Gerenciar serviços da Web

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/pt-br/ontap/system-admin/manage-web-services-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Índice

Gerenciar serviços da Web

Gerencie a visão geral dos serviços da Web

Você pode ativar ou desativar um serviço da Web para o cluster ou uma máquina virtual de armazenamento (SVM), exibir as configurações de serviços da Web e controlar se os usuários de uma função podem acessar um serviço da Web.

Você pode gerenciar os serviços da Web para o cluster ou uma SVM das seguintes maneiras:

- Ativar ou desativar um serviço Web específico
- Especificar se o acesso a um serviço da Web é restrito apenas a HTTP encriptado (SSL)
- Exibindo a disponibilidade de serviços da Web
- Permitir ou não permitir que usuários de uma função acessem um serviço da Web
- Exibindo as funções que têm permissão para acessar um serviço da Web

Para que um usuário acesse um serviço da Web, todas as seguintes condições devem ser atendidas:

- O usuário deve ser autenticado.

  Por exemplo, um serviço da Web pode solicitar um nome de usuário e uma senha. A resposta do usuário deve corresponder a uma conta válida.

- O utilizador tem de ser configurado com o método de acesso correto.

  A autenticação só é bem-sucedida para os usuários com o método de acesso correto para o serviço web fornecido. Para o serviço Web da API ONTAP (`ontapi`), os usuários devem ter o `ontapi` método de acesso. Para todos os outros serviços da Web, os usuários devem ter o `http` método de acesso.

  > Você usa os `security login` comandos para gerenciar os métodos de acesso e os métodos de autenticação dos usuários.

- O serviço Web deve ser configurado para permitir a função de controle de acesso do usuário.

  > Você usa os `vserver services web access` comandos para controlar o acesso de uma função a um serviço da Web.

Se um firewall estiver ativado, a política de firewall para o LIF a ser usado para serviços da Web deve ser configurada para permitir HTTP ou HTTPS.

Se você usar HTTPS para acesso ao serviço da Web, o SSL para o cluster ou SVM que ofereça o serviço da Web também deverá estar habilitado e fornecer um certificado digital para o cluster ou SVM.

Gerenciar o acesso aos serviços web do ONTAP

Um serviço da Web é um aplicativo que os usuários podem acessar usando HTTP ou HTTPS. O administrador do cluster pode configurar o mecanismo de protocolo da Web, configurar SSL, ativar um serviço da Web e permitir que os utilizadores de uma função

acedam a um serviço da Web.

A partir do ONTAP 9.6, são suportados os seguintes serviços Web:

- Infraestrutura do processador de serviço (`spi`)

  Esse serviço torna os arquivos de log, despejo de núcleo e MIB de um nó disponíveis para acesso HTTP ou HTTPS por meio do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó. A predefinição é `enabled`.

  Após uma solicitação de acesso aos arquivos de log ou arquivos de despejo de núcleo de um nó, o `spi` O serviço web cria automaticamente um ponto de montagem de um nó para o volume raiz de outro nó, onde os arquivos residem. Você não precisa criar o ponto de montagem manualmente.

- APIs do ONTAP (`ontapi`)

  Este serviço permite executar APIs do ONTAP para executar funções administrativas com um programa remoto. A predefinição é `enabled`.

  Este serviço pode ser necessário para algumas ferramentas de gerenciamento externas. Por exemplo, se você usar o System Manager, você deve deixar esse serviço habilitado.

- Descoberta do Data ONTAP (`disco`)

  Este serviço permite que os aplicativos de gerenciamento off-box descubram o cluster na rede. A predefinição é `enabled`.

- Diagnóstico de suporte (`supdiag`)

  Este serviço controla o acesso a um ambiente privilegiado no sistema para auxiliar na análise e resolução de problemas. A predefinição é `disabled`. Você deve habilitar este serviço somente quando direcionado pelo suporte técnico.

- System (`sysmgr`Manager)

  Esse serviço controla a disponibilidade do Gerenciador de sistema, que está incluído no ONTAP. A predefinição é `enabled`. Este serviço é suportado apenas no cluster.

- Atualização do controlador de gerenciamento de placa base (BMC) de firmware (`FW_BMC`)

  Este serviço permite-lhe transferir ficheiros de firmware do BMC. A predefinição é `enabled`.

- Documentação do ONTAP (`docs`)

  Este serviço fornece acesso à documentação do ONTAP. A predefinição é `enabled`.

- APIs RESTful do ONTAP (`docs_api`)

  Este serviço fornece acesso à documentação da API RESTful do ONTAP. A predefinição é `enabled`.

- Carregar e transferir ficheiros (`fud`)

  Este serviço oferece upload e download de arquivos. A predefinição é `enabled`.

- Mensagens do ONTAP (`ontapmsg`)

  Este serviço suporta uma interface de publicação e assinatura, permitindo que você se inscreva em eventos. A predefinição é `enabled`.

- Portal do ONTAP (`portal`)

  Este serviço implementa o gateway em um servidor virtual. A predefinição é `enabled`.

- Interface ONTAP RESTful (`rest`)

  Esse serviço dá suporte a uma interface RESTful que é usada para gerenciar remotamente todos os elementos da infraestrutura do cluster. A predefinição é `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

  Este serviço fornece recursos para dar suporte ao provedor de serviços SAML. A predefinição é `enabled`.

- Fornecedor de serviços SAML (`saml-sp`)

  Esse serviço oferece serviços como metadados SP e o serviço de asserção ao consumidor para o provedor de serviços. A predefinição é `enabled`.

A partir do ONTAP 9.7, são suportados os seguintes serviços adicionais:

- Arquivos de backup de (`backups`configuração)

  Este serviço permite-lhe transferir ficheiros de cópia de segurança de configuração. A predefinição é `enabled`.

- Segurança do ONTAP (`security`)

  Este serviço suporta o gerenciamento de token CSRF para autenticação aprimorada. A predefinição é `enabled`.

Gerencie o mecanismo de protocolo da Web no ONTAP

Você pode configurar o mecanismo de protocolo da Web no cluster para controlar se o acesso à Web é permitido e quais versões SSL podem ser usadas. Também pode apresentar as definições de configuração do motor de protocolo Web.

Você pode gerenciar o mecanismo de protocolo da Web no nível do cluster das seguintes maneiras:

- Você pode especificar se os clientes remotos podem usar HTTP ou HTTPS para acessar o conteúdo do serviço da Web usando o `system services web modify` comando com o `-external` parâmetro.
- Você pode especificar se SSLv3 deve ser usado para acesso seguro à Web usando o `security config modify` comando com o `-supported-protocol` parâmetro. Por padrão, o SSLv3 está desativado. Transport Layer Security 1,0 (TLSv1,0) está ativado e pode ser desativado se necessário.

  Saiba mais sobre `security config modify` o "Referência do comando ONTAP"na .

- Você pode ativar o modo de conformidade FIPS (Federal Information Processing Standard) 140-2 para interfaces de serviço da Web do plano de controle em todo o cluster.

  Por padrão, o modo de conformidade com o FIPS 140-2 está desativado.

  - **Quando o modo de conformidade com o FIPS 140-2 estiver desativado**, é possível ativar o modo de conformidade com o FIPS 140-2 definindo o `is-fips-enabled` parâmetro como `true` para `security config modify` o comando e, em seguida, usando o `security config show` comando para confirmar o status on-line.
  - **Quando o modo de conformidade com o FIPS 140-2 estiver ativado**
    - A partir do ONTAP 9.11.1, TLSv1, TLSv1,1 e SSLv3 estão desativados e apenas TSLv1,2 e TSLv1,3 permanecem ativados. Afeta outros sistemas e comunicações que são internos e externos ao ONTAP 9. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativar, TLSv1, TLSv1,1 e SSLv3 permanecerão desativados. O TLSv1,2 ou o TLSv1,3 permanecerão ativados dependendo da configuração anterior.
    - Para versões do ONTAP anteriores a 9.11.1, tanto o TLSv1 como o SSLv3 estão desativados e apenas o TLSv1,1 e o TLSv1,2 permanecem ativados. O ONTAP impede que você ative o TLSv1 e o SSLv3 quando o modo de conformidade FIPS 140-2 estiver ativado. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativá-lo, o TLSv1 e o SSLv3 permanecerão desativados, mas o TLSv1,2 ou o TLSv1,1 e o TLSv1,2 serão ativados dependendo da configuração anterior.
- Você pode exibir a configuração de segurança em todo o cluster usando o `system security config show` comando.

  Saiba mais sobre `security config show` o "Referência do comando ONTAP"na .

Se o firewall estiver ativado, a política de firewall para a interface lógica (LIF) a ser usada para serviços da Web deve ser configurada para permitir o acesso HTTP ou HTTPS.

Se você usar HTTPS para acesso ao serviço da Web, o SSL para o cluster ou a máquina virtual de armazenamento (SVM) que ofereça o serviço da Web também deverá estar habilitado e fornecer um certificado digital para o cluster ou SVM.

Nas configurações do MetroCluster, as alterações de configuração feitas para o mecanismo de protocolo da Web em um cluster não são replicadas no cluster de parceiros.

Comandos ONTAP para gerenciar o mecanismo de protocolo da web

Você usa os `system services web` comandos para gerenciar o mecanismo de protocolo da Web. Use os `system services firewall policy create` comandos e `network interface modify` para permitir que as solicitações de acesso à Web passem pelo firewall.

Se você quiser…	Use este comando…
Configure o mecanismo de protocolo da Web no nível do cluster: • Ative ou desative o mecanismo de protocolo da Web para o cluster • Ative ou desative o SSLv3 para o cluster • Ativar ou desativar a conformidade com o FIPS 140-2 para serviços Web seguros (HTTPS)	`system services web modify`
Exibir a configuração do mecanismo de protocolo da Web no nível do cluster, determinar se os protocolos da Web estão funcionais em todo o cluster e exibir se a conformidade com o FIPS 140-2 está ativada e on-line	`system services web show`
Exibir a configuração do mecanismo de protocolo da Web no nível do nó e a atividade de manipulação de serviços da Web para os nós no cluster	`system services web node show`
Crie uma política de firewall ou adicione um serviço de protocolo HTTP ou HTTPS a uma política de firewall existente para permitir que as solicitações de acesso à Web passem pelo firewall	`system services firewall policy create` Definir o `-service` parâmetro para `http` ou `https` permite que as solicitações de acesso à Web passem pelo firewall.
Associar uma política de firewall a um LIF	`network interface modify` Você pode usar o `-firewall-policy` parâmetro para modificar a política de firewall de um LIF.

Informações relacionadas

- "modificação da interface de rede"

Configurar acesso aos serviços web ONTAP

A configuração do acesso a serviços da Web permite que usuários autorizados usem HTTP ou HTTPS para acessar o conteúdo do serviço no cluster ou em uma máquina virtual de armazenamento (SVM).

Passos

1. Se um firewall estiver ativado, verifique se o acesso HTTP ou HTTPS está configurado na política de firewall para o LIF que será usado para serviços da Web:

   Você pode verificar se um firewall está habilitado usando o `system services firewall show` comando.

a. Para verificar se HTTP ou HTTPS está configurado na política de firewall, use o `system services firewall policy show` comando.

   Você define o `-service` parâmetro `system services firewall policy create` do comando para `http` ou `https` para ativar a diretiva para oferecer suporte ao acesso à Web.

b. Para verificar se a política de firewall que suporta HTTP ou HTTPS está associada ao LIF que fornece serviços da Web, use o `network interface show` comando com o `-firewall-policy` parâmetro.

   Saiba mais sobre `network interface show` o "Referência do comando ONTAP"na .

   Você usa o `network interface modify` comando com o `-firewall-policy` parâmetro para colocar a política de firewall em vigor para um LIF.

Saiba mais sobre `network interface modify` o "Referência do comando ONTAP"na .

2. Para configurar o mecanismo de protocolo da Web em nível de cluster e tornar o conteúdo do serviço da Web acessível, use o `system services web modify` comando.
3. Se você planeja usar serviços da Web seguros (HTTPS), ative o SSL e forneça informações de certificado digital para o cluster ou SVM usando o `security ssl modify` comando.

   Saiba mais sobre `security ssl modify` o "Referência do comando ONTAP"na .

4. Para ativar um serviço da Web para o cluster ou SVM, use o `vserver services web modify` comando.

   Repita essa etapa para cada serviço que você deseja habilitar para o cluster ou SVM.

5. Para autorizar uma função a acessar serviços da Web no cluster ou SVM, use o `vserver services web access create` comando.

   A função que você concede acesso já deve existir. Você pode exibir funções existentes usando o `security login role show` comando ou criar novas funções usando o `security login role create` comando.

   Saiba mais sobre `security login role show` e `security login role create` no "Referência do comando ONTAP".

6. Para uma função que tenha sido autorizada a acessar um serviço da Web, verifique se seus usuários também estão configurados com o método de acesso correto, verificando a saída do `security login show` comando.

   Para acessar o serviço Web da API ONTAP `ontapi`), um usuário deve ser configurado com o `ontapi` método de acesso. Para acessar todos os outros serviços da Web, um usuário deve ser configurado com o `http` método de acesso.

   Saiba mais sobre `security login show` o "Referência do comando ONTAP"na .

   Use o `security login create` comando para adicionar um método de acesso a um usuário. Saiba mais sobre `security login create` o "Referência do comando ONTAP"na .

Comandos ONTAP para gerenciamento de serviços web

Use os `vserver services web` comandos para gerenciar a disponibilidade de serviços da Web para o cluster ou uma máquina virtual de storage (SVM). Você usa os `vserver services web access` comandos para controlar o acesso de uma função a um serviço da Web.

Se você quiser…	Use este comando…
Configurar um serviço da Web para o cluster ou anSVM: • Ativar ou desativar um serviço Web • Especifique se apenas o HTTPS pode ser usado para acessar um serviço da Web	`vserver services web modify`
Exibir a configuração e a disponibilidade dos serviços da Web para o cluster ou anSVM	`vserver services web show`
Autorizar uma função a acessar um serviço da Web no cluster ou na anSVM	`vserver services web access create`
Exibir as funções autorizadas a acessar serviços da Web no cluster ou no anSVM	`vserver services web access show`
Impedir que uma função acesse um serviço da Web no cluster ou na anSVM	`vserver services web access delete`

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerenciar pontos de montagem em nós ONTAP

O `spi` serviço da Web cria automaticamente um ponto de montagem de um nó para o volume raiz de outro nó, mediante uma solicitação para acessar os arquivos de log ou arquivos centrais do nó. Embora você não precise gerenciar manualmente pontos de montagem, você pode fazê-lo usando os `system node root-mount` comandos.

Se você quiser…	Use este comando…
Crie manualmente um ponto de montagem de um nó para o volume raiz de outro nó	`system node root-mount create` Apenas um único ponto de montagem pode existir de um nó para outro.

Se você quiser…	Use este comando…
Exiba pontos de montagem existentes nos nós do cluster, incluindo o tempo em que um ponto de montagem foi criado e seu estado atual	`system node root-mount show`
Exclua um ponto de montagem de um nó para o volume raiz de outro nó e force as conexões ao ponto de montagem para fechar	`system node root-mount delete`

Informações relacionadas

"Referência do comando ONTAP"

Gerenciar SSL no ONTAP

Use os `security ssl` comandos para gerenciar o protocolo SSL para o cluster ou uma máquina virtual de armazenamento (SVM). O protocolo SSL melhora a segurança do acesso à Web usando um certificado digital para estabelecer uma conexão criptografada entre um servidor da Web e um navegador.

Você pode gerenciar SSL para o cluster ou uma máquina virtual de armazenamento (SVM) das seguintes maneiras:

- Ativar SSL
- Gerar e instalar um certificado digital e associá-lo ao cluster ou SVM
- Exibindo a configuração SSL para ver se o SSL foi ativado e, se disponível, o nome do certificado SSL
- Configuração de políticas de firewall para o cluster ou SVM, para que as solicitações de acesso à Web possam passar
- Definir quais versões SSL podem ser usadas
- Restringindo o acesso apenas a solicitações HTTPS para um serviço da Web

Comandos para gerenciar SSL

Use os `security ssl` comandos para gerenciar o protocolo SSL para o cluster ou uma máquina virtual de armazenamento (SVM).

Se você quiser…	Use este comando…
Ative o SSL para o cluster ou um SVM e associe um certificado digital a ele	`security ssl modify`
Exiba a configuração SSL e o nome do certificado para o cluster ou um SVM	`security ssl show`

Saiba mais sobre `security ssl modify` e `security ssl show` no "Referência do comando ONTAP".

Use HSTS para serviços web ONTAP

HTTP Strict Transport Security (HSTS) é um mecanismo de política de segurança web que ajuda a proteger sites contra ataques do tipo "man-in-the-middle", como ataques de downgrade de protocolo e sequestro de cookies. Ao impor o uso de HTTPS, o HSTS garante que todas as comunicações entre o navegador do usuário e o servidor sejam criptografadas. A partir do ONTAP 9.17.1, o ONTAP pode impor conexões HTTPS para serviços web ONTAP .

> O HSTS é aplicado pelo navegador somente após o estabelecimento de uma conexão HTTPS segura inicial com o ONTAP. Se o navegador não estabelecer uma conexão segura inicial, o HSTS não será aplicado. Consulte a documentação do seu navegador para obter informações sobre o gerenciamento de HSTS.

Sobre esta tarefa

- Para a versão 9.17.1 e versões superiores, o HSTS é habilitado por padrão para clusters ONTAP recém-instalados. Ao atualizar para a versão 9.17.1, o HSTS não é habilitado por padrão. Você deve habilitar o HSTS após a atualização.
- HSTS é compatível com todos "Serviços web ONTAP" .

Antes de começar

- Privilégios avançados são necessários para as seguintes tarefas.

Mostrar configuração HSTS

Você pode mostrar a configuração atual do HSTS para verificar se ela está habilitada e visualizar a configuração de idade máxima.

Passos

1. Use o `system services web show` comando para mostrar a configuração atual dos serviços web, incluindo configurações HSTS:

```
cluster-1::system services web*> show

                   External Web Services: true
                               HTTP Port: 80
                              HTTPS Port: 443
                         Protocol Status: online
                     Per Address Limit: 80
                    Wait Queue Capacity: 192
                           HTTP Enabled: true
                 CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                            HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

Habilite o HSTS e defina a idade máxima

A partir do ONTAP 9.17.1, o HSTS é habilitado por padrão no novo cluster ONTAP . Se você atualizar um cluster existente para a versão 9.17.1 ou posterior, precisará habilitar manualmente o HSTS no seu cluster para impor o uso de HTTPS. Você pode habilitar o HSTS e definir a idade máxima. Você pode alterar a idade máxima a qualquer momento se o HSTS estiver habilitado. Após a ativação do HSTS, os navegadores começarão a impor conexões seguras somente após o estabelecimento de uma conexão segura inicial.

Passos

1. Use o `system services web modify` comando para habilitar HSTS ou modificar a idade máxima:

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age` Especifica a duração, em segundos, durante a qual o navegador se lembrará de aplicar HTTPS. O valor padrão é 63072000 segundos (dois anos).

Desativar HSTS

Os navegadores salvam a configuração de idade máxima do HSTS a cada conexão e continuam a aplicar o HSTS durante todo o período, mesmo que o HSTS esteja desativado no ONTAP. Após a desativação, o navegador levará até o período máximo configurado para interromper a aplicação do HSTS. Se uma conexão segura se tornar impossível durante esse período, os navegadores que aplicam o HSTS não permitirão o acesso aos serviços web do ONTAP até que o problema seja resolvido ou a idade máxima do navegador expire.

Passos

1. Desabilite o HSTS usando o `system services web modify` comando:

```
system services web modify -hsts-enabled false
```

Informações relacionadas

"RFC 6797 - Segurança de Transporte Estrita HTTP (HSTS)"

Solucionar problemas de acesso ao serviço web ONTAP

Os erros de configuração causam problemas de acesso ao serviço da Web. Você pode resolver os erros garantindo que o LIF, a política de firewall, o mecanismo de protocolo da Web, os serviços da Web, os certificados digitais e a autorização de acesso do usuário estejam configurados corretamente.

A tabela a seguir ajuda a identificar e tratar erros de configuração do serviço da Web:

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
O navegador da Web retorna um `unable to connect` erro ou `failure to establish a connection` quando você tenta acessar um serviço da Web.	Seu LIF pode estar configurado incorretamente.	Certifique-se de que você pode fazer ping no LIF que fornece o serviço da Web. Você usa o `network ping` comando para fazer ping em um LIF.
O firewall pode estar configurado incorretamente.	Certifique-se de que uma política de firewall esteja configurada para suportar HTTP ou HTTPS e que a política esteja atribuída ao LIF que fornece o serviço da Web. Você usa os `system services firewall policy` comandos para gerenciar políticas de firewall. Você usa o `network interface modify` comando com o `-firewall-policy` parâmetro para associar uma política a um LIF.	Seu mecanismo de protocolo da Web pode estar desativado.

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
Certifique-se de que o mecanismo de protocolo da Web está ativado para que os serviços da Web estejam acessíveis. Você usa os `system services web` comandos para gerenciar o mecanismo de protocolo da Web para o cluster.	Seu navegador retorna um `not found` erro quando você tenta acessar um serviço da Web.	O serviço da Web pode estar desativado.
Certifique-se de que cada serviço Web ao qual você deseja permitir acesso esteja ativado individualmente. Você usa o `vserver services web modify` comando para habilitar um serviço da Web para acesso.	O navegador da Web não consegue fazer login em um serviço da Web com o nome de conta e a senha de um usuário.	O utilizador não pode ser autenticado, o método de acesso não está correto ou o utilizador não está autorizado a aceder ao serviço Web.

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
Certifique-se de que a conta de utilizador existe e está configurada com o método de acesso e o método de autenticação corretos. Além disso, certifique-se de que a função do utilizador está autorizada a aceder ao serviço Web. Você usa os `security login` comandos para gerenciar contas de usuário e seus métodos de acesso e métodos de autenticação. Acessar o serviço da Web da API do ONTAP requer o `ontapi` método de acesso. O acesso a todos os outros serviços da Web requer o `http` método de acesso. Você usa os `vserver services web access` comandos para gerenciar o acesso de uma função a um serviço da Web.	Você se coneta ao serviço da Web com HTTPS e o navegador da Web indica que sua conexão foi interrompida.	Talvez você não tenha o SSL ativado no cluster ou na máquina virtual de armazenamento (SVM) que fornece o serviço da Web.

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
Certifique-se de que o cluster ou SVM tenha SSL habilitado e que o certificado digital seja válido. Você usa os `security ssl` comandos para gerenciar a configuração SSL para servidores HTTP e o `security certificate show` comando para exibir informações de certificado digital.	Você se coneta ao serviço da Web com HTTPS e o navegador da Web indica que a conexão não é confiável.	Você pode estar usando um certificado digital autoassinado.

Informações relacionadas

- "Quais são as melhores práticas para configuração de rede para ONTAP?"
- "ping de rede"
- "modificação da interface de rede"
- "certificado de segurança generate-csr"
- "instalação do certificado de segurança"
- "certificado de segurança mostrar"
- "segurança ssl"

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 DESTE DOCUMENTO. 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 SOBRESSALENTES; 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 DESTE SOFTWARE, 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.