



Planeie a configuração do motor externo FPolicy

ONTAP 9

NetApp
January 17, 2025

Índice

- Planeie a configuração do motor externo FPolicy 1
 - Planeie a configuração do motor externo FPolicy 1
 - Informações adicionais sobre a configuração de mecanismos externos FPolicy para usar conexões autenticadas SSL 7
 - Os certificados não são replicados nas relações de recuperação de desastres do SVM com uma configuração que não preserve ID 8
 - Restrições para mecanismos externos de FPolicy com escopo de cluster com configurações de recuperação de desastres MetroCluster e SVM 9
- Preencha a folha de cálculo de configuração do motor externo FPolicy 9

Planeie a configuração do motor externo FPolicy

Planeie a configuração do motor externo FPolicy

Antes de configurar o mecanismo externo FPolicy, você deve entender o que significa criar um mecanismo externo e quais parâmetros de configuração estão disponíveis. Essas informações ajudam você a determinar quais valores definir para cada parâmetro.

Informações que são definidas ao criar o mecanismo externo FPolicy

A configuração do mecanismo externo define as informações que o FPolicy precisa para fazer e gerenciar conexões com os servidores FPolicy externos, incluindo o seguinte:

- Nome do SVM
- Nome do motor
- Os endereços IP dos servidores FPolicy primário e secundário e o número da porta TCP a serem usados ao fazer a conexão com os servidores FPolicy
- Se o tipo de motor é assíncrono ou síncrono
- Se o formato do motor é `xml` ou `protobuf`

Começando com ONTAP 9.15,1, você pode usar o `protobuf` formato do motor. Quando definido como `protobuf`, as mensagens de notificação são codificadas de forma binária usando o Google Protobuf. Antes de definir o formato do mecanismo como `protobuf`, certifique-se de que o servidor FPolicy também suporta `protobuf` a desserialização.

Uma vez que o formato `protobuf` é suportado a partir de ONTAP 9.15,1, você deve considerar o formato externo do motor antes de reverter para uma versão anterior do ONTAP. Se você reverter para uma versão anterior do ONTAP 9.15,1, trabalhe com seu parceiro FPolicy para:

- Altere cada formato do motor de `protobuf` para `xml`
- Elimine os motores com um formato de motor de `protobuf`
- Como autenticar a conexão entre o nó e o servidor FPolicy

Se você optar por configurar a autenticação SSL mútua, você também deve configurar parâmetros que fornecem informações de certificado SSL.

- Como gerir a ligação utilizando várias definições avançadas de privilégios


Isso inclui parâmetros que definem coisas como valores de tempo limite, valores de repetição, valores de `keep-alive`, valores máximos de solicitação, valores de tamanho de buffer enviados e recebidos e valores de tempo limite da sessão.

O `vserver fpolicy policy external-engine create` comando é usado para criar um mecanismo externo FPolicy.

Quais são os parâmetros básicos do motor externo

Você pode usar a seguinte tabela de parâmetros básicos de configuração do FPolicy para ajudá-lo a Planejar

sua configuração:

Tipo de informação	Opção
<p>SVM</p> <p>Especifica o nome do SVM que você deseja associar a esse mecanismo externo.</p> <p>Cada configuração de FPolicy é definida em um único SVM. O mecanismo externo, o evento de política, o escopo da política e a política que se combinam para criar uma configuração de política FPolicy devem estar associados ao mesmo SVM.</p>	<pre>-vserver vserver_name</pre>
<p>Nome do motor</p> <p>Especifica o nome a ser atribuído à configuração externa do motor. Você deve especificar o nome do mecanismo externo mais tarde quando criar a política FPolicy. Isto associa o motor externo à política.</p> <p>O nome pode ter até 256 caracteres.</p> <p> O nome deve ter até 200 caracteres se estiver configurando o nome do mecanismo externo em uma configuração de recuperação de desastres do MetroCluster ou SVM.</p> <p>O nome pode conter qualquer combinação dos seguintes caracteres de intervalo ASCII:</p> <ul style="list-style-type: none">• a através z• A através Z• 0 através 9• "»_", "-", and "»."	<pre>-engine-name engine_name</pre>
<p>Servidores FPolicy primários</p> <p>Especifica os servidores FPolicy primários para os quais o nó envia notificações para uma determinada política FPolicy. O valor é especificado como uma lista delimitada por vírgulas de endereços IP.</p> <p>Se mais de um endereço IP de servidor primário for especificado, cada nó no qual o SVM participa criará uma conexão de controle para cada servidor FPolicy primário especificado no momento em que a diretiva é ativada. Se você configurar vários servidores FPolicy primários, as notificações serão enviadas para os servidores FPolicy de forma redonda.</p> <p>Se o mecanismo externo for usado em uma configuração de recuperação de desastres do MetroCluster ou SVM, você deverá especificar os endereços IP dos servidores FPolicy no local de origem como servidores primários. Os endereços IP dos servidores FPolicy no local de destino devem ser especificados como servidores secundários.</p>	<pre>-primary-servers IP_address,...</pre>

<p><i>Número da porta</i></p> <p>Especifica o número da porta do serviço FPolicy.</p>	<p>-port integer</p>
<p><i>Servidores FPolicy secundários</i></p> <p>Especifica os servidores FPolicy secundários para os quais enviar eventos de acesso a arquivos para uma determinada política FPolicy. O valor é especificado como uma lista delimitada por vírgulas de endereços IP.</p> <p>Os servidores secundários são utilizados apenas quando nenhum dos servidores primários é alcançável. As conexões com servidores secundários são estabelecidas quando a diretiva está ativada, mas as notificações são enviadas para servidores secundários somente se nenhum dos servidores primários estiver acessível. Se você configurar vários servidores secundários, as notificações serão enviadas para os servidores FPolicy de forma redonda.</p>	<p>-secondary-servers IP_address,...</p>
<p><i>Tipo de motor externo</i></p> <p>Especifica se o mecanismo externo opera no modo síncrono ou assíncrono. Por padrão, o FPolicy opera no modo síncrono.</p> <p>Quando definido como <i>synchronous</i>, o processamento de solicitação de arquivo envia uma notificação para o servidor FPolicy, mas depois não continua até receber uma resposta do servidor FPolicy. Nesse ponto, o fluxo de solicitação continua ou o processamento resulta em negação, dependendo se a resposta do servidor FPolicy permite a ação solicitada.</p> <p>Quando definido como <i>asynchronous</i>, o processamento de solicitação de arquivo envia uma notificação para o servidor FPolicy e, em seguida, continua.</p>	<p>-extern-engine-type external_engine_type O valor para este parâmetro pode ser um dos seguintes:</p> <ul style="list-style-type: none"> • synchronous • asynchronous
<p><i>Formato externo do motor</i></p> <p>Especifique se o formato do mecanismo externo é xml ou protobuf.</p> <p>Começando com ONTAP 9.15.1, você pode usar o formato do mecanismo protobuf. Quando definido como <i>protobuf</i>, as mensagens de notificação são codificadas em forma binária usando o Google Protobuf. Antes de definir o formato do motor para <i>protobuf</i>, certifique-se de que o servidor FPolicy também suporta a desserialização de <i>protobuf</i>.</p>	<p>- extern-engine-format {protobuf ou xml</p>

<p><i>Opção SSL para comunicação com o servidor FPolicy</i></p> <p>Especifica a opção SSL para comunicação com o servidor FPolicy. Este é um parâmetro obrigatório. Você pode escolher uma das opções com base nas seguintes informações:</p> <ul style="list-style-type: none"> • Quando definido como <code>no-auth</code>, não ocorre autenticação. <p>O link de comunicação é estabelecido através do TCP.</p> <ul style="list-style-type: none"> • Quando definido como <code>server-auth</code>, o SVM autentica o servidor FPolicy usando autenticação de servidor SSL. • Quando definido como <code>mutual-auth</code>, a autenticação mútua ocorre entre o SVM e o servidor FPolicy; o SVM autentica o servidor FPolicy e o servidor FPolicy autentica o SVM. <p>Se você optar por configurar a autenticação SSL mútua, também deverá configurar os <code>-certificate-common-name</code> parâmetros , <code>-certificate-serial</code> e <code>-certificate-ca</code> .</p>	<pre>-ssl-option {no-auth</pre>
<p><code>server-auth</code></p>	<pre>`mutual-auth` Selecione</pre>
<p><i>Certificado FQDN ou nome comum personalizado</i></p> <p>Especifica o nome do certificado usado se a autenticação SSL entre o SVM e o servidor FPolicy estiver configurada. Você pode especificar o nome do certificado como um FQDN ou como um nome comum personalizado.</p> <p>Se você especificar <code>mutual-auth</code> para o <code>-ssl-option</code> parâmetro, será necessário especificar um valor para o <code>-certificate-common-name</code> parâmetro.</p>	<pre>-certificate-common-name text</pre>
<p><i>Número de série do certificado</i></p> <p>Especifica o número de série do certificado usado para autenticação se a autenticação SSL entre o SVM e o servidor FPolicy estiver configurada.</p> <p>Se você especificar <code>mutual-auth</code> para o <code>-ssl-option</code> parâmetro, será necessário especificar um valor para o <code>-certificate-serial</code> parâmetro.</p>	<pre>-certificate-serial text</pre>
<p><i>Autoridade de certificação</i></p> <p>Especifica o nome da CA do certificado usado para autenticação se a autenticação SSL entre o SVM e o servidor FPolicy estiver configurada.</p> <p>Se você especificar <code>mutual-auth</code> para o <code>-ssl-option</code> parâmetro, será necessário especificar um valor para o <code>-certificate-ca</code> parâmetro.</p>	<pre>-certificate-ca text</pre>

Quais são as opções avançadas do motor externo

Você pode usar a seguinte tabela de parâmetros avançados de configuração FPolicy à medida que planeja personalizar sua configuração com parâmetros avançados. Você usa esses parâmetros para modificar o comportamento de comunicação entre os nós de cluster e os servidores FPolicy:

Tipo de informação	Opção
<p><i>Tempo limite para cancelar uma solicitação</i></p> <p>Especifica o intervalo de tempo em horas (h), (m`minutos) ou segundos (`s) que o nó espera por uma resposta do servidor FPolicy.</p> <p>Se o intervalo de tempo limite passar, o nó envia uma solicitação de cancelamento para o servidor FPolicy. O nó então envia a notificação para um servidor FPolicy alternativo. Esse tempo limite ajuda a lidar com um servidor FPolicy que não está respondendo, o que pode melhorar a resposta do cliente SMB/NFS. Além disso, cancelar solicitações após um período de tempo limite pode ajudar a liberar recursos do sistema porque a solicitação de notificação é movida de um servidor FPolicy inativo/ruim para um servidor FPolicy alternativo.</p> <p>O intervalo para este valor é 0 através 100`de . Se o valor estiver definido como `0, a opção será desativada e as mensagens de solicitação de cancelamento não serão enviadas para o servidor FPolicy. A predefinição é 20s.</p>	<p>-reqs-cancel-timeout integer[h</p>
m	s]
<p><i>Tempo limite para abortar uma solicitação</i></p> <p>Especifica o tempo limite em horas (h), (m`minutos) ou segundos (`s) para abortar uma solicitação.</p> <p>O intervalo para este valor é 0 através `200`de .</p>	<p>-reqs-abort-timeout ` `integer[h</p>
m	s]
<p><i>Intervalo para envio de solicitações de status</i></p> <p>Especifica o intervalo em horas (h), minutos (m) ou segundos (s) após o qual uma solicitação de status é enviada ao servidor FPolicy.</p> <p>O intervalo para este valor é 0 através 50`de . Se o valor estiver definido como `0, a opção será desativada e as mensagens de solicitação de status não serão enviadas ao servidor FPolicy. A predefinição é 10s.</p>	<p>-status-req-interval integer[h</p>
m	s]

<p><i>Máximo de solicitações pendentes no servidor FPolicy</i></p> <p>Especifica o número máximo de solicitações pendentes que podem ser enfileiradas no servidor FPolicy.</p> <p>O intervalo para este valor é 1 através 10000`de . A predefinição é `500.</p>	<p>-max-server-reqs integer</p>
<p><i>Tempo limite para desconetar um servidor FPolicy não responsivo</i></p> <p>Especifica o intervalo de tempo em horas (h), (m`minutos) ou segundos (`s) após o qual a conexão com o servidor FPolicy é encerrada.</p> <p>A conexão é encerrada após o período de tempo limite somente se a fila do servidor FPolicy contiver o máximo de solicitações permitidas e nenhuma resposta for recebida dentro do período de tempo limite. O número máximo permitido de solicitações é 50 (o padrão) ou o número especificado pelo max-server-reqs- parâmetro.</p> <p>O intervalo para este valor é 1 através 100`de . A predefinição é `60s.</p>	<p>-server-progress -timeout integer[h</p>
<p>m</p>	<p>s]</p>
<p><i>Intervalo para enviar mensagens keep-alive para o servidor FPolicy</i></p> <p>Especifica o intervalo de tempo em horas (h), (m`minutos) ou segundos (`s) no qual as mensagens keep-alive são enviadas ao servidor FPolicy.</p> <p>As mensagens keep-alive detetam conexões semi-abertas.</p> <p>O intervalo para este valor é 10 através 600`de . Se o valor estiver definido como `0, a opção será desativada e as mensagens de manutenção em tempo real serão impedidas de serem enviadas para os servidores FPolicy. A predefinição é 120s.</p>	<p>-keep-alive-interval-integer[h</p>
<p>m</p>	<p>s]</p>
<p><i>Máximo de tentativas de reconexão</i></p> <p>Especifica o número máximo de vezes que o SVM tenta se reconectar ao servidor FPolicy depois que a conexão foi interrompida.</p> <p>O intervalo para este valor é 0 através 20`de . A predefinição é `5.</p>	<p>-max-connection-retries integer</p>

<p><i>Receive buffer size</i></p> <p>Especifica o tamanho do buffer de recepção do soquete conetado para o servidor FPolicy.</p> <p>O valor padrão é definido como 256 kilobytes (Kb). Quando o valor é definido como 0, o tamanho do buffer de recepção é definido para um valor definido pelo sistema.</p> <p>Por exemplo, se o tamanho padrão do buffer de recebimento do soquete for de 65536 bytes, definindo o valor ajustável como 0, o tamanho do buffer do soquete será definido como 65536 bytes. Você pode usar qualquer valor não padrão para definir o tamanho (em bytes) do buffer de recebimento.</p>	<pre>-recv-buffer-size integer</pre>
<p><i>Enviar tamanho do buffer</i></p> <p>Especifica o tamanho do buffer de envio do soquete conetado para o servidor FPolicy.</p> <p>O valor padrão é definido como 256 kilobytes (Kb). Quando o valor é definido como 0, o tamanho do buffer de envio é definido para um valor definido pelo sistema.</p> <p>Por exemplo, se o tamanho padrão do buffer de envio do soquete for definido como 65536 bytes, definindo o valor ajustável como 0, o tamanho do buffer do soquete será definido como 65536 bytes. Você pode usar qualquer valor não padrão para definir o tamanho (em bytes) do buffer de envio.</p>	<pre>-send-buffer-size integer</pre>
<p><i>Tempo limite para purgar um Session ID durante a reconexão</i></p> <p>Especifica o intervalo em horas (h), minutos (m) ou segundos (s) após o qual um novo Session ID é enviado ao servidor FPolicy durante tentativas de reconexão.</p> <p>Se a conexão entre o controlador de armazenamento e o servidor FPolicy for encerrada e a nova conexão for feita dentro do <code>-session-timeout</code> intervalo, o Session ID antigo será enviado para o servidor FPolicy para que ele possa enviar respostas para notificações antigas.</p> <p>O valor padrão é definido para 10 segundos.</p>	<pre>-session-timeout integer[m][integers]</pre>

Informações adicionais sobre a configuração de mecanismos externos FPolicy para usar conexões autenticadas SSL

Você precisa saber algumas informações adicionais se quiser configurar o mecanismo externo FPolicy para usar SSL ao se conectar a servidores FPolicy.

Autenticação de servidor SSL

Se você optar por configurar o mecanismo externo FPolicy para autenticação de servidor SSL, antes de criar o mecanismo externo, você deverá instalar o certificado público da autoridade de certificação (CA) que assinou o certificado do servidor FPolicy.

Autenticação mútua

Se você configurar mecanismos externos do FPolicy para usar a autenticação mútua SSL ao conectar LIFs de dados da máquina virtual de armazenamento (SVM) a servidores FPolicy externos, antes de criar o mecanismo externo, você deverá instalar o certificado público da CA que assinou o certificado do servidor FPolicy juntamente com o certificado público e o arquivo chave para autenticação do SVM. Não exclua este certificado enquanto nenhuma política FPolicy estiver usando o certificado instalado.

Se o certificado for excluído enquanto o FPolicy estiver usando-o para autenticação mútua ao se conectar a um servidor FPolicy externo, não será possível reativar uma política FPolicy desativada que use esse certificado. A política FPolicy não pode ser reativada nessa situação mesmo que um novo certificado com as mesmas configurações seja criado e instalado no SVM.

Se o certificado tiver sido excluído, você precisará instalar um novo certificado, criar novos mecanismos externos FPolicy que usam o novo certificado e associar os novos mecanismos externos à política FPolicy que você deseja reativar modificando a política FPolicy.

Instale certificados para SSL

O certificado público da CA que é usado para assinar o certificado do servidor FPolicy é instalado usando o `security certificate install` comando com o `-type` parâmetro definido como `client-ca`. A chave privada e o certificado público necessários para a autenticação do SVM são instalados usando o `security certificate install` comando com o `-type` parâmetro definido como `server`.

Os certificados não são replicados nas relações de recuperação de desastres do SVM com uma configuração que não preserve ID

Os certificados de segurança usados para autenticação SSL ao fazer conexões com servidores FPolicy não são replicados para destinos de recuperação de desastres SVM com configurações que não preservem ID. Embora a configuração do mecanismo externo FPolicy na SVM seja replicada, os certificados de segurança não são replicados. Tem de instalar manualmente os certificados de segurança no destino.

Quando você configura a relação de recuperação de desastres SVM, o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), todos os detalhes de configuração do FPolicy serão replicados, incluindo as informações do certificado de segurança. Só tem de instalar os certificados de segurança no destino se definir a opção como `false` (non-ID-Preserve).

Restrições para mecanismos externos de FPolicy com escopo de cluster com configurações de recuperação de desastres MetroCluster e SVM

Você pode criar um mecanismo externo FPolicy com escopo de cluster atribuindo a máquina virtual de armazenamento de cluster (SVM) ao mecanismo externo. No entanto, ao criar um mecanismo externo com escopo de cluster em uma configuração de recuperação de desastres MetroCluster ou SVM, há certas restrições ao escolher o método de autenticação usado pelo SVM para comunicação externa com o servidor FPolicy.

Há três opções de autenticação que você pode escolher ao criar servidores FPolicy externos: sem autenticação, autenticação de servidor SSL e autenticação mútua SSL. Embora não haja restrições ao escolher a opção de autenticação se o servidor FPolicy externo for atribuído a um SVM de dados, há restrições ao criar um mecanismo externo FPolicy com escopo de cluster:

Configuração	Permitido?
Recuperação de desastres MetroCluster ou SVM e um mecanismo externo FPolicy com escopo de cluster sem autenticação (SSL não está configurado)	Sim
Recuperação de desastres MetroCluster ou SVM e um mecanismo externo FPolicy com escopo de cluster com autenticação mútua SSL ou SSL	Não

- Se houver um mecanismo externo FPolicy com escopo de cluster e autenticação SSL e você quiser criar uma configuração de recuperação de desastres do MetroCluster ou SVM, modifique esse mecanismo externo para não usar autenticação ou remover o mecanismo externo antes de criar a configuração de recuperação de desastres do MetroCluster ou SVM.
- Se a configuração de recuperação de desastres do MetroCluster ou SVM já existir, o ONTAP impede que você crie um mecanismo externo FPolicy com escopo de cluster com autenticação SSL.

Preencha a folha de cálculo de configuração do motor externo FPolicy

Você pode usar esta Planilha para Registrar os valores que você precisa durante o processo de configuração do mecanismo externo FPolicy. Se um valor de parâmetro for necessário, você precisará determinar qual valor usar para esses parâmetros antes de configurar o mecanismo externo.

Informações para uma configuração externa básica do motor

Você deve Registrar se deseja incluir cada configuração de parâmetro na configuração do mecanismo externo e, em seguida, Registrar o valor para os parâmetros que deseja incluir.

Tipo de informação	Obrigatório	Incluir	Seus valores
--------------------	-------------	---------	--------------

Nome da máquina virtual de storage (SVM)	Sim	Sim	
Nome do motor	Sim	Sim	
Servidores FPolicy primários	Sim	Sim	
Número da porta	Sim	Sim	
Servidores FPolicy secundários	Não		
Tipo de motor externo	Não		
Opção SSL para comunicação com servidor FPolicy externo	Sim	Sim	
Certificado FQDN ou nome comum personalizado	Não		
Número de série do certificado	Não		
Autoridade de certificação	Não		

Informações para parâmetros externos avançados do motor

Para configurar um motor externo com parâmetros avançados, tem de introduzir o comando de configuração no modo de privilégio avançado.

Tipo de informação	Obrigatório	Incluir	Seus valores
Tempo limite para cancelar uma solicitação	Não		
Tempo limite para abortar uma solicitação	Não		
Intervalo para envio de solicitações de status	Não		
Máximo de solicitações pendentes no servidor FPolicy	Não		
Tempo limite para desconetar um servidor FPolicy não responsivo	Não		
Intervalo para enviar mensagens keep-alive para o servidor FPolicy	Não		

Máximo de tentativas de reconexão	Não		
Receber tamanho do buffer	Não		
Enviar tamanho do buffer	Não		
Tempo limite para purgar um Session ID durante a reconexão	Não		

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.