



Monitoramento de integridade

ONTAP 9

NetApp
January 08, 2026

Índice

Monitoramento de integridade	1
Saiba mais sobre o monitoramento de integridade do sistema ONTAP	1
Saiba mais sobre os componentes de monitoramento de integridade do ONTAP	1
Saiba mais sobre a resposta de alertas de integridade do sistema ONTAP	2
Saiba mais sobre a personalização do alerta de integridade do sistema ONTAP	2
Saiba mais sobre os gatilhos de alerta de saúde do ONTAP AutoSupport	3
Saiba mais sobre os monitores de integridade do cluster ONTAP disponíveis	3
Receber alertas de integridade do sistema ONTAP automaticamente	5
Responda à integridade do sistema ONTAP degradado	6
Saiba mais sobre como responder à integridade do sistema ONTAP degradado	6
Comandos para monitorar a integridade do seu sistema ONTAP	9
Apresentar o estado da integridade do sistema	9
Exibir o status da conectividade do nó	9
Monitore os switches de cluster e rede de armazenamento	10
Responder a alertas gerados	11
Configurar alertas futuros	11
Exiba informações sobre como o monitoramento de integridade é configurado	11
Veja as informações ambientais do ONTAP	12

Monitoramento de integridade

Saiba mais sobre o monitoramento de integridade do sistema ONTAP

Os monitores de integridade monitoram proativamente certas condições críticas no cluster e emitem alertas se detectarem uma falha ou risco. Se existirem alertas ativos, o estado de funcionamento do sistema comunica um estado degradado para o cluster. Os alertas incluem as informações de que você precisa para responder à integridade degradada do sistema.

Se o estado estiver degradado, pode visualizar detalhes sobre o problema, incluindo a causa provável e as ações de recuperação recomendadas. Depois de resolver o problema, o estado de funcionamento do sistema regressa automaticamente a OK.

O status de integridade do sistema reflete vários monitores de integridade separados. Um status degradado em um monitor de integridade individual causa um status degradado para a integridade geral do sistema.

Para obter detalhes sobre como o ONTAP suporta switches de cluster para monitoramento de integridade do sistema em seu cluster, consulte *Hardware Universe*.

["Switches suportados no Hardware Universe"](#)

Para obter detalhes sobre as causas das mensagens do AutoSupport do Monitor de integridade do comutador de cluster (CSHM) e as ações necessárias para resolver esses alertas, consulte o artigo da base de conhecimento.

["Mensagem do AutoSupport: Processo do monitor de saúde CSHM"](#)

Saiba mais sobre os componentes de monitoramento de integridade do ONTAP

Os monitores de saúde individuais têm um conjunto de políticas que acionam alertas quando ocorrem determinadas condições. Entender como funciona o monitoramento de saúde pode ajudá-lo a responder a problemas e controlar futuros alertas.

O monitoramento de integridade consiste nos seguintes componentes:

- Monitores de saúde individuais para subsistemas específicos, cada um dos quais tem seu próprio estado de saúde

Por exemplo, o subsistema Storage tem um monitor de integridade da conectividade de nó.

- Um monitor geral de integridade do sistema que consolida o estado de saúde dos monitores de saúde individuais

Um status degradado em qualquer subsistema resulta em um status degradado para todo o sistema. Se nenhum subsistema tiver alertas, o status geral do sistema é OK.

Cada monitor de saúde é composto pelos seguintes elementos-chave:

- Alerta de que o monitor de integridade pode potencialmente aumentar

Cada alerta tem uma definição, que inclui detalhes como a gravidade do alerta e sua causa provável.

- Políticas de saúde que identificam quando cada alerta é acionado

Cada política de saúde tem uma expressão de regra, que é a condição ou mudança exata que aciona o alerta.

Um monitor de integridade monitora e valida continuamente os recursos em seu subsistema para mudanças de condição ou estado. Quando uma condição ou mudança de estado corresponde a uma expressão de regra em uma política de saúde, o monitor de integridade gera um alerta. Um alerta faz com que o estado de funcionamento do subsistema e o estado geral do estado do sistema se degradem.

Saiba mais sobre a resposta de alertas de integridade do sistema ONTAP

Quando um alerta de integridade do sistema ocorre, você pode reconhecê-lo, saber mais sobre ele, reparar a condição subjacente e impedir que ele ocorra novamente.

Quando um monitor de saúde gera um alerta, você pode responder de qualquer uma das seguintes maneiras:

- Obtenha informações sobre o alerta, que inclui o recurso afetado, a gravidade do alerta, a causa provável, o possível efeito e as ações corretivas.
- Obtenha informações detalhadas sobre o alerta, como a hora em que o alerta foi gerado e se alguém já reconheceu o alerta.
- Obtenha informações relacionadas à integridade sobre o estado do recurso ou subsistema afetado, como um compartimento ou disco específico.
- Reconheça o alerta para indicar que alguém está trabalhando no problema e identifique-se como o ""reconhecimento"".
- Resolva o problema tomando as ações corretivas fornecidas no alerta, como a fixação de cabeamento para resolver um problema de conectividade.
- Exclua o alerta, se o sistema não o apagou automaticamente.
- Suprimir um alerta para impedir que ele afete o status de integridade de um subsistema.

Suprimir é útil quando você entende um problema. Depois de suprimir um alerta, ele ainda pode ocorrer, mas a integridade do subsistema é exibida como ""ok-with-suppressed."" quando o alerta suprimido ocorre.

Saiba mais sobre a personalização do alerta de integridade do sistema ONTAP

Você pode controlar quais alertas um monitor de integridade gera ativando e desativando as políticas de integridade do sistema que definem quando os alertas são acionados. Isso permite que você personalize o sistema de monitoramento de integridade para seu ambiente específico.

Você pode aprender o nome de uma política exibindo informações detalhadas sobre um alerta gerado ou

exibindo definições de política para um monitor de integridade específico, nó ou ID de alerta.

Desativar políticas de saúde é diferente de suprimir alertas. Quando você suprime um alerta, ele não afeta o status de integridade do subsistema, mas o alerta ainda pode ocorrer.

Se você desabilitar uma política, a condição ou estado definido em sua expressão de regra de política não acionará mais um alerta.

Exemplo de um alerta que você deseja desativar

Por exemplo, suponha que ocorra um alerta que não seja útil para você. Você usa o `system health alert show -instance` comando para obter o ID da política para o alerta. Você usa o ID da política no `system health policy definition show` comando para exibir informações sobre a política. Depois de analisar a expressão da regra e outras informações sobre a política, você decide desativar a política. Você usa o `system health policy definition modify` comando para desativar a política.

Informações relacionadas

- ["mostrar alerta de saúde do sistema"](#)

Saiba mais sobre os gatilhos de alerta de saúde do ONTAP AutoSupport

Os alertas de integridade do sistema acionam mensagens e eventos AutoSupport no sistema de Gestão de Eventos (EMS), permitindo-lhe monitorizar a integridade do sistema utilizando mensagens AutoSupport e o EMS, além de utilizar diretamente o sistema de monitorização de integridade.

O sistema envia uma mensagem AutoSupport dentro de cinco minutos após um alerta. A mensagem AutoSupport inclui todos os alertas gerados desde a mensagem AutoSupport anterior, exceto para alertas que duplicam um alerta para o mesmo recurso e causa provável na semana anterior.

Alguns alertas não acionam mensagens AutoSupport. Um alerta não aciona uma mensagem AutoSupport se a sua política de integridade desativar o envio de mensagens AutoSupport. Por exemplo, uma política de integridade pode desativar as mensagens do AutoSupport por padrão porque o AutoSupport já gera uma mensagem quando o problema ocorre. Você pode configurar políticas para não acionar mensagens AutoSupport usando o `system health policy definition modify` comando.

Você pode ver uma lista de todas as mensagens AutoSupport acionadas por alerta enviadas na semana anterior usando o `system health autosupport trigger history show` comando.

Os alertas também acionam a geração de eventos para o EMS. Um evento é gerado cada vez que um alerta é criado e cada vez que um alerta é apagado.

Saiba mais sobre os monitores de integridade do cluster ONTAP disponíveis

Existem vários monitores de integridade que monitorizam diferentes partes de um cluster. Os monitores de integridade ajudam você a se recuperar de erros nos sistemas ONTAP detetando eventos, enviando alertas para você e excluindo eventos conforme eles forem claros.

Nome do monitor de integridade (identificador)	Nome do subsistema (identificador)	Finalidade
Switch Ethernet	Interrutor (estado do interruptor)	<p>O Monitor de integridade do comutador Ethernet ONTAP (CSHM) monitora o status dos switches de rede de cluster e armazenamento enquanto coleta logs para análise. Por padrão, o CSHM polls cada switch via SNMPv2c a cada 5 minutos para atualizar tabelas de recursos com informações sobre capacidade de suporte, status de monitoramento, sensores de temperatura, utilização de CPU, configurações de interface e conexões, redundância de switch de cluster e operações de ventilador e fonte de alimentação. Além disso, se configurado, o CSHM coleta logs via SSH/SCP a cada hora, que são enviados através do AutoSupport para análise posterior. Mediante solicitação, o CSHM também pode executar uma coleção de log de suporte técnico mais detalhada usando SSH/SCP.</p> <p>"Monitoramento de integridade do switch" Consulte para obter mais detalhes.</p>
MetroCluster Fabric	Interrutor	Monitora a topologia da malha de back-end de configuração do MetroCluster e detecta configurações incorretas, como cabeamento e zoneamento incorretos e falhas de ISL.
MetroCluster Saúde	Interconexão, RAID e armazenamento	Monitora os adaptadores FC-VI, os adaptadores iniciador FC, os discos e agregados esquerdos e as portas entre clusters
Conetividade do nó (nó-conexão)	Operações ininterruptas de CIFS (CIFS-NDO)	Monitora conexões SMB para operações ininterruptas com aplicações Hyper-V.

Nome do monitor de integridade (identificador)	Nome do subsistema (identificador)	Finalidade
Storage (conexão SAS)	Monitora compartimentos, discos e adaptadores no nível do nó para ver os caminhos e as conexões apropriados.	Sistema
não aplicável	Agrega informações de outros monitores de saúde.	Conetividade do sistema (conexão do sistema)

Receber alertas de integridade do sistema ONTAP automaticamente

Você pode visualizar manualmente os alertas de integridade do sistema usando o `system health alert show` comando. No entanto, você deve assinar mensagens específicas do sistema de Gerenciamento de Eventos (EMS) para receber notificações automaticamente quando um monitor de integridade gera um alerta.

Sobre esta tarefa

O procedimento a seguir mostra como configurar notificações para todas as mensagens `hm.alert.raised` e todas as mensagens `hm.alert.cleared`.

Todas as mensagens `hm.alert.raised` e todas as mensagens `hm.alert.cleared` incluem um trap SNMP. Os nomes dos traps SNMP são `HealthMonitorAlertRaised` e `HealthMonitorAlertCleared`.

Saiba mais sobre `system health alert show` o ["Referência do comando ONTAP"](#) na .

Passos

1. Utilize o `event destination create` comando para definir o destino para o qual pretende enviar as mensagens EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

Saiba mais sobre `event destination create` o ["Referência do comando ONTAP"](#) na .

2. Utilize o `event route add-destinations` comando para encaminhar a `hm.alert.raised` mensagem e a `hm.alert.cleared` mensagem para um destino.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

Saiba mais sobre `event route add-destinations` o ["Referência do comando ONTAP"](#) na .

Informações relacionadas

- ["Visualize a rede ONTAP usando o Gerenciador do sistema"](#)
- ["Como configurar o monitoramento SNMP no DATA ONTAP"](#)

Responda à integridade do sistema ONTAP degradado

Quando o estado de funcionamento do sistema estiver degradado, pode apresentar alertas, ler sobre a causa provável e as ações correctivas, apresentar informações sobre o subsistema degradado e resolver o problema. Alertas suprimidos também são mostrados para que você possa modificá-los e ver se eles foram reconhecidos.

Sobre esta tarefa

Você pode descobrir que um alerta foi gerado visualizando uma mensagem AutoSupport ou um evento EMS, ou usando os `system health` comandos.

Passos

1. Use o `system health alert show` comando para visualizar os alertas que estão comprometendo a integridade do sistema.
2. Leia a causa provável, o possível efeito e as ações corretivas do alerta para determinar se você pode resolver o problema ou precisa de mais informações.
3. Se você precisar de mais informações, use o `system health alert show -instance` comando para exibir informações adicionais disponíveis para o alerta.
4. Use o `system health alert modify` comando com o `-acknowledge` parâmetro para indicar que você está trabalhando em um alerta específico.
5. Tome medidas corretivas para resolver o problema conforme descrito pelo `Corrective Actions` campo no alerta.

As ações corretivas podem incluir a reinicialização do sistema.

Quando o problema é resolvido, o alerta é automaticamente apagado. Se o subsistema não tiver outros alertas, a integridade do subsistema será alterada para OK. Se a integridade de todos os subsistemas estiver OK, o estado geral do sistema muda para OK.

6. Utilize o `system health status show` comando para confirmar se o estado de funcionamento do sistema é OK.

Se o estado de funcionamento do sistema não for OK , repita este procedimento.

Informações relacionadas

- ["alerta de saúde do sistema modificado"](#)

Saiba mais sobre como responder à integridade do sistema ONTAP degradado

Ao analisar um exemplo específico de integridade do sistema degradado causado por um compartimento que não tem dois caminhos para um nó, você pode ver o que a CLI exibe quando você responde a um alerta.

Depois de iniciar o ONTAP, você verifica a integridade do sistema e descobre que o status está degradado:

```
cluster1::>system health status show
Status
-----
degraded
```

Você mostra alertas para descobrir onde está o problema e vê que o compartimento 2 não tem dois caminhos para o node1:

```
cluster1::>system health alert show
Node: node1
Resource: Shelf ID 2
Severity: Major
Indication Time: Mon Nov 10 16:48:12 2013
Probable Cause: Disk shelf 2 does not have two paths to controller
node1.
Possible Effect: Access to disk shelf 2 via controller node1 will be
lost with a single hardware component failure (e.g.
cable, HBA, or IOM failure).
Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
3. Reboot the halted controllers.
4. Contact support personnel if the alert persists.
```

Você exibe detalhes sobre o alerta para obter mais informações, incluindo o ID de alerta:

```

cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
    Node: node1
    Monitor: node-connect
    Alert ID: DualPathToDiskShelf_Alert
    Alerting Resource: 50:05:0c:c1:02:00:0f:02
    Subsystem: SAS-connect
    Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
    Probable Cause: Connection_establishment_error
    Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
    Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
    hardware component failure (e.g. cable, HBA, or IOM failure).
    Acknowledge: false
    Suppress: false
    Policy: DualPathToDiskShelf_Policy
    Acknowledger: -
    Suppressor: -
    Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
    Alerting Resource Name: Shelf ID 2

```

Você reconhece o alerta para indicar que está trabalhando nele.

```

cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true

```

Você conserta o cabeamento entre as prateleiras 2 e node1 e reinicializa o sistema. Em seguida, você verifica novamente a integridade do sistema e vê se o status é OK:

```
cluster1::>system health status show
Status
-----
OK
```

Informações relacionadas

- ["alerta de saúde do sistema modificado"](#)

Comandos para monitorar a integridade do seu sistema ONTAP

Você pode usar os `system health` comandos para exibir informações sobre a integridade dos recursos do sistema, responder a alertas e configurar alertas futuros. O uso dos comandos CLI permite exibir informações detalhadas sobre como o monitoramento de integridade é configurado. Saiba mais sobre `system health` o ["Referência do comando ONTAP"](#) na .

Apresentar o estado da integridade do sistema

Se você quiser...	Use este comando...
Apresentar o estado de funcionamento do sistema, que reflete o estado geral dos monitores de saúde individuais	<code>system health status show</code>
Apresentar o estado de funcionamento dos subsistemas para os quais a monitorização de integridade está disponível	<code>system health subsystem show</code>

Exibir o status da conectividade do nó

Se você quiser...	Use este comando...
Exiba detalhes sobre a conectividade do nó para o compartimento de storage, incluindo informações de porta, velocidade da porta HBA, taxa de transferência de e/S e taxa de operações de e/S por segundo	<code>storage shelf show -connectivity</code> Use o <code>-instance</code> parâmetro para exibir informações detalhadas sobre cada prateleira.
Exiba informações sobre unidades e LUNs de storage, incluindo o espaço utilizável, os números de compartimento e compartimento e o nome do nó proprietário	<code>storage disk show</code> Use o <code>-instance</code> parâmetro para exibir informações detalhadas sobre cada unidade.

Se você quiser...	Use este comando...
Exiba informações detalhadas sobre as portas do compartimento de armazenamento, incluindo o tipo, a velocidade e o status da porta	<pre>storage port show</pre> <p>Use o <code>-instance</code> parâmetro para exibir informações detalhadas sobre cada adaptador.</p>

Monitore os switches de cluster e rede de armazenamento

Se você quiser...	Use este comando... (ONTAP 9.8 e posterior)	Use este comando... (ONTAP 9.7 e anteriores)
Apresentar os interruptores que o grupo de instrumentos monitoriza	<pre>system switch ethernet show</pre>	<pre>system cluster-switch show</pre>
Exibir os switches que o cluster monitora atualmente, incluindo os switches que você excluiu (mostrado na coluna motivo na saída do comando) Este comando está disponível no nível de privilégio avançado	<pre>system switch ethernet show-all</pre>	<pre>system cluster-switch show-all</pre>
Configurar o monitoramento de um switch não descoberto	<pre>system switch ethernet create</pre>	<pre>system cluster-switch create</pre>
Modificar informações sobre um switch que o cluster monitora (por exemplo, nome do dispositivo, endereço IP, versão SNMP e cadeia de caracteres da comunidade)	<pre>system switch ethernet modify</pre>	<pre>system cluster-switch modify</pre>
Desativar um interruptor da monitorização	<pre>system switch ethernet modify -disable-monitoring</pre>	<pre>system cluster-switch modify -disable-monitoring</pre>
Excluir um switch da monitoração	<pre>system switch ethernet delete</pre>	<pre>system cluster-switch delete</pre>
Remover permanentemente as informações de configuração do switch que são armazenadas no banco de dados (isso reabilita a descoberta automática do switch)	<pre>system switch ethernet delete -force</pre>	<pre>system cluster-switch delete -force</pre>
Execute a coleta de logs com um switch	<pre>system switch ethernet log</pre>	<pre>system cluster-switch log</pre>



"Monitoramento de integridade do switch" Consulte e "Configurar a coleção de registros" para obter mais detalhes.


Responder a alertas gerados



Se você quiser...	Use este comando...
Exiba informações sobre alertas gerados, como o recurso e o nó em que o alerta foi acionado, e a gravidade e a causa provável do alerta	<code>system health alert show</code>
Exibir informações sobre cada alerta gerado	<code>system health alert show -instance</code>
Indique que alguém está trabalhando em um alerta	<code>system health alert modify</code>
Confirme um alerta	<code>system health alert modify -acknowledge</code>
Suprimir um alerta subsequente para que não afete o estado de funcionamento de um subsistema	<code>system health alert modify -suppress</code>
Exclua um alerta que não foi apagado automaticamente	<code>system health alert delete</code>
Exiba informações sobre as mensagens do AutoSupport que alertas dispararam na última semana, por exemplo, para determinar se um alerta acionou uma mensagem do AutoSupport	<code>system health autosupport trigger history show</code>

Configurar alertas futuros

Se você quiser...	Use este comando...
Ative ou desative a política que controla se um estado de recurso específico gera um alerta específico	<code>system health policy definition modify</code>

Exiba informações sobre como o monitoramento de integridade é configurado

Se você quiser...	Use este comando...
Exibir informações sobre monitores de integridade, como seus nós, nomes, subsistemas e status	<code>system health config show</code> <div> Use o <code>-instance</code> parâmetro para exibir informações detalhadas sobre cada monitor de integridade.</div>

Se você quiser...	Use este comando...
Exiba informações sobre os alertas que um monitor de integridade pode gerar	<pre>system health alert definition show</pre> <div>  <p>Use o <code>-instance</code> parâmetro para exibir informações detalhadas sobre cada definição de alerta.</p> </div>
Exiba informações sobre as políticas do monitor de integridade, que determinam quando os alertas são gerados	<pre>system health policy definition show</pre> <div>  <p>Use o <code>-instance</code> parâmetro para exibir informações detalhadas sobre cada política. Use outros parâmetros para filtrar a lista de alertas - por exemplo, por status da política (habilitado ou não), monitor de integridade, alerta e assim por diante.</p> </div>

Informações relacionadas

- ["exposição de porta de armazenamento"](#)
- ["exposição de prateleiras de armazenamento"](#)
- ["exclusão de alerta de integridade do sistema"](#)

Veja as informações ambientais do ONTAP

Os sensores ajudam a monitorar os componentes ambientais do seu sistema. As informações que você pode visualizar sobre os sensores ambientais incluem seus avisos de tipo, nome, estado, valor e limite.

Passo

1. Para exibir informações sobre sensores ambientais, use o `system node environment sensors show` comando.

Informações sobre direitos autorais

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

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

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

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

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

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

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

Informações sobre marcas comerciais

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