



Use o monitoramento SNMP

StorageGRID software

NetApp
July 23, 2026

Índice

- Use o monitoramento SNMP 1
 - Use o monitoramento SNMP no StorageGRID 1
 - Capacidades 1
 - Suporte à versão SNMP 2
 - Limitações 2
 - Configure o agente SNMP no StorageGRID 2
 - Especifique a configuração básica 3
 - Insira as strings da comunidade 3
 - Criar destinos de trap 4
 - Criar endereços de agente 6
 - Criar usuários USM 7
 - Atualize o agente SNMP do StorageGRID 9
 - Acesse os arquivos MIB do StorageGRID 11
 - Acesse os arquivos MIB 11
 - Conteúdo do arquivo MIB 11
 - Objetos MIB 12

Use o monitoramento SNMP

Use o monitoramento SNMP no StorageGRID

Se você deseja monitorar StorageGRID usando o Protocolo Simples de Gerenciamento de Rede (SNMP), você deve configurar o agente SNMP que está incluído com o StorageGRID.

- ["Configurar o agente SNMP"](#)
- ["Atualize o agente SNMP"](#)

Capacidades

Cada nó do StorageGRID executa um agente SNMP, ou daemon, que fornece um MIB. O MIB do StorageGRID contém definições de tabelas e notificações para alertas. O MIB também contém informações de descrição do sistema, como plataforma e número do modelo para cada nó. Cada nó do StorageGRID também suporta um subconjunto de objetos MIB-II.



Veja ["Acesse os arquivos MIB"](#) se você deseja baixar os arquivos MIB nos nós da sua grid.

Inicialmente, o SNMP está desativado em todos os nós. Quando você configura o agente SNMP, todos os nós do StorageGRID recebem a mesma configuração.

O agente SNMP do StorageGRID suporta todas as três versões do protocolo SNMP. Ele fornece acesso MIB somente leitura para consultas e pode enviar dois tipos de notificações orientadas a eventos para um sistema de gerenciamento:

Armadilhas

Traps são notificações enviadas pelo agente SNMP que não exigem confirmação do sistema de gerenciamento. Traps servem para notificar o sistema de gerenciamento de que algo aconteceu no StorageGRID, como o acionamento de um alerta.

Traps são suportados em todas as três versões do SNMP.

Informa

Os informs são semelhantes aos traps, mas exigem confirmação do sistema de gerenciamento. Se o agente SNMP não receber uma confirmação dentro de um determinado período de tempo, ele reenviará o inform até que uma confirmação seja recebida ou o valor máximo de tentativas seja atingido.

Informs são suportados em SNMPv2c e SNMPv3.

As notificações de trap e inform são enviadas nos seguintes casos:

- Um alerta padrão ou personalizado é acionado em qualquer nível de severidade. Para suprimir as notificações SNMP de um alerta, você deve ["configurar um silêncio"](#) para o alerta. As notificações de alerta são enviadas pelo ["Nó de administração remetente preferencial"](#).

Cada alerta é mapeado para um dos três tipos de trap com base no nível de gravidade do alerta: activeMinorAlert, activeMajorAlert e activeCriticalAlert. Para obter uma lista dos alertas que podem acionar esses traps, consulte o ["Referência de alertas"](#).

Suporte à versão SNMP

A tabela fornece um resumo de alto nível do que é suportado para cada versão do SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Consultas (GET e GETNEXT)	Consultas MIB somente leitura	Consultas MIB somente leitura	Consultas MIB somente leitura
Autenticação de consulta	String comunitária	String comunitária	Usuário do Modelo de Segurança Baseado no Usuário (USM)
Notificações (TRAP e INFORM)	Apenas traps	Traps e informa	Traps e informa
Autenticação de notificação	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Comunidade de trap padrão ou uma string de comunidade personalizada para cada destino de trap	Usuário USM para cada destino de trap

Limitações

- StorageGRID suporta acesso MIB somente leitura. Acesso de leitura e gravação não é suportado.
- Todos os nós da grade recebem a mesma configuração.
- SNMPv3: StorageGRID não suporta o Modo de Suporte de Transporte (TSM).
- SNMPv3: o único protocolo de autenticação suportado é o SHA (HMAC-SHA-96).
- SNMPv3: o único protocolo de privacidade suportado é o AES.

Configure o agente SNMP no StorageGRID

Você pode configurar o agente SNMP do StorageGRID para usar um sistema de gerenciamento SNMP de terceiro para acesso somente leitura ao MIB e notificações.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Sobre esta tarefa

O agente SNMP do StorageGRID é compatível com SNMPv1, SNMPv2c e SNMPv3. Você pode configurar o agente para uma ou mais versões. Para SNMPv3, somente a autenticação User Security Model (USM) é suportada.

Todos os nós da grade utilizam a mesma configuração SNMP.

Especifique a configuração básica

Como primeiro passo, habilite o agente StorageGRID SNMP e forneça informações básicas.

Passos

1. Selecione **Configuração > Monitoramento > Agente SNMP**.

A página do agente SNMP é exibida.

2. Para ativar o agente SNMP em todos os nós da grid, selecione a caixa de seleção **Enable SNMP**.
3. Insira as seguintes informações na seção de configuração básica.

Campo	Descrição
Contato do sistema	Opcional. O contato principal para o sistema StorageGRID, que é retornado em mensagens SNMP como sysContact. O contato do sistema é normalmente um endereço de e-mail. Esse valor se aplica a todos os nós do sistema StorageGRID. O contato do sistema pode ter no máximo 255 caracteres.
Localização do sistema	Opcional. A localização do sistema StorageGRID, que é retornada nas mensagens SNMP como sysLocation. A localização do sistema pode ser qualquer informação útil para identificar onde seu sistema StorageGRID está localizado. Por exemplo, você pode usar o endereço da rua de uma instalação. Esse valor se aplica a todos os nós do sistema StorageGRID. Localização do sistema pode ter no máximo 255 caracteres.
Ativar notificações do agente SNMP	• Se selecionado, o agente SNMP do StorageGRID envia notificações de trap e inform. • Caso não seja selecionada, o agente SNMP permite acesso somente leitura ao MIB, mas não envia notificações SNMP.
Habilitar armadilhas de autenticação	Se selecionado, o agente SNMP do StorageGRID envia traps de autenticação se receber mensagens de protocolo com autenticação incorreta.

Insira as strings da comunidade

Se você utiliza SNMPv1 ou SNMPv2c, preencha a seção "Cadeias de comunidade".

Quando o sistema de gerenciamento consulta o StorageGRID MIB, ele envia uma string de comunidade. Se a string de comunidade corresponder a um dos valores especificados aqui, o agente SNMP envia uma resposta para o sistema de gerenciamento.

Passos

1. Para **Comunidade somente leitura**, opcionalmente insira uma string de comunidade para permitir acesso MIB somente leitura em endereços de agente IPv4 e IPv6.



Para garantir a segurança do seu sistema StorageGRID, não utilize "public" como string de comunidade. Se você deixar este campo em branco, o agente SNMP usará o ID da grade do seu sistema StorageGRID como string de comunidade.

Cada sequência de comunidade pode ter no máximo 32 caracteres e não pode conter caracteres de espaço em branco.

2. Selecione **Adicionar outra string de comunidade** para adicionar strings adicionais.

São permitidas até cinco strings.

Criar destinos de trap

Use a guia Destinos de trap na seção Outras configurações para definir um ou mais destinos para notificações de trap ou inform do StorageGRID. Quando você habilita o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando alertas são acionados. Notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifDown e coldStart).

Passos

1. No campo **Comunidade de traps padrão**, insira opcionalmente a string de comunidade padrão que você deseja usar para destinos de traps SNMPv1 ou SNMPv2.

Conforme necessário, você pode fornecer uma string de comunidade diferente ("personalizada") ao definir um destino de trap específico.

Comunidade trap padrão pode ter no máximo 32 caracteres e não pode conter caracteres de espaço em branco.

2. Para adicionar um destino de trap, selecione **Criar**.
3. Selecione qual versão do SNMP será usada para este destino de trap.
4. Preencha o formulário Criar destino de armadilha para a versão que você selecionou.

SNMPv1

Se você selecionou SNMPv1 como a versão, preencha estes campos.

Campo	Descrição
Tipo	Deve ser Trap para SNMPv1.
Host	Um endereço IPv4 ou IPv6 ou um nome de domínio totalmente qualificado (FQDN) para receber o trap.
Porta	Use 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo padrão de trap SNMP, a menos que você precise usar TCP.
String comunitária	Use a comunidade de captura padrão, se uma tiver sido especificada, ou insira uma string de comunidade personalizada para este destino de captura. A string de comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços em branco.

SNMPv2c

Se você selecionou SNMPv2c como a versão, preencha estes campos.

Campo	Descrição
Tipo	Se o destino será usado para traps ou informs.
Host	Um endereço IPv4 ou IPv6 ou FQDN para receber o trap.
Porta	Use a porta 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo padrão de trap SNMP, a menos que você precise usar TCP.
String comunitária	Use a comunidade de captura padrão, se uma tiver sido especificada, ou insira uma string de comunidade personalizada para este destino de captura. A string de comunidade personalizada pode ter no máximo 32 caracteres e não pode conter espaços em branco.

SNMPv3

Se você selecionou SNMPv3 como a versão, preencha estes campos.

Campo	Descrição
Tipo	Se o destino será usado para traps ou informs.
Host	Um endereço IPv4 ou IPv6 ou FQDN para receber o trap.
Porta	Use a porta 162, que é a porta padrão para traps SNMP, a menos que você precise usar outro valor.
Protocolo	Use UDP, que é o protocolo padrão de trap SNMP, a menos que você precise usar TCP.
Usuário USM	O usuário USM que será usado para autenticação. • Se você selecionou Trap, somente os usuários do USM sem IDs de mecanismo autorizados serão exibidos. • Se você selecionou Inform, somente os usuários do USM com IDs de mecanismo autorizados são exibidos. • Se nenhum usuário for exibido: i. Crie e salve o destino do trap. ii. Acesse Criar usuários USM e crie o usuário. iii. Retorne à aba Destinos da armadilha, selecione o destino salvo na tabela e selecione Editar. iv. Selecione o usuário.

5. Selecione **Create**.

O destino de trap é criado e adicionado à tabela.

Criar endereços de agente

Opcionalmente, use a guia Endereços do agente na seção Outras configurações para especificar um ou mais "endereços de escuta". Esses são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

Se você não configurar um endereço de agente, o endereço de escuta padrão será a porta UDP 161 em todas as redes StorageGRID.

Passos

1. Selecione **Create**.
2. Insira as seguintes informações.

Campo	Descrição
Protocolo de Internet	Se este endereço usará IPv4 ou IPv6. Por padrão, o SNMP usa IPv4.
Protocolo de transporte	Se este endereço usará UDP ou TCP. Por padrão, o SNMP usa UDP.
Rede StorageGRID	Em qual rede StorageGRID o agente ficará escutando. • Redes Grid, Admin e Client: o agente SNMP ficará à escuta de consultas em todas as três redes. • Rede de grid • Rede de administração • Rede de cliente Nota: Se você usar a Rede do Cliente para dados não seguros e criar um endereço de agente para a Rede do Cliente, esteja ciente de que o tráfego SNMP também será inseguro.
Porta	Opcionalmente, o número da porta em que o agente SNMP deve escutar. A porta UDP padrão para um agente SNMP é 161, mas você pode inserir qualquer número de porta não utilizado. Nota: Ao salvar o agente SNMP, StorageGRID abre automaticamente as portas de endereço do agente no firewall interno. Você deve garantir que quaisquer firewalls externos permitam o acesso a essas portas.

3. Selecione **Create**.

O endereço do agente é criado e adicionado à tabela.

Criar usuários USM

Se você estiver usando o SNMPv3, utilize a guia "Usuários USM" na seção "Outras configurações" para definir os usuários USM autorizados a consultar o MIB ou a receber traps e informs.



Para destinos SNMPv3 *trap*, recomenda-se que você crie um usuário USM para cada Admin Node. Se cada Admin Node não tiver um usuário USM, seu sistema de gerenciamento pode parar de receber notificações se o Admin Node primário ficar inativo.



Os destinos SNMPv3 *inform* devem ter usuários com IDs de mecanismo. Destinos SNMPv3 *trap* não podem ter usuários com IDs de mecanismo.

Essas etapas não se aplicam se você estiver usando apenas SNMPv1 ou SNMPv2c.

Passos

1. Selecione **Create**.
2. Insira as seguintes informações.

Campo	Descrição
Nome de usuário	Um nome único para este usuário do USM. Os nomes de usuário podem ter no máximo 32 caracteres e não podem conter caracteres de espaço em branco. O nome de usuário não pode ser alterado após o usuário ser criado.
Acesso MIB somente leitura	Se selecionado, este usuário deve ter acesso somente leitura ao MIB.
ID do mecanismo autorizado	Se este usuário for usado em um destino inform, o ID do mecanismo autorizado para este usuário. Insira de 10 a 64 caracteres hexadecimais (5 a 32 bytes) sem espaços. Este valor é obrigatório para usuários USM que serão selecionados em destinos de trap para informs. Este valor não é permitido para usuários USM que serão selecionados em destinos de trap para traps. Observação: Este campo não é exibido se você selecionou Acesso somente leitura ao MIB, pois os usuários do USM com acesso somente leitura ao MIB não podem ter engine IDs.
Nível de segurança	O nível de segurança para o usuário USM: • authPriv: Este usuário se comunica com autenticação e privacidade (criptografia). Você deve especificar um protocolo de autenticação e senha e um protocolo de privacidade e senha. • authNoPriv: Este usuário se comunica com autenticação e sem privacidade (sem criptografia). Você deve especificar um protocolo de autenticação e uma senha.
Protocolo de autenticação	Sempre configurado para SHA, que é o único protocolo suportado (HMAC-SHA-96).
Senha	A senha que este usuário usará para autenticação.
Protocolo de privacidade	Exibido somente se você selecionou authPriv e sempre definido como AES, que é o único protocolo de privacidade compatível.
Senha	Exibido somente se você selecionou authPriv. A senha que este usuário usará para privacidade.

3. Selecione **Create**.

O usuário USM é criado e adicionado à tabela.

4. Após concluir a configuração do agente SNMP, selecione **Save**.

A nova configuração do agente SNMP entra em vigor.

Atualize o agente SNMP do StorageGRID

Você pode desativar as notificações SNMP, atualizar as strings da comunidade ou adicionar ou remover endereços de agentes, usuários USM e destinos de trap.

Antes de começar

- Você está conectado ao Gerenciador de Grade usando um ["navegador web compatível"](#).
- Você tem o ["Permissão de acesso root"](#).

Sobre esta tarefa

Consulte ["Configurar o agente SNMP"](#) para obter detalhes sobre cada campo na página do agente SNMP. Você deve selecionar **Salvar** na parte inferior da página para confirmar as alterações feitas em cada guia.

Passos

1. Selecione **Configuração > Monitoramento > Agente SNMP**.

A página do agente SNMP é exibida.

2. Para desativar o agente SNMP em todos os nós da grade, desmarque a caixa de seleção **Enable SNMP** e selecione **Salvar**.

Se você reativar o agente SNMP, todas as configurações SNMP anteriores serão mantidas.

3. Opcionalmente, atualize as informações na seção configuração básica:

- a. Conforme necessário, atualize o **contato do sistema** e a **localização do sistema**.
- b. Opcionalmente, selecione ou desmarque a caixa de seleção **Ativar notificações do agente SNMP** para controlar se o agente SNMP do StorageGRID envia notificações de trap e inform.

Quando esta caixa de seleção está desmarcada, o agente SNMP suporta acesso MIB somente leitura, mas não envia notificações SNMP.

- c. Opcionalmente, selecione ou desmarque a caixa de seleção **Ativar traps de autenticação** para controlar se o agente SNMP do StorageGRID envia traps de autenticação quando recebe mensagens de protocolo autenticadas incorretamente.
4. Se você usa SNMPv1 ou SNMPv2c, opcionalmente atualize ou adicione uma **Comunidade somente leitura** na seção Cadeias de comunidade.
 5. Para atualizar os destinos das armadilhas, selecione a guia Destinos das armadilhas na seção Outras configurações.

Use esta aba para definir um ou mais destinos para notificações de trap ou inform do StorageGRID. Quando você habilita o agente SNMP e seleciona **Salvar**, o StorageGRID envia notificações para cada destino definido quando alertas são acionados. Notificações padrão também são enviadas para as entidades MIB-II suportadas (por exemplo, ifDown e coldStart).

Para obter detalhes sobre o que inserir, consulte ["Criar destinos de trap"](#).

- Opcionalmente, atualize ou remova a comunidade de trap padrão.

Se você remover a comunidade de trap padrão, primeiro deverá garantir que todos os destinos de trap existentes usem uma string de comunidade personalizada.

- Para adicionar um destino de trap, selecione **Criar**.
- Para editar um destino de trap, selecione o botão de opção e selecione **Editar**.
- Para remover um destino de trap, selecione o botão de opção e selecione **Remover**.
- Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

6. Para atualizar os endereços dos agentes, selecione a guia Endereços dos agentes na seção Outras configurações.

Use esta aba para especificar um ou mais "endereços de escuta". Estes são os endereços StorageGRID nos quais o agente SNMP pode receber consultas.

Para obter detalhes sobre o que inserir, consulte "[Criar endereços de agente](#)".

- Para adicionar um endereço de agente, selecione **Criar**.
- Para editar o endereço de um agente, selecione o botão de opção e selecione **Editar**.
- Para remover o endereço de um agente, selecione o botão de opção e selecione **Remover**.
- Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

7. Para atualizar os usuários do USM, selecione a guia "Usuários do USM" na seção "Outras configurações".

Use esta aba para definir os usuários do USM que estão autorizados a consultar o MIB ou a receber traps e informs.

Para obter detalhes sobre o que inserir, consulte "[Criar usuários USM](#)".

- Para adicionar um usuário USM, selecione **Criar**.
- Para editar um usuário do USM, selecione o botão de opção e selecione **Editar**.

O nome de usuário de um usuário USM existente não pode ser alterado. Se você precisar alterar um nome de usuário, deve remover o usuário e criar um novo.



Se você adicionar ou remover o ID do mecanismo autorizado de um usuário e esse usuário estiver selecionado para um destino, você deve editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

- Para remover um usuário do USM, selecione o botão de opção e selecione **Remover**.



Se o usuário que você removeu estiver selecionado para um destino de trap, você deve editar ou remover o destino. Caso contrário, ocorrerá um erro de validação ao salvar a configuração do agente SNMP.

- Para confirmar suas alterações, selecione **Salvar** na parte inferior da página.

8. Quando você atualizar a configuração do agente SNMP, selecione **Salvar**.

Acesse os arquivos MIB do StorageGRID

Os arquivos MIB contêm definições e informações sobre as propriedades dos recursos e serviços gerenciados para os nós da sua grid. Você pode acessar os arquivos MIB que definem os objetos e notificações para StorageGRID. Esses arquivos podem ser úteis para monitorar sua grid.

Consulte ["Use o monitoramento SNMP"](#) para obter mais informações sobre SNMP e arquivos MIB.

Acesse os arquivos MIB

Siga estes passos para acessar os arquivos MIB.

Passos

1. Selecione **Configuração > Monitoramento > Agente SNMP**.
2. Na página do agente SNMP, selecione o arquivo que você deseja baixar:
 - **NETAPP-STORAGEGRID-MIB.txt**: Define a tabela de alertas e notificações (traps) acessíveis em todos os Admin Nodes.
 - **ES-NETAPP-06-MIB.mib**: Define objetos e notificações para appliances baseados em E-Series.
 - **MIB_1_10.zip**: Define objetos e notificações para dispositivos com interface BMC.



Você também pode acessar os arquivos MIB no seguinte local em qualquer nó do StorageGRID: `/usr/share/snmp/mibs`

3. Para extrair os OIDs do StorageGRID do arquivo MIB:

- a. Obtenha o OID da raiz do StorageGRID MIB:

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Resultado: `.1.3.6.1.4.1.789.28669` (28669 é sempre o OID para StorageGRID)

- b. Procure o OID do StorageGRID em toda a árvore (usando `paste` para unir linhas):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



O ``snmptranslate`` comando possui diversas opções úteis para explorar o MIB. Este comando está disponível em qualquer nó do StorageGRID.

Conteúdo do arquivo MIB

Todos os objetos estão sob o OID do StorageGRID.

Nome do objeto	ID do objeto (OID)	Descrição
		O módulo MIB para entidades NetApp StorageGRID.

Objetos MIB

Nome do objeto	ID do objeto (OID)	Tipo	Acesso	Módulo MIB	Descrição
activeAlertCount		Integer32	Somente leitura	NETAPP-STORAGEGRID-MIB	O número de alertas ativos na activeAlertTable.
activeAlertTable		Sequência de ActiveAlertEntry	Não acessível	NETAPP-STORAGEGRID-MIB	Uma tabela de alertas ativos no StorageGRID.
activeAlertEntry		Sequência	Não acessível	NETAPP-STORAGEGRID-MIB	Um único alerta do StorageGRID, indexado pelo ID do alerta.
activeAlertId		String de octeto	Somente leitura	NETAPP-STORAGEGRID-MIB	O ID do alerta. Apenas exclusivo no conjunto atual de alertas ativos.
activeAlertName		String de octeto	Somente leitura	NETAPP-STORAGEGRID-MIB	O nome do alerta.
activeAlertInstance		String de octeto	Somente leitura	NETAPP-STORAGEGRID-MIB	O nome da entidade que gerou o alerta, normalmente o nome do nó.
activeAlertSeverity		String de octeto	Somente leitura	NETAPP-STORAGEGRID-MIB	A gravidade do alerta.
activeAlertStartTime		Data e hora	Somente leitura	NETAPP-STORAGEGRID-MIB	O horário em que o alerta foi acionado.

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.