Fonctionnement de FPolicy

ONTAP 9

NetApp
March 22, 2023

Table des matières

Fonctionnement de FPolicy

De quoi sont les deux parties de la solution FPolicy

FPolicy est un framework de notification d'accès aux fichiers utilisé pour surveiller et gérer les événements d'accès aux fichiers sur les machines virtuelles de stockage (SVM).

Une solution FPolicy possède deux parties. La structure ONTAP FPolicy gère les activités du cluster et envoie des notifications à des serveurs FPolicy externes. Les serveurs FPolicy externes traitent les notifications envoyées par ONTAP FPolicy.

Le framework ONTAP crée et gère la configuration FPolicy, surveille les événements de fichier et envoie des notifications aux serveurs FPolicy externes. ONTAP FPolicy fournit l'infrastructure qui permet la communication entre les serveurs FPolicy externes et les nœuds de machine virtuelle de stockage (SVM).

La structure FPolicy se connecte aux serveurs FPolicy externes et envoie des notifications pour certains événements du système de fichiers aux serveurs FPolicy lorsque ces événements se produisent suite à l'accès client. Les serveurs FPolicy externes traitent les notifications et réenvoient les réponses au nœud. Ce qui se produit à la suite du traitement des notifications dépend de l'application et si la communication entre le nœud et les serveurs externes est asynchrone ou synchrone.

Quelles sont les notifications synchrones et asynchrones

FPolicy envoie des notifications aux serveurs FPolicy externes par le biais de l'interface FPolicy. Les notifications sont envoyées en mode synchrone ou asynchrone. Le mode de notification détermine le rôle de ONTAP après l'envoi de notifications aux serveurs FPolicy.

- **Notifications asynchrones**

  Grâce aux notifications asynchrones, le nœud n'attend pas de réponse du serveur FPolicy, ce qui améliore le débit global du système. Ce type de notification est adapté aux applications où le serveur FPolicy n'exige aucune action résultant de l'évaluation des notifications. Par exemple, les notifications asynchrones sont utilisées lorsque l'administrateur de la machine virtuelle de stockage (SVM) souhaite surveiller et auditer l'activité d'accès aux fichiers.

  Lorsqu'un serveur FPolicy fonctionnant en mode asynchrone est en panne du réseau, les notifications FPolicy générées lors de la panne sont stockées sur le nœud de stockage. Lorsque le serveur FPolicy est de nouveau en ligne, il est averti des notifications stockées et peut les récupérer du nœud de stockage. La durée pendant laquelle les notifications peuvent être stockées en cas de panne peut être configurée pendant 10 minutes.

- **Notifications synchrones**

  Lorsqu'il est configuré pour s'exécuter en mode synchrone, le serveur FPolicy doit accuser réception de chaque notification avant que l'opération client ne puisse continuer. Ce type de notification est utilisé lorsqu'une action est requise en fonction des résultats de l'évaluation des notifications. Par exemple, les notifications synchrones sont utilisées lorsque l'administrateur du SVM souhaite autoriser ou refuser des requêtes en fonction de critères spécifiés sur le serveur FPolicy externe.

Applications synchrones et asynchrones

Il existe de nombreuses utilisations possibles pour les applications FPolicy, asynchrone et synchrone.

Les applications asynchrones sont celles où le serveur FPolicy externe n'affecte pas l'accès aux fichiers ou aux répertoires ou ne modifie pas les données du SVM. Par exemple :

- Journalisation des audits et des accès aux fichiers
- Gestion des ressources de stockage

Les applications synchrones sont celles dont l'accès aux données est modifié ou quand le serveur FPolicy externe. Par exemple :

- La gestion des quotas
- Blocage de l'accès aux fichiers
- Archivage des fichiers et gestion du stockage hiérarchisé
- Services de cryptage et de décryptage
- Services de compression et de décompression

Vous pouvez également utiliser le SDK pour FPolicy pour identifier et implémenter d'autres applications.

Rôles liés aux composants du cluster avec l'implémentation FPolicy

Le cluster, les SVM contenant les machines virtuelles de stockage et les LIF de données jouent tous un rôle dans l'implémentation d'une FPolicy.

- **cluster**

  Le cluster contient le framework de gestion FPolicy. Il gère et gère les informations relatives à toutes les configurations FPolicy du cluster.

- **SVM**

  Une configuration FPolicy est définie au niveau de la SVM. L'étendue de la configuration est le SVM, et ne fonctionne que sur les ressources SVM. Une configuration SVM ne peut pas surveiller et envoyer de notifications pour les demandes d'accès aux fichiers effectuées pour les données résidant sur une autre SVM.

  Les configurations FPolicy peuvent être définies sur le SVM d'administration. Une fois les configurations définies sur le SVM d'administration, elles peuvent être consultées et utilisées dans tous les SVM.

- **LIF de données**

  Les connexions aux serveurs FPolicy sont effectuées via les LIF de données appartenant au SVM avec la configuration FPolicy. Les LIF de données utilisées pour ces connexions peuvent basculer de la même manière que les LIF de données utilisées pour un accès client normal.

Fonctionnement de FPolicy avec des serveurs FPolicy externes

Fonctionnement de FPolicy avec les serveurs FPolicy externes

Une fois FPolicy configuré et activé sur le SVM, FPolicy s'exécute sur chaque nœud auquel le SVM participe. FPolicy est chargé de l'établissement et de la maintenance des connexions avec des serveurs FPolicy externes (serveurs FPolicy), pour le traitement des notifications, ainsi que pour la gestion des messages de notification vers et depuis des serveurs FPolicy.

Dans le cadre de la gestion des connexions, FPolicy possède également les responsabilités suivantes :

- Garantit que la notification des fichiers circule via le LIF correct vers le serveur FPolicy.
- Garantit que lorsque plusieurs serveurs FPolicy sont associés à une règle, l'équilibrage de la charge est réalisé lors de l'envoi de notifications aux serveurs FPolicy.
- Tentatives de rétablissement de la connexion en cas de panne de la connexion à un serveur FPolicy.
- Envoie les notifications aux serveurs FPolicy par le biais d'une session authentifiée.
- Gère la connexion de données de type passthrough établie par le serveur FPolicy pour le traitement des requêtes client lorsque la lecture-passe est activée.

Mode d'utilisation des canaux de contrôle pour les communications FPolicy

FPolicy initie une connexion du canal de contrôle à un serveur FPolicy externe à partir des LIFs de données de chaque nœud participant sur un SVM (Storage Virtual machine). FPolicy utilise des canaux de contrôle pour la transmission des notifications de fichiers. Par conséquent, un serveur FPolicy peut voir plusieurs connexions de canaux de contrôle basées sur la topologie SVM.

Utilisation des canaux privilégiés d'accès aux données pour la communication synchrone

Dans le cas d'une utilisation synchrone, le serveur FPolicy accède aux données résidant sur la machine virtuelle de stockage (SVM) via un chemin d'accès privilégié aux données. L'accès via le chemin privilégié expose l'ensemble du système de fichiers au serveur FPolicy. Elle peut accéder aux fichiers de données afin de collecter des informations, de scanner des fichiers, de lire des fichiers ou d'écrire dans des fichiers.

Étant donné que le serveur FPolicy externe peut accéder à l'intégralité du système de fichiers à partir de la racine de la SVM via le canal de données privilégié, la connexion de canal de données privilégié doit être sécurisée.

Comment les identifiants de connexion FPolicy sont utilisés avec les canaux d'accès aux données privilégiés

Le serveur FPolicy établit des connexions privilégiées aux données avec les nœuds du cluster grâce à des informations d'identification Windows spécifiques enregistrées avec la

configuration FPolicy. SMB est le seul protocole pris en charge pour établir une connexion de canal avec accès aux données privilégié.

Si le serveur FPolicy nécessite un accès privilégié aux données, les conditions suivantes doivent être remplies :

- Une licence SMB doit être activée sur le cluster.
- Le serveur FPolicy doit fonctionner avec les identifiants configurés dans la configuration FPolicy.

Lors de la connexion à un canal de données, FPolicy utilise les informations d'identification du nom d'utilisateur Windows spécifié. Les données sont accessibles via le partage ONTAP_ADMIN$ par l'administrateur.

L'attribution d'informations d'identification de super utilisateur pour l'accès privilégié aux données signifie

ONTAP utilise la combinaison de l'adresse IP et des identifiants de l'utilisateur configurés dans la configuration FPolicy pour attribuer les identifiants des super utilisateurs au serveur FPolicy.

Lorsque le serveur FPolicy accède aux données, l'état du super utilisateur accorde les privilèges suivants :

- Évitez les contrôles d'autorisation

  L'utilisateur évite les vérifications de l'accès aux fichiers et aux répertoires.

- Privilèges de verrouillage spéciaux

  ONTAP permet l'accès en lecture, en écriture ou en modification à n'importe quel fichier, indépendamment des verrous existants. Si le serveur FPolicy possède des verrous de plage d'octets sur le fichier, il entraîne la suppression immédiate des verrouillages existants sur ce dernier.

- Évitez les vérifications FPolicy

  L'accès ne génère aucune notification FPolicy.

Gestion du traitement des règles par FPolicy

Il peut y avoir plusieurs règles FPolicy attribuées à votre SVM (Storage Virtual machine) ; chacune avec une priorité différente. Pour créer une configuration FPolicy appropriée sur le SVM, il est important de comprendre la façon dont FPolicy gère le traitement des règles.

Chaque requête d'accès aux fichiers est initialement évaluée afin de déterminer les règles qui surveillent cet événement. S'il s'agit d'un événement surveillé, les informations relatives à l'événement surveillé et les politiques intéressées sont transmises à FPolicy où il est évalué. Chaque stratégie est évaluée par ordre de priorité attribuée.

Lors de la configuration des règles, vous devez tenir compte des recommandations suivantes :

- Lorsque vous voulez qu'une règle soit toujours évaluée avant d'autres règles, configurez-la avec une priorité plus élevée.

- Si le succès de l'opération d'accès aux fichiers demandée sur un événement contrôlé est une condition préalable à une demande de fichier évaluée par rapport à une autre stratégie, donnez à la stratégie qui contrôle le succès ou l'échec de l'opération de premier fichier une priorité plus élevée.

  Par exemple, si l'une des règles gère la fonctionnalité d'archivage et de restauration des fichiers FPolicy, et une seconde gère les opérations d'accès aux fichiers sur le fichier en ligne, la règle de gestion de la restauration des fichiers doit avoir une priorité plus élevée afin que le fichier soit restauré avant que l'opération gérée par la seconde stratégie puisse être autorisée.

- Si vous souhaitez évaluer toutes les règles pouvant s'appliquer à une opération d'accès aux fichiers, donnez une priorité inférieure aux règles synchrones.

Vous pouvez réorganiser les priorités de stratégie pour les stratégies existantes en modifiant le numéro de séquence de stratégie. Toutefois, pour que FPolicy évalue les règles en fonction de l'ordre de priorité modifié, vous devez désactiver et réactiver cette règle avec le numéro de séquence modifié.

Ce que est le processus de communication nœud à serveur FPolicy

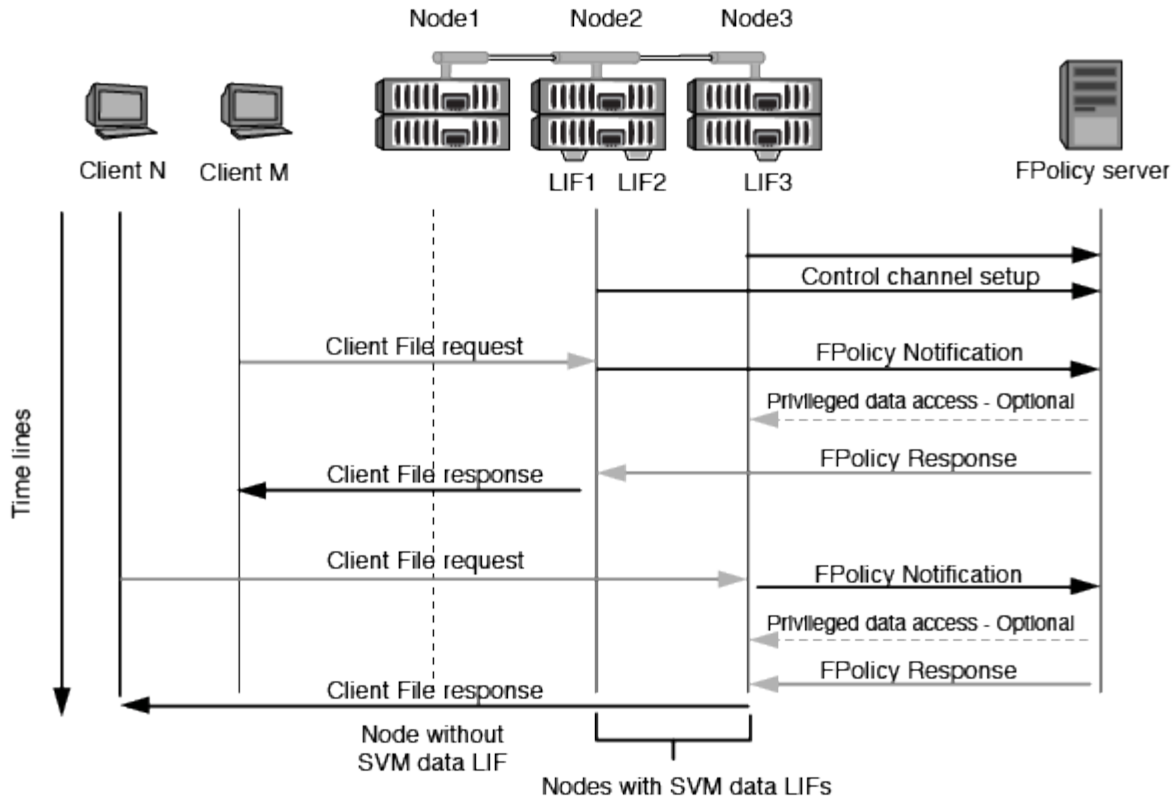
Pour planifier correctement la configuration de FPolicy, vous devez comprendre le processus de communication nœud à serveur FPolicy externe.

Chaque nœud qui participe sur chaque machine virtuelle de stockage (SVM) établit une connexion avec un serveur FPolicy externe (serveur FPolicy) à l'aide du protocole TCP/IP. Les connexions aux serveurs FPolicy sont configurées à l'aide des LIF de données du nœud. Par conséquent, un nœud participant ne peut établir une connexion que si le nœud possède une LIF de données opérationnelles pour le SVM.

Chaque processus FPolicy sur les nœuds participants tente d'établir une connexion avec le serveur FPolicy lorsque cette règle est activée. Il utilise l'adresse IP et le port du moteur externe FPolicy spécifiés dans la configuration des règles.

Cette connexion établit un canal de contrôle depuis chaque nœud participant sur chaque SVM vers le serveur FPolicy via la LIF de données. En outre, si des adresses LIF de données IPv4 et IPv6 sont présentes sur le même nœud participant, FPolicy tente d'établir des connexions pour IPv4 et IPv6. Par conséquent, dans un scénario où le SVM s'étend sur plusieurs nœuds ou si des adresses IPv4 et IPv6 sont présentes, le serveur FPolicy doit être prêt à traiter plusieurs requêtes de configuration de canal de contrôle provenant du cluster après l'activation de la politique FPolicy sur le SVM.

Par exemple, si un cluster possède trois nœuds—Node1, Node2 et nœud3- ainsi que les LIF de données du SVM se répartissent uniquement sur Node2 et nœud3, les canaux de contrôle sont lancés uniquement sur le nœud2 et celui du nœud3, indépendamment de la répartition des volumes de données. Supposons que Node2 possède deux LIF de données—LIF1 et LIF2—qui appartiennent à la SVM et que la connexion initiale est de LIF1. En cas d'échec de LIF1, FPolicy tente d'établir un canal de contrôle à partir de LIF2.



Comment FPolicy gère la communication externe lors de la migration ou du basculement de LIF

Les LIFs de données peuvent être migrées sur des ports data qui se trouvent sur le même nœud ou vers des ports data sur un nœud distant.

Lorsqu'une LIF de données subit une panne ou est migrée, une nouvelle connexion de canal de contrôle est établie vers le serveur FPolicy. FPolicy peut ensuite réessayer les requêtes des clients SMB et NFS ayant dépassé le délai d'attente. En conséquence, de nouvelles notifications sont envoyées aux serveurs FPolicy externes. Le nœud rejette les réponses du serveur FPolicy aux requêtes SMB et NFS d'origine avec temporisation.

Comment FPolicy gère la communication externe lors du basculement de nœud

Si le nœud de cluster qui héberge les ports de données utilisés pour la communication FPolicy tombe en panne, ONTAP interrompt la connexion entre le serveur FPolicy et le nœud.

Il est possible de diminuer l'impact du basculement de cluster sur le serveur FPolicy en configurant le gestionnaire des LIF afin de migrer le port de données utilisé dans la communication FPolicy vers un autre nœud actif. Une fois la migration terminée, une nouvelle connexion est établie à l'aide du nouveau port de données.

Si le LIF Manager n'est pas configuré pour migrer le port de données, le serveur FPolicy doit attendre que le nœud en panne soit activé. Une fois le nœud activé, une nouvelle connexion est lancée à partir de ce nœud avec un nouvel ID de session.

Le serveur FPolicy détecte les connexions interrompues avec le message du protocole de maintien de la disponibilité. Le délai d'expiration pour la purge de l'ID de session est déterminé lors de la configuration de FPolicy. Le délai de mise en veille par défaut est de deux minutes.

Fonctionnement des services FPolicy sur les espaces de noms des SVM

ONTAP offre un espace de noms de machine virtuelle de stockage unifié. Les volumes du cluster sont regroupés par des jonctions pour fournir un système de fichiers unique et logique. Le serveur FPolicy connaît la topologie de l'espace de noms et fournit des services FPolicy à l'échelle de l'espace de noms.

Le namespace est spécifique et contenu au sein du SVM ; par conséquent, vous pouvez voir le namespace uniquement depuis le contexte SVM. Les espaces de noms présentent les caractéristiques suivantes :

- Un nom d'espace unique existe dans chaque SVM, la racine de l'espace de noms étant le volume root, représenté dans le namespace par la barre oblique (/).
- Tous les autres volumes ont des points de jonction sous la racine (/).
- Les jonctions des volumes sont transparentes pour les clients.
- Une exportation NFS unique peut donner accès à l'espace de noms complet, sinon les export policy peuvent exporter des volumes spécifiques.
- Les partages SMB peuvent être créés sur le volume, dans des qtrees au sein du volume, ou sur n'importe quel répertoire dans le namespace.
- L'architecture d'espace de noms est flexible.

  Voici quelques exemples d'architectures d'espaces de noms classiques :

  - Un espace de noms avec une seule branche à la racine
  - Un espace de noms avec plusieurs branches à la racine
  - Un namespace avec plusieurs volumes non ramifiés en dehors de la racine

Informations sur le copyright

Informations sur les marques commerciales