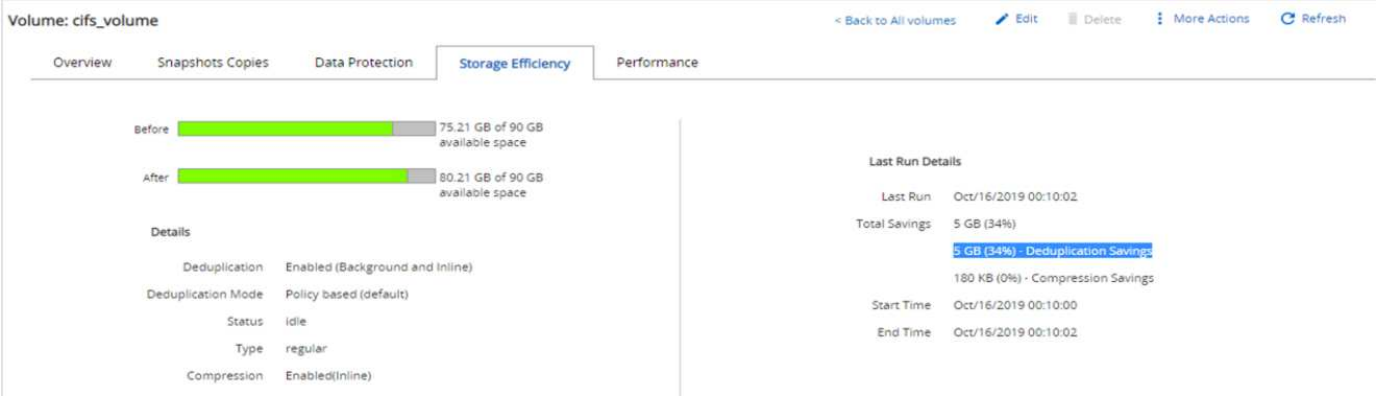
hébergeant le partage CIFS pendant l'attaque.



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 %.



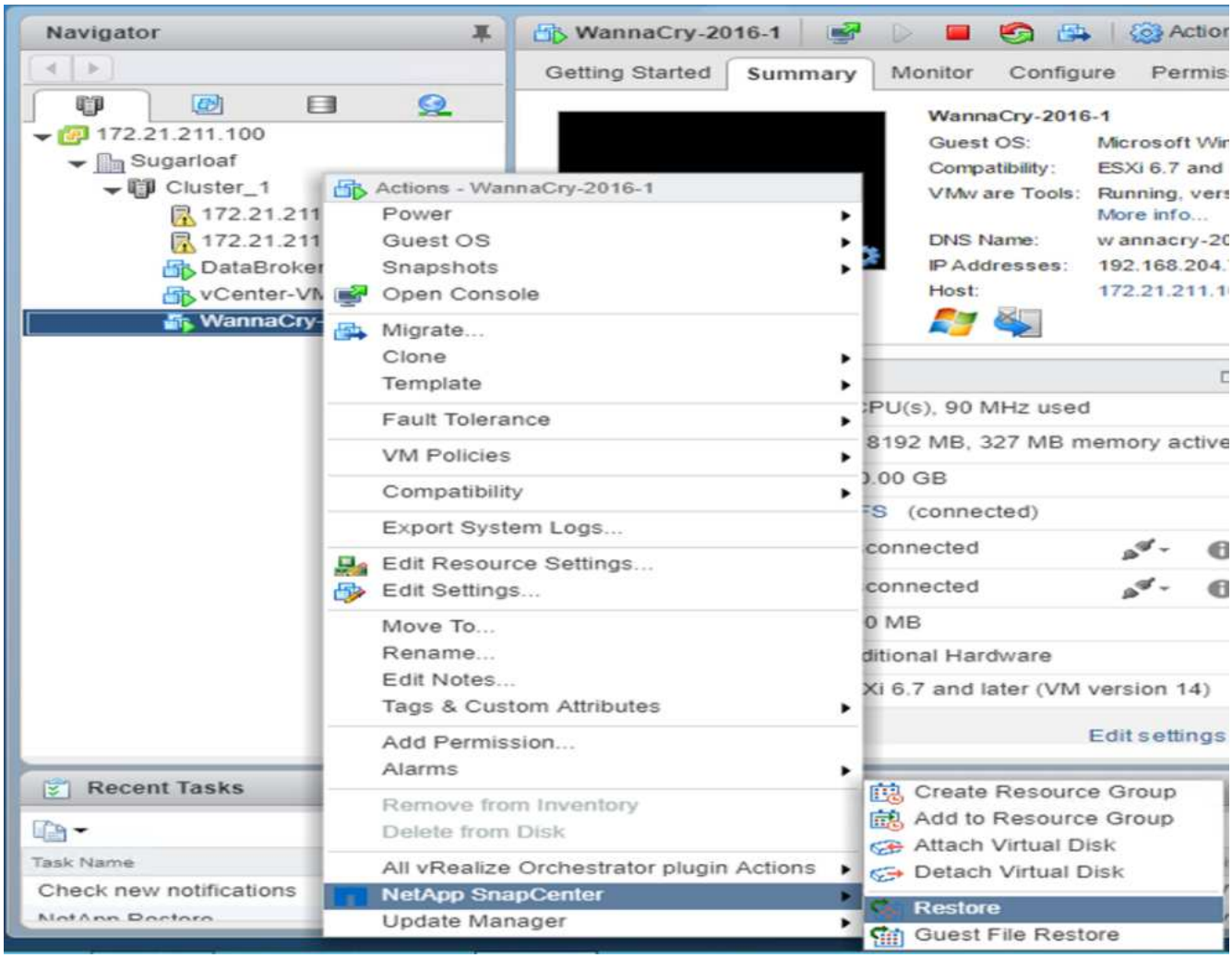
Résolution

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

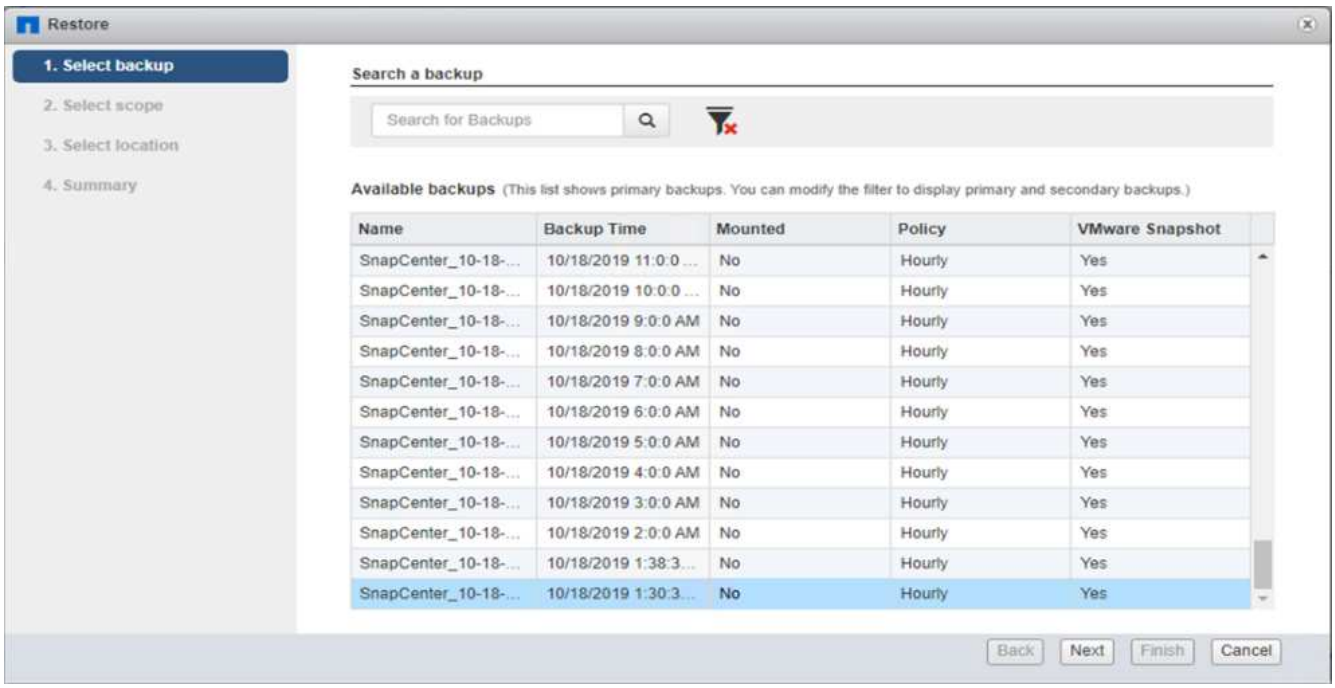
Restaurer VM

Pour restaurer la machine virtuelle, procédez comme suit :

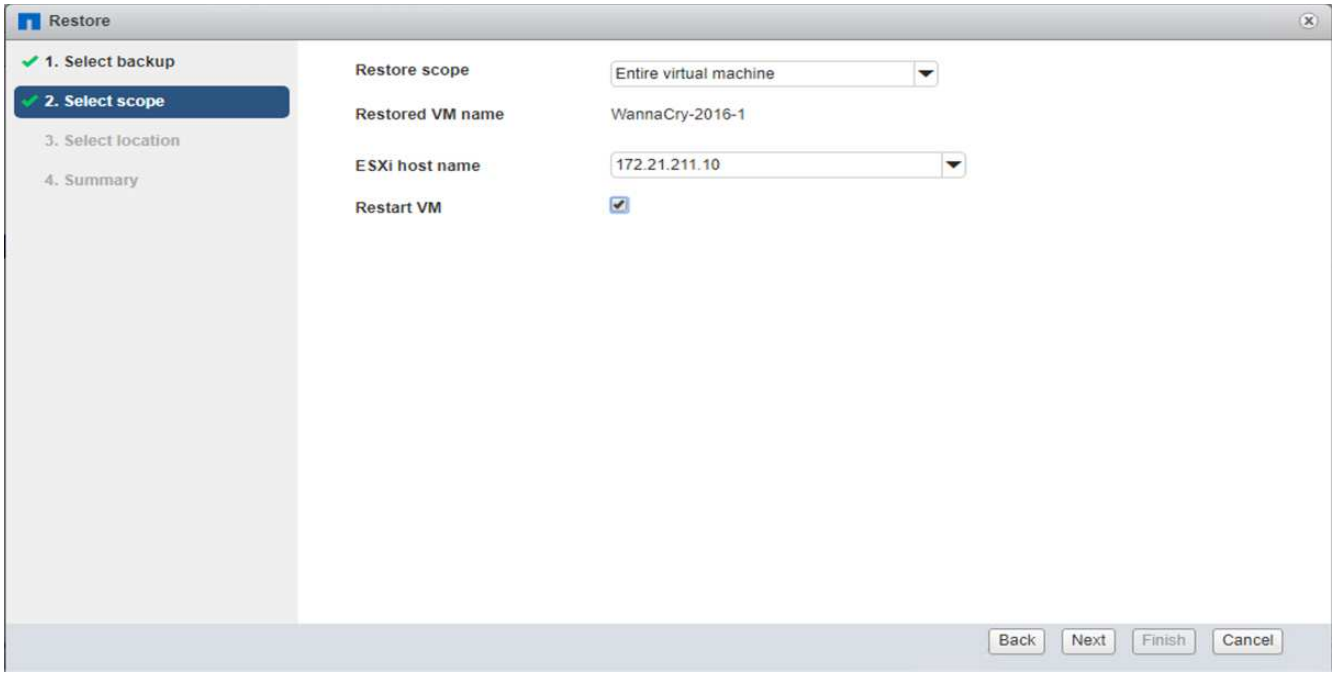
1. Utiliser la copie Snapshot que vous avez créée avec SnapCenter pour restaurer la machine virtuelle.



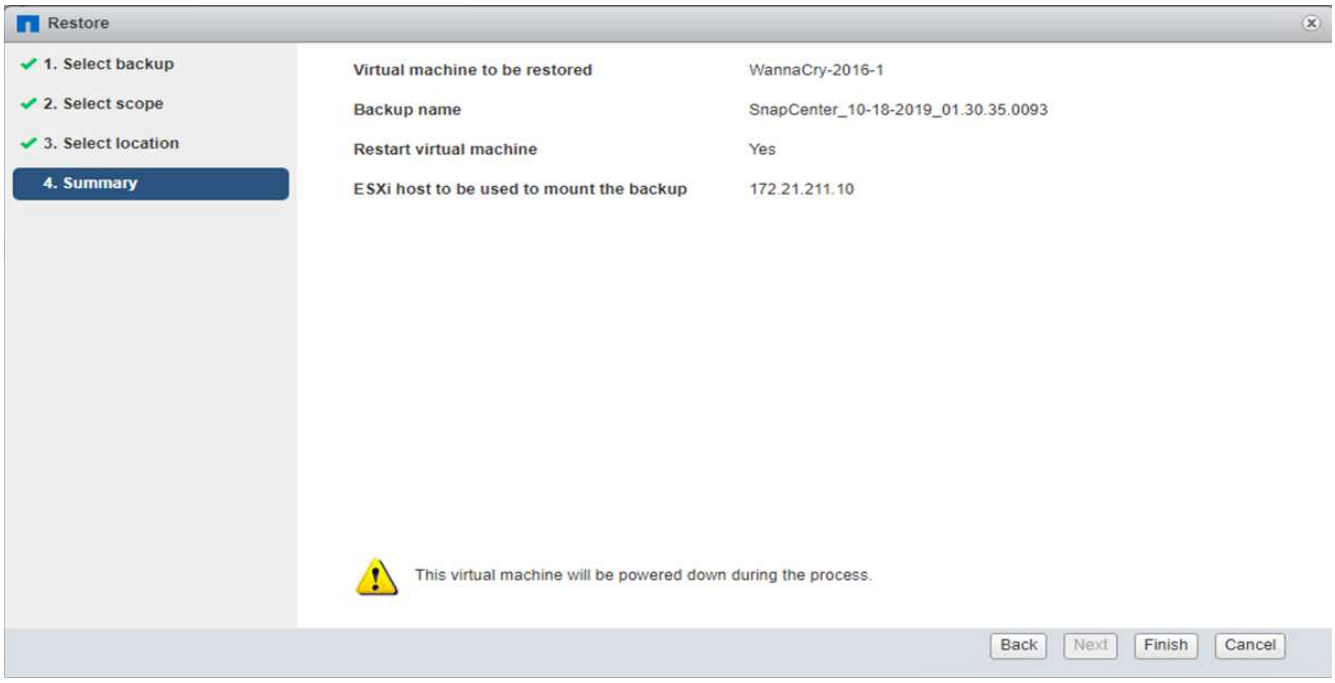
2. Sélectionnez la copie Snapshot cohérente avec VMware souhaitée pour la restauration.



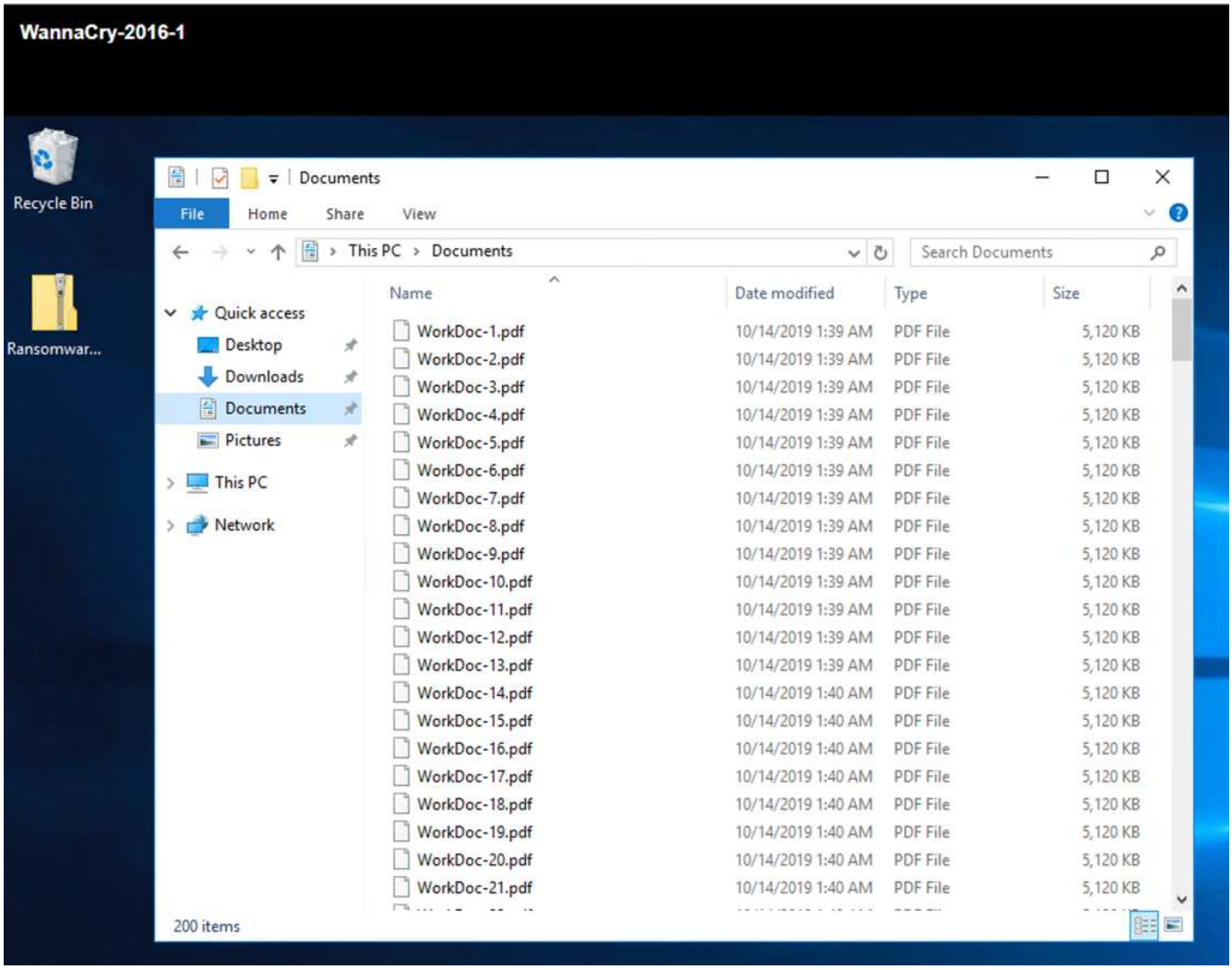
3. L'intégralité du serveur virtuel est restaurée et redémarrée.



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



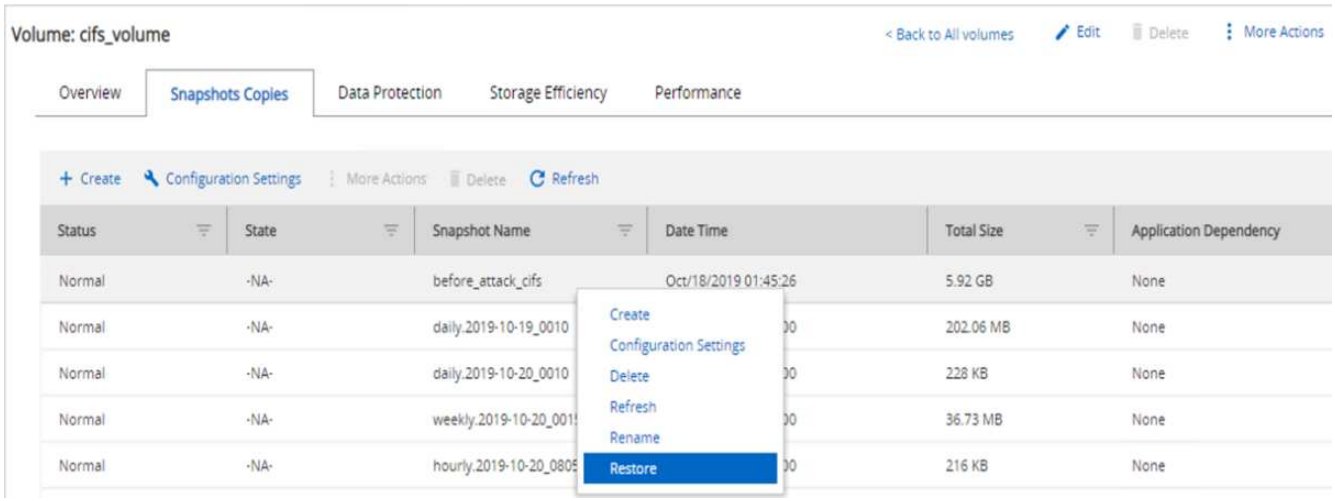
5. La machine virtuelle et ses fichiers sont restaurés.



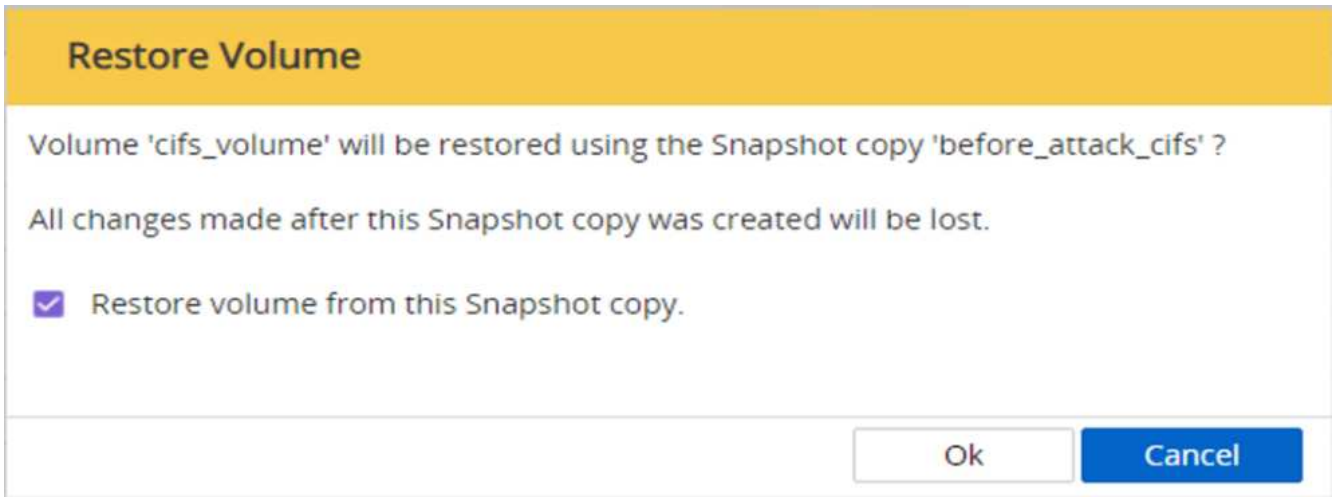
Restaurer le partage CIFS

Pour restaurer le partage CIFS, procédez comme suit :

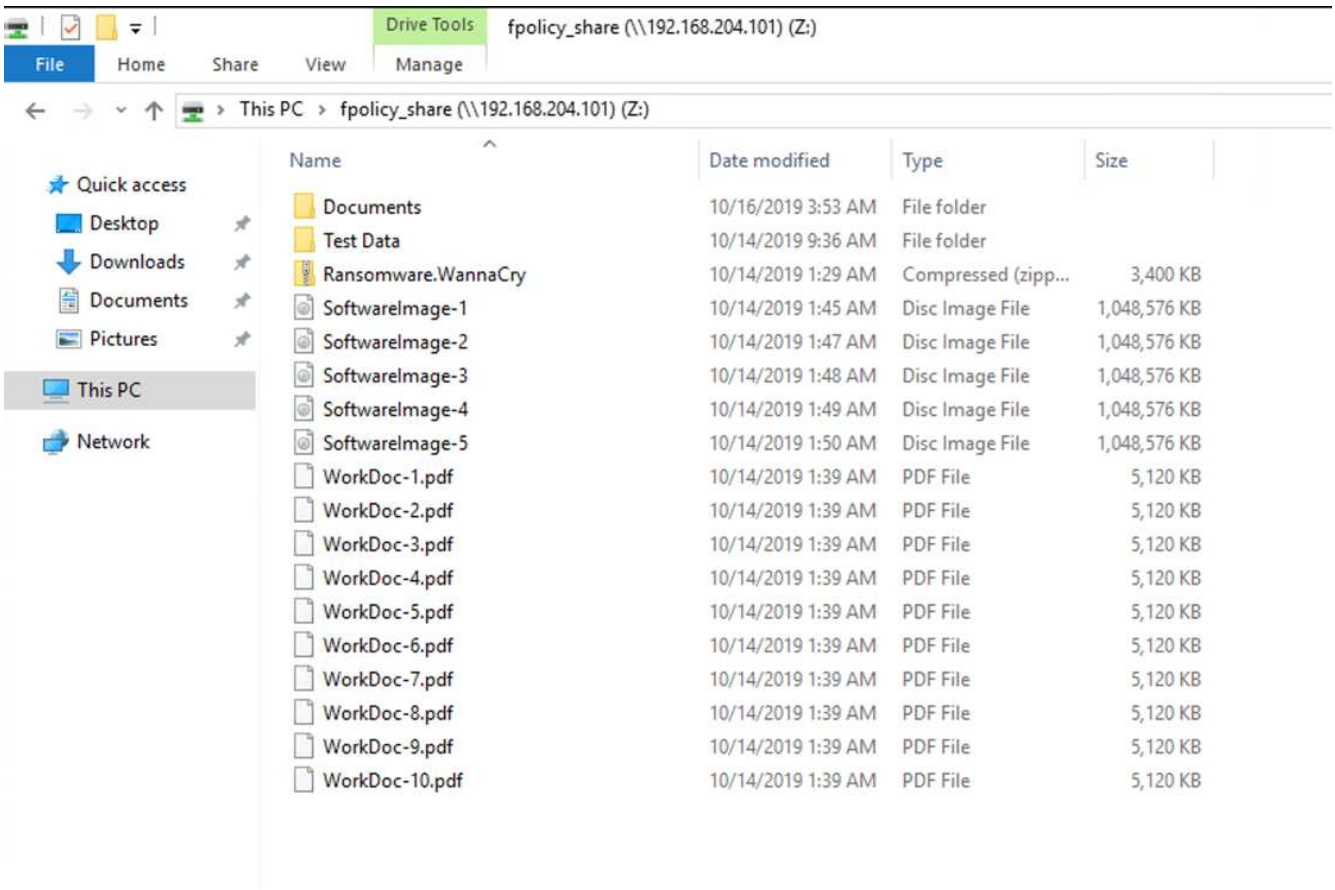
1. Utilisez la copie Snapshot du volume prise avant l'attaque pour restaurer le partage.



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

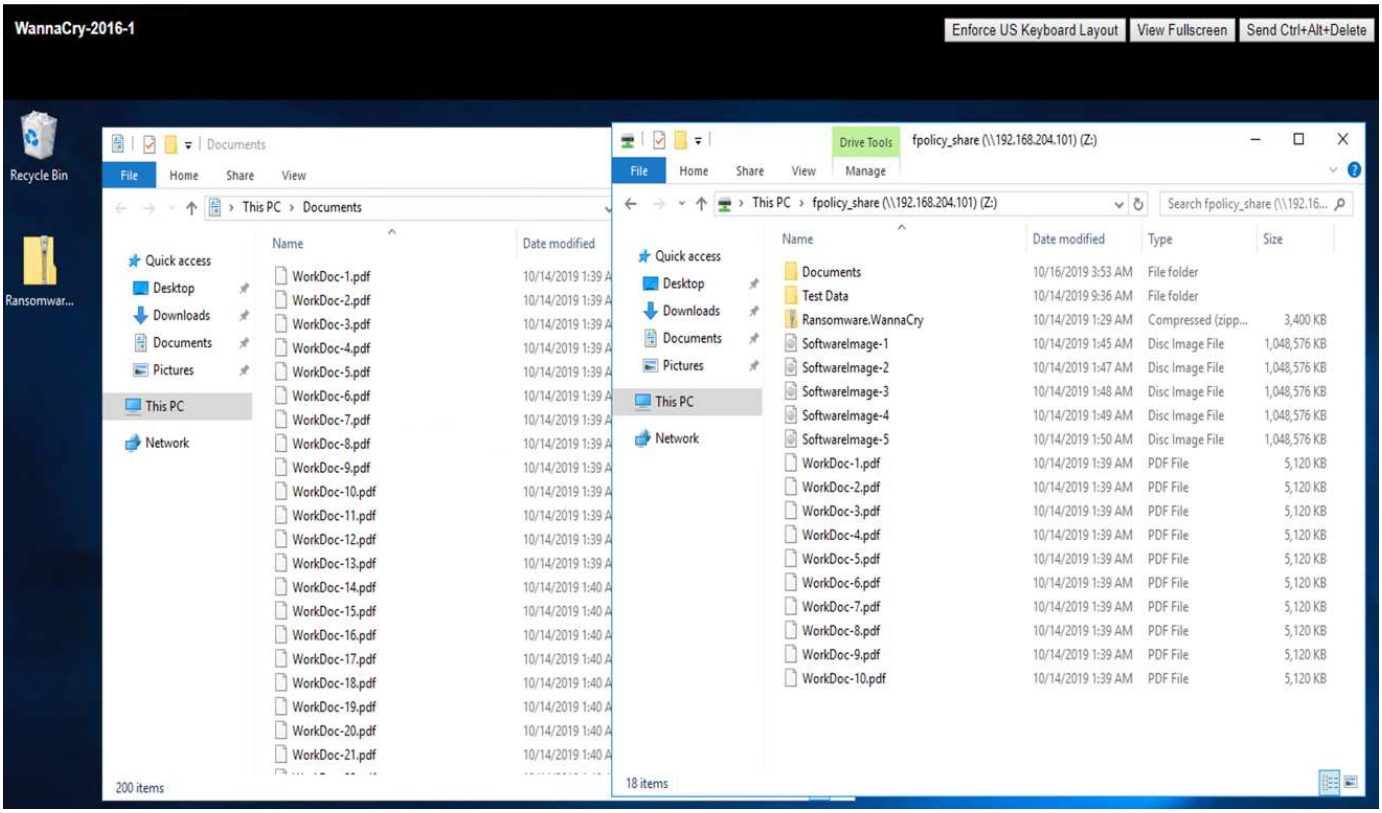
Configurer FPolicy

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

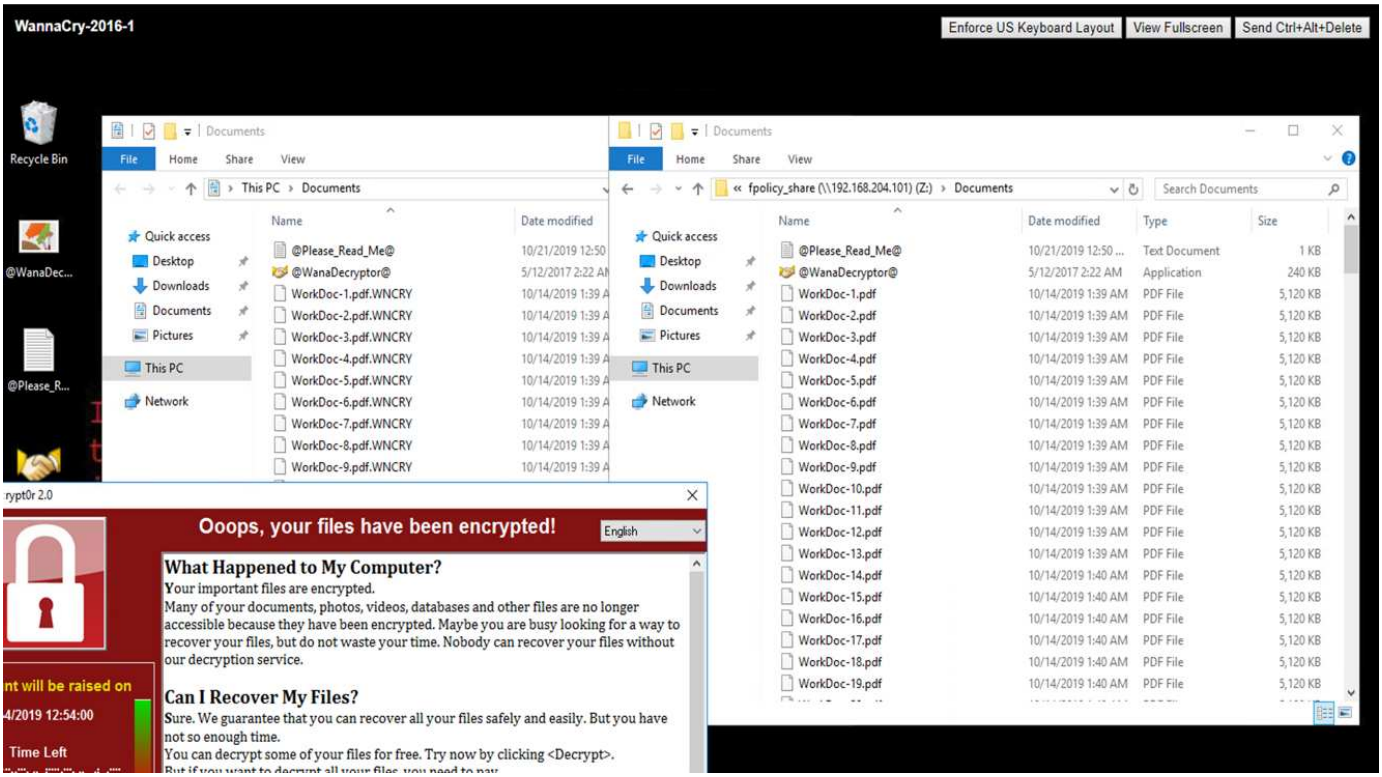
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create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

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.