



# Proteção autônoma contra ransomware

## ONTAP 9

NetApp  
January 17, 2025

# Índice

Proteção autônoma contra ransomware .....	1
Saiba mais sobre a proteção autônoma contra ransomware no ONTAP .....	1
Casos de uso e considerações da proteção autônoma contra ransomware .....	5
Ative a proteção Autonomous ransomware .....	9
Ative a proteção Autonomous ransomware por padrão em novos volumes .....	12
Ative ARP/AI com a atualização automática .....	15
Atualize a proteção Autonomous ransomware com AI (ARP/AI) .....	16
Mude para o modo ARP ativo após um período de aprendizagem .....	19
Pausar a proteção Autonomous ransomware para excluir eventos de workload da análise .....	21
Gerencie os parâmetros de detecção de ataques da proteção autônoma contra ransomware com o ONTAP .....	23
Responder a atividades anormais .....	27
Restaure os dados após um ataque de ransomware .....	31
Modificar opções para instantâneos automáticos .....	35

# Proteção autônoma contra ransomware

## Saiba mais sobre a proteção autônoma contra ransomware no ONTAP

A partir do ONTAP 9.10,1, o recurso Autonomous ransomware Protection (ARP) usa análise de workload em ambientes nas (NFS e SMB) para detectar e avisar proativamente sobre atividades anormais que podem indicar um ataque. Quando um ataque é suspeito, o ARP também cria novos snapshots, além da proteção existente fornecida por snapshots programados.

### Proteção autônoma contra ransomware com inteligência artificial (ARP/AI)

A partir do ONTAP 9.16,1, o ARP melhora a resiliência cibernética adotando um modelo de aprendizado de máquina para análise anti-ransomware que deteta formas de ransomware em constante evolução com 99% de precisão. O modelo de aprendizado de máquina do ARP é pré-treinado em um grande conjunto de dados de arquivos antes e depois de um ataque simulado de ransomware. Esse treinamento intensivo em recursos é feito fora do ONTAP, mas o aprendizado desse treinamento é usado para o modelo dentro do ONTAP.

#### Transição imediata para o modo ativo para ARP/AI com volumes FlexVol

Com os volumes ARP/AI e FlexVol, não [período de aprendizagem](#) há . O ARP/AI começa no modo ativo imediatamente após a instalação ou atualização para o 9,16. Depois de atualizar o cluster para o ONTAP 9.16,1, o ARP/AI será automaticamente ativado para volumes FlexVol existentes e novos se o ARP já estiver ativado para esses volumes.

["Saiba mais sobre como ativar o ARP/AI"](#)

#### Atualizações automáticas ARP/AI

Para manter a proteção atualizada contra as ameaças mais recentes de ransomware, o ARP/AI oferece atualizações automáticas frequentes que ocorrem fora dos quadros regulares de atualização e liberação do ONTAP. Se tiver ["atualizações automáticas ativadas"](#), também poderá começar a receber atualizações automáticas de segurança para ARP/AI depois de selecionar atualizações automáticas para ficheiros de segurança. Você também pode optar por fazer essas atualizações manualmente e controlar quando as atualizações ocorrem.

A partir do ONTAP 9.16,1, as atualizações de segurança para ARP/AI estão disponíveis usando o Gerenciador do sistema, além das atualizações de sistema e firmware.



O recurso ARP/AI atualmente suporta apenas nas. Embora o recurso de atualização automática exiba a disponibilidade de novos arquivos de segurança para implantação no System Manager, essas atualizações são aplicáveis apenas à proteção da carga de trabalho nas.

["Saiba mais sobre as atualizações ARP/AI"](#)

### Licenças e capacitação

O suporte ARP está incluído no ["Licença ONTAP ONE"](#). Se você não tiver a licença ONTAP One, outras licenças estarão disponíveis para usar ARP que diferem dependendo da sua versão do ONTAP.

Lançamentos da ONTAP	Licença
ONTAP 9.11,1 e posterior	Anti_ransomware
ONTAP 9.10,1	MT_EK_MGMT (gerenciamento de chaves de vários clientes)

- Se você estiver atualizando do ONTAP 9.10,1 para o ONTAP 9.11,1 ou posterior e o ARP já estiver configurado em seu sistema, não será necessário instalar a nova licença Anti-ransomware. Para novas configurações ARP, a nova licença é necessária.
- Se você estiver revertendo do ONTAP 9.11,1 ou posterior para o ONTAP 9.10,1 e tiver ativado o ARP com a licença Anti-ransomware, verá uma mensagem de aviso e poderá precisar reconfigurar o ARP.

["Saiba mais sobre como reverter ARP"](#).

## Estratégia de proteção contra ransomware da ONTAP

Uma estratégia eficaz de detecção de ransomware deve incluir mais do que uma única camada de proteção.

Uma analogia seria as características de segurança de um veículo. Você não confia em uma única característica, como um cinto de segurança, para protegê-lo completamente em um acidente. Os airbags, os travões antibloqueio e o aviso de colisão à frente são todos elementos de segurança adicionais que conduzirão a um resultado muito melhor. A proteção contra ransomware deve ser vista da mesma maneira.

Embora o ONTAP inclua recursos como FPolicy, snapshots, SnapLock e Active IQ Digital Advisor (também conhecido como consultor digital) para ajudar a proteger contra ransomware, as informações a seguir se concentram no recurso ARP on-box com recursos de aprendizado de máquina.

Para saber mais sobre outros recursos anti-ransomware do ONTAP, ["Portfólio de proteção de ransomware e NetApp"](#) consulte .

## O que o ARP deteta

O ARP é projetado para proteger contra ataques de negação de serviço, onde o invasor retém dados até que um resgate seja pago. O ARP oferece detecção de ransomware em tempo real com base em:

- Identificação dos dados recebidos como encriptados ou em texto simples.
- Análises que detectam:
  - **Entropia:** Uma avaliação da aleatoriedade dos dados em um arquivo
  - **Tipos de extensão de arquivo:** Uma extensão que não está em conformidade com o tipo de extensão normal
  - **IOPS de arquivos:** Um aumento na atividade de volume anormal com criptografia de dados (a partir de ONTAP 9.11,1)

O ARP pode detetar a propagação da maioria dos ataques de ransomware depois que apenas um pequeno número de arquivos é criptografado, tomar medidas automaticamente para proteger os dados e alertá-lo de que um ataque suspeito está acontecendo.



Nenhum sistema de prevenção ou detecção de ransomware pode garantir completamente a segurança de um ataque de ransomware. Embora seja possível que um ataque não seja detetado, o ARP atua como uma importante camada adicional de defesa se o software antivírus não conseguir detetar uma intrusão.

## Aprendizagem e modos ativos

ARP tem dois modos:

- **Modo de aprendizagem** (ou modo "funcionamento a seco")
- **Modo ativo** (ou modo "ativado")

### Modo de aprendizagem

Para todos os ARP em execução com ONTAP 9.10,1 a 9.15.1 e ARP usados para volumes FlexGroup com ONTAP 9.16,1, quando você ativa o ARP, ele é executado em *modo de aprendizagem*. No modo de aprendizagem, o sistema ONTAP desenvolve um perfil de alerta baseado nas áreas analíticas: Entropia, tipos de extensão de arquivo e IOPS de arquivos. Depois de executar o ARP no modo de aprendizado por tempo suficiente para avaliar as características da carga de trabalho, você pode alternar para o modo ativo e começar a proteger seus dados.

Recomenda-se que você deixe o ARP no modo de aprendizado por 30 dias. A partir do ONTAP 9.13,1, o ARP determina automaticamente o intervalo de aprendizagem ideal e automatiza o switch, que pode ocorrer antes de 30 dias.



O comando `security anti-ransomware volume workload-behavior show` mostra extensões de arquivo que foram detetadas no volume. Se você executar esse comando no início do modo de aprendizado e ele mostrar uma representação precisa dos tipos de arquivo, você não deve usar esses dados como base para mover para o modo ativo, já que o ONTAP ainda está coletando outras métricas.

### Modo ativo

Para ARP em execução com ONTAP 9.10,1 a 9.15.1, o ARP muda para *ative mode* após o intervalo de aprendizagem ideal ser concluído. Com o ARP/AI a partir do ONTAP 9.16,1, não há período de aprendizado quando o ARP é usado com volumes FlexVol. O ARP/AI nos volumes FlexVol começa no modo ativo imediatamente após a instalação ou atualização para o 9.16.1. Se você estiver usando ONTAP 9.16,1 e ARP com volumes FlexGroup, um período de aprendizado ainda será necessário antes da transição para o modo ativo.

Depois que o ARP mudou para o modo ativo, o ONTAP cria instantâneos ARP para proteger os dados se uma ameaça for detetada.

No modo ativo, se uma extensão de arquivo for sinalizada como anormal, você deve avaliar o alerta. Você pode agir no alerta para proteger seus dados ou você pode marcar o alerta como um falso positivo. Marcar um alerta como falso positivo atualiza o perfil de alerta. Por exemplo, se o alerta for acionado por uma nova extensão de arquivo e você marcar o alerta como um falso positivo, você não receberá um alerta na próxima vez que essa extensão de arquivo for observada.



A partir de ONTAP 9.11,1, você pode personalizar os parâmetros de detecção para ARP. Para obter mais informações, [Gerenciar parâmetros de detecção de ataque ARP](#) consulte .

## Avaliação de ameaças e instantâneos ARP

No modo ativo, o ARP avalia a probabilidade de ameaça com base nos dados de entrada medidos em relação às análises aprendidas. Uma medição é atribuída quando o ARP deteta uma ameaça:

- **Low:** A detecção mais precoce de uma anomalia no volume (por exemplo, uma nova extensão de arquivo é observada no volume). Este nível de detecção só está disponível em versões anteriores ao ONTAP 9.16,1 que não têm ARP/AI.
- **Moderado:** Vários arquivos com a mesma extensão de arquivo nunca visto-antes são observados.
  - No ONTAP 9.10,1, o limite de escalonamento para moderar é de 100 ou mais arquivos.
  - Começando com ONTAP 9.11,1, a quantidade de arquivo é modificável; seu valor padrão é 20.

Em uma situação de baixa ameaça, o ONTAP deteta uma anormalidade e cria um instantâneo do volume para criar o melhor ponto de recuperação. O ONTAP prepende o nome do instantâneo ARP `Anti-ransomware-backup` para torná-lo facilmente identificável; por exemplo `Anti_ransomware_backup.2022-12-20_1248,`.

A ameaça aumenta para moderar depois que o ONTAP executa um relatório de análise determinando se a anormalidade corresponde a um perfil de ransomware. As ameaças que permanecem no nível baixo são registradas e visíveis na seção **Eventos** do System Manager. Quando a probabilidade de ataque é moderada, o ONTAP gera uma notificação EMS, solicitando que você avalie a ameaça. O ONTAP não envia alertas sobre baixas ameaças, no entanto, começando com ONTAP 9.14,1, você pode [modificar definições de alertas](#). Para obter mais informações, [Responder a atividades anormais](#) consulte .

Você pode visualizar informações sobre uma ameaça, independentemente do nível, na seção **Eventos** do System Manager ou com o `security anti-ransomware volume show` comando.

Instantâneos ARP individuais são retidos por dois dias. Se houver vários instantâneos ARP, eles serão retidos por cinco dias por padrão. A partir do ONTAP 9.11,1, você pode modificar as configurações de retenção. Para obter mais informações, [Modificar opções para instantâneos](#) consulte .

## Como recuperar dados no ONTAP após um ataque de ransomware

Quando um ataque é suspeito, o sistema obtém um instantâneo de volume nesse momento e bloqueia essa cópia. Se o ataque for confirmado mais tarde, o volume poderá ser restaurado usando o instantâneo ARP.

Os instantâneos bloqueados não podem ser eliminados por meios normais. No entanto, se você decidir mais tarde marcar o ataque como um falso positivo, a cópia bloqueada será excluída.

Com o conhecimento dos arquivos afetados e o tempo de ataque, é possível recuperar seletivamente os arquivos afetados de vários snapshots, em vez de simplesmente reverter todo o volume para um dos snapshots.

O ARP se baseia na comprovada tecnologia de recuperação de desastres e proteção de dados da ONTAP para responder a ataques de ransomware. Consulte os tópicos a seguir para obter mais informações sobre como recuperar dados.

- ["Recuperar de instantâneos"](#)
- ["Recuperação inteligente de ransomware"](#)

## Proteção de verificação multi-admin para ARP

A partir do ONTAP 9.13,1, é recomendável ativar a verificação multi-admin (MAV) para que dois ou mais administradores de usuário autenticados sejam necessários para a configuração ARP (Autonomous ransomware Protection). Para obter mais informações, ["Ative a verificação de vários administradores"](#) consulte

## Casos de uso e considerações da proteção autônoma contra ransomware

A proteção autônoma contra ransomware (ARP) está disponível para workloads nas a partir do ONTAP 9.10,1. Antes de implantar o ARP, você deve estar ciente dos usos recomendados e das configurações suportadas, bem como das implicações de desempenho.

### Configurações suportadas e não suportadas

Ao decidir usar o ARP, é importante garantir que a carga de trabalho do seu volume seja adequada ao ARP e que atenda às configurações do sistema necessárias.

#### Workloads adequados

O ARP é adequado para:

- Bancos de dados no storage NFS
- Diretórios home do Windows ou do Linux

Como os usuários podem criar arquivos com extensões que não foram detetadas no período de aprendizado, há maior possibilidade de falsos positivos nessa carga de trabalho.

- Imagens e vídeo

Por exemplo, Registros de saúde e dados de automação de design eletrônico (EDA)

#### Cargas de trabalho inadequadas

O ARP não é adequado para:

- Cargas de trabalho com alta frequência de arquivos criam ou excluem (centenas de milhares de arquivos em poucos segundos; por exemplo, cargas de trabalho de teste/desenvolvimento).
- A detecção de ameaças do ARP depende de sua capacidade de reconhecer um aumento incomum na atividade de criação, renomeação ou exclusão de arquivos. Se o aplicativo em si for a origem da atividade do arquivo, ele não poderá ser distinguido efetivamente da atividade de ransomware.
- Cargas de trabalho em que o aplicativo ou o host criptografa dados. O ARP depende de distinguir os dados recebidos como criptografados ou não criptografados. Se o próprio aplicativo estiver criptografando os dados, a eficácia do recurso será reduzida. No entanto, o recurso ainda pode funcionar com base na atividade do arquivo (excluir, substituir ou criar, ou criar ou renomear com uma nova extensão de arquivo) e no tipo de arquivo.

## Configurações compatíveis

O ARP está disponível para volumes NFS e SMB FlexVol em sistemas ONTAP locais a partir do ONTAP 9.10,1.

O suporte para outras configurações e tipos de volume está disponível nas seguintes versões do ONTAP:

	ONTAP 9.16,1	ONTAP 9.15,1	ONTAP 9.14,1	ONTAP 9.13,1	ONTAP 9.12,1	ONTAP 9.11,1	ONTAP 9.10,1
Volumes protegidos com o SnapMirror assíncrono	✓	✓	✓	✓	✓		
SVMs protegidas com SnapMirror assíncrono (recuperação de desastres da SVM)	✓	✓	✓	✓	✓		
Mobilidade de ( `vserver migrate` dados os SVM )	✓	✓	✓	✓	✓		
Volumes FlexGroup*	✓	✓	✓	✓			
Verificação multi-admin	✓	✓	✓	✓			
ARP/AI com atualizações automáticas	✓						

\*ARP/AI não suporta volumes FlexGroup. Depois de ser atualizado para o ONTAP 9.16,1, os volumes FlexGroup habilitados para ARP continuam operando com o mesmo modelo ARP usado antes do ARP/AI.

### Interoperabilidade SnapMirror e ARP

A partir do ONTAP 9.12,1, o ARP é suportado em volumes de destino assíncronos do SnapMirror. ARP não é \*\* suportado com SnapMirror síncrono.

Se um volume de origem do SnapMirror estiver habilitado para ARP, o volume de destino do SnapMirror adquirirá automaticamente o estado de configuração ARP (aprendizado, habilitado e assim por diante), os dados de treinamento ARP e o instantâneo criado pelo ARP do volume de origem. Nenhuma capacitação explícita é necessária.

Enquanto o volume de destino consiste em instantâneos somente leitura (RO), nenhum processamento ARP é feito em seus dados. No entanto, quando o volume de destino do SnapMirror é convertido para leitura-gravação (RW), o ARP é ativado automaticamente no volume de destino convertido em RW. O volume de



destino não requer nenhum procedimento de aprendizagem adicional além do que já está gravado no volume de origem.

No ONTAP 9.10,1 e 9.11.1, o SnapMirror não transfere o estado de configuração ARP, os dados de treinamento e os snapshots dos volumes de origem para o destino. Assim, quando o volume de destino SnapMirror é convertido para RW, o ARP no volume de destino deve ser explicitamente ativado no modo de aprendizagem após a conversão.

### **ARP e máquinas virtuais**

O ARP é compatível com máquinas virtuais (VMs). A detecção ARP comporta-se de forma diferente para alterações dentro e fora da VM. O ARP não é recomendado para cargas de trabalho com arquivos de alta entropia dentro da VM.

### **Alterações fora da VM**

O ARP pode detetar alterações de extensão de arquivo em um volume NFS fora da VM se uma nova extensão entrar no volume criptografado ou uma extensão de arquivo mudar. As alterações de extensão de arquivo detetáveis são:

- .vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .NVRAM
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- .log
- - no.log

### **Alterações dentro da VM**

Se o ataque de ransomware segmentar a VM e os arquivos dentro da VM são alterados sem fazer alterações fora da VM, o ARP deteta a ameaça se a entropia padrão da VM for baixa (por exemplo, arquivos .txt, .docx ou .mp4). Embora o ARP crie um snapshot de proteção nesse cenário, ele não gera um alerta de ameaça porque as extensões de arquivo fora da VM não foram adulteradas.

Se, por padrão, os arquivos forem de alta entropia (por exemplo, arquivos .gzip ou protegidos por senha), os recursos de detecção do ARP são limitados. O ARP ainda pode tirar instantâneos proativos nesta instância; no entanto, nenhum alerta será acionado se as extensões de arquivo não tiverem sido adulteradas externamente.

### **Configurações não suportadas**

O ARP não é suportado nas seguintes configurações do sistema:

- Ambientes ONTAP S3
- AMBIENTES SAN

O ARP não suporta as seguintes configurações de volume:

- Volumes FlexGroup (em ONTAP 9.10,1 a 9.12.1. A partir do ONTAP 9.13,1, os volumes FlexGroup são suportados, mas são limitados ao modelo ARP usado antes do ARP/AI)
- Volumes FlexCache (ARP é suportado em volumes FlexVol de origem, mas não em volumes de cache)
- Volumes offline
- Volumes apenas de SAN
- Volumes SnapLock
- SnapMirror síncrono
- SnapMirror assíncrono (não suportado apenas no ONTAP 9.10,1 e 9.11.1. O SnapMirror Asynchronous é suportado a partir do ONTAP 9.12,1. Para obter mais informações, [\[snapmirror\]](#) consulte .)
- Volumes restritos
- Volumes raiz de VMs de storage
- Volumes de VMs de storage interrompidas

## Considerações sobre desempenho e frequência ARP

O ARP pode ter um impacto mínimo no desempenho do sistema, conforme medido no throughput e IOPS de pico. O impacto do recurso ARP depende das cargas de trabalho de volume específicas. Para workloads comuns, os seguintes limites de configuração são recomendados:

Características do workload	Limite de volume recomendado por nó	Degradação do desempenho quando o limite de volume por nó é excedido, passa:[*]
Leitura intensiva ou os dados podem ser comprimidos.	150	4% do máximo de IOPS
Não é possível compactar dados com uso intensivo de gravação.	60	10% do máximo de IOPS

Pass:[\*] o desempenho do sistema não é degradado além dessas porcentagens, independentemente do número de volumes adicionados além dos limites recomendados.

Como a análise ARP é executada em uma sequência priorizada, à medida que o número de volumes protegidos aumenta, a análise é executada em cada volume com menos frequência.

## Verificação multi-admin com volumes protegidos com ARP

A partir do ONTAP 9.13,1, você pode ativar a verificação multi-admin (MAV) para segurança adicional com o ARP. O MAV garante que pelo menos dois ou mais administradores autenticados sejam necessários para desativar o ARP, pausar o ARP ou marcar um ataque suspeito como falso positivo em um volume protegido. Aprenda a "[Ativar MAV para volumes protegidos por ARP](#)".

Você precisa definir administradores para um grupo MAV e criar regras MAV para os `security anti-ransomware volume disable` comandos, `security anti-ransomware volume pause` e `security anti-ransomware volume attack clear-suspect` ARP que deseja proteger. Cada administrador no grupo MAV deve aprovar cada nova solicitação de regra e "[Adicione a regra MAV novamente](#)" dentro das configurações MAV.

A partir do ONTAP 9.14,1, o ARP oferece alertas para a criação de um instantâneo ARP e para a observação de uma nova extensão de arquivo. Os alertas para esses eventos são desativados por padrão. Os alertas podem ser definidos no volume ou no nível da SVM. Você pode criar regras MAV no nível SVM usando `security anti-ransomware vserver event-log modify` ou no nível de volume com `security anti-ransomware volume event-log modify`.

### Próximas etapas

- ["Ative a proteção Autonomous ransomware"](#)
- ["Ativar MAV para volumes protegidos por ARP"](#)

## Ative a proteção Autonomous ransomware

A partir do ONTAP 9.10,1, você pode ativar a proteção autônoma contra ransomware (ARP) em um volume existente ou criar um novo volume e ativar o ARP desde o início.

Se você quiser configurar o cluster do ONTAP para que todos os novos volumes sejam ativados por padrão para a proteção autônoma contra ransomware (ARP), consulte este ["Procedimento ARP relacionado"](#).

### Sobre esta tarefa

- **Para ONTAP 9.10,1 a 9.15.1 e ARP com volumes FlexGroup** para essas versões do ONTAP, você deve sempre ativar o ARP inicialmente no ["modo de aprendizagem"](#) modo (ou "Dry-run"). Quando você ativa o ARP pela primeira vez no modo de aprendizado, o sistema analisa a carga de trabalho para caracterizar o comportamento normal. O início no modo ativo pode levar a relatórios falsos positivos excessivos.

Recomenda-se que o ARP seja executado no modo de aprendizagem por um mínimo de 30 dias. A partir do ONTAP 9.13,1, o ARP determina automaticamente o intervalo ideal do período de aprendizagem e automatiza o switch, que pode ocorrer antes de 30 dias.

- **Para ONTAP 9.16,1 e posterior com volumes FlexVol** quando você ativa o ARP, a proteção ARP/AI começa imediatamente no modo ativo. Nenhum período de aprendizagem é necessário.



Nos volumes existentes, os modos de aprendizagem e ativos aplicam-se apenas a dados recém-gravados, não a dados já existentes no volume. Os dados existentes não são digitalizados e analisados, porque as características do tráfego de dados normal anterior são assumidas com base nos novos dados depois que o volume é ativado para ARP.

### Antes de começar

- Você precisa ter uma VM de storage (SVM) habilitada para NFS, SMB (ou ambos).
- O [licença correta](#) tem de estar instalado para a versão do ONTAP.
- Você precisa ter um workload nas com clientes configurados.
- O volume em que deseja definir ARP deve estar protegido e ter um ["caminho de junção"](#) ativo .
- O volume tem de ser inferior a 100% cheio.
- É recomendável configurar o sistema EMS para enviar notificações por e-mail, que incluirão avisos de atividade ARP. Para obter mais informações, ["Configurar eventos EMS para enviar notificações por e-mail"](#) consulte .
- A partir do ONTAP 9.13,1, é recomendável ativar a verificação multi-admin (MAV) para que dois ou mais administradores de usuário autenticados sejam necessários para a configuração ARP (Autonomous ransomware Protection). Para obter mais informações, ["Ative a verificação de vários administradores"](#) consulte .

## **Ative ARP em um volume novo ou existente**

Você pode ativar o ARP usando o Gerenciador do sistema ou a CLI do ONTAP.

## System Manager

### Passos

1. Selecione **armazenamento > volumes** e, em seguida, selecione o volume que pretende proteger.
2. Na guia **Security** da visão geral **volumes**, selecione **Status** para alternar de Disabled (Desativado) para Enabled (habilitado).
  - Se você estiver usando ARP com ONTAP 9.15,1 ou anterior ou ONTAP 9.16,1 com volumes FlexGroup, selecione **Enabled in learning-mode** na caixa **Anti-ransomware**.



A partir do ONTAP 9.13,1, o ARP determina automaticamente o intervalo ideal do período de aprendizagem e automatiza o switch. "[Desative essa configuração na VM de armazenamento associada](#)" Pode controlar manualmente o modo de aprendizagem para a transição do modo ativo.

- Se você estiver usando ARP em volumes FlexVol com ONTAP 9.16,1 ou posterior, a funcionalidade ARP/AI não requer um período de aprendizado e o modo ativo é selecionado por padrão.
3. Você pode verificar o estado ARP do volume na caixa **Anti-ransomware**.

Para exibir o status ARP para todos os volumes: No painel **volumes**, selecione **Mostrar/Ocultar** e verifique se o status **Anti-ransomware** está marcado.

### CLI

O processo para ativar o ARP com a CLI difere se você estiver habilitando-o em um volume existente versus um novo volume.

#### Ative ARP em um volume existente

1. Modifique um volume existente para habilitar a proteção contra ransomware:
  - Para ONTAP 9.15,1 e anterior e ARP com volumes FlexGroup, defina o estado do volume para `dry-run` (modo de aprendizagem):

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver <svm_name>
```

- Para ONTAP 9.16,1 e posterior com volumes ARP/AI e FlexVol, defina o estado do volume para `active` (modo ativo):

```
security anti-ransomware volume active -volume <vol_name> -vserver <svm_name>
```

2. Se você atualizou para o ONTAP 9.13,1 ou posterior e o estado padrão ARP for `dry-run`, o aprendizado adaptável será ativado para que a alteração para o estado ativo seja feita automaticamente. Se você não quiser que esse comportamento seja ativado automaticamente, altere a configuração no nível SVM em todos os volumes associados:

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to-enabled false
```

3. Verifique o estado ARP do volume.

```
security anti-ransomware volume show
```

### Ative ARP em um novo volume

1. Crie um novo volume com ARP ativado antes de provisionar dados:

- Para ONTAP 9.15,1 e anterior e ARP com volumes FlexGroup, defina o estado para `dry-run` (modo de aprendizagem):

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path  
</path_name>
```

- Para ONTAP 9.16,1 e posterior com volumes ARP/AI e FlexVol, defina o estado para `active` (modo ativo):

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state active -junction-path  
</path_name>
```

2. Se você atualizou para o ONTAP 9.13,1 ou posterior e o estado padrão ARP for `dry-run`, o aprendizado adaptável será ativado para que a alteração para o estado ativo seja feita automaticamente. Se você não quiser que esse comportamento seja ativado automaticamente, altere a configuração no nível SVM em todos os volumes associados:

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to  
-enabled false
```

3. Verifique o estado ARP do volume.

```
security anti-ransomware volume show
```

### Informações relacionadas

- ["Mude para o modo ativo após um período de aprendizagem"](#)

## Ative a proteção Autonomous ransomware por padrão em novos volumes

A partir do ONTAP 9.10,1, você pode configurar VMs de armazenamento (SVMs) para que novos volumes sejam ativados por padrão com a proteção Autônoma contra ransomware (ARP). Você pode modificar essa configuração usando o System Manager ou com a CLI.

Se você quiser configurar apenas volumes individuais novos ou existentes sem tornar o ARP o padrão, consulte este ["Procedimento ARP relacionado"](#).

### Sobre esta tarefa

Por padrão, novos volumes são criados com ARP no modo desativado. O ARP só será ativado por padrão em novos volumes criados no SVM depois de ativar a funcionalidade ARP para volumes nas.

O ARP não será ativado automaticamente em volumes existentes. As alterações descritas neste

procedimento afetam apenas novos volumes. Aprenda a ["Ativar ARP para volumes existentes"](#).

- **Para ONTAP 9.10,1 a 9.15.1 e ARP com volumes FlexGroup** por padrão, novos volumes habilitados com ARP ativado são definidos como ["modo de aprendizagem"](#)modo (ou "Dry-run") no qual o sistema analisa a carga de trabalho para caracterizar o comportamento normal. O modo de aprendizagem pode ser transferido para o modo ativo manualmente (todas as versões ARP) ou automaticamente (começando no ARP 9.13.1). Com o ARP 9.13.1 e posterior, o aprendizado adaptável foi adicionado à análise ARP para que a mudança do modo de aprendizado para o modo ativo seja feita automaticamente.
- **Para ONTAP 9.16,1 e posterior com volumes FlexVol** quando você ativa o ARP, a proteção ARP/AI começa imediatamente no modo ativo. Nenhum período de aprendizagem é necessário.


#### Antes de começar

- O [licença correta](#) tem de estar instalado para a versão do ONTAP.
- O volume tem de ser inferior a 100% cheio.
- Os caminhos de junção devem estar ativos.
- A partir do ONTAP 9.13,1, é recomendável ativar a verificação multi-admin (MAV) para que dois ou mais administradores de usuários autenticados sejam necessários para operações anti-ransomware. ["Saiba mais"](#).

#### Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para ativar o ARP por padrão em novos volumes.

## System Manager

1. Selecione **Storage > Storage VMs** e, em seguida, selecione a VM de armazenamento que contém volumes que você deseja proteger com ARP.
2. Navegue até a guia **Configurações**. Em **Segurança**, localize o bloco **Anti-ransomware** e  selecione .
3. Marque a caixa para ativar o ARP para volumes nas. Marque a caixa adicional para ativar o ARP em todos os volumes nas elegíveis na VM de armazenamento.



Para o ONTAP 9.16,1, o modo ativo é ativado automaticamente por padrão para novos volumes do FlexVol e nenhum período de aprendizado é necessário.



Nos volumes existentes, os modos de aprendizagem e ativos aplicam-se apenas a dados recém-gravados, não a dados já existentes no volume. Os dados existentes não são digitalizados e analisados, porque as características do tráfego de dados normal anterior são assumidas com base nos novos dados depois que o volume é ativado para ARP.

4. Se você atualizou para o ARP 9.13.1 ou posterior, opcionalmente selecione **alternar automaticamente do modo de aprendizado para o modo ativo após aprendizado suficiente**. Isso permite que o ARP determine o intervalo ideal do período de aprendizado e automatize o switch para o modo ativo.

## CLI

- Modifique um SVM existente para ativar o ARP por padrão em novos volumes:

- Para volumes ONTAP 9.15,1 e anteriores e FlexGroup, defina o estado predefinido para `dry-run` (modo de aprendizagem):

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume-state dry-run
```

- Para ONTAP 9.16,1 e posterior com volumes ARP/AI e FlexVol, defina o estado padrão para `active` (modo ativo):

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume-state active
```

- Crie um novo SVM com ARP habilitado por padrão para novos volumes:

- Para volumes ONTAP 9.15,1 e anteriores e FlexGroup, defina o estado predefinido para `dry-run` (modo de aprendizagem):

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume-state dry-run <other parameters as needed>
```

- Para ONTAP 9.16,1 e posterior com volumes ARP/AI e FlexVol, defina o estado padrão para `active` (modo ativo):

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume-state active
```



- Se você atualizou para o ONTAP 9.13,1 ou posterior e o estado padrão for `dry-run`, o aprendizado adaptável será ativado para que a alteração para o estado ativo seja feita automaticamente. Modifique o SVM existente se você não quiser que esse comportamento seja ativado automaticamente:

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to-enabled false
```

#### Informações relacionadas

- ["Mude para o modo ativo após um período de aprendizagem"](#)

## Ative ARP/AI com a atualização automática

A partir do ONTAP 9.16,1, o ARP adotou a proteção autônoma contra ransomware com Inteligência artificial (ARP/AI) para melhorar a detecção e a resposta de ameaças. Depois de atualizar o cluster para o ONTAP 9.16,1, o ARP/AI será ativado automaticamente para volumes FlexVol se o ARP já estiver ativado para esses volumes. Se você não ativou o ARP ou não ativou as atualizações automáticas para o cluster, siga um dos cenários descritos neste procedimento.



Antes de atualizar para o ONTAP 9.16,1, ["Feche todas as detecções ARP existentes"](#).

#### Antes de começar

- Você deve ter volumes FlexVol para usar ARP/AI. Se você tiver volumes FlexGroup, o modelo ARP usado antes do ARP/AI continuará funcionando após a atualização para o ONTAP 9.16,1.



Quando você atualiza para o ONTAP 9.16,1, o ARP é ativado automaticamente no modo ativo para quaisquer instâncias ARP existentes com volumes FlexVol. Como o ARP/AI é treinado em um modelo extensivo de aprendizado de máquina, um período de aprendizado não é mais necessário. Quaisquer períodos de aprendizagem que não tenham sido concluídos antes da atualização serão automaticamente encerrados e os volumes serão transferidos para o modo ativo.

#### Passos

1. Siga o cenário específico da sua configuração:
  - \*Para novos clusters executando o ONTAP 9.16,1\* ["Ativar ARP"](#): . O ARP não está ativado por padrão. Depois de ativar o ARP, a funcionalidade ARP/AI é ativada automaticamente no modo ativo nos volumes que você escolher proteger.
  - **Para clusters existentes recentemente atualizados para ONTAP 9.16,1 que têm ARP ativado:** Nenhuma ação necessária. O ARP/AI se tornará automaticamente o novo método ARP de proteção contra ameaças nos volumes FlexVol que você escolheu proteger.
  - **Para clusters existentes recentemente atualizados para o ONTAP 9.16,1 que não tenham o ARP ativado:** ["Ativar ARP"](#). O ARP/AI se tornará automaticamente o novo método ARP de proteção contra ameaças depois de ativar o ARP.
2. Depois que o ARP/AI estiver ativado, decida se deseja que as atualizações de proteção ARP/AI sejam entregues e ["automaticamente ou manualmente"](#) instaladas.

## Informações relacionadas

- ["Atualizar ARP/AI"](#)

# Atualize a proteção Autonomous ransomware com AI (ARP/AI)

Para manter a proteção atualizada contra as ameaças mais recentes de ransomware, o ARP/AI oferece atualizações automáticas que ocorrem fora dos quadros regulares de liberação do ONTAP.

A partir do ONTAP 9.16,1, as atualizações de segurança para ARP/AI estão disponíveis em downloads de software do Gerenciador de sistema, além de atualizações de sistema e firmware. Se o cluster do ONTAP já estiver inscrito no "[atualizações automáticas de sistema e firmware](#)", você será notificado automaticamente quando as atualizações de segurança ARP/AI estiverem disponíveis. Você também pode alterar [atualizar preferências](#) para que o ONTAP instale as atualizações de segurança automaticamente.

Se desejar [Atualizar manualmente ARP/AI](#), você pode baixar atualizações do site de suporte da NetApp e instalá-las usando o Gerenciador do sistema.



O recurso ARP/AI atualmente suporta apenas nas. Embora o recurso de atualização automática exiba a disponibilidade de novos arquivos de segurança para implantação no System Manager, essas atualizações são aplicáveis apenas à proteção da carga de trabalho nas.

## Sobre esta tarefa

Para o ONTAP 9.16,1 e posterior, você só pode atualizar o ARP/AI usando o Gerenciador do sistema.

## Selecione uma preferência de atualização para ARP/AI

No System Manager, as definições na página Ativar atualizações automáticas para arquivos de segurança são definidas como `Show notifications` se já estiver registrado em atualizações automáticas de firmware e de sistema. Você pode alterar a configuração de atualização para `Automatically update` se preferir que o ONTAP aplique as atualizações mais recentes automaticamente. Se você usar um site escuro ou preferir executar atualizações manualmente, poderá optar por mostrar notificações ou ignorar automaticamente as atualizações de segurança.

## Antes de começar

Para atualizações automáticas de segurança, "[O AutoSupport e o AutoSupport OnDemand devem ser ativados e o protocolo de transporte deve ser definido como HTTPS](#)".

## Passos

1. No System Manager, clique em **Cluster > Settings > Software updates**.
2. Na seção **atualizações de software**, [→](#)selecione .
3. Na página **atualizações de software**, selecione a guia **todas as outras atualizações**.
4. Selecione a guia **todas as outras atualizações** e clique em **mais**.
5. Selecione **Editar definições de atualização automática**.
6. Na página Configurações de atualização automática, selecione **arquivos de segurança**.
7. Especifique a ação a ser tomada para arquivos de segurança (atualizações ARP/AI).

Você pode optar por atualizar, mostrar notificações ou ignorar atualizações automaticamente.



Para que as atualizações de segurança sejam atualizadas automaticamente, o AutoSupport e o AutoSupport OnDemand devem ser ativados e o protocolo de transporte deve ser definido como HTTPS.

8. Aceite os termos e condições e selecione **Guardar**.

## **Atualize manualmente o ARP/AI com o pacote de segurança mais recente**

Siga o procedimento apropriado, dependendo se você está registrado no Active IQ Unified Manager.



Certifique-se de instalar apenas uma atualização ARP mais recente do que a versão atual para evitar downgrades ARP não intencionais.

## ONTAP 9.16,1 e posterior com Consultor Digital

### Passos

1. No System Manager, vá para **Dashboard**.

Na seção **Saúde**, uma mensagem será exibida se houver atualizações de segurança recomendadas para o cluster.

2. Clique na mensagem de alerta.
3. Ao lado das atualizações de segurança na lista de atualizações recomendadas, selecione **ações**.
4. Clique em **Atualizar** para instalar a atualização imediatamente ou **Agendar** para programá-la para mais tarde.

Se a atualização já estiver agendada, você pode **Editar** ou **Cancelar**.

## ONTAP 9.16,1 e posterior sem Consultor Digital

### Passos

1. Navegue até "[Site de suporte da NetApp](#)" e inicie sessão.
2. Selecione o pacote de segurança que você deseja usar para atualizar seu cluster ARP/AI.
3. Copie os arquivos para um servidor HTTP ou FTP em sua rede ou para uma pasta local que pode ser acessada pelo cluster com ARP/AI.
4. No System Manager, clique em **Cluster > Settings > Software updates**.
5. Em **atualizações de software**, selecione a guia **todas as outras atualizações**.
6. No painel **atualizações manuais**, clique em **Adicionar arquivos de segurança** e adicione os arquivos usando uma destas preferências:
  - **Download do servidor**: Insira o URL do pacote de arquivos de segurança.
  - **Upload do cliente local**: Navegue até o arquivo TGZ baixado.




Certifique-se de que o nome do ficheiro começa com `ontap_security_file_arpai_` e `.tgz` tem como uma extensão de ficheiro.

7. Clique em **Add** para aplicar as atualizações.

## Verifique as atualizações ARP/AI

Para ver um histórico de atualizações automáticas que foram descartadas ou não foram instaladas, faça o seguinte:

1. No System Manager, clique em **Cluster > Settings > Software updates**.
2. Na seção **atualizações de software**,  selecione .
3. Na página **atualizações de software**, selecione a guia **todas as outras atualizações** e clique em **mais**.
4. Selecione **Ver todas as atualizações automáticas**.

### Informações relacionadas

- "[Ativar ARP/AI](#)"

- ["Assinaturas de e-mail para atualizações de software"](#)

## Mude para o modo ARP ativo após um período de aprendizagem

Para a proteção autônoma contra ransomware (ARP) 9.15.1 e anterior ou ARP em execução com volumes FlexGroup, alterne manualmente ou automaticamente um volume habilitado para ARP do modo de aprendizado para o modo ativo. Depois que o ARP tiver concluído uma execução de modo de aprendizagem de um mínimo recomendado de 30 dias, você pode alternar manualmente para o modo ativo. A partir do ONTAP 9.13,1, o ARP determina automaticamente o intervalo ideal do período de aprendizagem e automatiza o switch, que pode ocorrer antes de 30 dias.

Se você estiver usando ARP em volumes FlexVol com ONTAP 9.16,1 ou posterior, a funcionalidade ARP/AI não requer um período de aprendizado e o modo ativo é selecionado por padrão.



Nos volumes existentes, os modos de aprendizagem e ativos aplicam-se apenas a dados recém-gravados, não a dados já existentes no volume. Os dados existentes não são digitalizados e analisados, porque as características do tráfego de dados normal anterior são assumidas com base nos novos dados depois que o volume é ativado para ARP.

### Mude manualmente para o modo ativo após o período de aprendizagem

Para ONTAP 9.10,1 para 9.15.1 e ARP com volumes FlexGroup, você pode fazer a transição manualmente do modo de aprendizado ARP para o modo ativo usando o Gerenciador de sistema ou a CLI do ONTAP.

## System Manager

### Passos

1. Selecione **armazenamento > volumes** e, em seguida, selecione o volume que está pronto para o modo ativo.
2. Na guia **Segurança** da visão geral **volumes**, selecione **mudar para o modo ativo** na caixa Anti-ransomware.
3. Você pode verificar o estado ARP do volume na caixa **Anti-ransomware**.

## CLI

### Passos

1. Quando o período de aprendizagem terminar, modifique o volume protegido para mudar para o modo ativo se ainda não tiver sido feito automaticamente:

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

Você também pode alternar para o modo ativo com o comando modificar volume:

```
volume modify -volume <vol_name> -vserver <svm_name> -anti-ransomware-state  
active
```

2. Verifique o estado ARP do volume.

```
security anti-ransomware volume show
```

## Mudança automática do modo de aprendizagem para o modo ativo

A partir do ONTAP 9.13.1, a aprendizagem adaptável foi adicionada à análise ARP e a mudança do modo de aprendizagem para o modo ativo é feita automaticamente. A decisão autônoma do ARP de alternar automaticamente do modo de aprendizado para o modo ativo é baseada nas configurações das seguintes opções:

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent  
-anti-ransomware-auto-switch-duration-without-new-file-extension  
-anti-ransomware-auto-switch-minimum-learning-period  
-anti-ransomware-auto-switch-minimum-file-count  
-anti-ransomware-auto-switch-minimum-file-extension
```

Após 30 dias de aprendizagem, um volume é automaticamente alterado para o modo ativo, mesmo que uma ou mais destas condições não estejam satisfeitas. Ou seja, se o interruptor automático estiver ativado, o volume muda para o modo ativo após um máximo de 30 dias. O valor máximo de 30 dias é fixo e não modificável.

Para obter mais informações sobre opções de configuração ARP, incluindo valores padrão, consulte "[Referência do comando ONTAP](#)".

# Pausar a proteção Autonomous ransomware para excluir eventos de workload da análise

Se você está esperando eventos de carga de trabalho incomuns, você pode suspender e retomar temporariamente a análise ARP (Autonomous ransomware Protection) a qualquer momento.

A partir do ONTAP 9.13,1, você pode ativar a verificação multi-admin (MAV) para que dois ou mais administradores de usuário autenticados sejam necessários para pausar o ARP.

["Saiba mais sobre o MAV"](#).

## Sobre esta tarefa

Durante uma pausa ARP, nenhum evento é registrado nem nenhuma ação para novas gravações. No entanto, a operação de análise continua para logs anteriores em segundo plano.



Não use a função de desativação ARP para pausar a análise. Isso desativa o ARP no volume e todas as informações existentes sobre o comportamento da carga de trabalho aprendida são perdidas. Isso exigiria um reinício do período de aprendizagem.

## Passos

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para pausar o ARP.

## System Manager

1. Selecione **armazenamento > volumes** e, em seguida, selecione o volume em que deseja pausar ARP.
2. Na guia **Segurança** da visão geral dos volumes, selecione **Pausa anti-ransomware** na caixa **Anti-ransomware**.



A partir do ONTAP 9.13,1, se você estiver usando MAV para proteger suas configurações ARP, a operação de pausa solicitará que você obtenha a aprovação de um ou mais administradores adicionais. "A aprovação deve ser recebida de todos os administradores" Associado ao grupo de aprovação MAV ou à operação falhará.

## CLI

1. Pausar ARP em um volume:

```
security anti-ransomware volume pause -vserver svm_name -volume vol_name
```

2. Para retomar o processamento, use o resume comando:

```
security anti-ransomware volume resume -vserver svm_name -volume vol_name
```

3. Se você estiver usando MAV (disponível com ARP começando com ONTAP 9.13,1) para proteger suas configurações ARP, a operação de pausa solicitará que você obtenha a aprovação de um ou mais administradores adicionais. A aprovação deve ser recebida de todos os administradores associados ao grupo de aprovação MAV ou a operação falhará.

Se você estiver usando MAV e uma operação de pausa esperada precisar de aprovações adicionais, cada aprovador de grupo MAV faz o seguinte:

- a. Mostrar o pedido:

```
security multi-admin-verify request show
```

- b. Aprovar a solicitação:

```
security multi-admin-verify request approve -index[number returned from show request]
```

A resposta para o último aprovador de grupo indica que o volume foi modificado e o estado de ARP está pausado.

Se você estiver usando MAV e for um aprovador de grupo MAV, poderá rejeitar uma solicitação de operação de pausa:

```
security multi-admin-verify request veto -index[number returned from show request]
```



# Gerencie os parâmetros de detecção de ataques da proteção autônoma contra ransomware com o ONTAP

A partir do ONTAP 9.11,1, você pode modificar os parâmetros para a detecção de ransomware em um volume específico com a proteção autônoma ativada e relatar um aumento conhecido como atividade de arquivo normal. Ajustar os parâmetros de detecção ajuda a melhorar a precisão dos relatórios com base na sua carga de trabalho de volume específica.

## Como a detecção de ataque funciona

Quando o Autonomous ransomware Protection (ARP) está no modo de aprendizado, ele desenvolve valores de linha de base para comportamentos de volume. Estas são entropia, extensões de arquivo e, a partir de ONTAP 9.11,1, IOPS. Essas linhas de base são usadas para avaliar ameaças de ransomware. Para obter mais informações sobre esses critérios, [O que o ARP detecta](#) consulte .

No ONTAP 9.10,1, o ARP emite um aviso se detectar ambas as seguintes condições:

- Mais de 20 arquivos com extensões de arquivo não observadas anteriormente no volume
- Dados de alta entropia

A partir do ONTAP 9.11,1, o ARP emite um aviso de ameaça se *somente* uma condição for atendida. Por exemplo, se mais de 20 arquivos com extensões de arquivo que não foram observadas anteriormente no volume forem observados dentro de um período de 24 horas, o ARP irá categorizar isso como uma ameaça *independentemente* da entropia observada. Os valores de 24 horas e 20 arquivos são padrões, que podem ser modificados.



Para reduzir o número elevado de alertas falsos positivos, aceda a **armazenamento > volumes > Segurança > Configurar características da carga de trabalho** e desative **Monitorizar novos tipos de ficheiros**. Esta configuração é desativada por padrão no ONTAP 9.14,1 P7, 9.15.1 P1 e 9.16.1 RC e posterior.

A partir do ONTAP 9.14,1, você pode configurar alertas quando o ARP observa uma nova extensão de arquivo e quando o ARP cria um snapshot. Para obter mais informações, [\[modify-alerts\]](#) consulte .

Certos volumes e workloads exigem parâmetros de detecção diferentes. Por exemplo, seu volume habilitado para ARP pode hospedar vários tipos de extensões de arquivo, caso em que você pode querer modificar a contagem de limite para extensões de arquivo nunca antes vistas para um número maior do que o padrão de 20 ou desativar avisos baseados em extensões de arquivo nunca antes vistas. A partir do ONTAP 9.11,1, você pode modificar os parâmetros de detecção de ataque para que eles se ajustem melhor às suas cargas de trabalho específicas.

## Modificar parâmetros de detecção de ataque

Dependendo dos comportamentos esperados do seu volume habilitado para ARP, você pode querer modificar os parâmetros de detecção de ataque.

### Passos

1. Veja os parâmetros de detecção de ataque existentes:

```
security anti-ransomware volume attack-detection-parameters show -vserver
```

```
<svm_name> -volume <volume_name>
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume voll

Vserver Name : vs1
Volume Name : voll
Is Detection Based on High Entropy Data Rate? : true
Is Detection Based on Never Seen before File Extension? : true
Is Detection Based on File Create Rate? : true
Is Detection Based on File Rename Rate? : true
Is Detection Based on File Delete Rate? : true
Is Detection Relaxing Popular File Extensions? : true
High Entropy Data Surge Notify Percentage : 100
File Create Rate Surge Notify Percentage : 100
File Rename Rate Surge Notify Percentage : 100
File Delete Rate Surge Notify Percentage : 100
Never Seen before File Extensions Count Notify Threshold : 20
Never Seen before File Extensions Duration in Hour : 24
```

2. Todos os campos mostrados são modificáveis com valores booleanos ou inteiros. Para modificar um campo, use o `security anti-ransomware volume attack-detection-parameters modify` comando.

Saiba mais sobre `security anti-ransomware volume attack-detection-parameters modify` o ["Referência do comando ONTAP"](#) na .

## Relatar surtos conhecidos

O ARP continua a modificar os valores da linha de base para os parâmetros de detecção, mesmo no modo ativo. Se você souber de picos em sua atividade de volume, picos de uma vez ou um surto que é característico de um novo normal, você deve denunciá-los como seguros. Relatar manualmente esses picos como seguros ajuda a melhorar a precisão das avaliações de ameaças da ARP.

### Relatar um surto único

1. Se um surto único estiver ocorrendo em circunstâncias conhecidas e você quiser que o ARP relate um aumento semelhante em circunstâncias futuras, limpe o aumento do comportamento da carga de trabalho:

```
security anti-ransomware volume workload-behavior clear-surge -vserver
<svm_name> -volume <volume_name>
```

### Modifique a oscilação da linha de base

1. Se um surto relatado deve ser considerado comportamento normal da aplicação, reporte o surto como tal para modificar o valor de oscilação da linha de base.

```
security anti-ransomware volume workload-behavior update-baseline-from-surge
-vserver <svm_name> -volume <volume_name>
```

## Configurar alertas ARP

A partir do ONTAP 9.14,1, o ARP permite especificar alertas para dois eventos ARP:

- Observação de nova extensão de arquivo em um volume
- Criação de um instantâneo ARP

Os alertas desses dois eventos podem ser definidos em volumes individuais ou em toda a SVM. Se você ativar os alertas para o SVM, as configurações de alerta serão herdadas apenas por volumes criados após a ativação do alerta. Por padrão, os alertas não são ativados em nenhum volume.

Os alertas de eventos podem ser controlados com verificação multi-admin. Para obter mais informações, [Verificação multi-admin com volumes protegidos com ARP](#) consulte .

## System Manager

### Definir alertas para um volume

1. Navegue até **volumes**. Selecione o volume individual para o qual pretende modificar as definições.
2. Selecione a guia **Segurança** e, em seguida, **Configurações de Segurança de Eventos**.
3. Para receber alertas para **Nova extensão de arquivo detetada** e **instantâneo ransomware criado**, selecione o menu suspenso sob o título **gravidade**. Modifique a configuração de **não gerar evento** para **Aviso**.
4. Selecione **Guardar**.

### Definir alertas para um SVM

1. Navegue até **Storage VM** e selecione o SVM para o qual você deseja ativar as configurações.
2. Sob o título **Segurança**, localize o cartão **Anti-ransomware**. Selecione **⋮**, em seguida, **Editar gravidade do evento ransomware**.
3. Para receber alertas para **Nova extensão de arquivo detetada** e **instantâneo ransomware criado**, selecione o menu suspenso sob o título **gravidade**. Modifique a configuração de **não gerar evento** para **Aviso**.
4. Selecione **Guardar**.

## CLI

### Definir alertas para um volume

- Para definir alertas para uma nova extensão de arquivo:

```
security anti-ransomware volume event-log modify -vserver <svm_name> -is
-enabled-on-new-file-extension-seen true
```

- Para definir alertas para a criação de um instantâneo ARP:

```
security anti-ransomware volume event-log modify -vserver <svm_name> -is
-enabled-on-snapshot-copy-creation true
```

- Confirme suas configurações com o `anti-ransomware volume event-log show` comando.

### Definir alertas para um SVM

- Para definir alertas para uma nova extensão de arquivo:

```
security anti-ransomware vserver event-log modify -vserver <svm_name> -is
-enabled-on-new-file-extension-seen true
```

- Para definir alertas para a criação de um instantâneo ARP:

```
security anti-ransomware vserver event-log modify -vserver <svm_name> -is
-enabled-on-snapshot-copy-creation true
```

- Confirme suas configurações com o `security anti-ransomware vserver event-log show` comando.

## Informações relacionadas

- ["Entenda os ataques Autonomous ransomware Protection e o snapshot Autonomous ransomware Protection"](#).

## Responder a atividades anormais

Quando o Autonomous ransomware Protection (ARP) deteta atividade anormal em um volume protegido, ele emite um aviso. Você deve avaliar a notificação para determinar se a atividade é aceitável (falso positivo) ou se um ataque parece mal-intencionado. Depois de categorizar o ataque, você pode limpar o aviso e avisos sobre arquivos suspeitos.

Quando o ONTAP deteta uma anomalia, também cria ["Um instantâneo ARP"](#) o volume para criar o melhor ponto de recuperação. Os instantâneos ARP são retidos por dois a cinco dias por padrão.

Quando você categoriza um ataque, esses snapshots ARP são excluídos instantaneamente (ONTAP 9.15.1 e anteriores) ou retidos por um período abreviado iniciado pela operação de categorização (ONTAP 9.16.1 e posterior).



A partir do ONTAP 9.11.1, você pode modificar o [definições de retenção](#) para instantâneos ARP.

### Sobre esta tarefa

ARP exibe uma lista de arquivos suspeitos quando deteta qualquer combinação de alta entropia de dados, atividade de volume anormal com criptografia de dados e extensões de arquivos incomuns.

Quando o aviso ARP for emitido, responda designando a atividade do arquivo de duas maneiras:

- **Falso positivo**

O tipo de arquivo identificado é esperado em sua carga de trabalho e pode ser ignorado.

- **Possível ataque de ransomware**

O tipo de arquivo identificado é inesperado em sua carga de trabalho e deve ser Tratado como um potencial ataque.

Em ambos os casos, a monitorização normal é retomada após a atualização e limpeza dos avisos. O ARP Registra sua avaliação no perfil de avaliação de ameaças, usando sua escolha para monitorar atividades subsequentes de arquivos.

No caso de um ataque suspeito, você deve determinar se é um ataque, responder a ele, se for, e restaurar dados protegidos antes de limpar os avisos. ["Saiba mais sobre como se recuperar de um ataque de ransomware"](#).



Se você restaurar um volume inteiro, não há avisos para limpar.

### Antes de começar

O ARP deve estar em execução no modo ativo.

### Passos

Use o Gerenciador de sistema ou a CLI do ONTAP para responder a atividades anormais.

## System Manager


1. Quando receber uma notificação de "atividade anormal", siga o link. Alternativamente, navegue até a guia **Security** da visão geral **volumes**.

Os avisos são exibidos no painel **Visão geral** do menu **Eventos**.

2. Quando for apresentada uma mensagem sobre a detecção de atividade de volume anormal, consulte os tipos de ficheiro suspeitos.

Na guia **Segurança**, selecione a opção para revisar os tipos de arquivo suspeitos.

3. Na caixa de diálogo **tipos de arquivo suspeitos**, examine cada tipo de arquivo e marque-o como "Falso positivo" ou "ataque de potencial ransomware".

Se selecionou este valor...	Tome esta ação...
Falso positivo	<p>a. Selecione <b>Update</b> e <b>Clear Suspect File Types</b> para gravar sua decisão.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> A partir do ONTAP 9.13,1, se você estiver usando o MAV para proteger suas configurações ARP, a operação clara suspeita solicitará que você obtenha a aprovação de um ou mais administradores adicionais. "<a href="#">A aprovação deve ser recebida de todos os administradores</a>" Associado ao grupo de aprovação MAV ou à operação falhará.</div> <p>Esta ação limpa avisos sobre ficheiros suspeitos. Em seguida, o ARP retoma a monitorização normal do volume. Para o ONTAP 9.15.1 e versões anteriores, depois de limpar os tipos de arquivo suspeitos, os snapshots ARP são excluídos automaticamente. Para ARP/AI no ONTAP 9.16.1 e posterior, os snapshots ARP são excluídos automaticamente após um período de retenção abreviado acionado pela operação de categorização.</p>
Potencial ataque de ransomware	<p>a. Responder ao ataque e "<a href="#">restaurar dados protegidos</a>".</p> <p>b. Selecione <b>Update</b> e <b>Clear Suspect File Types</b> para gravar sua decisão e retomar o monitoramento ARP normal.</p> <p>Esta ação limpa o relatório de ataque. Não há avisos de tipo de arquivo suspeitos para limpar se você restaurou um volume inteiro. Para o ONTAP 9.15.1 e versões anteriores, depois de restaurar um volume, os instantâneos ARP são automaticamente excluídos. Para ARP/AI no ONTAP 9.16.1 e posterior, os snapshots ARP são excluídos automaticamente após um período de retenção abreviado acionado pela operação de categorização.</p>

## CLI

1. Quando receber uma notificação de um ataque de ransomware suspeito, verifique a hora e a

gravidade do ataque:

```
security anti-ransomware volume show -vserver <svm_name> -volume  
<vol_name>
```

Saída da amostra:

```
Vserver Name: vs0  
Volume Name: voll  
State: enabled  
Attack Probability: moderate  
Attack Timeline: 9/14/2021 01:03:23  
Number of Attacks: 1
```

Você também pode verificar mensagens EMS:

```
event log show -message-name callhome.arw.activity.seen
```

2. Gere um relatório de ataque e anote o local de saída:

```
security anti-ransomware volume attack generate-report -vserver  
<svm_name> -volume <vol_name> -dest-path <[svm_name:]vol_name/[sub-  
dir-name]>`
```

Exemplo de comando:

```
security anti-ransomware volume attack generate-report -vserver vs0  
-volume voll -dest-path vs0:voll
```

Saída da amostra:

```
Report "report_file_vs0_voll_14-09-2021_01-21-08" available at path  
"vs0:voll/"
```

3. Exibir o relatório em um sistema de cliente admin. Por exemplo:

```
cat report_file_vs0_voll_14-09-2021_01-21-08
```

4. Execute uma das seguintes ações com base na avaliação das extensões de arquivo:

- Falso positivo

Execute o seguinte comando para Registrar sua decisão, adicionando a nova extensão à lista dos permitidos e retomar o monitoramento normal Autonomous ransomware Protection:

```
anti-ransomware volume attack clear-suspect -vserver <svm_name>
-volume <vol_name> [<extension identifiers>] -false-positive true
```

Use o seguinte parâmetro opcional para identificar apenas extensões específicas como falsos positivos:

- [-extension <text>, ... ]: Extensões de ficheiro

```
`clear-suspect`Esta operação limpa avisos sobre ficheiros
suspeitos. Em seguida, o ARP retoma a monitorização normal do
volume. Para o ONTAP 9.15.1 e versões anteriores, depois de
limpar os tipos de arquivo suspeitos, os snapshots ARP são
excluídos automaticamente. Para ARP/AI no ONTAP 9.16.1 e
posterior, os snapshots ARP são excluídos automaticamente após
um período de retenção abreviado acionado pela operação de
categorização.
```

- Possível ataque de ransomware

Responder ao ataque e "[Recupere dados do instantâneo de backup criado pelo ARP](#)". Depois que os dados forem recuperados, execute o seguinte comando para Registrar sua decisão e retomar o monitoramento ARP normal:

```
anti-ransomware volume attack clear-suspect -vserver <svm_name>
-volume <vol_name> [<extension identifiers>] -false-positive
false
```

Use o seguinte parâmetro opcional para identificar apenas extensões específicas como possíveis ransomware:

- [-extension <text>, ... ]: Extensão do ficheiro

```
`clear-suspect`Esta operação limpa o relatório de ataque. Não
há avisos de tipo de arquivo suspeitos para limpar se você
restaurou um volume inteiro. Para o ONTAP 9.15.1 e versões
anteriores, depois de restaurar um volume, os instantâneos ARP
são automaticamente excluídos. Para ARP/AI no ONTAP 9.16.1 e
posterior, os snapshots ARP são excluídos automaticamente após
um período de retenção abreviado acionado pela operação de
categorização.
```



5. Se você estiver usando MAV e uma operação esperada `clear-suspect` precisar de aprovações adicionais, cada aprovador de grupo MAV deve:

a. Mostrar o pedido:

```
security multi-admin-verify request show
```

b. Aprovar a solicitação para retomar o monitoramento normal anti-ransomware:

```
security multi-admin-verify request approve -index[<number  
returned from show request>]
```

A resposta para o último aprovador do grupo indica que o volume foi modificado e um falso positivo é registrado.

6. Se você estiver usando MAV e for um aprovador de grupo MAV, também poderá rejeitar uma solicitação clara e suspeita:

```
security multi-admin-verify request veto -index[<number returned  
from show request>]
```

### Informações relacionadas

- ["KB: Entendendo os ataques Autonomous ransomware Protection e o snapshot Autonomous ransomware Protection"](#).
- ["Modificar opções de instantâneos automáticos"](#).

## Restaure os dados após um ataque de ransomware

O Autonomous ransomware Protection (ARP) cria snapshots nomeados `Anti_ransomware_backup` quando detecta uma potencial ameaça de ransomware. Você pode usar um desses snapshots ARP ou outro snapshot do volume para restaurar dados.

### Sobre esta tarefa

Se o volume tiver relações SnapMirror, replique manualmente todas as cópias espelhadas do volume imediatamente após a restauração a partir de um snapshot. Não fazer isso pode resultar em cópias espelhadas inutilizáveis que devem ser excluídas e recriadas.

Para restaurar a partir de um instantâneo diferente do `Anti_ransomware_backup` instantâneo após um ataque do sistema ter sido identificado, primeiro você deve liberar o instantâneo ARP.

Se nenhum ataque do sistema foi relatado, você deve primeiro restaurar a partir do `Anti_ransomware_backup` instantâneo e, em seguida, concluir uma restauração subsequente do volume a partir do instantâneo de sua escolha.

**Passos**

Você pode usar o Gerenciador do sistema ou a CLI do ONTAP para restaurar seus dados.

## System Manager

### Restaurar após um ataque ao sistema

1. Para restaurar a partir do instantâneo ARP, passe para a etapa dois. Para restaurar a partir de um instantâneo anterior, primeiro é necessário liberar o bloqueio no instantâneo ARP.
  - a. Selecione **armazenamento > volumes**.
  - b. Selecione **Segurança** e depois **Exibir tipos de arquivos suspeitos**.
  - c. Marque os arquivos como "possível ataque de ransomware".
  - d. Selecione **Update** e **Clear Suspect File Types**.

2. Exibir os instantâneos em volumes:


Selecione **armazenamento > volumes** e, em seguida, selecione o volume e **cópias Snapshot**.

3. Selecione  ao lado do instantâneo que deseja restaurar e depois **Restaurar**.

### Restaurar se um ataque do sistema não foi identificado

1. Exibir os instantâneos em volumes:

Selecione **armazenamento > volumes** e, em seguida, selecione o volume e **cópias Snapshot**.

2. Selecione -os escolha o `Anti_ransomware_backup` instantâneo.
3. Selecione **Restaurar**.
4. Retorne ao menu **cópias instantâneas** e escolha o instantâneo que deseja usar. Selecione **Restaurar**.

## CLI

### Restaurar após um ataque ao sistema

1. Para restaurar a partir do instantâneo ARP, passe para a etapa dois. Para restaurar dados de instantâneos anteriores, você deve liberar o bloqueio no instantâneo ARP.



Só é necessário liberar o SnapLock anti-ransomware antes de restaurar a partir de snapshots anteriores se você estiver usando o volume `snap restore` comando como descrito abaixo. Se você estiver restaurando dados usando o FlexClone, a Restauração Snap de Arquivo único ou outros métodos, isso não será necessário.

Marque o ataque como um possível ataque de ransomware (`-false-positive false`) e limpe os arquivos suspeitos (`clear-suspect`):

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive false
```

Use um dos seguintes parâmetros para identificar as extensões:

`[-seq-no integer]` Número de sequência do arquivo na lista suspeita.

`[-extension text, ... ]` Extensões de arquivo

`[-start-time date_time -end-time date_time]` começando e terminando tempos para o intervalo de arquivos a ser limpo, no formulário "MM/DD/AAAA HH:MM:SS".

2. Listar as cópias Snapshot em um volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

O exemplo a seguir mostra as cópias Snapshot vol1 no :

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

### 3. Restaure o conteúdo de um volume a partir de uma cópia Snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot  
<snapshot>
```

O exemplo a seguir restaura o conteúdo vol1 de :

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010
```

### Restaure se um ataque do sistema não foi identificado

#### 1. Listar as cópias Snapshot em um volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

O exemplo a seguir mostra as cópias Snapshot vol1 no :

```
clus1::> volume snapshot show -vserver vs1 -volume voll
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	voll	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

```
7 entries were displayed.
```

## 2. Restaure o conteúdo de um volume a partir de uma cópia Snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot  
<snapshot>
```

O exemplo a seguir restaura o conteúdo voll de :

```
cluster1::> volume snapshot restore -vserver vs0 -volume voll  
-snapshot daily.2013-01-25_0010
```

## 3. Repita as etapas 1 e 2 para restaurar o volume usando o instantâneo de desejo.

### Informações relacionadas

- ["KB: Prevenção e recuperação de ransomware no ONTAP"](#)

## Modificar opções para instantâneos automáticos

A partir do ONTAP 9.11,1, você pode usar a CLI para controlar as configurações de retenção de snapshots ARP (Autonomous ransomware Protection) que são gerados automaticamente em resposta a ataques suspeitos de ransomware.

### Antes de começar

Você só pode modificar as opções de instantâneos ARP em um nó SVM e não em outro ["Tipos de SVM"](#).

### Passos

1. Mostrar todas as definições atuais de instantâneos ARP:

```
options -option-name arw*
```



Para ver a página de manual, introduza `man options` na CLI do ONTAP.


## 2. Mostrar as definições atuais de instantâneos ARP selecionadas:

```
options -option-name <arw_setting_name>
```

## 3. Modificar as definições de instantâneos ARP:

```
options -option-name <arw_setting_name> -option-value  
<arw_setting_value>
```

As seguintes configurações são modificáveis:

Definição ARW	Descrição
<code>arw.snap.max.count</code>	Especifica o número máximo de instantâneos ARP que podem existir em um volume a qualquer momento. Cópias mais antigas são excluídas para garantir que o número total de snapshots ARP esteja dentro desse limite especificado.
<code>arw.snap.create.in terval.hours</code>	Especifica o intervalo <i>em horas</i> entre instantâneos ARP. Um novo snapshot ARP é criado quando um ataque baseado em entropia de dados é suspeito e o snapshot ARP criado mais recentemente é mais antigo do que o intervalo especificado.
<code>arw.snap.normal.re tain.interval.hour s</code>	Especifica a duração <i>em horas</i> para a qual um instantâneo ARP é retido. Quando um instantâneo ARP atinge o limite de retenção, qualquer outra cópia de instantâneos ARP criada antes de ser excluída. Não pode existir mais do que um instantâneo ARP mais antigo do que o limite de retenção.
<code>arw.snap.max.retai n.interval.days</code>	Especifica a duração máxima <i>in Days</i> para a qual um instantâneo ARP pode ser retido. Qualquer snapshot ARP com mais de uma duração é excluído quando não há nenhum ataque relatado no volume.   O intervalo máximo de retenção para instantâneos ARP é ignorado se uma ameaça moderada for detetada. O snapshot ARP criado em resposta à ameaça é retido até que você tenha respondido à ameaça. Quando você marca uma ameaça como um falso positivo, o ONTAP excluirá os snapshots ARP para o volume.

Definição ARW	Descrição
<code>arw.snap.create.interval.hours.post.max.count</code>	<p>Especifica o intervalo <i>em horas</i> entre instantâneos ARP quando o volume já contém o número máximo de instantâneos ARP. Quando o número máximo é atingido, um instantâneo ARP é excluído para abrir espaço para uma nova cópia. A nova velocidade de criação de instantâneos ARP pode ser reduzida para reter a cópia mais antiga usando esta opção. Se o volume já contiver o número máximo de instantâneos ARP, o intervalo especificado nesta opção será usado para a próxima criação de instantâneos ARP, em vez <code>arw.snap.create.interval.hours</code> de .</p>
<code>arw.surge.snap.interval.days</code>	<p>Especifica o intervalo <i>in Days</i> entre instantâneos ARP criados em resposta a picos de e/S. O ONTAP cria uma cópia de impulso de snapshot ARP quando há um aumento no tráfego de e/S e o último snapshot ARP criado é mais antigo do que esse intervalo especificado. Esta opção também especifica o período de retenção <i>in day</i> para um instantâneo de pico ARP.</p>
<code>arw.snap.new.extns.interval.hours</code>	<p>Esta opção especifica o intervalo <i>em horas</i> entre os instantâneos ARP criados quando uma nova extensão de arquivo é detetada. Um novo snapshot ARP é criado quando uma nova extensão de arquivo é observada; o snapshot anterior criado ao observar uma nova extensão de arquivo é mais antigo do que esse intervalo especificado. Em uma carga de trabalho que frequentemente cria novas extensões de arquivo, esse intervalo ajuda a controlar a frequência dos snapshots ARP. Essa opção existe independente do <code>arw.snap.create.interval.hours</code>, que especifica o intervalo para snapshots ARP baseados em entropia de dados.</p>

## 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.