



Gerenciar nós de administração

StorageGRID

NetApp
March 12, 2025

Índice

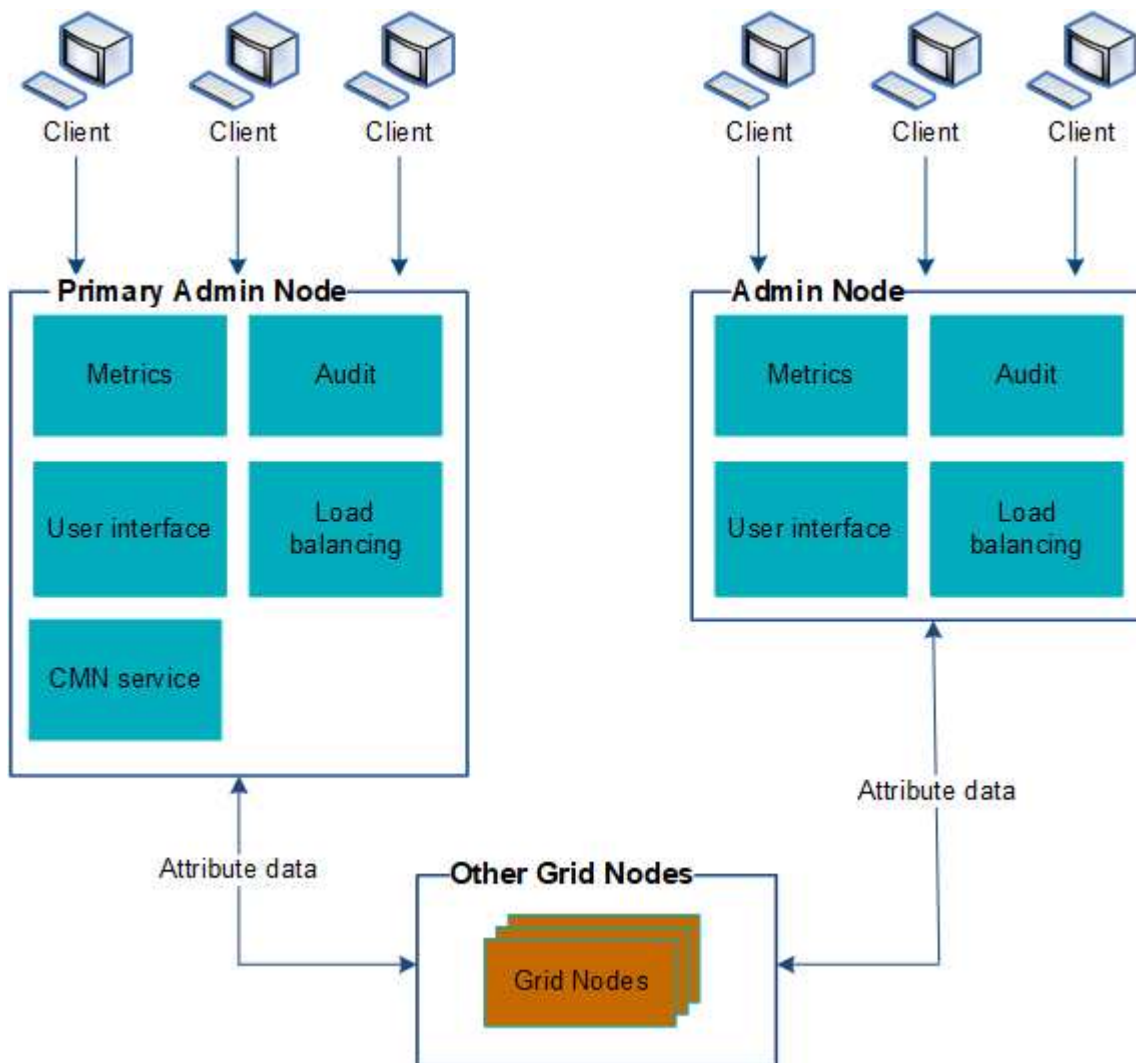
Gerenciar nós de administração	1
Use vários nós de administração	1
Identifique o nó de administração principal	2
Exibir status de notificação e filas	2
Como os nós de administração mostram alarmes reconhecidos (sistema legado)	3
Configurar acesso de cliente de auditoria	4
Configurar acesso de cliente de auditoria para NFS	4
Adicione um cliente de auditoria NFS a um compartilhamento de auditoria	6
Verificar a integração da auditoria NFS	8
Remover um cliente de auditoria NFS do compartilhamento de auditoria	8
Altere o endereço IP de um cliente de auditoria NFS	10

Gerenciar nós de administração

Use vários nós de administração

Um sistema StorageGRID pode incluir vários nós de administração para permitir que você monitore e configure continuamente seu sistema StorageGRID, mesmo se um nó de administração falhar.

Se um nó Admin ficar indisponível, o processamento de atributos continua, alertas e alarmes (sistema legado) ainda serão acionados e notificações de e-mail e pacotes AutoSupport ainda serão enviados. No entanto, ter vários nós de administração não fornece proteção contra failover, exceto notificações e pacotes de AutoSupport. Em particular, os reconhecimentos de alarmes feitos de um nó Admin não são copiados para outros nós Admin.



Existem duas opções para continuar a visualizar e configurar o sistema StorageGRID se um nó de administrador falhar:

- Os clientes da Web podem se reconectar a qualquer outro nó de administração disponível.
- Se um administrador do sistema tiver configurado um grupo de nós de administração de alta disponibilidade, os clientes da Web poderão continuar a aceder ao Gestor de grelha ou ao Gestor de

inquilinos utilizando o endereço IP virtual do grupo HA. "[Gerenciar grupos de alta disponibilidade](#)" Consulte



Ao usar um grupo de HA, o acesso é interrompido se o nó Admin ativo falhar. Os usuários devem fazer login novamente após o failover do endereço IP virtual do grupo HA para outro nó Admin no grupo.

Algumas tarefas de manutenção só podem ser executadas usando o nó de administração principal. Se o nó de administração principal falhar, ele deve ser recuperado antes que o sistema StorageGRID esteja totalmente funcional novamente.

Identifique o nó de administração principal

O nó de administração principal hospeda o serviço CMN. Alguns procedimentos de manutenção só podem ser executados usando o nó de administração principal.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um "[navegador da web suportado](#)".
- Você "[permissões de acesso específicas](#)" tem .

Passos

1. Selecione **SUPPORT > Tools > Grid topology**.
2. Selecione **site > Admin Node** e, em seguida, **+** selecione para expandir a árvore de topologia e mostrar os serviços hospedados neste Admin Node.

O nó de administração principal hospeda o serviço CMN.

3. Se este nó Admin não hospedar o serviço CMN, verifique os outros nós Admin.


Exibir status de notificação e filas





O serviço do sistema de gerenciamento de rede (NMS) nos nós de administração envia notificações para o servidor de e-mail. Você pode visualizar o status atual do serviço NMS e o tamanho de sua fila de notificações na página mecanismo de interface.

Para acessar a página mecanismo de interface, selecione **SUPPORT > Tools > Grid topology**. Finalmente, selecione **site > Admin Node > NMS > Interface Engine**.





Overview | Alarms | Reports | Configuration

Main







 **Overview: NMS (170-176) - Interface Engine**
Updated: 2009-03-09 10:12:17 PDT

NMS Interface Engine Status:	Connected	 
Connected Services:	15	 

E-mail Notification Events

E-mail Notifications Status:	No Errors	 
E-mail Notifications Queued:	0	 

Database Connection Pool

Maximum Supported Capacity:	100	 
Remaining Capacity:	95 %	 
Active Connections:	5	 

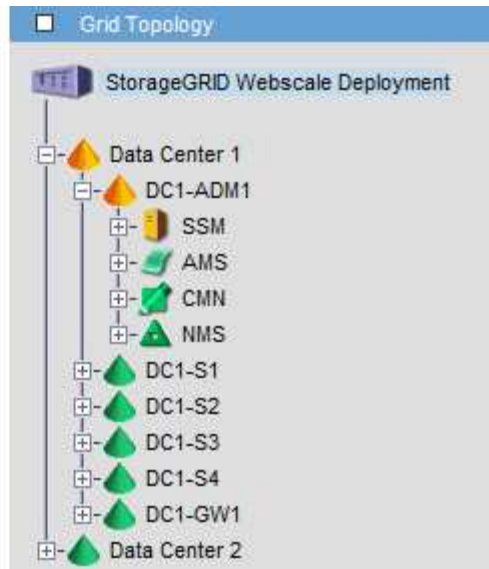
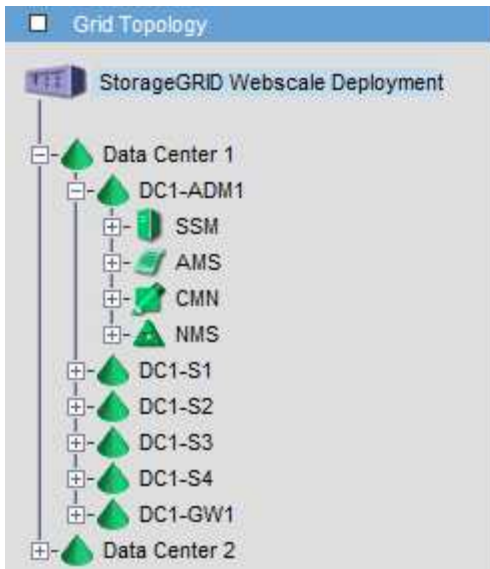
As notificações são processadas através da fila de notificações de e-mail e são enviadas para o servidor de e-mail uma após a outra na ordem em que são acionadas. Se houver um problema (por exemplo, um erro de conexão de rede) e o servidor de e-mail não estiver disponível quando a tentativa for feita para enviar a notificação, uma tentativa de reenviar a notificação para o servidor de e-mail continuará por um período de 60 segundos. Se a notificação não for enviada para o servidor de correio após 60 segundos, a notificação será retirada da fila de notificações e será feita uma tentativa de enviar a próxima notificação na fila.

Como as notificações podem ser retiradas da fila de notificações sem serem enviadas, é possível que um alarme possa ser acionado sem que uma notificação seja enviada. Se uma notificação for descartada da fila sem ser enviada, o alarme menor MINS (Status da notificação de e-mail) será acionado.

Como os nós de administração mostram alarmes reconhecidos (sistema legado)

Quando você reconhece um alarme em um nó Admin, o alarme reconhecido não é copiado para nenhum outro nó Admin. Como os reconhecimentos não são copiados para outros nós de administração, a árvore de topologia de grade pode não ter a mesma aparência para cada nó de administração.

Essa diferença pode ser útil ao conectar clientes da Web. Os clientes da Web podem ter visualizações diferentes do sistema StorageGRID com base nas necessidades do administrador.



Observe que as notificações são enviadas do nó Admin onde a confirmação ocorre.

Configurar acesso de cliente de auditoria

Configurar acesso de cliente de auditoria para NFS

O Admin Node, por meio do serviço do Audit Management System (AMS), Registra todos os eventos do sistema auditados em um arquivo de log disponível por meio do compartilhamento de auditoria, que é adicionado a cada Admin Node na instalação. O compartilhamento de auditoria é ativado automaticamente como um compartilhamento somente leitura.



O suporte para NFS foi obsoleto e será removido em uma versão futura.

Para acessar logs de auditoria, você pode configurar o acesso do cliente a compartilhamentos de auditoria para NFS. Ou, você pode ["use um servidor syslog externo"](#).

O sistema StorageGRID usa reconhecimento positivo para evitar a perda de mensagens de auditoria antes de serem gravadas no arquivo de log. Uma mensagem permanece na fila em um serviço até que o serviço AMS ou um serviço de relé de auditoria intermediária tenha reconhecido o controle dele. Para obter mais informações, ["Rever registros de auditoria"](#) consulte .

Antes de começar

- Você tem o `Passwords.txt` arquivo com a senha root/admin.
- Você tem o `Configuration.txt` arquivo (disponível no Pacote de recuperação).
- O cliente de auditoria está usando o NFS versão 3 (NFSv3).

Sobre esta tarefa

Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

Passos

1. Faça login no nó de administração principal:

- a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- c. Digite o seguinte comando para mudar para root: `su -`
- d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Confirme se todos os serviços têm estado em execução ou verificado. Introduza: `storagegrid-status`

Se algum serviço não estiver listado como em execução ou verificado, resolva problemas antes de continuar.

3. Retorne à linha de comando. Pressione **Ctrl * C***.

4. Inicie o utilitário de configuração NFS. Introduza: `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share      | add-ip-to-share       | validate-config      |  
| enable-disable-share | remove-ip-from-share  | refresh-config      |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

5. Adicione o cliente de auditoria: `add-audit-share`

- a. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: `client_IP_address`
- b. Quando solicitado, pressione **Enter**.

6. Se mais de um cliente de auditoria tiver permissão para acessar o compartilhamento de auditoria, adicione o endereço IP do usuário adicional: `add-ip-to-share`

- a. Introduza o número da partilha de auditoria: `audit_share_number`
- b. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: `client_IP_address`
- c. Quando solicitado, pressione **Enter**.

O utilitário de configuração NFS é exibido.

- d. Repita essas subetapas para cada cliente de auditoria adicional que tenha acesso ao compartilhamento de auditoria.

7. Opcionalmente, verifique sua configuração.

- a. Introduza o seguinte: `validate-config`

Os serviços são verificados e exibidos.

b. Quando solicitado, pressione **Enter**.

O utilitário de configuração NFS é exibido.

c. Feche o utilitário de configuração NFS: `exit`

8. Determine se você deve habilitar compartilhamentos de auditoria em outros sites.

- Se a implantação do StorageGRID for um único local, vá para a próxima etapa.
- Se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:

i. Inicie sessão remotamente no Admin Node do site:

A. Introduza o seguinte comando: `ssh admin@grid_node_IP`

B. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

C. Digite o seguinte comando para mudar para root: `su -`

D. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

ii. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó Admin adicional.

iii. Feche o login de shell seguro remoto para o Admin Node remoto. Introduza: `exit`

9. Faça logout do shell de comando: `exit`

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Conceda acesso ao compartilhamento de auditoria a um novo cliente de auditoria NFS adicionando seu endereço IP ao compartilhamento ou remova um cliente de auditoria existente removendo seu endereço IP.

Adicione um cliente de auditoria NFS a um compartilhamento de auditoria

Os clientes de auditoria NFS têm acesso a um compartilhamento de auditoria com base em seu endereço IP. Conceda acesso ao compartilhamento de auditoria a um novo cliente de auditoria NFS adicionando seu endereço IP ao compartilhamento de auditoria.



O suporte para NFS foi obsoleto e será removido em uma versão futura.

Antes de começar

- Você tem o `Passwords.txt` arquivo com a senha da conta root/admin.
- Você tem o `Configuration.txt` arquivo (disponível no Pacote de recuperação).
- O cliente de auditoria está usando o NFS versão 3 (NFSv3).

Passos

1. Faça login no nó de administração principal:

a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`

b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

c. Digite o seguinte comando para mudar para root: `su -`

d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Inicie o utilitário de configuração NFS: `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share      | add-ip-to-share       | validate-config      |  
| enable-disable-share | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

3. Introduza: `add-ip-to-share`

Uma lista de compartilhamentos de auditoria NFS habilitados no Admin Node é exibida. O compartilhamento de auditoria é listado como: `/var/local/log`

4. Introduza o número da partilha de auditoria: `audit_share_number`

5. Quando solicitado, insira o endereço IP ou o intervalo de endereços IP do cliente de auditoria para o compartilhamento de auditoria: `client_IP_address`

O cliente de auditoria é adicionado ao compartilhamento de auditoria.

6. Quando solicitado, pressione **Enter**.

O utilitário de configuração NFS é exibido.

7. Repita as etapas para cada cliente de auditoria que deve ser adicionado ao compartilhamento de auditoria.

8. Opcionalmente, verifique sua configuração: `validate-config`

Os serviços são verificados e exibidos.

a. Quando solicitado, pressione **Enter**.

O utilitário de configuração NFS é exibido.

9. Feche o utilitário de configuração NFS: `exit`

10. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

Caso contrário, se a implantação do StorageGRID incluir nós de administração em outros sites, ative opcionalmente esses compartilhamentos de auditoria, conforme necessário:

a. Faça login remotamente no Admin Node de um site:

i. Introduza o seguinte comando: `ssh admin@grid_node_IP`

- ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- b. Repita estas etapas para configurar os partilhaamentos de auditoria para cada nó de administração.
 - c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`
11. Faça logout do shell de comando: `exit`

Verificar a integração da auditoria NFS

Depois de configurar um partilhaamento de auditoria e adicionar um cliente de auditoria NFS, você pode montar o partilhaamento de cliente de auditoria e verificar se os arquivos estão disponíveis no partilhaamento de auditoria.



O suporte para NFS foi obsoleto e será removido em uma versão futura.

Passos

1. Verifique a conectividade (ou variante para o sistema cliente) usando o endereço IP do lado do cliente do nó Admin que hospeda o serviço AMS. Introduza: `ping IP_address`

Verifique se o servidor responde, indicando conectividade.

2. Monte o partilhaamento de auditoria somente leitura usando um comando apropriado ao sistema operacional cliente. Um exemplo de comando Linux é (Enter em uma linha):

```
mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/log myAudit
```

Use o endereço IP do nó de administração que hospeda o serviço AMS e o nome de partilhaamento predefinido para o sistema de auditoria. O ponto de montagem pode ser qualquer nome selecionado pelo cliente (por exemplo, `myAudit` no comando anterior).

3. Verifique se os arquivos estão disponíveis no partilhaamento de auditoria. Introduza: `ls myAudit /*`

```
`_myAudit_`onde está o ponto de montagem da partilha de auditoria. Deve haver pelo menos um arquivo de log listado.
```

Remover um cliente de auditoria NFS do partilhaamento de auditoria

Os clientes de auditoria NFS têm acesso a um partilhaamento de auditoria com base em seu endereço IP. Você pode remover um cliente de auditoria existente removendo seu endereço IP.

Antes de começar

- Você tem o `Passwords.txt` arquivo com a senha da conta root/admin.
- Você tem o `Configuration.txt` arquivo (disponível no Pacote de recuperação).

Sobre esta tarefa

Não é possível remover o último endereço IP permitido para acessar o compartilhamento de auditoria.

Passos

1. Faça login no nó de administração principal:

- Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- Digite o seguinte comando para mudar para root: `su -`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Inicie o utilitário de configuração NFS: `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share       | add-ip-to-share       | validate-config      |  
| enable-disable-share  | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

3. Remova o endereço IP do compartilhamento de auditoria: `remove-ip-from-share`

Uma lista numerada de compartilhamentos de auditoria configurados no servidor é exibida. O compartilhamento de auditoria é listado como: `/var/local/log`

4. Introduza o número correspondente à partilha de auditoria: `audit_share_number`

É apresentada uma lista numerada de endereços IP permitidos para aceder à partilha de auditoria.

5. Introduza o número correspondente ao endereço IP que pretende remover.

O compartilhamento de auditoria é atualizado e o acesso não é mais permitido a partir de qualquer cliente de auditoria com este endereço IP.

6. Quando solicitado, pressione **Enter**.

O utilitário de configuração NFS é exibido.

7. Feche o utilitário de configuração NFS: `exit`

8. Se a implantação do StorageGRID for uma implantação de vários locais de data center com nós de administração adicionais nos outros sites, desative esses compartilhamentos de auditoria conforme necessário:

- Faça login remotamente no Admin Node de cada site:
 - Introduza o seguinte comando: `ssh admin@grid_node_IP`

- ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - iii. Digite o seguinte comando para mudar para root: `su -`
 - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
 - b. Repita estas etapas para configurar os partilhaamentos de auditoria para cada nó Admin adicional.
 - c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`
9. Faça logout do shell de comando: `exit`

Altere o endereço IP de um cliente de auditoria NFS

Conclua estas etapas se precisar alterar o endereço IP de um cliente de auditoria NFS.

Passos

1. Adicione um novo endereço IP a um partilhaamento de auditoria NFS existente.
2. Remova o endereço IP original.

Informações relacionadas

- ["Adicione um cliente de auditoria NFS a um partilhaamento de auditoria"](#)
- ["Remover um cliente de auditoria NFS do partilhaamento de auditoria"](#)

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.