



Use o ONTAP para gerenciar seus dados

ASA r2

NetApp
March 31, 2026

Índice

Use o ONTAP para gerenciar seus dados	1
Demonstrações de vídeo do sistema de storage ASA R2	1
Gerencie seu storage	1
Provisione storage SAN ONTAP nos sistemas ASA R2	1
Clonar dados em sistemas de storage ASA R2	7
Gerenciar grupos de hosts	11
Gerenciar unidades de armazenamento	12
Migrar VMs de armazenamento	14
Limites de armazenamento do ASA R2	20
Proteja seus dados	21
Crie snapshots para fazer backup de seus dados em sistemas de storage ASA R2	21
Gerenciar reserva de instantâneos	25
Crie um relacionamento de pares de VMs de armazenamento intercluster em sistemas de armazenamento ASA r2	27
Configurar a replicação de instantâneos	28
Configurar sincronização ativa do SnapMirror	34
Gerenciar sincronização ativa do SnapMirror	39
Restaure os dados em sistemas de storage ASA R2	43
Gerenciar grupos de consistência	45
Gerenciar políticas e programações de proteção de dados da ONTAP em sistemas de storage ASA R2	53
Proteja seus dados	55
Criptografia de dados em repouso em sistemas de storage ASA R2	55
Migre chaves de criptografia de dados ONTAP entre gerenciadores de chaves no sistema ASA R2	56
Proteção contra ataques de ransomware	59
Conexões NVMe seguras em seus sistemas de storage ASA R2	66
Conexões IP seguras em seus sistemas de storage ASA R2	66

Use o ONTAP para gerenciar seus dados

Demonstrações de vídeo do sistema de storage ASA R2

Veja vídeos curtos que demonstram como usar o Gerenciador de sistemas do ONTAP para executar tarefas comuns de forma rápida e fácil em seus sistemas de storage ASA R2.

[Configure protocolos SAN no sistema ASA R2](#)

"[Transcrição de vídeo](#)"

[Provisione storage SAN em seu sistema ASA R2](#)

"[Transcrição de vídeo](#)"

[Replique dados para um cluster remoto a partir de um sistema ASA R2](#)

"[Transcrição de vídeo](#)"

Gerencie seu storage

Provisione storage SAN ONTAP nos sistemas ASA R2

Quando você provisiona o storage, permite que seus hosts SAN leiam e gravem dados nos sistemas de storage ASA R2. Para provisionar o armazenamento, use o Gerenciador do sistema do ONTAP para criar unidades de armazenamento, adicionar iniciadores de host e mapear o host para uma unidade de armazenamento. Você também precisa executar etapas no host para ativar as operações de leitura/gravação.

Crie unidades de armazenamento

Em um sistema ASA r2, uma unidade de armazenamento disponibiliza espaço de armazenamento para os hosts SAN realizarem operações de dados. Uma unidade de armazenamento refere-se a um LUN para hosts SCSI ou a um namespace NVMe para hosts NVMe. Se o seu cluster estiver configurado para suportar hosts SCSI, você será solicitado a criar um LUN. Se o seu cluster estiver configurado para suportar hosts NVMe, você será solicitado a criar um namespace NVMe.

Uma unidade de armazenamento ASA r2 tem uma capacidade máxima de 128 TB. Veja o "[NetApp Hardware Universe](#)" Para obter as informações mais recentes sobre os limites de armazenamento para sistemas ASA r2.

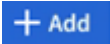
Você adiciona e mapeia iniciadores de host para a unidade de armazenamento como parte do processo de criação da unidade de armazenamento. Você também pode "[adicionar](#)" e "[mapa](#)". Os iniciadores do host são criados após a criação das unidades de armazenamento.

A partir do ONTAP 9.18.1, você pode modificar a reserva de snapshots e habilitar a exclusão automática de snapshots ao criar uma unidade de armazenamento. A reserva de snapshots é a quantidade de espaço na unidade de armazenamento reservada especificamente para snapshots. Quando a reserva de snapshots está configurada com exclusão automática de snapshots, os snapshots mais antigos são excluídos automaticamente quando o espaço usado pelos snapshots excede a reserva de snapshots.

"Saiba mais sobre a reserva de snapshots em sistemas ASA r2."

As unidades de storage são provisionadas de forma thin por padrão. O thin provisioning permite que a unidade de storage cresça até o tamanho alocado, mas não reserva o espaço antecipadamente. O espaço é alocado dinamicamente a partir do espaço livre, conforme necessário. Isso permite que você obtenha maior eficiência de storage ao *provisionar em excesso* o espaço disponível. Por exemplo, suponha que você tenha 1 TB de espaço livre e precise criar quatro unidades de storage de 1 TB. Em vez de adicionar imediatamente 3 TB de capacidade de storage ao seu sistema, você pode criar as unidades de storage, monitorar a utilização do espaço e aumentar sua capacidade de storage à medida que as unidades de storage consomem espaço real. Saiba mais sobre "[provisionamento fino](#)".

Passos

1. No System Manager, selecione **Storage** (armazenamento) e, em seguida,  **Add** selecione .
2. Introduza um nome para a nova unidade de armazenamento.
3. Introduza o número de unidades que pretende criar.

Se você criar mais de uma unidade de armazenamento, cada unidade será criada com a mesma capacidade, sistema operacional host e mapeamento de host.

Para otimizar o balanceamento da carga de trabalho em toda a zona de disponibilidade de armazenamento, crie um número par de unidades de armazenamento.

4. Introduza a capacidade da unidade de armazenamento e, em seguida, selecione o sistema operativo anfitrião.



Se você estiver criando mais de uma unidade de storage, cada unidade será criada com a mesma capacidade. Multiplique o número de unidades de storage que você está criando pela capacidade desejada para garantir que você tenha espaço utilizável suficiente. Se você não tiver espaço livre e optar por provisionar em excesso, monitore a utilização atentamente para evitar ficar sem espaço e perder dados.

5. Aceite o **mapeamento de host** selecionado automaticamente ou selecione um grupo de host diferente para a unidade de armazenamento a ser mapeada.

Mapeamento de host refere-se ao grupo de hosts ao qual a nova unidade de armazenamento será mapeada. Se houver um grupo de hosts preexistente para o tipo de host selecionado para sua nova unidade de armazenamento, o grupo de hosts preexistente será selecionado automaticamente para seu mapeamento de hosts. Você pode aceitar o grupo de hosts selecionado automaticamente ou pode selecionar um grupo de hosts diferente.

Caso não exista um grupo de hosts pré-existente para hosts em execução no sistema operacional que você especificou, ONTAP cria um novo grupo de hosts automaticamente.

6. Se você quiser fazer qualquer uma das seguintes opções, selecione **mais opções** e conclua as etapas necessárias.

Opção	Passos
<p>Altere a política de qualidade do serviço (QoS) padrão</p> <p>Se a política de QoS padrão não tiver sido definida anteriormente na máquina virtual de armazenamento (VM) na qual a unidade de armazenamento está sendo criada, essa opção não estará disponível.</p>	<p>a. Em armazenamento e otimização, ao lado de qualidade do serviço (QoS), ▼ seleccione .</p> <p>b. Seleccione uma política de QoS existente.</p>
<p>Crie uma nova política de QoS</p>	<p>a. Em armazenamento e otimização, ao lado de qualidade do serviço (QoS), ▼ seleccione .</p> <p>b. Seleccione Definir nova política.</p> <p>c. Introduza um nome para a nova política de QoS.</p> <p>d. Defina um limite de QoS, uma garantia de QoS ou ambos.</p> <p>i. Opcionalmente, em limit, insira um limite máximo de throughput, um limite máximo de IOPS ou ambos.</p> <p>A configuração de uma taxa de transferência máxima e de IOPS para uma unidade de storage restringe o impacto nos recursos do sistema, de modo que não prejudique o desempenho de workloads críticos.</p> <p>ii. Opcionalmente, em Guarantee, insira uma taxa de transferência mínima, um mínimo de IOPS ou ambos.</p> <p>Definir uma taxa de transferência mínima e IOPS para uma unidade de storage garante que ela atenda aos requisitos mínimos de desempenho, independentemente da demanda por workloads da concorrência.</p> <p>e. Seleccione Adicionar.</p>
<p>Altere o nível de serviço de desempenho padrão.</p>	<p>a. Em armazenamento e otimização, ao lado do nível de serviço de desempenho, ▼ seleccione .</p> <p>b. Seleccione desempenho.</p> <p>Os sistemas ASA r2 oferecem dois níveis de desempenho. O nível de desempenho padrão é Extremo, que é o nível mais alto disponível. Você pode diminuir o nível para Desempenho.</p>
<p>Modifique a reserva de snapshots padrão e habilite a exclusão automática de snapshots.</p>	<p>a. Em Reserva de snapshots %, insira o valor numérico correspondente à porcentagem do espaço da unidade de armazenamento que você deseja alocar para snapshots.</p> <p>b. Seleccione Excluir automaticamente snapshots antigos.</p>

Opção	Passos
Adicione um novo host SCSI	<p>a. Em informações do host, selecione SCSI para o protocolo de conexão.</p> <p>b. Selecione o sistema operacional do host.</p> <p>c. Em Mapeamento do host, selecione novos hosts.</p> <p>d. Selecione FC ou iSCSI.</p> <p>e. Selecione iniciadores de host existentes ou selecione Adicionar iniciador para adicionar um novo iniciador de host.</p> <p>Um exemplo de uma WWPN FC válida é "01:02:03:04:0a:0b:0c:0d". Exemplos de nomes de iniciadores iSCSI válidos são "iqn.1995-08.com.example:string" e "eui.0123456789abcdef".</p>
Crie um novo grupo de hosts SCSI	<p>a. Em informações do host, selecione SCSI para o protocolo de conexão.</p> <p>b. Selecione o sistema operacional do host.</p> <p>c. Em Mapeamento do host, selecione novo grupo de hosts.</p> <p>d. Introduza um nome para o grupo anfitrião e, em seguida, selecione os anfitriões a adicionar ao grupo.</p>
Adicionar um novo subsistema NVMe	<p>a. Em informações do host, selecione NVMe para o protocolo de conexão.</p> <p>b. Selecione o sistema operacional do host.</p> <p>c. Em Mapeamento do host, selecione novo subsistema NVMe.</p> <p>d. Introduza um nome para o subsistema ou aceite o nome predefinido.</p> <p>e. Introduza um nome para o iniciador.</p> <p>f. Se pretender ativar a autenticação na banda ou a TLS (Transport Layer Security), <input checked="" type="checkbox"/> selecione e, em seguida, selecione as suas opções.</p> <p>A autenticação na banda permite autenticação bidirecional e unidirecional segura entre os hosts NVMe e o sistema ASA R2.</p> <p>O TLS criptografa todos os dados enviados pela rede entre seus hosts NVMe/TCP e seu sistema ASA R2.</p> <p>g. Selecione Adicionar iniciador para adicionar mais iniciadores.</p> <p>Formate o NQN do host como <nqn.yyyy-mm> seguido por um nome de domínio totalmente qualificado. O ano deve ser igual ou posterior a 1970. O comprimento máximo total deve ser 223. Um exemplo de um iniciador NVMe válido é nqn.2014-08.com.example:string</p>

7. Selecione **Adicionar**.

O que se segue?

Suas unidades de storage são criadas e mapeadas para seus hosts. Agora você pode "[criar instantâneos](#)" proteger os dados no seu sistema ASA R2.

Para mais informações

Saiba mais "[Como os sistemas ASA R2 usam máquinas virtuais de armazenamento](#)" sobre o .

Adicione iniciadores de host

Você pode adicionar novos iniciadores de host ao seu sistema ASA R2 a qualquer momento. Os iniciadores tornam os hosts elegíveis para acessar unidades de armazenamento e executar operações de dados.

Antes de começar

Se você quiser replicar a configuração do host para um cluster de destino durante o processo de adição de iniciadores de host, o cluster deve estar em um relacionamento de replicação. Opcionalmente, você pode "[crie uma relação de replicação](#)" depois que seu host for adicionado.

Adicione iniciadores de host para hosts SCSI ou NVMe.

SCSI anfitriões

Passos

1. Selecione **Host**.
2. Selecione **SCSI**; em seguida, **+ Add** selecione .
3. Digite o nome do host, selecione o sistema operacional do host e insira uma descrição do host.
4. Se você quiser replicar a configuração do host para um cluster de destino, selecione **replique a configuração do host** e, em seguida, selecione o cluster de destino.

O cluster precisa estar em uma relação de replicação para replicar a configuração do host.

5. Adicione hosts novos ou existentes.

Adicione novos hosts	Adicionar hosts existentes
<ol style="list-style-type: none">a. Selecione novos hosts.b. Selecione FC ou iSCSI; em seguida, selecione os iniciadores do host.c. Opcionalmente, selecione Configurar proximidade do host. A configuração da proximidade do host permite que o ONTAP identifique a controladora mais próxima do host para otimização do caminho de dados e redução da latência. Isso só se aplica se você tiver replicado dados para um local remoto. Se não tiver configurado a replicação de instantâneos, não será necessário selecionar esta opção.d. Se precisar adicionar novos iniciadores, selecione Adicionar iniciadores.	<ol style="list-style-type: none">a. Selecione hosts existentes.b. Selecione o host que você deseja adicionar.c. Selecione Adicionar.

6. Selecione **Adicionar**.

O que se segue?

Seus hosts SCSI são adicionados ao seu sistema ASA R2 e você está pronto para mapear seus hosts para suas unidades de armazenamento.

Hosts NVMe

Passos

1. Selecione **Host**.
2. Selecione **NVMe**; em seguida, **+ Add** selecione .
3. Insira um nome para o subsistema NVMe, selecione o sistema operacional host e insira uma descrição.
4. Selecione **Adicionar iniciador**.


O que se segue?

Seus hosts NVMe são adicionados ao sistema ASA R2 e você está pronto para mapear seus hosts para suas unidades de storage.

Mapear a unidade de armazenamento para um host

Após criar as unidades de armazenamento ASA r2 e adicionar os iniciadores de host, mapeie os hosts para as unidades de armazenamento para começar a fornecer dados. As unidades de armazenamento são mapeadas para os hosts como parte do processo de criação da unidade de armazenamento. Você também pode mapear unidades de armazenamento existentes para hosts novos ou existentes a qualquer momento.

Passos

1. Selecione **armazenamento**.
2. Passe o cursor sobre o nome da unidade de armazenamento que pretende mapear.
3.  Selecione ; em seguida, selecione **Map to hosts**.
4. Selecione os hosts que deseja mapear para a unidade de armazenamento; em seguida, selecione **Map**.

O que se segue?

Sua unidade de armazenamento é mapeada para seus hosts e você está pronto para concluir o processo de provisionamento em seus hosts.

Provisionamento completo no lado do host

Depois de criar suas unidades de armazenamento, adicionar seus iniciadores de host e mapear suas unidades de armazenamento, há etapas que você deve executar em seus hosts antes que eles possam ler e gravar dados em seu sistema ASA R2.

Passos

1. Para FC e FC/NVMe, defina a zona dos switches FC por WWPN.

Use uma zona por iniciador e inclua todas as portas de destino em cada zona.
2. Descubra a nova unidade de armazenamento.
3. Inicialize a unidade de armazenamento e um sistema de criação de ficheiros.
4. Verifique se o host pode ler e gravar dados na unidade de armazenamento.

O que se segue?

Você concluiu o processo de provisionamento e está pronto para começar a fornecer dados. Agora você pode ["criar instantâneos"](#) proteger os dados no seu sistema ASA R2.

Para mais informações

Para obter mais detalhes sobre a configuração do lado do host, consulte ["Documentação do host SAN ONTAP"](#) para seu host específico.


Clonar dados em sistemas de storage ASA R2

A clonagem de dados cria cópias de unidades de storage e grupos de consistência no sistema ASA R2 usando o Gerenciador de sistemas do ONTAP que pode ser usado para desenvolvimento de aplicações, testes, backups, migração de dados ou outras funções administrativas.

Clonar unidades de storage

Ao clonar uma unidade de storage, você cria uma nova unidade de storage no sistema ASA R2 que é uma cópia gravável e pontual da unidade de storage clonada.

Passos

1. No System Manager, selecione **Storage**.
2. Passe o Mouse sobre o nome da unidade de armazenamento que você deseja clonar.
3.  Selecione ; em seguida, selecione **Clone**.
4. Aceite o nome padrão para a nova unidade de armazenamento que será criada como um clone ou insira um novo.
5. Selecione o sistema operacional do host.

Um novo snapshot é criado para o clone por padrão.

6. Se você quiser usar um snapshot existente, criar um novo grupo de hosts ou adicionar um novo host, selecione **mais opções**.

Opção	Passos
Use um instantâneo existente	<ol style="list-style-type: none">a. Em Snapshot to clone, selecione Use an existing snapshot.b. Selecione o instantâneo que deseja usar para o clone.
Crie um novo grupo de hosts	<ol style="list-style-type: none">a. Em Host mapping, selecione New host group.b. Insira um nome para o novo grupo de hosts; em seguida, selecione os iniciadores de host a serem incluídos no grupo.
Adicione um novo host	<ol style="list-style-type: none">a. Em Host mapping, selecione New hosts.b. Insira o nome a para o novo host; em seguida, selecione FC ou iSCSI.c. Selecione os iniciadores do host na lista de iniciadores existentes ou selecione Adicionar para adicionar novos iniciadores para o host.

7. Selecione **Clone**.

O que se segue?

Criou uma nova unidade de armazenamento idêntica à unidade de armazenamento clonada. Agora está pronto para utilizar a nova unidade de armazenamento, conforme necessário.

Grupos de consistência de clones

Ao clonar um grupo de consistência, você cria um novo grupo de consistência idêntico à estrutura, às unidades de storage e aos dados do grupo de consistência clonado. Use um clone de grupo de consistência para realizar testes de aplicações ou migrar dados. Suponha, por exemplo, que você precise migrar uma carga de trabalho de produção de um grupo de consistência. Você pode clonar o grupo de consistência para

criar uma cópia do workload de produção e mantê-lo como um backup até que a migração seja concluída.


O clone é criado a partir de um snapshot do grupo de consistência que está sendo clonado. O snapshot usado para o clone é feito no momento em que o processo de clonagem é iniciado por padrão. Você pode modificar o comportamento padrão para usar um instantâneo pré-existente.

Mapeamentos de unidades de armazenamento são copiados como parte do processo de clonagem. As políticas de snapshot não são copiadas como parte do processo de clonagem.

É possível criar clones de grupos de consistência armazenados localmente no sistema ASA R2 ou de grupos de consistência replicados para locais remotos.

Clone usando snapshot local

Passos


1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja clonar.
3.  Selecione e, em seguida, selecione **Clone**.
4. Insira um nome para o clone do grupo de consistência ou aceite o nome padrão.
5. Selecione o sistema operacional do host.
6. Se você quiser dissociar o clone do grupo de consistência de origem e alocar espaço em disco, selecione **Split clone**.
7. Se você quiser usar um snapshot existente, criar um novo grupo de hosts ou adicionar um novo host para o clone, selecione **mais opções**.

Opção	Passos
Use um instantâneo existente	<ol style="list-style-type: none">a. Em Snapshot to clone, selecione Use an existing snapshot.b. Selecione o instantâneo que deseja usar para o clone.
Crie um novo grupo de hosts	<ol style="list-style-type: none">a. Em Host mapping, selecione New host group.b. Insira um nome para o novo grupo de hosts; em seguida, selecione os iniciadores de host a serem incluídos no grupo.
Adicione um novo host	<ol style="list-style-type: none">a. Em Host mapping, selecione New hosts.b. Introduza o nome do novo nome de anfitrião; em seguida, selecione FC ou iSCSI.c. Selecione os iniciadores do host na lista de iniciadores existentes ou selecione Adicionar iniciador para adicionar novos iniciadores para o host.

8. Selecione **Clone**.

Clone usando snapshot remoto

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Passe o Mouse sobre o **Source** que você deseja clonar.
3.  Selecione e, em seguida, selecione **Clone**.
4. Selecione o cluster de origem e a VM de armazenamento; em seguida, introduza um nome para o novo grupo de consistência ou aceite o nome predefinido.
5. Selecione o instantâneo para clonar; em seguida, selecione **Clone**.

O que se segue?

Clonou um grupo de consistência a partir da sua localização remota. O novo grupo de consistência está disponível localmente no seu sistema ASA R2 para ser usado conforme necessário.

O que se segue?

Para proteger seus dados, você deve "[criar instantâneos](#)" do grupo de consistência clonada.

Clone de grupo de consistência dividida

Quando você divide um clone de grupo de consistência, dissocia o clone do grupo de consistência de origem e aloca espaço em disco para o clone. O clone se torna um grupo de consistência autônomo que pode ser usado independentemente do grupo de consistência de origem.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o clone do grupo de consistência que você deseja dividir.
3. Selecione **Split clone**.
4. Selecione **Split**.

Resultado

O clone é dissociado do grupo de consistência de origem e o espaço em disco é alocado para o clone.

Gerenciar grupos de hosts

Crie grupos de hosts no seu sistema ASA r2

Em um sistema ASA R2, um *grupo de hosts* é o mecanismo usado para dar aos hosts acesso a unidades de armazenamento. Um grupo de hosts se refere a um iggroup para hosts SCSI ou a um subsistema NVMe para hosts NVMe. Um host só pode ver as unidades de armazenamento mapeadas para os grupos de hosts aos quais pertence. Quando um grupo de hosts é mapeado para uma unidade de armazenamento, os hosts que são membros do grupo são então capazes de montar (criar diretórios e estruturas de arquivo) a unidade de armazenamento.

Os grupos de hosts são criados automaticamente ou manualmente quando você cria suas unidades de storage. Opcionalmente, você pode usar as etapas a seguir para criar grupos de hosts antes ou depois da criação da unidade de armazenamento.

Passos

1. No System Manager, selecione **Host**.
2. Selecione os hosts que você deseja adicionar ao grupo de hosts.

Depois de selecionar o primeiro host, a opção para adicionar a um grupo de hosts aparece acima da lista de hosts.

3. Selecione **Adicionar ao grupo anfitrião**.
4. PESQUISE e selecione o grupo de hosts ao qual você deseja adicionar o host.

O que se segue?

Você criou um grupo de hosts e agora pode ["mapeie-o para uma unidade de armazenamento"](#) .

Excluir um grupo de hosts no seu sistema ASA r2

Em um sistema ASA r2, um grupo de hosts é o mecanismo usado para conceder aos hosts acesso às unidades de armazenamento. Um grupo de hosts refere-se a um igroup para hosts SCSI ou a um subsistema NVMe para hosts NVMe. Um host só pode ver as unidades de armazenamento mapeadas aos grupos de hosts aos quais pertence. Talvez você queira excluir um grupo de hosts se não quiser mais que os hosts do grupo tenham acesso às unidades de armazenamento mapeadas a ele.

Passos

1. No System Manager, selecione **Storage**.
2. Em **Mapeamento de host**, selecione o grupo de hosts que você deseja excluir.
3. Selecione **Armazenamento mapeado**.
4. Selecione **Mais**; depois selecione **Excluir**.
5. Selecione para verificar se você deseja continuar; depois selecione **Excluir**.

O que se segue?

O grupo de hosts é excluído. Os hosts que estavam no grupo não têm mais acesso às unidades de armazenamento mapeadas para o grupo de hosts.

Gerenciar unidades de armazenamento

Modificar unidades de storage em sistemas de storage ASA R2

Para otimizar o desempenho no seu sistema ASA r2, pode ser necessário modificar suas unidades de storage para aumentar a capacidade, atualizar as políticas de QoS ou alterar os hosts mapeados para as unidades. Por exemplo, se uma nova carga de trabalho crítica de um aplicativo for adicionada a uma unidade de storage existente, pode ser necessário alterar a política de Quality of Service (QoS) aplicada à unidade de storage para suportar o nível de desempenho necessário para o novo aplicativo.

Aumentar a capacidade

Aumente o tamanho de uma unidade de armazenamento antes de atingir a capacidade máxima para evitar a perda de acesso aos dados que pode ocorrer se a unidade de armazenamento ficar sem espaço gravável. A capacidade de uma unidade de armazenamento pode ser aumentada para 128 TB, que é o tamanho máximo permitido pela ONTAP.

Modifique mapeamentos de host

Modifique os hosts mapeados para uma unidade de storage para auxiliar no balanceamento de cargas de trabalho ou na reconfiguração de recursos do sistema.

Modificar política de QoS

As políticas de qualidade do serviço (QoS) garantem que a performance de workloads essenciais não seja degradada pelos workloads da concorrência. Você pode usar políticas de QoS para definir uma taxa de transferência de QoS *limit* e uma taxa de transferência de QoS *guarantee*.


- Limite de taxa de transferência de QoS

A taxa de transferência de QoS *limit* restringe o impacto de um workload nos recursos do sistema, limitando a taxa de transferência do workload a um número máximo de IOPS ou Mbps, ou IOPS e Mbps.

- Garantia de taxa de transferência de QoS

A taxa de transferência de QoS *guarantee* garante que workloads críticos atendam aos destinos mínimos de taxa de transferência, independentemente da demanda por workloads da concorrência, garantindo que a taxa de transferência para o workload crítico não fique abaixo de um número mínimo de IOPS ou Mbps, ou IOPS e Mbps.

Passos

1. No System Manager, selecione **Storage**.
2. Passe o Mouse sobre o nome da unidade de armazenamento que você deseja editar.
3.  Selecione ; em seguida, selecione **Editar**.
4. Atualize os parâmetros da unidade de armazenamento conforme necessário para aumentar a capacidade, alterar a política de QoS e atualizar o mapeamento do host.

O que se segue?

Se tiver aumentado o tamanho da sua unidade de armazenamento, tem de voltar a digitalizar a unidade de armazenamento no anfitrião para que o anfitrião reconheça a alteração de tamanho.

Mova unidades de storage nos sistemas de storage ASA R2


Se uma zona de disponibilidade de storage estiver com pouco espaço, você poderá mover unidades de armazenamento para outra zona de disponibilidade de armazenamento para equilibrar a utilização de armazenamento no cluster.

Você pode mover uma unidade de armazenamento enquanto a unidade de armazenamento está on-line e fornecendo dados. A operação de movimentação não causa interrupções.

Antes de começar

- Você deve estar executando o ONTAP 9.16,1 ou posterior.
- O cluster precisa ser composto por quatro ou mais nós.

Passos

1. No System Manager, selecione **Storage** (armazenamento) e, em seguida, selecione a unidade de armazenamento que pretende mover.
2.  Selecione ; em seguida, selecione **mover**.
3. Selecione a zona de disponibilidade de armazenamento para a qual pretende mover a unidade de armazenamento; em seguida, selecione **mover**.


Excluir unidades de armazenamento em sistemas de armazenamento ASA R2

Elimine uma unidade de armazenamento se já não necessitar de manter os dados contidos na unidade. A exclusão de unidades de armazenamento que não são mais necessárias pode ajudá-lo a liberar espaço necessário para outros aplicativos host.

Antes de começar

Se a unidade de armazenamento que você deseja excluir estiver em um grupo de consistência que esteja em um relacionamento de replicação, você deverá ["retire a unidade de armazenamento do grupo de consistência"](#) antes de excluí-lo.

Passos

1. No System Manager, selecione **Storage**.
2. Passe o Mouse sobre o nome da unidade de armazenamento que você deseja excluir.
3.  Selecione ; em seguida, selecione **Delete**.
4. Reconheça que a exclusão não pode ser desfeita.
5. Selecione **Eliminar**.

O que se segue?

Você pode usar o espaço liberado da unidade de armazenamento excluída para ["aumente o tamanho"](#) unidades de armazenamento que precisam de capacidade adicional.

Migrar VMs de armazenamento

Migrar uma VM de armazenamento de um cluster ASA para um cluster ASA R2.

A partir do ONTAP 9.18.1, você pode migrar uma máquina virtual (VM) de armazenamento de qualquer cluster ASA para qualquer cluster ASA R2 sem interrupções. A migração de um cluster ASA para um cluster ASA r2 permite adotar a arquitetura simplificada e otimizada dos sistemas ASA r2 para ambientes exclusivamente SAN.

A migração de máquinas virtuais de armazenamento entre sistemas de armazenamento ASA e ASA R2 é suportada da seguinte forma:

De qualquer um dos seguintes sistemas ASA :	Para qualquer um dos seguintes sistemas ASA r2:
<ul style="list-style-type: none">• ASA C800• ASA C400• ASA C250• ASA A900• ASA A800• ASA A400• ASA A250• ASA A150• ASA AFF A800• ASA AFF A700• ASA AFF A400• ASA AFF A250• ASA AFF A220	<ul style="list-style-type: none">• ASA A1K• ASA C30• ASA A90• ASA A70• ASA A50• ASA A30• ASA A20



Para obter a lista mais atualizada de sistemas ASA e ASA r2, consulte "[NetApp Hardware Universe](#)". Os sistemas ASA r2 estão listados no NetApp Hardware Universe como "ASA Série A/Série C (Novo)".

Você só pode migrar uma VM de armazenamento para um cluster ASA r2 a partir de um cluster ASA. A migração de qualquer outro tipo de sistema ONTAP não é suportada.

Antes de começar

Todos os nós do cluster ASA r2 e o próprio cluster ASA devem estar executando o ONTAP 9.18.1 ou posterior. As versões de patch do ONTAP 9.18.1 nos nós do cluster podem variar.

Etapa 1: Verifique o status da VM de armazenamento ASA

Antes de migrar uma VM de armazenamento de um sistema ASA, não deve haver namespaces NVMe ou vVols presentes, e cada volume na VM de armazenamento deve conter apenas um LUN. A migração de namespaces NVMe e vVols não é suportada. A arquitetura dos sistemas ASA r2 exige que os volumes contenham um único LUN.

Passos

1. Verifique se não há namespaces NVMe presentes na máquina virtual de armazenamento:

```
vserver nvme namespace show -vserver <storage_VM>
```

Se as entradas forem exibidas, os objetos NVMe devem ser "[convertido](#)" para LUNs ou removidos. Veja o `vserver nvme namespace delete` e o `vserver nvme subsystem delete` comandos no "[Referência do comando ONTAP](#)" Para obter mais informações.

2. Verifique se não há vVols presentes na VM de armazenamento:

```
lun show -vserver <storage_VM> -class protocol-endpoint,vvol
```

Caso existam vVols, eles devem ser copiados para outra VM de armazenamento e, em seguida, excluídos da VM de armazenamento a ser migrada. Veja o `lun copy` e `lun delete` comandos no "[Referência do comando ONTAP](#)" Para obter mais informações.

3. Verifique se cada volume na máquina virtual de armazenamento contém um único LUN:

```
lun show -vserver <storage_VM>
```

Se um volume contiver mais de um LUN, use o `volume create` e `lun move` comandos para criar uma relação de volume para LUN de 1:1. Veja o "[Referência do comando ONTAP](#)" para mais informações.

O que vem a seguir?

Você está pronto para criar uma relação de pares de cluster entre seus clusters ASA e ASA R2.

Etapa 2: Crie uma relação de pares de cluster entre seus clusters ASA e ASA R2.

Antes de migrar uma VM de armazenamento de um cluster ASA para um cluster ASA R2, você precisa criar uma relação de pares. Uma relação ponto a ponto define conexões de rede que permitem que clusters ONTAP e máquinas virtuais de armazenamento troquem dados com segurança.

Antes de começar

Você deve ter criado LIFs intercluster em todos os nós dos clusters que estão sendo interligados, usando um dos seguintes métodos.

- ["Configure LIFs intercluster em portas de dados compartilhadas."](#)
- ["Configure LIFs intercluster em portas de dados dedicadas."](#)
- ["Configure LIFs entre clusters em espaços IP personalizados."](#)

Passos

1. No cluster ASA r2, crie uma relação de pares com o cluster ASA e gere uma senha:

```
cluster peer create -peer-addr <ASA_cluster_LIF_IPs> -generate  
-passphrase
```

O exemplo a seguir cria uma relação de pares entre o cluster 1 e o cluster 2 e gera uma senha automática pelo sistema:

```
cluster1::> cluster peer create -peer-addr 10.98.191.193 -generate  
-passphrase  
Passphrase: UCa+6lRVICXeL/gq1WrK7ShR  
Peer Cluster Name: cluster2  
Initial Allowed Vserver Peers: -  
Expiration Time: 6/7/2017 09:16:10 +5:30  
Intercluster LIF IP: 10.140.106.185  
Warning: make a note of the passphrase - it cannot be displayed again.
```

2. Copie a senha gerada.
3. No cluster ASA , crie uma relação de pares com o cluster ASA r2:

```
cluster peer create -peer-addr <ASA_r2_LIF_IPs>
```

4. Digite a senha gerada no cluster ASA r2.
5. Verifique se a relação de pares do cluster foi criada:

```
cluster peer show
```

O exemplo a seguir exibe a saída esperada para clusters emparelhados com sucesso.

```
cluster1::> cluster peer show
```

Peer Cluster Name	Cluster Serial Number	Availability	
Authentication			
-----	-----	-----	

cluster2	1-80-123456	Available	ok

Resultado

Os clusters ASA e ASA R2 estão interligados e os dados das máquinas virtuais de armazenamento podem ser transferidos com segurança.

O que vem a seguir?

Você está pronto para preparar sua VM de armazenamento ASA para migração.

Etapa 3: Prepare-se para a migração da VM de armazenamento de um cluster ASA para um cluster ASA R2.

Antes de migrar uma máquina virtual (VM) de armazenamento de um cluster ASA para um cluster ASA R2, você deve executar uma verificação prévia de migração e corrigir quaisquer problemas necessários. Não é possível realizar a migração até que a verificação prévia seja concluída com sucesso.

Passo

1. A partir do seu cluster ASA r2, execute a verificação prévia de migração:

```
vserver migrate start -vserver <storage_VM> -source-cluster  
<asa_cluster> -check-only true
```

Caso precise corrigir algum problema para preparar seu cluster ASA para migração, o problema e a ação corretiva serão exibidos. Corrija o problema e repita a verificação prévia até que ela seja concluída com sucesso.

O que vem a seguir?

Você está pronto para migrar sua VM de armazenamento do seu cluster ASA para um cluster ASA R2.

Etapa 4: Migrar uma VM de armazenamento ASA para um cluster ASA R2

Após preparar o cluster ASA e criar a relação de pares necessária com o cluster ASA R2, você pode iniciar a migração da VM de armazenamento.

Ao realizar uma migração de VM de armazenamento, é uma prática recomendada deixar 30% de folga na CPU tanto no cluster ASA quanto no cluster ASA R2 para permitir a execução da carga de trabalho da CPU.

Sobre esta tarefa

Após a migração da máquina virtual de armazenamento, os clientes são automaticamente transferidos para o cluster ASA r2 e a máquina virtual de armazenamento no cluster ASA é removida automaticamente. A migração automática e a remoção automática de máquinas virtuais de armazenamento estão ativadas por padrão. Opcionalmente, você pode desativá-los e realizar a migração e a remoção da máquina virtual de armazenamento manualmente.

Antes de começar

- O cluster ASA r2 deve ter espaço livre suficiente para acomodar a VM de armazenamento migrada.
- Se a máquina virtual de armazenamento do ASA contiver volumes criptografados, o gerenciador de chaves integrado ou o gerenciador de chaves externo no sistema ASA r2 deverá ser configurado no nível do cluster.
- As seguintes operações não podem ser executadas no cluster ASA de origem:
 - operações de failover
 - WAFLIRON
 - Impressão digital
 - Movimentação, rehostedagem, clonagem, criação, conversão ou análise de volume

Passos

1. A partir do cluster ASA r2, inicie a migração da VM de armazenamento:

```
vserver migrate start -vserver <storage_VM_name> -source-cluster  
<ASA_cluster>
```

Para desativar a transição automática, use o `-auto-cutover false` parâmetro. Para desativar a remoção automática da VM de armazenamento ASA, use o `-auto-source-cleanup false` parâmetro.

2. Acompanhe o andamento da migração.

```
vserver migrate show -vserver <storage_VM_name>
```

Quando a migração estiver concluída, o **status** será exibido como **migration-complete**.



Se precisar pausar ou cancelar a migração antes do início da transição automática, use o `vserver migrate pause` e o `vserver migrate abort` comandos. Você deve pausar a migração antes de cancelá-la. Não é possível cancelar a migração após o início do processo de transição.

Resultado

A máquina virtual de armazenamento foi migrada do cluster ASA para o cluster ASA R2. O nome e o UUID da máquina virtual de armazenamento, o nome da LIF de dados, o endereço IP e os nomes dos objetos, como o nome do volume, permanecem inalterados. Os UUIDs dos objetos migrados na VM de armazenamento são atualizados.

O que vem a seguir?

Se você desativou a migração automática e a remoção automática de máquinas virtuais de armazenamento, "[Migre manualmente seus clientes ASA para o cluster ASA R2 e remova a VM de armazenamento do cluster ASA.](#)" .

Migrar clientes e limpar a VM de armazenamento de origem após a migração para um sistema ASA r2.

Após uma máquina virtual (VM) de armazenamento ser migrada de um cluster ASA para

um cluster ASA R2, por padrão, os clientes são automaticamente transferidos para o cluster ASA R2 e a VM de armazenamento no cluster ASA é removida automaticamente. Se você optou por desativar a transferência e remoção automáticas da VM de armazenamento ASA durante a migração, será necessário executar essas etapas manualmente após a conclusão da migração.

Migrar manualmente os clientes para um sistema ASA r2 após a migração de uma máquina virtual de armazenamento.

Se você desativar a transição automática de clientes durante a migração de uma VM de armazenamento de um cluster ASA para um cluster ASA R2, após a conclusão bem-sucedida da migração, execute a transição manualmente para que a VM de armazenamento ASA R2 possa fornecer dados aos clientes.

Passos

1. No cluster ASA r2, execute manualmente a migração do cliente:

```
vserver migrate cutover -vserver <storage_VM_name>
```

2. Verifique se a operação de transição foi concluída:

```
vserver migrate show
```

Resultado

Os dados estão sendo fornecidos aos seus clientes a partir da máquina virtual de armazenamento no seu cluster ASA r2.

O que vem a seguir?

Agora você está pronto para remover a VM de armazenamento do cluster ASA de origem.

Remover manualmente uma VM de armazenamento ASA após a migração para um cluster ASA R2

Se você desativar a limpeza automática da origem durante a migração de uma VM de armazenamento de um cluster ASA para um cluster ASA R2, após a conclusão da migração, remova a VM de armazenamento do cluster ASA para liberar espaço de armazenamento.

Antes de começar

Seus clientes devem estar fornecendo dados do cluster ASA r2.

Passos

1. No cluster ASA , verifique se o status da VM de armazenamento ASA é **Pronto para limpeza de origem**:

```
vserver migrate show
```

2. Remova a VM de armazenamento ASA :

```
vserver migrate source-cleanup -vserver <storage_VM_name>
```

Resultado

A máquina virtual de armazenamento no seu cluster ASA foi removida.

Limites de armazenamento do ASA R2

Para obter o melhor desempenho, configuração e suporte, você deve estar ciente dos limites de armazenamento do ASA r2.

Para obter uma lista completa dos limites de armazenamento mais atuais do ASA R2, "[NetApp Hardware Universe](#)" consulte .

Os sistemas ASA r2 suportam os seguintes limites de armazenamento:

	Máximo por par de HA	Máximo por grupo
Grupos de consistência	256	256
Aplicações empresariais	100	350
Nós	2	12
Grupos de replicação	50	50
Tamanho da zona de disponibilidade de armazenamento	2 PB	2 PB
Unidades de armazenamento	10.000	30.000
Tamanho da unidade de armazenamento	128 TB	128 TB
Unidades de armazenamento por grupo de consistência	256	256
Grupos de consistência infantil por grupo de consistência parental	64	64
Máquinas virtuais de armazenamento	<ul style="list-style-type: none">• 256 (ONTAP 9.18.1 e posterior)• 32 (ONTAP 9.17.1 e versões anteriores)	<ul style="list-style-type: none">• 256 (ONTAP 9.18.1 e posterior)• 32 (ONTAP 9.17.1 e versões anteriores)
Máquinas virtuais	800	1200

Limites para relacionamentos assíncronos do SnapMirror

Os limites a seguir se aplicam a unidades de armazenamento e grupos de consistência em um relacionamento de replicação assíncrona do SnapMirror . Para obter uma lista completa dos limites de armazenamento mais recentes do ASA r2, "[NetApp Hardware Universe](#)" .

Limite máximo	Por par de HA	Por cluster
Grupos de consistência	250	750
Unidades de armazenamento	4.000	6.000

Limites para relacionamento de sincronização ativa do SnapMirror

Os limites a seguir se aplicam a unidades de armazenamento e grupos de consistência em um relacionamento de replicação de sincronização ativa do SnapMirror. A sincronização ativa do SnapMirror é suportada a partir do ONTAP 9.17.1, somente em clusters de dois nós. A partir do ONTAP 9.18.1, a sincronização ativa do SnapMirror é suportada em clusters de quatro nós.

Para obter uma lista completa dos limites de armazenamento mais recentes do ASA r2, "[NetApp Hardware Universe](#)".

Limite máximo	Por par de HA
Grupos de consistência	50
Unidades de armazenamento	400

Proteja seus dados

Crie snapshots para fazer backup de seus dados em sistemas de storage ASA R2

Crie um snapshot para fazer backup dos dados no seu sistema ASA r2. Utilize o ONTAP System Manager para criar um snapshot manual de uma única unidade de armazenamento ou para criar um grupo de consistência e agendar snapshots automáticos de várias unidades de armazenamento simultaneamente.

Passo 1: Opcionalmente, crie um grupo de consistência

Um grupo de consistência é uma coleção de unidades de armazenamento que são gerenciadas como uma única unidade. Crie grupos de consistência para simplificar o gerenciamento de storage e a proteção de dados para workloads de aplicações que abrangem várias unidades de storage. Por exemplo, suponha que você tenha um banco de dados composto por 10 unidades de armazenamento em um grupo de consistência, e você precisa fazer backup de todo o banco de dados. Em vez de fazer backup de cada unidade de armazenamento, você pode fazer backup de todo o banco de dados simplesmente adicionando proteção de dados snapshot ao grupo de consistência.

Crie um grupo de consistência usando novas unidades de armazenamento ou crie um grupo de consistência usando unidades de armazenamento existentes.

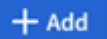
A partir do ONTAP 9.18.1, você pode definir a porcentagem de reserva de snapshots e habilitar a exclusão automática de snapshots ao criar um grupo de consistência com novas unidades de armazenamento. A reserva de snapshots é a quantidade de espaço na unidade de armazenamento reservada especificamente para snapshots. Quando a reserva de snapshots está configurada com exclusão automática de snapshots, os snapshots mais antigos são excluídos automaticamente quando o espaço usado pelos snapshots excede a reserva de snapshots. Se a reserva de snapshots e a exclusão automática de snapshots estiverem ativadas em um grupo de consistência pai, elas serão ativadas em todos os grupos de consistência filho existentes. Se novos grupos de consistência filhos forem adicionados, eles não herdarão as configurações de reserva e exclusão de instantâneos do grupo pai.

"[Saiba mais sobre a reserva de snapshots em sistemas de armazenamento ASA r2.](#)"

A partir do ONTAP 9.16.1, ao criar grupos de consistência usando novas unidades de armazenamento, você pode configurar até cinco grupos de consistência filhos. "[Saiba mais sobre grupos de consistência infantil em sistemas ASA r2.](#)"

Use novas unidades de armazenamento

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2.  Selecione ; em seguida, selecione **usando novas unidades de armazenamento**.
3. Introduza um nome para a nova unidade de armazenamento, o número de unidades e a capacidade por unidade.

Se você criar mais de uma unidade, cada unidade será criada com a mesma capacidade e o mesmo sistema operacional host por padrão. Opcionalmente, você pode atribuir uma capacidade diferente a cada unidade.

4. Se você quiser fazer qualquer uma das seguintes opções, selecione **mais opções** e conclua as etapas necessárias.

Opção	Passos
Atribua uma capacidade diferente a cada unidade de armazenamento	Selecione Adicionar uma capacidade diferente .
Altere o nível de serviço de desempenho padrão	Em nível de serviço de desempenho , selecione um nível de serviço diferente. Os sistemas ASA r2 oferecem dois níveis de desempenho. O nível de desempenho padrão é Extremo , que é o nível mais alto disponível. Você pode reduzir o nível de desempenho para Desempenho .
Modifique a reserva de snapshots padrão e habilite a exclusão automática de snapshots.	a. Em Reserva de snapshots % , insira o valor numérico correspondente à porcentagem do espaço da unidade de armazenamento que você deseja alocar para snapshots. b. Selecione Excluir automaticamente snapshots antigos .
Crie um grupo de consistência filho	Selecione Adicionar grupo de consistência filho .

5. Selecione o sistema operacional do host e o mapeamento do host.
6. Selecione **Adicionar**.

O que se segue?

Você criou um grupo de consistência contendo as unidades de armazenamento que deseja proteger. Agora você pode criar um instantâneo.

Use unidades de armazenamento existentes

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2.  Selecione ; em seguida, selecione **usando unidades de armazenamento existentes**.

3. Introduza um nome para o grupo de consistência; em seguida, procure e selecione as unidades de armazenamento que pretende incluir no grupo de consistência.

4. Selecione **Adicionar**.

O que se segue?

Você criou um grupo de consistência contendo as unidades de armazenamento que deseja proteger. Agora você pode criar um instantâneo.

Passo 2: Crie um instantâneo

Um instantâneo é uma cópia local e somente leitura de seus dados que você pode usar para restaurar unidades de armazenamento em pontos específicos no tempo.

Os instantâneos podem ser criados sob demanda ou podem ser criados automaticamente em intervalos regulares com base em um "[política e agendamento de snapshot](#)". A política e a programação de snapshot especificam quando criar os snapshots, quantas cópias devem ser mantidas, como nomeá-los e como rotulá-los para replicação. Por exemplo, um sistema pode criar um snapshot todos os dias às 12:10 da manhã, reter as duas cópias mais recentes, nomeá-las "diariamente" (anexado com um carimbo de data/hora) e rotulá-las "diariamente" para replicação.

Tipos de instantâneos

Você pode criar um snapshot sob demanda de uma única unidade de armazenamento ou de um grupo de consistência. Você pode criar snapshots automatizados de um grupo de consistência que contém várias unidades de storage. Não é possível criar instantâneos automatizados de uma única unidade de armazenamento.

- Snapshots sob demanda

Você pode criar um instantâneo sob demanda de uma unidade de armazenamento a qualquer momento. A unidade de armazenamento não precisa ser membro de um grupo de consistência para ser protegida por um snapshot sob demanda. Se você criar um snapshot sob demanda de uma unidade de armazenamento que seja membro de um grupo de consistência, as outras unidades de armazenamento no grupo de consistência não serão incluídas no snapshot sob demanda. Se você criar um instantâneo sob demanda de um grupo de consistência, todas as unidades de armazenamento do grupo de consistência serão incluídas no instantâneo.


- Snapshots automatizados

Snapshots automatizados são criados usando políticas de snapshot. Para aplicar uma política de instantâneos a uma unidade de armazenamento para criação automática de instantâneos, a unidade de armazenamento deve ser membro de um grupo de consistência. Se você aplicar uma política de snapshot a um grupo de consistência, todas as unidades de storage do grupo de consistência serão protegidas com snapshots automatizados.

Crie um instantâneo de um grupo de consistência ou de uma unidade de armazenamento.

Instantâneo de um grupo de consistência

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o nome do grupo de consistência que você deseja proteger.
3.  Selecione ; em seguida, selecione **proteger**.
4. Se você quiser criar um instantâneo imediato sob demanda, em **proteção local**, selecione **Adicionar um instantâneo agora**.

A proteção local cria o instantâneo no mesmo cluster que contém a unidade de armazenamento.



- a. Insira um nome para o instantâneo ou aceite o nome padrão; em seguida, opcionalmente, insira um rótulo SnapMirror.

A etiqueta SnapMirror é utilizada pelo destino remoto.

5. Se você quiser criar snapshots automatizados usando uma política de snapshot, selecione **Agendar snapshots**.

- a. Selecione uma política de instantâneos.

Aceite a política de instantâneos padrão, selecione uma política existente ou crie uma nova política.

Opção	Passos
Selecione uma política de instantâneos existente	 Selecione ao lado da política padrão e, em seguida, selecione a política existente que você deseja usar.
Crie uma nova política de snapshot	<ol style="list-style-type: none">i.  Add Selecione ; em seguida, introduza os parâmetros da política de instantâneos.ii. Selecione Adicionar política.

6. Se você quiser replicar seus snapshots para um cluster remoto, em **proteção remota**, selecione **replicar para um cluster remoto**.


- a. Selecione o cluster de origem e a VM de armazenamento e, em seguida, selecione a política de replicação.

A transferência inicial de dados para replicação começa imediatamente por padrão.

7. Selecione **Guardar**.

Instantâneo da unidade de armazenamento

Passos

1. No System Manager, selecione **Storage**.
2. Passe o Mouse sobre o nome da unidade de armazenamento que você deseja proteger.
3.  Selecione ; em seguida, selecione **proteger**. Se você quiser criar um instantâneo imediato sob demanda, em **proteção local**, selecione **Adicionar um instantâneo agora**.

A proteção local cria o instantâneo no mesmo cluster que contém a unidade de armazenamento.

4. Insira um nome para o instantâneo ou aceite o nome padrão; em seguida, opcionalmente, insira um rótulo SnapMirror.

A etiqueta SnapMirror é utilizada pelo destino remoto.

5. Se você quiser criar snapshots automatizados usando uma política de snapshot, selecione **Agendar snapshots**.

- a. Selecione uma política de instantâneos.

Aceite a política de instantâneos padrão, selecione uma política existente ou crie uma nova política.

Opção	Passos
Selecione uma política de instantâneos existente	✓ Selecione ao lado da política padrão e, em seguida, selecione a política existente que você deseja usar.
Crie uma nova política de snapshot	<ol style="list-style-type: none">i. + Add Selecione ; em seguida, introduza os parâmetros da política de instantâneos.ii. Selecione Adicionar política.

6. Se você quiser replicar seus snapshots para um cluster remoto, em **proteção remota**, selecione **replicar para um cluster remoto**.

- a. Selecione o cluster de origem e a VM de armazenamento e, em seguida, selecione a política de replicação.

A transferência inicial de dados para replicação começa imediatamente por padrão.

7. Selecione **Guardar**.

O que se segue?

Agora que seus dados estão protegidos com snapshots, você deve "[configurar a replicação de instantâneos](#)" copiar seus grupos de consistência para um local geograficamente remoto para backup e recuperação de desastres.

Gerenciar reserva de instantâneos

Saiba mais sobre a reserva de snapshots do ONTAP no armazenamento ASA r2.

A reserva de snapshots é a quantidade de espaço na unidade de armazenamento reservada especificamente para snapshots. Quando a reserva de snapshots está configurada com exclusão automática de snapshots, os snapshots mais antigos são excluídos automaticamente quando o espaço usado pelos snapshots excede a reserva de snapshots. Isso impede que os snapshots consumam espaço na sua unidade de armazenamento destinada aos dados do usuário.

A reserva de snapshots é definida como uma porcentagem do tamanho total da unidade de armazenamento.

Por exemplo, se a unidade de armazenamento for de 50 GB e você definir a reserva de snapshots para 10%, a quantidade de espaço reservada para snapshots será de 5 GB. Quando o espaço utilizado pelos snapshots atinge 5 GB, os snapshots mais antigos são excluídos automaticamente para liberar espaço para novos snapshots. Se o tamanho da unidade de armazenamento aumentar para 100 GB, a reserva de snapshots aumentará para 10 GB. A reserva máxima de snapshots que você pode definir é de 200%. Se sua unidade de armazenamento atingir o tamanho máximo de 128 TB, uma reserva de snapshots de 200% permite que você faça 2 snapshots completos.

Por padrão, a reserva de snapshots está definida como 0% e a exclusão automática de snapshots não está habilitada.

A partir do ONTAP 9.18.1, você pode modificar a reserva de snapshots padrão durante ou após a criação de unidades de armazenamento e durante a criação de grupos de consistência. Você também pode modificar a reserva de snapshots padrão em máquinas virtuais (VMs) de armazenamento existentes. No ONTAP 9.17.1 e versões anteriores, não é possível modificar essas configurações.

A reserva de snapshots é definida com a mesma porcentagem para todas as unidades de armazenamento em um grupo de consistência no momento em que o grupo de consistência é criado. A reserva de snapshots deve ser configurada individualmente em todas as unidades de armazenamento adicionadas posteriormente.

Modificar a reserva de snapshots em um sistema de armazenamento ASA r2


A reserva de snapshots é a quantidade de espaço na unidade de armazenamento reservada especificamente para snapshots. Por padrão, a reserva de snapshots está definida como 0%. A partir do ONTAP 9.18.1, você pode modificar a reserva de snapshots padrão da unidade de armazenamento e ativar a exclusão automática de snapshots. A exclusão automática de instantâneos está desativada por padrão. Quando um valor de reserva de snapshots é definido e a exclusão automática de snapshots está ativada, os snapshots mais antigos são excluídos automaticamente quando o espaço usado pelos snapshots excede a reserva de snapshots. Isso impede que os snapshots consumam espaço na sua unidade de armazenamento destinada aos dados do usuário.

["Saiba mais sobre a reserva de snapshots em sistemas de armazenamento ASA r2."](#)

Modificar reserva de snapshots em unidades de armazenamento

Para definir valores de reserva de snapshots diferentes, configure cada unidade de armazenamento individualmente. Para usar o mesmo valor em todas as unidades de armazenamento, modifique a reserva de snapshots na máquina virtual de armazenamento.

Passos

1. No System Manager, selecione **Storage**.
2. Passe o cursor sobre o nome da unidade de armazenamento para a qual deseja definir a reserva de snapshots.
3. Selecione  Em seguida, selecione **Editar**.
4. Em **Reserva de snapshots %**, insira o valor numérico correspondente à porcentagem do espaço da unidade de armazenamento que você deseja alocar para snapshots.
5. Verifique se a opção **Excluir automaticamente snapshots antigos** está selecionada.
6. Selecione **Guardar**.


Resultado

A reserva de snapshots está definida para a porcentagem que você especificou. Se o espaço consumido pelos snapshots atingir o limite reservado, os snapshots mais antigos serão excluídos automaticamente.

Modificar a reserva de snapshots em uma VM de armazenamento

Para definir a mesma reserva de snapshots para todas as unidades de armazenamento em uma VM de armazenamento, aplique a porcentagem desejada à VM de armazenamento. Quando a reserva de snapshots é aplicada à máquina virtual de armazenamento, ela é aplicada a todas as unidades de armazenamento recém-criadas dentro da máquina virtual de armazenamento. Essa configuração não se aplica a unidades de armazenamento criadas antes da modificação da configuração.

Passos

1. No Gerenciador de Sistemas, selecione **Cluster > VMs de Armazenamento**; em seguida, selecione **Configurações**.
2. Em **Políticas**, ao lado de **Instantâneos**, selecione  Em seguida, selecione **Definir/editar reserva de instantâneo padrão**.
3. Em **Reserva de snapshots %**, insira o valor numérico correspondente à porcentagem do espaço da unidade de armazenamento que você deseja alocar para snapshots.
4. Verifique se a opção **Excluir automaticamente snapshots antigos** está selecionada.
5. Selecione **Guardar**.

Resultado

A reserva de snapshots para unidades de armazenamento recém-criadas é definida com a porcentagem especificada. Se a quantidade de espaço consumida pelos snapshots nessas unidades de armazenamento atingir a reserva, os snapshots mais antigos serão excluídos automaticamente.

Crie um relacionamento de pares de VMs de armazenamento intercluster em sistemas de armazenamento ASA r2

Um relacionamento de pares define conexões de rede que permitem que clusters e máquinas virtuais (VMs) de armazenamento troquem dados com segurança. Crie relacionamentos de pares entre VMs de armazenamento em diferentes clusters para permitir a proteção de dados e a recuperação de desastres usando o SnapMirror.

["Saiba mais sobre relacionamentos entre pares"](#) .

Antes de começar

Você deve ter estabelecido um relacionamento de par de cluster entre os clusters local e remoto antes de poder criar um relacionamento de par de VM de armazenamento. "[Criar um relacionamento de pares de cluster](#)" se você ainda não o fez.

Passos

1. No Gerenciador do Sistema, selecione **Proteção > Visão geral**.
2. Em **Pares de VM de armazenamento** selecione **Adicionar um par de VM de armazenamento**.
3. Selecione a VM de armazenamento no cluster local; em seguida, selecione a VM de armazenamento no cluster remoto.
4. Selecione **Adicionar um peer de VM de armazenamento**.

Configurar a replicação de instantâneos

Replique snapshots para um cluster remoto a partir dos sistemas de storage ASA R2

A replicação de instantâneos é um processo no qual os grupos de consistência no seu sistema ASA R2 são copiados para um local remoto geograficamente. Após a replicação inicial, as alterações aos grupos de consistência são copiadas para o local remoto com base em uma política de replicação. Grupos de consistência replicados podem ser usados para recuperação de desastres ou migração de dados.



A replicação de instantâneos para um sistema de armazenamento ASA r2 só é suportada de e para outro sistema de armazenamento ASA r2. Não é possível replicar instantâneos de um sistema ASA r2 para um sistema ASA, AFF ou FAS ou de um sistema ASA, AFF ou FAS para um sistema ASA r2.

Para configurar a replicação Snapshot, é necessário estabelecer uma relação de replicação entre o sistema ASA R2 e o local remoto. A relação de replicação é regida por uma política de replicação. Uma política padrão para replicar todos os snapshots é criada durante a configuração do cluster. Você pode usar a política padrão ou, opcionalmente, criar uma nova política.

A partir do ONTAP 9.17.1, você pode aplicar políticas de replicação assíncrona a grupos de consistência em um relacionamento hierárquico. A replicação assíncrona não é suportada para grupos de consistência em relacionamentos hierárquicos no ONTAP 9.16.1.

["Saiba mais sobre grupos de consistência hierárquicos \(pai/filho\)"](#) .

Passo 1: Crie um relacionamento de pares de cluster

Antes de proteger seus dados replicando-os em um cluster remoto, é necessário criar um relacionamento de peers de clusters entre o cluster local e o cluster remoto.

Antes de começar

Os pré-requisitos para peering de cluster são os mesmos para sistemas ASA r2 e outros sistemas ONTAP . ["Revise os pré-requisitos para o peering de cluster"](#) .

Passos

1. No cluster local, no System Manager, selecione **Cluster > Settings**.
2. Em **Intercluster Settings** ao lado de **Cluster Peers** ; selecione e, em seguida, selecione **Add a cluster peer**.
3. Selecione **Launch Remote cluster**; isso gera uma senha que você usará para autenticar com o cluster remoto.
4. Depois que a frase-passe do cluster remoto for gerada, cole-a em **Passphrase** no cluster local.
5. **+ Add** Selecione ; em seguida, introduza o endereço IP da interface de rede entre clusters.
6. Selecione **Iniciar peering de cluster**.

O que se segue?

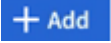
Você fez um pedido para o cluster ASA R2 local com um cluster remoto. Agora você pode criar uma relação de replicação.

Etapa 2: Opcionalmente, crie uma política de replicação personalizada

A política de replicação define quando as atualizações executadas no cluster ASA r2 são replicadas para o site remoto. O ONTAP inclui várias políticas de proteção de dados predefinidas que você pode usar para seus relacionamentos de replicação. Se as políticas predefinidas não atenderem às suas necessidades, você poderá criar uma política de replicação personalizada.

Aprenda sobre ["políticas de proteção de dados ONTAP predefinidas"](#) .

Passos

1. No System Manager, selecione **proteção > políticas**; em seguida, selecione **políticas de replicação**.
2.  Seleccione .
3. Introduza um nome para a política de replicação ou aceite o nome predefinido; em seguida, introduza uma descrição.
4. Selecione o **âmbito da política**.

Se quiser aplicar a política de replicação a todo o cluster, selecione **Cluster**. Se desejar que a diretiva de replicação seja aplicada apenas às unidades de armazenamento em uma VM de armazenamento específica, selecione **Storage VM**.

5. Para o **Tipo de política**, selecione **Assíncrono**.



Com a política assíncrona, os dados são copiados para o site remoto depois de serem gravados na origem. A replicação síncrona não é suportada para sistemas ASA r2.

6. Em **Transferir instantâneos da fonte**, aceite o agendamento de transferência padrão ou selecione outro.
7. Selecione para transferir todos os instantâneos ou para criar regras para determinar quais instantâneos transferir.
8. Opcionalmente, ative a compactação de rede.
9. Selecione **Guardar**.

O que se segue?

Você criou uma política de replicação e agora está pronto para criar uma relação de replicação entre o sistema ASA R2 e o local remoto.

Para mais informações

Saiba mais ["VMs de armazenamento para acesso ao cliente"](#)sobre o .

Passo 3: Crie uma relação de replicação

Uma relação de replicação de snapshot estabelece uma conexão entre o sistema ASA R2 e um local remoto para que você possa replicar grupos de consistência para um cluster remoto. Os grupos de consistência replicados podem ser usados para recuperação de desastres ou para migração de dados.

Para proteção contra ataques de ransomware, ao configurar sua relação de replicação, você pode optar por bloquear os snapshots de destino. Os instantâneos bloqueados não podem ser eliminados acidentalmente ou maliciosamente. Use snapshots bloqueados para recuperar dados se uma unidade de storage for comprometida por um ataque de ransomware.

Antes de começar

- ["Saiba mais sobre políticas de replicação"](#) .


Ao criar um relacionamento de replicação, você deve selecionar a política de replicação apropriada para seu relacionamento de replicação. Você pode usar uma política predefinida ou criar uma política personalizada.

- Se quiser bloquear os instantâneos de destino, tem de "[Inicialize o relógio de conformidade do Snapshot](#)" antes de criar a relação de replicação.

Crie uma relação de replicação com ou sem instantâneos de destino bloqueados.

Com instantâneos bloqueados

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Selecione um grupo de consistência.
3.  Selecione ; em seguida, selecione **proteger**.
4. Em **proteção remota**, selecione **replicar para um cluster remoto**.
5. Selecione a política **replicação**.

Você deve selecionar uma política de replicação *Vault*.

6. Selecione **Definições de destino**.
7. Selecione **Bloquear instantâneos de destino para evitar a exclusão**
8. Introduza o período máximo e mínimo de retenção de dados.
9. Para atrasar o início da transferência de dados, desmarque **Iniciar transferência imediatamente**.

A transferência inicial de dados começa imediatamente por padrão.

10. Opcionalmente, para substituir o agendamento de transferência padrão, selecione **Configurações de destino** e, em seguida, selecione **Substituir agendamento de transferência**.


Seu plano de transferência deve ser de no mínimo 30 minutos para ser suportado.


11. Selecione **Guardar**.

Sem instantâneos bloqueados

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Selecione para criar a relação de replicação com o destino local ou a origem local.

Opção	Passos
Destinos locais	<ol style="list-style-type: none">a. Selecione destinos locais e, em seguida,  selecione .b. Procure e selecione o grupo de consistência de origem. <p>O grupo de consistência <i>source</i> refere-se ao grupo de consistência no cluster local que você deseja replicar.</p>

Opção	Passos
Fontes locais	<ol style="list-style-type: none"> Selecione fontes locais e, em seguida,  selecione . Procure e selecione o grupo de consistência de origem. Em destino de replicação, selecione o cluster para o qual replicar; em seguida, selecione a VM de armazenamento.

- Selecione uma política de replicação.
- Para atrasar o início da transferência de dados, selecione **Definições de destino**; em seguida, desmarque **Iniciar transferência imediatamente**.

A transferência inicial de dados começa imediatamente por padrão.

- Opcionalmente, para substituir o agendamento de transferência padrão, selecione **Configurações de destino** e, em seguida, selecione **Substituir agendamento de transferência**.

Seu plano de transferência deve ser de no mínimo 30 minutos para ser suportado.

- Selecione **Guardar**.


O que se segue?

Agora que você criou uma política de replicação e um relacionamento, sua transferência de dados inicial começa conforme definido na política de replicação. Opcionalmente, você pode testar o failover de replicação para verificar se o failover bem-sucedido pode ocorrer se o sistema ASA R2 ficar offline.

Etapa 4: Teste o failover de replicação

Opcionalmente, valide que você pode fornecer dados com êxito de unidades de armazenamento replicadas em um cluster remoto se o cluster de origem estiver offline.

Passos

- No System Manager, selecione **proteção > replicação**.
- Passo o Mouse sobre a relação de replicação que você deseja testar e  selecione .
- Selecione **failover de teste**.
- Insira as informações de failover e, em seguida, selecione **failover de teste**.

O que se segue?

Agora que seus dados estão protegidos com replicação snapshot para recuperação de desastres, você deve **"criptografia de dados em repouso"** fazê-lo para que não possa ser lido se um disco no sistema ASA R2 for reutilizado, devolvido, extraviado ou roubado.

Saiba mais sobre as políticas de proteção de dados predefinidas do ONTAP

A política de replicação define quando as atualizações executadas no cluster ASA r2 são replicadas para o site remoto. O ONTAP inclui várias políticas de proteção de dados predefinidas que você pode usar para seus relacionamentos de replicação.

Se as políticas predefinidas não atenderem às suas necessidades, você pode ["criar uma política de replicação personalizada"](#) .



Os sistemas ASA r2 não suportam replicação síncrona.

Os sistemas ASA r2 suportam as seguintes políticas de proteção predefinidas.


Política	Descrição	Tipo de política
Assíncrono	Uma política unificada de cofre e assíncrona do SnapMirror para espelhar o sistema de arquivos ativo mais recente e instantâneos diários e semanais com um cronograma de transferência por hora.	Assíncrono
FailOverDuplex Automatizado	Política para SnapMirror síncrono com garantia de RTO zero e replicação de sincronização bidirecional.	Sincronização ativa do SnapMirror
CloudBackupPadrão	Política de cofre com regra diária.	Assíncrono
Backup diário	Política de cofre com uma regra diária e um cronograma de transferência diário.	Assíncrono
DPDefault	Política assíncrona do SnapMirror para espelhar todos os instantâneos e o último sistema de arquivos ativo.	Assíncrono
MirrorAllSnapshots	Política assíncrona do SnapMirror para espelhar todos os instantâneos e o último sistema de arquivos ativo.	Assíncrono
MirrorAllSnapshotsDiscardNetwork	Política assíncrona do SnapMirror para espelhar todos os instantâneos e o último sistema de arquivos ativo, excluindo as configurações de rede.	Assíncrono
Espelho e Cofre	Uma política unificada assíncrona e de cofre do SnapMirror para espelhar o sistema de arquivos ativo mais recente e instantâneos diários e semanais.	Assíncrono
Rede de descarte de espelho e cofre	Uma política unificada de cofre e assíncrona do SnapMirror para espelhar o sistema de arquivos ativo mais recente e instantâneos diários e semanais, excluindo as configurações de rede.	Assíncrono
MirrorLatest	Política assíncrona do SnapMirror para espelhar o último sistema de arquivos ativo.	Assíncrono
Unified7year	Política unificada do SnapMirror com retenção de 7 anos.	Assíncrono
XDPPadrão	Política de cofre com regras diárias e semanais.	Assíncrono

Interrompa um relacionamento de replicação assíncrona no seu sistema ASA r2

Em certas situações, pode ser necessário interromper um relacionamento de replicação assíncrona. Por exemplo, se você estiver executando o ONTAP 9.16.1 e quiser aumentar o tamanho de um grupo de consistência que está em um relacionamento de replicação

assíncrona, será necessário quebrar o relacionamento antes de poder modificar o tamanho do grupo de consistência.

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Selecione **Destinos locais** ou **Fontes locais**.
3. Ao lado do relacionamento que você deseja interromper, selecione  ; então selecione **Quebrar**.
4. Selecione **Quebrar**.

Resultado

O relacionamento assíncrono entre o grupo de consistência primário e secundário é quebrado.

Configurar sincronização ativa do SnapMirror

Fluxo de trabalho de configuração de sincronização ativa do SnapMirror

A proteção de dados de sincronização ativa do ONTAP SnapMirror permite que os serviços empresariais continuem operando mesmo em caso de falha total do site, permitindo que os aplicativos realizem failover de forma transparente usando uma cópia secundária. Com a sincronização ativa do SnapMirror , não é necessária intervenção manual ou script personalizado para acionar um failover.

Embora os procedimentos do System Manager para configurar a sincronização ativa do SnapMirror sejam diferentes em sistemas ASA r2 do que em sistemas NetApp FAS, AFF e ASA que executam a personalidade ONTAP unificada, os requisitos, a arquitetura e a operação da sincronização ativa do SnapMirror são os mesmos.

Sobre esta tarefa

A partir do ONTAP 9.18.1, a sincronização ativa do SnapMirror é suportada em configurações de quatro nós. No ONTAP 9.17.1, a sincronização ativa do SnapMirror é suportada apenas em configurações de dois nós.

["Saiba mais sobre recuperação de desastres com sincronização ativa SnapMirror no seu sistema ASA r2"](#)

Em sistemas ASA r2, a sincronização ativa do SnapMirror suporta configurações simétricas ativa/ativa. Em uma configuração simétrica ativa/ativa, ambos os sites podem acessar o armazenamento local para E/S ativa.

Saiba mais sobre ["configurações simétricas ativas/ativas"](#) .

1

Prepare-se para configurar a sincronização ativa do SnapMirror .

Para ["prepare-se para configurar a sincronização ativa do SnapMirror"](#) no seu sistema ASA r2, você deve revisar os pré-requisitos de configuração, confirmar o suporte para seus sistemas operacionais host e estar ciente dos limites de objetos que podem afetar a configuração específica.

2

Confirme a configuração do seu cluster.

Antes de configurar a sincronização ativa do SnapMirror , você deve ["confirme se seus clusters ASA r2 estão nos relacionamentos de peering adequados e atendem a outros requisitos de configuração"](#) .

3**Instale o ONTAP Mediator.**

Você pode usar o ONTAP Mediator ou o ONTAP Cloud Mediator para monitorar a integridade do seu cluster e garantir a continuidade dos negócios. Se estiver usando o ONTAP Mediator, você deve: ["instale-o"](#) no seu host. Se estiver usando o ONTAP Cloud Mediator, você pode pular esta etapa.

4**Configure o ONTAP Mediator ou o ONTAP Cloud Mediator usando certificados autoassinados.**

Você deve ["configurar o mediador ONTAP ou o mediador de nuvem ONTAP"](#) antes de poder começar a usá-lo com o SnapMirror Active Sync para monitoramento de cluster.

5**Configurar sincronização ativa do SnapMirror .**

["Configurar sincronização ativa do SnapMirror"](#) para criar uma cópia dos seus dados em um site secundário e permitir que seus aplicativos host façam failover de forma automática e transparente no caso de um desastre.

Informações relacionadas

- ["Saiba mais sobre a sincronização ativa do SnapMirror"](#) .
- ["Saiba mais sobre as personalidades da ONTAP"](#).

Preparar para configurar a sincronização ativa do SnapMirror em sistemas ASA r2

Para se preparar para configurar a sincronização ativa do SnapMirror no seu sistema ASA r2, você deve revisar os pré-requisitos de configuração, confirmar o suporte para os sistemas operacionais dos seus hosts e estar ciente dos limites de objetos que podem afetar a configuração específica.

Passos

1. Revise a sincronização ativa do SnapMirror ["pré-requisitos"](#) .
2. ["Confirme se os sistemas operacionais do seu host são suportados"](#) para sincronização ativa do SnapMirror .
3. Revise o ["limites do objeto"](#) que podem impactar sua configuração.
4. Verifique o suporte do protocolo do host para sincronização ativa do SnapMirror no seu sistema ASA r2.

O suporte para sincronização ativa do SnapMirror em sistemas ASA r2 varia de acordo com a versão do ONTAP e o protocolo do host.

Começando com ONTAP...	A sincronização ativa do SnapMirror suporta...
9.17.1	<ul style="list-style-type: none"> • iSCSI • FC • NVMe/FC • NVMe/TCP

Começando com ONTAP...	A sincronização ativa do SnapMirror suporta...
9.16.0	<ul style="list-style-type: none"> • iSCSI • FC

Limitações do protocolo NVMe com sincronização ativa SnapMirror em sistemas ASA r2

Antes de configurar a sincronização ativa do SnapMirror em um sistema ASA r2 com hosts NVMe, você deve estar ciente de certas limitações do protocolo NVMe.

Todas as unidades de armazenamento NVMe no subsistema NVMe devem ser membros do mesmo grupo de consistência e devem fazer parte do mesmo relacionamento de sincronização ativa do SnapMirror .

Os protocolos NVMe/FC e NVMe/TCP são suportados com sincronização ativa do SnapMirror da seguinte forma:

- Somente em clusters de 2 nós
- Somente em hosts ESXi
- Somente com configurações simétricas ativas/ativas

Configurações ativas/ativas assimétricas não são suportadas com hosts NVMe.

A sincronização ativa do SnapMirror com NVMe não oferece suporte ao seguinte:

- Subsistemas mapeados para mais de um grupo de consistência

Um grupo de consistência pode ser mapeado com vários subsistemas, mas cada subsistema pode ser mapeado para apenas um grupo de consistência.

- Expansão de grupos de consistência em um relacionamento de sincronização ativa do SnapMirror
- Mapeando unidades de armazenamento NVMe que não estão em um relacionamento de sincronização ativa do SnapMirror para subsistemas replicados
- Removendo uma unidade de armazenamento de um grupo de consistência
- Mudança de geometria do grupo de consistência
- ["Transferência de dados descarregados da Microsoft \(ODX\)"](#)

O que vem a seguir?

Depois de concluir a preparação necessária para habilitar a sincronização ativa do SnapMirror , você deve ["confirme a configuração do seu cluster"](#) .

Confirme a configuração do cluster ASA r2 antes de configurar a sincronização ativa do SnapMirror

A sincronização ativa do SnapMirror depende de clusters pareados para proteger seus dados em caso de failover. Antes de configurar a sincronização ativa do SnapMirror , você deve confirmar se seus clusters ASA r2 estão em um relacionamento de pareamento compatível e atendem a outros requisitos de configuração.

Passos

1. Confirme se existe um relacionamento de peering de cluster entre os clusters.



O espaço IP padrão é exigido pela sincronização ativa do SnapMirror para relacionamentos entre pares de cluster. Um espaço IP personalizado não é suportado.

["Criar um relacionamento de pares de cluster"](#) .

2. Confirme se existe um relacionamento de mesmo nível entre as máquinas virtuais de armazenamento (VMs) em cada cluster.

["Criar um relacionamento entre pares de VMs de armazenamento entre clusters"](#) .

3. Confirme se pelo menos um LIF foi criado em cada nó do cluster.

["Criar um LIF"](#).

4. Confirme se as unidades de armazenamento necessárias foram criadas e mapeadas para grupos de hosts.

["Criar uma unidade de armazenamento"](#) e ["mapear a unidade de armazenamento para um grupo de hosts"](#) .

5. Examine novamente o host do aplicativo para descobrir novas unidades de armazenamento.

O que se segue?

Depois de confirmar a configuração do cluster, você estará pronto para ["instalar o ONTAP Mediator"](#) .

Instalar o ONTAP Mediator em sistemas ASA r2

Para instalar o ONTAP Mediator no seu sistema ASA r2, você deve seguir o mesmo procedimento usado para instalar o ONTAP Mediator em todos os outros sistemas ONTAP .

A instalação do ONTAP Mediator inclui a preparação para a instalação, a ativação do acesso aos repositórios, o download do pacote do ONTAP Mediator, a verificação da assinatura do código, a instalação do pacote no host e a execução de tarefas pós-instalação.

Para instalar o ONTAP Mediator, siga ["este fluxo de trabalho"](#)

O que vem a seguir

Após a instalação do ONTAP Mediator, você deve ["configurar o ONTAP Mediator usando certificados autoassinados"](#) .

Configurar o ONTAP Mediator ou o ONTAP Cloud Mediator em sistemas ASA r2

Você deve configurar o ONTAP Mediator ou o ONTAP Cloud Mediator antes de começar a usar a sincronização ativa do SnapMirror para monitoramento de cluster. O ONTAP Mediator e o ONTAP Cloud Mediator fornecem um armazenamento persistente e protegido para metadados de alta disponibilidade (HA) usados pelos clusters ONTAP em um relacionamento de sincronização ativa do SnapMirror . Além disso, ambos os mediadores fornecem uma funcionalidade de consulta de integridade de nó síncrona para auxiliar na determinação de quorum e servem como um proxy de ping para

detecção de atividade do controlador.

Antes de começar

Se você estiver usando o ONTAP Cloud Mediator, verifique se o seu sistema ASA r2 atende aos requisitos "[pré-requisitos](#)".

Passos

1. No Gerenciador do Sistema, selecione **Proteção > Visão geral**.
2. No painel direito, em **Mediadores**, selecione **Adicionar um mediador**.
3. Selecione o **Tipo de mediador**.
4. Para um mediador **na nuvem**, insira o ID da organização, o ID do cliente e o segredo do cliente. Para um mediador **local**, insira o endereço IP, a porta, o nome de usuário e a senha do mediador.
5. Selecione o peer de cluster na lista de peers de cluster qualificados ou selecione **Adicionar um peer de cluster** para adicionar um novo.
6. Adicione as informações do certificado
 - Se você estiver usando um certificado autoassinado, copie o conteúdo do `intermediate.crt` arquivo e cole-o no campo **Certificado** ou selecione **Importar** para navegar até o `intermediate.crt` arquivo e importar as informações do certificado.
 - Se você estiver usando um certificado de terceiros, insira as informações do certificado no campo **Certificado**.
7. Selecione **Adicionar**.

O que se segue?

Depois de inicializar o mediador, você pode "[configurar sincronização ativa do SnapMirror](#)" para criar uma cópia dos seus dados em um site secundário e permitir que seus aplicativos host façam failover de forma automática e transparente em caso de desastre.

Configurar a sincronização ativa do SnapMirror em sistemas ASA r2

Configure a sincronização ativa do SnapMirror para criar uma cópia dos seus dados em um site secundário e permitir que seus aplicativos host façam failover de forma automática e transparente em caso de desastre.

Em sistemas ASA r2, a sincronização ativa do SnapMirror suporta configurações simétricas ativa/ativa. Em uma configuração simétrica ativa/ativa, ambos os sites podem acessar o armazenamento local para E/S ativa.

Sobre esta tarefa

Se você estiver usando o protocolo iSCSI ou FC e usar ferramentas ONTAP para VMware Sphere, você pode opcionalmente "[use o ONTAP Tools para VMware para configurar a sincronização ativa do SnapMirror](#)".

Antes de começar

"[Criar um grupo de consistência](#)" no site primário com novas unidades de armazenamento. Se você quiser criar uma configuração ativa/ativa simétrica não uniforme, crie também um grupo de consistência no site secundário com novas unidades de armazenamento.

Saiba mais sobre "[não uniforme](#)" configurações simétricas ativas/ativas.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o mouse sobre o nome do grupo de consistência que você deseja proteger com a sincronização ativa do SnapMirror .
3. Selecione **⋮** e então selecione **Proteger**.
4. Em **proteção remota**, selecione **replicar para um cluster remoto**.
5. Selecione um peer de cluster existente ou escolha **Adicionar um novo**.
6. Selecione a VM de armazenamento.
7. Para a política de replicação, selecione **AutomatedFailOverDuplex**.
8. Se você estiver criando uma configuração ativa/ativa simétrica não uniforme, selecione **Configurações de destino**; em seguida, insira o nome do novo grupo de consistência de destino criado antes de iniciar este procedimento.
9. Selecione **Guardar**.

Resultado

A sincronização ativa do SnapMirror é configurada para proteger seus dados para que você possa continuar as operações com objetivo de ponto de recuperação próximo de zero (RPO) e objetivo de tempo de recuperação próximo de zero (RTO) em caso de desastre.

Gerenciar sincronização ativa do SnapMirror

Reconfigure o ONTAP Mediator ou o ONTAP Cloud Mediator para usar um certificado de terceiros em sistemas ASA r2

Se você configurar o ONTAP Mediator ou o ONTAP Cloud Mediator com um certificado autoassinado, poderá reconfigurar o mediador para usar um certificado de terceiros. Certificados de terceiros podem ser preferidos ou exigidos pela sua organização por motivos de segurança.

Etapa 1: remover a configuração do mediador

Para reconfigurar o mediador, você deve primeiro remover sua configuração atual do cluster.

Passos

1. No Gerenciador do Sistema, selecione **Proteção > Visão geral**.
2. No painel direito, em **Mediadores**, selecione **⋮** ao lado do peer de cluster com a configuração do mediador que você deseja remover; em seguida, selecione **Remover**.

Se você tiver vários mediadores instalados e quiser remover todas as configurações, selecione **⋮** ao lado de **Mediadores**; depois selecione **Remover**.


3. Selecione **Remover** para confirmar que deseja remover a configuração do mediador.

Etapa 2: remover o certificado autoassinado

Após a remoção da configuração do mediador, você deve remover o certificado autoassinado associado do cluster.

Passos

1. Selecione **Cluster > Settings**.

2. Em **Segurança**, selecione **Certificados**.
3. Selecione o certificado que você deseja remover.
4.  Selecione ; em seguida, selecione **Delete**.

Etapa 3: Reinstale o mediador com um certificado de terceiros

Depois de remover o certificado autoassinado associado, você pode reconfigurar o mediador com o certificado de terceiros.

Passos

1. Selecione **Proteção > Visão geral**.
2. No painel direito, em **Mediadores**, selecione **Adicionar um mediador**.
3. Selecione o **Tipo de mediador**.
4. Para um mediador **na nuvem**, insira o ID da organização, o ID do cliente e o segredo do cliente. Para um mediador **local**, insira o endereço IP, a porta, o nome de usuário do mediador e a senha do mediador.
5. Selecione um peer de cluster na lista de peers de cluster qualificados ou selecione **Adicionar um peer de cluster** para adicionar um novo.
6. Em **Certificado**, insira as informações do certificado de terceiros.
7. Selecione **Adicionar**.

Resultado

O ONTAP Mediator ou o ONTAP Cloud Mediator é reconfigurado para usar o certificado de terceiros. Agora você pode usar o mediador para gerenciar relacionamentos de sincronização ativos do SnapMirror .


Executar um failover planejado de clusters ASA r2 em um relacionamento de sincronização ativa do SnapMirror

O SnapMirror Active Sync oferece disponibilidade contínua para aplicativos críticos de negócios, criando uma cópia dos seus dados em um site secundário e permitindo que seus aplicativos host façam failover de forma automática e transparente em caso de desastre. Pode ser necessário executar um failover planejado do seu relacionamento com o SnapMirror Active Sync para testar o processo de failover ou realizar manutenção no site principal.

Antes de começar

- O relacionamento de sincronização ativa do SnapMirror deve estar sincronizado.
- Não é possível iniciar um failover planejado quando uma operação não disruptiva, como uma movimentação de unidade de armazenamento, estiver em andamento.
- O ONTAP Mediator ou ONTAP Cloud Mediator deve estar configurado, conectado e em quorum.

Passos

1. Selecione **Proteção > Replicação**.
2. Selecione o relacionamento de sincronização ativa do SnapMirror no qual você deseja fazer failover.
3. Selecione  ; então selecione **Failover**.

O que vem a seguir

Use o `snapmirror failover show` comando na interface de linha de comando (CLI) do ONTAP para monitorar o status do failover.

Reestabeleça o relacionamento de sincronização ativa do SnapMirror após um failover não planejado de seus clusters ASA r2


Nos sistemas ASA r2, SnapMirror active sync suporta configurações ativo-ativo simétricas. Em uma configuração ativo-ativo simétrica, ambos os sites podem acessar o armazenamento local para E/S ativa. Se o cluster de origem falhar ou for isolado, o mediador aciona um failover automático não planejado (AUFO) e processa todas as operações de E/S do cluster de destino até que o cluster de origem se recupere.

Se você experimentar um AUFO da sua relação de sincronização ativa SnapMirror, você deve restabelecer a relação e retomar as operações no cluster de origem assim que ele voltar a ficar online.

Antes de começar

- O relacionamento de sincronização ativa do SnapMirror deve estar sincronizado.
- Não é possível iniciar um failover planejado quando uma operação não disruptiva, como uma movimentação de unidade de armazenamento, estiver em andamento.
- O Mediador ONTAP deve estar configurado, conectado e em quorum.
- Para recuperar caminhos de E/S perdidos ou atualizar os estados dos caminhos de E/S em seus hosts, você precisa executar uma nova verificação de armazenamento/adaptador nos hosts após o cluster de armazenamento primário retomar a operação.

Passos

1. Selecione **Proteção > Replicação**.
2. Selecione o relacionamento de sincronização ativa do SnapMirror que você precisa restabelecer.
3. Aguarde até que o status do relacionamento exiba **InSync**.
4. Selecione  ; em seguida, selecione **Failover** para retomar as operações no cluster primário original.

Excluir um relacionamento de sincronização ativo do SnapMirror no seu sistema ASA r2


Se você não precisar mais de RPO e RTO próximos de zero para um aplicativo comercial, remova a proteção de sincronização ativa do SnapMirror excluindo o relacionamento de sincronização ativa do SnapMirror associado. Se você estiver executando o ONTAP 9.16.1 em um sistema ASA r2, talvez também seja necessário excluir o relacionamento de sincronização ativa do SnapMirror antes de poder fazer determinadas alterações de geometria em grupos de consistência em um relacionamento de sincronização ativa do SnapMirror .

Etapa 1: encerrar a replicação do host

Se o grupo de hosts do cluster de origem for replicado para o cluster de destino e os grupos de consistência de destino forem mapeados para o grupo de hosts replicado, você deverá encerrar a replicação de hosts no cluster de origem antes de poder excluir o relacionamento de sincronização ativa do SnapMirror .

Passos


1. No System Manager, selecione **Host**.

2. Ao lado de um host que contém o grupo de hosts que você deseja parar de replicar, selecione  e, em seguida, selecione **Editar**.
3. Desmarque **Replicar configuração do host** e selecione **Atualizar**.

Etapa 2: Excluir o relacionamento de sincronização ativa do SnapMirror

Para remover a proteção de sincronização ativa do SnapMirror de um grupo de consistência, você deve excluir o relacionamento de sincronização ativa do SnapMirror .

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Selecione **Destinos locais** ou **Fontes locais**.
3. Ao lado do relacionamento de sincronização ativa do SnapMirror que você deseja remover, selecione  ; então selecione **Excluir**.
4. Selecione **Liberar os instantâneos base do grupo de consistência de origem**.
5. Selecione **Eliminar**.

Resultado

O relacionamento de sincronização ativa do SnapMirror é removido e os instantâneos base do grupo de consistência de origem são liberados. As unidades de armazenamento no grupo de consistência não são mais protegidas pela sincronização ativa do SnapMirror .

O que se segue?

["Configurar a replicação de instantâneos"](#) para copiar o grupo de consistência para um local geograficamente remoto para backup e recuperação de desastres.

Remova o ONTAP Mediator ou o ONTAP Cloud Mediator do seu sistema ASA r2

Você pode usar apenas um tipo de mediador por vez para sincronização ativa do SnapMirror no seu sistema ASA r2. Se você optar por alterar seu tipo de mediador, deverá remover sua instância atual antes de instalar outra instância.

Passos

Você deve usar a interface de linha de comando (CLI) do ONTAP para remover o ONTAP Mediator ou o ONTAP Cloud Mediator.

Mediador ONTAP

1. Remover o Mediador ONTAP :

```
snapmirror mediator remove -mediator-address <address> -peer-cluster <peerClusterName>
```

Exemplo:

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer -cluster cluster_xyz
```

Mediador de Nuvem ONTAP

1. Remover o ONTAP Cloud Mediator:

```
snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
```

Exemplo:

```
snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
```

Informações relacionadas

- ["remover mediador snapmirror"](#)

Restaure os dados em sistemas de storage ASA R2

Os dados em um grupo de consistência ou unidade de armazenamento protegida por instantâneos podem ser restaurados se forem perdidos ou corrompidos.

Restaure um grupo de consistência

A restauração de um grupo de consistência substitui os dados em todas as unidades de storage do grupo de consistência pelos dados de um snapshot. As alterações feitas nas unidades de armazenamento após a criação do instantâneo não são restauradas.


É possível restaurar um grupo de consistência a partir de um instantâneo local ou remoto.

Restaurar a partir de um instantâneo local

Passos


1. No System Manager, selecione **proteção > grupos de consistência**.
2. Clique duas vezes no grupo de consistência que contém os dados que você precisa restaurar.

Abre-se a página de detalhes do grupo de consistência.

3. Selecione **Snapshots**.
4. Selecione o instantâneo que pretende restaurar e, em seguida,  selecione .
5. Selecione **Restore consistency group from this snapshot**; then Select **Restore**.

Restaurar a partir de um instantâneo remoto

Passos

1. No System Manager, selecione **proteção > replicação**.
2. Selecione **destinos locais**.
3. Selecione **fonte** que deseja restaurar e  selecione .
4. Selecione **Restaurar**.
5. Selecione o cluster, a VM de armazenamento e o grupo de consistência para o qual você deseja restaurar os dados.
6. Selecione o instantâneo a partir do qual pretende restaurar.
7. Quando solicitado, digite "Restore" (restaurar); em seguida, selecione **Restore** (Restaurar).

Resultado

Seu grupo de consistência é restaurado ao ponto no tempo do snapshot usado para restauração.


Restaurar uma unidade de armazenamento

A restauração de uma unidade de armazenamento substitui todos os dados da unidade de armazenamento pelos dados de um instantâneo. As alterações efetuadas na unidade de armazenamento após a criação do instantâneo não são restauradas.

Passos

1. No System Manager, selecione **Storage**.
2. Faça duplo clique na unidade de armazenamento que contém os dados que necessita de restaurar.

Abre-se a página de detalhes da unidade de armazenamento.

3. Selecione **Snapshots**.
4. Selecione o instantâneo que pretende restaurar.
5.  Selecione ; em seguida, selecione **Restore**.
6. Selecione **Use este instantâneo para restaurar a unidade de armazenamento**; em seguida, selecione **Restore**.

Resultado

Sua unidade de armazenamento é restaurada até o ponto no tempo do instantâneo usado para restauração.

Gerenciar grupos de consistência

Saiba mais sobre grupos de consistência ONTAP em sistemas de armazenamento ASA r2

Um grupo de consistência é uma coleção de unidades de armazenamento que são gerenciadas como uma única unidade. Use grupos de consistência para simplificar o gerenciamento de armazenamento.

Por exemplo, suponha que você tenha um banco de dados com 10 unidades de armazenamento em um grupo de consistência e precise fazer backup de todo o banco de dados. Em vez de fazer backup de cada unidade de armazenamento, você pode fazer backup de todo o banco de dados simplesmente adicionando proteção de dados de instantâneo ao grupo de consistência. Fazer backup das unidades de armazenamento como um grupo de consistência em vez de individualmente também fornece um backup consistente de todas as unidades, enquanto fazer backup das unidades individualmente pode criar inconsistências.

A partir do ONTAP 9.16.1, você pode usar o System Manager para criar grupos de consistência hierárquicos no seu sistema ASA r2. Em uma estrutura hierárquica, um ou mais grupos de consistência são configurados como filhos em um grupo de consistência pai.

Os grupos hierárquicos de consistência permitem que você aplique políticas de snapshot individuais a cada grupo filho de consistência e replique os snapshots de todos os grupos filhos de consistência a um cluster remoto como uma única unidade replicando o pai. Isso simplifica a proteção e o gerenciamento de dados para estruturas de dados complexas. Por exemplo, suponha que você crie um grupo de consistência pai chamado SVM1_app que contém dois grupos de consistência filhos: SVM1app_data para dados de aplicativos e SVM1app_logs para logs de aplicativos. Os instantâneos de SVM1app_data são tirados a cada 15 minutos e os instantâneos de SVM1app_logs são tirados a cada hora. O grupo de consistência pai SVM1_app, tem uma política do SnapMirror que replica os snapshots de ambos SVM1app_data e SVM1app_logs para um cluster remoto a cada 24 horas. O grupo de consistência pai SVM1_app é gerenciado como uma única unidade e os grupos de consistência filho são gerenciados como unidades separadas.

Grupos de consistência em relacionamentos de replicação

A partir do ONTAP 9.17.1, você pode fazer as seguintes alterações de geometria em grupos de consistência em um relacionamento de replicação assíncrona ou em um relacionamento de sincronização ativa do SnapMirror sem interromper ou excluir o relacionamento. Quando ocorre uma alteração de geometria no grupo de consistência primário, a alteração é replicada para o grupo de consistência secundário.

- ["Modificar o tamanho de uma unidade de armazenamento"](#) adicionando ou removendo unidades de armazenamento.
- ["Promova um único grupo de consistência"](#) para um grupo de consistência pai.
- ["Rebaixar um grupo de consistência pai"](#) para um único grupo de consistência.
- ["Desanexar um grupo de consistência filho"](#) de um grupo de consistência pai.
- ["Crie um grupo de consistência filho"](#) usando um grupo de consistência existente.

No ONTAP 9.16.1, você deve ["quebrar o relacionamento de replicação assíncrona"](#) e ["excluir o relacionamento de sincronização ativa do SnapMirror"](#) antes de fazer alterações de geometria no grupo de consistência.

Proteja grupos de consistência no seu sistema ASA r2 com instantâneos

Crie instantâneos dos grupos de consistência no seu sistema de armazenamento ASA r2 para proteger os dados nas unidades de armazenamento que fazem parte do grupo de

consistência. Se não precisar mais proteger os dados em nenhuma das unidades de armazenamento no grupo de consistência, você poderá remover a proteção de instantâneo do grupo de consistência.


Se não precisar mais proteger os dados de unidades de armazenamento específicas no grupo de consistência, você poderá remover essas unidades de armazenamento do grupo de consistência.

Adicionar proteção de dados de snapshot a um grupo de consistência





Quando você adiciona proteção de dados de snapshot a um grupo de consistência, os snapshots locais do grupo de consistência são feitos em intervalos regulares com base em uma programação predefinida.

Você pode usar snapshots que "restaurar dados" estão perdidos ou corrompidos.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja proteger.
3.  Selecione ; em seguida, selecione **Editar**.
4. Em **proteção local**, selecione **Agendar instantâneos**.
5. Selecione uma política de instantâneos.

Aceite a política de instantâneos padrão, selecione uma política existente ou crie uma nova política.

Opção	Passos
Selecione uma política de instantâneos existente	 Selecione ao lado da política padrão e, em seguida, selecione a política existente que você deseja usar.
Crie uma nova política de snapshot	<ol style="list-style-type: none">a.  Add Selecione ; em seguida, introduza o novo nome da política.b. Selecione o escopo da política.c. Em horários,  Add selecione .d. Selecione o nome que aparece em Nome da agenda; em seguida,  selecione .e. Selecione o agendamento da política.f. Em máximo de instantâneos, insira o número máximo de instantâneos que você deseja manter do grupo de consistência.g. Opcionalmente, sob SnapMirror label, digite um rótulo SnapMirror.h. Selecione Guardar.

6. Selecione **Guardar**.


O que vem a seguir

Agora que seus dados estão protegidos com snapshots, você deve "configurar a replicação de instantâneos" copiar seus grupos de consistência para um local geograficamente remoto para backup e recuperação de desastres.

Remova a proteção de dados do snapshot de um grupo de consistência

Quando você remove a proteção de dados de snapshot de um grupo de consistência, os snapshots são desabilitados para todas as unidades de armazenamento no grupo de consistência.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja parar de proteger.
3.  Selecione ; em seguida, selecione **Editar**.
4. Em **proteção local**, desmarque Agendar instantâneos.
5. Selecione **Editar**.

Resultado

Os instantâneos não serão tirados para nenhuma das unidades de armazenamento no grupo consistência.

Modifique o tamanho dos grupos de consistência no seu sistema ASA r2

Aumente ou diminua o tamanho de um grupo de consistência modificando o número de unidades de armazenamento no grupo de consistência.

Adicione unidades de armazenamento a um grupo de consistência

Expanda a quantidade de armazenamento gerenciado por um grupo de consistência adicionando unidades de armazenamento novas ou existentes ao grupo.

A partir do ONTAP 9.18.1, você pode configurar a reserva de snapshots e a exclusão automática de snapshots para limitar a quantidade de espaço usada pelos snapshots em suas unidades de armazenamento. Ao adicionar uma unidade de armazenamento a um grupo de consistência existente, a reserva de snapshots e a exclusão automática de snapshots são definidas da seguinte forma por padrão.

Se você adicionar...	A porcentagem de reserva instantânea está definida como...	A exclusão automática de instantâneos é...
Novas unidades de armazenamento	0	Desabilitado
Unidades de armazenamento existentes	Inalterado	Inalterado

Você pode modificar as configurações padrão para novas unidades de armazenamento ao criá-las. Você também pode "[modificar unidades de armazenamento existentes](#)" para atualizar suas configurações atuais.


["Saiba mais sobre a reserva de snapshots em sistemas de armazenamento ASA r2."](#)

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja expandir estiver em um relacionamento de sincronização ativo do SnapMirror, você deve "[excluir o relacionamento de sincronização ativa do SnapMirror](#)" antes de poder adicionar unidades de armazenamento. Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência estiver em um relacionamento de replicação assíncrona, você deve "[romper o relacionamento](#)" antes de poder expandir o grupo de consistência. Excluir o relacionamento de sincronização ativo do SnapMirror ou quebrar o relacionamento assíncrono antes de expandir um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.


Adicionar unidades de armazenamento existentes

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja expandir.
3.  Selecione ; em seguida, selecione **expandir**.
4. Selecione **usando unidades de armazenamento existentes**.
5. Selecione as unidades de armazenamento a serem adicionadas ao grupo de consistência; em seguida, selecione **expandir**.

Adicione novas unidades de armazenamento

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja expandir.
3.  Selecione ; em seguida, selecione **expandir**.
4. Selecione **usando novas unidades de armazenamento**.
5. Introduza o número de unidades que pretende criar e a capacidade por unidade.

Se você criar mais de uma unidade, cada unidade será criada com a mesma capacidade e o mesmo sistema operacional host. Para atribuir uma capacidade diferente a cada unidade, selecione **Adicionar uma capacidade diferente**.

6. Selecione **expandir**.

O que vem a seguir

Depois de criar uma nova unidade de armazenamento, "[adicione iniciadores de host](#)"deverá e "[mapeie a unidade de armazenamento recém-criada para um host](#)". A adição de iniciadores de host torna os hosts elegíveis para acessar as unidades de armazenamento e executar operações de dados. O mapeamento de uma unidade de armazenamento para um host permite que a unidade de armazenamento comece a fornecer dados para o host para o qual está mapeado.

O que se segue?

Os instantâneos existentes do grupo de consistência não incluem as unidades de armazenamento recém-adicionadas. Você deve "[crie um instantâneo imediato](#)"do seu grupo de consistência para proteger suas unidades de storage recém-adicionadas até que o próximo snapshot agendado seja criado automaticamente.

Remova uma unidade de armazenamento de um grupo de consistência

Remova uma unidade de armazenamento de um grupo de consistência para excluí-la, gerenciá-la como parte de um grupo de consistência diferente ou interromper a proteção de seus dados. Remover uma unidade de armazenamento de um grupo de consistência rompe a relação entre a unidade de armazenamento e o grupo de consistência, mas não exclui a unidade de armazenamento.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Clique duas vezes no grupo de consistência do qual você deseja remover uma unidade de armazenamento.

3. Na seção **Visão geral**, em **unidades de armazenamento**, selecione a unidade de armazenamento que deseja remover; em seguida, selecione **Remover do grupo de consistência**.

Resultado

A unidade de armazenamento já não é membro do grupo de consistência.

O que vem a seguir

Se precisar continuar a proteção de dados para a unidade de armazenamento, adicione a unidade de armazenamento a outro grupo de consistência.


Excluir grupos de consistência no seu sistema ASA r2

Se não precisar mais gerenciar os membros de um grupo de consistência como uma única unidade, você poderá excluir o grupo de consistência. Depois que um grupo de consistência é excluído, as unidades de armazenamento que estavam anteriormente no grupo permanecem ativas no cluster. Se o grupo de consistência estiver em um relacionamento de replicação, as cópias replicadas permanecerão no cluster remoto.

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja excluir estiver em um relacionamento de sincronização ativo do SnapMirror, você deverá ["excluir o relacionamento de sincronização ativa do SnapMirror"](#) antes de excluir o grupo de consistência. Excluir esse relacionamento antes de modificar um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja excluir.
3.  Selecione ; em seguida, selecione **Delete**.
4. Aceite o aviso e, em seguida, selecione **Delete**.

O que se segue?

Depois de excluir um grupo de consistência, as unidades de armazenamento anteriormente no grupo de consistência não serão mais protegidas por instantâneos. Considere adicionar essas unidades de armazenamento a outro grupo de consistência para protegê-las contra a perda de dados.

Gerenciar grupos de consistência hierárquica no seu sistema ASA r2

A partir do ONTAP 9.16.1, você pode usar o System Manager para criar grupos de consistência hierárquicos no seu sistema ASA r2. Em uma estrutura hierárquica, um ou mais grupos de consistência são configurados como filhos em um grupo de consistência pai. Você pode aplicar políticas de instantâneos individuais a cada grupo de consistência filho e replicar os instantâneos de todos os grupos de consistência filho para um cluster remoto como uma única unidade replicando o pai. Isso simplifica a proteção e o gerenciamento de dados para estruturas de dados complexas.

Promover um grupo de consistência existente para um grupo de consistência pai


Se você promover um grupo de consistência existente para um pai, um novo grupo de consistência filho será criado e as unidades de armazenamento pertencentes ao grupo de consistência promovido serão movidas

para o novo grupo de consistência filho. Unidades de armazenamento não podem ser associadas diretamente a um grupo de consistência pai.

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja promover estiver em um relacionamento de sincronização ativa do SnapMirror, você deve "[excluir o relacionamento de sincronização ativa do SnapMirror](#)" antes que o grupo de consistência possa ser promovido. Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência estiver em um relacionamento de replicação assíncrona, você deve "[romper o relacionamento](#)" antes de poder promover o grupo de consistência. Excluir o relacionamento de sincronização ativo do SnapMirror ou quebrar o relacionamento assíncrono antes de promover um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência que você deseja converter em um grupo de consistência pai.
3.  Selecione ; em seguida, selecione **promover para o grupo de consistência pai**.
4. Insira um nome para o novo grupo de consistência filho ou aceite o nome padrão; em seguida, selecione o tipo de componente do grupo de consistência.
5. Selecione **promover**.

O que se segue?

Você pode criar grupos de consistência filhos adicionais sob o grupo de consistência pai. Você também pode "[configurar a replicação de instantâneos](#)" para copiar os grupos de consistência pai e filho para um local geograficamente remoto para backup e recuperação de desastres.


Demote um grupo de consistência pai para um único grupo de consistência

Quando você rebaixa um grupo de consistência pai para um único grupo de consistência, as unidades de armazenamento dos grupos de consistência filho associados são adicionadas ao grupo de consistência pai. Os grupos de consistência filhos são excluídos e o pai é então gerenciado como um único grupo de consistência.

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja rebaixar estiver em um relacionamento de sincronização ativa do SnapMirror, você deve "[excluir o relacionamento de sincronização ativa do SnapMirror](#)" antes que o grupo de consistência possa ser rebaixado. Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência estiver em um relacionamento de replicação assíncrona, você deve "[romper o relacionamento](#)" antes de poder rebaixar o grupo de consistência. Excluir o relacionamento de sincronização ativo do SnapMirror ou quebrar o relacionamento assíncrono antes de expandir um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência pai que você deseja rebaixar.
3.  Selecione ; em seguida, selecione **demote para um único grupo de consistência**.
4. Selecione **demote**

O que se segue?

"[Adicionar uma política de instantâneos](#)" para o grupo de consistência rebaixado para proteger as unidades de

armazenamento que foram gerenciadas anteriormente pelos grupos de consistência infantil.


Crie um grupo de consistência filho

A criação de grupos de consistência filho permite que você aplique políticas de instantâneo individuais a cada filho. A partir do ONTAP 9.17.1, você também pode aplicar políticas de replicação individuais diretamente a cada filho. No ONTAP 9.16.1, as políticas de replicação podem ser aplicadas somente no nível pai.

Você pode criar um grupo de consistência filho a partir de um grupo de consistência novo ou existente.

De um novo grupo de consistência

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Passe o Mouse sobre o grupo de consistência pai ao qual você deseja adicionar um grupo de consistência filho.
3.  Selecione ; em seguida, selecione **Adicionar um novo grupo de consistência filho**.
4. Insira um nome para o grupo de consistência filho ou aceite o nome padrão; em seguida, selecione o tipo de componente do grupo de consistência.
5. Selecione para adicionar unidades de armazenamento existentes ao grupo de consistência filho ou para criar novas unidades de armazenamento.

Se criar novas unidades de armazenamento, introduza o número de unidades que pretende criar e a capacidade por unidade; em seguida, introduza as informações do anfitrião.

Se você criar mais de uma unidade de armazenamento, cada unidade será criada com a mesma capacidade e o mesmo sistema operacional host. Para atribuir uma capacidade diferente a cada unidade, selecione **Adicionar uma capacidade diferente**.


6. Selecione **Adicionar**.

De um grupo de consistência existente

Antes de começar

Se o grupo de consistência que você deseja usar já for filho de outro grupo de consistência, você deve "[desconectá-lo do grupo de consistência pai existente](#)" antes de poder movê-lo para um novo grupo de consistência pai.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Selecione o grupo de consistência existente que você gostaria de criar um grupo de consistência filho.
3.  Selecione ; em seguida, selecione **mover sob grupo de consistência diferente**.
4. Insira um novo nome para o grupo de consistência filho ou aceite o nome padrão; em seguida, selecione o tipo de componente do grupo de consistência.
5. Selecione o grupo de consistência existente que você gostaria de fazer o grupo de consistência pai ou selecione para criar um novo grupo de consistência pai.

Se você selecionar criar um novo grupo de consistência pai, digite um nome para o grupo de consistência pai ou aceite o nome padrão; em seguida, selecione o tipo de componente do aplicativo de consistência.

6. Selecione **mover**.

O que vem a seguir

Depois de criar um grupo de consistência filho, você pode "[aplicar políticas individuais de proteção de snapshot](#)" para cada grupo de consistência infantil. Você também pode "[configurar políticas de replicação](#)" nos grupos de consistência pai e filho para replicar os grupos de consistência em um local remoto.


Separe um grupo de consistência filho de um grupo de consistência pai

Quando você separa um grupo de consistência filho de um grupo de consistência pai, o grupo de consistência filho é removido do grupo de consistência pai e é gerenciado como um único grupo de consistência. A política de replicação aplicada ao pai não é mais aplicada ao grupo de consistência filho desanexado.

Antes de começar

Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência que deseja destacar estiver em um relacionamento de sincronização ativo do SnapMirror, você deve "[excluir o relacionamento de sincronização ativa do SnapMirror](#)" antes que o grupo de consistência possa ser destacado. Se você estiver executando o ONTAP 9.16.1 e o grupo de consistência estiver em um relacionamento de replicação assíncrona, você deve "[romper o relacionamento](#)" antes de poder desanexar o grupo de consistência. Excluir o relacionamento de sincronização ativo do SnapMirror ou quebrar o relacionamento assíncrono antes de expandir um grupo de consistência não é necessário no ONTAP 9.17.1 e versões posteriores.

Passos

1. No System Manager, selecione **proteção > grupos de consistência**.
2. Selecione o grupo de consistência pai.
3. Selecione sobre o grupo de consistência filho que deseja separar.
4.  Selecione ; em seguida, selecione **Desanexar do pai**.
5. Insira um novo nome para o grupo de consistência que você está desanexando ou aceite o nome padrão; em seguida, selecione o tipo de aplicativo do grupo de consistência.
6. Selecione **Desanexar**.

O que se segue?

"[Configure uma política de replicação](#)" para replicar os instantâneos do grupo de consistência filho desanexado em um cluster remoto.

Gerenciar políticas e programações de proteção de dados da ONTAP em sistemas de storage ASA R2

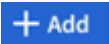
Use políticas de snapshot para proteger os dados nos grupos de consistência em uma programação automatizada. Use programações de políticas nas políticas de snapshot para determinar com que frequência os snapshots são feitos.

Crie um novo cronograma de política de proteção

Um cronograma de política de proteção define com que frequência uma política de snapshots é executada. Você pode criar programações para serem executadas em intervalos regulares com base em vários dias, horas ou minutos. Por exemplo, você pode criar uma programação para executar a cada hora ou para executar apenas uma vez por dia. Você também pode criar programações para serem executadas em horários específicos em dias específicos da semana ou mês. Por exemplo, você pode criar uma agenda para ser executada às 12:15am no dia 20th de cada mês.

A definição de várias programações de políticas de proteção oferece a flexibilidade de aumentar ou diminuir a frequência de snapshots para diferentes aplicações. Isso permite que você forneça um nível maior de proteção e um risco menor de perda de dados para seus workloads essenciais do que o que pode ser necessário para workloads menos essenciais.

Passos

1. Selecione **proteção > políticas**; em seguida, selecione **Programação**.
2.  Selecione .
3. Introduza um nome para a programação e, em seguida, selecione os parâmetros de programação.
4. Selecione **Guardar**.

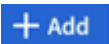
O que se segue?

Agora que você criou uma nova agenda de políticas, pode usar a programação recém-criada em suas políticas para definir quando os snapshots são feitos.

Criar uma política de snapshot

Uma política de snapshot define com que frequência os snapshots são feitos, o número máximo de snapshots permitidos e o tempo de retenção dos snapshots.

Passos

1. No System Manager, selecione **proteção > políticas**; em seguida, selecione **políticas Snapshot**.
2.  Selecione .
3. Introduza um nome para a política de instantâneos.
4. Selecione **Cluster** para aplicar a política a todo o cluster. Selecione **Storage VM** para aplicar a política a uma VM de armazenamento individual.
5. Selecione **Adicionar um agendamento**; em seguida, insira o agendamento da política de snapshot.
6. Selecione **Adicionar política**.


O que se segue?

Agora que você criou uma política de snapshot, pode aplicá-la a um grupo de consistência. Os instantâneos serão tirados do grupo de consistência com base nos parâmetros definidos na política de instantâneos.

Aplique uma política de snapshot a um grupo de consistência

Aplique uma política de snapshot a um grupo de consistência para criar, reter e rotular automaticamente snapshots do grupo de consistência.

Passos

1. No System Manager, selecione **proteção > políticas**; em seguida, selecione **políticas Snapshot**.
2. Passe o Mouse sobre o nome da política de snapshot que você deseja aplicar.
3.  Selecione ; em seguida, selecione **aplicar**.
4. Selecione os grupos de consistência aos quais você deseja aplicar a política de snapshot; em seguida, selecione **aplicar**.

O que se segue?

Agora que seus dados estão protegidos com snapshots, você deve "[configure uma relação de replicação](#)" copiar seus grupos de consistência para um local geograficamente remoto para backup e recuperação de desastres.

Edite, exclua ou desative uma política de snapshot

Edite uma política de instantâneos para modificar o nome da política, o número máximo de instantâneos ou o rótulo SnapMirror. Exclua uma política para removê-la e seus dados de backup associados do cluster.

Desative uma política para interromper temporariamente a criação ou transferência de instantâneos especificados pela política.

Passos

1. No System Manager, selecione **proteção > políticas**; em seguida, selecione **políticas Snapshot**.
2. Passe o Mouse sobre o nome da política de snapshot que você deseja editar.
3.  Selecione ; em seguida, selecione **Edit**, **Delete** ou **Disable**.


Resultado

Você modificou, excluiu ou desativou a política de snapshot.

Editar uma política de replicação

Edite uma política de replicação para modificar a descrição da política, o agendamento de transferência e as regras. Também pode editar a política para ativar ou desativar a compressão de rede.

Passos

1. No System Manager, selecione **proteção > políticas**.
2. Selecione **políticas de replicação**.
3. Passe o Mouse sobre a política de replicação que você deseja editar; em seguida,  selecione .
4. Selecione **Editar**.
5. Atualize a política; em seguida, selecione **Salvar**.

Resultado

Você modificou a política de replicação.

Proteja seus dados

Criptografia de dados em repouso em sistemas de storage ASA R2

Ao criptografar dados em repouso, não é possível ler se um meio de storage é reutilizado, devolvido, extraviado ou roubado. Você pode usar o Gerenciador de sistemas do ONTAP para criptografar seus dados em nível de hardware e software para proteção de camada dupla.

O NetApp Storage Encryption (NSE) é compatível com a criptografia de hardware usando unidades de autcriptografia (SEDs). Os SEDs criptografam dados conforme são gravados. Cada SED contém uma chave de criptografia exclusiva. Os dados criptografados armazenados no SED não podem ser lidos sem a chave de criptografia do SED. Os nós que tentam ler de um SED devem ser autenticados para acessar a chave de criptografia do SED. Os nós são autenticados pela obtenção de uma chave de autenticação de um gerenciador de chaves e, em seguida, apresentando a chave de autenticação à SED. Se a chave de autenticação for válida, o SED dará ao nó a sua chave de encriptação para aceder aos dados que contém.



Nos sistemas ASA r2, os SEDs são suportados apenas para SSDs baseados em NVMe.

Use o gerenciador de chaves integrado do ASA R2 ou um gerenciador de chaves externo para fornecer chaves de autenticação aos nós.

Além do NSE, você também pode habilitar a criptografia de software para adicionar outra camada de

segurança aos seus dados.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, em **criptografia**, selecione **Configurar**.
3. Configure o gerenciador de chaves.

Opção	Passos
Configure o Onboard Key Manager	<ol style="list-style-type: none">a. Selecione Onboard Key Manager para adicionar os servidores de chave.b. Introduza uma frase-passe.
Configurar um gerenciador de chaves externo	<ol style="list-style-type: none">a. Selecione Gerenciador de chaves externo para adicionar os servidores de chaves.b. + Add Selecione para adicionar os servidores de chaves.c. Adicione os certificados de CA do servidor KMIP.d. Adicione os certificados de cliente KMIP.

4. Selecione **criptação de camada dupla** para ativar a encriptação de software.
5. Selecione **Guardar**.

O que se segue?

Agora que você criptografou seus dados em repouso, se estiver usando o protocolo NVMe/TCP, poderá "[criptografe todos os dados enviados pela rede](#)" entre o host NVMe/TCP e o sistema ASA R2.

Migre chaves de criptografia de dados ONTAP entre gerenciadores de chaves no sistema ASA R2

Você pode gerenciar suas chaves de criptografia de dados usando o Gerenciador de chaves integrado do ONTAP no sistema ASA R2 ou um gerenciador de chaves externo (ou ambos). Os gerenciadores de chaves externos só podem ser ativados no nível de VM de armazenamento. No nível do cluster do ONTAP, você pode ativar o gerenciador de chaves integrado ou um gerenciador de chaves externo.

Se ativar o seu gestor de chaves na...	Você pode usar...
Somente no nível do cluster	O gerenciador de chaves integrado ou um gerenciador de chaves externo
Somente no nível de VM de armazenamento	Apenas um gerenciador de chaves externo

Se ativar o seu gestor de chaves na...	Você pode usar...
Tanto no nível do cluster quanto no nível da VM de armazenamento	<p>Uma das seguintes combinações de gerenciador de chaves:</p> <ul style="list-style-type: none"> • Opção 1 <p>Nível de cluster: Gerenciador de chaves integrado</p> <p>Nível de VM de armazenamento: Gerenciador de chaves externo</p> • Opção 2 <p>Nível de cluster: Gerenciador de chaves externo</p> <p>Nível de VM de armazenamento: Gerenciador de chaves externo</p>

Migre chaves entre os gerenciadores-chave no nível do cluster do ONTAP

A partir do ONTAP 9.16.1, você pode usar a interface de linha de comando (CLI) do ONTAP para migrar chaves entre gerenciadores de chaves no nível do cluster.

De bordo para externo

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Criar uma configuração de gerenciador de chaves externo inativo:

```
security key-manager external create-config
```

3. Mude para o gerenciador de chaves externo:

```
security key-manager keystore enable -vserver <storage_vm_name>  
-type KMIP
```

4. Exclua a configuração do gerenciador de chaves integrado:

```
security key-manager keystore delete-config -vserver  
<storage_vm_name> -type OKM
```

5. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Do externo ao integrado

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Criar uma configuração inativa do gerenciador de chaves integrado:

```
security key-manager onboard create-config
```

3. Ative a configuração do gerenciador de chaves integrado:

```
security key-manager keystore enable -vserver <storage_vm_name>
-type OKM
```

4. Exclua a configuração do gerenciador de chaves externo

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type KMIP
```

5. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Migre chaves entre gerenciadores de chaves em cluster ONTAP e níveis de VM de armazenamento

Você pode usar a interface de linha de comando (CLI) do ONTAP para migrar chaves entre o gerenciador de chaves no nível do cluster e um gerenciador de chaves no nível da VM de storage.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Migrar as chaves:

```
security key-manager key migrate -from-vserver <storage_vm_name> -to
-vserver <storage_vm_name>
```

3. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Proteção contra ataques de ransomware

Crie instantâneos à prova de violação para proteger contra ataques de ransomware em sistemas de armazenamento ASA r2


Para maior proteção contra ataques de ransomware, replique snapshots para um cluster remoto e bloqueie os snapshots de destino para torná-los à prova de violação. Os instantâneos bloqueados não podem ser eliminados acidentalmente ou maliciosamente. Use snapshots bloqueados para recuperar dados caso uma unidade de storage seja

comprometida por um ataque de ransomware.

Inicialize o relógio SnapLock Compliance

Antes de criar snapshots à prova de adulteração, é necessário inicializar o relógio SnapLock Compliance nos clusters local e de destino.

Passos

1. Selecione **Cluster > Overview**.
2. Na seção **nós**, selecione **Inicializar Relógio SnapLock Compliance**.
3. Selecione **Inicializar**.
4. Verifique se o relógio de conformidade foi inicializado.
 - a. Selecione **Cluster > Overview**.
 - b. Na seção **nós**,  selecione ; em seguida, selecione **Relógio SnapLock Compliance**.

O que vem a seguir?

Depois de inicializar o relógio SnapLock Compliance nos clusters local e de destino, você estará pronto para ["crie uma relação de replicação com instantâneos bloqueados"](#).

Habilite a proteção autônoma contra ransomware com IA em seus sistemas de armazenamento ASA r2

A partir do ONTAP 9.17.1, você pode usar a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) para proteger os dados no seu sistema ASA r2. A ARP/AI detecta rapidamente potenciais ameaças de ransomware, cria automaticamente um snapshot da ARP para proteger seus dados e exibe uma mensagem de aviso no Gerenciador do Sistema para alertá-lo sobre atividades suspeitas.

O ARP aprimora a resiliência cibernética ao adotar um modelo de aprendizado de máquina para análise antiransomware que detecta formas de ransomware em constante evolução com 98% de precisão em ambientes SAN. O modelo de aprendizado de máquina do ARP é pré-treinado em um grande conjunto de dados de arquivos, tanto antes quanto depois de um ataque de ransomware simulado. Esse treinamento que exige muitos recursos é realizado fora do ONTAP, e o modelo pré-treinado resultante desse treinamento é incluído on-box com o ONTAP. Esse modelo não é acessível nem modificável. O ARP/AI é ativado imediatamente após a capacitação; não há ["período de aprendizagem"](#).



Nenhum sistema de detecção ou prevenção de ransomware pode garantir completamente a segurança contra um ataque de ransomware. Embora um ataque possa passar despercebido, ARP/AI atua como uma importante camada adicional de defesa caso o software antivírus falhe em detectar uma intrusão.

Sobre esta tarefa

- O suporte ARP/AI está incluído no ["Licença ONTAP One"](#) .
- ARP/AI não é compatível com unidades de armazenamento protegidas por SnapMirror active sync, SnapMirror synchronous ou SnapLock.
- A partir do ONTAP 9.18.1, o ARP/AI é ativado por padrão em todas as unidades de armazenamento recém-criadas 12 horas após a atualização para o ONTAP 9.18.1 ou a inicialização de um novo cluster ASA r2 com ONTAP 9.18.1.
- Depois de habilitar o ARP/AI, você deve ["habilite atualizações automáticas para seus arquivos de](#)


[segurança](#)" para receber automaticamente novas atualizações de segurança.

Ative o ARP/AI em todas as unidades de armazenamento no cluster

Se você estiver executando ONTAP 9.17.1, você pode habilitar ARP/AI em todas as unidades de armazenamento criadas no cluster por padrão.

No ONTAP 9.18.1 e versões posteriores, ARP/AI está habilitado por padrão em todas as novas unidades de armazenamento. Se você tiver unidades de armazenamento criadas no ONTAP 9.17.1 para as quais ARP/AI não está habilitado, você pode habilitá-lo manualmente.

Passos


1. No System Manager, selecione **Cluster > Settings**.
2. Ao lado de **Anti-ransomware**, selecione  e, em seguida, selecione **Ativar em todas as unidades de armazenamento existentes**.
3. Selecione **Ativar**.

Habilite ARP/AI em todas as unidades de armazenamento em uma VM de armazenamento.

Se você estiver executando ONTAP 9.17.1, poderá habilitar ARP/AI em todas as unidades de armazenamento criadas em uma máquina virtual de armazenamento (VM) por padrão. Isso significa que qualquer nova unidade de armazenamento criada na máquina virtual de armazenamento terá ARP/AI habilitado automaticamente. Você também pode aplicar ARP/AI a unidades de armazenamento existentes na máquina virtual de armazenamento.

No ONTAP 9.18.1 e versões posteriores, ARP/AI está habilitado por padrão em todas as novas unidades de armazenamento. Se você tiver unidades de armazenamento criadas no ONTAP 9.17.1 para as quais ARP/AI não está habilitado, você pode habilitá-lo manualmente.

Passos

1. No Gerenciador do Sistema, selecione **Cluster > VMs de Armazenamento**.
2. Selecione a VM de armazenamento na qual você deseja habilitar o ARP/AI.
3. Na seção **Segurança**, ao lado de **Anti-ransomware**, selecione ; então selecione **Editar configurações anti-ransomware**.
4. Selecione **Ativar anti-ransomware**.

Isso habilita ARP/AI em todas as futuras unidades de armazenamento criadas na VM de armazenamento selecionada por padrão.

5. Para aplicar o ARP às unidades de armazenamento existentes na VM de armazenamento selecionada, selecione **Aplicar esta alteração a todas as unidades de armazenamento existentes aplicáveis nesta VM de armazenamento**.
6. Selecione **Guardar**.

Resultado


Todas as novas unidades de armazenamento que você criar na máquina virtual de armazenamento são protegidas contra ataques de ransomware por padrão, e qualquer atividade suspeita será relatada a você no Gerenciador de Sistemas.

Habilite ARP/AI em unidades de armazenamento específicas em uma VM de armazenamento.

Se você estiver executando ONTAP 9.17.1 e não quiser que ARP/AI esteja habilitado em todas as unidades de armazenamento em uma storage VM, você pode selecionar as unidades específicas que deseja habilitar.

No ONTAP 9.18.1 e versões posteriores, ARP/AI está habilitado por padrão em todas as novas unidades de armazenamento. Se você tiver unidades de armazenamento criadas no ONTAP 9.17.1 para as quais ARP/AI não está habilitado, você pode habilitá-lo manualmente.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione as unidades de armazenamento para as quais você deseja habilitar ARP/AI.
3. Selecione  ; então selecione **Ativar anti-ransomware**.
4. Selecione **Ativar**.

Resultado

As unidades de armazenamento selecionadas são protegidas contra ataques de ransomware, e atividades suspeitas são reportadas a você no Gerenciador do Sistema.

Desative a proteção autônoma contra ransomware padrão em seus sistemas de armazenamento ASA r2


Ao inicializar um novo cluster ONTAP 9.18.1 ASA r2 ou ao atualizar seu cluster para ONTAP 9.18.1, o ARP/AI é ativado automaticamente por padrão em todas as novas unidades de armazenamento após um período de carência de 12 horas. Se você não desativar o ARP/AI durante o período de carência, ele será ativado em todo o cluster para as novas unidades de armazenamento quando o período de carência terminar.

As unidades de armazenamento criadas no ONTAP 9.17.1 devem ser "[ativado manualmente](#)" para ARP/AI.

Passos

Você pode desativar a capacitação padrão durante ou após o período de carência inicial de 12 horas.

System Manager

1. Selecione **Cluster > Settings**.
2. Desativar ARP:
 - Para desativar durante o período de carência de 12 horas:
 - i. Em **Anti-ransomware**, selecione **Don't enable** e depois selecione **Disable**.
 - Para desativar após o período de carência de 12 horas:
 - i. Em **Anti-ransomware**, selecione  e desmarque **Ativar para novas unidades de armazenamento**.
 - ii. Selecione **Save**

CLI

1. Verifique o status de capacitação padrão:

```
security anti-ransomware auto-enable show
```

2. Desative a capacitação padrão para volumes existentes e novos:

```
security anti-ransomware auto-enable modify -default-existing-volume  
-state false -default-new-volume-state false
```

Modificar períodos de retenção de snapshots ARP/AI em sistemas de armazenamento ASA r2

Se a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) detectar atividade anormal em uma ou mais unidades de armazenamento do seu sistema ASA r2, ela criará automaticamente um snapshot ARP para proteger os dados da unidade de armazenamento. Dependendo da sua capacidade de armazenamento e dos requisitos de negócios para seus dados, você pode aumentar ou diminuir o período de retenção padrão do snapshot ARP. Por exemplo, você pode aumentar o período de retenção para aplicativos críticos para os negócios, de modo que, se necessário, tenha períodos de retenção mais longos para recuperação de dados, ou pode diminuir o período de retenção para aplicativos não críticos, economizando espaço de armazenamento.

O período de retenção padrão para o snapshot do ARP varia dependendo da ação que você toma em resposta à atividade anormal.

Se você tomar essa atitude...	Os instantâneos ARP são retidos por padrão para...
Marcar como falso positivo	12 horas
Marcar como potencial ataque de ransomware	7 dias

Se você tomar essa atitude...	Os instantâneos ARP são retidos por padrão para...
Não tome medidas imediatas	10 dias

Os períodos de retenção padrão podem ser modificados usando a interface de linha de comando (CLI) do ONTAP . Veja "[Modificar opções para snapshots automáticos do ONTAP](#)" para saber as etapas para alterar o período de retenção padrão.

Responda à proteção autônoma contra ransomware com alertas de IA em sistemas de armazenamento ASA r2

Se a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) detectar atividade anormal em uma ou mais unidades de armazenamento do seu sistema ASA r2, um aviso será gerado no painel do Gerenciador de Sistemas. Você deve visualizar o aviso, verificar a atividade e, se necessário, tomar medidas para impedir qualquer ameaça potencial aos seus dados.

Se uma mensagem de aviso ARP/AI for exibida, antes de tomar qualquer medida, você deve usar o verificador de integridade do aplicativo apropriado para verificar a integridade dos dados na unidade de armazenamento. Verificar a integridade dos dados da unidade de armazenamento ajuda a determinar se a atividade é aceitável ou se se trata de um possível ataque de ransomware.

Se a atividade anormal for ...	Então faça isto...
Aceitável	Marque a atividade como um falso positivo.
Um potencial ataque de ransomware	Marque a atividade como um possível ataque de ransomware.
Indeterminado	Não tome medidas imediatas. Monitore a unidade de armazenamento por até 7 dias. Se a unidade de armazenamento continuar operando normalmente, marque a atividade como um falso positivo. Se a unidade de armazenamento continuar apresentando atividade anormal, marque a atividade como um possível ataque de ransomware.

Passos

1. No System Manager, selecione **Dashboard**.

Se o ARP detectar atividade anormal em uma ou mais unidades de armazenamento, uma mensagem será exibida em **Avisos**.

2. Selecione a mensagem de aviso.
3. Em **Visão geral de eventos**, selecione a mensagem **Avisos** que indica o número de unidades de armazenamento com atividade anormal.
4. Em **Unidades de armazenamento com atividade anormal**, selecione a unidade de armazenamento.
5. Selecione **Segurança**.

Se houver atividade anormal na unidade de armazenamento, uma mensagem será exibida em **Anti-ransomware**.

6. Selecione **Escolher uma ação**.

7. Selecione **Marcar como falso positivo** ou selecione **Marcar como possível ataque de ransomware**.

O que se segue?

Se você observar picos na atividade de suas unidades de armazenamento, sejam eles pontuais ou característicos de um novo padrão, você deve reportá-los como seguros. Reportar esses picos manualmente como seguros ajuda a melhorar a precisão das avaliações de ameaças do ARP. Saiba como "[relatar picos conhecidos de ARP/AI](#)".

Pause ou retome a Proteção Autônoma contra Ransomware com IA em seus sistemas de armazenamento ASA r2

A partir do ONTAP 9.17.1, você pode usar a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) para proteger os dados no seu sistema ASA r2. Se estiver planejando um evento de carga de trabalho incomum, você pode suspender temporariamente a análise de ARP/AI para evitar detecções de falsos positivos de ataques de ransomware. Após a conclusão do evento de carga de trabalho, você pode retomar a análise de ARP/AI.

Pausar ARP/AI

Antes de iniciar um evento de carga de trabalho incomum, pode ser necessário suspender temporariamente a análise de ARP/AI para evitar detecções de falsos positivos de ataques de ransomware.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione as unidades de armazenamento para as quais você deseja pausar o ARP/AI.
3. Selecione **Pausar anti-ransomware**.

Resultado

A análise de ARP/AI é pausada para as unidades de armazenamento selecionadas, e nenhuma atividade suspeita é relatada a você no Gerenciador do Sistema até que você retome o ARP/AI.

Retomar ARP/AI

Se você pausar o ARP/AI durante uma carga de trabalho incomum, após a conclusão da carga de trabalho, você deverá retomá-la para proteger seus dados contra ataques de ransomware.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione as unidades de armazenamento para as quais você deseja retomar o ARP/AI.
3. Selecione **Retomar anti-ransomware**.

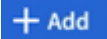

Resultado

A análise de potenciais ataques de ransomware é retomada e atividades suspeitas são reportadas a você no Gerenciador do Sistema.

Conexões NVMe seguras em seus sistemas de storage ASA R2

Se você estiver usando o protocolo NVMe, poderá configurar a autenticação na banda para aprimorar a segurança dos dados. A autenticação na banda permite autenticação bidirecional e unidirecional segura entre os hosts NVMe e o sistema ASA R2. A autenticação na banda está disponível para todos os hosts NVMe. Se você estiver usando o protocolo NVMe/TCP, poderá aprimorar ainda mais a segurança dos dados configurando a segurança da camada de transporte (TLS) para criptografar todos os dados enviados pela rede entre os hosts NVMe/TCP e o sistema ASA R2.

Passos

1. Selecione **hosts**; em seguida, selecione **NVMe**.
2.  Selecione .
3. Insira o nome do host e selecione o sistema operacional do host.
4. Insira uma descrição do host; em seguida, selecione a VM de armazenamento a ser conectada ao host.
5.  Selecione ao lado do nome do host.
6. Selecione **Autenticação na banda**.
7. Se você estiver usando o protocolo NVMe/TCP, selecione **exigir segurança da camada de transporte (TLS)**.
8. Selecione **Adicionar**.

Resultado

A segurança dos seus dados é melhorada com autenticação na banda e/ou TLS.

Conexões IP seguras em seus sistemas de storage ASA R2

Se você estiver usando o protocolo IP no sistema ASA R2, poderá configurar a segurança IP (IPsec) para melhorar a segurança dos dados. O IPsec é um padrão da Internet que fornece criptografia de dados em trânsito, autenticação para o tráfego que flui entre os pontos de extremidade da rede em um nível IP e proteção contra repetição e ataques mal-intencionados contra seus dados.

Para sistemas ASA R2, o IPsec está disponível para hosts iSCSI e NVMe/TCP.

Em determinados sistemas ASA R2, várias operações criptográficas, como verificações de criptografia e integridade, podem ser descarregadas para uma placa de controlador de interface de rede (NIC) suportada. A taxa de transferência para operações descarregadas para a placa NIC é de aproximadamente 5% ou menos. Isso pode melhorar significativamente o desempenho e a taxa de transferência do tráfego de rede protegido pelo IPsec.

A partir do ONTAP 9.18.1, o suporte para descarregamento de hardware IPsec foi estendido ao tráfego IPv6.

As seguintes placas de rede são compatíveis com o descarregamento de hardware nos seguintes sistemas ASA r2 e versões do ONTAP :

Placa NIC suportada	Sistemas ASA r2	Versão ONTAP
X50135A (Controlador Ethernet 2p, 40G/100G)	<ul style="list-style-type: none"> • ASA A1K • ASA A90 • ASA A70 	ONTAP 9.17.1 e posterior
X60135A (Controlador Ethernet 2p, 40G/100G)	<ul style="list-style-type: none"> • ASA A50 • ASA A30 • ASA A20 	ONTAP 9.17.1 e posterior
X50131A - (controlador Ethernet 2P, 40G/100g/200g/400G)	<ul style="list-style-type: none"> • ASA A1K • ASA A90 • ASA A70 	ONTAP 9.16.1 e posterior
X60132A - (controlador Ethernet 4P, 10G/25G)	<ul style="list-style-type: none"> • ASA A50 • ASA A30 • ASA A20 	ONTAP 9.16.1 e posterior

Veja o "[NetApp Hardware Universe](#)" Para obter mais informações sobre os sistemas e placas suportados.

O que se segue?

O IPsec é configurado no seu sistema ASA r2 da mesma forma que em outros sistemas ONTAP . Para mais informações, consulte "[Prepare-se para configurar a segurança IP para a rede 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 SOBRESSALIENTES; 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.