Proteja seus dados

ASA r2

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/pt-br/asa-r2/secure-data/encrypt-data-at-rest.html on February 11, 2026. Always check docs.netapp.com for the latest.

Índice

Proteja seus dados . . . 1
- Criptografia de dados em repouso em sistemas de storage ASA R2 . . . 1
- Migre chaves de criptografia de dados ONTAP entre gerenciadores de chaves no sistema ASA R2 . . . 2
  - Migre chaves entre os gerenciadores-chave no nível do cluster do ONTAP . . . 2
  - Migre chaves entre gerenciadores de chaves em cluster ONTAP e níveis de VM de armazenamento . . . 4
- Proteção contra ataques de ransomware . . . 4
  - Crie instantâneos à prova de violação para proteger contra ataques de ransomware em sistemas de armazenamento ASA r2 . . . 4
  - Habilite a proteção autônoma contra ransomware com IA em seus sistemas de armazenamento ASA r2 . . . 5
  - Desative a proteção autônoma padrão contra ransomware em seus sistemas de armazenamento ASA r2 . . . 7
  - Modificar períodos de retenção de snapshots ARP/AI em sistemas de armazenamento ASA r2 . . . 8
  - Responda à proteção autônoma contra ransomware com alertas de IA em sistemas de armazenamento ASA r2 . . . 9
  - Pause ou retome a proteção autônoma contra ransomware com IA em seus sistemas de armazenamento ASA r2 . . . 10
- Conexões NVMe seguras em seus sistemas de storage ASA R2 . . . 11
- Conexões IP seguras em seus sistemas de storage ASA R2 . . . 11

Proteja seus dados

Criptografia de dados em repouso em sistemas de storage ASA R2

Ao criptografar dados em repouso, não é possível ler se um meio de storage é reutilizado, devolvido, extraviado ou roubado. Você pode usar o Gerenciador de sistemas do ONTAP para criptografar seus dados em nível de hardware e software para proteção de camada dupla.

O NetApp Storage Encryption (NSE) é compatível com a criptografia de hardware usando unidades de autocriptografia (SEDs). Os SEDs criptografam dados conforme são gravados. Cada SED contém uma chave de criptografia exclusiva. Os dados criptografados armazenados no SED não podem ser lidos sem a chave de criptografia do SED. Os nós que tentam ler de um SED devem ser autenticados para acessar a chave de criptografia do SED. Os nós são autenticados pela obtenção de uma chave de autenticação de um gerenciador de chaves e, em seguida, apresentando a chave de autenticação à SED. Se a chave de autenticação for válida, o SED dará ao nó a sua chave de encriptação para aceder aos dados que contém.

Nos sistemas ASA r2, os SEDs são suportados apenas para SSDs baseados em NVMe.

Use o gerenciador de chaves integrado do ASA R2 ou um gerenciador de chaves externo para fornecer chaves de autenticação aos nós.

Além do NSE, você também pode habilitar a criptografia de software para adicionar outra camada de segurança aos seus dados.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, em **criptografia**, selecione **Configurar**.
3. Configure o gerenciador de chaves.

Opção	Passos
Configure o Onboard Key Manager	a. Selecione **Onboard Key Manager** para adicionar os servidores de chave. b. Introduza uma frase-passe.
Configurar um gerenciador de chaves externo	a. Selecione **Gerenciador de chaves externo** para adicionar os servidores de chaves. b. + Add Selecione para adicionar os servidores de chaves. c. Adicione os certificados de CA do servidor KMIP. d. Adicione os certificados de cliente KMIP.

4. Selecione **encriptação de camada dupla** para ativar a encriptação de software.

5. Selecione **Guardar**.

O que se segue?

Agora que você criptografou seus dados em repouso, se estiver usando o protocolo NVMe/TCP, poderá "criptografe todos os dados enviados pela rede" entre o host NVMe/TCP e o sistema ASA R2.

Migre chaves de criptografia de dados ONTAP entre gerenciadores de chaves no sistema ASA R2

Você pode gerenciar suas chaves de criptografia de dados usando o Gerenciador de chaves integrado do ONTAP no sistema ASA R2 ou um gerenciador de chaves externo (ou ambos). Os gerenciadores de chaves externos só podem ser ativados no nível de VM de armazenamento. No nível do cluster do ONTAP, você pode ativar o gerenciador de chaves integrado ou um gerenciador de chaves externo.

Se ativar o seu gestor de chaves na…	**Você pode usar…**
Somente no nível do cluster	O gerenciador de chaves integrado ou um gerenciador de chaves externo
Somente no nível de VM de armazenamento	Apenas um gerenciador de chaves externo
Tanto no nível do cluster quanto no nível da VM de armazenamento	Uma das seguintes combinações de gerenciador de chaves: • Opção 1 Nível de cluster: Gerenciador de chaves integrado Nível de VM de armazenamento: Gerenciador de chaves externo • Opção 2 Nível de cluster: Gerenciador de chaves externo Nível de VM de armazenamento: Gerenciador de chaves externo

Migre chaves entre os gerenciadores-chave no nível do cluster do ONTAP

A partir do ONTAP 9.16.1, você pode usar a interface de linha de comando (CLI) do ONTAP para migrar chaves entre gerenciadores de chaves no nível do cluster.

De bordo para externo

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Criar uma configuração de gerenciador de chaves externo inativo:

```
security key-manager external create-config
```

3. Mude para o gerenciador de chaves externo:

```
security key-manager keystore enable -vserver <storage_vm_name>
-type KMIP
```

4. Exclua a configuração do gerenciador de chaves integrado:

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type OKM
```

5. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Do externo ao integrado

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Criar uma configuração inativa do gerenciador de chaves integrado:

```
security key-manager onboard create-config
```

3. Ative a configuração do gerenciador de chaves integrado:

```
security key-manager keystore enable -vserver <storage_vm_name>
-type OKM
```

4. Exclua a configuração do gerenciador de chaves externo

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type KMIP
```

5. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Migre chaves entre gerenciadores de chaves em cluster ONTAP e níveis de VM de armazenamento

Você pode usar a interface de linha de comando (CLI) do ONTAP para migrar chaves entre o gerenciador de chaves no nível do cluster e um gerenciador de chaves no nível da VM de storage.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Migrar as chaves:

```
security key-manager key migrate -from-vserver <storage_vm_name> -to
-vserver <storage_vm_name>
```

3. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Proteção contra ataques de ransomware

Crie instantâneos à prova de violação para proteger contra ataques de ransomware em sistemas de armazenamento ASA r2

Para maior proteção contra ataques de ransomware, replique snapshots para um cluster remoto e bloqueie os snapshots de destino para torná-los à prova de violação. Os

instantâneos bloqueados não podem ser eliminados acidentalmente ou maliciosamente. Use snapshots bloqueados para recuperar dados caso uma unidade de storage seja comprometida por um ataque de ransomware.

Inicialize o relógio SnapLock Compliance

Antes de criar snapshots à prova de adulteração, é necessário inicializar o relógio SnapLock Compliance nos clusters local e de destino.

Passos

1. Selecione **Cluster > Overview**.
2. Na seção **nós**, selecione **Inicializar Relógio SnapLock Compliance**.
3. Selecione **Inicializar**.
4. Verifique se o relógio de conformidade foi inicializado.
   a. Selecione **Cluster > Overview**.
   b. Na seção **nós**, selecione ; em seguida, selecione **Relógio SnapLock Compliance**.

O que vem a seguir?

Depois de inicializar o relógio SnapLock Compliance nos clusters local e de destino, você estará pronto para "crie uma relação de replicação com instantâneos bloqueados".

Habilite a proteção autônoma contra ransomware com IA em seus sistemas de armazenamento ASA r2

A partir do ONTAP 9.17.1, você pode usar a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) para proteger os dados no seu sistema ASA r2. A ARP/AI detecta rapidamente potenciais ameaças de ransomware, cria automaticamente um snapshot da ARP para proteger seus dados e exibe uma mensagem de aviso no Gerenciador do Sistema para alertá-lo sobre atividades suspeitas.

O ARP aprimora a resiliência cibernética ao adotar um modelo de aprendizado de máquina para análise antiransomware que detecta formas de ransomware em constante evolução com 98% de precisão em ambientes SAN. O modelo de aprendizado de máquina do ARP é pré-treinado em um grande conjunto de dados de arquivos, tanto antes quanto depois de um ataque de ransomware simulado. Esse treinamento que exige muitos recursos é realizado fora do ONTAP, e o modelo pré-treinado resultante desse treinamento é incluído on-box com o ONTAP. Esse modelo não é acessível nem modificável. O ARP/AI é ativado imediatamente após a capacitação; não há "período de aprendizagem".

> Nenhum sistema de detecção ou prevenção de ransomware pode garantir completamente a segurança contra um ataque de ransomware. Embora um ataque possa passar despercebido, ARP/AI atua como uma importante camada adicional de defesa caso o software antivírus falhe em detectar uma intrusão.

Sobre esta tarefa

- O suporte ARP/AI está incluído no "Licença ONTAP One" .
- ARP/AI não é compatível com unidades de armazenamento protegidas por SnapMirror active sync, SnapMirror synchronous ou SnapLock.
- A partir do ONTAP 9.18.1, o ARP/AI é ativado por padrão em todas as unidades de armazenamento

recém-criadas 12 horas após a atualização para o ONTAP 9.18.1 ou a inicialização de um novo cluster ASA r2 com ONTAP 9.18.1.

- Depois de habilitar o ARP/AI, você deve "habilite atualizações automáticas para seus arquivos de segurança" para receber automaticamente novas atualizações de segurança.

Ative o ARP/AI em todas as unidades de armazenamento no cluster

Se você estiver executando ONTAP 9.17.1, você pode habilitar ARP/AI em todas as unidades de armazenamento criadas no cluster por padrão.

No ONTAP 9.18.1 e versões posteriores, ARP/AI está habilitado por padrão em todas as novas unidades de armazenamento. Se você tiver unidades de armazenamento criadas no ONTAP 9.17.1 para as quais ARP/AI não está habilitado, você pode habilitá-lo manualmente.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Ao lado de **Anti-ransomware**, selecione ⋮ e, em seguida, selecione **Ativar em todas as unidades de armazenamento existentes**.
3. Selecione **Ativar**.

Habilite ARP/AI em todas as unidades de armazenamento em uma VM de armazenamento.

Se você estiver executando ONTAP 9.17.1, poderá habilitar ARP/AI em todas as unidades de armazenamento criadas em uma máquina virtual de armazenamento (VM) por padrão. Isso significa que qualquer nova unidade de armazenamento criada na máquina virtual de armazenamento terá ARP/AI habilitado automaticamente. Você também pode aplicar ARP/AI a unidades de armazenamento existentes na máquina virtual de armazenamento.

No ONTAP 9.18.1 e versões posteriores, ARP/AI está habilitado por padrão em todas as novas unidades de armazenamento. Se você tiver unidades de armazenamento criadas no ONTAP 9.17.1 para as quais ARP/AI não está habilitado, você pode habilitá-lo manualmente.

Passos

1. No Gerenciador do Sistema, selecione **Cluster > VMs de Armazenamento**.
2. Selecione a VM de armazenamento na qual você deseja habilitar o ARP/AI.
3. Na seção **Segurança**, ao lado de **Anti-ransomware**, selecione ⋮ ; então selecione **Editar configurações anti-ransomware**.
4. Selecione **Ativar anti-ransomware**.

   Isso habilita ARP/AI em todas as futuras unidades de armazenamento criadas na VM de armazenamento selecionada por padrão.

5. Para aplicar o ARP às unidades de armazenamento existentes na VM de armazenamento selecionada, selecione **Aplicar esta alteração a todas as unidades de armazenamento existentes aplicáveis nesta VM de armazenamento**.
6. Selecione **Guardar**.

Resultado

Todas as novas unidades de armazenamento que você criar na máquina virtual de armazenamento são protegidas contra ataques de ransomware por padrão, e qualquer atividade suspeita será relatada a você no Gerenciador de Sistemas.

Habilite ARP/AI em unidades de armazenamento específicas em uma VM de armazenamento.

Se você estiver executando ONTAP 9.17.1 e não quiser que ARP/AI esteja habilitado em todas as unidades de armazenamento em uma storage VM, você pode selecionar as unidades específicas que deseja habilitar.

No ONTAP 9.18.1 e versões posteriores, ARP/AI está habilitado por padrão em todas as novas unidades de armazenamento. Se você tiver unidades de armazenamento criadas no ONTAP 9.17.1 para as quais ARP/AI não está habilitado, você pode habilitá-lo manualmente.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione as unidades de armazenamento para as quais você deseja habilitar ARP/AI.
3. Selecione ⋮ ; então selecione **Ativar anti-ransomware**.
4. Selecione **Ativar**.

Resultado

As unidades de armazenamento selecionadas são protegidas contra ataques de ransomware, e atividades suspeitas são reportadas a você no Gerenciador do Sistema.

Desative a proteção autônoma padrão contra ransomware em seus sistemas de armazenamento ASA r2

Ao inicializar um novo cluster ONTAP 9.18.1 ASA r2 ou ao atualizar seu cluster para ONTAP 9.18.1, o ARP/AI é ativado automaticamente por padrão em todas as novas unidades de armazenamento após um período de carência de 12 horas. Se você não desativar o ARP/AI durante o período de carência, ele será ativado em todo o cluster para as novas unidades de armazenamento quando o período de carência terminar.

As unidades de armazenamento criadas no ONTAP 9.17.1 devem ser "ativado manualmente" para ARP/AI.

Passos

Você pode desativar a capacitação padrão durante ou após o período de carência inicial de 12 horas.

System Manager

1. Selecione **Cluster > Settings**.
2. Desativar ARP:
   - Para desativar durante o período de carência de 12 horas:
     i. Em **Anti-ransomware**, selecione **Don't enable** e depois selecione **Disable**.
   - Para desativar após o período de carência de 12 horas:
     i. Em **Anti-ransomware**, selecione e desmarque **Ativar para novas unidades de armazenamento**.
     ii. Selecione **Save**

CLI

1. Verifique o status de capacitação padrão:

```
security anti-ransomware auto-enable show
```

2. Desative a capacitação padrão para volumes existentes e novos:

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

Modificar períodos de retenção de snapshots ARP/AI em sistemas de armazenamento ASA r2

Se a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) detectar atividade anormal em uma ou mais unidades de armazenamento do seu sistema ASA r2, ela criará automaticamente um snapshot ARP para proteger os dados da unidade de armazenamento. Dependendo da sua capacidade de armazenamento e dos requisitos de negócios para seus dados, você pode aumentar ou diminuir o período de retenção padrão do snapshot ARP. Por exemplo, você pode aumentar o período de retenção para aplicativos críticos para os negócios, de modo que, se necessário, tenha períodos de retenção mais longos para recuperação de dados, ou pode diminuir o período de retenção para aplicativos não críticos, economizando espaço de armazenamento.

O período de retenção padrão para o snapshot do ARP varia dependendo da ação que você toma em resposta à atividade anormal.

Se você tomar essa atitude…	Os instantâneos ARP são retidos por padrão para…
Marcar como falso positivo	12 horas
Marcar como potencial ataque de ransomware	7 dias

Se você tomar essa atitude…	Os instantâneos ARP são retidos por padrão para…
Não tome medidas imediatas	10 dias

Os períodos de retenção padrão podem ser modificados usando a interface de linha de comando (CLI) do ONTAP . Veja "Modificar opções para snapshots automáticos do ONTAP" para saber as etapas para alterar o período de retenção padrão.

Responda à proteção autônoma contra ransomware com alertas de IA em sistemas de armazenamento ASA r2

Se a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) detectar atividade anormal em uma ou mais unidades de armazenamento do seu sistema ASA r2, um aviso será gerado no painel do Gerenciador de Sistemas. Você deve visualizar o aviso, verificar a atividade e, se necessário, tomar medidas para impedir qualquer ameaça potencial aos seus dados.

Se uma mensagem de aviso ARP/AI for exibida, antes de tomar qualquer medida, você deve usar o verificador de integridade do aplicativo apropriado para verificar a integridade dos dados na unidade de armazenamento. Verificar a integridade dos dados da unidade de armazenamento ajuda a determinar se a atividade é aceitável ou se se trata de um possível ataque de ransomware.

Se a atividade anormal for …	Então faça isto…
Aceitável	Marque a atividade como um falso positivo.
Um potencial ataque de ransomware	Marque a atividade como um possível ataque de ransomware.
Indeterminado	Não tome medidas imediatas. Monitore a unidade de armazenamento por até 7 dias. Se a unidade de armazenamento continuar operando normalmente, marque a atividade como um falso positivo. Se a unidade de armazenamento continuar apresentando atividade anormal, marque a atividade como um possível ataque de ransomware.

Passos

1. No System Manager, selecione **Dashboard**.

   Se o ARP detectar atividade anormal em uma ou mais unidades de armazenamento, uma mensagem será exibida em **Avisos**.

2. Selecione a mensagem de aviso.
3. Em **Visão geral de eventos**, selecione a mensagem **Avisos** que indica o número de unidades de armazenamento com atividade anormal.
4. Em **Unidades de armazenamento com atividade anormal**, selecione a unidade de armazenamento.
5. Selecione **Segurança**.

   Se houver atividade anormal na unidade de armazenamento, uma mensagem será exibida em **Anti-ransomware**.

6. Selecione **Escolher uma ação**.
7. Selecione **Marcar como falso positivo** ou selecione **Marcar como possível ataque de ransomware**.

O que se segue?

Se você observar picos na atividade de suas unidades de armazenamento, sejam eles pontuais ou característicos de um novo padrão, você deve reportá-los como seguros. Reportar esses picos manualmente como seguros ajuda a melhorar a precisão das avaliações de ameaças do ARP. Saiba como "relatar picos conhecidos de ARP/AI".

Pause ou retome a proteção autônoma contra ransomware com IA em seus sistemas de armazenamento ASA r2

A partir do ONTAP 9.17.1, você pode usar a Proteção Autônoma contra Ransomware com Inteligência Artificial (ARP/AI) para proteger os dados no seu sistema ASA r2. Se estiver planejando um evento de carga de trabalho incomum, você pode suspender temporariamente a análise de ARP/AI para evitar detecções de falsos positivos de ataques de ransomware. Após a conclusão do evento de carga de trabalho, você pode retomar a análise de ARP/AI.

Pausar ARP/AI

Antes de iniciar um evento de carga de trabalho incomum, pode ser necessário suspender temporariamente a análise de ARP/AI para evitar detecções de falsos positivos de ataques de ransomware.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione as unidades de armazenamento para as quais você deseja pausar o ARP/AI.
3. Selecione **Pausar anti-ransomware**.

Resultado

A análise de ARP/AI é pausada para as unidades de armazenamento selecionadas, e nenhuma atividade suspeita é relatada a você no Gerenciador do Sistema até que você retome o ARP/AI.

Retomar ARP/AI

Se você pausar o ARP/AI durante uma carga de trabalho incomum, após a conclusão da carga de trabalho, você deverá retomá-la para proteger seus dados contra ataques de ransomware.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione as unidades de armazenamento para as quais você deseja retomar o ARP/AI.
3. Selecione **Retomar anti-ransomware**.

Resultado

A análise de potenciais ataques de ransomware é retomada e atividades suspeitas são reportadas a você no Gerenciador do Sistema.

Conexões NVMe seguras em seus sistemas de storage ASA R2

Se você estiver usando o protocolo NVMe, poderá configurar a autenticação na banda para aprimorar a segurança dos dados. A autenticação na banda permite autenticação bidirecional e unidirecional segura entre os hosts NVMe e o sistema ASA R2. A autenticação na banda está disponível para todos os hosts NVMe. Se você estiver usando o protocolo NVMe/TCP, poderá aprimorar ainda mais a segurança dos dados configurando a segurança da camada de transporte (TLS) para criptografar todos os dados enviados pela rede entre os hosts NVMe/TCP e o sistema ASA R2.

Passos

1. Selecione **hosts**; em seguida, selecione **NVMe**.
2. + Add Selecione .
3. Insira o nome do host e selecione o sistema operacional do host.
4. Insira uma descrição do host; em seguida, selecione a VM de armazenamento a ser conetada ao host.
5. Selecione ao lado do nome do host.
6. Selecione **Autenticação na banda**.
7. Se você estiver usando o protocolo NVMe/TCP, selecione **exigir segurança da camada de transporte (TLS)**.
8. Selecione **Adicionar**.

Resultado

A segurança dos seus dados é melhorada com autenticação na banda e/ou TLS.

Conexões IP seguras em seus sistemas de storage ASA R2

Se você estiver usando o protocolo IP no sistema ASA R2, poderá configurar a segurança IP (IPsec) para melhorar a segurança dos dados. O IPsec é um padrão da Internet que fornece criptografia de dados em trânsito, autenticação para o tráfego que flui entre os pontos de extremidade da rede em um nível IP e proteção contra repetição e ataques mal-intencionados contra seus dados.

Para sistemas ASA R2, o IPsec está disponível para hosts iSCSI e NVMe/TCP.

Em determinados sistemas ASA R2, várias operações criptográficas, como verificações de criptografia e integridade, podem ser descarregadas para uma placa de controlador de interface de rede (NIC) suportada. A taxa de transferência para operações descarregadas para a placa NIC é de aproximadamente 5% ou menos. Isso pode melhorar significativamente o desempenho e a taxa de transferência do tráfego de rede protegido pelo IPsec.

A partir do ONTAP 9.18.1, o suporte para descarregamento de hardware IPsec foi estendido ao tráfego IPv6.

As seguintes placas de rede são compatíveis com o descarregamento de hardware nos seguintes sistemas ASA r2 e versões do ONTAP :

Placa NIC suportada	Sistemas ASA r2	Versão ONTAP
X50135A (Controlador Ethernet 2p, 40G/100G)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.17.1 e posterior
X60135A (Controlador Ethernet 2p, 40G/100G)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.17.1 e posterior
X50131A - (controlador Ethernet 2P, 40G/100g/200g/400G)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.16.1 e posterior
X60132A - (controlador Ethernet 4P, 10G/25G)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 e posterior

Veja o"NetApp Hardware Universe" Para obter mais informações sobre os sistemas e placas suportados.

O que se segue?

O IPsec é configurado no seu sistema ASA r2 da mesma forma que em outros sistemas ONTAP . Para mais informações, consulte "Prepare-se para configurar a segurança IP para a rede ONTAP.".

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.