



Proteja seus dados

Amazon FSx for NetApp ONTAP

NetApp

February 11, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/workload-fsx-ontap/data-protection-overview.html> on February 11, 2026. Always check docs.netapp.com for the latest.

Índice

Proteja seus dados	1
Tipos de proteção de dados no NetApp Workload Factory	1
Tipos de proteção de dados	1
Práticas recomendadas para proteger seus dados de workload	2
Proteja os dados de workload com snapshots	2
Proteja os dados da sua carga de trabalho com a proteção autônoma contra ransomware da NetApp com IA	2
Proteger os dados de workload com replicação de volume	2
Proteja seus dados de workload com backups	3
Recomendações para proteger os dados de workload	3
Usar instantâneos	3
Crie um snapshot manual de um volume do FSX for ONTAP	3
Crie uma política de snapshot para VMs de armazenamento no Workload Factory	4
Restaurar um volume de um snapshot no Workload Factory	6
Use backups para armazenamento de objetos	7
Crie um backup manual de um volume no NetApp Workload Factory	7
Restaurar um volume de um backup no NetApp Workload Factory	7
Usar replicação	8
Crie um relacionamento de replicação no NetApp Workload Factory	8
Inicializar um relacionamento de replicação no NetApp Workload Factory	11
Proteja seus dados com a proteção autônoma contra ransomware da NetApp com IA	12
Habilitar ARP/AI para um sistema de arquivos ou um volume	13
Validar ataques de ransomware	15
Recuperar dados após um ataque de ransomware	15
Clonar um volume no NetApp Workload Factory	16
Use dados de cluster ONTAP local no NetApp Workload Factory	16
Descubra um cluster ONTAP no local	17
Replique dados de volume de um cluster ONTAP no local	18
Remover um cluster ONTAP local do NetApp Workload Factory	20
Proteja seus dados com um cofre cibernético.	20

Proteja seus dados

Tipos de proteção de dados no NetApp Workload Factory

O FSx para ONTAP oferece suporte a snapshots, NetApp Autonomous Ransomware Protection com IA, replicação e backups para proteção de dados. Recomendamos que você use uma combinação de tipos de proteção de dados para se preparar para o inevitável e proteger seus dados.

Tipos de proteção de dados

A proteção de dados para seus workloads ajuda a garantir que você se recupere de qualquer perda de dados a qualquer momento. Saiba mais sobre os tipos de proteção de dados antes de selecionar os recursos que você usará.

Instantâneos

Um instantâneo cria uma imagem pontual e somente leitura de um volume dentro do volume de origem como uma cópia instantânea. Você pode usar a cópia snapshot para recuperar arquivos individuais ou restaurar todo o conteúdo de um volume. Os instantâneos são a base de todos os métodos de backup. A cópia snapshot criada no volume é usada para manter o volume replicado e o arquivo de backup sincronizados com as alterações feitas no volume de origem.

Proteção autônoma contra ransomware da NetApp com IA

O NetApp Autonomous Ransomware Protection com IA (ARP/AI) usa análise de carga de trabalho em ambientes NAS (NFS/SMB) para detectar e alertar sobre atividades anormais que podem ser um ataque de ransomware. Quando há suspeita de ataque, o ARP/AI também cria novos snapshots imutáveis, além da proteção existente fornecida pelos snapshots agendados.

Replicação

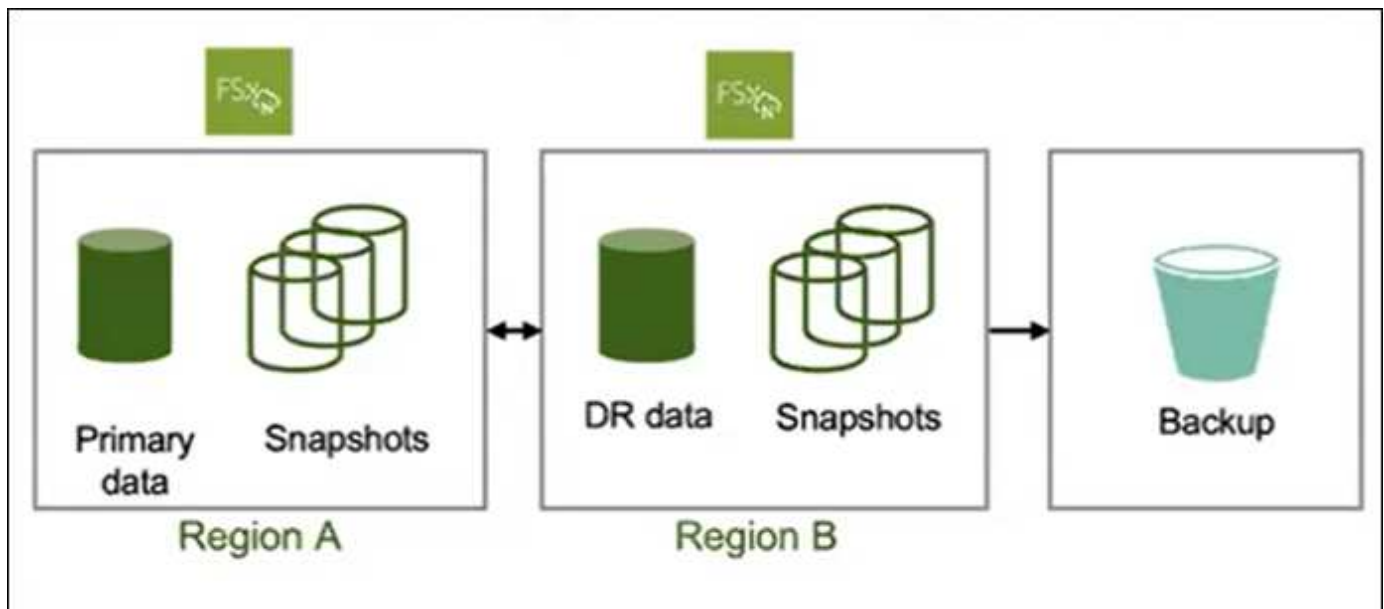
A replicação cria uma cópia secundária de seus dados em outro sistema de arquivos do FSX for ONTAP e atualiza continuamente os dados secundários. Seus dados permanecem atuais e disponíveis sempre que você precisar, como para recuperação de desastres.

Você pode optar por criar volumes replicados em outro sistema de arquivos do FSX for ONTAP e arquivos de backup na nuvem. Ou você pode escolher apenas criar volumes replicados ou arquivos de backup - é sua escolha.

Backups

Você pode criar backups de seus dados na nuvem para fins de proteção e retenção de longo prazo. Se necessário, você pode restaurar um volume, pasta ou arquivos individuais do backup para o mesmo sistema de arquivos em funcionamento ou diferente.

O diagrama a seguir mostra uma representação visual da proteção de dados do FSX for ONTAP storage usando snapshots, replicação entre regiões e backup para armazenamento de objetos.



Práticas recomendadas para proteger seus dados de workload

O FSX para ONTAP oferece várias opções de proteção de dados que podem ser combinadas para atingir seus objetivos de tempo e ponto de recuperação selecionados. Para obter a melhor proteção possível, recomendamos que você use snapshots de volume e backups de volume.

O objetivo do ponto de restauração (RPO) descreve como é garantida a cópia mais recente dos seus dados, o que depende da frequência com que as cópias são feitas. Um objetivo de tempo de recuperação (rto) define quanto tempo leva para restaurar seus dados.

Proteja os dados de workload com snapshots

Os instantâneos são versões virtuais pontuais de um volume que são tiradas de forma programada. Você pode acessar snapshots usando comandos padrão do sistema de arquivos. Os snapshots fornecem um RPO de apenas uma hora. O rto depende da quantidade de dados a serem restaurados e é limitado principalmente pelo limite de taxa de transferência de volume. Os instantâneos também permitem que os usuários restaurem arquivos e diretórios específicos, o que diminui o rto ainda mais. Os instantâneos consomem apenas espaço de volume adicional para alterações feitas no volume.

Proteja os dados da sua carga de trabalho com a proteção autônoma contra ransomware da NetApp com IA

A proteção autônoma contra ransomware da NetApp com IA (ARP/AI) atua como uma importante camada adicional de defesa caso o software antivírus não consiga detectar uma intrusão. Definir uma política de ARP/AI a habilita para todas as VMs de armazenamento e todos os volumes existentes e recém-criados. Uma vez ativado, o ARP/AI detecta e protege todos os volumes e VMs de armazenamento. Se uma extensão de arquivo for sinalizada como anormal, você deve avaliar o alerta.

Proteger os dados de workload com replicação de volume

A replicação de volume cria uma cópia dos dados mais recentes de um volume, incluindo todos os snapshots em uma região diferente. Se você não puder pagar RTOs de várias horas de uma operação de restauração de volume total a partir de um backup de volume, considere executar uma replicação de volume. Embora a replicação de volume garanta que os dados recentes estejam disponíveis em uma região diferente para você usar, você precisa ajustar seus clientes para usar o volume na outra região.

Proteja seus dados de workload com backups

Os backups de volume fornecem cópias pontuais e independentes do seu volume. Eles podem ser usados para armazenar backups antigos e fornecer a segunda cópia necessária de seus dados. As programações de backup diárias, semanais e mensais permitem RPOs a partir de um dia. Os backups de volume só podem ser restaurados como um todo. A criação de um volume a partir de um backup (rto) pode levar de horas a muitos dias, dependendo do tamanho do backup.

Recomendações para proteger os dados de workload

Considere as recomendações a seguir para proteger seus dados de workload.

- Use a replicação de volume para recuperação de desastres: se seu aplicativo exigir um RTO baixo, considere usar a replicação de volume para replicar seus dados para outra região.
- Usar backups de volume em conjunto com snapshots: Usar os dois recursos juntos garante que você seja capaz de restaurar seus arquivos de snapshots e realizar restaurações completas em caso de perda de volume usando backups.
- Definir uma política de backup de volume: Certifique-se de que a política de backup atenda aos requisitos da sua empresa para idade e frequência de backup. Recomendamos manter um mínimo de dois backups diários para cada volume.
- Definir uma programação de instantâneos: Os instantâneos mais antigos têm menos probabilidade de serem usados para restaurar dados. Recomendamos que você defina um agendamento de snapshot que leve em consideração os retornos decrescentes de manter snapshots antigos em relação ao custo para capacidade adicional de snapshot.
- Habilite uma política ARP/AI para seu sistema de arquivos ou volumes individuais para adicionar uma camada adicional de proteção para proteger seus dados contra ataques de ransomware.

Usar instantâneos

Crie um snapshot manual de um volume do FSX for ONTAP

Crie um snapshot manual de um volume FSx para ONTAP no NetApp Workload Factory. Snapshots são versões pontuais do conteúdo do seu volume.

Os snapshots são recursos de volumes e são capturas instantâneas de seus dados que consomem espaço apenas para dados modificados. Como os dados mudam com o tempo, os snapshots geralmente consomem mais espaço à medida que envelhecem.

O FSX para ONTAP volumes usa cópia-on-write just-in-time para que todos os arquivos não modificados em snapshots não consumam nenhuma capacidade do volume.




Os snapshots não são cópias de seus dados. Se você quiser fazer cópias de seus dados, considere usar os backups do FSX for ONTAP ou os recursos de replicação de volume.

Antes de começar

Você deve associar um link para criar um instantâneo manual de um volume. ["Aprenda como associar um link existente ou criar e associar um novo link"](#). Após os associados da ligação, volte a esta operação.

Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).

2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos que contém o volume para criar um snapshot e então selecione **Gerenciar**.
5. Na visão geral do sistema de arquivos, selecione a guia **volumes**.
6. Na aba **Volumes**, selecione o menu de ações para o volume a ser protegido com instantâneos.
7. Selecione **Ações de proteção de dados** e depois **Gerenciar instantâneos**.
8. Na página Gerenciar instantâneos, selecione **Criar instantâneo**.
9. Na caixa de diálogo Criar um instantâneo, faça o seguinte:
 - a. Digite um nome de instantâneo no campo **Nome do instantâneo**.
 - b. Opcionalmente, selecione um rótulo ou crie um novo rótulo.
 - c. Defina o **período de retenção** como um número de horas, dias, meses ou anos.
 - d. Opcional: **Torne este snapshot imutável** para evitar que ele seja excluído durante o período de retenção.

Aceite a declaração sobre snapshots imutáveis.
10. Selecione **criar**.

Crie uma política de snapshot para VMs de armazenamento no Workload Factory

Crie uma política de snapshot personalizada para VMs de armazenamento no Workload Factory para gerenciar a criação e a retenção de snapshots. Uma política de snapshot define como o sistema cria snapshots para uma VM de armazenamento. Você pode criar uma política de snapshot para uma VM de armazenamento em um sistema de arquivos FSx para ONTAP . Você também pode compartilhar a política entre várias VMs de armazenamento.

Sobre esta tarefa

Você pode criar uma política de snapshot personalizada que difere das três políticas de snapshot internas do FSX for ONTAP:

- `default`
- `default-1weekly`
- `none`

Por padrão, cada volume está associado à política de snapshot do sistema de arquivos `default`. Recomendamos o uso desta política para a maioria das cargas de trabalho.


A personalização de uma política permite especificar quando criar snapshots, quantas cópias devem ser mantidas e como nomeá-las.

Antes de começar

- Depois que uma política de snapshot é criada, sua associação com as VM de armazenamento não pode ser modificada, mas você sempre pode adicionar ou remover a política de volumes.

- Considere o seguinte sobre a capacidade de snapshot antes de usar snapshots:
 - Para a maioria dos conjuntos de dados, uma capacidade adicional de 20% é suficiente para manter snapshots por até quatro semanas. À medida que os dados envelhecem, o uso delas para restaurações torna-se menos provável.
 - A substituição de todos os dados em um snapshot consome capacidade de volume significativa, o que depende do provisionamento da capacidade do volume.
- Para criar uma política de snapshot personalizada, você deve associar um link. ["Aprenda como associar um link existente ou criar e associar um novo link"](#). Após os associados da ligação, volte a esta operação.

Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos com o volume e, em seguida, selecione **Gerenciar**.
5. Na visão geral do sistema de arquivos, selecione a guia **Storage VMs**.
6. Na guia **VMs de armazenamento**, selecione o menu de ações do volume a ser protegido com instantâneos agendados, depois **Ações avançadas** e, por fim, **Gerenciar políticas de instantâneos**.
7. Na página de gerenciamento de políticas de instantâneos, selecione **criar política de instantâneos**.
8. No campo **Nome da política de instantâneo**, insira um nome para a política de instantâneo.
9. Opcionalmente, insira uma descrição para a política de snapshot.
10. Em **Policy schedule e copies**, selecione quando criar snapshots. Por exemplo, a cada minuto ou hora.

Pode selecionar mais de uma frequência.
11. Em **número de cópias**, introduza o número de cópias a reter.

O número máximo de cópias é 1.023.
12. Opcional: Em **convenção de nomenclatura**, insira um **prefixo** para a política.
13. **Etiqueta de retenção** é preenchida automaticamente.

Este rótulo refere-se ao SnapMirror, ou rótulo de replicação que é usado para selecionar somente snapshots especificados para replicação da origem para o sistema de arquivos de destino.
14. Opcional: Ative **instantâneos imutáveis** para qualquer horário que você precisar, defina o **período de retenção** para cada horário e aceite a instrução para continuar.

A ativação de instantâneos imutáveis bloqueia todos os instantâneos nesta política de instantâneos para impedir que os instantâneos sejam excluídos durante o período de retenção.
15. **Compartilhar entre VMs de armazenamento**: Habilitado por padrão. Quando ativada, a política de snapshot é compartilhada em todas as VMs de armazenamento no sistema de arquivos. Desative para criar uma política de snapshot para uma única VM de armazenamento.
16. Selecione **criar**.

Restaurar um volume de um snapshot no Workload Factory

No Workload Factory, você pode restaurar dados de um instantâneo para um volume existente ou para um novo volume. A operação de restauração permite a recuperação em um determinado momento quando um volume contém arquivos excluídos ou corrompidos.

Sobre esta tarefa

Você tem a opção de restaurar dados de um instantâneo para um volume existente ou para um novo volume.


A criação de um novo volume a partir de um instantâneo faz uma cópia de um volume inteiro em poucos segundos, independentemente do tamanho do volume. A cópia recém-criada representa um novo volume.

Antes de começar

Considere as seguintes limitações antes de criar um volume a partir de um instantâneo:

- Só é possível restaurar um volume a partir de um instantâneo se tiver uma cópia instantânea existente do volume.
- Alterações nos modelos de permissão: Se você usar essa operação para alternar o tipo de protocolo nas (Network-Attached Storage), ela também pode alternar o modelo de permissão fornecido pelo estilo de segurança. Você pode ter problemas de permissão de acesso a arquivos, que você só pode corrigir manualmente com acesso de administrador usando as ferramentas de cliente nas para configuração de permissões.

Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos com o volume e, em seguida, selecione **Gerenciar**.
5. Na visão geral do sistema de arquivos, selecione a guia **volumes**.
6. Na guia **Volumes**, selecione o menu de ações para o volume a ser restaurado a partir de um instantâneo.
7. Selecione **Ações de proteção de dados** e depois **Gerenciar instantâneos**.
8. Na página Gerenciar instantâneos, selecione o menu de ações do instantâneo a ser restaurado e, em seguida, selecione **Restaurar**.
9. Na caixa de diálogo Restaurar volume de um instantâneo, selecione entre as seguintes opções:
 - Alterne para selecionar **Restaurar como um novo volume**.

No campo **Nome do volume restaurado**, insira um nome exclusivo para o volume a ser restaurado.
 - Restaurar dados de um instantâneo para um volume existente. Esta operação exclui permanentemente quaisquer dados que foram modificados após o momento da criação do instantâneo.

Aceite a declaração para prosseguir.
10. Selecione **Restaurar**.

Use backups para armazenamento de objetos

Crie um backup manual de um volume no NetApp Workload Factory

Crie um backup manual de um volume fora dos backups agendados regularmente no NetApp Workload Factory.

Sobre esta tarefa


Os backups do FSX para ONTAP são por volume, portanto, cada backup contém apenas os dados em um determinado volume.

Os backups do FSX para ONTAP são incrementais, o que significa que apenas os dados no volume que foram alterados após o backup mais recente ser salvo. Isso minimiza o tempo necessário para criar o backup e o armazenamento necessários para o backup, o que economiza em custos de storage não duplicando dados.

Antes de começar

Para fazer backups de seus volumes, tanto o volume quanto o sistema de arquivos precisam ter capacidade de armazenamento SSD disponível suficiente para armazenar o snapshot de backup. Ao tirar um snapshot de backup, a capacidade de storage adicional consumida pelo snapshot não pode fazer com que o volume exceda 98% da utilização do storage SSD. Se isso acontecer, o backup falhará.

Passos


1. Inicie sessão utilizando uma das ["experiências de console"](#).
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos com o volume e, em seguida, selecione **Gerenciar**.
5. Na visão geral do sistema de arquivos, selecione a guia **volumes**.
6. Na aba **Volumes**, selecione o botão de ação do volume para fazer backup.
7. Selecione **ações de proteção de dados, FSX for ONTAP backup** e, em seguida, **Backup manual**.
8. Na caixa de diálogo cópia de segurança manual, introduza um nome para a cópia de segurança.
9. Selecione **Backup**.

Restaurar um volume de um backup no NetApp Workload Factory

No NetApp Workload Factory, você pode restaurar um volume de um backup para qualquer sistema de arquivos FSx for ONTAP na sua conta da AWS.

A fábrica de carga de trabalho determina se você tem capacidade suficiente para a restauração e pode adicionar automaticamente a capacidade da camada de storage SSD, caso não o faça.

Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.

4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos com o volume e, em seguida, selecione **Gerenciar**.
5. Na visão geral do sistema de arquivos, selecione a guia **volumes**.
6. Na aba **Volumes**, selecione o menu de ações para o volume a ser restaurado a partir de um backup.
7. Selecione **ações de proteção de dados, FSX for ONTAP backup** e, em seguida, **Restaurar a partir de um backup**.
8. Na caixa de diálogo Restaurar a partir de uma cópia de segurança, forneça o seguinte:
 - a. * Sistema de arquivos de destino*: Selecione o sistema de arquivos de destino no menu suspenso.
 - b. **Target storage VM**: Selecione a VM de armazenamento de destino no menu suspenso.
 - c. **Nome da cópia de segurança**: Selecione o nome da cópia de segurança no menu pendente.
 - d. **Nome do volume restaurado**: Insira o nome do volume restaurado.
9. Verifique a capacidade do sistema de arquivos para a operação de restauração.

Quando a capacidade do sistema de arquivos é limitada, pode ocorrer o seguinte:

- A restauração pode levar a capacidade utilizada além do limite especificado. Você pode concluir a operação de restauração. Considere ["Adicionar manualmente a capacidade da camada de storage SSD"](#) ou selecionar o Workload Factory para adicionar automaticamente a capacidade do nível de armazenamento SSD.
- A restauração requer capacidade SSD adicional. Você deve selecionar o Workload Factory para adicionar automaticamente a capacidade de armazenamento SSD para continuar.

10. Selecione **Restaurar**.

Usar replicação

Crie um relacionamento de replicação no NetApp Workload Factory

Crie uma relação de replicação para um sistema de arquivos FSx for ONTAP no NetApp Workload Factory para evitar perda de dados em caso de desastre imprevisto. A replicação é suportada entre dois sistemas de arquivos FSx for ONTAP e entre um sistema ONTAP local e um sistema de arquivos FSx for ONTAP.

Sobre esta tarefa

A replicação protege seus dados caso um desastre afete sua região.

Esta operação cria uma relação de replicação para volumes de origem em um sistema de arquivos FSx for ONTAP ou em um sistema ONTAP local.

Os volumes replicados no sistema de arquivos de destino são volumes de proteção de dados (DP) e seguem o formato de nomenclatura: {OriginalVolumeName}_copy.

Ao replicar um volume de origem com arquivos imutáveis, o volume de destino e o sistema de arquivos permanecem bloqueados até que o período de retenção dos arquivos imutáveis no volume de origem termine. O recurso de arquivos imutáveis está disponível quando você ["criar um volume"](#) para um sistema de arquivos FSx for ONTAP.



- A replicação não é suportada para volumes em bloco que utilizam os protocolos iSCSI ou NVMe.
- É possível replicar um volume de origem (leitura/gravação) ou um volume de proteção de dados (DP). A replicação em cascata é compatível, mas um terceiro salto não é. Saiba mais ["replicação em cascata"](#) sobre o .


Antes de começar

Revise estes requisitos antes de começar.

- Você deve ter um sistema de arquivos FSx for ONTAP para usar como destino na relação de replicação.
- O sistema de arquivos FSx for ONTAP que você usa para a relação de replicação deve ter um link associado. ["Aprenda como associar um link existente ou criar e associar um novo link"](#). Depois de associar o link, retorne a esta operação.
- Para replicação de um sistema ONTAP local para um sistema de arquivos FSx for ONTAP, certifique-se de ter descoberto o sistema ONTAP local.

Siga estes passos para replicar volumes específicos ou todos os volumes em um sistema de arquivos.

Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos que contém o(s) volume(s) a ser(em) replicado(s) e, em seguida, selecione **Gerenciar**.
5. Replique todos os volumes em um sistema de arquivos ou replique volumes selecionados.
 - Para replicar todos os volumes em um sistema de arquivos: Na visão geral do sistema de arquivos, selecione **replique dados**.
 - Para replicar volumes selecionados: Na visão geral do sistema de arquivos, selecione a guia **volumes**.

Na tabela volumes, selecione um ou mais volumes e, em seguida, selecione **replique dados**.
6. Na página replicar dados, em destino replicação, forneça o seguinte:
 - a. **Caso de uso:** Selecione um dos seguintes casos de uso para a replicação. Dependendo do caso de uso selecionado, o Workload Factory preenche o formulário com valores recomendados de acordo com as melhores práticas. Você pode aceitar os valores recomendados ou fazer alterações à medida que preenche o formulário.
 - Migração: Transfere seus dados para o sistema de arquivos FSX for ONTAP de destino
 - Recuperação de desastres quentes: Garante alta disponibilidade e recuperação rápida de desastres para cargas de trabalho críticas
 - Recuperação de desastres fria ou arquivada:
 - Recuperação de desastres inativos: Usa objetivos de tempo de recuperação (rto) mais longos e objetos de ponto de recuperação (RPO) para reduzir custos
 - Arquivamento: Replica dados para storage e conformidade de longo prazo
 - Outros

Além disso, a seleção de caso de uso determina a política de replicação ou a política de SnapMirror (ONTAP). Os termos usados para descrever políticas de replicação vêm "[Documentação do ONTAP 9](#)" do .

- Para migração e outros, a política de replicação é chamada *MirrorAllSnapshots*. *MirrorAllSnapshots* é uma política assíncrona para espelhar todos os snapshots e o sistema de arquivos ativo mais recente.
- Para recuperação de desastres de arquivos, inativos ou quentes, a política de replicação é chamada *MirrorAndVault*. *MirrorAndVault* é uma política assíncrona e de cofre para espelhar o mais recente sistema de arquivos ativo e instantâneos diários e semanais.

Para todos os casos de uso, se você habilitar snapshots para retenção de longo prazo, a política de replicação padrão é *MirrorAndVault*.

- b. **FSX para sistema de arquivos ONTAP:** Selecione credenciais, região e nome do sistema de arquivos FSX for ONTAP para o sistema de arquivos FSX for ONTAP de destino.
- c. **Nome da VM de armazenamento:** Selecione a VM de armazenamento no menu suspenso. A VM de armazenamento selecionada é o destino para todos os volumes selecionados neste relacionamento de replicação.
- d. **Nome do volume:** O nome do volume de destino é gerado automaticamente com o seguinte {OriginalVolumeName}_copy formato . Pode utilizar o nome do volume gerado automaticamente ou introduzir outro nome de volume.
- e. **Política de disposição em categorias:** Selecione a política de disposição em categorias para os dados armazenados no volume de destino. A política de disposição em categorias padrão é a política de disposição em categorias recomendada para o caso de uso selecionado.

Balanceado (Automático) é a política de camadas padrão ao criar um volume usando o console do Workload Factory. Para obter mais informações sobre políticas de níveis de volume, consulte "[Capacidade de armazenamento de volume](#)" na documentação do AWS FSx para NetApp ONTAP . Observe que o Workload Factory usa nomes baseados em casos de uso no console do Workload Factory para políticas de camadas e inclui nomes de políticas de camadas do FSx para ONTAP entre parênteses.

Se você selecionou o caso de uso de migração, o Workload Factory seleciona automaticamente copiar a política de camadas do volume de origem para o volume de destino. Você pode desmarcar a opção de copiar a política de camadas e selecionar uma política de camadas que se aplique ao volume selecionado para replicação.

- a. **Taxa máxima de transferência:** Selecione **limitada** e insira o limite máximo de transferência em MB/s. Em alternativa, selecione **Unlimited**.

Sem um limite, o desempenho da rede e do aplicativo pode declinar. Como alternativa, recomendamos uma taxa de transferência ilimitada para os sistemas de arquivos FSX for ONTAP para cargas de trabalho críticas, por exemplo, aquelas que são usadas principalmente para recuperação de desastres.

7. Em Configurações de replicação, forneça o seguinte:

- a. **Intervalo de replicação:** Selecione a frequência em que os instantâneos são transferidos do volume de origem para o volume de destino.
- b. **Retenção de longo prazo:** Opcionalmente, habilite snapshots para retenção de longo prazo. A retenção de longo prazo permite que os serviços empresariais continuem operando mesmo em caso de falha completa do local, dando suporte ao failover de aplicações de forma transparente, usando uma cópia secundária.

Replicações sem retenção de longo prazo usam a política *MirrorAllSnapshots*. Habilitar a retenção de longo prazo atribui a política *MirrorAndVault* à replicação.

Se você habilitar a retenção a longo prazo, selecione uma política existente ou crie uma nova política para definir os snapshots a serem replicados e o número a ser retido.



Rótulos de origem e destino correspondentes são necessários para retenção a longo prazo. Se desejar, a fábrica Workload pode criar rótulos ausentes para você.

- **Escolha uma política existente:** Selecione uma política existente no menu suspenso.
 - **Criar uma nova política:** insira um **nome de política**.
 - c. **Snapshots imutáveis:** Opcional. Selecione **Ativar instantâneos imutáveis** para evitar que os instantâneos obtidos nesta política sejam excluídos durante o período de retenção.
 - Defina o **período de retenção** em número de horas, dias, meses ou anos.
 - **Políticas de snapshot:** Na tabela, selecione a frequência da política de snapshot e o número de cópias a reter. Pode selecionar mais de uma política de instantâneos.
 - d. **Ponto de acesso S3:** Opcionalmente, conecte um ponto de acesso S3 para acessar dados do sistema de arquivos FSx for ONTAP residentes em volumes NFS ou SMB/CIFS por meio das APIs do AWS S3. Somente o tipo de acesso a arquivos é suportado. Fornecendo os seguintes detalhes:
 - **Nome do ponto de acesso S3:** Insira o nome do ponto de acesso S3.
 - **Usuário:** Selecione um usuário existente com acesso ao volume ou crie um novo usuário.
 - **Tipo de usuário:** Selecione **UNIX** ou **Windows** como o tipo de usuário.
 - **Configuração de rede:** Selecione **Internet** ou **nuvem privada virtual (VPC)**. O tipo de rede que você escolher determina se o ponto de acesso é acessível pela internet ou restrito a uma VPC específica.
 - **Habilitar metadados:** Habilitar metadados cria uma tabela S3 contendo todos os objetos acessíveis pelo ponto de acesso S3, que você pode usar para auditoria, governança, automação, análise e otimização. Habilitar metadados acarreta custos adicionais da AWS. Consulte ["Documentação de preços do Amazon S3"](#) para mais informações.
 - e. **Etiquetas de ponto de acesso S3:** opcionalmente, você pode adicionar até 50 etiquetas.
8. Selecione **criar**.

Resultado

A relação de replicação aparece na guia **relacionamentos de replicação** no sistema de arquivos FSX for ONTAP de destino.

Inicializar um relacionamento de replicação no NetApp Workload Factory

Inicialize um relacionamento de replicação entre os volumes de origem e de destino para transferir o snapshot e todos os blocos de dados no NetApp Workload Factory.

Sobre esta tarefa


A inicialização executa uma transferência *Baseline*: Ele faz um instantâneo do volume de origem e, em seguida, transfere o instantâneo e todos os blocos de dados que ele faz referência ao volume de destino.

Antes de começar

Considere quando você optar por concluir esta operação. A inicialização pode ser demorada. Você pode

querer executar a transferência de linha de base em horas fora do pico.

Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos a ser atualizado e, em seguida, selecione **Gerenciar**.
5. Na visão geral do sistema de arquivos, selecione a guia **relacionamentos de replicação**.
6. Na guia Relacionamentos de replicação, selecione o menu de ações do relacionamento de replicação a ser inicializado.
7. Selecione **Inicializar**.
8. Na caixa de diálogo Inicializar relacionamento, selecione **Inicializar**.

Proteja seus dados com a proteção autônoma contra ransomware da NetApp com IA

Proteja seus dados com o NetApp Autonomous Ransomware Protection com IA (ARP/AI), um recurso que usa análise de carga de trabalho em ambientes NAS (NFS/SMB) para detectar e alertar sobre atividades anormais que podem ser um ataque de ransomware. Quando há suspeita de um ataque, o ARP/AI também cria novos instantâneos imutáveis a partir dos quais você pode restaurar seus dados.

Sobre esta tarefa

Use ARP/AI para se proteger contra ataques de negação de serviço, em que o invasor retém dados até que um resgate seja pago. ARP/AI oferece detecção de ransomware em tempo real com base em:

- Identificação dos dados recebidos como encriptados ou em texto simples.
- Análises que detectam:
 - **Entropia:** Uma avaliação da aleatoriedade dos dados em um arquivo
 - **Tipos de extensão de arquivo:** Uma extensão que não está em conformidade com o tipo de extensão normal
 - **IOPS de arquivos:** Um aumento na atividade de volume anormal com criptografia de dados

O ARP/AI pode detectar a propagação da maioria dos ataques de ransomware depois que apenas um pequeno número de arquivos é criptografado, tomar medidas automaticamente para proteger os dados e alertá-lo sobre a ocorrência de um ataque suspeito.

O recurso ARP/AI é atualizado automaticamente de acordo com a versão do ONTAP executada Amazon FSx for NetApp ONTAP, para que você não precise fazer atualizações manuais.

Aprendizagem e modos ativos

O ARP/AI opera primeiro no *modo de aprendizagem* e depois muda automaticamente para o *modo ativo*.

- **Modo de aprendizagem:** Quando você habilita o ARP/AI, ele é executado no *modo de aprendizagem*. No modo de aprendizagem, o sistema de arquivos FSx para ONTAP desenvolve um perfil de alerta

com base nas áreas analíticas: entropia, tipos de extensão de arquivo e IOPS de arquivo. Depois que o sistema de arquivos executa o ARP/AI no modo de aprendizagem por tempo suficiente para avaliar as características da carga de trabalho, o Workload Factory alterna automaticamente para o ARP/AI no *modo ativo* e começa a proteger seus dados.

- **Modo ativo:** depois que o ARP/AI muda para o *modo ativo*, o FSx para ONTAP cria instantâneos de ARP/AI para proteger os dados se uma ameaça for detectada.

No modo ativo, se uma extensão de arquivo for sinalizada como anormal, você deve avaliar o alerta. Você pode agir no alerta para proteger seus dados ou você pode marcar o alerta como um falso positivo. Marcar um alerta como falso positivo atualiza o perfil de alerta. Por exemplo, se o alerta for acionado por uma nova extensão de arquivo e você marcar o alerta como um falso positivo, você não receberá um alerta na próxima vez que essa extensão de arquivo for observada.

Volumes FlexVol que contêm um dispositivo de bloco iniciam o ARP/AI no modo ativo.

Configurações não suportadas

As configurações a seguir não suportam o uso de ARP/AI.

- Volumes iSCSI
- Volumes NVMe

Habilitar ARP/AI para um sistema de arquivos ou um volume

Habilitar ARP/AI para um sistema de arquivos adiciona proteção para todos os volumes NAS existentes e NAS recém-criados (NFS/SMB) automaticamente. Você também pode habilitar ARP/AI para volumes individuais.


Após habilitar o ARP/AI, se ocorrer um ataque e você identificar que ele é real, o Workload Factory configurará automaticamente uma política de snapshot que tira até seis snapshots a cada quatro horas. Cada instantâneo fica bloqueado por 2 a 5 dias.

Antes de começar

Para habilitar ARP/AI para um sistema de arquivos ou um volume, você deve associar um link. ["Aprenda como associar um link existente ou criar e associar um novo link"](#). Após o link associar, retorne a esta operação.


Habilitar ARP/AI para um sistema de arquivos

Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos para habilitar ARP/AI e então selecione **Gerenciar**.
5. Em Informações, selecione o ícone de lápis ao lado de **Proteção Autônoma contra Ransomware**. O ícone de lápis aparece ao lado da seta quando o mouse passa sobre a linha **Proteção Autônoma contra Ransomware**.
6. Na página NetApp Autonomous Ransomware Protection com IA (ARP/AI), faça o seguinte:
 - a. Habilitar ou desabilitar o recurso.
 - b. **Criação automática de snapshots**: Selecione o número máximo de snapshots a serem retidos e o intervalo de tempo entre os snapshots. O padrão é 6 instantâneos a cada 4 horas.
 - c. **Snapshots imutáveis**: Selecione o período de retenção padrão em horas e o número máximo de dias para reter snapshots imutáveis. Ative esta opção para garantir que os instantâneos não possam ser excluídos ou modificados até que o período de retenção especificado termine.
 - d. **Deteção**: Opcionalmente, selecione qualquer um dos seguintes parâmetros para escanear e detectar anomalias automaticamente.
7. Aceite a declaração para prosseguir.
8. Selecione **Apply** para salvar as alterações.

Habilitar ARP/AI para um volume


Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos para habilitar ARP/AI e então selecione **Gerenciar**.
5. Na guia Volumes, selecione o menu de ações do volume para habilitar ARP/AI, depois **Ações de proteção de dados** e depois **Gerenciar ARP/AI**.
6. Na caixa de diálogo Gerenciar ARP/AI, faça o seguinte:
 - a. Habilitar ou desabilitar o recurso.
 - b. **Deteção**: Opcionalmente, selecione qualquer um dos seguintes parâmetros para escanear e detectar anomalias automaticamente.
7. Aceite a declaração para prosseguir.
8. Selecione **Apply** para salvar as alterações.

Validar ataques de ransomware

Determine se um ataque é um falso alarme ou um incidente de ransomware genuíno.

Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2.  Selecione o menu **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o sistema de arquivos para validar ataques de ransomware.
5. Na visão geral do sistema de arquivos, selecione a guia **volumes**.
6. Selecione **Analyze attacks** no bloco Autonomous ransomware Protection.
7. Baixe o relatório de eventos de ataque para analisar se algum arquivo ou pasta foi comprometido e, em seguida, decidir se ocorreu um ataque.
8. Se nenhum ataque ocorreu, selecione **False Alarm** para o volume na tabela e, em seguida, selecione **Close**.
9. Se um ataque tiver ocorrido, selecione **Real Attack** para o volume na tabela. A caixa de diálogo Restaurar dados de volume comprometidos é aberta. Você pode prosseguir para [recupere seus dados](#) imediatamente ou selecionar **Fechar** e voltar para concluir o processo de recuperação mais tarde.


Recuperar dados após um ataque de ransomware

Quando há suspeita de um ataque, o sistema tira um instantâneo do volume naquele momento e bloqueia essa cópia. Se o ataque for confirmado posteriormente, os arquivos afetados ou o volume inteiro poderão ser restaurados usando o snapshot ARP/AI.

Os instantâneos bloqueados não podem ser eliminados até que o período de retenção termine. No entanto, se você decidir mais tarde marcar o ataque como um falso positivo, a cópia bloqueada será excluída.

Com o conhecimento dos arquivos afetados e o tempo de ataque, é possível recuperar seletivamente os arquivos afetados de vários snapshots, em vez de simplesmente reverter todo o volume para um dos snapshots.

Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2.  Selecione o menu **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o sistema de arquivos para recuperar os dados.
5. Na visão geral do sistema de arquivos, selecione a guia **volumes**.
6. Selecione **Analyze attacks** no bloco Autonomous ransomware Protection.
7. Se um ataque tiver ocorrido, selecione **Real Attack** para o volume na tabela.
8. Na caixa de diálogo Restaurar dados de volume comprometidos, siga as instruções para restaurar no nível do arquivo ou no nível do volume. Na maioria dos casos, você irá restaurar arquivos em vez de um volume inteiro.
9. Depois de concluir a restauração, selecione **Fechar**.

Resultado

Os dados comprometidos foram restaurados.

Clonar um volume no NetApp Workload Factory

Clone um volume no NetApp Workload Factory para criar um volume de leitura/gravação do volume original para teste.

O clone reflete o estado atual e pontual dos dados. Você também pode usar clones para conceder acesso aos dados a outros usuários sem conceder a eles acesso aos dados de produção.


Sobre esta tarefa

A clonagem de volume é compatível apenas com volumes FlexClone.

Quando um volume é clonado, um volume gravável é criado com referências a instantâneos do volume pai. A criação de clones ocorre em segundos. Os dados clonados não residem no clone de volume, mas residem no volume pai. Todos os novos dados gravados no volume após a criação do clone residem no clone.

Para que um volume clonado contenha todos os dados do volume pai e quaisquer novos dados adicionados ao clone após a criação, você precisará "[divida o clone](#)" do volume pai. Além disso, você não pode excluir um volume pai se ele tiver um clone. Um clone deve ser dividido antes que um volume pai possa ser excluído.

Passos

1. Inicie sessão utilizando uma das "[experiências de console](#)".
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **FSx para ONTAP**.
4. No **FSx for ONTAP**, selecione o menu de ações do sistema de arquivos FSx for ONTAP que contém o volume a ser clonado e selecione **Gerenciar**.
5. Na guia Visão geral do sistema de arquivos, selecione a guia **volumes**.
6. Na aba Volumes, selecione o menu de ações do volume a ser clonado.
7. Selecione **ações de proteção de dados** e, em seguida, **volume Clone**.
8. Na caixa de diálogo Clone volume (Clonar volume), introduza um nome para o clone de volume.
9. Selecione **Clone**.

Use dados de cluster ONTAP local no NetApp Workload Factory

Descubra e replique dados ONTAP locais no NetApp Workload Factory para que eles possam ser usados para enriquecer bases de conhecimento de IA.

Sobre esta tarefa

Para usar dados de um cluster ONTAP on-premises, você primeiro precisa descobrir o cluster ONTAP on-premises. Depois de descobrir um cluster do ONTAP no local, você pode usar os dados para qualquer um dos seguintes casos de uso.

Casos de uso

Observe que o principal caso de uso para a carga de trabalho do GenAI é o foco dessa série de tarefas.

- **Carga de trabalho do GenAI:** Replique dados de volume no local do ONTAP para um sistema de arquivos FSX for ONTAP para que os dados possam ser usados ["Enriquecer as bases de conhecimento de IA"](#)no .
- **Backup e migração para a nuvem:** Os dados de volume ONTAP replicados no local para um sistema de arquivos FSX for ONTAP podem ser usados como backup na nuvem.
- **Disposição em camadas de dados:** Após a replicação, os dados de volume ONTAP no local com pouca frequência podem ser dispostos da camada de storage SSD para a camada de storage do pool de capacidade.

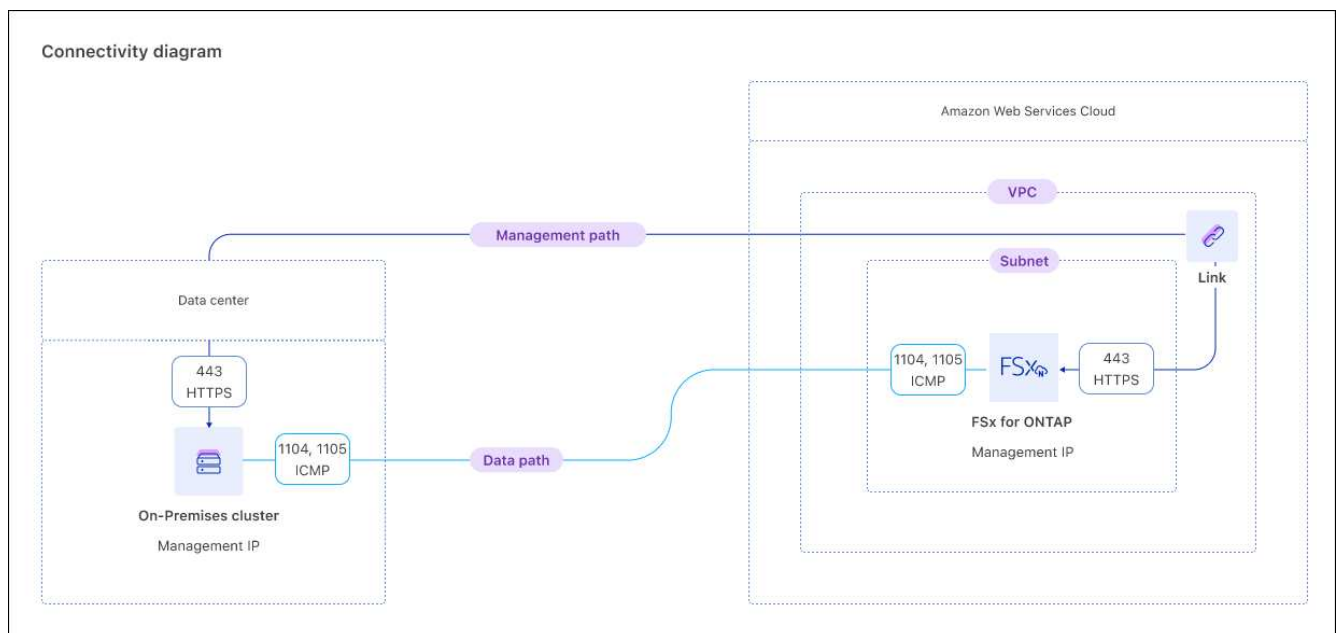
Descubra um cluster ONTAP no local

Descubra um cluster ONTAP local no NetApp Workload Factory para que você possa replicar os dados em um sistema de arquivos Amazon FSx for NetApp ONTAP .


Antes de começar

Certifique-se de que tem o seguinte antes de começar:

- Um sistema de arquivos FSX for ONTAP para replicação.
- Um link conectado para se associar ao cluster no local descoberto. Se você não tem um link, você precisará ["crie um"](#).
- Credenciais de usuário do ONTAP com permissões necessárias.
- ONTAP on-premises versão 9,8 e superior.
- Conetividade como mostrado no diagrama a seguir.



Passos

1. Inicie sessão utilizando uma das ["experiências de console"](#).
2. Selecione o menu  Em seguida, selecione **Armazenamento**.

3. Selecione a guia **On-Premises ONTAP**.
4. Selecione **Discover**.
5. Reveja os pré-requisitos e selecione **seguinte**.
6. Na página Discover ONTAP on-premises, forneça o seguinte em **Configuração de cluster**:
 - a. **Link**: Selecione um link. O link será associado ao cluster local para criar conectividade entre o cluster e o Workload Factory.

Se você não criou um link, siga as instruções e, em seguida, retorne a esta operação e selecione o link.
 - b. **Endereço IP do cluster**: Forneça o endereço IP para que o cluster ONTAP local seja replicado.
 - c. **Credenciais ONTAP**: Insira as credenciais ONTAP para o cluster ONTAP no local. Certifique-se de que o usuário tem as permissões necessárias.
7. Selecione **Discover** para iniciar o processo de descoberta.

Resultado

O cluster ONTAP no local é descoberto e agora aparece na guia **On-Premise ONTAP**.

Agora você pode visualizar os dados no cluster do ONTAP no local e [Replique os dados para um sistema de arquivos do FSX for ONTAP](#) no .


Replique dados de volume de um cluster ONTAP no local

Replique dados de volume de um cluster do ONTAP no local para um sistema de arquivos FSX for ONTAP. Após a replicação, os dados podem ser usados para enriquecer as bases de conhecimento de IA.

Antes de começar

- Você precisa descobrir um cluster do ONTAP no local para replicar seus dados de volume.
- Você deve ter um sistema de arquivos FSX for ONTAP disponível para ser o destino para a replicação.
- Tanto o cluster ONTAP no local quanto o sistema de arquivos FSX for ONTAP que você usa para a relação de replicação devem ter um link associado. "[Aprenda como associar um link existente ou criar e associar um novo link](#)". Após os associados da ligação, volte a esta operação.

Passos

1. Inicie sessão utilizando uma das "[experiências de console](#)".
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **On-premises ONTAP**.
4. Para encontrar volumes por VM de armazenamento, você pode **Selecionar VM de armazenamento** no menu suspenso.
5. Selecione um ou mais volumes para replicar e, em seguida, selecione **replicar**.
6. Na página criar replicação, em destino replicação, forneça o seguinte:
 - a. **FSX para sistema de arquivos ONTAP**: Selecione credenciais, região e nome do sistema de arquivos FSX for ONTAP para o sistema de arquivos FSX for ONTAP de destino.
 - b. **Nome da VM de armazenamento**: Selecione a VM de armazenamento no menu suspenso.
 - c. **Nome do volume**: O nome do volume de destino é gerado automaticamente com o seguinte

{OriginalVolumeName}_copy formato . Pode utilizar o nome do volume gerado automaticamente ou introduzir outro nome de volume.

d. **Dados em categorias:** Selecione a política de disposição em camadas para os dados armazenados no volume de destino.

- **Automático:** A política de camadas padrão ao criar um volume usando a interface de usuário do Workload Factory FSx para ONTAP . Coloca em camadas todos os dados frios, incluindo dados do usuário e instantâneos, na camada de armazenamento do pool de capacidade por um período de tempo específico.
- **Somente snapshot:** Categoriza somente os dados snapshot para a camada de storage do pool de capacidade.
- **Nenhum:** Mantém todos os dados do seu volume na camada de storage primário.
- **All:** Marca todos os dados do usuário e dados instantâneos como inativos e os armazena na camada de armazenamento do pool de capacidade.

Observe que algumas políticas de disposição em categorias têm um período de resfriamento mínimo associado que define o tempo, ou *dias de resfriamento*, que os dados do usuário em um volume devem permanecer inativos para que os dados sejam considerados "frios" e movidos para a camada de storage do pool de capacidade. O período de resfriamento começa quando os dados são gravados no disco.

Para obter mais informações sobre políticas de disposição em camadas de volume, consulte a ["Capacidade de armazenamento de volume"](#) documentação do AWS FSX for NetApp ONTAP.

a. **Taxa máxima de transferência:** Selecione **limitada** e insira o limite máximo de transferência em MIB/s. Em alternativa, selecione **Unlimited**.

Sem um limite, o desempenho da rede e do aplicativo pode declinar. Como alternativa, recomendamos uma taxa de transferência ilimitada para os sistemas de arquivos FSX for ONTAP para cargas de trabalho críticas, por exemplo, aquelas que são usadas principalmente para recuperação de desastres.

7. Em Configurações de replicação, forneça o seguinte:

- a. **Intervalo de replicação:** Selecione a frequência em que os instantâneos são transferidos do volume de origem para o volume de destino.
- b. **Retenção de longo prazo:** Opcionalmente, habilite snapshots para retenção de longo prazo.

Se você habilitar a retenção a longo prazo, selecione uma política existente ou crie uma nova política para definir os snapshots a serem replicados e o número a ser retido.

- Para uma política existente, selecione **escolha uma política existente** e, em seguida, selecione a política existente no menu suspenso.
- Para uma nova política, selecione **criar uma nova política** e forneça o seguinte:
 - **Nome da política:** Insira um nome de política.
 - **Políticas de snapshot:** Na tabela, selecione a frequência da política de snapshot e o número de cópias a reter. Pode selecionar mais de uma política de instantâneos.

8. Selecione **criar**.

Resultado

A relação de replicação aparece na guia **relacionamentos de replicação** no sistema de arquivos FSX for ONTAP de destino.


Remover um cluster ONTAP local do NetApp Workload Factory

Remova um cluster ONTAP local do NetApp Workload Factory quando necessário.

Antes de começar

É necessário "[eliminar todas as relações de replicação existentes](#)" para quaisquer volumes no cluster do ONTAP no local antes de remover o cluster para que não haja relacionamentos quebrados.

Passos

1. Inicie sessão utilizando uma das "[experiências de console](#)".
2. Selecione o menu  Em seguida, selecione **Armazenamento**.
3. No menu Armazenamento, selecione **On-premises ONTAP**.
4. Selecione o cluster ONTAP local a ser removido.
5. Selecione o menu de ações e selecione **Remover do Workload Factory**.

Resultado

O cluster ONTAP local é removido do NetApp Workload Factory.

Proteja seus dados com um cofre cibernético.

Um volume de cofre cibernético é um local de armazenamento isolado e seguro usado para guardar cópias de segurança dos seus dados, protegendo-os contra ataques de ransomware e outras ameaças cibernéticas. Como parte da criação do cofre, você criará um volume de cofre cibernético, desativará todos os protocolos do cliente, configurará uma relação de replicação entre o volume de origem e o volume do cofre cibernético e criará snapshots imutáveis no volume do cofre cibernético.

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.

O cofre cibernético é um repositório de dados "isolado da internet", imutável e indelével, imune a ameaças que afetam a rede principal, como malware, ransomware ou mesmo ameaças internas. Um cofre cibernético pode ser criado com instantâneos imutáveis e indelévels.

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.

FSx para cofres cibernéticos ONTAP

O Amazon FSx for NetApp ONTAP é compatível como origem e destino de cofre cibernético.

Implementação

A Workload Factory oferece assistência na criação de uma arquitetura de cofre cibernético. Após você entrar em contato com a NetApp para manifestar seu interesse na implementação de um cofre cibernético, um especialista da NetApp entrará em contato para discutir suas necessidades.

Envie um e-mail para ng-FSx-CyberVault@netapp.com para começar.

Informações relacionadas

Para obter mais informações sobre cofres cibernéticos e como configurar essa arquitetura, consulte o ["Documentação do cofre cibernético ONTAP"](#).

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.