Cyber-coffre ONTAP

NetApp Solutions

NetApp
November 12, 2024

Sommaire

Cyber-coffre ONTAP

Présentation du cyber-coffre-fort ONTAP

La principale menace qui nécessite la mise en œuvre d'un cybercoffre est la prévalence croissante et la sophistication croissante des cyberattaques, en particulier les violations de données et les ransomware. "Avec une augmentation du phishing" de plus en plus sophistiquées lorsqu'il s'agit de voler des informations d'identification, les informations d'identification utilisées pour lancer une attaque par ransomware peuvent ensuite être utilisées pour accéder aux systèmes d'infrastructure. Dans ce cas, même les systèmes d'infrastructure durcis courent le risque d'être attaqués. La seule défense contre un système compromis est de protéger et d'isoler vos données dans un cyber-coffre.

Le cyber-coffre basé sur ONTAP de NetApp offre aux entreprises une solution complète et flexible pour protéger leurs données les plus stratégiques. En exploitant la « Air gapping » logique associée à des méthodologies de renforcement solides, ONTAP vous permet de créer des environnements de stockage isolés et sécurisés, résilients face aux cybermenaces en constante évolution. Avec ONTAP, vous pouvez assurer la confidentialité, l'intégrité et la disponibilité de vos données tout en conservant l'agilité et l'efficacité de votre infrastructure de stockage.

Depuis juillet 2024, le contenu des rapports techniques publiés au format PDF a été intégré à la documentation produit de ONTAP. De plus, les nouveaux rapports techniques tels que ce document n'auront plus de numéro TR.

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

Un cybercoffre est une technique spécifique de protection des données qui implique de stocker les données stratégiques dans un environnement isolé et séparé de l'infrastructure INFORMATIQUE principale.

Référentiel de données « à air Gap », **immuable** et **indélébile**, à l'abri des menaces qui affectent le réseau principal, telles que les logiciels malveillants, les ransomware ou même les menaces internes. Un cyber-coffre-fort peut être réalisé avec des instantanés **immuables** et **indélébiles**.

Les sauvegardes de « air gapping » qui utilisent des méthodes traditionnelles impliquent la création d'espace et la séparation physique des supports primaire et secondaire. En déplaçant le support hors site et/ou en coupant la connectivité, les hackers 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 cyber-coffre

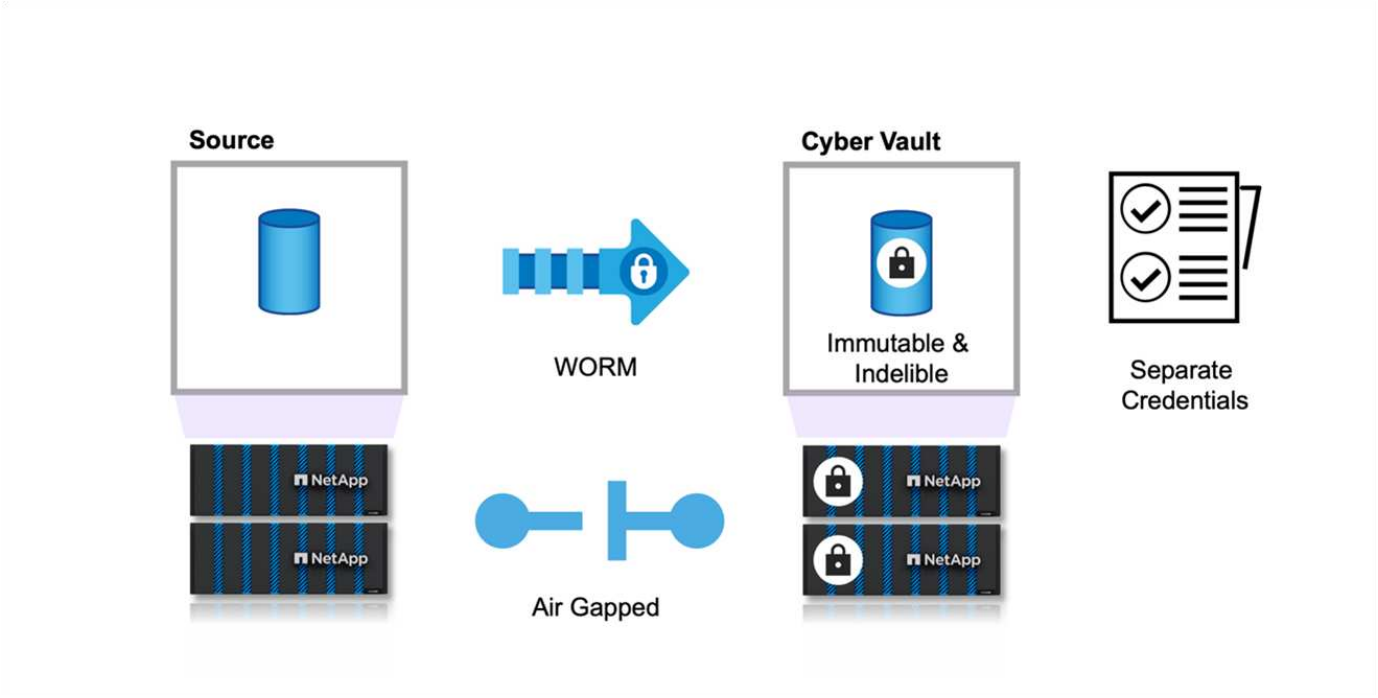
Les principales fonctionnalités de l'architecture de référence NetApp pour un coffre-fort virtuel sont les suivantes :

- Infrastructure de stockage sécurisée et isolée (p. ex., systèmes de stockage à air Gap)
- Les copies des données doivent être à la fois **immuables** et **indélébiles**, sans exception
- Contrôles d'accès stricts et authentification multifacteur
- Fonctionnalités de restauration rapide des données

Vous pouvez utiliser le stockage NetApp avec ONTAP en tant que cyber-coffre à air Gap en tirant parti de

"Copies Snapshot SnapLock Compliance pour protéger WORM". Vous pouvez effectuer toutes les tâches SnapLock Compliance de base sur le Cyber Vault. Une fois configurés, les volumes du Cyber Vault sont automatiquement protégés, ce qui vous évite d'archiver manuellement les copies Snapshot en mode WORM. Vous trouverez plus d'informations sur la mise en 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 se conformer à ces règlements (rapport de vérification disponible sur demande). En utilisant SnapLock Compliance avec cette certification, vous bénéficiez d'un mécanisme renforcé pour le contrôle aérien de vos données, sur lequel s'appuient les plus grandes institutions financières du monde pour assurer la conservation et la récupération des dossiers bancaires.



Terminologie Cyber Vault ONTAP

Il s'agit des termes couramment utilisés dans les architectures de cyber-coffre.

- Protection anti-ransomware autonome (ARP)* - la fonctionnalité de protection anti-ransomware autonome (ARP) utilise l'analyse de workloads dans les environnements NAS (NFS et SMB) pour détecter de manière proactive et en temps réel les activités anormales qui pourraient indiquer une attaque par ransomware. Lorsqu'une attaque est suspectée, ARP crée également de nouvelles copies Snapshot, en plus de la protection existante à partir de copies Snapshot planifiées. Pour plus d'informations, reportez-vous à la section "Documentation ONTAP sur la protection anti-ransomware autonome"

Air-Gap (logique) - vous pouvez configurer le stockage NetApp avec ONTAP en tant que cyber-coffre logique à air Gap en exploitant "Copies Snapshot SnapLock Compliance pour protéger WORM"

Air Gap (physique) - Un système physique à air comprimé n'a pas de connectivité réseau. Les sauvegardes sur bande permettent de déplacer les images vers un autre emplacement. L'air Gap logique de SnapLock Compliance est tout aussi robuste qu'un système physique à air comprimé.

Bastion Host - Un ordinateur dédié sur un réseau isolé, configuré pour résister aux attaques.

Copies Snapshot immuables : copies Snapshot qui ne peuvent pas être modifiées, sans exception (y

compris une organisation de support ou la capacité à formater le système de stockage de niveau inférieur).

Copies Snapshot indélébiles - copies Snapshot qui ne peuvent pas être supprimées, sans exception (y compris une organisation de support ou la possibilité de mettre en forme le système de stockage de bas niveau).

Copies Snapshot inviolables - copies Snapshot inviolables utilisez la fonction horloge SnapLock Compliance pour verrouiller les copies Snapshot pendant une période spécifiée. Ces snapshots verrouillés ne peuvent être supprimés par aucun utilisateur ni par la prise en charge de NetApp. Vous pouvez utiliser des copies Snapshot verrouillées pour restaurer des données si un volume est compromis par une attaque par ransomware, un logiciel malveillant, un hacker, un administrateur peu scrupuleux ou une suppression accidentelle. Pour plus d'informations, reportez-vous à la section "Documentation ONTAP sur les copies Snapshot inviolables"

SnapLock - SnapLock est une solution de conformité hautes performances pour les entreprises qui utilisent le stockage WORM pour conserver les fichiers sous une forme non modifiée à des fins réglementaires et de gouvernance. Pour plus d'informations, voir "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 archivage sécurisé (une copie des données avec conservation plus longue des copies Snapshot) ou les deux sur un système secondaire, sur site ou dans le cloud. Ces copies peuvent être utilisées à de nombreuses fins, telles qu'un incident, une migration vers le cloud ou un archivage sécurisé (lors de l'utilisation de la règle de copie et du verrouillage du coffre-fort). Pour plus d'informations, reportez-vous à la section "Documentation ONTAP sur SnapMirror"

SnapVault - dans ONTAP 9.3 SnapVault était obsolète en faveur de la configuration de SnapMirror à l'aide de la stratégie Vault ou mirror-vault. C'est le terme, bien qu'il soit encore utilisé, a également été déprécié. Pour plus d'informations, voir "Documentation ONTAP sur SnapVault".

Dimensionnement de la baie cybernétique avec ONTAP

Pour dimensionner un cybersystème, il est nécessaire de comprendre la quantité de données à restaurer dans un objectif de délai de restauration (RTO) donné. De nombreux facteurs jouent un rôle important dans la conception d'une solution de cyber-coffre adaptée. Les performances et la capacité doivent être prises en compte lors du dimensionnement d'un cyber-coffre.

Considérations relatives au dimensionnement de la performance

1. Quels sont les modèles de plateforme source (FAS v AFF A-Series v AFF C-Series) ?
2. Quelle est la bande passante et la latence entre la source et le cyber-coffre ?
3. Quelle est la taille des fichiers et combien de fichiers sont-ils volumineux ?
4. Quel est votre objectif de délai de restauration ?
5. Quelle quantité de données devez-vous restaurer dans l'objectif de délai de restauration ?
6. Combien de relations « fan-in » SnapMirror le cybercoffre est-il en cours d'acquisition ?
7. Y aura-t-il des restaurations uniques ou multiples en même temps ?
8. Ces restaurations multiples auront-elles lieu sur le même système primaire ?
9. SnapMirror sera-t-il répliqué vers le coffre-fort pendant la restauration à partir d'un coffre-fort ?

Exemples de dimensionnement

Voici des exemples de différentes configurations de cyber-coffre.

				
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

Dimensionnement de la capacité

La quantité d'espace disque requise pour un volume de destination de cyber-coffre ONTAP dépend de divers facteurs, dont le plus important est le taux de modification des données dans le volume source. La planification des sauvegardes et la planification Snapshot sur le volume de destination affectent à la fois l'utilisation du disque sur le volume de destination, et le taux de modification sur le volume source n'est probablement pas constant. Il est conseillé de fournir une réserve de 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 une durée de conservation d'un mois dans ONTAP nécessite le calcul des besoins en stockage en fonction de plusieurs facteurs, notamment la taille du jeu de données principal, le taux de modification des données (taux de modification quotidien) et les économies réalisées grâce à la déduplication et à la compression (le cas échéant).

Voici l'approche étape par étape :

La première étape consiste à connaître la taille du ou des volumes source que vous protégez avec le cyber-coffre. Il s'agit de la quantité de données de base qui sera initialement répliquée vers la destination du cybercoffre. Ensuite, estimez le taux de modification quotidien du jeu de données. Pourcentage de données qui changent chaque jour. Il est essentiel de bien comprendre la dynamique de vos données.

Par exemple :

- Taille du dataset primaire = 5 To
- Taux de changement quotidien = 5 % (0.05)
- Efficacité de la déduplication et de la compression = 50 % (0.50)

Voyons maintenant le calcul :

- Calculer le taux de modification des données quotidiennes :

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

- Calculer le total des données modifiées pour 30 jours :

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

- Calculer le stockage total requis :

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

- Appliquer les économies réalisées grâce à la déduplication et à la compression :

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

Résumé des besoins de stockage

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

> La surcharge liée aux métadonnées peut s'avérer supplémentaire pour les copies Snapshot, mais cette opération est généralement mineure.

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

> Prendre en compte la croissance des données au fil du temps pour garantir la pérennité du dimensionnement.

Création d'un cyber-coffre-fort avec ONTAP

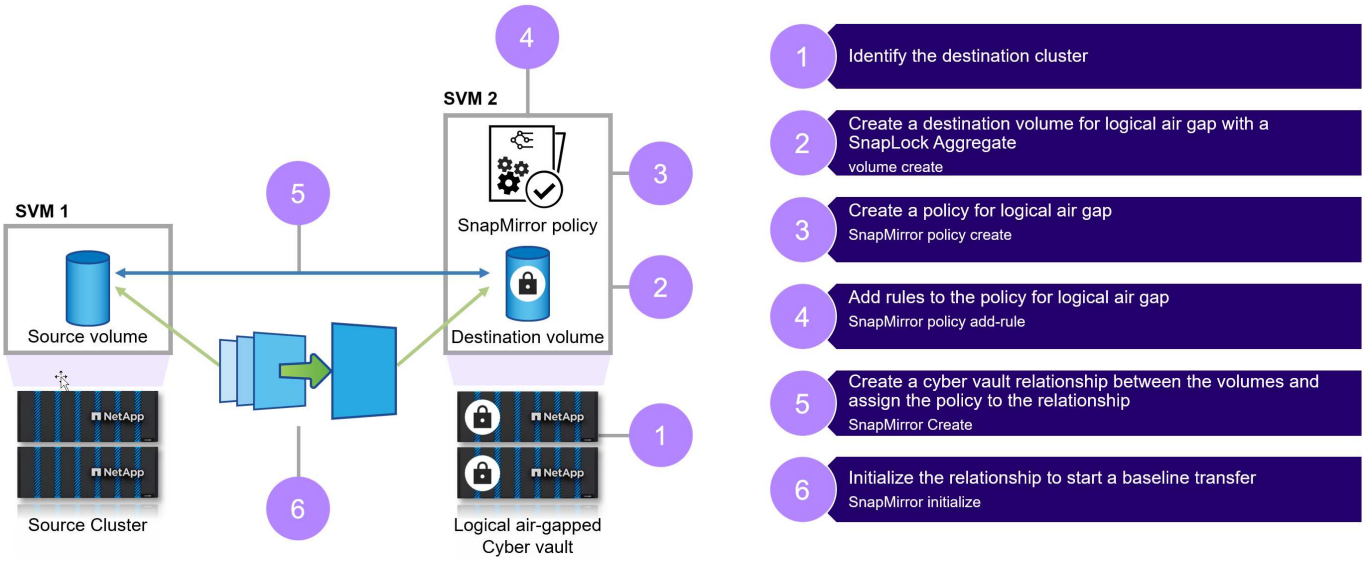
Les étapes ci-dessous vous aideront à créer un cyber-coffre-fort avec ONTAP.

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 destination doivent être créés dans des clusters associés avec des SVM peering. Pour plus d'informations, voir "Peering de clusters".
- Si la croissance automatique du volume est désactivée, l'espace disponible sur le volume de destination doit être au moins cinq pour cent supérieur à l'espace utilisé sur le volume source.

Description de la tâche

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



Étapes

1. Identifiez la baie de destination devant devenir le cyber-coffre-fort pour recevoir les données « air Gap ».
2. Sur la baie de destination, pour préparer le cyber-coffre-fort, "Installez la licence ONTAP One", "Initialiser l'horloge de conformité"et, si vous utilisez une version ONTAP antérieure à 9.10.1, "Créer un agrégat SnapLock Compliance".
3. Sur la baie de destination, créer 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. Depuis ONTAP 9.10.1, les volumes SnapLock et non SnapLock peuvent exister sur le même agrégat. Ainsi, vous n'avez plus besoin de créer un agrégat SnapLock distinct si vous utilisez ONTAP 9.10.1. Vous utilisez `-snaplock-type` l'option de volume pour spécifier un type de conformité. Dans les versions ONTAP antérieures à ONTAP 9.10.1, le mode SnapLock, la conformité est héritée de l'agrégat. Les volumes de destination flexibles de la version 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 SnapLock Compliance de 2 Go nommé `dstvolB` dans `SVM2` sur l'agrégat `node01_aggr`:

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

5. Sur le cluster de destination, pour créer l'air Gap, définissez la période de rétention par défaut, comme décrit à la section "Définir la période de conservation par défaut". Une période de conservation par défaut est affectée à un volume SnapLock cible du coffre-fort. La valeur de cette période est initialement définie sur un minimum de 0 ans et un maximum de 100 ans (à partir de ONTAP 9.10.1. Pour les versions précédentes de ONTAP, la valeur est comprise entre 0 et 70.) pour les volumes SnapLock Compliance. À chaque copie NetApp Snapshot, toutes les copies NetApp Snapshot sont conservées pendant cette période de conservation par défaut. La période-conservation-par-défaut doit être modifiée. La période de conservation peut être prolongée ultérieurement, si nécessaire, mais jamais raccourcie. Pour plus d'informations, voir "Aperçu de la durée 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 à l'aide d'une règle XDPDefault pour archiver les copies Snapshot avec une étiquette quotidienne et hebdomadaire selon un planning horaire :

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

   "Création d'une règle de réplication personnalisée" ou un "planification personnalisée" si les valeurs par défaut disponibles ne sont pas adaptées.

7. Sur le SVM destination, initialiser 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 le SVM1 et le volume de destination dstvolB sur le 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 l'heure d'expiration de la SnapLock appliquée aux copies Snapshot répliquées.

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

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

Renforcement de la sécurité des coffres-forts

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

Recommandations sur le renforcement du système Cyber Vault

- Isoler les plans de gestion du cybercoffre
- N'activez pas les LIFs de données sur le cluster de destination, car elles constituent un vecteur d'attaque supplémentaire
- Sur le cluster de destination, limiter l'accès du LIF intercluster au cluster source avec une politique de services
- Segmenter la LIF de gestion sur le cluster de destination pour un accès limité avec une politique de service et un hôte de base
- Limitez l'ensemble du trafic de données du cluster source vers le cyber-coffre pour n'autoriser que 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 des audits et le stockage des journaux à distance
- Permettre une vérification multiadministrateur et exiger une vérification auprès d'un administrateur en dehors de vos administrateurs de stockage habituels (par exemple, le personnel du RSSI)
- Mettez en œuvre des contrôles d'accès basés sur des rôles
- Authentification multifacteur administrative requise pour System Manager et ssh
- Utilisez l'authentification basée sur jeton pour les scripts et les appels de l'API REST

Reportez-vous au "Guide de renforcement ONTAP", "Présentation de la vérification multi-administrateur" et "Guide d'authentification multifacteur ONTAP" au pour savoir comment effectuer ces étapes de durcissement.

Interopérabilité avec le cyber-coffre-fort

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

Recommandations relatives au matériel ONTAP

Toutes les baies physiques unifiées ONTAP peuvent être utilisées pour la mise en œuvre d'un cybercoffre.

- Le stockage hybride FAS constitue la solution la plus économique.
- La gamme AFF C-Series offre la plus efficace en termes de consommation électrique et de densité.
- La gamme AFF A-Series est la plateforme la plus performante qui offre le meilleur RTO. Avec l'annonce récente de notre tout dernier système AFF A-Series, cette plateforme offrira la meilleure efficacité de stockage, sans compromis sur les performances.

Recommandations sur les logiciels ONTAP

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

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

Configuration MetroCluster

Pour les configurations MetroCluster, il est important de connaître les éléments suivants :

- Vous pouvez créer une relation SnapVault uniquement entre des SVM source synchrone, et non entre un SVM source synchrone et une SVM de destination synchrone.
- Vous pouvez créer une relation SnapVault depuis un volume d'un SVM source synchrone vers une SVM transmettant les données.
- Vous pouvez créer une relation SnapVault depuis un volume d'une SVM diffusant les données vers un volume DP au sein d'un SVM source synchrone.

Foire aux questions sur le cyber-coffre-fort

Cette FAQ s'adresse aux clients et partenaires NetApp. Il répond aux questions les plus fréquemment posées sur l'architecture de référence de cybercoffre basée sur ONTAP de NetApp.

Qu'est-ce qu'un cyber-coffre NetApp ?

Le cybercoffre est une technique spécifique de protection des données qui implique de stocker les données dans un environnement isolé et séparé de l'infrastructure INFORMATIQUE principale.

Le cybercoffre est un référentiel de données « à air Gap », immuable et indélébile, à l'abri des menaces qui affectent les données primaires, telles que les logiciels malveillants, les ransomware ou les menaces internes. Vous pouvez créer un coffre-fort cybernétique avec des copies Snapshot NetApp ONTAP immuables et indélébiles grâce à NetApp SnapLock Compliance. Sous la protection SnapLock Compliance, les données ne peuvent pas être modifiées ou supprimées, même par les administrateurs ONTAP ou le support NetApp.

Les sauvegardes de « air gapping » utilisant des méthodes traditionnelles impliquent la création d'espace et la séparation physique des supports principal et secondaire. Le « air Gap » avec le « cyber-coffre » consiste à utiliser un réseau de réplication des données distinct en dehors des réseaux d'accès aux données standard pour répliquer les copies Snapshot vers une destination indélébile.

Pour aller plus loin que les réseaux à air Gap, vous devez désactiver tous les protocoles d'accès aux données et de réplication sur le cyber-coffre lorsqu'ils ne sont pas nécessaires. Cela empêche l'accès aux données et leur exfiltration sur le site de destination. Avec SnapLock Compliance, la séparation physique n'est pas nécessaire. SnapLock Compliance protège vos copies Snapshot en lecture seule, à un point dans le temps, pour une restauration rapide des données, à l'abri de la suppression et des immuables.

L'approche de NetApp en matière de cyber-coffre

Le cyber-coffre NetApp, optimisé par SnapLock, offre aux entreprises une solution complète et flexible pour protéger leurs données les plus stratégiques. En tirant parti des technologies de renforcement dans ONTAP, NetApp vous permet de créer un coffre-fort cybernétique, isolé et sécurisé, à l'abri des cyber-menaces en constante évolution. Avec NetApp, vous pouvez assurer la confidentialité, l'intégrité et la disponibilité de vos données tout en conservant l'agilité et l'efficacité de votre infrastructure de stockage.

Les principales fonctionnalités de l'architecture de référence NetApp pour un coffre-fort virtuel sont les suivantes :

- Infrastructure de stockage sécurisée et isolée (p. ex., systèmes de stockage à air Gap)
- Des copies de sauvegarde de vos données sont à la fois immuables et indélébiles
- Contrôles d'accès stricts et séparés, vérification multiadministrateur et authentification multifacteur
- Fonctionnalités de restauration rapide des données

Foire aux questions sur le cyber-coffre-fort

Le cyber-coffre-fort est-il un produit de NetApp ?

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

Le cybercoffre avec NetApp est-il juste un autre nom pour LockVault ou SnapVault ?

LockVault était une fonctionnalité de Data ONTAP 7-Mode qui n'est pas disponible dans les versions actuelles de ONTAP.

SnapVault était un terme hérité de ce qui est désormais accompli avec la règle de copie de SnapMirror. Cette règle permet à la destination de conserver une quantité différente de copies Snapshot par rapport au volume source.

Le cybercoffre utilise SnapMirror avec la règle de copie Vault et SnapLock Compliance ensemble pour créer une copie immuable et indélébile des données.

Quel matériel NetApp puis-je utiliser pour un cybercoffre, un FAS, le Flash à capacité ou le Flash à performance ?

Cette architecture de référence pour la cyber-copie s'applique à l'ensemble du portefeuille matériel ONTAP. Les clients peuvent utiliser les plateformes AFF A-Series, AFF C-Series ou FAS comme coffre-fort. Les plateformes Flash offrent les délais de restauration les plus courts, tandis que les plateformes sur disque constituent la solution la plus économique. Selon la quantité de données récupérées et si plusieurs restaurations se produisent en parallèle, l'utilisation de systèmes sur disque (FAS) peut prendre plusieurs jours, voire plusieurs semaines. Contactez un représentant NetApp ou un représentant partenaire pour dimensionner correctement une solution de cyber-sécurité en fonction des besoins de l'entreprise.

Puis-je utiliser Cloud Volumes ONTAP en tant que source de cyber-coffre-fort ?

Oui. Cependant, l'utilisation de CVO comme source nécessite la réplication des données vers une destination de cybercopie sur site, car SnapLock Compliance est une exigence pour un cyber-coffre 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 cyber-sécurité ?

L'architecture du Cyber Vault repose sur l'indélébilité SnapLock Compliance de ONTAP et est conçue pour les implémentations sur site. Les architectures Cyber Vault basées sur le cloud sont actuellement à l'étude pour publication ultérieure.

Puis-je utiliser ONTAP Select en tant que source de cyber-coffre-fort ?

Oui, ONTAP Select peut être utilisé comme source pour un environnement matériel sur site de destination de cybercopie.

Puis-je utiliser ONTAP Select comme destination de cyber-sécurité ?

Non, ONTAP Select ne doit pas être utilisé comme destination de cyber-coffre, car il ne peut pas utiliser SnapLock Compliance.

Un cybercoffre avec NetApp utilise-t-il uniquement SnapMirror ?

Non, une architecture de cyber-coffre NetApp exploite de nombreuses fonctionnalités ONTAP pour créer une copie sécurisée, isolée, air Gap et renforcée de données. Pour plus d'informations sur les informations techniques supplémentaires à utiliser, reportez-vous à la question suivante.

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

La base d'un cyber-coffre NetApp est SnapMirror et SnapLock Compliance. Cependant, l'utilisation de fonctionnalités ONTAP supplémentaires, telles que les copies Snapshot inviolables, l'authentification multifacteur (MFA), la vérification multiadministrateur, le contrôle d'accès basé sur les rôles et la journalisation des audits locale et distante, améliore la sécurité et la sécurité de vos données.

En quoi les copies ONTAP Snapshot sont-elles meilleures que les autres pour un cybercoffre ?

Les copies Snapshot ONTAP sont immuables par défaut et peuvent être rendues indélébiles grâce à SnapLock Compliance. Même la prise en charge de NetApp ne peut pas supprimer les copies Snapshot SnapLock. La meilleure question à se poser est de savoir ce qui rend le cyber-coffre NetApp meilleur que les autres cyber-coffres de l'industrie. Tout d'abord, ONTAP est le stockage le plus sécurisé au monde et a obtenu la validation CSfC qui permet le stockage de données secrètes et les plus secrètes au repos sur les couches matérielles et logicielles. Plus d'informations sur "CSFC est disponible ici". De plus, ONTAP peut être air Gap au niveau de la couche de stockage, le système de cyber-coffre contrôlant la réplication permettant de créer un air Gap au sein du réseau de cyber-coffre.

Est-il possible que le volume source d'un cyber-coffre soit un volume compatible avec ONTAP Fabric Pool (volume hiérarchisé vers ONTAP S3 ou StorageGRID) ?

Non, Un volume source FabricPool indépendamment de la règle utilisée ne peut pas être répliqué vers une destination SnapLock Compliance.

Le cyber-coffre-fort NetApp fonctionne-t-il sur un profil ou une personnalité ONTAP différente ?

Non, il s'agit d'une architecture de référence. Les clients peuvent utiliser le "architecture de référence" et créer un cyber-coffre-fort ou utiliser "Scripts PowerShell pour créer, renforcer et valider"un cyber-coffre-fort.

Puis-je activer les protocoles de données tels que NFS, SMB et S3 dans un cybercoffre-fort ?

Par défaut, les protocoles de données doivent être désactivés sur le cyber-coffre-fort pour le sécuriser. Cependant, les protocoles de données peuvent être activés sur le cyber-coffre pour accéder aux données à des fins de restauration ou lorsque cela est nécessaire. Cette opération doit être effectuée de façon temporaire et désactivée une fois la récupération terminée.

Pouvez-vous convertir un environnement SnapVault existant en cyber-coffre ou tout réamorcer ?

Oui. On peut prendre un système qui est une destination SnapMirror (avec la stratégie de coffre-fort), désactiver les protocoles de données, renforcer le système selon le "Guide de renforcement ONTAP", l'isoler un emplacement sécurisé, et suivre les autres procédures de l'architecture de référence pour en faire un cyber-coffre sans avoir à réalimenter 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 cyber-coffre-fort

Pour en savoir plus sur les informations décrites dans cette cyber-chambre, consultez les informations supplémentaires et concepts de sécurité suivants.

- "Cyber-coffre NetApp : description des solutions de protection des données multicouches"
- "NetApp obtient la note AAA pour la solution de détection des ransomwares intégrée, la première solution du secteur basée sur l'IA"

- "Améliorez la cyberrésilience grâce au stockage le plus sécurisé au monde"
- "Guide ONTAP sur le renforcement de la sécurité"
- "« Zéro confiance » NetApp"
- "Cyberrésilience NetApp"
- "Protection des données NetApp"
- "Présentation du cluster et de SVM peering avec l'interface de ligne de commande"
- "Archivage SnapVault"
- "Configurer, analyser, script cron"

Création, renforcement et validation d'un cyber-coffre-fort ONTAP avec PowerShell

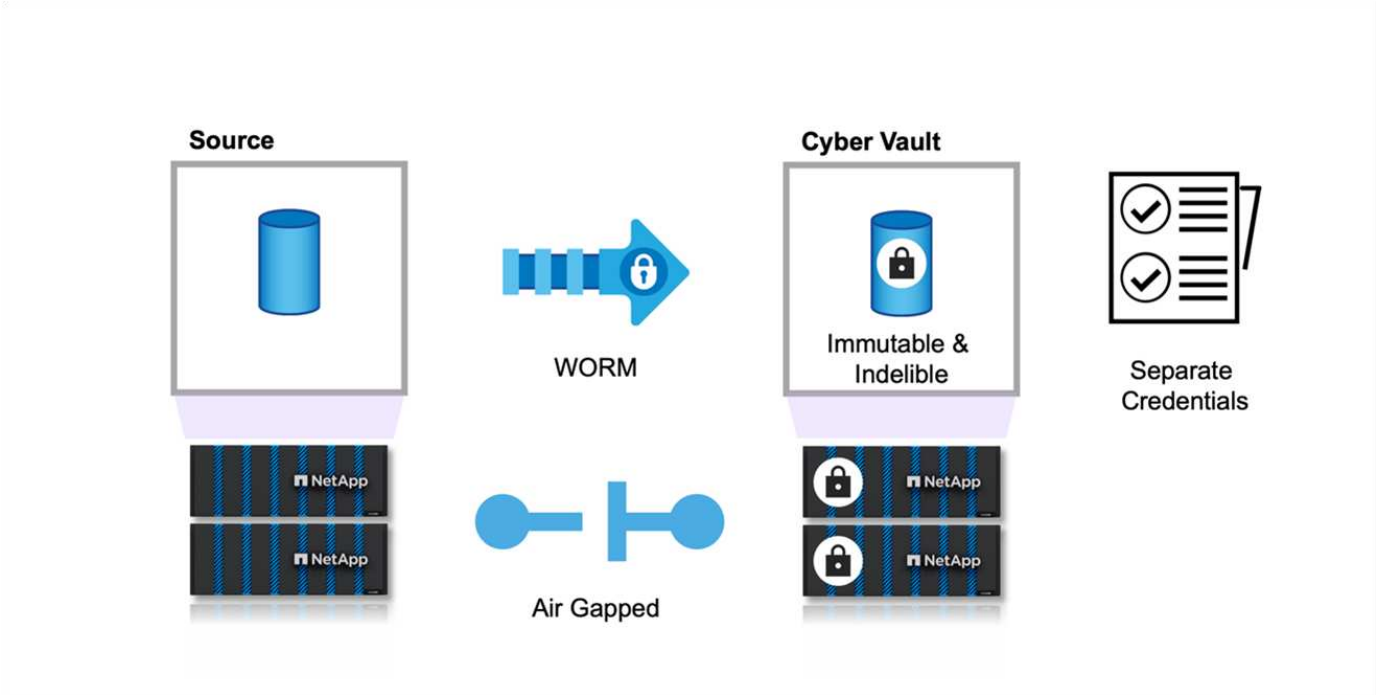
Présentation du cyber-coffre-fort ONTAP avec PowerShell

Dans le monde digital d'aujourd'hui, la protection des données stratégiques d'une entreprise n'est pas qu'une bonne pratique, c'est un impératif commercial. Les cybermenaces évoluent à un rythme sans précédent et les mesures classiques de protection des données ne suffisent plus à sécuriser les informations sensibles. C'est là qu'intervient un cyber-coffre. La solution de pointe de NetApp basée sur ONTAP associe des techniques de rodage avancées à des mesures de protection des données robustes afin de créer une barrière impénétrable contre les cybermenaces. En isolant les données les plus précieuses à l'aide d'une technologie de renforcement sécurisé, un cyber-coffre minimise la surface d'attaque, afin que les données les plus stratégiques restent confidentielles, intactes et immédiatement disponibles en cas de besoin.

Un cyber-coffre est une installation de stockage sécurisée qui se compose de plusieurs couches de protection, telles que des pare-feu, des réseaux et du stockage. Ces composants protègent les données de restauration essentielles nécessaires aux opérations métier critiques. Les composants du cyber-coffre se synchronisent régulièrement avec les données de production essentielles en fonction de la stratégie de coffre-fort, mais restent inaccessibles. Cette configuration isolée et déconnectée permet de garantir qu'en cas de cyber-attaque compromettant l'environnement de production, une récupération fiable et finale peut être facilement effectuée à partir du cyber-coffre.

NetApp permet de créer facilement un air Gap pour le cyber-coffre en configurant le réseau, en désactivant les LIF, en mettant à jour les règles du 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 cyber-attaques à distance et les tentatives d'accès non autorisées, ce qui rend le système à l'abri des menaces et des intrusions basées sur le réseau.

En combinant ces fonctionnalités à la protection SnapLock Compliance, les données ne peuvent pas être modifiées ni supprimées, même par les administrateurs ONTAP ou le support NetApp. SnapLock fait l'objet d'audits réguliers en conformité avec les réglementations SEC et FINRA, garantissant ainsi que la résilience des données respecte ces réglementations strictes en matière de WORM et de conservation des données dans le secteur bancaire. NetApp est le seul stockage d'entreprise validé par NSA CSfC pour le stockage de données les plus secrètes.



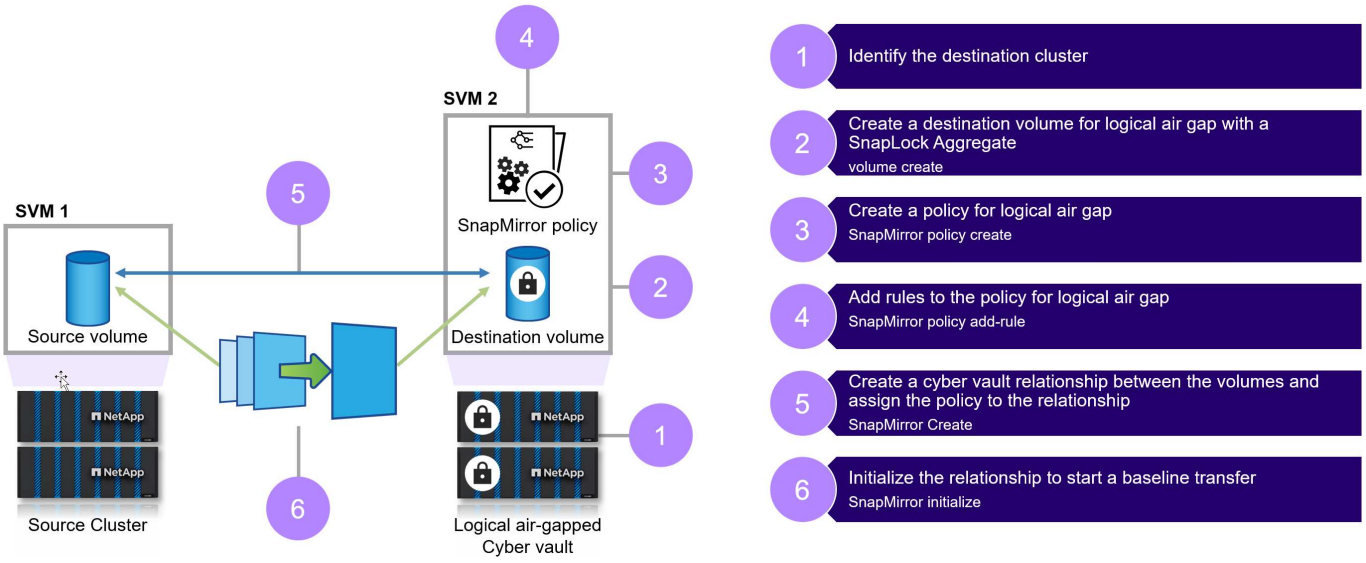
Ce document décrit la configuration automatisée de la solution cyberVault de NetApp pour le stockage ONTAP sur site vers un autre stockage ONTAP désigné, avec des snapshots immuables, qui ajoutent une couche de protection supplémentaire en cas d'attaques informatiques croissantes pour une restauration rapide. Dans le cadre de cette architecture, l'ensemble de la configuration est appliquée conformément aux bonnes pratiques de ONTAP. La dernière section contient des instructions pour effectuer une récupération en cas d'attaque.

La même solution s'applique pour créer le cybercoffre désigné dans AWS à l'aide de FSX ONTAP.

Étapes de haut niveau pour créer un cyber-coffre ONTAP

- Création de la relation de peering
  - Le site de production utilisant le stockage ONTAP est associé à un stockage ONTAP dédié au cybercoffre
- Créer un volume SnapLock Compliance
- Configurer la relation et la règle SnapMirror pour définir le libellé
  - La relation SnapMirror et les planifications appropriées sont configurées
- Définissez les rétentions avant de lancer le transfert SnapMirror (coffre-fort)
  - Le verrouillage de conservation est appliqué aux données copiées, ce qui empêche également les données d'être internes ou d'échouer. Vous ne pouvez pas supprimer les données avant l'expiration de la période de conservation
  - Les entreprises peuvent conserver ces données pendant quelques semaines/mois, selon leurs besoins
- Initialisation de la relation SnapMirror à partir d'étiquettes
  - L'amorçage initial et le transfert incrémentiel perpétuel s'effectue en fonction de la planification SnapMirror
  - Les données sont protégées (immuables et indélébiles) avec SnapLock Compliance, et elles peuvent être restaurées

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



Composants de la solution

NetApp ONTAP s'exécutant sur 9.15.1 clusters source et cible

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

Fonctionnalités utilisées à partir de la licence ONTAP One :

- Conformité SnapLock
- SnapMirror
- Vérification multi-administrateurs
- Toutes les fonctionnalités de renforcement exposées par ONTAP
- Informations d'identification RBAC distinctes pour le cyber-coffre

> Toutes les baies physiques unifiées ONTAP peuvent être utilisées pour une infrastructure informatique virtuelle, mais les systèmes Flash AFF C-Series basés sur la capacité et les systèmes Flash hybrides FAS constituent les plateformes idéales les plus économiques à cette fin. Veuillez consulter le "Dimensionnement du cyber-coffre ONTAP" pour obtenir des conseils de dimensionnement.

La création de cybercoffres ONTAP avec PowerShell

Les sauvegardes de « air gapping » qui utilisent des méthodes traditionnelles impliquent la création d'espace et la séparation physique des supports primaire et secondaire. En

déplaçant le support hors site et/ou en coupant la connectivité, les hackers 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 nécessaire. SnapLock Compliance protège les copies Snapshot archivées à un point dans le temps et en lecture seule. Les données sont ainsi rapidement accessibles, protégées contre la suppression et indélébiles, et protégées contre les modifications ou les immuables.

Conditions préalables

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 destination doivent être associés.
- Les SVM source et destination doivent être peering.
- Vérifiez que le chiffrement de peering de cluster est activé.

La configuration des transferts de données vers un cyber-coffre ONTAP nécessite plusieurs étapes. Sur le volume primaire, configurez une règle de snapshot qui spécifie les copies à créer et quand les créer à l'aide de planifications appropriées, puis attribuez des étiquettes pour spécifier les copies à transférer par SnapVault. Sur le stockage secondaire, une règle SnapMirror doit être créée, spécifiant les étiquettes des copies Snapshot à transférer et le nombre de ces copies à conserver dans le coffre-fort virtuel. Une fois ces stratégies configurées, créez la relation SnapVault et planifiez le transfert.

Ce document part du principe que le stockage principal et le cyber-coffre ONTAP désigné sont déjà configurés et configurés.

Le cluster du cybercoffre-fort peut se trouver dans le même data Center ou dans un data Center différent de celui des données source.

Étapes de création d'un cyber-coffre-fort ONTAP

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

La rétention par défaut est définie sur minimum. Une période de conservation par défaut est affectée à un volume SnapLock cible du coffre-fort. La valeur de cette période est initialement définie sur un minimum de 0 ans et un maximum de 100 ans (à partir de ONTAP 9.10.1. Pour les versions précédentes de ONTAP, la valeur est comprise entre 0 et 70.) pour les volumes SnapLock Compliance. À chaque copie NetApp Snapshot, toutes les copies NetApp Snapshot sont conservées pendant cette période de conservation par défaut. La période de conservation peut être prolongée ultérieurement, si nécessaire, mais jamais raccourcie. Pour plus d'informations, voir "Aperçu de la durée de conservation".

Les étapes ci-dessus comprennent les étapes manuelles. Les experts en sécurité conseillent d'automatiser le processus pour éviter la gestion manuelle, ce qui génère une marge d'erreur importante. Vous trouverez ci-dessous l'extrait de code qui automatise complètement les prérequis et la configuration de SnapLock Compliance et 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 cyber-coffre à air Gap utilisant SnapLock Compliance et SnapVault est prêt.

Avant de transférer les données d'instantané vers le cyber-coffre, la relation SnapVault doit être initialisée. Toutefois, avant cela, il est nécessaire d'effectuer un renforcement de la sécurité pour sécuriser le coffre-fort.

Renforcement des coffres-forts ONTAP avec PowerShell

Le coffre-fort virtuel ONTAP offre une meilleure résilience contre les cyberattaques que les solutions classiques. Lors de la conception d'une architecture pour améliorer la sécurité, il est essentiel de prendre des mesures pour réduire la surface d'attaque. Pour ce faire, plusieurs méthodes peuvent être utilisées, telles que l'implémentation de stratégies de mots de passe renforcées, l'activation du contrôle d'accès basé sur des rôles, le verrouillage des comptes utilisateur par défaut, la configuration des pare-feu et l'utilisation des flux d'approbation pour toute modification apportée au système Vault. En outre, la restriction des protocoles d'accès au réseau à partir d'une adresse IP spécifique peut aider à limiter les vulnérabilités potentielles.

ONTAP fournit un ensemble de commandes 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.

Meilleures pratiques de renforcement

Étapes manuelles

1. Créez un utilisateur désigné avec un rôle administratif prédéfini et personnalisé.
2. Créez un nouvel IPspace pour isoler le trafic réseau.
3. Créer un nouveau SVM résidant dans le nouvel IPspace.
4. Assurez-vous que les politiques de routage de pare-feu sont correctement configurées et que toutes les règles sont régulièrement vérifiées et mises à jour si nécessaire.

Interface de ligne de commande ONTAP ou via le script d'automatisation

1. Protection de l'administration avec la vérification multiadministrateur (MFA)
2. Activez le chiffrement des données standard « à la volée » entre les clusters.
3. Sécurisez SSH avec un chiffrement fort et appliquez des mots de passe sécurisés.
4. Activez la norme FIPS globale.
5. Telnet et Remote Shell (RSH) doivent être désactivés.
6. Verrouiller le compte admin par défaut.
7. Désactivez les LIFs de données et sécurisez les points d'accès distants.
8. Désactivez et supprimez les protocoles et services inutilisés ou externes.
9. Chiffrez le trafic réseau.
10. Utilisez le principe du privilège minimum lors de la configuration des rôles de superutilisateur et d'administration.
11. Limitez HTTPS et SSH à partir d'une adresse IP spécifique à l'aide de l'option IP autorisée.
12. Arrêter et reprendre la réplication en fonction du planning de transfert.

Bullets 1-4 a besoin d'une intervention manuelle, comme la désignation d'un réseau isolé, la séparation de l'IPspace, etc., et doit être réalisé au préalable. Vous trouverez des informations détaillées sur la configuration du durcissement dans le "Guide ONTAP sur le renforcement de la sécurité". 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 durcissement pour assurer la pérennité du contrôleur Vault. Le délai pendant lequel l'air Gap du cyber Vault est ouvert est aussi court que possible. SnapVault exploite la technologie Incremental Forever, qui ne déplacera les modifications depuis la dernière mise à jour vers le cyber-coffre-fort, réduisant ainsi la durée pendant laquelle le cyber-coffre-fort doit rester ouvert. Pour optimiser davantage le flux de travail, l'ouverture du cyber-coffre est coordonnée avec le planning de réplication afin de 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 cyber-coffre-fort ONTAP avec PowerShell

Un cyber-coffre robuste doit pouvoir résister à une attaque sophistiquée, même lorsque l'attaquant dispose d'informations d'identification pour accéder à l'environnement avec un Privileges élevé.

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

Exemple de code PowerShell pour valider la configuration par programmation.

```
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.

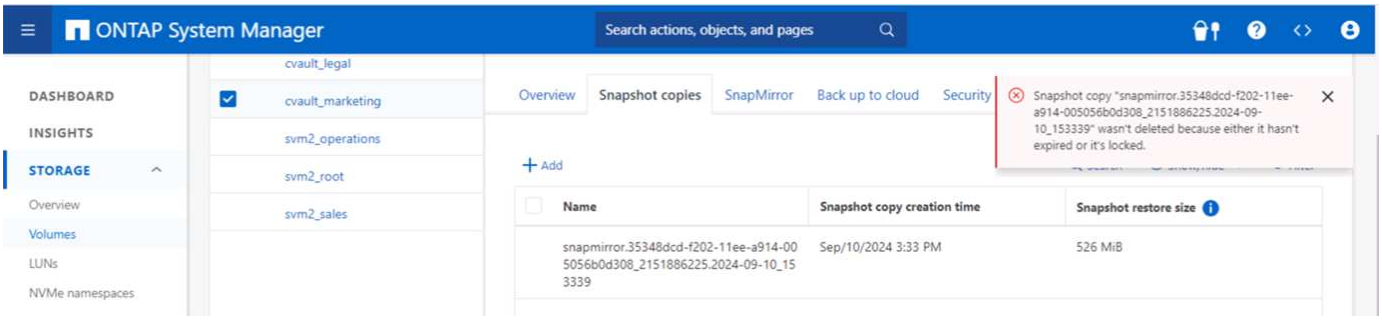
```
cluster2::> network connections  listening show
This table is currently empty.

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 indique qu'il n'est pas possible d'altérer les snapshots.



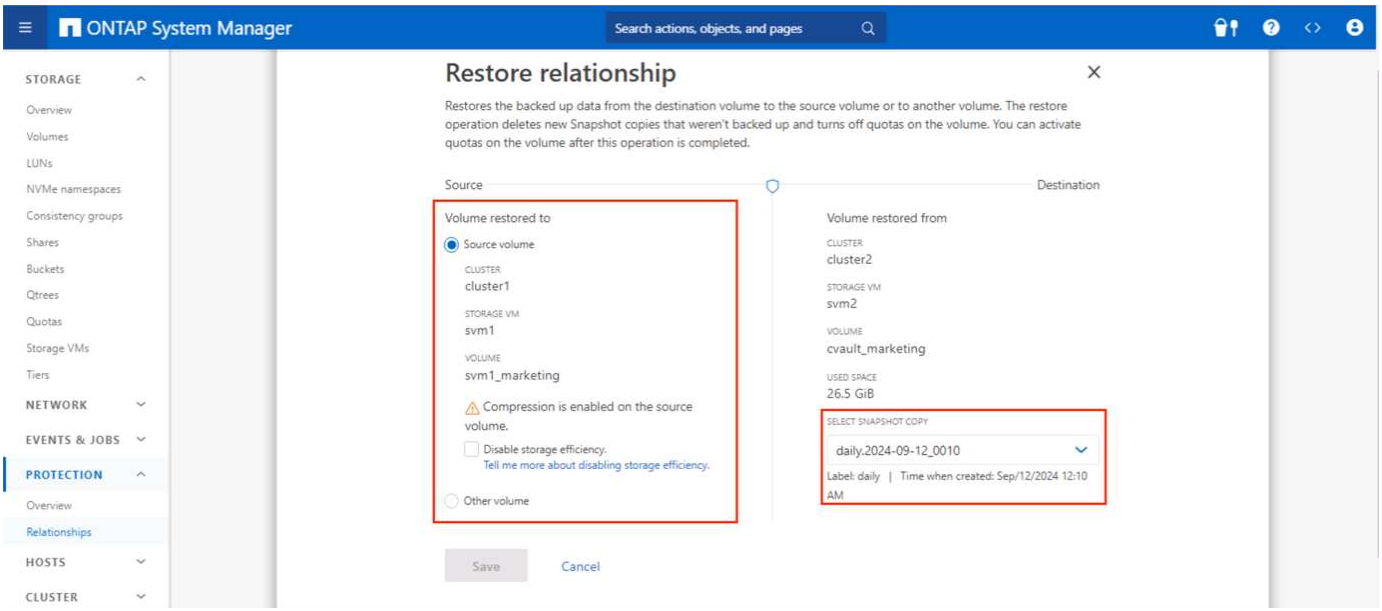
Pour valider et confirmer la fonctionnalité de mise en air, procédez comme suit :

- Tester les capacités d'isolation du réseau et la possibilité de mettre une connexion en veille lorsque les données ne sont pas transférées.
- Vérifiez que l'interface de gestion n'est accessible à partir d'aucune entité, à l'exception des adresses IP autorisées.
- Vérifier que la vérification multiadministrateur est en place pour fournir une couche supplémentaire d'approbation.
- Validez la capacité d'accès via l'interface de ligne de commandes et l'API REST
- A partir de la source, déclencher une opération de transfert vers le coffre-fort et s'assurer que la copie du coffre-fort ne peut pas être modifiée.
- Essayez de supprimer les copies snapshot immuables transférées vers le coffre-fort.
- Essayez de modifier la période de conservation en modifiant l'horloge du système.

Restauration des données ONTAP Cyber Vault

Si des données sont détruites dans le data Center de production, les données du cyber-coffre peuvent être restaurées en toute sécurité dans l'environnement choisi. Contrairement à une solution physiquement à air Gap, le cyber-coffre ONTAP à air Gap est construit à l'aide de fonctionnalités natives de ONTAP telles que SnapLock Compliance et SnapMirror. Il en résulte un processus de restauration à la fois rapide et facile à exécuter.

En cas d'attaque par ransomware et de nécessité de restaurer les données à partir du cybercoffre, le processus de restauration est simple et facile, car les copies Snapshot hébergées dans le cybercoffre sont utilisées pour restaurer les données chiffrées.



S'il s'agit d'un moyen plus rapide de remettre les données en ligne lorsque cela est nécessaire, afin de les valider, d'isoler et d'analyser rapidement les données à des fins de restauration. Ceci peut être facilement obtenu en utilisant avec FlexClone avec l'option SnapLock-type définie sur le type non-SnapLock.

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

La mise en pratique des procédures de restauration à partir du cyber-coffre permet de s'assurer que les étapes appropriées sont établies pour la connexion au cyber-coffre et la récupération des données. La planification et le test de la procédure sont essentiels pour toute reprise lors d'une cyberattaque.

Autres considérations

D'autres considérations sont à prendre en compte lors de la conception et du déploiement d'un cyber-coffre basé sur ONTAP.

Dimensionnement de la capacité

La quantité d'espace disque requise pour un volume de destination de cyber-coffre ONTAP dépend de divers facteurs, dont le plus important est le taux de modification des données dans le volume source. La planification des sauvegardes et la planification Snapshot sur le volume de destination affectent à la fois l'utilisation du disque sur le volume de destination, et le taux de modification sur le volume source n'est probablement pas constant. Il est conseillé de fournir une réserve de 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 une durée de conservation d'un mois dans ONTAP nécessite le calcul des besoins en stockage en fonction de plusieurs facteurs, notamment la taille du jeu de données principal, le taux de modification des données (taux de modification quotidien) et les économies réalisées grâce à la déduplication et à la compression (le cas échéant).

Voici l'approche étape par étape :

La première étape consiste à connaître la taille du ou des volumes source que vous protégez avec le cyber-coffre. Il s'agit de la quantité de données de base qui sera initialement répliquée vers la destination du cybercoffre. Ensuite, estimez le taux de modification quotidien du jeu de données. Pourcentage de données qui changent chaque jour. Il est essentiel de bien comprendre la dynamique de vos données.

Par exemple :

- Taille du dataset primaire = 5 To
- Taux de changement quotidien = 5 % (0.05)
- Efficacité de la déduplication et de la compression = 50 % (0.50)

Voyons maintenant le calcul :

- Calculer le taux de modification des données quotidiennes :

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

- Calculer le total des données modifiées pour 30 jours :

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

- Calculer le stockage total requis :

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

- Appliquer les économies réalisées grâce à la déduplication et à la compression :

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

Résumé des besoins de stockage

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

La surcharge liée aux métadonnées peut s'avérer supplémentaire pour les copies Snapshot, mais cette opération est généralement mineure.

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

Prendre en compte la croissance des données au fil du temps pour garantir la pérennité du dimensionnement.

Impact sur les performances au niveau principal/source

Comme le transfert de données est une opération de transfert, l'impact sur les performances du stockage primaire 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 virtuel. Lors de la configuration initiale de la relation et de la première sauvegarde complète, une quantité importante de données est transférée du système primaire vers le système de coffre-fort virtuel (le volume 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 doit uniquement suivre et transférer les blocs modifiés depuis la dernière sauvegarde. La charge d'E/S est donc bien inférieure à celle de la réplication initiale. Les mises à jour incrémentielles sont efficaces et ont un impact minimal sur les performances du stockage primaire. Le processus de copie s'exécute en arrière-plan, ce qui réduit les risques d'interférence avec les charges de travail de production du système principal.

- L'impact sur les performances est limité par le fait que le système de stockage dispose de suffisamment de ressources (CPU, mémoire et IOPS) pour gérer la charge supplémentaire.

Configurer, analyser, script cron

NetApp a créé "script unique pouvant être téléchargé"et utilisé pour configurer, vérifier et planifier les relations du cybercoffre.

Rôle de ce script

- Peering de clusters
- Peering de SVM
- Création de volume DP
- Relation SnapMirror et initialisation
- Renforcez le système ONTAP utilisé pour le cyber-coffre
- Arrêter et reprendre la relation en fonction du planning de transfert
- Validez régulièrement les paramètres de sécurité et générez un rapport indiquant toute anomalie

Comment utiliser ce script

"Téléchargez le script" pour utiliser le script, il vous suffit de suivre les étapes ci-dessous :

- Lancez Windows PowerShell en tant qu'administrateur.
- Accédez au répertoire contenant le script.
- Exécutez le script à l'aide de `.\` la syntaxe et des paramètres requis

> Veuillez vérifier toutes les informations saisies. Lors de la première exécution (mode de configuration), il demandera des informations d'identification pour la production et le nouveau système de cyber-coffre. Après cela, il créera les SVM peering (si inexistant), les volumes et la 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 vérifications de validation et configure le système comme étant à air comprimé.
- Analyse : fonction de surveillance et de reporting automatisée qui envoie des informations aux groupes de surveillance pour détecter les anomalies et les activités suspectes afin de s'assurer que les configurations ne sont pas modifiées.
- Cron : pour activer une infrastructure déconnectée, le mode cron automatise la désactivation de la LIF et arrête la relation de transfert.

Le transfert des données de ces volumes prend du temps selon les performances des systèmes et 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 de la solution ONTAP Cyber Vault PowerShell

En tirant parti des méthodes de renforcement robustes fournies par ONTAP, NetApp vous permet de créer un environnement de stockage isolé et sécurisé, résilient face aux cybermenaces en constante évolution. Tout cela s'effectue tout en conservant l'agilité et l'efficacité de l'infrastructure de stockage existante. Cet accès sécurisé permet aux entreprises d'atteindre leurs objectifs stricts en matière de sécurité et de disponibilité en modifiant au minimum leur personnel, leur structure de processus et leur structure technologique.

Le cybercoffre ONTAP utilise des fonctionnalités natives de ONTAP est une approche simple pour une protection supplémentaire qui permet de créer des copies immuables et indélébiles de vos données. L'ajout du cyber-coffre NetApp basé sur ONTAP à la stratégie de sécurité globale permettra de :

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