



# O que fazer após uma atualização do ONTAP

ONTAP 9

NetApp  
January 17, 2025

This PDF was generated from [https://docs.netapp.com/pt-br/ontap/upgrade/task\\_what\\_to\\_do\\_after\\_upgrade.html](https://docs.netapp.com/pt-br/ontap/upgrade/task_what_to_do_after_upgrade.html) on January 17, 2025. Always check docs.netapp.com for the latest.

# Índice

- O que fazer após uma atualização do ONTAP ..... 1
- O que fazer após uma atualização do ONTAP ..... 1
- Verifique o cluster após a atualização do ONTAP ..... 1
- Verifique se todos os LIFS estão em portas domésticas após a atualização do ONTAP ..... 4
- Configurações especiais ..... 5
- Atualize o Pacote de Qualificação de disco após uma atualização do ONTAP ..... 16

# O que fazer após uma atualização do ONTAP

## O que fazer após uma atualização do ONTAP

Depois de atualizar o ONTAP, há várias tarefas que você deve executar para verificar a prontidão do cluster.

1. ["Verifique o cluster"](#).

Depois de atualizar o ONTAP, verifique a versão do cluster, a integridade do cluster e a integridade do storage. Se você estiver usando uma configuração MetroCluster FC, também precisará verificar se o cluster está habilitado para switchover automático não planejado.

2. ["Verifique se todos os LIFs estão em portas residenciais"](#).

Durante uma reinicialização, alguns LIFs podem ter sido migrados para suas portas de failover atribuídas. Depois de atualizar um cluster, você deve habilitar e reverter quaisquer LIFs que não estejam em suas portas iniciais.

3. Verifique ["considerações especiais"](#) específico para o cluster.

Se existirem determinadas configurações no cluster, poderá ser necessário executar passos adicionais após a atualização.

4. ["Atualizar o Pacote de Qualificação de disco \(DQP\)"](#).

O DQP não é atualizado como parte de uma atualização do ONTAP.

## Verifique o cluster após a atualização do ONTAP

Depois de atualizar o ONTAP, verifique a versão do cluster, a integridade do cluster e a integridade do storage. Para configurações do MetroCluster FC, verifique também se o cluster está habilitado para switchover automático não planejado.

### Verifique a versão do cluster

Depois que todos os pares de HA tiverem sido atualizados, use o comando `version` para verificar se todos os nós estão executando a liberação de destino.

A versão do cluster é a versão mais baixa do ONTAP em execução em qualquer nó no cluster. Se a versão do cluster não for a versão de destino do ONTAP, você poderá atualizar o cluster.

1. Verifique se a versão do cluster é a versão de destino do ONTAP:

```
version
```

2. Se a versão do cluster não for a versão de destino do ONTAP, você deve verificar o status de atualização de todos os nós:

```
system node upgrade-revert show
```

## Verifique a integridade do cluster

Depois de atualizar um cluster, você deve verificar se os nós estão íntegros e qualificados para participar do cluster e se o cluster está em quórum.

1. Verifique se os nós do cluster estão online e estão qualificados para participar do cluster:

```
cluster show
```

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0                true   true
node1                true   true
```

Se algum nó não for saudável ou não for elegível, verifique se há erros nos logs do EMS e tome medidas corretivas.

2. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

3. Verifique os detalhes de configuração para cada processo RDB.

- A época do banco de dados relacional e as epochs do banco de dados devem corresponder para cada nó.
- O mestre de quórum por anel deve ser o mesmo para todos os nós.

Observe que cada anel pode ter um mestre de quórum diferente.

Para exibir este processo RDB...	Digite este comando...
Aplicação de gerenciamento	<code>cluster ring show -unitname mgmt</code>
Base de dados de localização de volume	<code>cluster ring show -unitname vlodb</code>
Gerenciador de interface virtual	<code>cluster ring show -unitname vifmgr</code>
Daemon de gerenciamento SAN	<code>cluster ring show -unitname bcomd</code>

Este exemplo mostra o processo do banco de dados de localização de volume:

```
cluster1::*> cluster ring show -unitname vldb
Node          UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----
node0         vldb      154          154      14847  node0      master
node1         vldb      154          154      14847  node0      secondary
node2         vldb      154          154      14847  node0      secondary
node3         vldb      154          154      14847  node0      secondary
4 entries were displayed.
```

4. Se você estiver operando em um ambiente SAN, verifique se cada nó está em um quórum de SAN:

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master          Cluster          Quorum          Availability
Operational
Node           Node           Status          Status          Status
-----
cluster1-01    cluster1-01    in-quorum      true
operational
cluster1-02    cluster1-02    in-quorum      true
operational
2 entries were displayed.
```

### Informações relacionadas

["Administração do sistema"](#)

### Verificar se o switchover não planejado automático está ativado (somente configurações MetroCluster FC)

Se o seu cluster estiver em uma configuração MetroCluster FC, você deve verificar se o switchover automático não planejado está ativado depois de atualizar o ONTAP.

Se estiver a utilizar uma configuração IP do MetroCluster, ignore este procedimento.

### Passos

1. Verifique se o switchover não planejado automático está ativado:

```
metrocluster show
```

Se o switchover não planejado automático estiver ativado, a seguinte instrução aparece na saída do comando:

```
AUSO Failure Domain auso-on-cluster-disaster
```

2. Se a instrução não aparecer, ative um switchover não planejado automático:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster
```

3. Verifique se um switchover não planejado automático foi ativado:

```
metrocluster show
```

#### Informações relacionadas

["Gerenciamento de disco e agregado"](#)

## Verifique se todos os LIFS estão em portas domésticas após a atualização do ONTAP

Durante a reinicialização que ocorre como parte do processo de atualização do ONTAP, alguns LIFs podem ser migrados de suas portas domésticas para suas portas de failover atribuídas. Após uma atualização, você precisa ativar e reverter quaisquer LIFs que não estejam em suas portas domésticas.

#### Passos

1. Apresentar o estado de todas as LIFs:

```
network interface show -fields home-port,curr-port
```

Se **Status Admin** estiver "inativo" ou **for home** for "false" para quaisquer LIFs, continue com a próxima etapa.

2. Ativar os LIFs de dados:

```
network interface modify {-role data} -status-admin up
```

3. Reverter LIFs para suas portas domésticas:

```
network interface revert *
```

4. Verifique se todos os LIFs estão em suas portas residenciais:

```
network interface show
```

Este exemplo mostra que todos os LIFs para SVM vs0 estão em suas portas domésticas.

```
cluster1::> network interface show -vserver vs0
      Logical      Status      Network      Current      Current      Is
Vserver Interface  Admin/Oper  Address/Mask  Node         Port         Home
-----
vs0
      data001      up/up      192.0.2.120/24  node0        e0e          true
      data002      up/up      192.0.2.121/24  node0        e0f          true
      data003      up/up      192.0.2.122/24  node0        e2a          true
      data004      up/up      192.0.2.123/24  node0        e2b          true
      data005      up/up      192.0.2.124/24  node1        e0e          true
      data006      up/up      192.0.2.125/24  node1        e0f          true
      data007      up/up      192.0.2.126/24  node1        e2a          true
      data008      up/up      192.0.2.127/24  node1        e2b          true
8 entries were displayed.
```

## Configurações especiais

### Verifique se há configurações específicas do ONTAP após uma atualização

Se o cluster estiver configurado com qualquer um dos seguintes recursos, talvez seja necessário executar etapas adicionais depois de atualizar o software ONTAP.

Pergunte a si mesmo...	Se a sua resposta for sim, então faça isso...
Eu atualizei do ONTAP 9.7 ou anterior para o ONTAP 9.8 ou posterior?	<a href="#">Verifique a configuração da rede</a> <a href="#">Remova o serviço EMS LIF das políticas de serviço de rede que não fornecem alcance para o destino EMS</a>
Meu cluster está em uma configuração do MetroCluster?	<a href="#">Verifique o status da rede e do armazenamento</a>
Tenho uma configuração SAN?	<a href="#">Verifique a configuração da SAN</a>
Eu atualizei do ONTAP 9.3 ou anterior e estou usando o NetApp Storage Encryption?	<a href="#">Reconfigure as conexões do servidor KMIP</a>
Tenho espelhos de partilha de carga?	<a href="#">Relocate os volumes de origem do espelho de compartilhamento de carga movidos</a>
Tenho contas de usuário para acesso ao processador de Serviço (SP) criadas antes do ONTAP 9.9,1?	<a href="#">Verifique a alteração nas contas que podem acessar o processador de serviço</a>

## Verifique a configuração da rede após uma atualização do ONTAP a partir do ONTAP 9.7x ou anterior

Depois de atualizar do ONTAP 9.7x ou anterior para o ONTAP 9.8 ou posterior, verifique a configuração da rede. Após a atualização, o ONTAP monitora automaticamente a acessibilidade da camada 2.

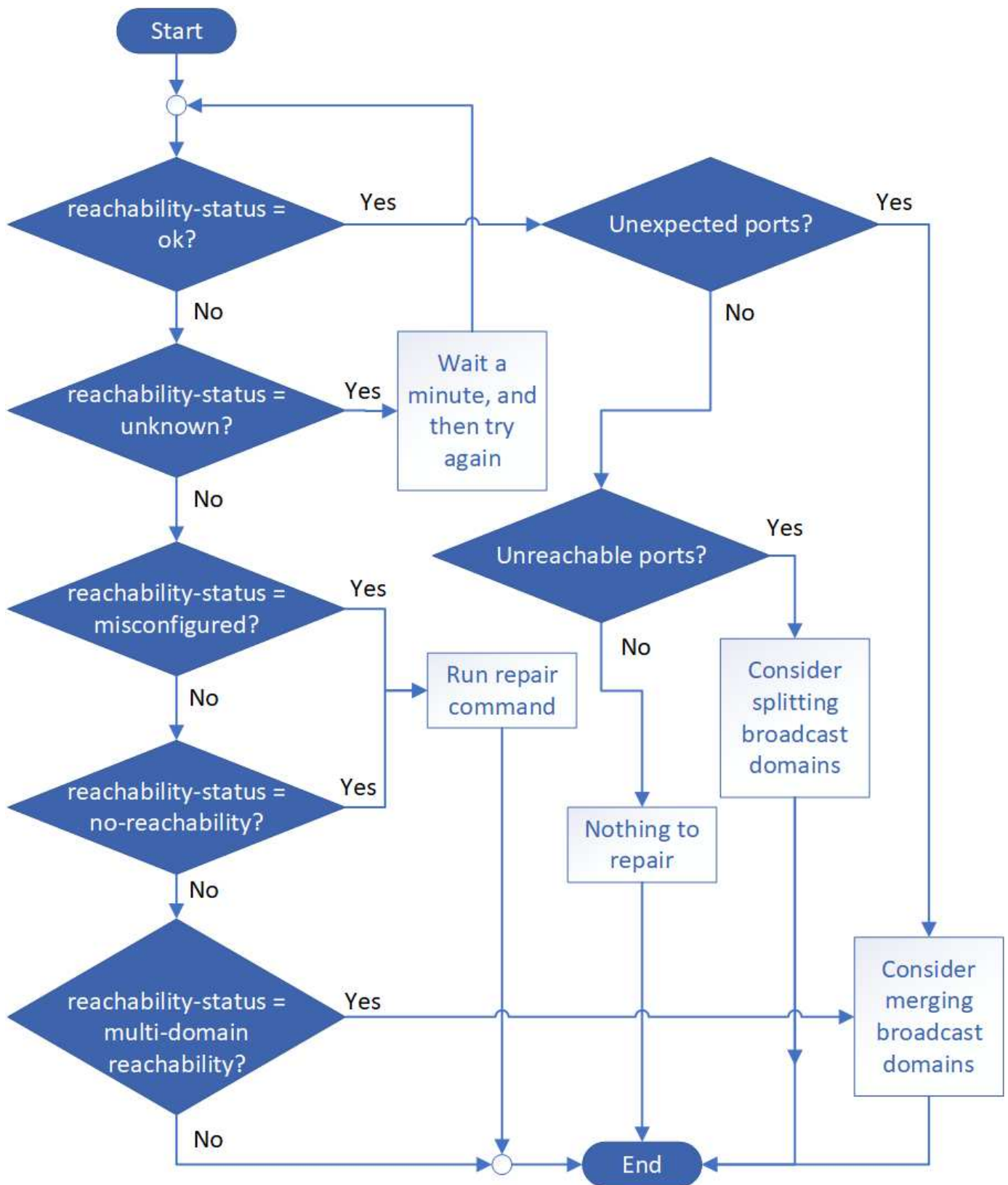
### Passo

1. Verifique se cada porta tem acessibilidade ao domínio de broadcast esperado:

```
network port reachability show -detail
```

O comando output contém resultados de acessibilidade. Use a seguinte árvore de decisão e tabela para entender os resultados de acessibilidade (status de acessibilidade) e determinar o que, se houver, fazer a seguir.





status de acessibilidade	Descrição
--------------------------	-----------

ok	<p>A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído.</p> <p>Se o status de acessibilidade for "ok", mas houver "portas inesperadas", considere mesclar um ou mais domínios de broadcast. Para obter mais informações, "<a href="#">Mesclar domínios de broadcast</a>" consulte .</p> <p>Se o status de acessibilidade for "ok", mas houver "portas inalcançáveis", considere dividir um ou mais domínios de broadcast. Para obter mais informações, "<a href="#">Dividir domínios de broadcast</a>" consulte .</p> <p>Se o status de acessibilidade for "ok" e não houver portas inesperadas ou inacessíveis, sua configuração está correta.</p>
acessibilidade mal configurada	<p>A porta não tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, a porta tem acessibilidade da camada 2 para um domínio de broadcast diferente.</p> <p>Você pode reparar a acessibilidade da porta. Ao executar o seguinte comando, o sistema atribuirá a porta ao domínio de broadcast ao qual tem acessibilidade:</p> <pre>network port reachability repair -node -port</pre> <p>Para obter mais informações, "<a href="#">Acessibilidade da porta de reparo</a>" consulte .</p>
sem acessibilidade	<p>A porta não tem acessibilidade da camada 2 para qualquer domínio de broadcast existente.</p> <p>Você pode reparar a acessibilidade da porta. Quando você executa o seguinte comando, o sistema atribuirá a porta a um novo domínio de broadcast criado automaticamente no IPspace padrão:</p> <pre>network port reachability repair -node -port</pre> <p>Para obter mais informações, "<a href="#">Acessibilidade da porta de reparo</a>" consulte .</p>
multidomínio-acessibilidade	<p>A porta tem acessibilidade da camada 2 ao domínio de broadcast atribuído; no entanto, também tem acessibilidade da camada 2 para pelo menos um outro domínio de broadcast.</p> <p>Examine a conectividade física e a configuração do switch para determinar se está incorreta ou se o domínio de broadcast atribuído à porta precisa ser mesclado com um ou mais domínios de broadcast.</p> <p>Para obter mais informações, consulte "<a href="#">Mesclar domínios de broadcast</a>" ou "<a href="#">Acessibilidade da porta de reparo</a>".</p>
desconhecido	<p>Se o status de acessibilidade for "desconhecido", aguarde alguns minutos e tente o comando novamente.</p>

Depois de reparar uma porta, você precisa verificar e resolver LIFs e VLANs deslocados. Se a porta fazia parte de um grupo de interfaces, você também precisa entender o que aconteceu com esse grupo de interfaces. Para obter mais informações, "[Acessibilidade da porta de reparo](#)" consulte .

## Remova o serviço de LIF EMS das políticas de serviço de rede após uma atualização do ONTAP

Se você tiver mensagens do sistema de gerenciamento de eventos (EMS) configuradas antes de atualizar do ONTAP 9,7 ou anterior para o ONTAP 9,8 ou posterior, após a atualização, as mensagens do EMS podem não ser entregues.

Durante a atualização, o Management-ems, que é o serviço EMS LIF, é adicionado a todas as políticas de serviço existentes. Isso permite que mensagens EMS sejam enviadas de qualquer uma das LIFs associadas a qualquer uma das políticas de serviço. Se o LIF selecionado não tiver acessibilidade ao destino de notificação de eventos, a mensagem não será entregue.

Para evitar isso, após a atualização, você deve remover o serviço EMS LIF das políticas de serviço de rede que não fornecem acessibilidade ao destino.

### Passos

1. Identificar as LIFs e as políticas de serviço de rede associadas através das quais as mensagens EMS podem ser enviadas:

```
network interface show -fields service-policy -services management-ems
```

```
vserver      lif      service-policy
-----
cluster-1    cluster_mgmt      default-management
cluster-1    node1-mgmt        default-management
cluster-1    node2-mgmt        default-management
cluster-1    inter_cluster    default-intercluster
4 entries were displayed.
```

2. Verifique se cada LIF tem conectividade com o destino EMS:

```
network ping -lif <lif_name> -vserver <svm_name> -destination
<destination_address>
```

Execute isso em cada nó.

## Exemplos

```
cluster-1::> network ping -lif nodel-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. Introduzir nível de privilégio avançado:

```
set advanced
```

4. Para os LIFs que não têm acessibilidade, remova o serviço Management-ems LIF das políticas de serviço correspondentes:

```
network interface service-policy remove-service -vserver <svm_name>
-policy <service_policy_name> -service management-ems
```

5. Verifique se o LIF de gestão-ems está agora associado apenas aos LIFs que fornecem acessibilidade ao destino EMS:

```
network interface show -fields service-policy -services management-ems
```

## Links relacionados

["LIFs e políticas de serviço no ONTAP 9.6 e posteriores"](#)

## Verifique o status da rede e do armazenamento para configurações do MetroCluster após uma atualização do ONTAP

Depois de atualizar um cluster ONTAP em uma configuração do MetroCluster, verifique o status das LIFs, agregados e volumes para cada cluster.

1. Verifique o status de LIF:

```
network interface show
```

Em operação normal, os LIFs para SVMs de origem devem ter um status de administrador de up e estar localizados em seus nós de origem. Os LIFs para SVMs de destino não precisam estar ativos ou localizados em seus nós de origem. No switchover, todos os LIFs têm um status de administrador de up, mas eles não precisam estar localizados em seus nós domésticos.

```

cluster1::> network interface show
          Logical      Status      Network      Current
Current Is
Vserver   Interface  Admin/Oper  Address/Mask  Node      Port
Home
-----
Cluster
          cluster1-a1_clus1
          up/up    192.0.2.1/24  cluster1-01
          true
          e2a
          cluster1-a1_clus2
          up/up    192.0.2.2/24  cluster1-01
          true
          e2b
cluster1-01
          clus_mgmt    up/up    198.51.100.1/24  cluster1-01
          true
          e3a
          cluster1-a1_inet4_intercluster1
          up/up    198.51.100.2/24  cluster1-01
          true
          e3c
          ...

27 entries were displayed.

```

## 2. Verifique o estado dos agregados:

```
storage aggregate show -state !online
```

Este comando exibe todos os agregados que estão *não* online. Em operação normal, todos os agregados localizados no local devem estar on-line. No entanto, se a configuração do MetroCluster estiver em switchover, os agregados de raiz no local de recuperação de desastres podem estar offline.

Este exemplo mostra um cluster em funcionamento normal:

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

Este exemplo mostra um cluster em switchover, no qual os agregados raiz no local de recuperação de

desastres estão offline:

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State  #Vols  Nodes           RAID
Status
-----
-----
aggr0_b1
          0B          0B    0% offline    0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
          0B          0B    0% offline    0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.
```

### 3. Verifique o estado dos volumes:

```
volume show -state !online
```

Este comando exibe todos os volumes que estão *não* online.

Se a configuração do MetroCluster estiver em operação normal (ela não estiver no estado de switchover), a saída deverá mostrar todos os volumes pertencentes aos SVMs secundárias do cluster (aqueles com o nome SVM anexado a "-mc").

Esses volumes só estão online em caso de mudança.

Este exemplo mostra um cluster em operação normal, no qual os volumes no local de recuperação de desastres não estão online.

```

cluster1::> volume show -state !online
(volume show)
Vserver   Volume           Aggregate      State      Type      Size
Available Used%
-----
vs2-mc    vol1             aggr1_b1      -          RW        -
-         -
vs2-mc    root_vs2        aggr0_b1      -          RW        -
-         -
vs2-mc    vol2             aggr1_b1      -          RW        -
-         -
vs2-mc    vol3             aggr1_b1      -          RW        -
-         -
vs2-mc    vol4             aggr1_b1      -          RW        -
-         -
5 entries were displayed.

```

#### 4. Verifique se não existem volumes inconsistentes:

```

volume show -is-inconsistent true

```

Consulte o artigo da base de dados de Conhecimento ["Volume Mostrando WAFL inconsistente"](#) sobre como resolver os volumes inconsistentes.

## Verifique a configuração da SAN após uma atualização do ONTAP

Após uma atualização do ONTAP, em um ambiente SAN, você deve verificar se cada iniciador que foi conectado a um LIF antes da atualização foi reconectado com êxito ao LIF.

#### 1. Verifique se cada iniciador está conectado ao LIF correto.

Você deve comparar a lista de iniciadores com a lista que você fez durante a preparação da atualização. Se você estiver executando o ONTAP 9.11,1 ou posterior, use o Gerenciador do sistema para exibir o status da conexão, pois ele oferece uma exibição muito mais clara do que a CLI.

## System Manager

- a. No System Manager, clique em **hosts > SAN Initiator Groups**.

A página exibe uma lista de grupos de iniciadores (grupos de iniciadores). Se a lista for grande, você pode visualizar páginas adicionais da lista clicando nos números de página no canto inferior direito da página.

As colunas exibem várias informações sobre os grupos. A partir de 9.11.1, o estado da ligação do grupo também é apresentado. Passe o Mouse sobre alertas de status para ver detalhes.

## CLI

- Listar iniciadores iSCSI:

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- Listar iniciadores FC:

```
fc initiator show -fields igroup,wwpn,lif
```

## Reconfigure as conexões do servidor KMIP após uma atualização do ONTAP 9.2 ou anterior

Depois de atualizar do ONTAP 9.2 ou anterior para o ONTAP 9.3 ou posterior, você precisa reconfigurar todas as conexões de servidor de gerenciamento de chaves externas (KMIP).

### Passos

1. Configurar a conectividade do gerenciador de chaves:

```
security key-manager setup
```

2. Adicione seus servidores KMIP:

```
security key-manager add -address <key_management_server_ip_address>
```

3. Verifique se os servidores KMIP estão conectados:

```
security key-manager show -status
```

4. Consultar os servidores-chave:



```
security key-manager query
```

5. Crie uma nova chave de autenticação e frase-passe:

```
security key-manager create-key -prompt-for-key true
```

A frase-passe tem de ter um mínimo de 32 caracteres.

6. Consultar a nova chave de autenticação:

```
security key-manager query
```

7. Atribua a nova chave de autenticação aos seus discos de encriptação automática (SEDs):

```
storage encryption disk modify -disk <disk_ID> -data-key-id <key_ID>
```



Certifique-se de que está a utilizar a nova chave de autenticação da sua consulta.

8. Se necessário, atribua uma chave FIPS às SEDs:

```
storage encryption disk modify -disk <disk_id> -fips-key-id  
<fips_authentication_key_id>
```

Se a configuração de segurança exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2-2, você deve criar uma chave separada para cada uma. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com o FIPS usada para acesso aos dados.

## Relocate os volumes de origem de espelho de compartilhamento de carga movidos após uma atualização do ONTAP

Depois de atualizar o ONTAP, você precisa mover os volumes de origem de espelhamento de compartilhamento de carga de volta para os locais de pré-atualização.

### Passos

1. Identifique o local para o qual você está movendo o volume de origem do espelho de compartilhamento de carga usando o Registro que você criou antes de mover o volume de origem do espelho de compartilhamento de carga.
2. Mova o volume de origem do espelho de compartilhamento de carga de volta para sua localização original:

## Alteração nas contas de usuário que podem acessar o processador de serviço após uma atualização do ONTAP

Se você criou contas de usuário no ONTAP 9.8 ou anterior que possam acessar o processador de serviço (SP) com uma função não admin e atualizar para o ONTAP 9.9,1 ou posterior, qualquer valor não admin no `-role` parâmetro será modificado para `admin`.

Para obter mais informações, "[Contas que podem acessar o SP](#)" consulte .

## Atualize o Pacote de Qualificação de disco após uma atualização do ONTAP

Depois de atualizar seu software ONTAP, você deve baixar e instalar o Pacote de Qualificação de disco do ONTAP (DQP). O DQP não é atualizado como parte de uma atualização do ONTAP.

O DQP contém os parâmetros adequados para a interação ONTAP com todas as unidades recém-qualificadas. Se a sua versão do DQP não contiver informações para uma unidade recém-qualificada, o ONTAP não terá as informações para configurar corretamente a unidade.

É prática recomendada atualizar o DQP a cada trimestre. Você também deve atualizar o DQP pelas seguintes razões:

- Sempre que você adicionar um novo tipo ou tamanho de unidade a um nó no cluster  
Por exemplo, se você já tiver unidades de 1 TB e adicionar unidades de 2 TB, precisará verificar a atualização DQP mais recente.
- Sempre que atualizar o firmware do disco
- Sempre que estiverem disponíveis ficheiros DQP ou firmware de disco mais recentes

### Informações relacionadas

- "[NetApp Downloads: Pacote de Qualificação de disco](#)"
- "[Downloads do NetApp: Firmware da unidade de disco](#)"

## **Informações sobre direitos autorais**

Copyright © 2025 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.