Proteção de dados com o cofre cibernético ONTAP

NetApp data management solutions

NetApp
August 18, 2025

Índice

Proteção de dados com o cofre cibernético ONTAP . . . 1
- Visão geral do cofre cibernético ONTAP . . . 1
  - O que é um cofre cibernético? . . . 1
  - Abordagem da NetApp para cofre cibernético . . . 1
- Terminologia ONTAP do cofre cibernético . . . 2
- Dimensionamento de cofre cibernético com ONTAP . . . 3
  - Considerações sobre dimensionamento de desempenho . . . 3
  - Considerações sobre dimensionamento de capacidade . . . 4
- Criando um cofre cibernético com ONTAP . . . 5
- Fortalecimento do cofre cibernético . . . 7
  - Recomendações para o reforço do cofre cibernético . . . 7
- Interoperabilidade do cofre cibernético . . . 8
  - Recomendações de hardware ONTAP . . . 8
  - Recomendações de software ONTAP . . . 8
  - Configuração do MetroCluster . . . 8
- Perguntas frequentes sobre o Cyber Vault . . . 9
  - O que é um cofre cibernético da NetApp ? . . . 9
  - Abordagem da NetApp para cofre cibernético . . . 9
  - Perguntas frequentes sobre o Cyber Vault . . . 10
- Recursos do cofre cibernético . . . 13
- Criação, reforço e validação de um cofre cibernético ONTAP com PowerShell . . . 14
  - Visão geral do cofre cibernético ONTAP com PowerShell . . . 14
  - Criação de cofre cibernético ONTAP com PowerShell . . . 16
  - Fortalecimento do cofre cibernético ONTAP com PowerShell . . . 20
  - Validação do cofre cibernético ONTAP com PowerShell . . . 27
  - Recuperação de dados do cofre cibernético ONTAP . . . 32
  - Considerações adicionais . . . 33
  - Configurar, analisar, script cron . . . 35
  - Conclusão da solução PowerShell do cofre cibernético ONTAP . . . 36

Proteção de dados com o cofre cibernético ONTAP

Visão geral do cofre cibernético ONTAP

A principal ameaça que exige a implementação de um cofre cibernético é a prevalência crescente e a sofisticação crescente dos ataques cibernéticos, especialmente ransomware e violações de dados. "Com o aumento do phishing" e métodos cada vez mais sofisticados de roubo de credenciais, as credenciais usadas para iniciar um ataque de ransomware podem ser usadas para acessar sistemas de infraestrutura. Nesses casos, até mesmo sistemas de infraestrutura reforçados correm risco de ataque. A única defesa contra um sistema comprometido é ter seus dados protegidos e isolados em um cofre cibernético.

O cofre cibernético baseado em ONTAP da NetApp fornece às organizações uma solução abrangente e flexível para proteger seus ativos de dados mais críticos. Ao aproveitar o air-gapping lógico com metodologias de proteção robustas, o ONTAP permite que você crie ambientes de armazenamento seguros e isolados, resilientes contra ameaças cibernéticas em evolução. Com o ONTAP, você pode garantir a confidencialidade, integridade e disponibilidade dos seus dados, mantendo a agilidade e a eficiência da sua infraestrutura de armazenamento.

> A partir de julho de 2024, o conteúdo de relatórios técnicos publicados anteriormente como PDFs foi integrado à documentação do produto ONTAP . Além disso, novos relatórios técnicos (TRs) como este documento não receberão mais números de TR.

O que é um cofre cibernético?

Um cofre cibernético é uma técnica específica de proteção de dados que envolve o armazenamento de dados críticos em um ambiente isolado, separado da infraestrutura primária de TI.

Repositório de dados "isolado", **imutável** e **indelével**, imune a ameaças que afetam a rede principal, como malware, ransomware ou até mesmo ameaças internas. Um cofre cibernético pode ser alcançado com instantâneos **imutáveis** e **indeléveis**.

Os backups com air-gapping que usam métodos tradicionais envolvem a criação de espaço e a separação física das mídias primária e secundária. Ao mover a mídia para outro local e/ou cortar a conectividade, os criminosos não têm acesso aos dados. Isso protege os dados, mas pode levar a tempos de recuperação mais lentos.

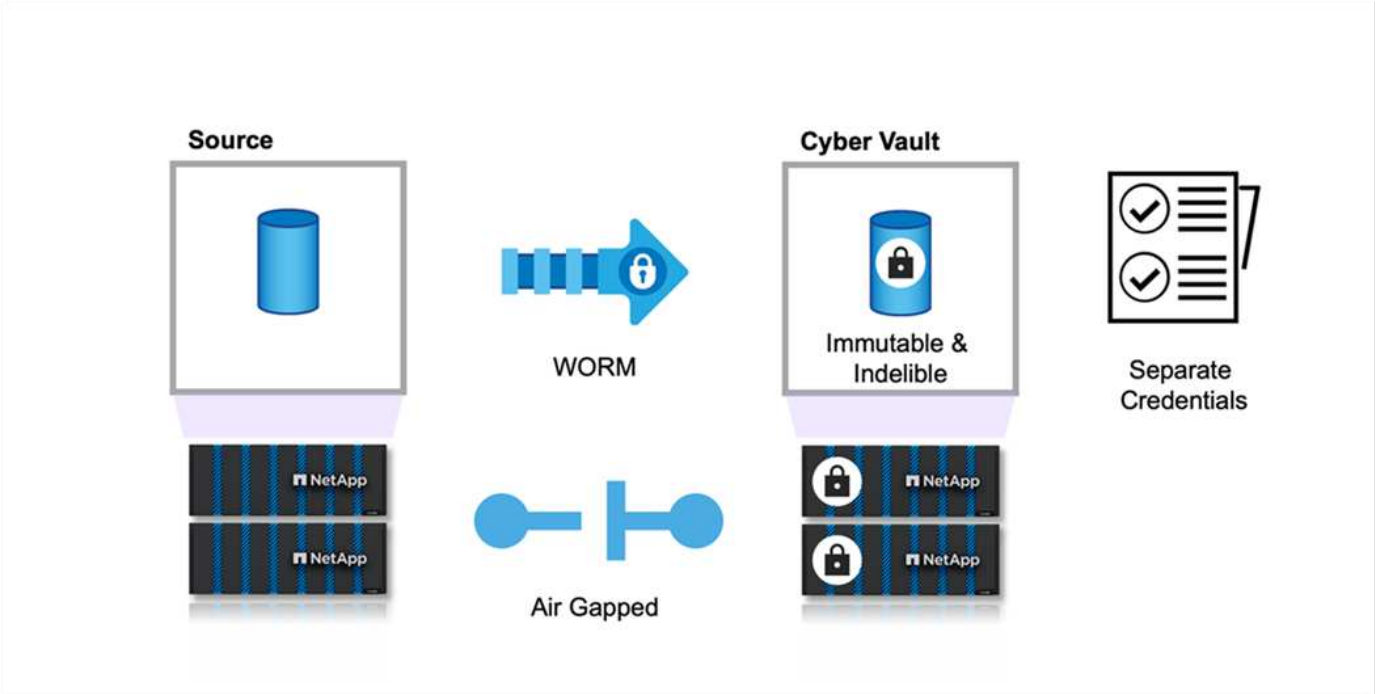
Abordagem da NetApp para cofre cibernético

Os principais recursos da arquitetura de referência da NetApp para um cofre cibernético incluem:

- Infraestrutura de armazenamento segura e isolada (por exemplo, sistemas de armazenamento com isolamento de ar)
- As cópias dos dados devem ser **imutáveis** e **indeléveis** sem exceção
- Controles de acesso rigorosos e autenticação multifator
- Capacidades de restauração rápida de dados

Você pode usar o armazenamento NetApp com ONTAP como um cofre cibernético isolado, aproveitando"SnapLock Compliance com cópias de Snapshot protegidas por WORM" . Você pode executar todas as tarefas básicas de SnapLock Compliance no cofre cibernético. Uma vez configurados, os volumes do Cyber Vault são protegidos automaticamente, eliminando a necessidade de enviar manualmente as cópias do Snapshot para o WORM. Mais informações sobre o air-gapping lógico podem ser encontradas aqui"blog"

O SnapLock Compliance é usado para estar em conformidade com os regulamentos bancários e financeiros SEC 70-a-4(f), FINRA 4511(c) e CFTC 1.31(c)-(d). Foi certificado pela Cohasset Associates para aderir a esses regulamentos (relatório de auditoria disponível mediante solicitação). Ao usar o SnapLock Compliance com esta certificação, você obtém um mecanismo reforçado para proteção de seus dados, no qual as maiores instituições financeiras do mundo confiam para garantir tanto a retenção quanto a recuperação de registros bancários.



Terminologia ONTAP do cofre cibernético

Esses são os termos comumente usados em arquiteturas de cofres cibernéticos.

Proteção Autônoma contra Ransomware (ARP) - O recurso Proteção Autônoma contra Ransomware (ARP) usa análise de carga de trabalho em ambientes NAS (NFS e SMB) para detectar e alertar proativamente e em tempo real sobre atividades anormais que podem indicar um ataque de ransomware. Quando há suspeita de ataque, o ARP também cria novas cópias de Snapshot, além da proteção existente de cópias de Snapshot agendadas. Para mais informações, consulte o"Documentação do ONTAP sobre Proteção Autônoma contra Ransomware"

Air-gap (lógico) - Você pode configurar o armazenamento NetApp com ONTAP como um cofre cibernético lógico com air-gap, aproveitando"SnapLock Compliance com cópias de Snapshot protegidas por WORM"

Air-gap (Físico) - Um sistema físico air-gap não tem conectividade de rede com ele. Usando backups em fita, você pode mover as imagens para outro local. O sistema de air-gap lógico SnapLock Compliance é tão robusto quanto um sistema de air-gap físico.

Host Bastion - Um computador dedicado em uma rede isolada, configurado para resistir a ataques.

Cópias de snapshot imutáveis - Cópias de snapshot que não podem ser modificadas, sem exceção (incluindo uma organização de suporte ou a capacidade de formatar em baixo nível o sistema de armazenamento).

Cópias de instantâneos indeléveis - Cópias de instantâneos que não podem ser excluídas, sem exceção (incluindo uma organização de suporte ou a capacidade de formatar em baixo nível o sistema de armazenamento).

Cópias Snapshot à prova de violação - Cópias Snapshot à prova de violação usam o recurso de relógio de SnapLock Compliance para bloquear cópias Snapshot por um período especificado. Esses snapshots bloqueados não podem ser excluídos por nenhum usuário ou pelo suporte da NetApp . Você pode usar cópias bloqueadas do Snapshot para recuperar dados se um volume for comprometido por um ataque de ransomware, malware, hacker, administrador desonesto ou exclusão acidental. Para mais informações, consulte o"Documentação ONTAP sobre cópias de Snapshot à prova de violação"

- SnapLock* - O SnapLock é uma solução de conformidade de alto desempenho para organizações que usam armazenamento WORM para reter arquivos em formato inalterado para fins regulatórios e de governança. Para obter mais informações, consulte o "Documentação ONTAP sobre SnapLock" .
- SnapMirror* - SnapMirror é uma tecnologia de replicação de recuperação de desastres, projetada para replicar dados de forma eficiente. O SnapMirror pode criar um espelho (ou cópia exata dos dados), um cofre (uma cópia dos dados com retenção de cópia do Snapshot mais longa) ou ambos para um sistema secundário, no local ou na nuvem. Essas cópias podem ser usadas para muitos propósitos diferentes, como em um desastre, em um estouro na nuvem ou em um cofre cibernético (ao usar a política de cofre e bloquear o cofre). Para mais informações, consulte o"Documentação do ONTAP no SnapMirror"
- SnapVault* - No ONTAP 9.3, o SnapVault foi descontinuado em favor da configuração do SnapMirror usando a política vault ou mirror-vault. Esse termo, embora ainda usado, também foi depreciado. Para obter mais informações, consulte o "Documentação do ONTAP no SnapVault" .

Dimensionamento de cofre cibernético com ONTAP

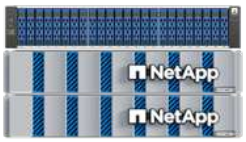
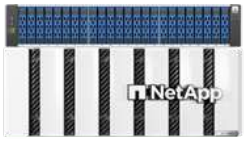
Dimensionar um cofre cibernético requer entender quantos dados precisarão ser restaurados em um determinado Objetivo de Tempo de Recuperação (RTO). Muitos fatores influenciam no projeto adequado de uma solução de cofre cibernético do tamanho certo. Tanto o desempenho quanto a capacidade devem ser considerados ao dimensionar um cofre cibernético.

Considerações sobre dimensionamento de desempenho

1. Quais são os modelos de plataforma de origem (FAS v AFF A-Series v AFF C-Series)?
2. Qual é a largura de banda e a latência entre a origem e o cofre cibernético?
3. Qual é o tamanho dos arquivos e quantos arquivos são?
4. Qual é sua meta de tempo de recuperação?
5. Quantos dados você precisa recuperar dentro do RTO?
6. Quantos relacionamentos de fãs do SnapMirror o cofre cibernético irá ingerir?
7. Haverá recuperações únicas ou múltiplas acontecendo ao mesmo tempo?
8. Essas múltiplas recuperações ocorrerão no mesmo primário?
9. O SnapMirror será replicado para o cofre durante uma recuperação de um cofre?

Exemplos de dimensionamento

Aqui estão exemplos de diferentes configurações de cofre cibernético.

				
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

Considerações sobre dimensionamento de capacidade

A quantidade de espaço em disco necessária para um volume de destino do cofre cibernético ONTAP depende de vários fatores, sendo o mais importante a taxa de alteração dos dados no volume de origem. O agendamento de backup e o agendamento de instantâneo no volume de destino afetam o uso do disco no volume de destino, e a taxa de alteração no volume de origem provavelmente não será constante. É uma boa ideia fornecer um buffer de capacidade de armazenamento adicional acima daquela necessária para acomodar futuras mudanças no comportamento do usuário final ou do aplicativo.

Dimensionar um relacionamento para 1 mês de retenção no ONTAP requer o cálculo dos requisitos de armazenamento com base em vários fatores, incluindo o tamanho do conjunto de dados primário, a taxa de alteração de dados (taxa de alteração diária) e a economia com desduplicação e compactação (se aplicável).

Aqui está a abordagem passo a passo:

O primeiro passo é saber o tamanho do(s) volume(s) de origem que você está protegendo com o cofre cibernético. Essa é a quantidade base de dados que será inicialmente replicada para o destino do cofre cibernético. Em seguida, estime a taxa de alteração diária do conjunto de dados. Esta é a porcentagem de dados que mudam todos os dias. É crucial ter uma boa compreensão de quão dinâmicos são seus dados.

Por exemplo:

- Tamanho do conjunto de dados primário = 5 TB
- Taxa de variação diária = 5% (0,05)
- Eficiência de desduplicação e compressão = 50% (0,50)

Agora, vamos analisar o cálculo:

- Calcular a taxa de alteração diária de dados:

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

- Calcule o total de dados alterados em 30 dias:

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

- Calcule o armazenamento total necessário:

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

- Aplique economias de desduplicação e compactação:

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

Resumo das necessidades de armazenamento

- Sem eficiência: seriam necessários **12,5 TB** para armazenar 30 dias de dados do cofre cibernético.
- Com 50% de eficiência: seriam necessários **6,25 TB** de armazenamento após desduplicação e compactação.

> Cópias de instantâneos podem ter sobrecarga adicional devido aos metadados, mas isso geralmente é mínimo.

> Se vários backups forem feitos por dia, ajuste o cálculo pelo número de cópias de Snapshot feitas a cada dia.

> Considere o crescimento dos dados ao longo do tempo para garantir que o dimensionamento seja à prova do futuro.

Criando um cofre cibernético com ONTAP

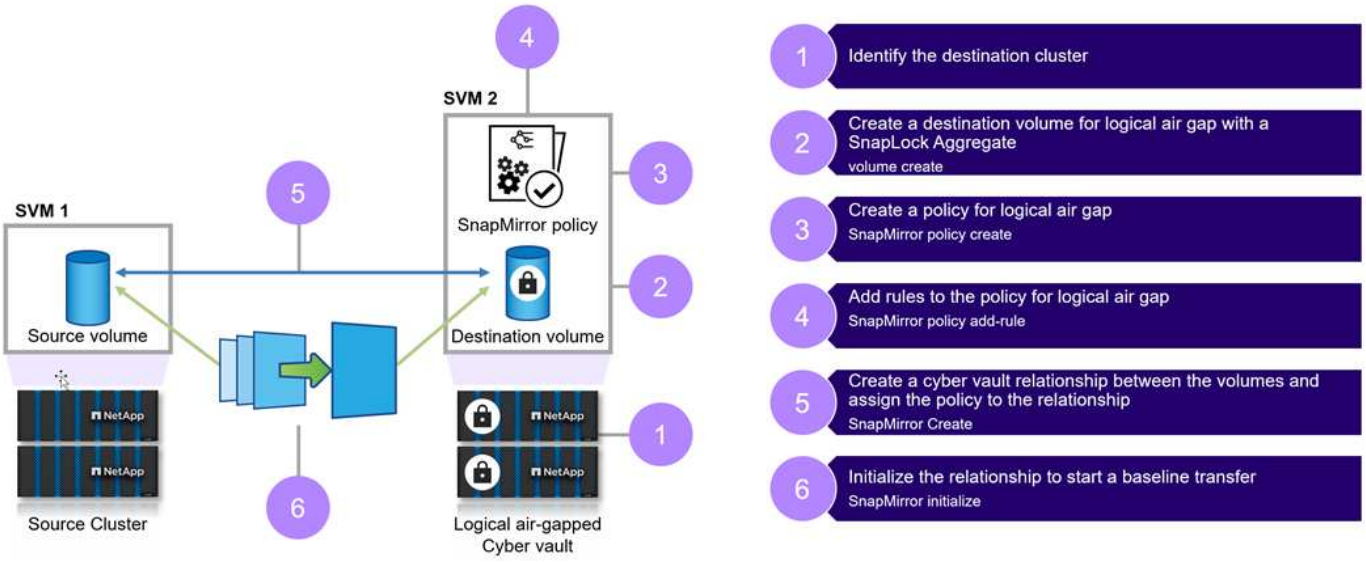
As etapas abaixo ajudarão na criação de um cofre cibernético com o ONTAP.

Antes de começar

- O cluster de origem deve estar executando o ONTAP 9 ou posterior.
- Os agregados de origem e destino devem ser de 64 bits.
- Os volumes de origem e destino devem ser criados em clusters pareados com SVMs pareadas. Para obter mais informações, consulte "Cluster Peering" .
- Se o crescimento automático de volume estiver desabilitado, o espaço livre no volume de destino deverá ser pelo menos cinco por cento maior que o espaço usado no volume de origem.

Sobre esta tarefa

A ilustração a seguir mostra o procedimento para inicializar um relacionamento de cofre de SnapLock Compliance :



Passos

1. Identifique a matriz de destino que se tornará o cofre cibernético para receber os dados isolados.
2. Na matriz de destino, para preparar o cofre cibernético,"instalar a licença ONTAP One" ,"inicializar o Relógio de Conformidade" , e, se você estiver usando uma versão do ONTAP anterior à 9.10.1,"criar um agregado de SnapLock Compliance" .
3. Na matriz de destino, crie um volume de destino SnapLock Compliance do tipo DP:

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

4. A partir do ONTAP 9.10.1, volumes SnapLock e não SnapLock podem existir no mesmo agregado; portanto, você não precisa mais criar um agregado SnapLock separado se estiver usando o ONTAP 9.10.1. Você usa o volume `-snaplock-type` opção para especificar um tipo de conformidade. Em versões do ONTAP anteriores ao ONTAP 9.10.1, o modo SnapLock e a conformidade são herdados do agregado. Volumes de destino com versão flexível não são suportados. A configuração de idioma do volume de destino deve corresponder à configuração de idioma do volume de origem.

   O comando a seguir cria um volume de SnapLock Compliance de 2 GB denominado `dstvolB` em `SVM2` no agregado `node01_aggr` :

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

5. No cluster de destino, para criar o air-gap, defina o período de retenção padrão, conforme descrito em"Defina o período de retenção padrão" . Um volume SnapLock que é um destino de cofre tem um período de retenção padrão atribuído a ele. O valor para esse período é inicialmente definido como um mínimo de 0 anos e um máximo de 100 anos (começando com o ONTAP 9.10.1. Para versões anteriores do ONTAP , o valor é de 0 a 70.) para volumes de SnapLock Compliance . Cada cópia do NetApp Snapshot é confirmada inicialmente com esse período de retenção padrão. O período de retenção padrão deve ser alterado. O período de retenção pode ser estendido posteriormente, se necessário, mas nunca encurtado. Para obter mais informações, consulte "Visão geral do tempo de retenção definido" .

Os provedores de serviços devem considerar as datas de término do contrato do cliente ao determinar o período de retenção. Por exemplo, se o período de retenção do cofre cibernético for de 30 dias e o contrato do cliente terminar antes do período de retenção expirar, os dados no cofre cibernético não poderão ser excluídos até que o período de retenção expire.

6. "Criar um novo relacionamento de replicação"entre a origem não SnapLock e o novo destino SnapLock que você criou na Etapa 3.

   Este exemplo cria um novo relacionamento SnapMirror com o volume SnapLock de destino dstvolB usando uma política de XDPDefault para armazenar cópias de Snapshot rotuladas diariamente e semanalmente em uma programação horária:

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

   "Crie uma política de replicação personalizada"ou um"agendamento personalizado" se os padrões disponíveis não forem adequados.

7. No SVM de destino, inicialize o relacionamento SnapVault criado na Etapa 5:

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

8. O comando a seguir inicializa o relacionamento entre o volume de origem srcvolA no SVM1 e o volume de destino dstvolB no SVM2:

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

9. Depois que o relacionamento for inicializado e ficar ocioso, use o comando snapshot show no destino para verificar o tempo de expiração do SnapLock aplicado às cópias replicadas do Snapshot.

   Este exemplo lista as cópias do Snapshot no volume dstvolB que têm o rótulo SnapMirror e a data de expiração do SnapLock :

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

Fortalecimento do cofre cibernético

Estas são recomendações adicionais para proteger um cofre cibernético ONTAP . Consulte o guia de proteção ONTAP abaixo para obter mais recomendações e procedimentos.

Recomendações para o reforço do cofre cibernético

- Isole os planos de gerenciamento do cofre cibernético
- Não habilite LIFs de dados no cluster de destino, pois eles são um vetor de ataque adicional
- No cluster de destino, limite o acesso LIF entre clusters ao cluster de origem com uma política de serviço
- Segmente o LIF de gerenciamento no cluster de destino para acesso limitado com uma política de serviço e um host bastião

- Restringir todo o tráfego de dados do cluster de origem para o cofre cibernético para permitir apenas as portas necessárias para o tráfego do SnapMirror
- Sempre que possível, desabilite quaisquer métodos de acesso de gerenciamento desnecessários no ONTAP para diminuir a superfície de ataque
- Habilitar registro de auditoria e armazenamento remoto de logs
- Habilitar verificação de vários administradores e exigir verificação de um administrador fora dos seus administradores de armazenamento regulares (por exemplo, equipe CISO)
- Implementar controles de acesso baseados em funções
- Exigir autenticação administrativa multifator para o System Manager e ssh
- Use autenticação baseada em token para scripts e chamadas de API REST

Por favor, consulte o"Guia de endurecimento ONTAP" ,"Visão geral da verificação de vários administradores" e"Guia de autenticação multifator ONTAP" para saber como realizar essas etapas de endurecimento.

Interoperabilidade do cofre cibernético

O hardware e o software ONTAP podem ser usados para criar uma configuração de cofre cibernético.

Recomendações de hardware ONTAP

Todos os conjuntos físicos unificados do ONTAP podem ser usados para uma implementação de cofre cibernético.

- O armazenamento híbrido FAS oferece a solução mais econômica.
- A Série C da AFF oferece o consumo de energia e a densidade mais eficientes.
- A AFF A-Series é a plataforma de melhor desempenho que oferece o melhor RTO. Com o recente anúncio da nossa mais recente série AFF A, esta plataforma oferecerá a melhor eficiência de armazenamento sem comprometer o desempenho.

Recomendações de software ONTAP

A partir do ONTAP 9.14.1, você pode especificar períodos de retenção para rótulos SnapMirror específicos na política SnapMirror do relacionamento SnapMirror para que as cópias replicadas do Snapshot do volume de origem para o volume de destino sejam retidas pelo período de retenção especificado na regra. Se nenhum período de retenção for especificado, o período de retenção padrão do volume de destino será usado.

A partir do ONTAP 9.13.1, você pode restaurar instantaneamente uma cópia bloqueada do Snapshot no volume SnapLock de destino de um relacionamento de cofre SnapLock criando um FlexClone com a opção snaplock-type definida como "não snaplock" e especificando a cópia do Snapshot como o "instantâneo pai" ao executar a operação de criação de clone de volume. Saiba mais sobre "criando um volume FlexClone com um tipo SnapLock" .

Configuração do MetroCluster

Para configurações do MetroCluster , você deve estar ciente do seguinte:

- Você pode criar um relacionamento SnapVault somente entre SVMs de origem de sincronização, não entre uma SVM de origem de sincronização e uma SVM de destino de sincronização.

- Você pode criar um relacionamento SnapVault de um volume em um SVM de origem de sincronização para um SVM de serviço de dados.
- Você pode criar um relacionamento SnapVault de um volume em um SVM de serviço de dados para um volume DP em um SVM de origem de sincronização.

Perguntas frequentes sobre o Cyber Vault

Estas perguntas frequentes são destinadas a clientes e parceiros da NetApp . Ele responde a perguntas frequentes sobre a arquitetura de referência do cofre cibernético baseado em ONTAP da NetApp.

O que é um cofre cibernético da NetApp ?

O cofre cibernético é uma técnica específica de proteção de dados que envolve o armazenamento de dados em um ambiente isolado, separado da infraestrutura primária de TI.

O cofre cibernético é um repositório de dados "isolado", imutável e indelével, imune a ameaças que afetam os dados primários, como malware, ransomware ou ameaças internas. Um cofre cibernético pode ser obtido com cópias imutáveis do NetApp ONTAP Snapshot e tornado indelével com o NetApp SnapLock Compliance. Enquanto estiver sob a proteção de SnapLock Compliance , os dados não podem ser modificados ou excluídos, nem mesmo pelos administradores do ONTAP ou pelo Suporte da NetApp .

Os backups com air-gapping usando métodos tradicionais envolvem a criação de espaço e a separação física das mídias primária e secundária. O air-gapping com cofre cibernético inclui o uso de uma rede de replicação de dados separada, fora das redes de acesso a dados padrão, para replicar cópias do Snapshot para um destino indelével.

Outros passos além das redes isoladas envolvem desabilitar todos os protocolos de acesso e replicação de dados no cofre cibernético quando eles não são necessários. Isso evita o acesso ou a exfiltração de dados no site de destino. Com o SnapLock Compliance, a separação física não é necessária. O SnapLock Compliance protege suas cópias de Snapshot em cofre, em um ponto específico no tempo e somente leitura, resultando em recuperação rápida de dados, seguras contra exclusão e imutáveis.

Abordagem da NetApp para cofre cibernético

O NetApp Cyber Vault, com tecnologia SnapLock, fornece às organizações uma solução abrangente e flexível para proteger seus ativos de dados mais críticos. Ao aproveitar as tecnologias de proteção do ONTAP, a NetApp permite que você crie um cofre cibernético seguro, isolado e com isolamento, imune a ameaças cibernéticas em evolução. Com a NetApp, você pode garantir a confidencialidade, a integridade e a disponibilidade dos seus dados, mantendo a agilidade e a eficiência da sua infraestrutura de armazenamento.

Os principais recursos da arquitetura de referência da NetApp para um cofre cibernético incluem:

- Infraestrutura de armazenamento segura e isolada (por exemplo, sistemas de armazenamento com isolamento de ar)
- As cópias de segurança dos seus dados são imutáveis e indeléveis
- Controles de acesso rigorosos e separados, verificação de vários administradores e autenticação multifator
- Capacidades de restauração rápida de dados

Perguntas frequentes sobre o Cyber Vault

O Cyber Vault é um produto da NetApp?

Não, "cyber vault" é um termo que abrange todo o setor. A NetApp criou uma arquitetura de referência para facilitar aos clientes a criação de seus próprios cofres cibernéticos e o aproveitamento de dezenas de recursos de segurança do ONTAP para ajudar a proteger seus dados contra ameaças cibernéticas. Mais informações estão disponíveis em"Site de documentação do ONTAP" .

O Cyber Vault com NetApp é apenas outro nome para LockVault ou SnapVault?

LockVault era um recurso do Data ONTAP 7-mode que não está disponível nas versões atuais do ONTAP.

SnapVault era um termo antigo para o que agora é realizado com a política de cofre do SnapMirror. Esta política permite que o destino retenha uma quantidade diferente de cópias do Snapshot do volume de origem.

O Cyber Vault usa o SnapMirror com a política de cofre e o SnapLock Compliance juntos para criar uma cópia imutável e indelével dos dados.

Qual hardware NetApp posso usar para um cofre cibernético, FAS, flash de capacidade ou flash de desempenho?

Essa arquitetura de referência para proteção cibernética se aplica a todo o portfólio de hardware ONTAP . Os clientes podem usar as plataformas AFF Série A, AFF Série C ou FAS como cofre. Plataformas baseadas em flash fornecerão os tempos de recuperação mais rápidos, enquanto plataformas baseadas em disco fornecerão a solução mais econômica. Dependendo da quantidade de dados que estão sendo recuperados e se várias recuperações estão acontecendo em paralelo, o uso de sistemas baseados em disco (FAS) pode levar dias ou semanas para ser concluído. Consulte um representante da NetApp ou parceiro para dimensionar adequadamente uma solução de cofre cibernético para atender aos requisitos do negócio.

Posso usar o Cloud Volumes ONTAP como uma fonte de cofre cibernético?

Sim, no entanto, usar o CVO como fonte exige que os dados sejam replicados para um destino de cofre cibernético local, pois a SnapLock Compliance é um requisito para um cofre cibernético ONTAP . A replicação de dados de uma instância CVO baseada em hiperescalador pode incorrer em cobranças de saída.

Posso usar o Cloud Volumes ONTAP como um destino de cofre cibernético?

A arquitetura do Cyber Vault depende da indelével conformidade do SnapLock da ONTAP e foi projetada para implementações locais. Arquiteturas de Cyber Vault baseadas em nuvem estão sob investigação para publicação futura.

Posso usar o ONTAP Select como uma fonte de cofre cibernético?

Sim, o ONTAP Select pode ser usado como uma fonte para um destino de cofre cibernético baseado em hardware local.

Posso usar o ONTAP Select como destino de cofre cibernético?

Não, o ONTAP Select não deve ser usado como destino de cofre cibernético, pois não tem a capacidade de usar o SnapLock Compliance.

Um cofre cibernético com NetApp usa apenas o SnapMirror?

Não, uma arquitetura de cofre cibernético da NetApp aproveita muitos recursos do ONTAP para criar uma cópia de dados segura, isolada, protegida e protegida. Para mais informações sobre quais técnicas adicionais podem ser usadas, veja a próxima pergunta.

Existe alguma outra tecnologia ou configuração usada para o cofre cibernético?

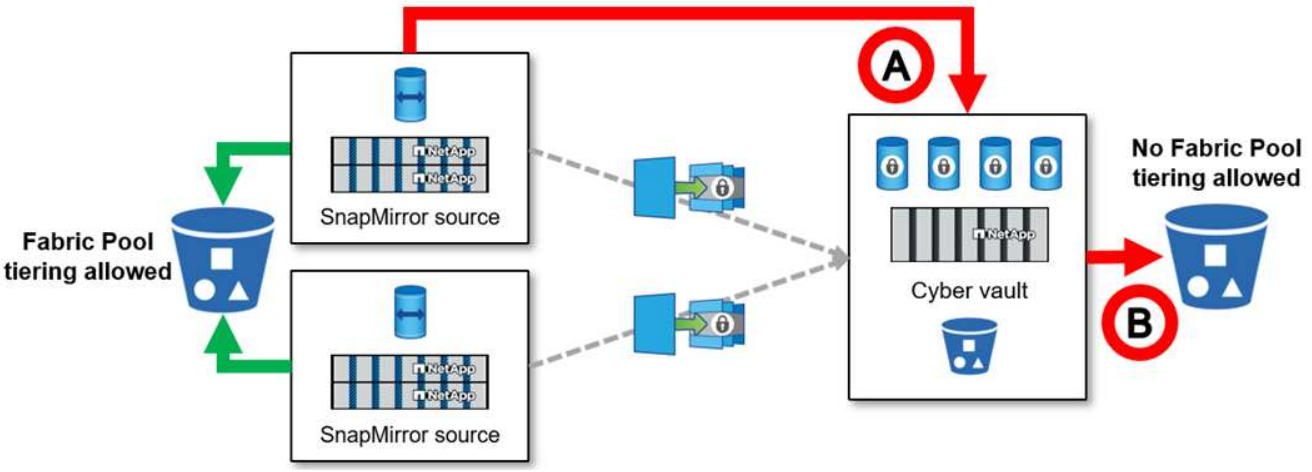
A base de um cofre cibernético da NetApp é a conformidade com SnapMirror e SnapLock Compliance, mas o uso de recursos ONTAP adicionais, como cópias de Snapshot à prova de violação, autenticação multifator (MFA), verificação de vários administradores, controle de acesso baseado em funções e registro de auditoria remota e local, melhora a segurança dos dados.

O que torna as cópias do ONTAP Snapshot melhores do que outras para um cofre cibernético?

As cópias do ONTAP Snapshot são imutáveis por padrão e podem se tornar indeléveis com o SnapLock Compliance. Nem mesmo o suporte da NetApp consegue excluir as cópias do SnapLock Snapshot. A melhor pergunta a se fazer é o que torna o NetApp Cyber Vault melhor do que outros Cyber Vaults do setor. Primeiro, o ONTAP é o armazenamento mais seguro do planeta e obteve a validação do CSfC, que permite o armazenamento de dados secretos e ultrassecretos em repouso nas camadas de hardware e software. Mais informações em"O CSfC pode ser encontrado aqui" . Além disso, o ONTAP pode ser isolado na camada de armazenamento, com o sistema de cofre cibernético controlando a replicação, permitindo que um espaço de ar seja criado dentro da rede de cofre cibernético.

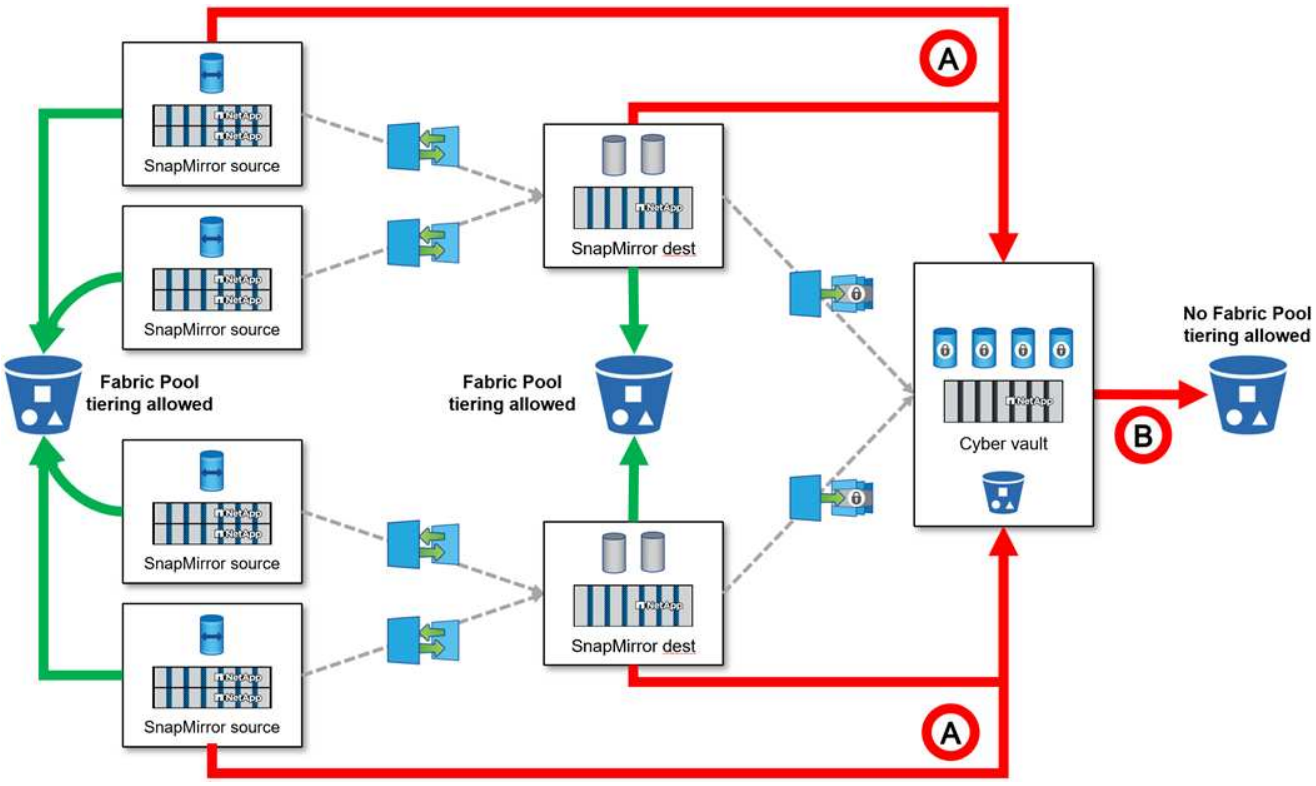
Um volume em um cofre cibernético pode usar o ONTAP Fabric Pool?

Não, um volume de cofre cibernético (destino SnapLock Compliance SnapMirror) não pode ser dividido em camadas usando o Fabric Pool, independentemente da política.



Existem vários cenários em que o pool Fabric **não pode** ser usado com um cofre cibernético.

1. As camadas frias do Fabric Pool **não podem** usar um cluster de cofre cibernético. Isso ocorre porque a ativação do protocolo S3 invalida a natureza segura da arquitetura de referência do cofre cibernético. Além disso, o bucket S3 usado para o pool de Fabric não pode ser protegido.
2. Os volumes de SnapLock Compliance no cofre cibernético **não podem** ser hierarquizados em um bucket S3, pois os dados estão bloqueados no volume.



O ONTAP S3 Worm está disponível em um cofre cibernético?

Não, o S3 é um protocolo de acesso a dados que invalida a natureza segura da arquitetura de referência.

O NetApp Cyber Vault é executado em uma personalidade ou perfil ONTAP diferente?

Não, é uma arquitetura de referência. Os clientes podem usar o"arquitetura de referência" e construir um cofre cibernético, ou pode usar o"Scripts do PowerShell para criar, proteger e validar" um cofre cibernético.

Posso ativar protocolos de dados como NFS, SMB e S3 em um cofre cibernético?

Por padrão, os protocolos de dados devem ser desabilitados no cofre cibernético para torná-lo seguro. No entanto, protocolos de dados podem ser habilitados no cofre cibernético para acessar dados para recuperação ou quando necessário. Isso deve ser feito temporariamente e desativado após a recuperação ser concluída.

É possível converter um ambiente SnapVault existente em um cofre cibernético ou é necessário redefinir tudo?

Sim. Poderíamos pegar um sistema que é um destino SnapMirror (com política de cofre), desabilitar os protocolos de dados, fortalecer o sistema conforme"Guia de endurecimento ONTAP" , isole-o em um local seguro e siga os outros procedimentos na arquitetura de referência para torná-lo um cofre cibernético sem precisar redefinir o destino.

Tem alguma dúvida adicional? Envie um e-mail para ng-cyber-vault@netapp.com com suas perguntas! Responderemos e adicionaremos suas perguntas às Perguntas Frequentes.

Recursos do cofre cibernético

Para saber mais sobre as informações descritas nestas informações do cofre cibernético, consulte as seguintes informações adicionais e conceitos de segurança.

- "NetApp Cyber Vault: Resumo de soluções de proteção de dados em várias camadas"
- "A NetApp recebeu a classificação AAA como a primeira solução de detecção de ransomware on-box baseada em IA do setor"
- "Aumente a resiliência cibernética com o armazenamento mais seguro do planeta"
- "Guia de reforço de segurança ONTAP"
- "Confiança Zero da NetApp"
- "Resiliência cibernética da NetApp"
- "Proteção de dados da NetApp"
- "Visão geral do peering de cluster e SVM com a CLI"
- "Arquivamento SnapVault"
- "Configurar, analisar, script cron"

Criação, reforço e validação de um cofre cibernético ONTAP com PowerShell

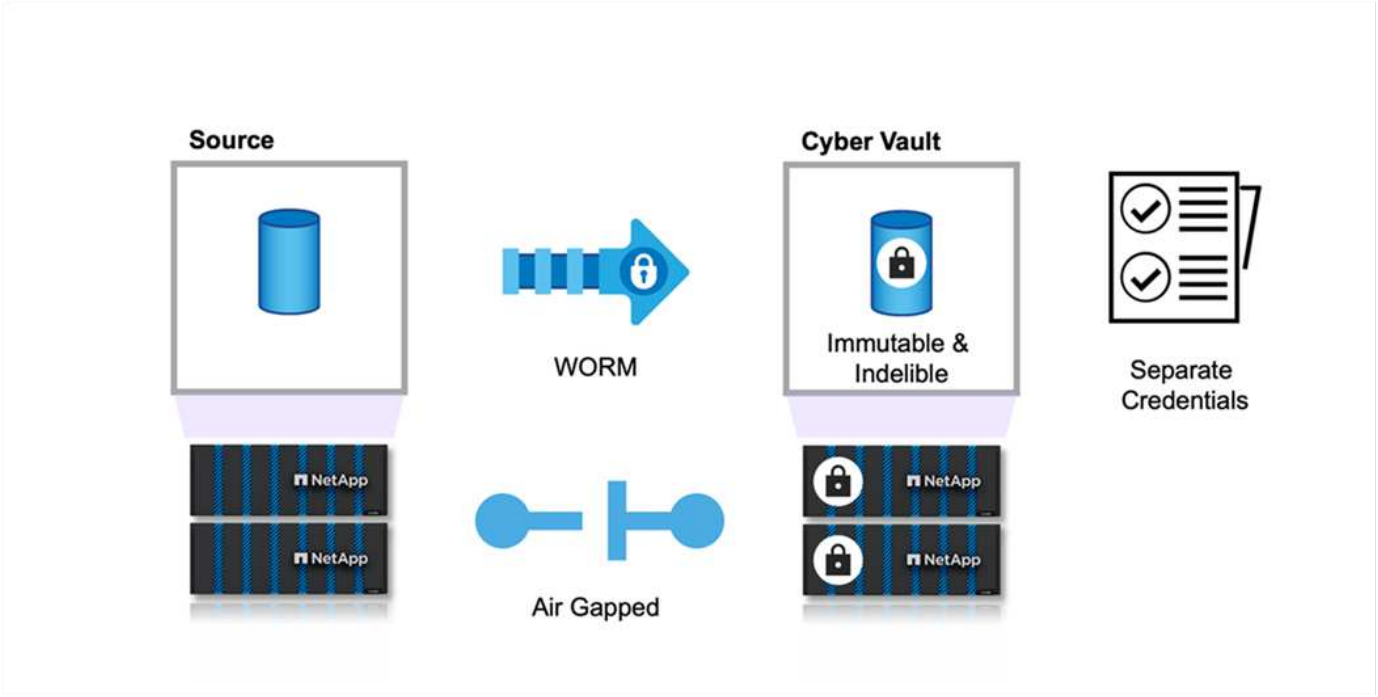
Visão geral do cofre cibernético ONTAP com PowerShell

No cenário digital atual, proteger os ativos de dados críticos de uma organização não é apenas uma prática recomendada, é um imperativo comercial. As ameaças cibernéticas estão evoluindo em um ritmo sem precedentes, e as medidas tradicionais de proteção de dados não são mais suficientes para manter as informações confidenciais seguras. É aí que entra um cofre cibernético. A solução de ponta baseada em ONTAP da NetApp combina técnicas avançadas de air-gapping com medidas robustas de proteção de dados para criar uma barreira impenetrável contra ameaças cibernéticas. Ao isolar os dados mais valiosos com tecnologia de proteção segura, um cofre cibernético minimiza a superfície de ataque para que os dados mais críticos permaneçam confidenciais, intactos e prontamente disponíveis quando necessário.

Um cofre cibernético é uma instalação de armazenamento segura que consiste em várias camadas de proteção, como firewalls, rede e armazenamento. Esses componentes protegem dados de recuperação vitais necessários para operações comerciais cruciais. Os componentes do cofre cibernético são sincronizados regularmente com os dados essenciais de produção com base na política do cofre, mas, de outra forma, permanecem inacessíveis. Essa configuração isolada e desconectada garante que, no caso de um ataque cibernético que comprometa o ambiente de produção, uma recuperação confiável e final possa ser facilmente realizada a partir do cofre cibernético.

O NetApp permite a criação fácil de um air-gap para o cofre cibernético configurando a rede, desabilitando LIFs, atualizando regras de firewall e isolando o sistema de redes externas e da Internet. Essa abordagem robusta desconecta efetivamente o sistema de redes externas e da Internet, fornecendo proteção incomparável contra ataques cibernéticos remotos e tentativas de acesso não autorizado, tornando o sistema imune a ameaças e intrusões baseadas na rede.

Combinando isso com a proteção SnapLock Compliance , os dados não podem ser modificados ou excluídos, nem mesmo pelos administradores do ONTAP ou pelo Suporte da NetApp . O SnapLock é auditado regularmente de acordo com as regulamentações da SEC e da FINRA, garantindo que a resiliência dos dados atenda a essas rigorosas regulamentações de WORM e retenção de dados do setor bancário. O NetApp é o único armazenamento empresarial validado pela NSA CSfC para armazenar dados ultrassecretos.



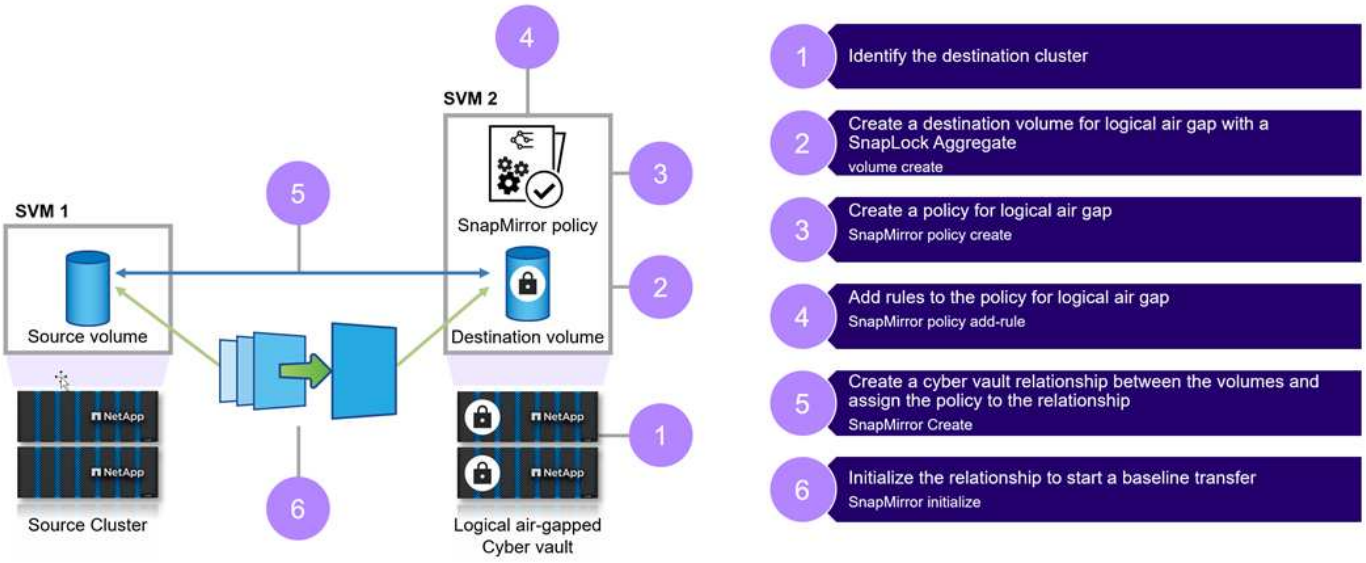
Este documento descreve a configuração automatizada do cofre cibernético da NetApp para armazenamento ONTAP local para outro armazenamento ONTAP designado com instantâneos imutáveis, adicionando uma camada extra de proteção contra ataques cibernéticos crescentes para recuperação rápida. Como parte dessa arquitetura, toda a configuração é aplicada de acordo com as melhores práticas do ONTAP . A última seção contém instruções para executar uma recuperação em caso de ataque.

A mesma solução é aplicável para criar o cofre cibernético designado na AWS usando o FSx ONTAP.

Etapas de alto nível para criar um cofre cibernético ONTAP

- Criar relacionamento de peering
  - O site de produção que usa o armazenamento ONTAP é pareado com o armazenamento ONTAP do cofre cibernético designado
- Criar volume de SnapLock Compliance
- Configurar relacionamento e regra do SnapMirror para definir rótulo
  - O relacionamento SnapMirror e os cronogramas apropriados são configurados
- Defina retenções antes de iniciar a transferência do SnapMirror (cofre)
  - O bloqueio de retenção é aplicado aos dados copiados, o que os previne ainda mais contra qualquer acesso interno ou falha de dados. Com isso, os dados não podem ser excluídos antes do término do período de retenção
  - As organizações podem manter esses dados por algumas semanas/meses, dependendo de suas necessidades
- Inicializar o relacionamento SnapMirror com base em rótulos
  - A semeadura inicial e a transferência incremental permanente ocorrem com base no cronograma do SnapMirror
  - Os dados são protegidos (imutáveis e indeléveis) com a conformidade SnapLock e estão disponíveis para recuperação

- Implementar controles rigorosos de transferência de dados
  - O cofre cibernético é desbloqueado por um período limitado com dados do site de produção e é sincronizado com os dados no cofre. Uma vez concluída a transferência, a conexão é desconectada, fechada e bloqueada novamente
- Recuperação rápida
  - Se o primário for afetado no local de produção, os dados do cofre cibernético serão recuperados com segurança para a produção original ou para outro ambiente escolhido



Componentes da solução

NetApp ONTAP executando 9.15.1 em clusters de origem e destino.

ONTAP One: licença completa do NetApp ONTAP.

Recursos usados da licença ONTAP One:

- SnapLock Compliance
- SnapMirror
- Verificação de vários administradores
- Todos os recursos de proteção expostos pelo ONTAP
- Credenciais RBAC separadas para cofre cibernético

> Todos os conjuntos físicos unificados ONTAP podem ser usados para um cofre cibernético, no entanto, os sistemas flash baseados em capacidade da série C da AFF e os sistemas flash híbridos da FAS são as plataformas ideais mais econômicas para essa finalidade. Por favor consulte o"Dimensionamento do cofre cibernético ONTAP" para orientação de dimensionamento.

Criação de cofre cibernético ONTAP com PowerShell

Os backups com air-gapping que usam métodos tradicionais envolvem a criação de espaço e a separação física das mídias primária e secundária. Ao mover a mídia para

outro local e/ou cortar a conectividade, os criminosos não têm acesso aos dados. Isso protege os dados, mas pode levar a tempos de recuperação mais lentos. Com o SnapLock Compliance, a separação física não é necessária. O SnapLock Compliance protege cópias somente leitura e de ponto no tempo do snapshot armazenado, resultando em dados que são rapidamente acessíveis, protegidos contra exclusão ou indeléveis e protegidos contra modificação ou imutáveis.

Pré-requisitos

Antes de iniciar as etapas da próxima seção deste documento, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O cluster de origem deve estar executando o ONTAP 9 ou posterior.
- Os agregados de origem e destino devem ser de 64 bits.
- Os clusters de origem e destino devem ser pareados.
- Os SVMs de origem e destino devem ser pareados.
- Certifique-se de que a criptografia de peering de cluster esteja habilitada.

Configurar transferências de dados para um cofre cibernético ONTAP requer várias etapas. No volume primário, configure uma política de instantâneo que especifique quais cópias criar e quando criá-las usando programações apropriadas e atribua rótulos para especificar quais cópias devem ser transferidas pelo SnapVault. No secundário, uma política SnapMirror deve ser criada para especificar os rótulos das cópias do Snapshot a serem transferidas e quantas dessas cópias devem ser mantidas no cofre cibernético. Depois de configurar essas políticas, crie o relacionamento SnapVault e estabeleça um cronograma de transferência.

Este documento pressupõe que o armazenamento primário e o cofre cibernético ONTAP designado já estejam configurados e instalados.

O cluster do Cyber Vault pode estar no mesmo data center ou em um data center diferente dos dados de origem.

Etapas para criar um cofre cibernético ONTAP

1. Use o ONTAP CLI ou o System Manager para inicializar o relógio de conformidade.
2. Crie um volume de proteção de dados com a conformidade com o SnapLock ativada.
3. Use o comando SnapMirror create para criar relacionamentos de proteção de dados do SnapVault .
4. Defina o período de retenção padrão de SnapLock Compliance para o volume de destino.

A retenção padrão é "Definida como mínima". Um volume SnapLock que é um destino de cofre tem um período de retenção padrão atribuído a ele. O valor para esse período é inicialmente definido como um mínimo de 0 anos e um máximo de 100 anos (começando com o ONTAP 9.10.1. Para versões anteriores do ONTAP , o valor é de 0 a 70.) para volumes de SnapLock Compliance . Cada cópia do NetApp Snapshot é confirmada inicialmente com esse período de retenção padrão. O período de retenção pode ser estendido posteriormente, se necessário, mas nunca encurtado. Para obter mais informações, consulte "Visão geral do tempo de retenção definido" .

O acima abrange etapas manuais. Especialistas em segurança aconselham automatizar o processo para

evitar o gerenciamento manual, que introduz grande margem de erro. Abaixo está o trecho de código que automatiza completamente os pré-requisitos e a configuração de conformidade do SnapLock e a inicialização do relógio.

Aqui está um exemplo de código do PowerShell para inicializar o relógio de conformidade do 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
    }
}
```

Aqui está um exemplo de código do PowerShell para configurar um cofre cibernético 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. Após a conclusão das etapas acima, o cofre cibernético isolado usando SnapLock Compliance e SnapVault estará pronto.

Antes de transferir dados do snapshot para o cyber vault, o relacionamento do SnapVault deve ser inicializado. No entanto, antes disso, é necessário executar o reforço da segurança para proteger o cofre.

Fortalecimento do cofre cibernético ONTAP com PowerShell

O cofre cibernético ONTAP oferece melhor resiliência contra ataques cibernéticos em comparação às soluções tradicionais. Ao projetar uma arquitetura para aumentar a segurança, é crucial considerar medidas para reduzir a área de superfície de ataque. Isso pode ser alcançado por meio de vários métodos, como implementar políticas de senhas reforçadas, habilitar o RBAC, bloquear contas de usuários padrão, configurar firewalls e utilizar fluxos de aprovação para quaisquer alterações no sistema de cofre. Além disso, restringir protocolos de acesso à rede de endereços IP específicos pode ajudar a limitar potenciais vulnerabilidades.

O ONTAP fornece um conjunto de controles que permitem proteger o armazenamento ONTAP . Use o"orientações e configurações para ONTAP" para ajudar a organização a atingir os objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade do sistema de informação.

Melhores práticas de proteção

Etapas manuais

1. Crie um usuário designado com função administrativa predefinida e personalizada.

2. Crie um novo IPspace para isolar o tráfego de rede.
3. Crie um novo SVM residindo no novo IPspace.
4. Garanta que as políticas de roteamento do firewall estejam configuradas corretamente e que todas as regras sejam auditadas e atualizadas regularmente, conforme necessário.

ONTAP CLI ou via script de automação

1. Proteja a administração com a Verificação Multiadministradora (MFA)
2. Habilite a criptografia para dados padrão "em trânsito" entre clusters.
3. SSH seguro com criptografia forte e imponha senhas seguras.
4. Habilitar FIPS global.
5. Telnet e Remote Shell (RSH) devem ser desabilitados.
6. Bloquear conta de administrador padrão.
7. Desabilite LIFs de dados e proteja pontos de acesso remoto.
8. Desabilite e remova protocolos e serviços não utilizados ou estranhos.
9. Criptografe o tráfego de rede.
10. Use o princípio do menor privilégio ao configurar funções de superusuário e administrativas.
11. Restrinja HTTPS e SSH de endereços IP específicos usando a opção de IP permitido.
12. Desative e retome a replicação com base no cronograma de transferência.

Os marcadores 1 a 4 precisam de intervenção manual, como designar uma rede isolada, segregar o espaço IP e assim por diante, e precisam ser executados previamente. Informações detalhadas para configurar o endurecimento podem ser encontradas em"Guia de reforço de segurança ONTAP" . O restante pode ser facilmente automatizado para fins de implantação e monitoramento. O objetivo dessa abordagem orquestrada é fornecer um mecanismo para automatizar as etapas de proteção para proteger o controlador do cofre no futuro. O período de tempo em que o cofre cibernético fica aberto é o mais curto possível. O SnapVault utiliza a tecnologia incremental para sempre, que moverá apenas as alterações desde a última atualização para o cofre cibernético, minimizando assim o tempo que o cofre cibernético deve permanecer aberto. Para otimizar ainda mais o fluxo de trabalho, a abertura do cofre cibernético é coordenada com o cronograma de replicação para garantir a menor janela de conexão.

Aqui está um exemplo de código do PowerShell para proteger um controlador 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
    }
}
```

Validação do cofre cibernético ONTAP com PowerShell

Um cofre cibernético robusto deve ser capaz de resistir a um ataque sofisticado, mesmo quando o invasor tem credenciais para acessar o ambiente com privilégios elevados.

Uma vez que as regras estejam em vigor, uma tentativa (assumindo que de alguma forma o invasor conseguiu entrar) de excluir um snapshot no lado do cofre falhará. O mesmo se aplica a todas as configurações de proteção, impondo as restrições necessárias e protegendo o sistema.

Exemplo de código do PowerShell para validar a configuração de forma programada.

```
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
    }
}
```

Esta captura de tela mostra que não há conexões no controlador do vault.

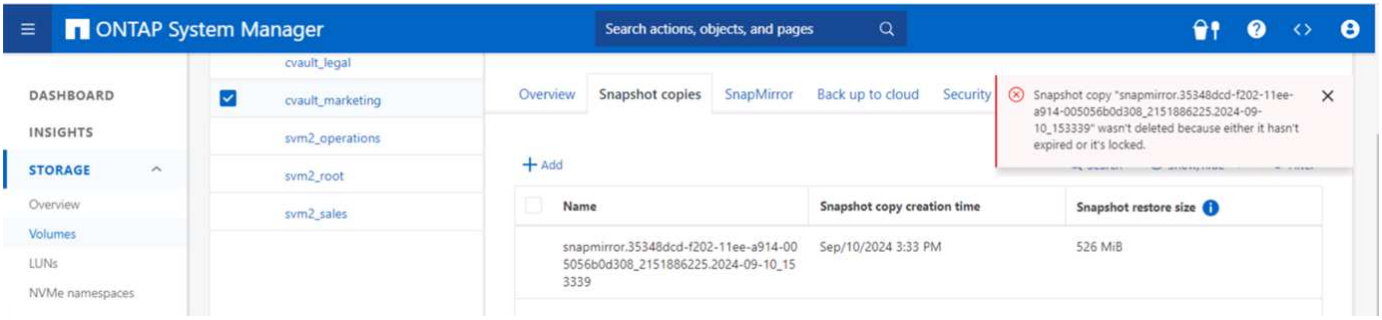
```
cluster2::> network connections  listening show
This table is currently empty.

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

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

cluster2::>
```

Esta captura de tela mostra que não há possibilidade de adulterar os instantâneos.



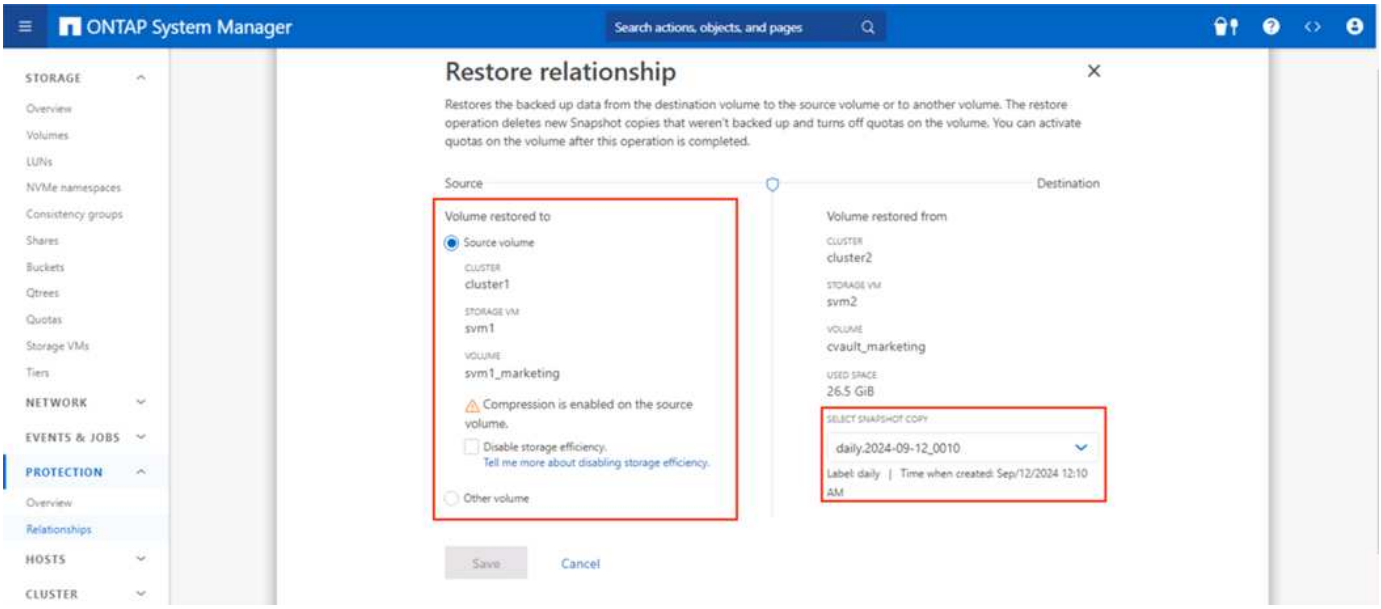
Para validar e confirmar a funcionalidade de air-gapping, siga as etapas abaixo:

- Teste os recursos de isolamento de rede e a capacidade de desativar uma conexão quando os dados não estiverem sendo transferidos.
- Verifique se a interface de gerenciamento não pode ser acessada de nenhuma entidade além dos endereços IP permitidos.
- A verificação de vários administradores está em vigor para fornecer uma camada adicional de aprovação.
- Validar a capacidade de acesso via CLI e REST API
- A partir da origem, acione uma operação de transferência para o cofre e garanta que a cópia em cofre não possa ser modificada.
- Tente excluir as cópias imutáveis do snapshot que são transferidas para o cofre.
- Tente modificar o período de retenção adulterando o relógio do sistema.

Recuperação de dados do cofre cibernético ONTAP

Se os dados forem destruídos no datacenter de produção, os dados do cofre cibernético podem ser recuperados com segurança no ambiente escolhido. Diferentemente de uma solução fisicamente isolada, o cofre cibernético ONTAP isolado é criado usando recursos nativos do ONTAP , como SnapLock Compliance e SnapMirror. O resultado é um processo de recuperação rápido e fácil de executar.

No caso de um ataque de ransomware e necessidade de recuperação do cofre cibernético, o processo de recuperação é simples e fácil, pois as cópias instantâneas armazenadas no cofre cibernético são usadas para restaurar os dados criptografados.



Se o requisito for fornecer um método mais rápido para colocar os dados novamente online quando necessário, valide, isole e analise rapidamente os dados para recuperação. Isso pode ser facilmente alcançado usando o FlexClone com a opção do tipo snaplock definida como tipo não snaplock.

> ⓘ A partir do ONTAP 9.13.1, a restauração de uma cópia bloqueada do Snapshot no volume SnapLock de destino de um relacionamento de cofre SnapLock pode ser restaurada instantaneamente criando um FlexClone com a opção snaplock-type definida como "não snaplock". Ao executar a operação de criação de clone de volume, especifique a cópia do Snapshot como "parent-snapshot". Mais informações sobre como criar um volume FlexClone com um tipo SnapLock"aqui."

> ⓘ Praticar procedimentos de recuperação do cofre cibernético garantirá que as etapas adequadas sejam estabelecidas para conectar-se ao cofre cibernético e recuperar dados. Planejar e testar o procedimento é essencial para qualquer recuperação durante um evento de ataque cibernético.

Considerações adicionais

Há considerações adicionais ao projetar e implantar um cofre cibernético baseado em ONTAP .

Considerações sobre dimensionamento de capacidade

A quantidade de espaço em disco necessária para um volume de destino do cofre cibernético ONTAP depende de vários fatores, sendo o mais importante a taxa de alteração dos dados no volume de origem. O agendamento de backup e o agendamento de instantâneo no volume de destino afetam o uso do disco no volume de destino, e a taxa de alteração no volume de origem provavelmente não será constante. É uma boa ideia fornecer um buffer de capacidade de armazenamento adicional acima daquela necessária para acomodar futuras mudanças no comportamento do usuário final ou do aplicativo.

Dimensionar um relacionamento para 1 mês de retenção no ONTAP requer o cálculo dos requisitos de armazenamento com base em vários fatores, incluindo o tamanho do conjunto de dados primário, a taxa de alteração de dados (taxa de alteração diária) e a economia com desduplicação e compactação (se aplicável).

Aqui está a abordagem passo a passo:

O primeiro passo é saber o tamanho do(s) volume(s) de origem que você está protegendo com o cofre cibernético. Essa é a quantidade base de dados que será inicialmente replicada para o destino do cofre cibernético. Em seguida, estime a taxa de alteração diária do conjunto de dados. Esta é a porcentagem de dados que mudam todos os dias. É crucial ter uma boa compreensão de quão dinâmicos são seus dados.

Por exemplo:

- Tamanho do conjunto de dados primário = 5 TB
- Taxa de variação diária = 5% (0,05)
- Eficiência de desduplicação e compressão = 50% (0,50)

Agora, vamos analisar o cálculo:

- Calcular a taxa de alteração diária de dados:

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

- Calcule o total de dados alterados em 30 dias:

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

- Calcule o armazenamento total necessário:

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

- Aplique economias de desduplicação e compactação:

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

Resumo das necessidades de armazenamento

- Sem eficiência: seriam necessários **12,5 TB** para armazenar 30 dias de dados do cofre cibernético.
- Com 50% de eficiência: seriam necessários **6,25 TB** de armazenamento após desduplicação e compactação.

Cópias de instantâneos podem ter sobrecarga adicional devido aos metadados, mas isso geralmente é mínimo.

Se vários backups forem feitos por dia, ajuste o cálculo pelo número de cópias de Snapshot feitas a cada dia.

Considere o crescimento dos dados ao longo do tempo para garantir que o dimensionamento seja à prova do futuro.

Impacto no desempenho no primário/fonte

Como a transferência de dados é uma operação pull, o impacto no desempenho do armazenamento primário pode variar dependendo da carga de trabalho, do volume de dados e da frequência dos backups. No entanto, o impacto geral no desempenho do sistema primário é geralmente moderado e gerenciável, pois a

transferência de dados é projetada para descarregar tarefas de proteção de dados e backup para o sistema de armazenamento do cofre cibernético. Durante a configuração inicial do relacionamento e o primeiro backup completo, uma quantidade significativa de dados é transferida do sistema primário para o sistema de cofre cibernético (o volume SnapLock Compliance). Isso pode levar ao aumento do tráfego de rede e da carga de E/S no sistema primário. Após a conclusão do backup completo inicial, o ONTAP só precisa rastrear e transferir os blocos que foram alterados desde o último backup. Isso resulta em uma carga de E/S muito menor em comparação à replicação inicial. Atualizações incrementais são eficientes e têm impacto mínimo no desempenho do armazenamento primário. O processo do vault é executado em segundo plano, o que reduz as chances de interferência nas cargas de trabalho de produção do sistema primário.

- Garantir que o sistema de armazenamento tenha recursos suficientes (CPU, memória e IOPs) para lidar com a carga adicional atenua o impacto no desempenho.

Configurar, analisar, script cron

A NetApp criou um"script único que pode ser baixado" e usado para configurar, verificar e agendar relacionamentos de cofre cibernético.

O que este script faz

- Peering de cluster
- Peering SVM
- Criação de volume DP
- Relacionamento e inicialização do SnapMirror
- Fortalecer o sistema ONTAP usado para o cofre cibernético
- Acalme-se e retome o relacionamento com base no cronograma de transferência
- Valide as configurações de segurança periodicamente e gere um relatório mostrando quaisquer anomalias

Como usar este script

"Baixe o script"e para usar o script, basta seguir os passos abaixo:

- Inicie o Windows PowerShell como administrador.
- Navegue até o diretório que contém o script.
- Execute o script usando `.\` sintaxe junto com os parâmetros necessários

> Por favor, certifique-se de que todas as informações foram inseridas. Na primeira execução (modo de configuração), ele solicitará credenciais para o sistema de produção e para o novo sistema de cofre cibernético. Depois disso, ele criará os peerings SVM (se não existirem), os volumes e o SnapMirror entre o sistema e os inicializará.

> O modo Cron pode ser usado para agendar a inatividade e a retomada da transferência de dados.

Modos de operação

O script de automação fornece 3 modos de execução - `configure` , `analyze` e `cron` .

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

- Configurar - Executa as verificações de validação e configura o sistema como air-gapped.
- Analisar - Recurso de monitoramento e relatórios automatizados para enviar informações aos grupos de monitoramento sobre anomalias e atividades suspeitas para garantir que as configurações não sejam desviadas.
- Cron - Para habilitar a infraestrutura desconectada, o modo cron automatiza a desativação do LIF e desativa o relacionamento de transferência.

Levará algum tempo para transferir os dados nos volumes selecionados, dependendo do desempenho dos sistemas e da quantidade de dados.

```
./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"
```

Conclusão da solução PowerShell do cofre cibernético ONTAP

Ao aproveitar o air-gapping com metodologias de proteção robustas fornecidas pelo ONTAP, a NetApp permite que você crie um ambiente de armazenamento seguro e isolado, resiliente contra ameaças cibernéticas em evolução. Tudo isso é realizado mantendo a agilidade e a eficiência da infraestrutura de armazenamento existente. Esse acesso seguro permite que as empresas atinjam suas metas rigorosas de segurança e tempo de atividade com alterações mínimas em sua estrutura atual de pessoas, processos e tecnologia.

O cofre cibernético ONTAP usa recursos nativos no ONTAP , uma abordagem fácil para proteção adicional para criar cópias imutáveis e indeléveis dos seus dados. Adicionar o cofre cibernético baseado em ONTAP da NetApp à postura geral de segurança irá:

- Crie um ambiente separado e desconectado das redes de produção e backup e restrinja o acesso dos usuários a ele.

Informações sobre direitos autorais

Informações sobre marcas comerciais