Protection des données avec le coffre-fort cybernétique ONTAP

NetApp data management solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions-dataops/cyber-vault/ontap-cyber-vault-overview.html on August 18, 2025. Always check docs.netapp.com for the latest.

Sommaire

Protection des données avec le coffre-fort cybernétique ONTAP . . . 1
- Présentation du coffre-fort cybernétique ONTAP . . . 1
  - Qu’est-ce qu’un coffre-fort informatique ? . . . 1
  - L’approche de NetApp en matière de coffre-fort informatique . . . 1
- Terminologie de Cyber Vault ONTAP . . . 2
- Dimensionnement d’un coffre-fort informatique avec ONTAP . . . 3
  - Considérations relatives au dimensionnement des performances . . . 3
  - Considérations relatives au dimensionnement de la capacité . . . 4
- Créer un coffre-fort informatique avec ONTAP . . . 5
- Renforcement des coffres-forts informatiques . . . 7
  - Recommandations pour renforcer les coffres-forts informatiques . . . 7
- Interopérabilité des coffres-forts cybernétiques . . . 8
  - Recommandations matérielles ONTAP . . . 8
  - Recommandations du logiciel ONTAP . . . 8
  - Configuration de MetroCluster . . . 8
- Questions fréquemment posées sur le coffre-fort cybernétique . . . 9
  - Qu’est-ce qu’un coffre-fort cybernétique NetApp ? . . . 9
  - L’approche de NetApp en matière de coffre-fort informatique . . . 9
  - Questions fréquemment posées sur le coffre-fort cybernétique . . . 10
- Ressources du coffre-fort cybernétique . . . 13
- Création, renforcement et validation d’un coffre-fort cybernétique ONTAP avec PowerShell . . . 14
  - Présentation du coffre-fort cybernétique ONTAP avec PowerShell . . . 14
  - Création d’un coffre-fort cybernétique ONTAP avec PowerShell . . . 16
  - Renforcement du coffre-fort cybernétique ONTAP avec PowerShell . . . 20
  - Validation du coffre-fort cybernétique ONTAP avec PowerShell . . . 27
  - Récupération de données du coffre-fort cybernétique ONTAP . . . 32
  - Considérations supplémentaires . . . 33
  - Configurer, analyser, script cron . . . 35
  - Conclusion sur la solution PowerShell du coffre-fort cybernétique ONTAP . . . 36

Protection des données avec le coffre-fort cybernétique ONTAP

Présentation du coffre-fort cybernétique ONTAP

La principale menace qui nécessite la mise en œuvre d'un coffre-fort informatique est la prévalence croissante et la sophistication croissante des cyberattaques, en particulier les ransomwares et les violations de données. "Avec une augmentation du phishing" et des méthodes de vol d'informations d'identification toujours plus sophistiquées, les informations d'identification utilisées pour lancer une attaque par ransomware pourraient ensuite être utilisées pour accéder aux systèmes d'infrastructure. Dans ces cas, même les systèmes d'infrastructure renforcés risquent d'être attaqués. La seule défense contre un système compromis est de protéger et d'isoler vos données dans un coffre-fort informatique.

Le coffre-fort cybernétique basé sur ONTAP de NetApp offre aux entreprises une solution complète et flexible pour protéger leurs actifs de données les plus critiques. En exploitant l'espacement logique avec des méthodologies de renforcement robustes, ONTAP vous permet de créer des environnements de stockage sécurisés et isolés, résilients face aux cybermenaces en constante évolution. Avec ONTAP, vous pouvez garantir la confidentialité, l'intégrité et la disponibilité de vos données tout en maintenant l'agilité et l'efficacité de votre infrastructure de stockage.

> À partir de juillet 2024, le contenu des rapports techniques précédemment publiés au format PDF a été intégré à la documentation des produits ONTAP . De plus, les nouveaux rapports techniques (TR) tels que ce document ne recevront plus de numéros TR.

Qu'est-ce qu'un coffre-fort informatique ?

Un coffre-fort informatique est une technique spécifique de protection des données qui consiste à stocker des données critiques dans un environnement isolé, séparé de l'infrastructure informatique principale.

Référentiel de données « isolé », **immuable** et **indélébile**, immunisé contre les menaces affectant le réseau principal, telles que les logiciels malveillants, les rançongiciels ou même les menaces internes. Un coffre-fort informatique peut être réalisé avec des instantanés **immuables** et **indélébiles**.

Les sauvegardes par espacement d'air qui utilisent des méthodes traditionnelles impliquent la création d'espace et la séparation physique des supports primaire et secondaire. En déplaçant les médias hors site et/ou en coupant la connectivité, les mauvais acteurs n'ont pas accès aux données. Cela protège les données mais peut entraîner des temps de récupération plus lents.

L'approche de NetApp en matière de coffre-fort informatique

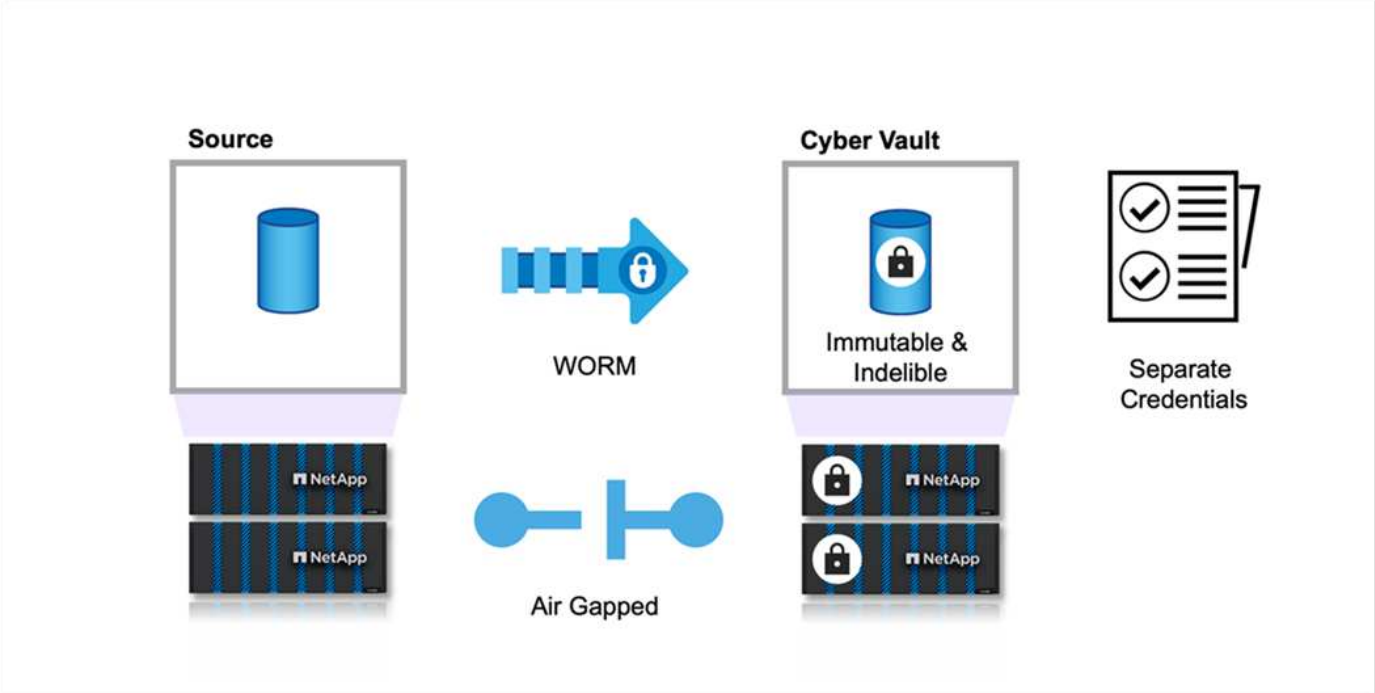
Les principales caractéristiques de l'architecture de référence NetApp pour un coffre-fort informatique comprennent :

- Infrastructure de stockage sécurisée et isolée (par exemple, systèmes de stockage isolés)
- Les copies des données doivent être à la fois **immuables** et **indélébiles** sans exception
- Contrôles d'accès stricts et authentification multifactorielle

- Capacités de restauration rapide des données

Vous pouvez utiliser le stockage NetApp avec ONTAP comme un coffre-fort cybernétique isolé en tirant parti"SnapLock Compliance aux copies Snapshot protégées par WORM" . Vous pouvez effectuer toutes les tâches de SnapLock Compliance de base sur le coffre-fort Cyber. Une fois configurés, les volumes Cyber Vault sont automatiquement protégés, éliminant ainsi le besoin de valider manuellement les copies Snapshot sur WORM. Vous trouverez plus d'informations sur l'espacement d'air logique dans ce document."blog"

SnapLock Compliance est utilisé pour se conformer aux réglementations bancaires et financières SEC 70-a-4(f), FINRA 4511(c) et CFTC 1.31(c)-(d). Il a été certifié par Cohasset Associates pour adhérer à ces réglementations (rapport d'audit disponible sur demande). En utilisant SnapLock Compliance avec cette certification, vous obtenez un mécanisme renforcé pour l'isolement de vos données sur lequel s'appuient les plus grandes institutions financières du monde pour garantir à la fois la conservation et la récupération des dossiers bancaires.



Terminologie de Cyber Vault ONTAP

Ce sont les termes couramment utilisés dans les architectures de coffres-forts cybernétiques.

Protection autonome contre les ransomwares (ARP) - La fonction de protection autonome contre les ransomwares (ARP) utilise l'analyse de la charge de travail dans les environnements NAS (NFS et SMB) pour détecter et avertir de manière proactive et en temps réel des activités anormales pouvant indiquer une attaque de ransomware. Lorsqu'une attaque est suspectée, ARP crée également de nouvelles copies Snapshot, en plus de la protection existante contre les copies Snapshot planifiées. Pour plus d'informations, consultez le"Documentation ONTAP sur la protection autonome contre les ransomwares"

Air-gap (logique) - Vous pouvez configurer le stockage NetApp avec ONTAP comme un coffre-fort cybernétique logique à air-gap en tirant parti de"SnapLock Compliance aux copies Snapshot protégées par WORM"

Air-gap (physique) - Un système physique isolé n'a aucune connectivité réseau. À l'aide de sauvegardes sur

bande, vous pouvez déplacer les images vers un autre emplacement. L'espace d'air logique SnapLock Compliance est tout aussi robuste qu'un système d'espace d'air physique.

Hôte bastion - Un ordinateur dédié sur un réseau isolé, configuré pour résister aux attaques.

Copies instantanées immuables - Copies instantanées qui ne peuvent pas être modifiées, sans exception (y compris une organisation de support ou la possibilité de formater de bas niveau le système de stockage).

Copies instantanées indélébiles - Copies instantanées qui ne peuvent pas être supprimées, sans exception (y compris une organisation de support ou la possibilité de formater à bas niveau le système de stockage).

Copies instantanées inviolables - Les copies instantanées inviolables utilisent la fonction d'horloge de SnapLock Compliance pour verrouiller les copies instantanées pendant une période spécifiée. Ces instantanés verrouillés ne peuvent pas être supprimés par un utilisateur ou par le support NetApp . Vous pouvez utiliser des copies Snapshot verrouillées pour récupérer des données si un volume est compromis par une attaque de ransomware, un logiciel malveillant, un pirate informatique, un administrateur malveillant ou une suppression accidentelle. Pour plus d'informations, consultez le"Documentation ONTAP sur les copies instantanées inviolables"

- SnapLock* - SnapLock est une solution de conformité haute performance pour les organisations qui utilisent le stockage WORM pour conserver des fichiers sous une forme non modifiée à des fins réglementaires et de gouvernance. Pour plus d'informations, consultez le "Documentation ONTAP sur SnapLock" .
- SnapMirror* - SnapMirror est une technologie de réplication de reprise après sinistre, conçue pour répliquer efficacement les données. SnapMirror peut créer un miroir (ou une copie exacte des données), un coffre-fort (une copie des données avec une conservation de copie Snapshot plus longue), ou les deux sur un système secondaire, sur site ou dans le cloud. Ces copies peuvent être utilisées à de nombreuses fins différentes, telles qu'une catastrophe, une explosion vers le cloud ou un coffre-fort informatique (lors de l'utilisation de la politique de coffre-fort et du verrouillage du coffre-fort). Pour plus d'informations, consultez le"Documentation ONTAP sur SnapMirror"
- SnapVault* - Dans ONTAP 9.3, SnapVault a été abandonné au profit de la configuration de SnapMirror à l'aide de la stratégie de coffre-fort ou de coffre-fort miroir. Ce terme, bien que toujours utilisé, a également été déprécié. Pour plus d'informations, consultez le "Documentation ONTAP sur SnapVault" .

Dimensionnement d'un coffre-fort informatique avec ONTAP

Le dimensionnement d'un coffre-fort informatique nécessite de comprendre la quantité de données qui devront être restaurées dans un objectif de temps de récupération (RTO) donné. De nombreux facteurs entrent en jeu dans la conception d'une solution de coffre-fort informatique de taille adaptée. Les performances et la capacité doivent être prises en compte lors du dimensionnement d'un coffre-fort informatique.

Considérations relatives au dimensionnement des performances

1. Quels sont les modèles de plateformes sources (FAS v AFF A-Series v AFF C-Series) ?
2. Quelle est la bande passante et la latence entre la source et le coffre-fort informatique ?
3. Quelle est la taille des fichiers et combien de fichiers ?
4. Quel est votre objectif de temps de récupération ?
5. Quelle quantité de données devez-vous récupérer dans le cadre du RTO ?

6. Combien de relations de fan-in SnapMirror le coffre-fort cybernétique va-t-il ingérer ?
7. Y aura-t-il une ou plusieurs récupérations en même temps ?
8. Ces multiples récupérations se produiront-elles lors de la même primaire ?
9. SnapMirror sera-t-il répliqué vers le coffre-fort lors d'une récupération à partir d'un coffre-fort ?

Exemples de dimensionnement

Voici des exemples de différentes configurations de coffres-forts cybernétiques.

Platform	AFF A1K	AFF C400	AFF C250	FAS70
Estimated RTO (100TB)	5 HR	18 HR	24 HR	24> HR
Relative cost	High	Moderate	Low	Ultra Low

Considérations relatives au dimensionnement de la capacité

La quantité d'espace disque requise pour un volume de destination de coffre-fort cybernétique ONTAP dépend de divers facteurs, dont le plus important est le taux de variation des données dans le volume source. La planification de sauvegarde et la planification d'instantanés sur le volume de destination affectent toutes deux l'utilisation du disque sur le volume de destination, et le taux de changement sur le volume source n'est probablement pas constant. Il est judicieux de prévoir une capacité de stockage supplémentaire au-delà de celle requise pour s'adapter aux changements futurs du comportement de l'utilisateur final ou de l'application.

Le dimensionnement d'une relation pour 1 mois de rétention dans ONTAP nécessite de calculer les besoins de stockage en fonction de plusieurs facteurs, notamment la taille de l'ensemble de données principal, le taux de modification des données (taux de modification quotidien) et les économies de déduplication et de compression (le cas échéant).

Voici l'approche étape par étape :

La première étape consiste à connaître la taille du ou des volumes sources que vous protégez avec le coffre-fort numérique. Il s'agit de la quantité de base de données qui sera initialement répliquée vers la destination du coffre-fort informatique. Ensuite, estimez le taux de variation quotidien de l'ensemble de données. Il s'agit du pourcentage de données qui change chaque jour. Il est essentiel de bien comprendre le caractère dynamique de vos données.

Par exemple:

- Taille du jeu de données principal = 5 To
- Taux de variation quotidien = 5 % (0,05)
- Efficacité de déduplication et de compression = 50 % (0,50)

Maintenant, passons en revue le calcul :

- Calculer le taux de variation des données quotidiennes :

```
Changed data per day = 5000 * 5% = 250GB
```

- Calculez le total des données modifiées sur 30 jours :

```
Total changed data in 30 days = 250 GB * 30 = 7.5TB
```

- Calculez le stockage total requis :

```
TOTAL = 5TB + 7.5TB = 12.5TB
```

- Appliquer les économies de déduplication et de compression :

```
EFFECTIVE = 12.5TB * 50% = 6.25TB
```

Résumé des besoins de stockage

- Sans efficacité : il faudrait **12,5 To** pour stocker 30 jours de données du coffre-fort informatique.
- Avec une efficacité de 50 % : il faudrait **6,25 To** de stockage après déduplication et compression.

> Les copies instantanées peuvent entraîner une surcharge supplémentaire en raison des métadonnées, mais celle-ci est généralement mineure.

> Si plusieurs sauvegardes sont effectuées par jour, ajustez le calcul en fonction du nombre de copies Snapshot effectuées chaque jour.

> Tenez compte de la croissance des données au fil du temps pour garantir que le dimensionnement est à l'épreuve du temps.

Créer un coffre-fort informatique avec ONTAP

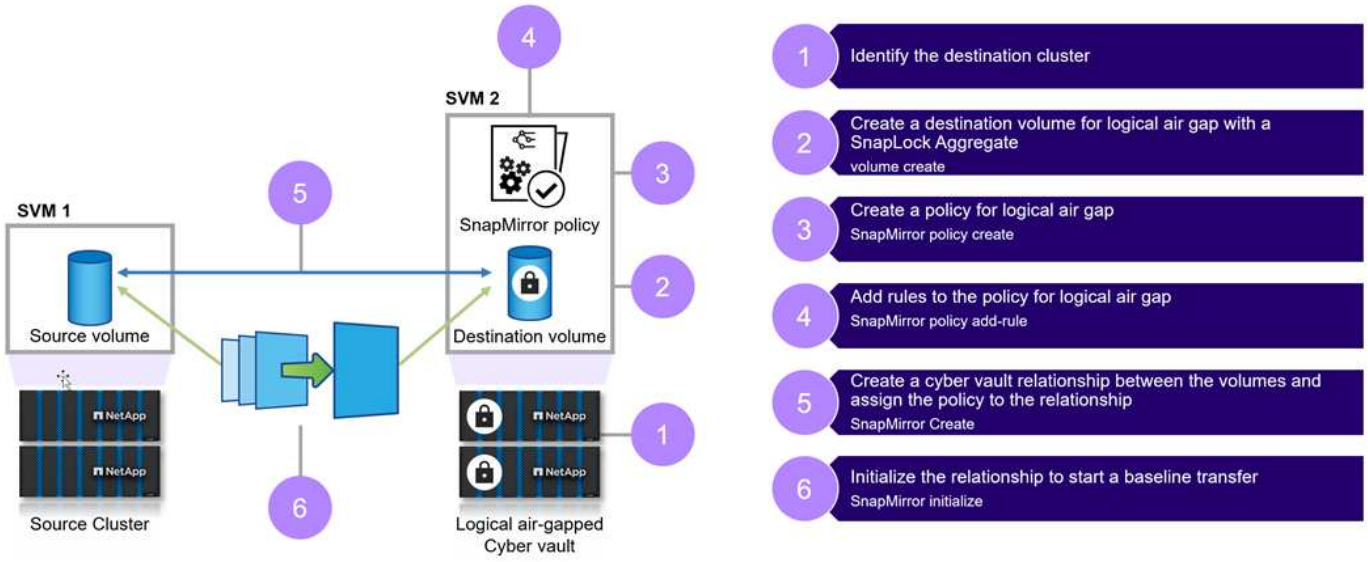
Les étapes ci-dessous vous aideront à créer un coffre-fort informatique avec ONTAP.

Avant de commencer

- Le cluster source doit exécuter ONTAP 9 ou une version ultérieure.
- Les agrégats source et de destination doivent être de 64 bits.
- Les volumes source et de destination doivent être créés dans des clusters appairés avec des SVM appairés. Pour plus d'informations, consultez la section "Appairage de cluster" .
- Si la croissance automatique du volume est désactivée, l'espace libre sur le volume de destination doit être au moins cinq pour cent supérieur à l'espace utilisé sur le volume source.

À propos de cette tâche

L'illustration suivante montre la procédure d'initialisation d'une relation de coffre de SnapLock Compliance :



Étapes

1. Identifiez le tableau de destination qui deviendra le coffre-fort cybernétique destiné à recevoir les données isolées.
2. Sur la baie de destination, pour préparer le coffre-fort cybernétique,"installer la licence ONTAP One" ,"initialiser l'horloge de conformité" , et, si vous utilisez une version ONTAP antérieure à 9.10.1,"créer un agrégat de SnapLock Compliance" .
3. Sur la baie de destination, créez un volume de destination SnapLock Compliance de type DP :

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name
   -snaplock-type compliance|enterprise -type DP -size size
   ```

4. À partir d' ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat ; par conséquent, vous n'êtes plus obligé de créer un agrégat SnapLock distinct si vous utilisez ONTAP 9.10.1. Vous utilisez le volume `-snaplock-type` option permettant de spécifier un type de conformité. Dans les versions ONTAP antérieures à ONTAP 9.10.1, le mode SnapLock , Compliance est hérité de l'agrégat. Les volumes de destination à version flexible ne sont pas pris en charge. Le paramètre de langue du volume de destination doit correspondre au paramètre de langue du volume source.

   La commande suivante crée un volume de SnapLock Compliance de 2 Go nommé `dstvolB` dans `SVM2` sur l'ensemble `node01_aggr` :

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate node01_aggr
   -snaplock-type compliance -type DP -size 2GB
   ```

5. Sur le cluster de destination, pour créer l'espace aérien, définissez la période de rétention par défaut, comme décrit dans"Définir la période de conservation par défaut" . Un volume SnapLock qui est une destination de coffre-fort dispose d'une période de rétention par défaut qui lui est attribuée. La valeur de cette période est initialement fixée à un minimum de 0 an et à un maximum de 100 ans (à partir de ONTAP 9.10.1. Pour les versions antérieures ONTAP , la valeur est comprise entre 0 et 70.) pour les volumes de SnapLock Compliance . Chaque copie NetApp Snapshot est initialement validée avec cette période de conservation par défaut. La période de conservation par défaut doit être modifiée. La période de conservation peut être prolongée ultérieurement, si nécessaire, mais jamais raccourcie. Pour plus d'informations, consultez la section "Aperçu de la durée de conservation des paramètres" .

> Les fournisseurs de services doivent tenir compte des dates de fin de contrat du client lors de la détermination de la période de conservation. Par exemple, si la période de conservation du coffre-fort électronique est de 30 jours et que le contrat du client se termine avant l'expiration de la période de conservation, les données du coffre-fort électronique ne peuvent pas être supprimées avant l'expiration de la période de conservation.

6. "Créer une nouvelle relation de réplication"entre la source non SnapLock et la nouvelle destination SnapLock que vous avez créée à l'étape 3.

   Cet exemple crée une nouvelle relation SnapMirror avec le volume SnapLock de destination dstvolB en utilisant une stratégie XDPDefault pour sauvegarder des copies Snapshot étiquetées quotidiennement et hebdomadairement selon un calendrier horaire :

   ```
   cluster2::> snapmirror create -source-path SVM1:srcvolA -destination-path
   SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
   ```

   "Créer une politique de réplication personnalisée"ou un"horaire personnalisé" si les valeurs par défaut disponibles ne conviennent pas.

7. Sur le SVM de destination, initialisez la relation SnapVault créée à l'étape 5 :

   ```
   snapmirror initialize -destination-path destination_path
   ```

8. La commande suivante initialise la relation entre le volume source srcvolA sur SVM1 et le volume de destination dstvolB sur SVM2 :

   ```
   cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```

9. Une fois la relation initialisée et inactive, utilisez la commande snapshot show sur la destination pour vérifier le délai d'expiration SnapLock appliqué aux copies Snapshot répliquées.

   Cet exemple répertorie les copies Snapshot sur le volume dstvolB qui ont l'étiquette SnapMirror et la date d'expiration SnapLock :

   ```
   cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields snapmirror-
   label, snaplock-expiry-time
   ```

Renforcement des coffres-forts informatiques

Voici les recommandations supplémentaires pour renforcer un coffre-fort cybernétique ONTAP . Veuillez consulter le guide de durcissement ONTAP ci-dessous pour plus de recommandations et de procédures.

Recommandations pour renforcer les coffres-forts informatiques

- Isoler les plans de gestion du coffre-fort cybernétique
- N'activez pas les LIF de données sur le cluster de destination car ils constituent un vecteur d'attaque supplémentaire
- Sur le cluster de destination, limitez l'accès LIF intercluster au cluster source avec une politique de service
- Segmentez le LIF de gestion sur le cluster de destination pour un accès limité avec une politique de

service et un hôte bastion

- Restreindre tout le trafic de données du cluster source vers le coffre-fort cybernétique pour autoriser uniquement les ports requis pour le trafic SnapMirror
- Dans la mesure du possible, désactivez toutes les méthodes d'accès de gestion inutiles dans ONTAP pour réduire la surface d'attaque.
- Activer la journalisation d'audit et le stockage des journaux à distance
- Activez la vérification multi-administrateur et exigez la vérification d'un administrateur extérieur à vos administrateurs de stockage habituels (par exemple, le personnel du CISO)
- Mettre en œuvre des contrôles d'accès basés sur les rôles
- Exiger une authentification administrative multifacteur pour le Gestionnaire système et SSH
- Utiliser l'authentification basée sur des jetons pour les scripts et les appels d'API REST

Veuillez vous référer à la"Guide de durcissement ONTAP" ,"Présentation de la vérification multi-administrateur" et"Guide d'authentification multifacteur ONTAP" pour savoir comment réaliser ces étapes de durcissement.

Interopérabilité des coffres-forts cybernétiques

Le matériel et le logiciel ONTAP peuvent être utilisés pour créer une configuration de coffre-fort cybernétique.

Recommandations matérielles ONTAP

Toutes les baies physiques unifiées ONTAP peuvent être utilisées pour une implémentation de coffre-fort cybernétique.

- Le stockage hybride FAS offre la solution la plus rentable.
- La série AFF C offre la consommation d'énergie et la densité les plus efficaces.
- AFF A-Series est la plateforme la plus performante offrant le meilleur RTO. Avec l'annonce récente de notre dernière série AFF A, cette plate-forme offrira la meilleure efficacité de stockage sans compromis sur les performances.

Recommandations du logiciel ONTAP

À partir d' ONTAP 9.14.1, vous pouvez spécifier des périodes de rétention pour des étiquettes SnapMirror spécifiques dans la stratégie SnapMirror de la relation SnapMirror afin que les copies Snapshot répliquées du volume source vers le volume de destination soient conservées pendant la période de rétention spécifiée dans la règle. Si aucune période de rétention n'est spécifiée, la période de rétention par défaut du volume de destination est utilisée.

À partir d' ONTAP 9.13.1, vous pouvez restaurer instantanément une copie Snapshot verrouillée sur le volume SnapLock de destination d'une relation de coffre SnapLock en créant un FlexClone avec l'option snaplock-type définie sur « non-snaplock » et en spécifiant la copie Snapshot comme « parent-snapshot » lors de l'exécution de l'opération de création de clone de volume. En savoir plus sur "création d'un volume FlexClone avec un type SnapLock" .

Configuration de MetroCluster

Pour les configurations MetroCluster , vous devez tenir compte des points suivants :

- Vous pouvez créer une relation SnapVault uniquement entre des SVM sources de synchronisation, et non entre une SVM source de synchronisation et une SVM de destination de synchronisation.
- Vous pouvez créer une relation SnapVault à partir d'un volume sur une SVM source de synchronisation vers une SVM de service de données.
- Vous pouvez créer une relation SnapVault à partir d'un volume sur un SVM de service de données vers un volume DP sur un SVM source de synchronisation.

Questions fréquemment posées sur le coffre-fort cybernétique

Cette FAQ est destinée aux clients et partenaires NetApp . Il répond aux questions fréquemment posées sur l'architecture de référence du coffre-fort cybernétique basé sur ONTAP de NetApp.

Qu'est-ce qu'un coffre-fort cybernétique NetApp ?

Le coffre-fort informatique est une technique spécifique de protection des données qui consiste à stocker les données dans un environnement isolé, séparé de l'infrastructure informatique principale.

Un coffre-fort informatique est un référentiel de données « isolé », immuable et indélébile, immunisé contre les menaces affectant les données primaires, telles que les logiciels malveillants, les rançongiciels ou les menaces internes. Un coffre-fort cybernétique peut être réalisé avec des copies immuables de NetApp ONTAP Snapshot et rendu indélébile avec NetApp SnapLock Compliance. Sous la protection de SnapLock Compliance , les données ne peuvent pas être modifiées ou supprimées, même par les administrateurs ONTAP ou le support NetApp .

Les sauvegardes par espacement d'air utilisant des méthodes traditionnelles impliquent de créer de l'espace et de séparer physiquement les supports primaire et secondaire. L'espace aérien avec cyber-coffre-fort comprend l'utilisation d'un réseau de réplication de données distinct en dehors des réseaux d'accès aux données standard pour répliquer les copies Snapshot vers une destination indélébile.

D'autres mesures au-delà des réseaux isolés impliquent la désactivation de tous les protocoles d'accès aux données et de réplication sur le coffre-fort informatique lorsqu'ils ne sont pas nécessaires. Cela empêche l'accès aux données ou l'exfiltration de données sur le site de destination. Avec SnapLock Compliance, la séparation physique n'est pas requise. SnapLock Compliance protège vos copies Snapshot en lecture seule, à un instant T, stockées dans un coffre-fort, ce qui permet une récupération rapide des données, à l'abri de la suppression et immuable.

L'approche de NetApp en matière de coffre-fort informatique

NetApp Cyber Vault, optimisé par SnapLock, offre aux organisations une solution complète et flexible pour protéger leurs actifs de données les plus critiques. En exploitant les technologies de renforcement d' ONTAP, NetApp vous permet de créer un coffre-fort cybernétique sécurisé, isolé et isolé, immunisé contre les cybermenaces en constante évolution. Avec NetApp, vous pouvez garantir la confidentialité, l'intégrité et la disponibilité de vos données tout en maintenant l'agilité et l'efficacité de votre infrastructure de stockage.

Les principales caractéristiques de l'architecture de référence NetApp pour un coffre-fort informatique comprennent :

- Infrastructure de stockage sécurisée et isolée (par exemple, systèmes de stockage isolés)
- Les copies de sauvegarde de vos données sont à la fois immuables et indélébiles

- Contrôles d'accès stricts et séparés, vérification multi-administrateur et authentification multifacteur
- Capacités de restauration rapide des données

Questions fréquemment posées sur le coffre-fort cybernétique

Cyber Vault est-il un produit de NetApp?

Non, « cyber-coffre-fort » est un terme utilisé dans toute l'industrie. NetApp a créé une architecture de référence pour permettre aux clients de créer facilement leurs propres coffres-forts cybernétiques et d'exploiter les dizaines de fonctionnalités de sécurité ONTAP pour aider à protéger leurs données contre les cybermenaces. Plus d'informations sont disponibles sur le"Site de documentation ONTAP" .

Cyber Vault avec NetApp est-il juste un autre nom pour LockVault ou SnapVault?

LockVault était une fonctionnalité du mode Data ONTAP 7 qui n'est pas disponible dans les versions actuelles d' ONTAP.

SnapVault était un terme hérité pour ce qui est maintenant accompli avec la politique de coffre-fort de SnapMirror. Cette politique permet à la destination de conserver une quantité différente de copies Snapshot que le volume source.

Cyber Vault utilise SnapMirror avec la politique de coffre-fort et la SnapLock Compliance ensemble pour créer une copie immuable et indélébile des données.

Quel matériel NetApp puis-je utiliser pour un coffre-fort cybernétique, un FAS, un flash de capacité ou un flash de performance ?

Cette architecture de référence pour le cyber-voûte s'applique à l'ensemble du portefeuille matériel ONTAP . Les clients peuvent utiliser les plates-formes AFF A-Series, AFF C-Series ou FAS comme coffre-fort. Les plates-formes basées sur Flash offriront les temps de récupération les plus rapides, tandis que les plates-formes basées sur disque offriront la solution la plus rentable. Selon la quantité de données récupérées et si plusieurs récupérations se produisent en parallèle, l'utilisation de systèmes sur disque (FAS) peut prendre des jours, voire des semaines. Veuillez consulter un représentant NetApp ou un partenaire pour dimensionner correctement une solution de coffre-fort informatique afin de répondre aux exigences de l'entreprise.

Puis-je utiliser Cloud Volumes ONTAP comme source de coffre-fort informatique ?

Oui, cependant, l'utilisation de CVO comme source nécessite que les données soient répliquées vers une destination de coffre-fort cybernétique sur site, car la SnapLock Compliance est une exigence pour un coffre-fort cybernétique ONTAP . La réplication des données à partir d'une instance CVO basée sur un hyperscaler peut entraîner des frais de sortie.

Puis-je utiliser Cloud Volumes ONTAP comme destination de coffre-fort informatique ?

L'architecture Cyber Vault s'appuie sur l'indélébilité de la conformité SnapLock d'ONTAP et est conçue pour les implémentations sur site. Les architectures Cyber Vault basées sur le cloud sont à l'étude en vue d'une publication future.

Puis-je utiliser ONTAP Select comme source de coffre-fort informatique ?

Oui, ONTAP Select peut être utilisé comme source vers une destination de coffre-fort cybernétique basée sur du matériel sur site.

Puis-je utiliser ONTAP Select comme destination de coffre-fort informatique ?

Non, ONTAP Select ne doit pas être utilisé comme destination de coffre-fort informatique car il n'a pas la capacité d'utiliser SnapLock Compliance.

Un coffre-fort cybernétique avec NetApp utilise-t-il simplement SnapMirror?

Non, une architecture de coffre-fort cybernétique NetApp exploite de nombreuses fonctionnalités ONTAP pour créer une copie sécurisée, isolée, isolée et renforcée des données. Pour plus d'informations sur les techniques supplémentaires qui peuvent être utilisées, consultez la question suivante.

Existe-t-il d'autres technologies ou configurations utilisées pour le coffre-fort cybernétique ?

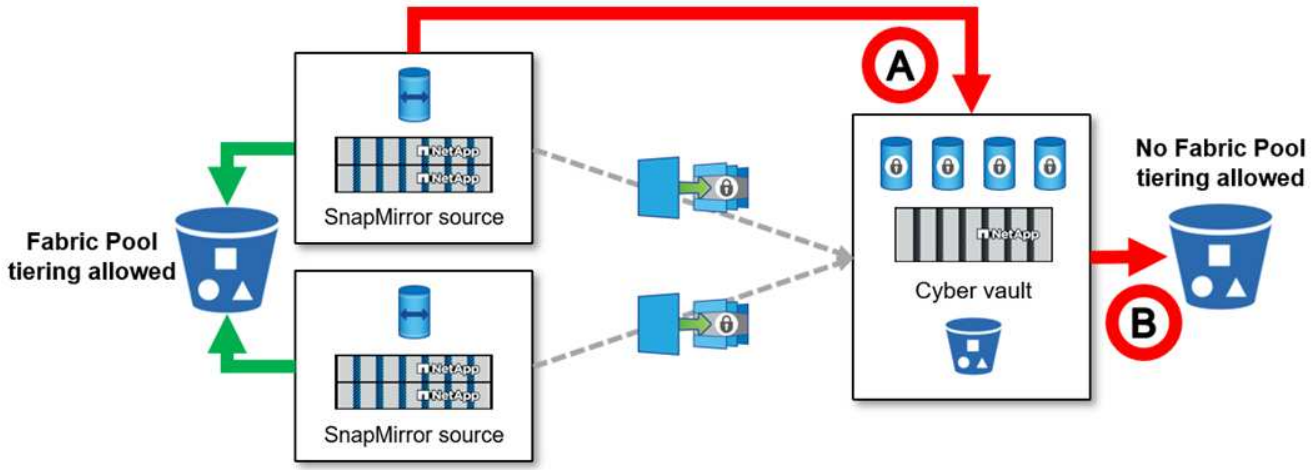
La base d'un coffre-fort cybernétique NetApp est SnapMirror et SnapLock Compliance, mais l'utilisation de fonctionnalités ONTAP supplémentaires telles que les copies Snapshot inviolables, l'authentification multifacteur (MFA), la vérification multi-administrateur, le contrôle d'accès basé sur les rôles et la journalisation d'audit à distance et locale, améliore la sécurité et la sûreté des données.

Qu'est-ce qui rend les copies ONTAP Snapshot meilleures que les autres pour un coffre-fort informatique ?

Les copies d'instantanés ONTAP sont immuables par défaut et peuvent être rendues indélébiles avec SnapLock Compliance. Même le support NetApp ne peut pas supprimer les copies SnapLock Snapshot. La meilleure question à se poser est de savoir ce qui rend le coffre-fort cybernétique de NetApp meilleur que les autres coffres-forts cybernétiques du secteur. Tout d'abord, ONTAP est le stockage le plus sécurisé de la planète et a obtenu la validation CSfC qui permet le stockage de données secrètes et top secrètes au repos au niveau des couches matérielles et logicielles. Plus d'informations sur"Le CSfC peut être trouvé ici" . De plus, ONTAP peut être isolé au niveau de la couche de stockage, le système de coffre-fort cybernétique contrôlant la réplication, ce qui permet de créer un espace d'air au sein du réseau de coffre-fort cybernétique.

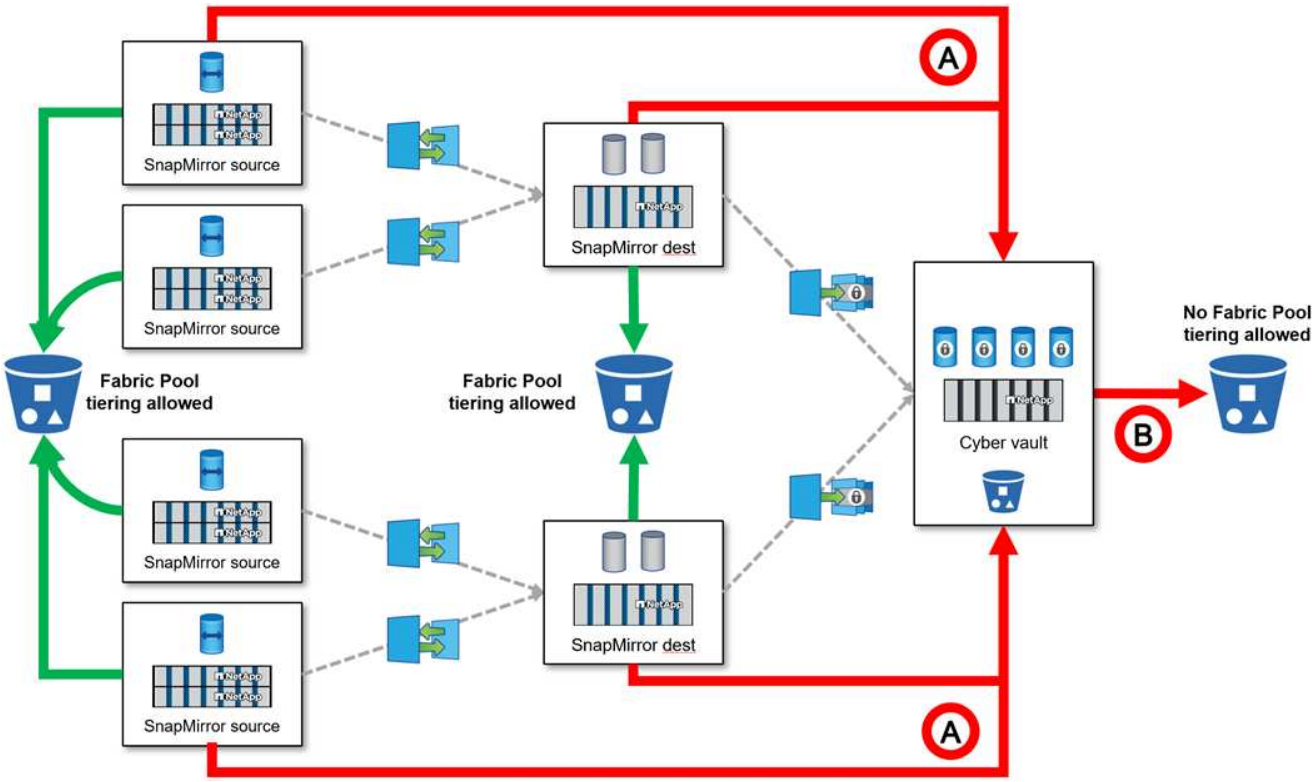
Un volume sur un coffre-fort cybernétique peut-il utiliser ONTAP Fabric Pool ?

Non, un volume de coffre-fort cybernétique (destination SnapLock Compliance SnapMirror) ne peut pas être hiérarchisé à l'aide de Fabric Pool, quelle que soit la politique.



Il existe plusieurs scénarios dans lesquels le pool Fabric **ne peut pas** être utilisé avec un coffre-fort cybernétique.

1. Les niveaux froids de Fabric Pool **ne peuvent pas** utiliser un cluster de coffre-fort cybernétique. Cela est dû au fait que l'activation du protocole S3 invalide la nature sécurisée de l'architecture de référence du coffre-fort cybernétique. De plus, le bucket S3 utilisé pour le pool Fabric ne peut pas être protégé.
2. Les volumes de SnapLock Compliance sur le coffre-fort cybernétique **ne peuvent pas** être hiérarchisés vers un compartiment S3 car les données sont verrouillées dans le volume.



ONTAP S3 Worm est-il disponible sur un coffre-fort informatique ?

Non, S3 est un protocole d'accès aux données qui invalide la nature sécurisée de l'architecture de référence.

NetApp Cyber Vault fonctionne-t-il sur une personnalité ou un profil ONTAP différent ?

Non, c'est une architecture de référence. Les clients peuvent utiliser le"architecture de référence" et construire un coffre-fort cybernétique, ou peut utiliser le"Scripts PowerShell pour créer, renforcer et valider" un coffre-fort cybernétique.

Puis-je activer des protocoles de données tels que NFS, SMB et S3 dans un coffre-fort informatique ?

Par défaut, les protocoles de données doivent être désactivés sur le coffre-fort informatique pour le sécuriser. Cependant, des protocoles de données peuvent être activés sur le coffre-fort informatique pour accéder aux données à des fins de récupération ou en cas de besoin. Cela doit être fait de manière temporaire et désactivé une fois la récupération terminée.

Pouvez-vous convertir un environnement SnapVault existant en un coffre-fort numérique ou devez-vous tout réensemencer ?

Oui. On pourrait prendre un système qui est une destination SnapMirror (avec une politique de coffre-fort), désactiver les protocoles de données, renforcer le système selon le"Guide de durcissement ONTAP" , isolez-le dans un emplacement sécurisé et suivez les autres procédures de l'architecture de référence pour en faire un coffre-fort cybernétique sans avoir à réensemencer la destination.

Vous avez des questions supplémentaires ? Veuillez envoyer un e-mail à ng-cyber-vault@netapp.com avec vos questions ! Nous répondrons et ajouterons vos questions à la FAQ.

Ressources du coffre-fort cybernétique

Pour en savoir plus sur les informations décrites dans ces informations sur le coffre-fort informatique, reportez-vous aux informations supplémentaires et aux concepts de sécurité suivants.

- "Coffre-fort cybernétique NetApp : résumé des solutions de protection des données multicouches"
- "NetApp obtient la note AAA pour sa première solution de détection de ransomwares intégrée basée sur l'IA"
- "Améliorez la cyber-résilience avec le stockage le plus sécurisé de la planète"
- "Guide de renforcement de la sécurité ONTAP"
- "NetApp Zero Trust"
- "Cyber-résilience de NetApp"
- "Protection des données NetApp"
- "Présentation du peering de cluster et de SVM avec la CLI"
- "Archivage SnapVault"

- "Configurer, analyser, script cron"

Création, renforcement et validation d’un coffre-fort cybernétique ONTAP avec PowerShell

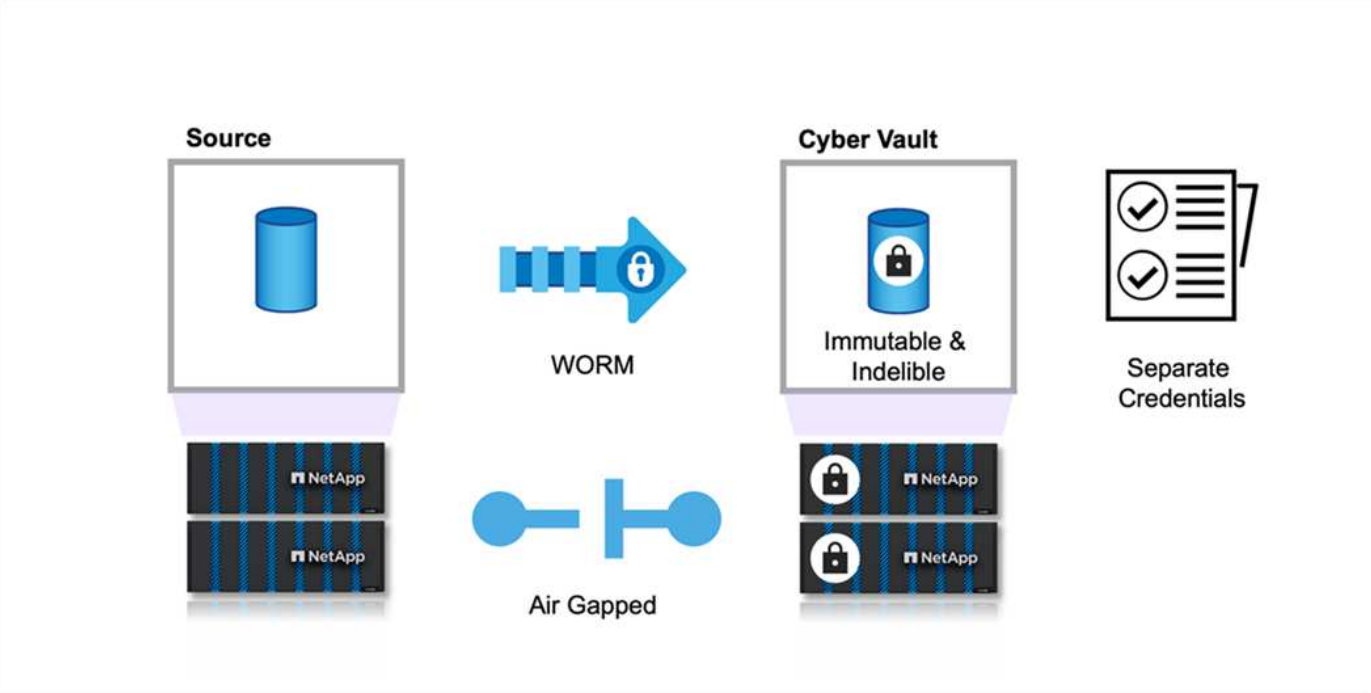
Présentation du coffre-fort cybernétique ONTAP avec PowerShell

Dans le paysage numérique actuel, la protection des données critiques d’une organisation n’est pas seulement une bonne pratique : c’est un impératif commercial. Les cybermenaces évoluent à un rythme sans précédent et les mesures traditionnelles de protection des données ne suffisent plus à assurer la sécurité des informations sensibles. C’est là qu’un coffre-fort informatique entre en jeu. La solution de pointe basée sur ONTAP de NetApp combine des techniques avancées d’espacement d’air avec des mesures robustes de protection des données pour créer une barrière impénétrable contre les cybermenaces. En isolant les données les plus précieuses grâce à une technologie de renforcement sécurisée, un coffre-fort informatique minimise la surface d’attaque afin que les données les plus critiques restent confidentielles, intactes et facilement disponibles en cas de besoin.

Un coffre-fort informatique est une installation de stockage sécurisée composée de plusieurs couches de protection, telles que des pare-feu, des réseaux et du stockage. Ces composants protègent les données de récupération vitales nécessaires aux opérations commerciales cruciales. Les composants du coffre-fort cybernétique se synchronisent régulièrement avec les données de production essentielles en fonction de la politique du coffre-fort, mais restent autrement inaccessibles. Cette configuration isolée et déconnectée garantit qu’en cas de cyberattaque compromettant l’environnement de production, une récupération fiable et définitive peut être facilement effectuée à partir du coffre-fort cybernétique.

NetApp permet de créer facilement un espace d’air pour le coffre-fort cybernétique en configurant le réseau, en désactivant les LIF, en mettant à jour les règles de pare-feu et en isolant le système des réseaux externes et d’Internet. Cette approche robuste déconnecte efficacement le système des réseaux externes et d’Internet, offrant une protection inégalée contre les cyberattaques à distance et les tentatives d’accès non autorisées, rendant le système immunisé contre les menaces et les intrusions basées sur le réseau.

En combinant cela avec la protection de SnapLock Compliance , les données ne peuvent pas être modifiées ou supprimées, même par les administrateurs ONTAP ou le support NetApp . SnapLock est régulièrement audité par rapport aux réglementations SEC et FINRA, garantissant que la résilience des données répond à ces réglementations strictes WORM et de conservation des données du secteur bancaire. NetApp est le seul stockage d’entreprise validé par la NSA CSfC pour stocker des données top secrètes.



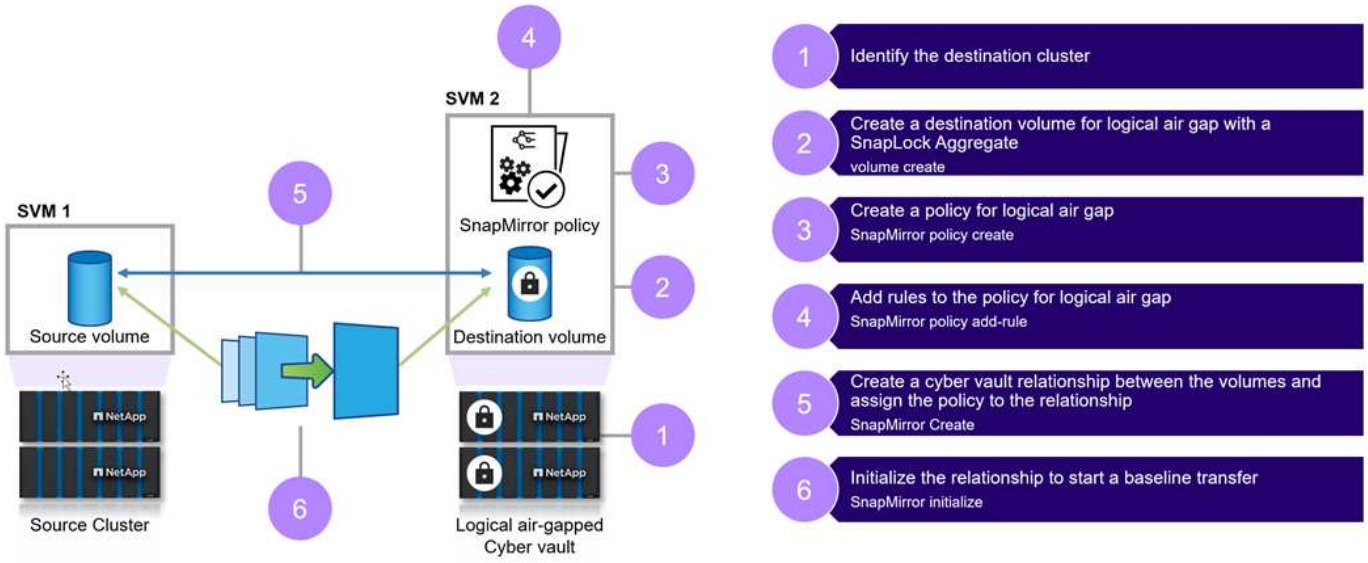
Ce document décrit la configuration automatisée du coffre-fort cybernétique de NetApp pour le stockage ONTAP sur site vers un autre stockage ONTAP désigné avec des instantanés immuables ajoutant une couche de protection supplémentaire contre les cyberattaques croissantes pour une récupération rapide. Dans le cadre de cette architecture, l'ensemble de la configuration est appliqué conformément aux meilleures pratiques ONTAP . La dernière section contient des instructions pour effectuer une récupération en cas d'attaque.

> La même solution est applicable pour créer le coffre-fort cybernétique désigné dans AWS à l'aide de FSx ONTAP.

Étapes de haut niveau pour créer un coffre-fort cybernétique ONTAP

- Créer une relation de peering
  - Le site de production utilisant le stockage ONTAP est couplé au stockage ONTAP du coffre-fort cybernétique désigné
- Créer un volume de SnapLock Compliance
- Configurer la relation et la règle SnapMirror pour définir l'étiquette
  - La relation SnapMirror et les planifications appropriées sont configurées
- Définir les rétentions avant de lancer le transfert SnapMirror (coffre-fort)
  - Le verrouillage de rétention est appliqué aux données copiées, ce qui empêche en outre toute tentative d'intrusion ou de défaillance des données. Grâce à cela, les données ne peuvent pas être supprimées avant l'expiration de la période de conservation.
  - Les organisations peuvent conserver ces données pendant quelques semaines/mois en fonction de leurs besoins.
- Initialiser la relation SnapMirror en fonction des étiquettes
  - L'amorçage initial et le transfert incrémentiel permanent se produisent en fonction de la planification SnapMirror
  - Les données sont protégées (immuables et indélébiles) grâce à la conformité SnapLock et sont disponibles pour la récupération.

- Mettre en œuvre des contrôles stricts de transfert de données
  - Le coffre-fort Cyber est déverrouillé pendant une période limitée avec les données du site de production et est synchronisé avec les données du coffre-fort. Une fois le transfert terminé, la connexion est déconnectée, fermée et à nouveau verrouillée
- Récupération rapide
  - Si le primaire est affecté sur le site de production, les données du coffre-fort informatique sont récupérées en toute sécurité vers la production d'origine ou vers un autre environnement choisi.



Composants de la solution

NetApp ONTAP exécutant 9.15.1 sur les clusters source et de destination.

ONTAP One : la licence tout-en-un de NetApp ONTAP.

Fonctionnalités utilisées à partir de la licence ONTAP One :

- SnapLock Compliance
- SnapMirror
- Vérification multi-administrateur
- Toutes les capacités de renforcement exposées par ONTAP
- Identifiants RBAC distincts pour le coffre-fort numérique

> Toutes les baies physiques unifiées ONTAP peuvent être utilisées pour un coffre-fort cybernétique. Cependant, les systèmes flash basés sur la capacité de la série C AFF et les systèmes flash hybrides FAS sont les plates-formes idéales les plus rentables à cette fin. Veuillez consulter le"Dimensionnement du coffre-fort cybernétique ONTAP" pour obtenir des conseils sur les tailles.

Création d'un coffre-fort cybernétique ONTAP avec PowerShell

Les sauvegardes par espacement d'air qui utilisent des méthodes traditionnelles impliquent la création d'espace et la séparation physique des supports primaire et

secondaire. En déplaçant les médias hors site et/ou en coupant la connectivité, les mauvais acteurs n'ont pas accès aux données. Cela protège les données mais peut entraîner des temps de récupération plus lents. Avec SnapLock Compliance, la séparation physique n'est pas requise. SnapLock Compliance protège les copies instantanées en lecture seule, à un instant T, des instantanés, ce qui permet d'obtenir des données rapidement accessibles, à l'abri de la suppression ou indélébiles, et à l'abri de toute modification ou immuables.

Prérequis

Avant de commencer les étapes de la section suivante de ce document, assurez-vous que les conditions préalables suivantes sont remplies :

- Le cluster source doit exécuter ONTAP 9 ou une version ultérieure.
- Les agrégats source et de destination doivent être de 64 bits.
- Les clusters source et de destination doivent être appairés.
- Les SVM source et de destination doivent être appairées.
- Assurez-vous que le chiffrement de l'appairage de cluster est activé.

La configuration des transferts de données vers un coffre-fort cybernétique ONTAP nécessite plusieurs étapes. Sur le volume principal, configurez une stratégie de snapshot qui spécifie les copies à créer et quand les créer en utilisant des planifications appropriées et attribuez des étiquettes pour spécifier les copies qui doivent être transférées par SnapVault. Au niveau secondaire, une politique SnapMirror doit être créée qui spécifie les étiquettes des copies Snapshot à transférer et le nombre de ces copies qui doivent être conservées dans le coffre-fort cybernétique. Après avoir configuré ces stratégies, créez la relation SnapVault et établissez un calendrier de transfert.

Ce document suppose que le stockage principal et le coffre-fort cybernétique ONTAP désigné sont déjà configurés et installés.

Le cluster de coffres-forts cybernétiques peut se trouver dans le même centre de données ou dans un centre de données différent de celui des données sources.

Étapes pour créer un coffre-fort numérique ONTAP

1. Utilisez l'interface de ligne de commande ONTAP ou le gestionnaire système pour initialiser l'horloge de conformité.
2. Créez un volume de protection des données avec la conformité SnapLock activée.
3. Utilisez la commande SnapMirror create pour créer des relations de protection des données SnapVault .
4. Définissez la période de conservation de SnapLock Compliance par défaut pour le volume de destination.

> La rétention par défaut est « Définie au minimum ». Un volume SnapLock qui est une destination de coffre-fort dispose d'une période de rétention par défaut qui lui est attribuée. La valeur de cette période est initialement fixée à un minimum de 0 an et à un maximum de 100 ans (à partir de ONTAP 9.10.1. Pour les versions antérieures ONTAP , la valeur est comprise entre 0 et 70.) pour les volumes de SnapLock Compliance . Chaque copie NetApp Snapshot est initialement validée avec cette période de conservation par défaut. La période de conservation peut être prolongée ultérieurement, si nécessaire, mais jamais raccourcie. Pour plus d'informations, consultez la section "Aperçu de la durée de conservation des paramètres" .

Ce qui précède comprend les étapes manuelles. Les experts en sécurité conseillent d'automatiser le processus pour éviter la gestion manuelle qui introduit une grande marge d'erreur. Vous trouverez ci-dessous l'extrait de code qui automatise complètement les prérequis et la configuration de la conformité SnapLock et de l'initialisation de l'horloge.

Voici un exemple de code PowerShell pour initialiser l'horloge de conformité ONTAP .

```
function initializeSnapLockComplianceClock {
    try {
        $nodes = Get-NcNode

        $isInitialized = $false
        logMessage -message "Cheking if snaplock compliance clock is
initialized"
        foreach($node in $nodes) {
            $check = Get-NcSnaplockComplianceClock -Node $node.Node
            if ($check.SnaplockComplianceClockSpecified -eq "True") {
                $isInitialized = $true
            }
        }

        if ($isInitialized) {
            logMessage -message "SnapLock Compliance clock already
initialized" -type "SUCCESS"
        } else {
            logMessage -message "Initializing SnapLock compliance clock"
            foreach($node in $nodes) {
                Set-NcSnaplockComplianceClock -Node $node.Node
            }
            logMessage -message "Successfully initialized SnapLock
Compliance clock" -type "SUCCESS"
        }
    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

Voici un exemple de code PowerShell pour configurer un cyber-coffre-fort ONTAP .

```
function configureCyberVault {
    for($i = 0; $i -lt $DESTINATION_VOLUME_NAMES.Length; $i++) {
        try {
            # checking if the volume already exists and is of type
snaplock compliance
            logMessage -message "Checking if SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) already exists in vServer
$DESTINATION_VSERVER"
            $volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Volume
$DESTINATION_VOLUME_NAMES[$i] | Select-Object -Property Name, State,
TotalSize, Aggregate, Vserver, Snaplock | Where-Object { $_.Snaplock.Type
-eq "compliance" }
            if($volume) {
                $volume
                logMessage -message "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) already exists in vServer
$DESTINATION_VSERVER" -type "SUCCESS"
            } else {
                # Create SnapLock Compliance volume
                logMessage -message "Creating SnapLock Compliance volume:
$($DESTINATION_VOLUME_NAMES[$i])"
                New-NcVol -Name $DESTINATION_VOLUME_NAMES[$i] -Aggregate
$DESTINATION_AGGREGATE_NAMES[$i] -SnaplockType Compliance -Type DP -Size
$DESTINATION_VOLUME_SIZES[$i] -ErrorAction Stop | Select-Object -Property
Name, State, TotalSize, Aggregate, Vserver
                logMessage -message "Volume $($DESTINATION_VOLUME_NAMES[
$i]) created successfully" -type "SUCCESS"
            }

            # Set SnapLock volume attributes
            logMessage -message "Setting SnapLock volume attributes for
volume: $($DESTINATION_VOLUME_NAMES[$i])"
            Set-NcSnaplockVolAttr -Volume $DESTINATION_VOLUME_NAMES[$i]
-MinimumRetentionPeriod $SNAPLOCK_MIN_RETENTION -MaximumRetentionPeriod
$SNAPLOCK_MAX_RETENTION -ErrorAction Stop | Select-Object -Property Type,
MinimumRetentionPeriod, MaximumRetentionPeriod
            logMessage -message "SnapLock volume attributes set
successfully for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"

            # checking snapmirror relationship
            logMessage -message "Checking if SnapMirror relationship
exists between source volume $($SOURCE_VOLUME_NAMES[$i]) and destination
SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])"
            $snapmirror = Get-NcSnapmirror | Select-Object SourceCluster,
SourceLocation, DestinationCluster, DestinationLocation, Status,
```

```
MirrorState | Where-Object { $_.SourceCluster -eq
$SOURCE_ONTAP_CLUSTER_NAME -and $_.SourceLocation -eq "$($SOURCE_VSERVER)
:$($SOURCE_VOLUME_NAMES[$i])" -and $_.DestinationCluster -eq
$DESTINATION_ONTAP_CLUSTER_NAME -and $_.DestinationLocation -eq "
$($DESTINATION_VSERVER):$($DESTINATION_VOLUME_NAMES[$i])" -and ($_.Status
-eq "snapmirrored" -or $_.Status -eq "uninitialized") }
            if($snapmirror) {
                $snapmirror
                logMessage -message "SnapMirror relationship already
exists for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"
            } else {
                # Create SnapMirror relationship
                logMessage -message "Creating SnapMirror relationship for
volume: $($DESTINATION_VOLUME_NAMES[$i])"
                New-NcSnapmirror -SourceCluster $SOURCE_ONTAP_CLUSTER_NAME
-SourceVserver $SOURCE_VSERVER -SourceVolume $SOURCE_VOLUME_NAMES[$i]
-DestinationCluster $DESTINATION_ONTAP_CLUSTER_NAME -DestinationVserver
$DESTINATION_VSERVER -DestinationVolume $DESTINATION_VOLUME_NAMES[$i]
-Policy $SNAPMIRROR_PROTECTION_POLICY -Schedule $SNAPMIRROR_SCHEDULE
-ErrorAction Stop | Select-Object -Property SourceCluster, SourceLocation,
DestinationCluster, DestinationLocation, Status, Policy, Schedule
                logMessage -message "SnapMirror relationship created
successfully for volume: $($DESTINATION_VOLUME_NAMES[$i])" -type "SUCCESS"
            }

        } catch {
            handleError -errorMessage $_.Exception.Message
        }
    }
}
```

1. Une fois les étapes ci-dessus terminées, le coffre-fort cybernétique isolé utilisant SnapLock Compliance et SnapVault est prêt.

Avant de transférer les données instantanées vers le coffre-fort cybernétique, la relation SnapVault doit être initialisée. Cependant, avant cela, il est nécessaire de procéder à un renforcement de la sécurité pour sécuriser le coffre-fort.

Renforcement du coffre-fort cybernétique ONTAP avec PowerShell

Le coffre-fort cybernétique ONTAP offre une meilleure résilience contre les cyberattaques par rapport aux solutions traditionnelles. Lors de la conception d'une architecture visant à améliorer la sécurité, il est essentiel d'envisager des mesures visant à réduire la surface d'attaque. Cela peut être réalisé grâce à diverses méthodes telles que la mise en œuvre de politiques de mot de passe renforcées, l'activation du RBAC, le verrouillage des comptes d'utilisateurs par défaut, la configuration de pare-feu et l'utilisation de flux d'approbation pour toute modification du système de coffre-fort. De plus, restreindre les

protocoles d'accès au réseau à partir d'une adresse IP spécifique peut aider à limiter les vulnérabilités potentielles.

ONTAP fournit un ensemble de contrôles qui permettent de renforcer le stockage ONTAP . Utilisez le"paramètres de guidage et de configuration pour ONTAP" pour aider l'organisation à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité des systèmes d'information.

Renforcement des meilleures pratiques

Étapes manuelles

1. Créez un utilisateur désigné avec un rôle administratif prédéfini et personnalisé.
2. Créez un nouvel espace IP pour isoler le trafic réseau.
3. Créez une nouvelle SVM résidant dans le nouvel espace IP.
4. Assurez-vous que les politiques de routage du pare-feu sont correctement configurées et que toutes les règles sont régulièrement auditées et mises à jour selon les besoins.

ONTAP CLI ou via un script d'automatisation

1. Protégez l'administration avec la vérification multi-administrateur (MFA)
2. Activer le cryptage des données standard « en vol » entre les clusters.
3. Sécurisez SSH avec un chiffrement puissant et appliquez des mots de passe sécurisés.
4. Activer le FIPS global.
5. Telnet et Remote Shell (RSH) doivent être désactivés.
6. Verrouiller le compte administrateur par défaut.
7. Désactivez les LIF de données et sécurisez les points d'accès à distance.
8. Désactivez et supprimez les protocoles et services inutilisés ou superflus.
9. Crypter le trafic réseau.
10. Utilisez le principe du moindre privilège lors de la configuration des rôles de superutilisateur et d'administrateur.
11. Restreignez HTTPS et SSH à partir d'une adresse IP spécifique à l'aide de l'option IP autorisée.
12. Mettez en pause et reprenez la réplication en fonction du calendrier de transfert.

Les puces 1 à 4 nécessitent une intervention manuelle comme la désignation d'un réseau isolé, la séparation de l'espace IP, etc. et doivent être effectuées au préalable. Des informations détaillées pour configurer le durcissement peuvent être trouvées dans le"Guide de renforcement de la sécurité ONTAP" . Le reste peut être facilement automatisé pour faciliter le déploiement et la surveillance. L'objectif de cette approche orchestrée est de fournir un mécanisme permettant d'automatiser les étapes de renforcement pour assurer la pérennité du contrôleur de coffre-fort. La période pendant laquelle le cyber-coffre-fort est ouvert est aussi courte que possible. SnapVault exploite la technologie incrémentielle permanente, qui déplacera uniquement les modifications depuis la dernière mise à jour dans le coffre-fort numérique, minimisant ainsi la durée pendant laquelle le coffre-fort numérique doit rester ouvert. Pour optimiser davantage le flux de travail, l'ouverture du coffre-fort informatique est coordonnée avec le calendrier de réplication pour garantir la plus petite fenêtre de connexion.

Voici un exemple de code PowerShell pour renforcer un contrôleur ONTAP .

```
function removeSvmDataProtocols {
    try {

        # checking NFS service is disabled
        logMessage -message "Checking if NFS service is disabled on
vServer $DESTINATION_VSERVER"
        $nfsService = Get-NcNfsService
        if($nfsService) {
            # Remove NFS
            logMessage -message "Removing NFS protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcNfsService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "NFS protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "NFS service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking CIFS/SMB server is disabled
        logMessage -message "Checking if CIFS/SMB server is disabled on
vServer $DESTINATION_VSERVER"
        $cifsServer = Get-NcCifsServer
        if($cifsServer) {
            # Remove SMB/CIFS
            logMessage -message "Removing SMB/CIFS protocol on vServer :
$DESTINATION_VSERVER"
            $domainAdministratorUsername = Read-Host -Prompt "Enter Domain
administrator username"
            $domainAdministratorPassword = Read-Host -Prompt "Enter Domain
administrator password" -AsSecureString
            $plainPassword = [Runtime.InteropServices.Marshal
]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($
domainAdministratorPassword))
            Remove-NcCifsServer -VserverContext $DESTINATION_VSERVER
-AdminUsername $domainAdministratorUsername -AdminPassword $plainPassword
-Confirm:$false -ErrorAction Stop
            logMessage -message "SMB/CIFS protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "CIFS/SMB server is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking iSCSI service is disabled
```

```
        logMessage -message "Checking if iSCSI service is disabled on
vServer $DESTINATION_VSERVER"
        $iscsiService = Get-NcIscsiService
        if($iscsiService) {
            # Remove iSCSI
            logMessage -message "Removing iSCSI protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcIscsiService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "iSCSI protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "iSCSI service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking FCP service is disabled
        logMessage -message "Checking if FCP service is disabled on
vServer $DESTINATION_VSERVER"
        $fcpService = Get-NcFcpService
        if($fcpService) {
            # Remove FCP
            logMessage -message "Removing FC protocol on vServer :
$DESTINATION_VSERVER"
            Remove-NcFcpService -VserverContext $DESTINATION_VSERVER
-Confirm:$false
            logMessage -message "FC protocol removed on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"
        } else {
            logMessage -message "FCP service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function disableSvmDataLifs {
    try {
        logMessage -message "Finding all data lifs on vServer :
$DESTINATION_VSERVER"
        $dataLifs = Get-NcNetInterface -Vserver $DESTINATION_VSERVER |
Where-Object { $_.Role -contains "data_core" }
        $dataLifs | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address
```

```
        logMessage -message "Disabling all data lifs on vServer :
$DESTINATION_VSERVER"
        # Disable the filtered data LIFs
        foreach ($lif in $dataLifs) {
            $disableLif = Set-NcNetInterface -Vserver $DESTINATION_VSERVER
-Name $lif.InterfaceName -AdministrativeStatus down -ErrorAction Stop
            $disableLif | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address
        }
        logMessage -message "Disabled all data lifs on vServer :
$DESTINATION_VSERVER" -type "SUCCESS"

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}

function configureMultiAdminApproval {
    try {

        # check if multi admin verification is enabled
        logMessage -message "Checking if multi-admin verification is
enabled"
        $maaConfig = Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "set -privilege advanced;
security multi-admin-verify show"
        if ($maaConfig.Value -match "Enabled" -and $maaConfig.Value -match
"true") {
            $maaConfig
            logMessage -message "Multi-admin verification is configured
and enabled" -type "SUCCESS"
        } else {
            logMessage -message "Setting Multi-admin verification rules"
            # Define the commands to be restricted
            $rules = @(
                "cluster peer delete",
                "vserver peer delete",
                "volume snapshot policy modify",
                "volume snapshot rename",
                "vserver audit modify",
                "vserver audit delete",
                "vserver audit disable"
            )
            foreach($rule in $rules) {
                Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
```

```
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
rule create -operation `"$rule`""
            }

            logMessage -message "Creating multi admin verification group
for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP, Group name :
$MULTI_ADMIN_APPROVAL_GROUP_NAME, Users : $MULTI_ADMIN_APPROVAL_USERS,
Email : $MULTI_ADMIN_APPROVAL_EMAIL"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
approval-group create -name $MULTI_ADMIN_APPROVAL_GROUP_NAME -approvers
$MULTI_ADMIN_APPROVAL_USERS -email `"$MULTI_ADMIN_APPROVAL_EMAIL`""
            logMessage -message "Created multi admin verification group
for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP, Group name :
$MULTI_ADMIN_APPROVAL_GROUP_NAME, Users : $MULTI_ADMIN_APPROVAL_USERS,
Email : $MULTI_ADMIN_APPROVAL_EMAIL" -type "SUCCESS"

            logMessage -message "Enabling multi admin verification group
$MULTI_ADMIN_APPROVAL_GROUP_NAME"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -approval-groups $MULTI_ADMIN_APPROVAL_GROUP_NAME -required
-approvers 1 -enabled true"
            logMessage -message "Enabled multi admin verification group
$MULTI_ADMIN_APPROVAL_GROUP_NAME" -type "SUCCESS"

            logMessage -message "Enabling multi admin verification for
ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -enabled true"
            logMessage -message "Successfully enabled multi admin
verification for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP" -type
"SUCCESS"

            logMessage -message "Enabling multi admin verification for
ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP"
            Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "security multi-admin-verify
modify -enabled true"
            logMessage -message "Successfully enabled multi admin
verification for ONTAP Cluster $DESTINATION_ONTAP_CLUSTER_MGMT_IP" -type
"SUCCESS"
        }

    } catch {
```

```
        handleError -errorMessage $_.Exception.Message
    }
}

function additionalSecurityHardening {
    try {
        $command = "set -privilege advanced -confirmations off;security
protocol modify -application telnet -enabled false;"
        logMessage -message "Disabling Telnet"
        Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential
$DESTINATION_ONTAP_CREDS -Command $command
        logMessage -message "Disabled Telnet" -type "SUCCESS"

        #$command = "set -privilege advanced -confirmations off;security
config modify -interface SSL -is-fips-enabled true;"
        #logMessage -message "Enabling Global FIPS"
        ##Invoke-SSHCommand -SessionId $sshSession.SessionId -Command
$command -ErrorAction Stop
        #logMessage -message "Enabled Global FIPS" -type "SUCCESS"

        $command = "set -privilege advanced -confirmations off;network
interface service-policy modify-service -vserver cluster2 -policy default-
management -service management-https -allowed-addresses $ALLOWED_IPS;"
        logMessage -message "Restricting IP addresses $ALLOWED_IPS for
Cluster management HTTPS"
        Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential
$DESTINATION_ONTAP_CREDS -Command $command
        logMessage -message "Successfully restricted IP addresses
$ALLOWED_IPS for Cluster management HTTPS" -type "SUCCESS"

        #logMessage -message "Checking if audit logs volume audit_logs
exists"
        #$volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Name
audit_logs -ErrorAction Stop

        #if($volume) {
        #    logMessage -message "Volume audit_logs already exists!
Skipping creation"
        #} else {
        #    # Create audit logs volume
        #    logMessage -message "Creating audit logs volume : audit_logs"
        #    New-NcVol -Name audit_logs -Aggregate
$DESTINATION_AGGREGATE_NAME -Size 5g -ErrorAction Stop | Select-Object
-Property Name, State, TotalSize, Aggregate, Vserver
        #    logMessage -message "Volume audit_logs created successfully"
-type "SUCCESS"
```

```
        #}

        ## Mount audit logs volume to path /vol/audit_logs
        #logMessage -message "Creating junction path for volume audit_logs
at path /vol/audit_logs for vServer $DESTINATION_VSERVER"
        #Mount-NcVol -VserverContext $DESTINATION_VSERVER -Name audit_logs
-JunctionPath /audit_logs | Select-Object -Property Name, -JunctionPath
        #logMessage -message "Created junction path for volume audit_logs
at path /vol/audit_logs for vServer $DESTINATION_VSERVER" -type "SUCCESS"

        #logMessage -message "Enabling audit logging for vServer
$DESTINATION_VSERVER at path /vol/audit_logs"
        #$command = "set -privilege advanced -confirmations off;vserver
audit create -vserver $DESTINATION_VSERVER -destination /audit_logs
-format xml;"
        #Invoke-SSHCommand -SessionI  $sshSession.SessionId -Command
$command -ErrorAction Stop
        #logMessage -message "Successfully enabled audit logging for
vServer $DESTINATION_VSERVER at path /vol/audit_logs"

    } catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

Validation du coffre-fort cybernétique ONTAP avec PowerShell

Un coffre-fort informatique robuste doit être capable de résister à une attaque sophistiquée, même lorsque l'attaquant dispose d'informations d'identification pour accéder à l'environnement avec des privilèges élevés.

Une fois les règles en place, une tentative (en supposant que l'attaquant ait réussi à entrer) de supprimer un instantané côté coffre-fort échouera. Il en va de même pour tous les paramètres de durcissement en appliquant les restrictions nécessaires et en protégeant le système.

Exemple de code PowerShell pour valider la configuration selon un calendrier.

```
function analyze {

    for($i = 0; $i -lt $DESTINATION_VOLUME_NAMES.Length; $i++) {
        try {
            # checking if volume is of type SnapLock Compliance
            logMessage -message "Checking if SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) exists in vServer $DESTINATION_VSERVER"
            $volume = Get-NcVol -Vserver $DESTINATION_VSERVER -Volume
$DESTINATION_VOLUME_NAMES[$i] | Select-Object -Property Name, State,
```

```
TotalSize, Aggregate, Vserver, Snaplock | Where-Object { $_.Snaplock.Type
-eq "compliance" }
            if($volume) {
                $volume
                logMessage -message "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) exists in vServer $DESTINATION_VSERVER"
-type "SUCCESS"
            } else {
                handleError -errorMessage "SnapLock Compliance volume
$($DESTINATION_VOLUME_NAMES[$i]) does not exist in vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to create and configure the cyber vault SnapLock Compliance
volume"
            }

            # checking SnapMirror relationship
            logMessage -message "Checking if SnapMirror relationship
exists between source volume $($SOURCE_VOLUME_NAMES[$i]) and destination
SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])"
            $snapmirror = Get-NcSnapmirror | Select-Object SourceCluster,
SourceLocation, DestinationCluster, DestinationLocation, Status,
MirrorState | Where-Object { $_.SourceCluster -eq
$SOURCE_ONTAP_CLUSTER_NAME -and $_.SourceLocation -eq "$($SOURCE_VSERVER)
:$($SOURCE_VOLUME_NAMES[$i])" -and $_.DestinationCluster -eq
$DESTINATION_ONTAP_CLUSTER_NAME -and $_.DestinationLocation -eq "
$($DESTINATION_VSERVER):$($DESTINATION_VOLUME_NAMES[$i])" -and $_.Status
-eq "snapmirrored" }
            if($snapmirror) {
                $snapmirror
                logMessage -message "SnapMirror relationship successfully
configured and in healthy state" -type "SUCCESS"
            } else {
                handleError -errorMessage "SnapMirror relationship does
not exist between the source volume $($SOURCE_VOLUME_NAMES[$i]) and
destination SnapLock Compliance volume $($DESTINATION_VOLUME_NAMES[$i])
(or) SnapMirror status uninitialized/unhealthy. Recommendation: Run the
script with SCRIPT_MODE `"configure`" to create and configure the cyber
vault SnapLock Compliance volume and configure the SnapMirror
relationship"
            }
        }
        catch {
            handleError -errorMessage $_.Exception.Message
        }
    }
```

```
    try {

        # checking NFS service is disabled
        logMessage -message "Checking if NFS service is disabled on
vServer $DESTINATION_VSERVER"
        $nfsService = Get-NcNfsService
        if($nfsService) {
            handleError -errorMessage "NFS service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable NFS on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "NFS service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking CIFS/SMB server is disabled
        logMessage -message "Checking if CIFS/SMB server is disabled on
vServer $DESTINATION_VSERVER"
        $cifsServer = Get-NcCifsServer
        if($cifsServer) {
            handleError -errorMessage "CIFS/SMB server running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable CIFS/SMB on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "CIFS/SMB server is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking iSCSI service is disabled
        logMessage -message "Checking if iSCSI service is disabled on
vServer $DESTINATION_VSERVER"
        $iscsiService = Get-NcIscsiService
        if($iscsiService) {
            handleError -errorMessage "iSCSI service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable iSCSI on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "iSCSI service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking FCP service is disabled
        logMessage -message "Checking if FCP service is disabled on
vServer $DESTINATION_VSERVER"
        $fcpService = Get-NcFcpService
        if($fcpService) {
```

```
            handleError -errorMessage "FCP service running on vServer
$DESTINATION_VSERVER. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to disable FCP on vServer $DESTINATION_VSERVER"
        } else {
            logMessage -message "FCP service is disabled on vServer
$DESTINATION_VSERVER" -type "SUCCESS"
        }

        # checking if all data lifs are disabled on vServer
        logMessage -message "Finding all data lifs on vServer :
$DESTINATION_VSERVER"
        $dataLifs = Get-NcNetInterface -Vserver $DESTINATION_VSERVER |
Where-Object { $_.Role -contains "data_core" }
        $dataLifs | Select-Object -Property InterfaceName, OpStatus,
DataProtocols, Vserver, Address

        logMessage -message "Checking if all data lifs are disabled for
vServer : $DESTINATION_VSERVER"
        # Disable the filtered data LIFs
        foreach ($lif in $dataLifs) {
            $checkLif = Get-NcNetInterface -Vserver $DESTINATION_VSERVER
-Name $lif.InterfaceName | Where-Object { $_.OpStatus -eq "down" }
            if($checkLif) {
                logMessage -message "Data lif $($lif.InterfaceName)
disabled for vServer $DESTINATION_VSERVER" -type "SUCCESS"
            } else {
                handleError -errorMessage "Data lif $($lif.InterfaceName)
is enabled. Recommendation: Run the script with SCRIPT_MODE `"configure`"
to disable Data lifs for vServer $DESTINATION_VSERVER"
            }
        }
        logMessage -message "All data lifs are disabled for vServer :
$DESTINATION_VSERVER" -type "SUCCESS"

        # check if multi-admin verification is enabled
        logMessage -message "Checking if multi-admin verification is
enabled"
        $maaConfig = Invoke-NcSsh -Name $DESTINATION_ONTAP_CLUSTER_MGMT_IP
-Credential $DESTINATION_ONTAP_CREDS -Command "set -privilege advanced;
security multi-admin-verify show"
        if ($maaConfig.Value -match "Enabled" -and $maaConfig.Value -match
"true") {
            $maaConfig
            logMessage -message "Multi-admin verification is configured
and enabled" -type "SUCCESS"
        } else {
```

```
            handleError -errorMessage "Multi-admin verification is not
configured or not enabled. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to enable and configure Multi-admin verification"
        }

        # check if telnet is disabled
        logMessage -message "Checking if telnet is disabled"
        $telnetConfig = Invoke-NcSsh -Name
$DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential $DESTINATION_ONTAP_CREDS
-Command "set -privilege advanced; security protocol show -application
telnet"
        if ($telnetConfig.Value -match "enabled" -and $telnetConfig.Value
-match "false") {
            logMessage -message "Telnet is disabled" -type "SUCCESS"
        } else {
            handleError -errorMessage "Telnet is enabled. Recommendation:
Run the script with SCRIPT_MODE `"configure`" to disable telnet"
        }

        # check if network https is restricted to allowed IP addresses
        logMessage -message "Checking if HTTPS is restricted to allowed IP
addresses $ALLOWED_IPS"
        $networkServicePolicy = Invoke-NcSsh -Name
$DESTINATION_ONTAP_CLUSTER_MGMT_IP -Credential $DESTINATION_ONTAP_CREDS
-Command "set -privilege advanced; network interface service-policy show"
        if ($networkServicePolicy.Value -match "management-https:
$($ALLOWED_IPS)") {
            logMessage -message "HTTPS is restricted to allowed IP
addresses $ALLOWED_IPS" -type "SUCCESS"
        } else {
            handleError -errorMessage "HTTPS is not restricted to allowed
IP addresses $ALLOWED_IPS. Recommendation: Run the script with SCRIPT_MODE
`"configure`" to restrict allowed IP addresses for HTTPS management"
        }
    }
    catch {
        handleError -errorMessage $_.Exception.Message
    }
}
```

Cette capture d'écran montre qu'il n'y a aucune connexion sur le contrôleur de coffre-fort.

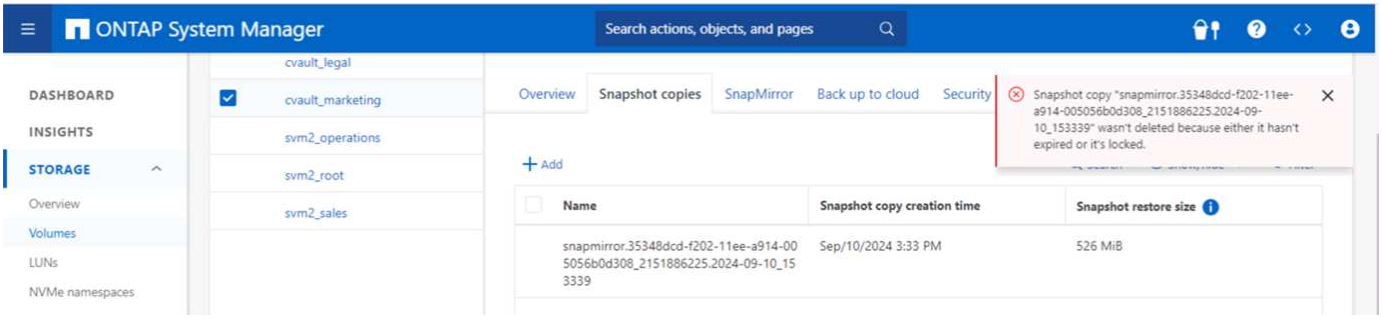
```
cluster2::> network connections  listening show
This table is currently empty.

cluster2::> network connections active show-services
This table is currently empty.

cluster2::> network connections active show-protocols
This table is currently empty.

cluster2::>
```

Cette capture d'écran montre qu'il n'est pas possible de falsifier les instantanés.



Pour valider et confirmer la fonctionnalité d'espacement d'air, suivez les étapes ci-dessous :

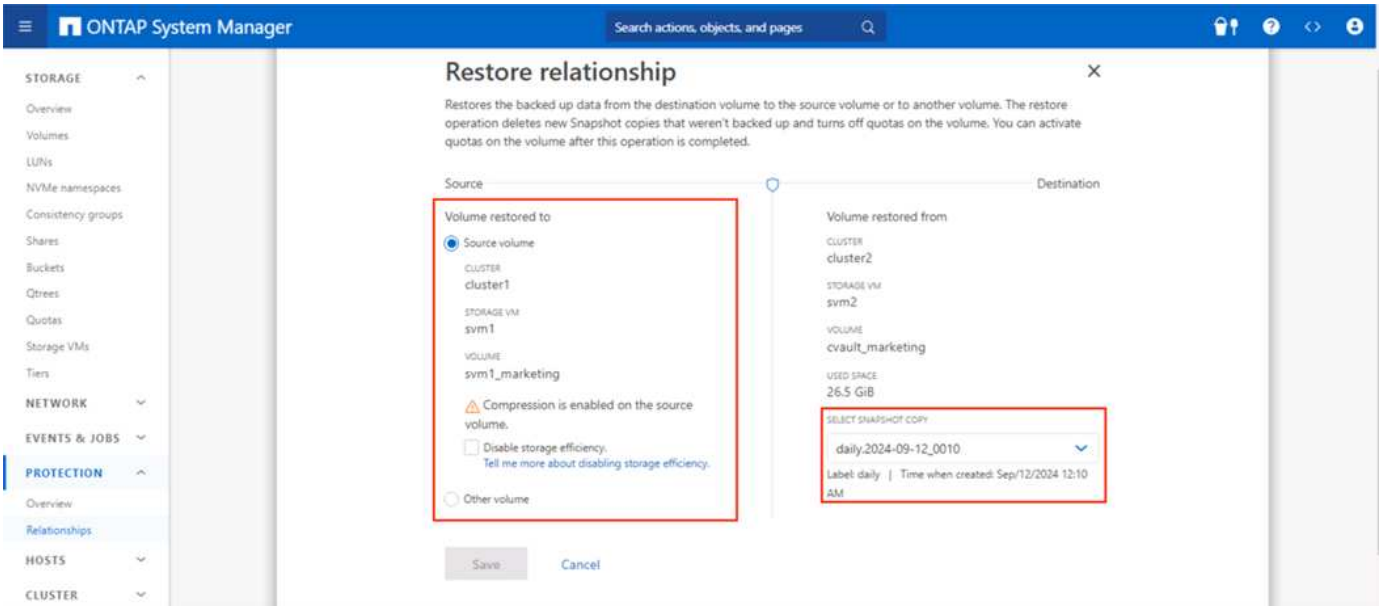
- Testez les capacités d'isolation du réseau et la possibilité de suspendre une connexion lorsque les données ne sont pas transférées.
- Vérifiez que l'interface de gestion n'est pas accessible à partir d'entités autres que les adresses IP autorisées.
- La vérification multi-administrateur est en place pour fournir une couche d'approbation supplémentaire.
- Valider la possibilité d'accéder via CLI et REST API
- À partir de la source, déclenchez une opération de transfert vers le coffre-fort et assurez-vous que la copie du coffre-fort ne peut pas être modifiée.
- Essayez de supprimer les copies instantanées immuables qui sont transférées vers le coffre-fort.
- Essayez de modifier la période de conservation en altérant l'horloge système.

Récupération de données du coffre-fort cybernétique ONTAP

Si des données sont détruites dans le centre de données de production, les données du coffre-fort informatique peuvent être récupérées en toute sécurité dans l'environnement choisi. Contrairement à une solution physiquement isolée, le coffre-fort cybernétique ONTAP isolé est construit à l'aide de fonctionnalités ONTAP natives telles que SnapLock Compliance et SnapMirror. Le résultat est un processus de récupération à la fois rapide et facile à exécuter.

En cas d'attaque par ransomware et de nécessité de récupération à partir du coffre-fort informatique, le processus de récupération est simple et facile car les copies instantanées hébergées dans le coffre-fort

informatique sont utilisées pour restaurer les données cryptées.



Si l'exigence est de fournir une méthode plus rapide pour remettre les données en ligne lorsque cela est nécessaire pour valider, isoler et analyser rapidement les données en vue de leur récupération. Cela peut être facilement réalisé en utilisant FlexClone avec l'option snaplock-type définie sur le type non-snaplock.

> À partir d' ONTAP 9.13.1, la restauration d'une copie Snapshot verrouillée sur le volume SnapLock de destination d'une relation de coffre SnapLock peut être instantanément restaurée en créant un FlexClone avec l'option snaplock-type définie sur « non-snaplock ». Lors de l'exécution de l'opération de création de clone de volume, spécifiez la copie Snapshot comme « parent-snapshot ». Plus d'informations sur la création d'un volume FlexClone avec un type SnapLock"ici."

> La mise en pratique des procédures de récupération à partir du coffre-fort informatique garantira que les étapes appropriées sont établies pour la connexion au coffre-fort informatique et la récupération des données. La planification et le test de la procédure sont essentiels pour toute récupération lors d'un événement de cyberattaque.

Considérations supplémentaires

Des considérations supplémentaires doivent être prises en compte lors de la conception et du déploiement d'un coffre-fort cybernétique basé sur ONTAP .

Considérations relatives au dimensionnement de la capacité

La quantité d'espace disque requise pour un volume de destination de coffre-fort cybernétique ONTAP dépend de divers facteurs, dont le plus important est le taux de variation des données dans le volume source. La planification de sauvegarde et la planification d'instantanés sur le volume de destination affectent toutes deux l'utilisation du disque sur le volume de destination, et le taux de changement sur le volume source n'est probablement pas constant. Il est judicieux de prévoir une capacité de stockage supplémentaire au-delà de celle requise pour s'adapter aux changements futurs du comportement de l'utilisateur final ou de l'application.

Le dimensionnement d'une relation pour 1 mois de rétention dans ONTAP nécessite de calculer les besoins de stockage en fonction de plusieurs facteurs, notamment la taille de l'ensemble de données principal, le taux de

modification des données (taux de modification quotidien) et les économies de déduplication et de compression (le cas échéant).

Voici l'approche étape par étape :

La première étape consiste à connaître la taille du ou des volumes sources que vous protégez avec le coffre-fort numérique. Il s'agit de la quantité de base de données qui sera initialement répliquée vers la destination du coffre-fort informatique. Ensuite, estimez le taux de variation quotidien de l'ensemble de données. Il s'agit du pourcentage de données qui change chaque jour. Il est essentiel de bien comprendre le caractère dynamique de vos données.

Par exemple:

- Taille du jeu de données principal = 5 To
- Taux de variation quotidien = 5 % (0,05)
- Efficacité de déduplication et de compression = 50 % (0,50)

Maintenant, passons en revue le calcul :

- Calculer le taux de variation des données quotidiennes :

  ```
  Changed data per day = 5000 * 5% = 250GB
  ```

- Calculez le total des données modifiées sur 30 jours :

  ```
  Total changed data in 30 days = 250 GB * 30 = 7.5TB
  ```

- Calculez le stockage total requis :

  ```
  TOTAL = 5TB + 7.5TB = 12.5TB
  ```

- Appliquer les économies de déduplication et de compression :

  ```
  EFFECTIVE = 12.5TB * 50% = 6.25TB
  ```

Résumé des besoins de stockage

- Sans efficacité : il faudrait **12,5 To** pour stocker 30 jours de données du coffre-fort informatique.
- Avec une efficacité de 50 % : il faudrait **6,25 To** de stockage après déduplication et compression.

> Les copies instantanées peuvent entraîner une surcharge supplémentaire en raison des métadonnées, mais celle-ci est généralement mineure.

> Si plusieurs sauvegardes sont effectuées par jour, ajustez le calcul en fonction du nombre de copies Snapshot effectuées chaque jour.

> Tenez compte de la croissance des données au fil du temps pour garantir que le dimensionnement est à l'épreuve du temps.

Impact sur les performances du primaire/de la source

Étant donné que le transfert de données est une opération d'extraction, l'impact sur les performances du stockage principal peut varier en fonction de la charge de travail, du volume de données et de la fréquence des sauvegardes. Cependant, l'impact global sur les performances du système principal est généralement modéré et gérable, car le transfert de données est conçu pour décharger les tâches de protection et de sauvegarde des données vers le système de stockage du coffre-fort informatique. Lors de la configuration initiale de la relation et de la première sauvegarde complète, une quantité importante de données est transférée du système principal vers le système de coffre-fort cybernétique (le volume de SnapLock Compliance). Cela peut entraîner une augmentation du trafic réseau et de la charge d'E/S sur le système principal. Une fois la sauvegarde complète initiale terminée, ONTAP n'a plus qu'à suivre et transférer les blocs qui ont changé depuis la dernière sauvegarde. Cela entraîne une charge d'E/S beaucoup plus faible par rapport à la réplication initiale. Les mises à jour incrémentielles sont efficaces et ont un impact minimal sur les performances du stockage principal. Le processus de coffre-fort s'exécute en arrière-plan, ce qui réduit les risques d'interférence avec les charges de travail de production du système principal.

- S'assurer que le système de stockage dispose de suffisamment de ressources (CPU, mémoire et IOPS) pour gérer la charge supplémentaire atténue l'impact sur les performances.

Configurer, analyser, script cron

NetApp a créé un"script unique pouvant être téléchargé" et utilisé pour configurer, vérifier et planifier les relations du coffre-fort cybernétique.

Ce que fait ce script

- Appairage de cluster
- Appairage SVM
- Création de volume DP
- Relation et initialisation SnapMirror
- Renforcer le système ONTAP utilisé pour le coffre-fort informatique
- Mettre en pause et reprendre la relation en fonction du calendrier de transfert
- Validez périodiquement les paramètres de sécurité et générez un rapport indiquant toute anomalie

Comment utiliser ce script

"Télécharger le script"et pour utiliser le script, suivez simplement les étapes ci-dessous :

- Lancez Windows PowerShell en tant qu'administrateur.
- Accédez au répertoire contenant le script.
- Exécutez le script en utilisant `.\` syntaxe avec les paramètres requis

> Veuillez vous assurer que toutes les informations sont saisies. Lors de la première exécution (mode de configuration), il demandera des informations d'identification pour le système de production et le nouveau système de coffre-fort cybernétique. Après cela, il créera les peerings SVM (s'ils n'existent pas), les volumes et le SnapMirror entre le système et les initialisera.

> Le mode Cron peut être utilisé pour planifier la mise en veille et la reprise du transfert de données.

Modes de fonctionnement

Le script d'automatisation fournit 3 modes d'exécution - `configure` , `analyze` et `cron` .

```
if($SCRIPT_MODE -eq "configure") {
        configure
    } elseif ($SCRIPT_MODE -eq "analyze") {
        analyze
    } elseif ($SCRIPT_MODE -eq "cron") {
        runCron
    }
```

- Configurer - Effectue les contrôles de validation et configure le système comme étant isolé.
- Analyser - Fonction de surveillance et de reporting automatisée pour envoyer des informations aux groupes de surveillance pour les anomalies et les activités suspectes afin de garantir que les configurations ne sont pas dérivées.
- Cron - Pour activer l'infrastructure déconnectée, le mode cron automatise la désactivation du LIF et suspend la relation de transfert.

Le transfert des données dans ces volumes sélectionnés prendra du temps en fonction des performances du système et de la quantité de données.

```
./script.ps1 -SOURCE_ONTAP_CLUSTER_MGMT_IP "172.21.166.157"
-SOURCE_ONTAP_CLUSTER_NAME "NTAP915_Src" -SOURCE_VSERVER "svm_NFS"
-SOURCE_VOLUME_NAME "Src_RP_Vol01" -DESTINATION_ONTAP_CLUSTER_MGMT_IP
"172.21.166.159" -DESTINATION_ONTAP_CLUSTER_NAME "NTAP915_Destn"
-DESTINATION_VSERVER "svm_nim_nfs" -DESTINATION_AGGREGATE_NAME
"NTAP915_Destn_01_VM_DISK_1" -DESTINATION_VOLUME_NAME "Dst_RP_Vol01_Vault"
-DESTINATION_VOLUME_SIZE "5g" -SNAPLOCK_MIN_RETENTION "15minutes"
-SNAPLOCK_MAX_RETENTION "30minutes" -SNAPMIRROR_PROTECTION_POLICY
"XDPDefault" -SNAPMIRROR_SCHEDULE "5min" -DESTINATION_CLUSTER_USERNAME
"admin" -DESTINATION_CLUSTER_PASSWORD "PASSWORD123"
```

Conclusion sur la solution PowerShell du coffre-fort cybernétique ONTAP

En exploitant l'espace aérien avec des méthodologies de renforcement robustes fournies par ONTAP, NetApp vous permet de créer un environnement de stockage sécurisé et isolé, résilient face aux cybermenaces en constante évolution. Tout cela est réalisé tout en maintenant l'agilité et l'efficacité de l'infrastructure de stockage existante. Cet accès sécurisé permet aux entreprises d'atteindre leurs objectifs rigoureux en matière de sécurité et de disponibilité avec un minimum de modifications de leur personnel, de leurs processus et de leur cadre technologique existants.

Le coffre-fort cybernétique ONTAP utilise les fonctionnalités natives d' ONTAP et constitue une approche simple pour une protection supplémentaire afin de créer des copies immuables et indélébiles de vos données. L'ajout du coffre-fort cybernétique basé sur ONTAP de NetApp à la posture de sécurité globale permettra de :

- Créez un environnement séparé et déconnecté des réseaux de production et de sauvegarde et limitez l’accès des utilisateurs à celui-ci.

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.