Entenda o FPolicy

ONTAP 9

NetApp
January 17, 2025

Índice

Entenda o FPolicy . . . 1
- Quais são as duas partes da solução FPolicy . . . 1
- Quais são as notificações síncronas e assíncronas . . . 1
- Armazenamentos persistentes de FPolicy . . . 2
- Tipos de configuração FPolicy . . . 3
- Funções que os componentes do cluster desempenham com a implementação do FPolicy . . . 4
- Como o FPolicy funciona com servidores FPolicy externos . . . 4
- Qual é o processo de comunicação do servidor FPolicy nó para externo . . . 6
- Como os serviços do FPolicy funcionam nos namespaces do SVM . . . 8
- Como o FPolicy passa-leitura melhora a usabilidade para o gerenciamento hierárquico de armazenamento . . . 9

Entenda o FPolicy

Quais são as duas partes da solução FPolicy

O FPolicy é uma estrutura de notificação de acesso a arquivos usada para monitorar e gerenciar eventos de acesso a arquivos em máquinas virtuais de armazenamento (SVMs) por meio de soluções de parceiros. Com as soluções do parceiro, você lida com vários casos de uso, como conformidade e governança de dados, proteção de ransomware e mobilidade de dados.

As soluções de parceiros incluem as soluções de 3rd partes compatíveis com a NetApp e os produtos NetApp para carga de trabalho Segurança e Cloud Data Sense.

Existem duas partes para uma solução FPolicy. A estrutura FPolicy do ONTAP gerencia atividades no cluster e envia notificações para o aplicativo de parceiros (também conhecido como servidores FPolicy externos). Servidores FPolicy externos processam notificações enviadas pelo ONTAP FPolicy para atender casos de uso do cliente.

A estrutura ONTAP cria e mantém a configuração FPolicy, monitora eventos de arquivo e envia notificações para servidores FPolicy externos. O ONTAP FPolicy fornece a infraestrutura que permite a comunicação entre servidores FPolicy externos e nós de máquina virtual de storage (SVM).

A estrutura FPolicy coneta-se a servidores FPolicy externos e envia notificações para determinados eventos do sistema de arquivos para os servidores FPolicy quando esses eventos ocorrem como resultado do acesso do cliente. Os servidores FPolicy externos processam as notificações e enviam respostas de volta para o nó. O que acontece como resultado do processamento de notificações depende do aplicativo e se a comunicação entre o nó e os servidores externos é assíncrona ou síncrona.

Quais são as notificações síncronas e assíncronas

O FPolicy envia notificações para servidores FPolicy externos através da interface FPolicy. As notificações são enviadas em modo síncrono ou assíncrono. O modo de notificação determina o que o ONTAP faz depois de enviar notificações para servidores FPolicy.

- **Notificações assíncronas**

  Com notificações assíncronas, o nó não espera por uma resposta do servidor FPolicy, que aumenta a taxa de transferência geral do sistema. Esse tipo de notificação é adequado para aplicativos em que o servidor FPolicy não exige que qualquer ação seja tomada como resultado da avaliação da notificação. Por exemplo, notificações assíncronas são usadas quando o administrador da máquina virtual de storage (SVM) deseja monitorar e auditar a atividade de acesso a arquivos.

  Se um servidor FPolicy que opera no modo assíncrono sofrer uma interrupção na rede, as notificações FPolicy geradas durante a interrupção serão armazenadas no nó de storage. Quando o servidor FPolicy volta online, ele é alertado das notificações armazenadas e pode buscá-las a partir do nó de armazenamento. O período de tempo em que as notificações podem ser armazenadas durante uma interrupção é configurável até 10 minutos.

  A partir do ONTAP 9.14,1, o FPolicy permite configurar um armazenamento persistente para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Armazenamentos

persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificações FPolicy para reduzir a latência do cliente. Configurações síncronas (obrigatórias ou não obrigatórias) e assíncronas obrigatórias não são suportadas.

- **Notificações síncronas**

  Quando configurado para ser executado no modo síncrono, o servidor FPolicy deve reconhecer todas as notificações antes que a operação do cliente possa continuar. Este tipo de notificação é utilizado quando uma ação é necessária com base nos resultados da avaliação da notificação. Por exemplo, as notificações síncronas são usadas quando o administrador da SVM deseja permitir ou negar solicitações com base nos critérios especificados no servidor FPolicy externo.

Aplicações síncronas e assíncronas

Existem muitos usos possíveis para aplicativos FPolicy, tanto assíncronos quanto síncronos.

Aplicações assíncronas são aquelas em que o servidor FPolicy externo não altera o acesso a arquivos ou diretórios nem modifica dados na máquina virtual de armazenamento (SVM). Por exemplo:

- Acesso a arquivos e Registro de auditoria
- Gerenciamento de recursos de storage

Os aplicativos síncronos são aqueles em que o acesso aos dados é alterado ou os dados são modificados pelo servidor FPolicy externo. Por exemplo:

- Gerenciamento de cota
- Bloqueio de acesso a arquivos
- Arquivamento de arquivos e gerenciamento de armazenamento hierárquico
- Serviços de criptografia e descriptografia
- Serviços de compressão e descompressão

Armazenamentos persistentes de FPolicy

Armazenamentos persistentes podem ajudar a desacoplar o processamento de e/S do cliente do processamento de notificações FPolicy para reduzir a latência do cliente. A partir do ONTAP 9.14,1, é possível configurar um armazenamento persistente FPolicy para capturar eventos de acesso a arquivos para políticas assíncronas não obrigatórias no SVM. Configurações síncronas (obrigatórias ou não obrigatórias) e assíncronas obrigatórias não são suportadas.

Esta funcionalidade só está disponível no modo externo FPolicy. A aplicação de parceiro que você usa precisa para dar suporte a esse recurso. Você deve trabalhar com seu parceiro para garantir que essa configuração do FPolicy seja suportada.

A partir do ONTAP 9.15,1, a configuração de armazenamento persistente do FPolicy é simplificada. O `persistent-store create` comando automatiza a criação de volume para o SVM e configura o volume com as práticas recomendadas de armazenamento persistente.

Para obter mais informações sobre as práticas recomendadas de armazenamento persistente, "Requisitos, considerações e práticas recomendadas para configurar o FPolicy"consulte .

Para obter informações sobre como adicionar armazenamentos persistentes, "Crie armazenamentos persistentes"consulte .

Tipos de configuração FPolicy

Existem dois tipos básicos de configuração FPolicy. Uma configuração usa servidores FPolicy externos para processar e agir mediante notificações. A outra configuração não usa servidores FPolicy externos; em vez disso, ele usa o servidor FPolicy interno e nativo do ONTAP para bloqueio de arquivos simples com base em extensões.

- * Configuração externa do servidor FPolicy*

  A notificação é enviada para o servidor FPolicy, que exibe a solicitação e aplica regras para determinar se o nó deve permitir a operação do arquivo solicitado. Para políticas síncronas, o servidor FPolicy envia uma resposta ao nó para permitir ou bloquear a operação de arquivo solicitada.

- * Configuração nativa do servidor FPolicy*

  A notificação é rastreada internamente. A solicitação é permitida ou negada com base nas configurações de extensão de arquivo configuradas no escopo FPolicy.

  Nota: As solicitações de extensão de arquivo negadas não são registradas.

Quando criar uma configuração FPolicy nativa

As configurações nativas de FPolicy usam o mecanismo interno de FPolicy do ONTAP para monitorar e bloquear operações de arquivos com base na extensão do arquivo. Esta solução não requer servidores FPolicy externos (servidores FPolicy). O uso de uma configuração de bloqueio de arquivos nativa é apropriado quando essa solução simples é tudo o que é necessário.

O bloqueio de arquivos nativos permite monitorar quaisquer operações de arquivos que correspondam a eventos de operação e filtragem configurados e, em seguida, negar acesso a arquivos com extensões específicas. Esta é a configuração padrão.

Esta configuração fornece um meio de bloquear o acesso a arquivos com base apenas na extensão do arquivo. Por exemplo, para bloquear arquivos que contêm `mp3` extensões, configure uma política para fornecer notificações para determinadas operações com extensões de arquivo de destino `mp3` do . A política é configurada para negar `mp3` solicitações de arquivos para operações que geram notificações.

O seguinte se aplica a configurações nativas de FPolicy:

- O mesmo conjunto de filtros e protocolos que são suportados pela triagem de arquivos baseada no servidor FPolicy também são suportados para bloqueio de arquivos nativos.
- O bloqueio de arquivos nativo e os aplicativos de triagem de arquivos baseados no servidor FPolicy podem ser configurados ao mesmo tempo.

  Para fazer isso, você pode configurar duas políticas FPolicy separadas para a máquina virtual de armazenamento (SVM), com uma configurada para bloqueio de arquivos nativos e uma configurada para triagem de arquivos baseada no servidor FPolicy.

- O recurso de bloqueio de arquivos nativo somente exibe arquivos com base nas extensões e não no conteúdo do arquivo.

- No caso de links simbólicos, o bloqueio de arquivos nativos usa a extensão de arquivo do arquivo raiz.

Saiba mais "FPolicy: Bloqueio de arquivos nativos"sobre o .

Quando criar uma configuração que use servidores FPolicy externos

As configurações FPolicy que usam servidores FPolicy externos para processar e gerenciar notificações fornecem soluções robustas para casos de uso em que mais do que simples bloqueio de arquivos com base na extensão de arquivo é necessário.

Você deve criar uma configuração que use servidores FPolicy externos quando quiser fazer coisas como monitorar e gravar eventos de acesso a arquivos, fornecer serviços de cota, executar bloqueio de arquivos com base em critérios diferentes de extensões de arquivo simples, fornecer serviços de migração de dados usando aplicativos de gerenciamento de storage hierárquico ou fornecer um conjunto refinado de políticas que monitoram apenas um subconjunto de dados na máquina virtual de armazenamento (SVM).

Funções que os componentes do cluster desempenham com a implementação do FPolicy

O cluster, as máquinas virtuais de armazenamento contido (SVMs) e os LIFs de dados desempenham um papel na implementação de FPolicy.

- **cluster**

  O cluster contém a estrutura de gerenciamento FPolicy e mantém e gerencia informações sobre todas as configurações do FPolicy no cluster.

- **SVM**

  Uma configuração de FPolicy é definida no nível da SVM. O escopo da configuração é o SVM, e só opera com recursos do SVM. Uma configuração do SVM não pode monitorar e enviar notificações de solicitações de acesso a arquivos feitas para dados residentes em outro SVM.

  As configurações de FPolicy podem ser definidas no SVM do administrador. Depois que as configurações são definidas no SVM de administrador, elas podem ser vistas e usadas em todos os SVMs.

- **LIFs de dados**

  As conexões com os servidores FPolicy são feitas por meio de LIFs de dados pertencentes ao SVM com a configuração FPolicy. Os LIFs de dados usados para essas conexões podem falhar da mesma maneira que os LIFs de dados usados para acesso normal ao cliente.

Como o FPolicy funciona com servidores FPolicy externos

Depois que o FPolicy é configurado e ativado na máquina virtual de storage (SVM), o FPolicy é executado em todos os nós nos quais o SVM participa. A FPolicy é responsável por estabelecer e manter conexões com servidores FPolicy externos (servidores FPolicy), processamento de notificações e gerenciamento de mensagens de notificação de e para servidores FPolicy.

Além disso, como parte do gerenciamento de conexão, a FPolicy tem as seguintes responsabilidades:

- Garante que a notificação de arquivos flua através do LIF correto para o servidor FPolicy.
- Garante que, quando vários servidores FPolicy estão associados a uma política, o balanceamento de carga é feito ao enviar notificações para os servidores FPolicy.
- Tenta restabelecer a ligação quando uma ligação a um servidor FPolicy é interrompida.
- Envia as notificações para servidores FPolicy em uma sessão autenticada.
- Gerencia a conexão de dados de leitura de passagem estabelecida pelo servidor FPolicy para atender as solicitações do cliente quando a leitura de passagem estiver ativada.

Como os canais de controle são usados para comunicação FPolicy

O FPolicy inicia uma conexão de canal de controle com um servidor FPolicy externo a partir das LIFs de dados de cada nó que participa de uma máquina virtual de armazenamento (SVM). O FPolicy usa canais de controle para transmitir notificações de arquivos; portanto, um servidor FPolicy pode ver várias conexões de canal de controle com base na topologia da SVM.

Como os canais privilegiados de acesso a dados são usados para comunicação síncrona

Com casos de uso síncronos, o servidor FPolicy acessa dados que residem na máquina virtual de storage (SVM) por meio de um caminho de acesso privilegiado aos dados. O acesso através do caminho privilegiado expõe o sistema de arquivos completo ao servidor FPolicy. Ele pode acessar arquivos de dados para coletar informações, digitalizar arquivos, ler arquivos ou escrever em arquivos.

Como o servidor FPolicy externo pode acessar todo o sistema de arquivos a partir da raiz do SVM por meio do canal de dados privilegiado, a conexão de canal de dados privilegiado deve estar segura.

Como as credenciais de conexão FPolicy são usadas com canais de acesso a dados privilegiados

O servidor FPolicy faz conexões de acesso privilegiado a dados para nós de cluster usando uma credencial de usuário específica do Windows que é salva com a configuração FPolicy. SMB é o único protocolo suportado para fazer uma conexão de canal de acesso a dados privilegiada.

Se o servidor FPolicy exigir acesso privilegiado a dados, as seguintes condições devem ser atendidas:

- Uma licença SMB deve estar ativada no cluster.
- O servidor FPolicy deve ser executado sob as credenciais configuradas na configuração FPolicy.

Ao fazer uma conexão de canal de dados, o FPolicy usa a credencial para o nome de usuário especificado do Windows. O acesso aos dados é feito através do administrador Share ONTAP_ADMIN.

O que significa conceder credenciais de super usuário para acesso privilegiado a dados

O ONTAP usa a combinação do endereço IP e da credencial do usuário configurada na configuração FPolicy para conceder credenciais de super usuário ao servidor FPolicy.

O status de super usuário concede o seguinte Privileges quando o servidor FPolicy acessa dados:

- Evite verificações de permissão

O usuário evita verificações de arquivos e acesso a diretórios.

- Privileges de bloqueio especial

  O ONTAP permite ler, gravar ou modificar o acesso a qualquer arquivo, independentemente dos bloqueios existentes. Se o servidor FPolicy pegar bloqueios de intervalo de bytes no arquivo, isso resulta na remoção imediata de bloqueios existentes no arquivo.

- Ignorar quaisquer verificações de FPolicy

  O Access não gera nenhuma notificação FPolicy.

Como a FPolicy gerencia o processamento de políticas

Pode haver várias políticas de FPolicy atribuídas à sua máquina virtual de storage (SVM), cada uma com uma prioridade diferente. Para criar uma configuração de FPolicy apropriada no SVM, é importante entender como o FPolicy gerencia o processamento de políticas.

Cada solicitação de acesso ao arquivo é inicialmente avaliada para determinar quais políticas estão monitorando esse evento. Se for um evento monitorado, as informações sobre o evento monitorado junto com as políticas de interesse são passadas para a FPolicy, onde é avaliado. Cada política é avaliada por ordem da prioridade atribuída.

Você deve considerar as seguintes recomendações ao configurar políticas:

- Quando você quiser que uma política seja sempre avaliada antes de outras políticas, configure essa política com uma prioridade mais alta.
- Se o sucesso da operação de acesso a arquivos solicitados em um evento monitorado for um pré-requisito para uma solicitação de arquivo que é avaliada em relação a outra política, dê prioridade à política que controla o sucesso ou falha da operação do primeiro arquivo.

  Por exemplo, se uma diretiva gerencia a funcionalidade de arquivamento e restauração de arquivos FPolicy e uma segunda diretiva gerencia as operações de acesso de arquivos no arquivo on-line, a política que gerencia a restauração de arquivos deve ter uma prioridade maior para que o arquivo seja restaurado antes que a operação gerenciada pela segunda diretiva possa ser permitida.

- Se você quiser que todas as políticas que possam ser aplicadas a uma operação de acesso a arquivos sejam avaliadas, dê prioridade menor às políticas síncronas.

Você pode reordenar as prioridades de política para políticas existentes modificando o número de sequência de políticas. No entanto, para que o FPolicy avalie as políticas com base na ordem de prioridade modificada, você deve desativar e reativar a política com o número de sequência modificado.

Qual é o processo de comunicação do servidor FPolicy nó para externo

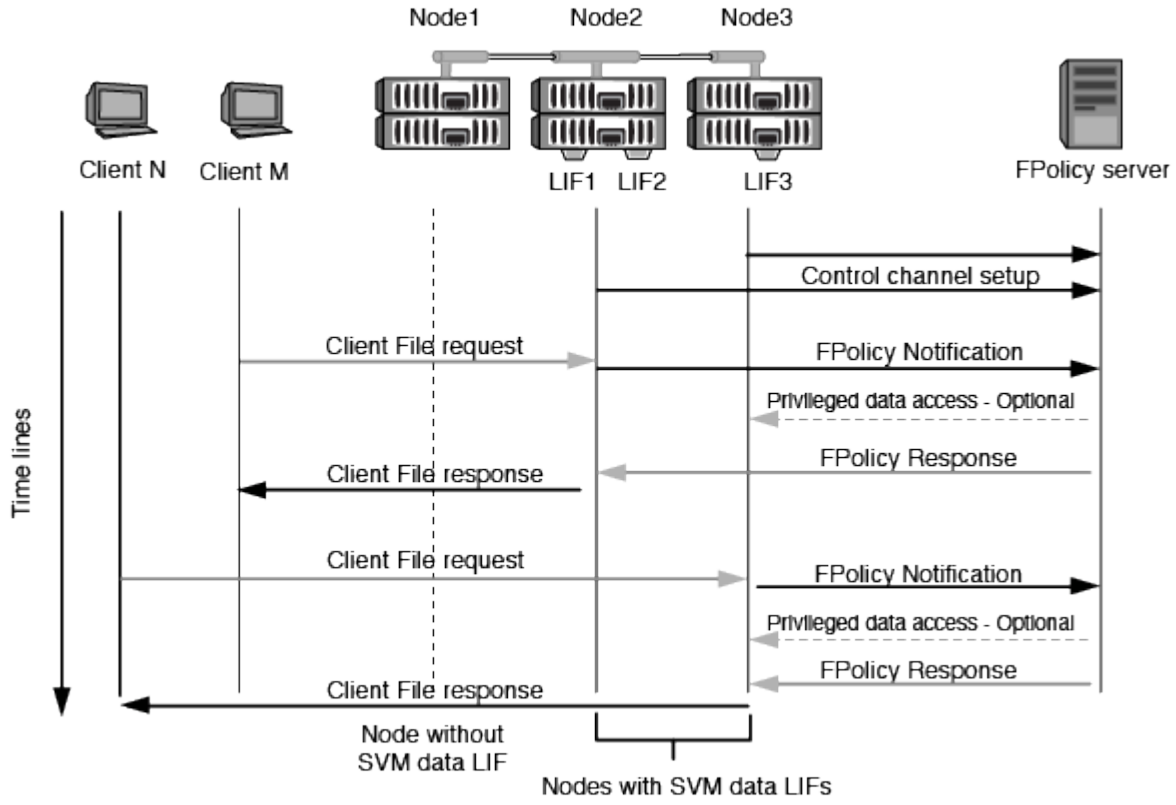
Para Planejar adequadamente a configuração do FPolicy, você deve entender o que é o processo de comunicação do servidor FPolicy de nó para externo.

Cada nó que participa de cada máquina virtual de armazenamento (SVM) inicia uma conexão com um servidor FPolicy externo (servidor FPolicy) usando TCP/IP. As conexões com os servidores FPolicy são configuradas usando LIFs de dados de nó; portanto, um nó participante pode configurar uma conexão somente se o nó tiver um LIF de dados operacional para o SVM.

Cada processo de FPolicy nos nós participantes tenta estabelecer uma conexão com o servidor FPolicy quando a diretiva está ativada. Ele usa o endereço IP e a porta do mecanismo externo FPolicy especificado na configuração da política.

A conexão estabelece um canal de controle de cada um dos nós participantes de cada SVM para o servidor FPolicy por meio do data LIF. Além disso, se os endereços de LIF de dados IPv4 e IPv6 estiverem presentes no mesmo nó participante, o FPolicy tentará estabelecer conexões para IPv4 e IPv6. Portanto, em um cenário em que o SVM se estende por vários nós ou se ambos os endereços IPv4 e IPv6 estiverem presentes, o servidor FPolicy deve estar pronto para várias solicitações de configuração de canal de controle do cluster após a diretiva FPolicy ser ativada no SVM.

Por exemplo, se um cluster tiver três nós - Node1, Node2 e Node3 - e os LIFs de dados SVM estiverem espalhados por apenas Node2 e Node3, os canais de controle serão iniciados apenas a partir de Node2 e Node3, independentemente da distribuição dos volumes de dados. Digamos que o Node2 tem duas LIFs de dados - LIF1 e LIF2 - que pertencem ao SVM e que a conexão inicial é de LIF1. Se o LIF1 falhar, o FPolicy tentará estabelecer um canal de controle a partir do LIF2.



Como o FPolicy gerencia a comunicação externa durante a migração de LIF ou failover

As LIFs de dados podem ser migradas para portas de dados no mesmo nó ou para portas de dados em um nó remoto.

Quando um LIF de dados falha ou é migrado, uma nova conexão de canal de controle é feita para o servidor FPolicy. O FPolicy pode, então, tentar novamente solicitações de clientes SMB e NFS que expiraram, com o resultado de novas notificações serem enviadas para os servidores FPolicy externos. O nó rejeita as respostas do servidor FPolicy às solicitações SMB e NFS originais e com tempo limite.

Como o FPolicy gerencia a comunicação externa durante o failover de nó

Se o nó do cluster que hospeda as portas de dados usadas para comunicação FPolicy falhar, o ONTAP rompe a conexão entre o servidor FPolicy e o nó.

O impactos do failover de cluster no servidor FPolicy pode ser atenuado configurando a política de failover para migrar a porta de dados usada na comunicação FPolicy para outro nó ativo. Após a conclusão da migração, uma nova conexão é estabelecida usando a nova porta de dados.

Se a política de failover não estiver configurada para migrar a porta de dados, o servidor FPolicy deverá aguardar que o nó com falha apareça. Depois que o nó estiver ativo, uma nova conexão será iniciada a partir desse nó com um novo Session ID.

> O servidor FPolicy deteta conexões quebradas com a mensagem do protocolo keep-alive. O tempo limite para a purga do Session ID é determinado ao configurar o FPolicy. O limite de tempo de espera predefinido é de dois minutos.

Como os serviços do FPolicy funcionam nos namespaces do SVM

O ONTAP fornece um namespace unificado de máquina virtual de storage (SVM). Os volumes no cluster são Unidos por junções para fornecer um único sistema de arquivos lógico. O servidor FPolicy está ciente da topologia do namespace e fornece serviços FPolicy em todo o namespace.

O namespace é específico e contido no SVM. Portanto, você pode ver o namespace somente no contexto SVM. Os namespaces têm as seguintes caraterísticas:

- Existe um namespace único em cada SVM, com a raiz do namespace sendo o volume raiz, representado no namespace como barra (/).
- Todos os outros volumes têm pontos de junção abaixo da raiz (/).
- Junções de volume são transparentes para os clientes.
- Uma única exportação de NFS pode fornecer acesso ao namespace completo. Caso contrário, as políticas de exportação podem exportar volumes específicos.
- Compartilhamentos SMB podem ser criados no volume ou em qtrees dentro do volume, ou em qualquer diretório dentro do namespace.
- A arquitetura do namespace é flexível.

  Exemplos de arquiteturas de namespace típicas são os seguintes:

  - Um namespace com um único ramo fora da raiz
  - Um namespace com vários ramificações fora da raiz
  - Um namespace com vários volumes não ramificados fora da raiz

Como o FPolicy passa-leitura melhora a usabilidade para o gerenciamento hierárquico de armazenamento

A passagem-leitura permite que o servidor FPolicy (funcionando como servidor de gerenciamento de armazenamento hierárquico (HSM)) forneça acesso de leitura a arquivos off-line sem ter que recuperar o arquivo do sistema de armazenamento secundário para o sistema de armazenamento primário.

Quando um servidor FPolicy é configurado para fornecer HSM a arquivos residentes em um servidor SMB, a migração de arquivos baseada em políticas ocorre onde os arquivos são armazenados off-line no armazenamento secundário e apenas um arquivo stub permanece no armazenamento primário. Mesmo que um arquivo stub apareça como um arquivo normal para os clientes, ele é na verdade um arquivo esparso que é do mesmo tamanho do arquivo original. O arquivo esparso tem o bit off-line SMB definido e aponta para o arquivo real que foi migrado para o armazenamento secundário.

Normalmente, quando uma solicitação de leitura para um arquivo off-line é recebida, o conteúdo solicitado deve ser recuperado de volta para o armazenamento primário e, em seguida, acessado através do armazenamento primário. A necessidade de recuperar dados de volta ao armazenamento primário tem vários efeitos indesejáveis. Entre os efeitos indesejáveis está o aumento da latência das solicitações do cliente causado pela necessidade de recuperar o conteúdo antes de responder à solicitação e o aumento do consumo de espaço necessário para os arquivos recuperados no armazenamento primário.

O FPolicy Passthrough-read permite que o servidor HSM (o servidor FPolicy) forneça acesso de leitura a arquivos offline migrados sem ter que recuperar o arquivo do sistema de armazenamento secundário para o sistema de armazenamento primário. Em vez de recuperar os arquivos de volta ao armazenamento primário, as solicitações de leitura podem ser atendidas diretamente do armazenamento secundário.

> O descarregamento de cópia (ODX) não é suportado com a operação de passagem-leitura FPolicy.

A passagem-leitura melhora a usabilidade, fornecendo os seguintes benefícios:

- As solicitações de leitura podem ser atendidas mesmo que o armazenamento primário não tenha espaço suficiente para recuperar os dados solicitados de volta ao armazenamento primário.
- Melhor gerenciamento de capacidade e desempenho quando um surto de recuperação de dados pode ocorrer, como se um script ou uma solução de backup precisar acessar muitos arquivos off-line.
- As solicitações de leitura de arquivos off-line em cópias Snapshot podem ser atendidas.

  Como as cópias Snapshot são somente leitura, o servidor FPolicy não pode restaurar o arquivo original se o arquivo stub estiver localizado em uma cópia Snapshot. Usar a passagem-leitura elimina esse problema.

- As políticas podem ser configuradas para controlar quando as solicitações de leitura são atendidas por meio do acesso ao arquivo no armazenamento secundário e quando o arquivo off-line deve ser recuperado para o armazenamento primário.

  Por exemplo, uma política pode ser criada no servidor HSM que especifica o número de vezes que o arquivo off-line pode ser acessado em um período de tempo especificado antes que o arquivo seja migrado de volta para o armazenamento primário. Este tipo de política evita a memorização de ficheiros que raramente são acedidos.

Como as solicitações de leitura são gerenciadas quando a passagem-leitura FPolicy está ativada

Você deve entender como as solicitações de leitura são gerenciadas quando o FPolicy Passthrough-READ está habilitado para que você possa configurar de forma otimizada a conetividade entre a máquina virtual de armazenamento (SVM) e os servidores FPolicy.

Quando a leitura de passagem FPolicy está ativada e o SVM recebe uma solicitação para um arquivo off-line, o FPolicy envia uma notificação para o servidor FPolicy (servidor HSM) por meio do canal de conexão padrão.

Após receber a notificação, o servidor FPolicy lê os dados do caminho do arquivo enviado na notificação e envia os dados solicitados para o SVM por meio da conexão de dados privilegiados de leitura de passagem estabelecida entre o SVM e o servidor FPolicy.

Depois que os dados são enviados, o servidor FPolicy responde à solicitação de leitura como uma PERMISSÃO ou NEGAÇÃO. Com base se a solicitação de leitura é permitida ou negada, o ONTAP envia as informações solicitadas ou envia uma mensagem de erro ao cliente.

Informações sobre direitos autorais

Informações sobre marcas comerciais