



# **Analysez FPolicy**

## **ONTAP 9**

NetApp  
April 24, 2024

# Sommaire

- Analysez FPolicy ..... 1
  - De quoi sont les deux parties de la solution FPolicy ..... 1
  - Quelles sont les notifications synchrones et asynchrones ..... 1
  - Les magasins persistants FPolicy ..... 2
  - Types de configuration FPolicy ..... 3
  - Rôles liés aux composants du cluster avec l'implémentation FPolicy ..... 5
  - Fonctionnement de FPolicy avec des serveurs FPolicy externes ..... 5
  - Ce que est le processus de communication nœud à serveur FPolicy ..... 7
  - Fonctionnement des services FPolicy sur les espaces de noms des SVM ..... 9
  - La fonctionnalité de gestion du stockage hiérarchique de FPolicy permet d'améliorer la facilité d'utilisation de la gestion hiérarchique du stockage ..... 9

# Analysez FPolicy

## De quoi sont les deux parties de la solution FPolicy

FPolicy est un système de notification d'accès aux fichiers qui permet de surveiller et de gérer les événements d'accès aux fichiers sur les machines virtuelles de stockage (SVM) à l'aide de solutions partenaires. Les solutions de partenaires vous aident à prendre en charge divers cas d'utilisation tels que la gouvernance et la conformité des données, la protection contre les ransomwares et la mobilité des données.

Les solutions partenaires incluent à la fois les solutions tierces prises en charge par NetApp et les produits NetApp sécurité des workloads et Cloud Data Sense.

Une solution FPolicy possède deux parties. La structure ONTAP FPolicy gère les activités sur le cluster et envoie des notifications à l'application partenaire (ou serveurs externes FPolicy). Les serveurs externes FPolicy traitent les notifications envoyées par ONTAP FPolicy pour répondre aux cas d'utilisation des clients.

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.

À partir de ONTAP 9.14.1, FPolicy permet de configurer un magasin persistant pour capturer les événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications

FPolicy afin de réduire la latence du client. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

- **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

## **Les magasins persistants FPolicy**

À partir de ONTAP 9.14.1, FPolicy permet de configurer un magasin persistant pour capturer les événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

Cette fonctionnalité est uniquement disponible en mode externe FPolicy. L'application partenaire que vous utilisez doit prendre en charge cette fonctionnalité. Vous devez collaborer avec votre partenaire pour vous assurer que cette configuration FPolicy est prise en charge.

### **Et des meilleures pratiques**

Les administrateurs du cluster doivent configurer un volume pour le magasin persistant sur chaque SVM sur lequel FPolicy est activé. Lorsqu'il est configuré, un magasin persistant capture tous les événements FPolicy correspondants, qui sont ensuite traités dans le pipeline FPolicy et envoyés au serveur externe.

Le stockage persistant reste tel qu'il était au moment de la réception du dernier événement en cas de

redémarrage inattendu ou lorsque FPolicy est désactivé et réactivé. Après une opération de basculement, les nouveaux événements sont stockés et traités par le nœud partenaire. Après une opération de rétablissement, le magasin persistant reprend le traitement de tout événement non traité qui pourrait rester en provenance de lorsque le basculement du nœud s'est produit. Les événements en direct seraient prioritaires sur les événements non traités.

Si le volume du magasin persistant passe d'un nœud à un autre dans la même SVM, les notifications qui ne sont pas encore traitées seront également déplacées vers le nouveau nœud. Vous devez exécuter à nouveau `le fpolicy persistent-store create` sur l'un des nœuds après le déplacement du volume, afin de garantir que la notification en attente est transmise au serveur externe.

Le volume de stockage persistant est configuré par SVM. Pour chaque SVM activé FPolicy, vous devez créer un volume de stockage persistant.

Créez le volume de stockage persistant sur le nœud avec les LIF qui prévoient que le trafic maximal sera surveillé par Fpolicy.

Si les notifications accumulées dans le magasin persistant dépassent la taille du volume provisionné, FPolicy commence à supprimer la notification entrante avec les messages EMS appropriés.

Le nom du volume de stockage persistant et le chemin de jonction spécifiés au moment de la création du volume doivent correspondre.

Définissez la règle de snapshot sur `none` pour ce volume au lieu de `default`. Cela permet de s'assurer qu'il n'y a pas de restauration accidentelle de l'instantané, ce qui entraîne la perte des événements actuels et d'empêcher le traitement des événements en double.

Rendre le volume de stockage persistant inaccessible pour l'accès au protocole utilisateur externe (CIFS/NFS) afin d'éviter toute corruption accidentelle ou suppression des enregistrements d'événements persistants. Pour ce faire, une fois FPolicy activé, démontez le volume dans ONTAP pour supprimer le chemin de jonction, ce qui le rend inaccessible pour l'accès au protocole utilisateur.

Pour plus d'informations, voir "[Créez des magasins persistants](#)".

## Types de configuration FPolicy

Il existe deux types de configuration de base pour les serveurs FPolicy. Une seule configuration utilise des serveurs FPolicy externes pour traiter les notifications et agir. L'autre configuration n'utilise pas de serveurs FPolicy externes. Il utilise à la place le serveur FPolicy interne et natif ONTAP pour bloquer simplement les fichiers en fonction des extensions.

- **Configuration de serveur FPolicy externe**

La notification est envoyée au serveur FPolicy qui présente la requête et applique des règles pour déterminer si le nœud doit autoriser l'opération de fichier demandée. Pour les règles synchrones, le serveur FPolicy envoie ensuite une réponse au nœud pour autoriser ou bloquer l'opération de fichier demandée.

- **Configuration de serveur FPolicy native**

La notification est tramée en interne. La requête est autorisée ou refusée en fonction des paramètres d'extension de fichier configurés dans le cadre FPolicy.

**Remarque** : les demandes d'extension de fichier refusées ne sont pas consignées.

## Quand créer une configuration FPolicy native

Les configurations FPolicy natives utilisent le moteur FPolicy interne de ONTAP pour surveiller et bloquer les opérations basées sur l'extension du fichier. Cette solution ne nécessite pas de serveurs FPolicy externes (serveurs FPolicy). L'utilisation d'une configuration native de blocage de fichiers est appropriée lorsque cette solution simple est tout ce qui est nécessaire.

Le blocage de fichiers natif vous permet de surveiller toutes les opérations de fichiers qui correspondent aux événements de filtrage et d'opération configurés, puis de refuser l'accès aux fichiers avec des extensions particulières. Il s'agit de la configuration par défaut.

Cette configuration permet de bloquer l'accès aux fichiers en fonction de l'extension du fichier uniquement. Par exemple, pour bloquer les fichiers contenant mp3 extensions, vous configurez une stratégie pour fournir des notifications pour certaines opérations avec des extensions de fichier cible de mp3. La règle est configurée pour refuser mp3 demandes de fichiers pour les opérations qui génèrent des notifications.

Les configurations FPolicy natives sont les suivantes :

- Le blocage de fichiers natif est également pris en charge par le filtrage de fichiers basé sur serveur FPolicy.
- Les applications natives de blocage de fichiers et de filtrage de fichiers sur serveur FPolicy peuvent être configurées simultanément.

Pour ce faire, vous pouvez configurer deux règles FPolicy distinctes pour la machine virtuelle de stockage (SVM), une configurée pour le blocage natif des fichiers et une configurée pour le filtrage des fichiers basé sur serveur FPolicy.

- La fonctionnalité native de blocage de fichiers ne permet d'afficher que les fichiers basés sur les extensions et non sur le contenu du fichier.
- Dans le cas de liens symboliques, le blocage de fichiers natif utilise l'extension de fichier du fichier racine.

En savoir plus sur ["FPolicy : blocage de fichiers natif"](#).

## Quand créer une configuration utilisant des serveurs FPolicy externes

Les configurations FPolicy qui utilisent des serveurs FPolicy externes pour traiter et gérer les notifications proposent des solutions fiables pour les cas d'utilisation où il est nécessaire de bloquer simplement des fichiers en fonction de l'extension des fichiers.

Pour ce faire, vous devez créer une configuration qui utilise des serveurs FPolicy externes lorsque vous souhaitez effectuer des tâches telles que la surveillance et l'enregistrement des événements d'accès aux fichiers, fournir des services de quotas, exécuter des blocages de fichiers selon des critères autres que les extensions de fichiers simples, fournir des services de migration des données à l'aide d'applications de gestion du stockage hiérarchisé, Vous pouvez également proposer un ensemble de règles à très grande granularité qui contrôlent uniquement un sous-ensemble de données du serveur virtuel de stockage (SVM).

# 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

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.

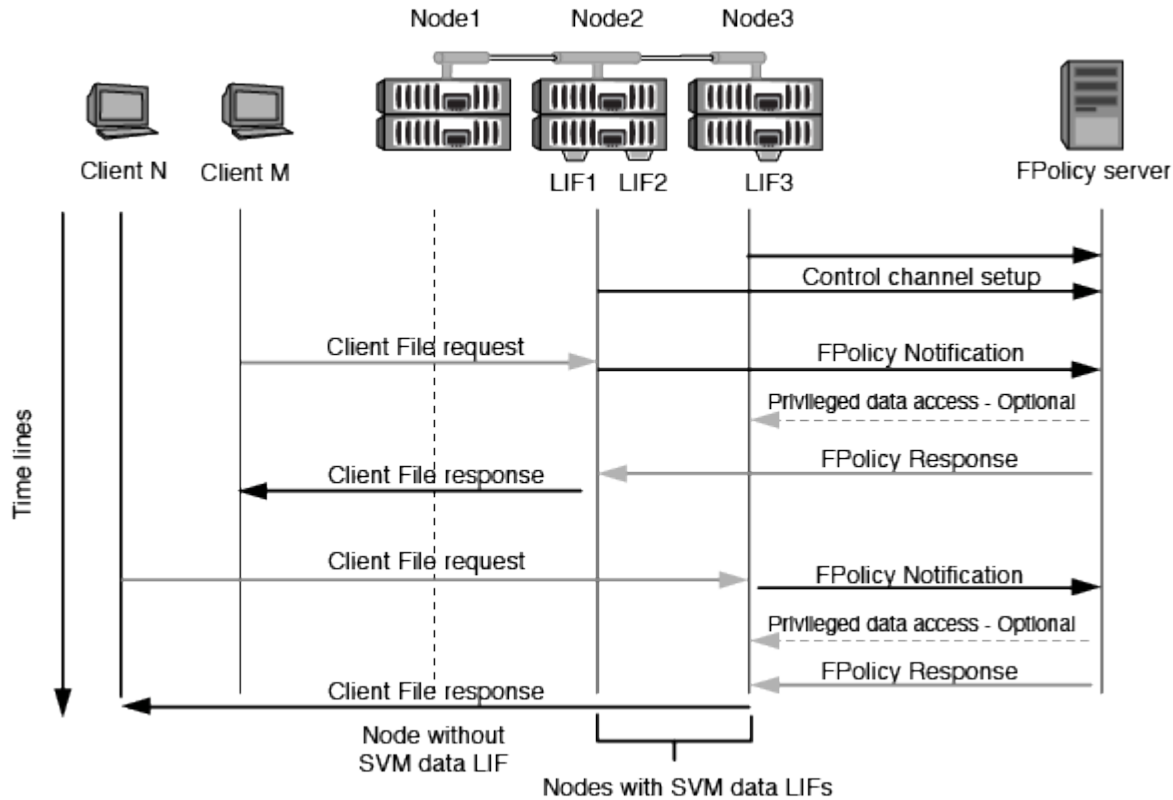
Chaque nœud qui participe sur chaque machine virtuelle de stockage (SVM) établit une connexion avec un serveur FPolicy externe (serveur FPolicy) à l'aide du protocole TCP/IP. Les connexions aux serveurs FPolicy sont configurées à l'aide des LIF de données du nœud. Par conséquent, un nœud participant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

Vous pouvez atténuer l'impact du basculement de cluster sur le serveur FPolicy en configurant la règle de

basculement pour 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 la règle de basculement n'est pas configurée pour migrer le port de données, le serveur FPolicy doit attendre l'apparition du nœud défaillant. 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

## La fonctionnalité de gestion du stockage hiérarchique de FPolicy permet d'améliorer la facilité d'utilisation de la gestion hiérarchique du stockage

La fonctionnalité Passthrough Read permet au serveur FPolicy (fonctionnant comme serveur HSM (gestion hiérarchique du stockage)) de fournir un accès en lecture aux fichiers hors ligne sans avoir à rappeler le fichier du système de stockage secondaire au système de stockage primaire.

Lorsqu'un serveur FPolicy est configuré pour fournir HSM les fichiers stockés sur un serveur SMB, la migration de fichiers basée sur des règles se produit lorsque les fichiers sont stockés hors ligne sur le stockage secondaire et qu'un seul fichier stub reste sur le stockage primaire. Même si un fichier stub apparaît comme un fichier normal pour les clients, il s'agit en fait d'un fichier parse de la même taille que le fichier d'origine. Le fichier sparse a le jeu de bits hors ligne SMB et pointe vers le fichier réel qui a été migré vers le stockage secondaire.

En général, lorsqu'une demande de lecture pour un fichier hors ligne est reçue, le contenu demandé doit être rappelé dans le stockage principal, puis accessible par le biais du stockage principal. Le besoin de rappeler des données dans le stockage primaire a plusieurs effets indésirables. L'augmentation de la latence aux demandes des clients, due à la nécessité de rappeler le contenu avant de répondre à la demande et l'augmentation de la consommation d'espace nécessaire pour les fichiers rappelés sur l'infrastructure de stockage primaire, soit un effet indésirable.

La fonctionnalité de passerelle FPolicy permet au serveur HSM (serveur FPolicy) de fournir un accès en lecture aux fichiers migrés hors ligne sans avoir à rappeler le fichier du système de stockage secondaire au système de stockage primaire. Au lieu de rappeler les fichiers dans le stockage primaire, les demandes de lecture peuvent être traitées directement depuis le système de stockage secondaire.



La fonction de déchargement des copies (ODX) n'est pas prise en charge par l'opération de lecture intermédiaire FPolicy.

La fonctionnalité Passthrough Read améliore la convivialité en offrant les avantages suivants :

- Les demandes de lecture peuvent être traitées même si l'espace de stockage primaire n'est pas suffisant pour récupérer les données demandées dans le stockage primaire.
- Meilleure gestion de la capacité et des performances lorsqu'une poussée de récupération des données peut se produire, par exemple si un script ou une solution de sauvegarde doit accéder à de nombreux fichiers hors ligne.
- Les demandes de lecture de fichiers hors ligne des copies Snapshot peuvent être traitées.

Étant donné que les copies Snapshot sont en lecture seule, le serveur FPolicy ne peut pas restaurer le fichier d'origine si le fichier stub est situé dans une copie Snapshot. L'utilisation de la lecture passthrough élimine ce problème.

- Des règles peuvent être définies pour définir ce contrôle lorsque les demandes de lecture sont traitées par l'accès au fichier sur le système de stockage secondaire et lorsqu'un fichier hors ligne doit être rappelé sur le système de stockage principal.

Par exemple, il est possible de créer une règle sur le serveur HSM qui spécifie le nombre d'accès au fichier hors ligne pendant une période donnée avant que le fichier ne soit remigré vers le stockage principal. Ce type de stratégie évite de rappeler les fichiers rarement utilisés.

## **Mode de gestion des requêtes de lecture lors de l'activation du mode de gestion FPolicy**

Vous devez comprendre comment les requêtes de lecture sont gérées lorsque le mode de lecture intermédiaire FPolicy est activé afin de pouvoir configurer de manière optimale la connectivité entre le SVM et les serveurs FPolicy.

Lorsque la fonction de lecture intermédiaire FPolicy est activée et que le SVM reçoit une demande de fichier hors ligne, FPolicy envoie une notification au serveur FPolicy (serveur HSM) par l'intermédiaire du canal de connexion standard.

Après avoir reçu la notification, le serveur FPolicy lit les données du chemin de fichier envoyé dans la notification et envoie les données demandées à la SVM via la connexion de données privilégiée par lecture-intermédiaire établie entre le SVM et le serveur FPolicy.

Une fois les données envoyées, le serveur FPolicy répond à la demande de lecture comme ALLOW ou DENY. En fonction de l'autorisation ou du refus de la demande de lecture, ONTAP envoie les informations demandées ou envoie un message d'erreur au client.

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

**LÉGENDE DE RESTRICTION DES DROITS :** L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.