



Utilisez FPolicy pour le contrôle et la gestion des fichiers sur SVM

ONTAP 9

NetApp
September 12, 2024

Sommaire

- Utilisez FPolicy pour le contrôle et la gestion des fichiers sur SVM. 1
 - Analysez FPolicy 1
 - Planification de la configuration FPolicy. 10
 - Créer la configuration FPolicy 49
 - Gérer les configurations FPolicy 57

Utilisez FPolicy pour le contrôle et la gestion des fichiers sur SVM

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

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. Depuis la version ONTAP 9.14.1, vous pouvez configurer un magasin persistant FPolicy pour capturer les événements d'accès aux fichiers pour des règles asynchrones non obligatoires dans la SVM. 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.

À partir de ONTAP 9.15.1, la configuration du stockage persistant FPolicy est simplifiée. Le `persistent-store create` Automatise la création de volume pour la SVM et configure le volume avec les bonnes pratiques de stockage persistant.

Pour plus d'informations sur les meilleures pratiques en matière de stockage persistant, reportez-vous à la section ["D'exigences, de considérations et de meilleures pratiques pour la configuration de FPolicy"](#).

Pour plus d'informations sur l'ajout de magasins persistants, reportez-vous à la section ["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 utilisés pour ces connexions peuvent basculer de la même manière que les LIF de données utilisés 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

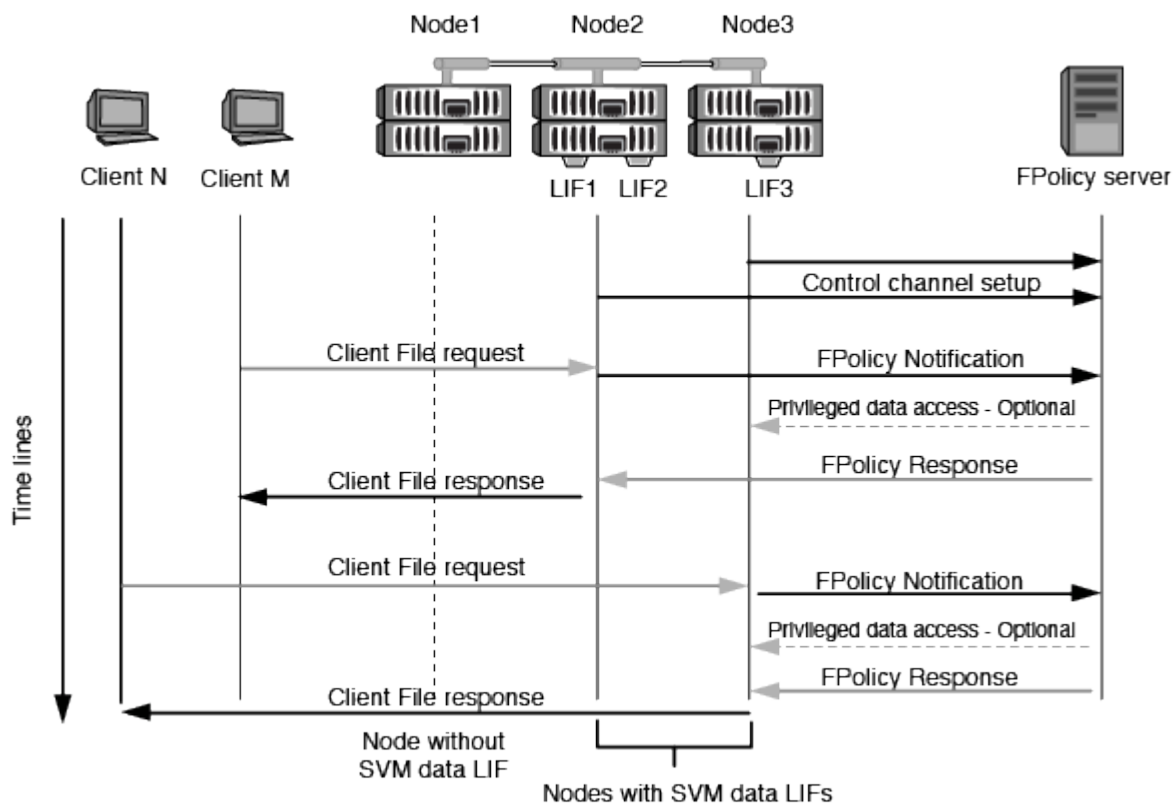
Pour planifier correctement la configuration de FPolicy, vous devez comprendre le processus de communication nœud à serveur FPolicy externe.

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.

Planification de la configuration FPolicy

D'exigences, de considérations et de meilleures pratiques pour la configuration de FPolicy

Avant de créer et de configurer des configurations FPolicy sur vos machines virtuelles de stockage (SVM), vous devez connaître certaines exigences, considérations et meilleures pratiques relatives à la configuration de FPolicy.

Les fonctionnalités FPolicy sont configurées soit via l'interface de ligne de commandes soit via l'API REST.

Conditions requises pour la configuration de FPolicy

Avant de configurer et d'activer FPolicy sur votre machine virtuelle de stockage (SVM), vous devez connaître certaines exigences.

- Tous les nœuds du cluster doivent exécuter une version de ONTAP qui prend en charge FPolicy.
- Si vous n'utilisez pas le moteur FPolicy natif ONTAP, vous devez installer des serveurs FPolicy externes (serveurs FPolicy).
- Les serveurs FPolicy doivent être installés sur un serveur accessible depuis les LIFs de données du SVM sur lequel les règles FPolicy sont activées.



Depuis la version ONTAP 9.8, ONTAP fournit un service LIF client pour les connexions FPolicy sortantes avec l'ajout du `data-fpolicy-client` service. ["En savoir plus sur les LIF et les règles de service"](#).

- L'adresse IP du serveur FPolicy doit être configurée en tant que serveur principal ou secondaire dans la configuration du moteur externe de la politique FPolicy.
- Si les serveurs FPolicy accèdent aux données sur un canal de données privilégié, les exigences supplémentaires suivantes doivent être respectées :
 - SMB doit être sous licence sur le cluster.

Un accès privilégié aux données se fait à l'aide de connexions SMB.

- Les informations d'identification utilisateur doivent être configurées pour accéder aux fichiers via le canal de données privilégié.
- Le serveur FPolicy doit fonctionner avec les identifiants configurés dans la configuration FPolicy.
- Toutes les LIFs de données utilisées pour communiquer avec les serveurs FPolicy doivent être configurées de sorte à avoir `cifs` comme l'un des protocoles autorisés.

Cela inclut les LIFs utilisées pour les connexions passthrough-read.

Meilleures pratiques et recommandations lors de la configuration de FPolicy

Lors de la configuration de FPolicy sur des machines virtuelles de stockage (SVM), familiarisez-vous avec les bonnes pratiques et recommandations générales de configuration pour garantir que votre configuration FPolicy offre des performances de contrôle fiables et des résultats qui répondent à vos besoins.

Pour obtenir des instructions spécifiques relatives aux performances, au dimensionnement et à la configuration, utilisez votre application partenaire FPolicy.

Magasins persistants

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.

- Avant d'utiliser la fonction de stockage persistant, assurez-vous que vos applications partenaires prennent en charge cette configuration.
- Vous avez besoin d'un magasin persistant pour chaque SVM sur lequel FPolicy est activé.
 - Il n'est possible de configurer qu'un seul magasin persistant sur chaque SVM. Ce magasin persistant unique doit être utilisé pour toutes les configurations FPolicy de cette SVM, même si les règles proviennent de différents partenaires.
- ONTAP 9.15.1 ou version ultérieure :
 - Le magasin persistant, son volume et sa configuration de volume sont gérés automatiquement lorsque vous créez le magasin persistant.
- ONTAP 9.14.1 :
 - Le magasin persistant, son volume et sa configuration de volume sont gérés manuellement.
- Créez le volume de stockage persistant sur le nœud avec les LIF qui veulent que le trafic maximal soit surveillé par FPolicy.
 - ONTAP 9.15.1 ou version ultérieure : les volumes sont automatiquement créés et configurés lors de la création du magasin persistant.
 - ONTAP 9.14.1 : les administrateurs de cluster doivent créer et configurer un volume pour le magasin persistant sur chaque SVM sur lequel FPolicy est activé.
- 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.
 - ONTAP 9.15.1 ou version ultérieure : en plus du `size` paramètre, le `autosize-mode` peut aider le volume à croître ou à diminuer en fonction de la quantité d'espace utilisé.
 - ONTAP 9.14.1 : le `size` le paramètre est configuré lors de la création du volume pour fournir une limite

maximale.

- Définissez la règle de snapshot sur `none` pour le volume de stockage persistant 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.
 - ONTAP 9.15.1 ou version ultérieure : le `snapshot-policy` le paramètre est automatiquement configuré sur `aucun` lors de la création du magasin persistant.
 - ONTAP 9.14.1 : le `snapshot-policy` le paramètre est configuré sur `none` lors de la création du volume.
- 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.
 - ONTAP 9.15.1 ou version ultérieure : ONTAP bloque automatiquement le volume depuis l'accès aux protocoles utilisateur externes (CIFS/NFS) lors de la création du magasin persistant.
 - ONTAP 9.14.1 : une fois FPolicy activé, démontez le volume dans ONTAP pour supprimer la Junction path. Cela le rend inaccessible pour l'accès au protocole utilisateur externe (CIFS/NFS).

Pour plus d'informations, reportez-vous à la section ["Les magasins persistants FPolicy"](#) et ["Créez des magasins persistants"](#).

Basculement et rétablissement du magasin persistant

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 sont 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 les notifications en attente sont envoyées au serveur externe.

Configuration des règles

La configuration du moteur externe FPolicy, les événements et l'étendue des SVM peuvent améliorer votre expérience et votre sécurité globale.

- Configuration du moteur externe FPolicy pour les SVM :
 - Le renforcement de la sécurité implique des coûts de performance. L'activation de la communication SSL (Secure Sockets Layer) a un effet sur les performances lors de l'accès aux partages.
 - Le moteur externe FPolicy doit être configuré avec plusieurs serveurs FPolicy de manière à fournir la résilience et la haute disponibilité du traitement des notifications du serveur FPolicy.
- Configuration des événements FPolicy pour les SVM :

La surveillance des opérations de fichiers influence votre expérience globale. Par exemple, le filtrage des opérations de fichiers indésirables côté stockage améliore votre expérience. NetApp recommande de configurer les éléments suivants :

- Surveillance des types minimaux d'opérations de fichiers et activation du nombre maximal de filtres sans rompre le cas d'utilisation.

- Utilisation de filtres pour les opérations getattr, lecture, écriture, ouverture et fermeture. La part des environnements de home Directory SMB et NFS est élevée.
- Configuration du périmètre FPolicy pour les SVM :

Limitez l'étendue des règles aux objets de stockage concernés, tels que les partages, les volumes et les exportations, au lieu de les activer sur l'ensemble du SVM. NetApp recommande de vérifier les extensions de répertoire. Si le `is-file-extension-check-on-directories-enabled` le paramètre est défini sur `true`, les objets de répertoire sont soumis aux mêmes vérifications d'extension que les fichiers ordinaires.

Configuration du réseau

La connectivité réseau entre le serveur FPolicy et le contrôleur doit présenter une faible latence. NetApp recommande de séparer le trafic FPolicy du trafic client en utilisant un réseau privé.

De plus, vous devez placer des serveurs externes FPolicy (serveurs FPolicy) à proximité immédiate du cluster avec une connectivité à large bande passante afin d'obtenir une latence minimale et une connectivité à large bande passante.



Si la LIF du trafic FPolicy est configurée sur un port différent de la LIF pour le trafic client, la LIF FPolicy peut basculer vers l'autre nœud en raison d'une défaillance de port. Par conséquent, le serveur FPolicy devient inaccessible depuis le nœud ce qui provoque l'échec des notifications FPolicy pour les opérations de fichier sur le nœud. Pour éviter ce problème, vérifiez que le serveur FPolicy peut être accessible via au moins une LIF du nœud afin de traiter les requêtes FPolicy pour les opérations de fichiers effectuées sur ce nœud.

Configuration matérielle

Vous pouvez avoir le serveur FPolicy sur un serveur physique ou virtuel. Si le serveur FPolicy se trouve dans un environnement virtuel, vous devez allouer des ressources dédiées (CPU, réseau et mémoire) au serveur virtuel.

Le taux nœud/serveur FPolicy du cluster doit être optimisé pour s'assurer que les serveurs FPolicy ne sont pas surchargés et peuvent introduire des latences lorsque le SVM répond aux demandes du client. Le ratio optimal dépend de l'application partenaire pour laquelle le serveur FPolicy est utilisé. NetApp recommande de faire équipe avec ses partenaires pour déterminer la valeur appropriée.

Configuration à règles multiples

La règle FPolicy pour le blocage natif a la priorité la plus élevée, quel que soit le numéro de séquence, et les règles qui modifient la décision ont une priorité plus élevée que les autres. La priorité de la règle dépend de l'utilisation. NetApp recommande de faire équipe avec ses partenaires pour déterminer la priorité appropriée.

Considérations de taille

FPolicy effectue un contrôle en ligne des opérations SMB et NFS, envoie des notifications au serveur externe et attend une réponse, selon le mode de communication externe du moteur (synchrone ou asynchrone). Ce processus affecte les performances des accès SMB et NFS ainsi que des ressources CPU.

Pour résoudre tout problème, NetApp recommande de travailler avec ses partenaires pour évaluer et dimensionner l'environnement avant d'activer FPolicy. Les performances sont affectées par plusieurs facteurs, notamment le nombre d'utilisateurs, les caractéristiques de la charge de travail, tels que les opérations par utilisateur et la taille des données, la latence du réseau et les défaillances ou la lenteur du serveur.

Contrôle des performances

FPolicy est un système basé sur les notifications. Les notifications sont envoyées à un serveur externe pour traitement et pour générer une réponse à ONTAP. Ce processus aller-retour augmente la latence pour l'accès client.

La surveillance des compteurs de performances sur le serveur FPolicy et dans ONTAP vous permet d'identifier les goulets d'étranglement dans la solution et de configurer les paramètres nécessaires pour une solution optimale. Par exemple, une augmentation de la latence FPolicy a un effet en cascade sur la latence d'accès SMB et NFS. Par conséquent, vous devez contrôler à la fois la charge de travail (SMB et NFS) et la latence FPolicy. En outre, vous pouvez utiliser des règles de qualité de service dans ONTAP pour configurer une charge de travail pour chaque volume ou SVM activé pour FPolicy.

NetApp recommande d'exécuter `statistics show -object workload` commande permettant d'afficher les statistiques des charges de travail. De plus, vous devez surveiller les paramètres suivants :

- Latences moyennes, en lecture et en écriture
- Nombre total d'opérations
- Compteurs de lecture et d'écriture

Vous pouvez contrôler les performances des sous-systèmes FPolicy à l'aide des compteurs FPolicy suivants.



Vous devez être en mode diagnostic pour collecter les statistiques relatives à FPolicy.

Étapes

1. Collectez les compteurs FPolicy :

- `statistics start -object fpolicy -instance instance_name -sample-id ID`
- `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`

2. Afficher les compteurs FPolicy :

- `statistics show -object fpolicy -instance instance_name -sample-id ID`
- `statistics show -object fpolicy_server -instance instance_name -sample-id ID`

Le `fpolicy` et `fpolicy_server` les compteurs fournissent des informations sur plusieurs paramètres de performances décrits dans le tableau suivant.

Compteurs	Description
• compteurs « fpolicy »*	demandes_abandonnées
Nombre de demandes d'écran pour lesquelles le traitement est abandonné sur le SVM	nombre_événements
Liste des événements entraînant une notification	latence_demande_max

Compteurs	Description
Latence maximale des demandes d'écran	demandes_en_attente
Nombre total de demandes d'écran en cours de traitement	requêtes_traitées
Nombre total de requêtes d'écran effectuées via le traitement fpolicy sur la SVM	liste_latence_de_la_demande
Histogramme de latence pour les demandes d'écran	taux_envoyé_demandes
Nombre de demandes d'écran envoyées par seconde	taux_de_réception_demandes
Nombre de demandes d'écran reçues par seconde	<ul style="list-style-type: none"> compteurs « fpolicy_server »*
latence_demande_max	Latence maximale pour une demande d'écran
demandes_en_attente	Nombre total de demandes d'écran en attente de réponse
latence_de_la_demande	Latence moyenne pour une demande d'écran
liste_latence_de_la_demande	Histogramme de latence pour les demandes d'écran
taux_envoyé_demande	Nombre de requêtes d'écran envoyées au serveur FPolicy par seconde
taux_de_réception_réponse	Nombre de réponses d'écran reçues du serveur FPolicy par seconde

Gérer le flux de travail FPolicy et la dépendance vis-à-vis d'autres technologies

NetApp recommande de désactiver une règle FPolicy avant d'apporter toute modification de la configuration. Par exemple, si vous souhaitez ajouter ou modifier une adresse IP dans le moteur externe configuré pour la stratégie activé, désactivez d'abord la stratégie.

Si vous configurez FPolicy pour surveiller les volumes NetApp FlexCache, NetApp vous recommande de ne pas configurer FPolicy pour surveiller les opérations de lecture et de fichier getattr. La surveillance de ces opérations dans ONTAP nécessite la récupération des données I2P (inode-to-path). Les données I2P ne pouvant pas être récupérées à partir de volumes FlexCache, elles doivent être récupérées à partir du volume d'origine. Le contrôle de ces opérations élimine donc les avantages de performance que FlexCache peut offrir.

Lorsque FPolicy et une solution antivirus externe sont déployés, la solution antivirus reçoit d'abord les notifications. Le traitement FPolicy démarre uniquement une fois l'analyse antivirus terminée. Il est important de dimensionner correctement les solutions antivirus, car une analyse antivirus lente peut affecter les performances globales.

Considérations relatives à la mise à niveau en lecture directe et au rétablissement

Vous devez connaître certaines considérations relatives à la mise à niveau et à la restauration avant de procéder à une mise à niveau vers une version de ONTAP qui prend en charge la lecture d'un mot de passe-passe ou avant de restaurer une version qui ne prend pas en charge la lecture d'un fichier passthrough.

Mise à niveau

Une fois que tous les nœuds sont mis à niveau vers une version de ONTAP qui prend en charge le mode de lecture intermédiaire FPolicy, le cluster est capable d'utiliser la fonctionnalité de lecture intermédiaire. Cependant, la lecture du mot de passe est désactivée par défaut sur les configurations FPolicy existantes. Pour utiliser la lecture passerelle sur les configurations FPolicy existantes, vous devez désactiver la règle FPolicy et modifier la configuration, puis réactiver la configuration.

Rétablissement

Avant de revenir à une version de ONTAP qui ne prend pas en charge la lecture passthrough FPolicy, vous devez remplir les conditions suivantes :

- Désactivez toutes les stratégies à l'aide de passthrough-read, puis modifiez les configurations affectées pour qu'elles n'utilisent pas passthrough-read.
- Désactivez la fonctionnalité FPolicy sur le cluster en désactivant chaque politique FPolicy sur le cluster.

Avant de revenir à une version de ONTAP qui ne prend pas en charge les magasins persistants, assurez-vous qu'aucune des règles FPolicy ne dispose d'un magasin persistant configuré. Si un magasin persistant est configuré, la restauration échouera.

Quelles sont les étapes de configuration d'une configuration FPolicy

Avant de pouvoir surveiller l'accès aux fichiers, FPolicy doit être créé et activé sur la machine virtuelle de stockage (SVM) pour laquelle les services FPolicy sont requis.

Les étapes de configuration et d'activation d'une configuration FPolicy sur le SVM sont les suivantes :

1. Créer un moteur externe FPolicy.

Le moteur externe FPolicy identifie les serveurs FPolicy externes associés à une configuration FPolicy spécifique. Si le moteur interne FPolicy « natif » est utilisé pour créer une configuration native de blocage de fichiers, il n'est pas nécessaire de créer un moteur externe FPolicy.

À partir de ONTAP 9.15.1, vous pouvez utiliser le `protobuf` format du moteur. Lorsqu'il est réglé sur `protobuf`, Les messages de notification sont codés sous forme binaire à l'aide de Google Protobuf. Avant de régler le format du moteur sur `protobuf`, Assurez-vous que le serveur FPolicy prend également en charge `protobuf` désérialisation. Pour plus d'informations, voir "[Planification de la configuration du moteur externe FPolicy](#)"

2. Créez un événement FPolicy.

Un événement FPolicy décrit ce que la règle FPolicy doit surveiller. Les événements consistent en des protocoles et des opérations de fichiers à surveiller et peuvent contenir une liste de filtres. Les événements utilisent des filtres pour restreindre la liste des événements surveillés pour lesquels le moteur externe FPolicy doit envoyer des notifications. Les événements spécifient également si la règle surveille les opérations de volume.

3. Créez un magasin persistant FPolicy (en option).

À partir de ONTAP 9.14.1, FPolicy vous permet de configurer votre système "magasins persistants" Pour capturer les événements d'accès aux fichiers pour les politiques asynchrones non obligatoires dans la SVM. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

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.

À partir de ONTAP 9.15.1, la configuration du stockage persistant FPolicy est simplifiée. Le `persistent-store-create` Automatise la création de volume pour le SVM et configure le volume pour le magasin persistant.

4. Créez une règle FPolicy.

Il incombe à la politique FPolicy d'associer, au périmètre approprié, l'ensemble des événements à surveiller et pour lesquels des notifications d'événements surveillés doivent être envoyées au serveur FPolicy désigné (ou au moteur natif si aucun serveur FPolicy n'est configuré). Cette politique définit également si le serveur FPolicy possède des droits d'accès privilégiés aux données pour lesquelles il reçoit des notifications. Un serveur FPolicy a besoin d'un accès privilégié si le serveur doit accéder aux données. Les cas d'utilisation classiques où un accès privilégié est nécessaire comprennent le blocage de fichiers, la gestion des quotas et la gestion hiérarchique du stockage. C'est l'endroit où vous spécifiez si la configuration de cette règle utilise un serveur FPolicy ou le serveur FPolicy interne « natif ».

Une stratégie spécifie si le filtrage est obligatoire. Si le filtrage est obligatoire et que tous les serveurs FPolicy sont en panne ou qu'aucune réponse n'est reçue des serveurs FPolicy dans une période de temporisation définie, l'accès aux fichiers est refusé.

Les limites d'une politique sont le SVM. Une politique ne peut s'appliquer à plusieurs SVM. Cependant, un SVM spécifique peut avoir plusieurs règles FPolicy, avec chacune des combinaisons de périmètre, d'événements et de configurations de serveur externes mêmes ou différentes.

5. Configuration de la portée de la règle

Le périmètre FPolicy détermine quels volumes, partages ou règles d'exportation agissent ou excluent par la surveillance. L'étendue détermine également quelles extensions de fichier doivent être incluses ou exclues de la surveillance FPolicy.



Les listes d'exclusion ont priorité sur les listes d'inclusion.

6. Activez la règle FPolicy.

Lorsque la stratégie est activée, les canaux de contrôle et, éventuellement, les canaux de données privilégiés sont connectés. Le processus FPolicy dédié aux nœuds sur lesquels le SVM participe à la surveillance de l'accès aux fichiers et aux dossiers. Pour les événements correspondant aux critères configurés, il envoie des notifications aux serveurs FPolicy (ou au moteur natif si aucun serveur FPolicy n'est configuré).



Si la stratégie utilise un blocage de fichiers natif, un moteur externe n'est pas configuré ou associé à la stratégie.

Planification de la configuration du moteur externe FPolicy

Planification de la configuration du moteur externe FPolicy

Avant de configurer le moteur externe FPolicy, vous devez comprendre la signification de la création d'un moteur externe et les paramètres de configuration disponibles. Ces informations vous aident à déterminer les valeurs à définir pour chaque paramètre.

Informations définies lors de la création du moteur externe FPolicy

La configuration de moteur externe définit les informations dont FPolicy a besoin pour établir et gérer des connexions aux serveurs externes FPolicy, notamment :

- Nom du SVM
- Nom du moteur
- Les adresses IP des serveurs FPolicy principaux et secondaires et le numéro de port TCP à utiliser lors de la connexion aux serveurs FPolicy
- Indique si le type de moteur est asynchrone ou synchrone
- Indique si le format du moteur est `xml` ou `protobuf`

À partir de ONTAP 9.15.1, vous pouvez utiliser le `protobuf` format du moteur. Lorsqu'il est réglé sur `protobuf`, Les messages de notification sont codés sous forme binaire à l'aide de Google Protobuf. Avant de régler le format du moteur sur `protobuf`, Assurez-vous que le serveur FPolicy prend également en charge `protobuf` désérialisation.

Étant donné que le format `protobuf` est pris en charge à partir de ONTAP 9.15.1, vous devez prendre en compte le format du moteur externe avant de revenir à une version antérieure de ONTAP. Si vous restaurez une version antérieure à ONTAP 9.15.1, contactez votre partenaire FPolicy pour :

- Modifiez chaque format de moteur de `protobuf` à `xml`
- Supprimer les moteurs avec un format de moteur de `protobuf`
- Authentification de la connexion entre le nœud et le serveur FPolicy

Si vous choisissez de configurer l'authentification SSL mutuelle, vous devez également configurer les paramètres qui fournissent les informations de certificat SSL.

- Comment gérer la connexion à l'aide de divers paramètres de privilèges avancés

Cela inclut des paramètres qui définissent des éléments tels que les valeurs de temporisation, les valeurs de relance, les valeurs de maintien de la vie, les valeurs maximales de demande, les valeurs de taille de tampon de réception et d'envoi, ainsi que les valeurs de temporisation de la session.

Le `vserver fpolicy policy external-engine create` Permet de créer un moteur externe FPolicy.

Quels sont les paramètres externes de base du moteur

Pour planifier la configuration, vous pouvez utiliser le tableau suivant des paramètres de configuration de base de FPolicy :

Type d'information	Option
--------------------	--------

<p>SVM</p> <p>Spécifie le nom du SVM que vous souhaitez associer à ce moteur externe.</p> <p>Chaque configuration FPolicy est définie au sein d'un seul SVM. Le moteur externe, l'événement de politique, l'étendue des règles et la politique associés pour créer une configuration de politique FPolicy doivent tous être associés au même SVM.</p>	<p><code>-vserver vserver_name</code></p>
<p>Nom du moteur</p> <p>Spécifie le nom à attribuer à la configuration du moteur externe. Vous devez spécifier le nom du moteur externe ultérieurement lors de la création de la règle FPolicy. Ceci associe le moteur externe à la politique.</p> <p>Le nom peut comporter jusqu'à 256 caractères.</p> <div data-bbox="167 720 220 772" data-label="Image"></div> <p>Le nom doit comporter jusqu'à 200 caractères si vous configurez le nom du moteur externe dans une configuration de reprise après incident de MetroCluster ou de SVM.</p> <p>Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants :</p> <ul style="list-style-type: none"> • a à z • A à Z • 0 à 9 • «»_», «»-", and ".» 	<p><code>-engine-name engine_name</code></p>
<p>Serveurs FPolicy primaires</p> <p>Spécifie les serveurs FPolicy principaux vers lesquels le nœud envoie des notifications pour une règle FPolicy donnée. La valeur est indiquée comme une liste d'adresses IP délimitée par des virgules.</p> <p>Si plusieurs adresses IP de serveur principal sont spécifiées, chaque nœud sur lequel le SVM participe crée une connexion de contrôle à chaque serveur FPolicy principal spécifié au moment de l'activation de la règle. Si vous configurez plusieurs serveurs FPolicy principaux, des notifications sont envoyées selon une séquence périodique aux serveurs FPolicy.</p> <p>Si le moteur externe est utilisé dans une configuration de reprise sur incident de MetroCluster ou de SVM, indiquez les adresses IP des serveurs FPolicy du site source en tant que serveurs principaux. Les adresses IP des serveurs FPolicy du site de destination doivent être spécifiées en tant que serveurs secondaires.</p>	<p><code>-primary-servers IP_address,...</code></p>
<p>Numéro de port</p> <p>Spécifie le numéro de port du service FPolicy.</p>	<p><code>-port integer</code></p>

<p><i>Serveurs FPolicy secondaires</i></p> <p>Spécifie les serveurs FPolicy secondaires vers lesquels envoyer les événements d'accès aux fichiers pour une politique FPolicy donnée. La valeur est indiquée comme une liste d'adresses IP délimitée par des virgules.</p> <p>Les serveurs secondaires sont utilisés uniquement lorsqu'aucun des serveurs primaires n'est accessible. Les connexions aux serveurs secondaires sont établies lorsque la stratégie est activée, mais les notifications sont envoyées aux serveurs secondaires uniquement si aucun des serveurs primaires n'est accessible. Si vous configurez plusieurs serveurs secondaires, des notifications sont envoyées aux serveurs FPolicy de manière périodique.</p>	<p>-secondary-servers IP_address,...</p>
<p><i>Type de moteur externe</i></p> <p>Indique si le moteur externe fonctionne en mode synchrone ou asynchrone. Par défaut, FPolicy fonctionne en mode synchrone.</p> <p>Lorsqu'il est réglé sur <code>synchronous</code>, Le traitement des requêtes de fichier envoie une notification au serveur FPolicy, mais ne se poursuit qu'après avoir reçu une réponse du serveur FPolicy. À ce stade, le flux de demande continue ou le traitement génère un déni, selon que la réponse du serveur FPolicy permet l'action demandée.</p> <p>Lorsqu'il est réglé sur <code>asynchronous</code>, Le traitement des requêtes de fichier envoie une notification au serveur FPolicy, puis continue.</p>	<p>-extern-engine-type external_engine_type La valeur de ce paramètre peut être l'une des suivantes :</p> <ul style="list-style-type: none"> • synchronous • asynchronous
<p><i>Format de moteur externe</i></p> <p>Spécifiez si le format du moteur externe est xml ou protobuf.</p> <p>À partir de ONTAP 9.15.1, vous pouvez utiliser le format du moteur protobuf. Lorsqu'ils sont définis sur protobuf, les messages de notification sont codés sous forme binaire à l'aide de Google Protobuf. Avant de définir le format du moteur sur protobuf, assurez-vous que le serveur FPolicy prend également en charge la désérialisation des protobuf.</p>	<p>- extern-engine-format {protobuf ou xml}</p>

<p><i>Option SSL pour la communication avec le serveur FPolicy</i></p> <p>Spécifie l'option SSL pour la communication avec le serveur FPolicy. Ce paramètre est obligatoire. Vous pouvez choisir l'une des options en fonction des informations suivantes :</p> <ul style="list-style-type: none"> Lorsqu'il est réglé sur <code>no-auth</code>, aucune authentification n'a lieu. <p>La liaison de communication est établie sur TCP.</p> <ul style="list-style-type: none"> Lorsqu'il est réglé sur <code>server-auth</code>, Le SVM authentifie le serveur FPolicy à l'aide de l'authentification du serveur SSL. Lorsqu'il est réglé sur <code>mutual-auth</code>, L'authentification mutuelle a lieu entre le SVM et le serveur FPolicy ; le SVM authentifie le serveur FPolicy et le serveur FPolicy authentifie le SVM. <p>Si vous choisissez de configurer l'authentification SSL mutuelle, vous devez également configurer l' <code>-certificate-common-name</code>, <code>-certificate-serial</code>, et <code>-certificate-ca</code> paramètres.</p>	<p><code>-ssl-option {no-auth</code></p>
<p><code>server-auth</code></p>	<p><code>mutual-auth}</code></p>
<p><i>FQDN du certificat ou nom commun personnalisé</i></p> <p>Spécifie le nom du certificat utilisé si l'authentification SSL entre le SVM et le serveur FPolicy est configurée. Vous pouvez spécifier le nom du certificat en tant que FQDN ou en tant que nom commun personnalisé.</p> <p>Si vous spécifiez <code>mutual-auth</code> pour le <code>-ssl-option</code> paramètre, vous devez spécifier une valeur pour le <code>-certificate-common-name</code> paramètre.</p>	<p><code>-certificate-common-name text</code></p>
<p><i>Numéro de série du certificat</i></p> <p>Spécifie le numéro de série du certificat utilisé pour l'authentification si l'authentification SSL entre le SVM et le serveur FPolicy est configurée.</p> <p>Si vous spécifiez <code>mutual-auth</code> pour le <code>-ssl-option</code> paramètre, vous devez spécifier une valeur pour le <code>-certificate-serial</code> paramètre.</p>	<p><code>-certificate-serial text</code></p>
<p><i>Autorité de certification</i></p> <p>Spécifie le nom de l'autorité de certification du certificat utilisé pour l'authentification si l'authentification SSL entre le SVM et le serveur FPolicy est configurée.</p> <p>Si vous spécifiez <code>mutual-auth</code> pour le <code>-ssl-option</code> paramètre, vous devez spécifier une valeur pour le <code>-certificate-ca</code> paramètre.</p>	<p><code>-certificate-ca text</code></p>

Quelles sont les options avancées du moteur externe

Vous pouvez utiliser le tableau suivant des paramètres de configuration avancée FPolicy pour personnaliser ou non votre configuration avec des paramètres avancés. Ces paramètres permettent de modifier le comportement de communication entre les nœuds du cluster et les serveurs FPolicy :

Type d'information	Option
<p><i>Délai d'annulation d'une demande</i></p> <p>Spécifie l'intervalle de temps en heures (h), minutes (m), ou secondes (s) Que le nœud attend une réponse du serveur FPolicy.</p> <p>Si l'intervalle de temporisation passe, le nœud envoie une requête d'annulation au serveur FPolicy. Le nœud envoie ensuite la notification à un autre serveur FPolicy. Ce délai aide à gérer un serveur FPolicy qui ne répond pas, ce qui peut améliorer la réponse des clients SMB/NFS. Par ailleurs, l'annulation des demandes après une période de temporisation peut faciliter la libération des ressources système, car la demande de notification est déplacée d'un serveur FPolicy défaillant/défectueux vers un autre serveur FPolicy.</p> <p>La plage de cette valeur est de 0 à 100. Si la valeur est définie sur 0, L'option est désactivée et les messages de requête d'annulation ne sont pas envoyés au serveur FPolicy. La valeur par défaut est 20s.</p>	<p>-reqs-cancel-timeout integer[h</p>
m	s]
<p><i>Délai d'attente pour l'abandon d'une demande</i></p> <p>Spécifie le délai d'expiration en heures (h), minutes (m), ou secondes (s) pour l'abandon d'une demande.</p> <p>La plage de cette valeur est de 0 à 200.</p>	<p>-reqs-abort-timeout `integer[h</p>
m	s]
<p><i>Intervalle pour l'envoi de demandes d'état</i></p> <p>Spécifie l'intervalle en heures (h), minutes (m), ou secondes (s) Après quoi une requête d'état est envoyée au serveur FPolicy.</p> <p>La plage de cette valeur est de 0 à 50. Si la valeur est définie sur 0, L'option est désactivée et les messages de requête d'état ne sont pas envoyés au serveur FPolicy. La valeur par défaut est 10s.</p>	<p>-status-req-interval integer[h</p>
m	s]
<p><i>Nombre maximal de requêtes en attente sur le serveur FPolicy</i></p> <p>Spécifie le nombre maximal de requêtes en attente pouvant être mises en file d'attente sur le serveur FPolicy.</p> <p>La plage de cette valeur est de 1 à 10000. La valeur par défaut est 500.</p>	<p>-max-server-reqs integer</p>

<p><i>Timeout pour la déconnexion d'un serveur FPolicy non réactif</i></p> <p>Spécifie l'intervalle de temps en heures (h), minutes (m), ou secondes (s) Après quoi la connexion au serveur FPolicy est interrompue.</p> <p>La connexion est interrompue après le délai d'expiration uniquement si la file d'attente du serveur FPolicy contient le nombre maximal de requêtes autorisées et qu'aucune réponse n'est reçue dans le délai d'expiration. Le nombre maximal de demandes est de 50 (valeur par défaut) ou le numéro spécifié par le <code>max-server-reqs</code> paramètre.</p> <p>La plage de cette valeur est de 1 à 100. La valeur par défaut est 60s.</p>	<pre>-server-progress -timeout integer[h</pre>
m	s]
<p><i>Intervalle d'envoi de messages de maintien de la disponibilité au serveur FPolicy</i></p> <p>Spécifie l'intervalle de temps en heures (h), minutes (m), ou secondes (s) À laquelle les messages de maintien de la disponibilité sont envoyés au serveur FPolicy.</p> <p>Les messages de maintien de la vie détectent les connexions à demi-ouverture.</p> <p>La plage de cette valeur est de 10 à 600. Si la valeur est définie sur 0, L'option est désactivée et les messages de maintien en service ne peuvent pas être envoyés aux serveurs FPolicy. La valeur par défaut est 120s.</p>	<pre>-keep-alive-interval-integer[h</pre>
m	s]
<p><i>Tentatives de reconnexion maximales</i></p> <p>Spécifie le nombre maximal de fois que le SVM tente de se reconnecter au serveur FPolicy une fois la connexion interrompue.</p> <p>La plage de cette valeur est de 0 à 20. La valeur par défaut est 5.</p>	<pre>-max-connection-retries integer</pre>
<p><i>Taille du tampon de réception</i></p> <p>Spécifie la taille du tampon de réception du socket connecté pour le serveur FPolicy.</p> <p>La valeur par défaut est 256 kilo-octets (Ko). Lorsque la valeur est définie sur 0, la taille du tampon de réception est définie sur une valeur définie par le système.</p> <p>Par exemple, si la taille par défaut de la mémoire tampon de réception du socket est de 65536 octets, en définissant la valeur ajustable sur 0, la taille de la mémoire tampon de socket est définie sur 65536 octets. Vous pouvez utiliser n'importe quelle valeur autre que celle par défaut pour définir la taille (en octets) du tampon de réception.</p>	<pre>-recv-buffer-size integer</pre>

<p><i>Envoyer la taille du tampon</i></p> <p>Spécifie la taille du tampon d'envoi du socket connecté pour le serveur FPolicy.</p> <p>La valeur par défaut est 256 kilo-octets (Ko). Lorsque la valeur est définie sur 0, la taille du tampon d'envoi est définie sur une valeur définie par le système.</p> <p>Par exemple, si la taille par défaut du tampon d'envoi du socket est définie sur 65536 octets, en définissant la valeur ajustable sur 0, la taille de la mémoire tampon du socket est définie sur 65536 octets. Vous pouvez utiliser n'importe quelle valeur autre que celle par défaut pour définir la taille (en octets) du tampon d'envoi.</p>	<pre>-send-buffer-size integer</pre>
<p><i>Délai de purge d'un ID de session pendant la reconnexion</i></p> <p>Spécifie l'intervalle en heures (h), minutes (m), ou secondes (s) Après quoi un nouvel ID de session est envoyé au serveur FPolicy pendant les tentatives de reconnexion.</p> <p>Si la connexion entre le contrôleur de stockage et le serveur FPolicy est interrompue et la reconnexion est effectuée au sein du <code>-session -timeout</code> Intervalle, l'ancien ID de session est envoyé au serveur FPolicy pour qu'il puisse envoyer les réponses aux anciennes notifications.</p> <p>La valeur par défaut est définie sur 10 secondes.</p>	<pre>-session-timeout [integerh][integerm][integer s]</pre>

Informations supplémentaires sur la configuration des moteurs externes FPolicy pour utiliser les connexions authentifiées SSL

Vous devez connaître des informations supplémentaires pour configurer le moteur externe FPolicy de façon à utiliser le protocole SSL lors de la connexion aux serveurs FPolicy.

Authentification de serveur SSL

Si vous choisissez de configurer le moteur externe FPolicy pour l'authentification du serveur SSL, vous devez installer le certificat public de l'autorité de certification (CA) qui a signé le certificat du serveur FPolicy avant de créer le moteur externe.

Authentification mutuelle

Si vous configurez les moteurs externes FPolicy pour utiliser l'authentification mutuelle SSL lors du raccordement des LIF de données des machines virtuelles de stockage aux serveurs FPolicy externes, avant de créer le moteur externe, Vous devez installer le certificat public de l'autorité de certification qui a signé le certificat du serveur FPolicy avec le certificat public et le fichier de clé pour l'authentification de la SVM. Vous ne devez pas supprimer ce certificat lorsque des règles FPolicy utilisent le certificat installé.

Si le certificat est supprimé pendant que FPolicy l'utilise pour l'authentification mutuelle lors de la connexion à un serveur FPolicy externe, vous ne pouvez pas réactiver une règle FPolicy désactivée qui utilise ce certificat. La politique FPolicy ne peut pas être réactivée dans ce cas, même si un nouveau certificat avec les mêmes paramètres est créé et installé sur le SVM.

Si le certificat a été supprimé, vous devez installer un nouveau certificat, créer de nouveaux moteurs externes FPolicy utilisant le nouveau certificat et associer les nouveaux moteurs externes à la politique FPolicy que vous souhaitez réactiver en modifiant la règle FPolicy.

Installer les certificats pour SSL

Le certificat public de l'autorité de certification utilisé pour signer le certificat du serveur FPolicy est installé à l'aide du `security certificate install` commande avec `-type` paramètre défini sur `client-ca`. La clé privée et le certificat public requis pour l'authentification de la SVM sont installés à l'aide de `security certificate install` commande avec `-type` paramètre défini sur `server`.

Les certificats ne sont pas répliqués dans les relations de SVM de reprise après incident avec une configuration sans ID-preserve

Les certificats de sécurité utilisés pour l'authentification SSL lors des connexions aux serveurs FPolicy ne répliquent pas les données vers des destinations de reprise après incident des SVM avec des configurations sans ID-preserve. Bien que la configuration du moteur externe FPolicy sur le SVM soit répliquée, les certificats de sécurité ne sont pas répliqués. Vous devez installer manuellement les certificats de sécurité sur la destination.

Lorsque vous configurez la relation de SVM Disaster Recovery, la valeur que vous sélectionnez pour le `-identity-preserve` de la `snamirror create` La commande détermine les détails de configuration répliqués dans le SVM de destination.

Si vous définissez le `-identity-preserve` option à `true` (ID-preserve), tous les détails de la configuration FPolicy sont répliqués, y compris les informations du certificat de sécurité. Vous devez installer les certificats de sécurité sur la destination uniquement si vous définissez l'option sur `false` (Non-ID-preserve).

Restrictions liées aux moteurs externes FPolicy avec configurations de reprise après incident MetroCluster et SVM

Vous pouvez créer un moteur externe FPolicy à étendue du cluster en attribuant la machine virtuelle de stockage du cluster (SVM) au moteur externe. Cependant, lors de la création d'un moteur externe « cluster-scoped » dans une configuration de reprise après incident de MetroCluster ou de SVM, il existe certaines restrictions lors du choix de la méthode d'authentification utilisée par le SVM pour la communication externe avec le serveur FPolicy.

Il existe trois options d'authentification que vous pouvez choisir lors de la création de serveurs FPolicy externes : aucune authentification, authentification de serveur SSL et authentification mutuelle SSL. Bien qu'il n'y ait aucune restriction lors du choix de l'option d'authentification si le serveur FPolicy externe est affecté à un SVM de données, il existe des restrictions lors de la création d'un moteur externe FPolicy d'étendue au cluster :

Configuration	Autorisé ?
Reprise après incident de MetroCluster ou SVM et moteur externe FPolicy à étendue du cluster sans authentification (le protocole SSL n'est pas configuré)	Oui.

Reprise après incident de MetroCluster ou SVM et moteur externe FPolicy à étendue du cluster avec serveur SSL ou authentification mutuelle SSL	Non
--	-----

- En cas d'existence d'un moteur externe FPolicy avec authentification SSL et que vous souhaitez créer une configuration de reprise après incident MetroCluster ou SVM, vous devez modifier ce moteur externe afin qu'il n'utilise aucune authentification ou supprimer le moteur externe avant de créer la configuration de reprise après incident MetroCluster ou SVM.
- Si la configuration de reprise après incident de MetroCluster ou SVM existe déjà, ONTAP vous empêche de créer un moteur externe FPolicy à étendue du cluster avec l'authentification SSL.

Remplir la fiche de configuration du moteur externe FPolicy

Vous pouvez utiliser cette fiche technique pour enregistrer les valeurs nécessaires lors du processus de configuration du moteur externe FPolicy. Si une valeur de paramètre est requise, vous devez déterminer la valeur à utiliser pour ces paramètres avant de configurer le moteur externe.

Informations concernant la configuration de base d'un moteur externe

Vous devez indiquer si vous souhaitez inclure chaque paramètre dans la configuration du moteur externe, puis enregistrer la valeur des paramètres que vous souhaitez inclure.

Type d'information	Obligatoire	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	Oui.	
Nom du moteur	Oui.	Oui.	
Serveurs FPolicy principaux	Oui.	Oui.	
Numéro de port	Oui.	Oui.	
Serveurs FPolicy secondaires	Non		
Type de moteur externe	Non		
Option SSL pour la communication avec le serveur FPolicy externe	Oui.	Oui.	
Nom de domaine complet du certificat ou nom commun personnalisé	Non		
Numéro de série du certificat	Non		
Autorité de certification	Non		

Informations relatives aux paramètres avancés du moteur externe

Pour configurer un moteur externe avec des paramètres avancés, vous devez saisir la commande de configuration en mode Advanced Privilege.

Type d'information	Obligatoire	Inclure	Vos valeurs
Délai d'annulation d'une demande	Non		
Délai d'abandon d'une demande	Non		
Intervalle d'envoi des demandes d'état	Non		
Nombre maximal de requêtes en attente sur le serveur FPolicy	Non		
Délai de déconnexion d'un serveur FPolicy non réactif	Non		
Intervalle d'envoi de messages de sauvegarde au serveur FPolicy	Non		
Nombre maximal de tentatives de reconnexion	Non		
Taille de la mémoire tampon de réception	Non		
Taille de la mémoire tampon d'envoi	Non		
Délai de purge d'un ID de session pendant la reconnexion	Non		

Planification de la configuration des événements FPolicy

Planifier l'présentation de la configuration des événements FPolicy

Avant de configurer des événements FPolicy, vous devez comprendre ce qu'il signifie pour créer un événement FPolicy. Vous devez déterminer les protocoles à surveiller, les événements à surveiller et les filtres d'événements à utiliser. Ces informations vous aident à planifier les valeurs que vous souhaitez définir.

Ce qu'il signifie pour créer un événement FPolicy

La création de l'événement FPolicy consiste à définir les informations nécessaires au processus FPolicy pour déterminer les opérations d'accès aux fichiers à surveiller et pour lesquelles des notifications d'événements surveillés doivent être envoyées au serveur FPolicy externe. La configuration des événements FPolicy définit les informations de configuration suivantes :

- Nom de la machine virtuelle de stockage (SVM)

- Nom de l'événement
- Les protocoles à surveiller

FPolicy peut surveiller les opérations d'accès aux fichiers SMB, NFSv3 et NFSv4, et, à partir de ONTAP 9.15.1, NFSv4.1.

- Quelles opérations de fichier surveiller

Toutes les opérations de fichier ne sont pas valides pour chaque protocole.

- Les filtres de fichier à configurer

Seules certaines combinaisons d'opérations de fichier et de filtres sont valides. Chaque protocole dispose de son propre ensemble de combinaisons prises en charge.

- Contrôler le montage et le démontage de volumes






Il y a une dépendance avec trois des paramètres (`-protocol`, `-file-operations`, `-filters`). Les combinaisons suivantes sont valides pour les trois paramètres :

- Vous pouvez spécifier le `-protocol` et `-file-operations` paramètres.
- Vous pouvez spécifier les trois paramètres.
- Vous ne pouvez spécifier aucun des paramètres.

Contenu de la configuration des événements FPolicy

Pour vous aider à planifier votre configuration, vous pouvez utiliser la liste suivante de paramètres de configuration des événements FPolicy disponibles :

Type d'information	Option
<p>SVM</p> <p>Spécifie le nom du SVM que vous souhaitez associer à cet événement FPolicy.</p> <p>Chaque configuration FPolicy est définie au sein d'un seul SVM. Le moteur externe, l'événement de politique, l'étendue des règles et la politique associés pour créer une configuration de politique FPolicy doivent tous être associés au même SVM.</p>	<p><code>-vserver vserver_name</code></p>

<p>Nom de l'événement</p> <p>Spécifie le nom à attribuer à l'événement FPolicy. Lorsque vous créez la politique FPolicy, vous associez l'événement FPolicy à la règle à l'aide du nom de l'événement.</p> <p>Le nom peut comporter jusqu'à 256 caractères.</p> <div data-bbox="167 401 220 457">  </div> <p>Le nom doit comporter jusqu'à 200 caractères si vous configurez l'événement dans une configuration de reprise d'activité de MetroCluster ou de SVM.</p> <p>Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants :</p> <ul style="list-style-type: none"> • a à z • A à Z • 0 à 9 • « _ ", "' -, and ". » 	<p><code>-event-name event_name</code></p>
<p>Protocole</p> <p>Spécifie le protocole à configurer pour l'événement FPolicy. La liste pour <code>-protocol</code> peut inclure l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> • cifs • nfsv3 • nfsv4 <div data-bbox="167 1283 220 1339">  </div> <p>Si vous spécifiez <code>-protocol</code>, vous devez alors spécifier une valeur valide dans l' <code>-file-operations</code> paramètre. Au fur et à mesure que la version du protocole change, les valeurs valides peuvent changer.</p> <div data-bbox="167 1440 220 1497">  </div> <p>À partir de ONTAP 9.15.1, nfsv4 vous permet de capturer les événements NFSv4.0 et NFSv4.1.</p>	<p><code>-protocol protocol</code></p>

Opérations_fichier

Spécifie la liste des opérations sur les fichiers pour l'événement FPolicy.

L'événement vérifie les opérations spécifiées dans cette liste à partir de toutes les demandes client utilisant le protocole spécifié dans `-protocol` paramètre. Vous pouvez lister une ou plusieurs opérations de fichier à l'aide d'une liste délimitée par des virgules. La liste pour `-file-operations` peut inclure une ou plusieurs des valeurs suivantes :

- `close` pour les opérations de fermeture de fichier
- `create` pour les opérations de création de fichier
- `create-dir` pour les opérations de création de répertoire
- `delete` pour les opérations de suppression de fichier
- `delete_dir` pour les opérations de suppression de répertoire
- `getattr` pour obtenir les opérations d'attribut
- `link` pour les opérations de liaison
- `lookup` pour les opérations de recherche
- `open` pour les opérations d'ouverture de fichier
- `read` pour les opérations de lecture de fichiers
- `write` pour les opérations d'écriture de fichiers
- `rename` pour les opérations de renommage de fichiers
- `rename_dir` pour les opérations de renommage de répertoire
- `setattr` pour les opérations de définition d'attribut
- `symlink` pour les opérations de lien symbolique



Si vous spécifiez `-file-operations`, vous devez alors spécifier un protocole valide dans l' `-protocol` paramètre.

`-file-operations`
`file_operations,...`

Filtres

-filters filter, ...

Spécifie la liste des filtres pour une opération de fichier donnée pour le protocole spécifié. Les valeurs dans le `-filters` paramètre utilisé pour filtrer les demandes client. La liste peut comprendre un ou plusieurs des éléments suivants :



Si vous spécifiez le `-filters` paramètre, vous devez ensuite spécifier également des valeurs valides pour le `-file-operations` et `-protocol` paramètres.

- `monitor-ads` option permettant de filtrer la demande client pour un autre flux de données.
- `close-with-modification` option permettant de filtrer la demande client pour fermer avec modification.
- `close-without-modification` option permettant de filtrer la demande client pour la fermeture sans modification.
- `first-read` option permettant de filtrer la demande client pour la première lecture.
- `first-write` option permettant de filtrer la demande client pour la première écriture.
- `offline-bit` option permettant de filtrer la demande client pour le jeu de bits hors ligne.

La configuration de ce filtre permet au serveur FPolicy de recevoir une notification uniquement lorsque des fichiers hors ligne sont utilisés.

- `open-with-delete-intent` option permettant de filtrer la demande client pour ouvrir avec l'intention de suppression.

La configuration de ce filtre entraîne la réception d'une notification sur le serveur FPolicy uniquement lorsqu'une tentative est effectuée pour ouvrir un fichier avec l'intention de le supprimer. Ceci est utilisé par les systèmes de fichiers lorsque `FILE_DELETE_ON_CLOSE` l'indicateur est spécifié.

- `open-with-write-intent` option permettant de filtrer la demande client pour ouvrir avec une intention d'écriture.

La configuration de ce filtre entraîne la réception d'une notification sur le serveur FPolicy uniquement lorsqu'une tentative est effectuée pour ouvrir un fichier avec l'intention d'y écrire un objet.

- `write-with-size-change` option permettant de filtrer la demande d'écriture client avec changement de taille.
- `setattr-with-owner-change` option permettant de filtrer les demandes `setattr` du client pour changer le propriétaire d'un fichier ou d'un répertoire.
- `setattr-with-group-change` option permettant de filtrer les demandes `setattr` du client pour changer le groupe d'un fichier ou d'un répertoire.

`setattr-with-sacl-change` Option permettant de filtrer les demandes `setattr` du client pour changer la SACL sur un fichier ou un

<p><i>Est une opération de volume requise</i></p> <p>Spécifie si une surveillance est requise pour les opérations de montage et de démontage de volumes. La valeur par défaut est <code>false</code>.</p>	<pre>-volume-operation {true</pre>
<pre>false}</pre> <pre>-filters filter, ...</pre>	<p><i>Notifications de refus d'accès FPolicy</i></p> <p>À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Ces notifications sont précieuses pour la sécurité, la protection contre les ransomware et la gouvernance. Des notifications seront générées pour l'opération de fichier ayant échoué en raison d'un manque d'autorisation, notamment :</p> <ul style="list-style-type: none"> • Défaillances dues aux autorisations NTFS. • Échecs dus aux bits de mode Unix. • Défaillances dues à des ACL NFSv4.
<pre>-monitor-fileop-failure {true</pre>	<pre>false}</pre>

• **Opérations de fichiers et combinaisons de filtres prises en charge que FPolicy peut surveiller pour SMB** : `exclude-directory` option permettant de filtrer les demandes client pour les opérations d'annuaire.

Lorsque ce filtre est spécifié, les opérations du répertoire ne sont pas surveillées. Lorsque vous configurez votre événement FPolicy, vous devez savoir que seules certaines combinaisons d'opérations et de filtres sont prises en charge pour la surveillance des opérations d'accès aux fichiers SMB.

Le tableau suivant fournit la liste des combinaisons d'opérations de fichiers et de filtres prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers SMB :

Opérations de fichiers prises en charge	Filtres pris en charge
fermer	surveillance-ads, hors ligne-bit, fermeture-avec-modification, fermeture-sans-modification, gros-avec-lecture, exclure-répertoire
création	surveillance-ads, hors ligne-bit

dir_de_création	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
supprimer	surveillance-ads, hors ligne-bit
dir_de_suppression	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
getattr	offline-bit, exclude-dir
la transparence	monitor-ads, offline-bit, open-with-delete-intentionnel, open-with-write-intentions, exclude-dir
lecture	surveillance-ads, hors-ligne-bit, première lecture
écriture	surveillance-ads, hors-ligne-bit, première-écriture, écriture-avec-changement de taille
renommer	surveillance-ads, hors ligne-bit
rename_dir	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
définir	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Le tableau suivant répertorie les combinaisons de filtres et d'opérations de fichiers refusés d'accès pris en charge pour la surveillance FPolicy des événements d'accès aux fichiers SMB :

Opération de fichier d'accès refusé prise en charge	Filtres pris en charge
la transparence	NA

Opérations de fichiers et combinaisons de filtres prises en charge pouvant être moniteurs par FPolicy pour NFSv3

Lorsque vous configurez votre événement FPolicy, vous devez savoir que seules certaines combinaisons d'opérations sur les fichiers et de filtres sont prises en charge pour surveiller les opérations d'accès aux fichiers NFSv3.

Le tableau suivant répertorie les opérations de fichiers et les combinaisons de filtres prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv3 :

Opérations de fichiers prises en charge	Filtres pris en charge
création	bit hors ligne
dir_de_création	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
supprimer	bit hors ligne
dir_de_suppression	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
lien	bit hors ligne
recherche	offline-bit, exclude-dir
lecture	bit hors ligne, première lecture
écriture	bit hors ligne, première écriture, écriture avec changement de taille
renommer	bit hors ligne
rename_dir	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
définir	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modif_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	bit hors ligne

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Le tableau suivant répertorie les combinaisons de filtres et d'opérations de fichiers refusés d'accès prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv3 :

Opération de fichier d'accès refusé prise en charge	Filtres pris en charge
l'accès	NA
création	NA
dir_de_création	NA
supprimer	NA
dir_de_suppression	NA

lien	NA
lecture	NA
renommer	NA
rename_dir	NA
définir	NA
écriture	NA

Opérations de fichiers et combinaisons de filtres prises en charge que FPolicy peut surveiller pour NFSv4

Lorsque vous configurez votre événement FPolicy, vous devez savoir que seules certaines combinaisons d'opérations et de filtres sont prises en charge pour surveiller les opérations d'accès aux fichiers NFSv4.

À partir de ONTAP 9.15.1, FPolicy prend en charge le protocole NFSv4.1.

La liste des opérations de fichiers et des combinaisons de filtres prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv4 ou NFSv4.1 est fournie dans le tableau suivant :

Opérations de fichiers prises en charge	Filtres pris en charge
fermer	bit hors ligne, répertoire d'exclusion
création	bit hors ligne
dir_de_création	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
supprimer	bit hors ligne
dir_de_suppression	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
getattr	bit hors ligne, répertoire d'exclusion
lien	bit hors ligne
recherche	bit hors ligne, répertoire d'exclusion
la transparence	bit hors ligne, répertoire d'exclusion
lecture	bit hors ligne, première lecture

écriture	bit hors ligne, première écriture, écriture avec changement de taille
renommer	bit hors ligne
rename_dir	Aucun filtre n'est actuellement pris en charge pour cette opération de fichier.
définir	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	bit hors ligne

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. La liste des combinaisons de filtres et d'opérations de fichiers refusés d'accès prises en charge pour la surveillance FPolicy des événements d'accès aux fichiers NFSv4 ou NFSv4.1 est fournie dans le tableau suivant :

Opération de fichier d'accès refusé prise en charge	Filtres pris en charge
l'accès	NA
création	NA
dir_de_création	NA
supprimer	NA
dir_de_suppression	NA
lien	NA
la transparence	NA
lecture	NA
renommer	NA
rename_dir	NA
définir	NA
écriture	NA

Remplissez la fiche de configuration des événements FPolicy

Vous pouvez utiliser cette fiche pour enregistrer les valeurs nécessaires lors du processus de configuration des événements FPolicy. Si une valeur de paramètre est requise, vous devez déterminer la valeur à utiliser pour ces paramètres avant de configurer l'événement FPolicy.

Vous devez indiquer si vous souhaitez inclure chaque paramètre dans la configuration des événements FPolicy, puis noter la valeur des paramètres que vous souhaitez inclure.

Type d'information	Obligatoire	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	Oui.	
Nom de l'événement	Oui.	Oui.	
Protocole	Non		
Opérations sur les fichiers	Non		
Filtres	Non		
Opération de volume	Non		
Événements d'accès refusé (Support à partir de ONTAP 9.13)	Non		

Planifiez la configuration de la règle FPolicy

Planifier l'présentation de la configuration de la règle FPolicy

Avant de configurer la règle FPolicy, vous devez comprendre les paramètres requis lors de la création de la règle ainsi que les raisons pour lesquelles vous pouvez vouloir configurer certains paramètres facultatifs. Ces informations vous aident à déterminer les valeurs à définir pour chaque paramètre.

Lors de la création d'une politique FPolicy, vous associez cette règle à ce qui suit :


- Le serveur virtuel de stockage (SVM)
- Un ou plusieurs événements FPolicy
- Moteur externe FPolicy

Vous pouvez également configurer plusieurs paramètres de stratégie facultatifs.

Contenu de la configuration des règles FPolicy

Vous pouvez utiliser la liste suivante de règles FPolicy disponibles et de paramètres facultatifs pour vous aider

à planifier votre configuration :

Type d'information	Option	Obligatoire	Valeur par défaut
<p><i>Nom du SVM</i></p> <p>Spécifie le nom du SVM sur lequel vous souhaitez créer une politique FPolicy.</p>	<p>-vserver vserver_name</p>	Oui.	Aucune
<p><i>Nom de la politique</i></p> <p>Spécifie le nom de la politique FPolicy.</p> <p>Le nom peut comporter jusqu'à 256 caractères.</p> <div>  <p>Le nom doit comporter jusqu'à 200 caractères si la stratégie est configurée dans une configuration de reprise après incident de MetroCluster ou de SVM.</p> </div> <p>Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants :</p> <ul style="list-style-type: none"> • a à z • A à Z • 0 à 9 • «»_», «»-", and ".» 	<p>-policy-name policy_name</p>	Oui.	Aucune

<p><i>Noms d'événements</i></p> <p>Spécifie une liste d'événements séparés par des virgules à associer à la politique FPolicy.</p> <ul style="list-style-type: none"> • Vous pouvez associer plusieurs événements à une stratégie. • Un événement est spécifique à un protocole. • Vous pouvez utiliser une seule stratégie pour surveiller les événements d'accès aux fichiers pour plusieurs protocoles en créant un événement pour chaque protocole que la stratégie doit surveiller, puis en associant les événements à la stratégie. • Les événements doivent déjà exister. 	<pre>-events event_name, ...</pre>	Oui.	Aucune
<p><i>Magasin permanent</i></p> <p>Depuis la version ONTAP 9.14.1, ce paramètre spécifie le magasin persistant qui capture les événements d'accès aux fichiers pour des politiques asynchrones non obligatoires dans la SVM.</p>	<pre>-persistent -store persistent_stor e_name</pre>	Non	Aucune

<p><i>Nom du moteur externe</i></p> <p>Spécifie le nom du moteur externe à associer à la politique FPolicy.</p> <ul style="list-style-type: none"> • Un moteur externe contient les informations requises par le nœud pour envoyer des notifications à un serveur FPolicy. • Vous pouvez configurer FPolicy de façon à utiliser le moteur externe natif ONTAP pour simplifier le blocage des fichiers ou à utiliser un moteur externe configuré pour utiliser des serveurs FPolicy externes (serveurs FPolicy) pour obtenir des fonctions plus sophistiquées de blocage et de gestion des fichiers. • Si vous souhaitez utiliser le moteur externe natif, vous ne pouvez pas spécifier de valeur pour ce paramètre ou vous pouvez le spécifier <code>native</code> comme valeur. • Si vous souhaitez utiliser des serveurs FPolicy, la configuration du moteur externe doit déjà exister. 	<p><code>-engine</code> <code>engine_name</code></p>	<p>Oui (à moins que la politique n'utilise le moteur natif ONTAP interne)</p>	<p><code>native</code></p>
<p><i>Est un screening obligatoire</i></p> <p>Indique si un filtrage d'accès aux fichiers obligatoire est requis.</p> <ul style="list-style-type: none"> • Le paramètre de filtrage obligatoire détermine quelle action est prise en cas d'incident d'accès aux fichiers lorsque tous les serveurs principaux et secondaires sont en panne ou qu'aucune réponse n'est reçue des serveurs FPolicy au cours d'une période de temporisation donnée. • Lorsqu'il est réglé sur <code>true</code>, les événements d'accès aux fichiers sont refusés. • Lorsqu'il est réglé sur <code>false</code>, les événements d'accès aux fichiers sont autorisés. 	<p><code>-is-mandatory</code> <code>{true</code></p>	<p><code>false}</code></p>	<p>Non</p>

true	<p>Autoriser l'accès privilégié</p> <p>Indique si vous souhaitez que le serveur FPolicy possède un accès privilégié aux fichiers et dossiers surveillés à l'aide d'une connexion de données privilégiée.</p> <p>S'ils sont configurés, les serveurs FPolicy peuvent accéder aux fichiers à partir de la racine de l'SVM contenant les données surveillées à l'aide de la connexion de données privilégiée.</p> <p>Pour l'accès privilégié aux données, SMB doit être sous licence sur le cluster et toutes les LIFs de données utilisées pour se connecter aux serveurs FPolicy doivent être configurées de ce fait <code>cifs</code> comme l'un des protocoles autorisés.</p> <p>Si vous souhaitez configurer la policy pour autoriser les accès privilégiés, vous devez également spécifier le nom d'utilisateur du compte que vous souhaitez que le serveur FPolicy utilise pour cet accès privilégié.</p>	<p>-allow -privileged -access {yes</p>	no}
------	--	--	-----

Non (sauf si la lecture passthrough est activée)	no	<p><i>Nom d'utilisateur privilégié</i></p> <p>Spécifie le nom d'utilisateur du compte que les serveurs FPolicy utilisent pour l'accès aux données privilégié.</p> <ul style="list-style-type: none"> • La valeur de ce paramètre doit utiliser le format "daomain\user name". • Si -allow -privileged -access est défini sur no, toute valeur définie pour ce paramètre est ignorée. 	<p>-privileged</p> <p>-user-name</p> <p>user_name</p>
--	----	--	---

Non (sauf si l'accès privilégié est activé)	Aucune	<p><i>Autoriser la lecture_passthrough</i></p> <p>Spécifie si les serveurs FPolicy peuvent fournir des services de passe-lecture pour les fichiers qui ont été archivés sur le stockage secondaire (fichiers hors ligne) par les serveurs FPolicy :</p> <ul style="list-style-type: none"> • Passthrough-read est un moyen de lire les données pour les fichiers hors ligne sans restaurer les données dans le stockage primaire. <p>La lecture Passthrough réduit les latences de réponse. Les fichiers ne sont donc pas rappelés dans le stockage primaire, ce qui évite de l'avoir à remonter pour répondre à la demande de lecture. De plus, la lecture intermédiaire optimise l'efficacité du stockage puisque vous n'avez plus besoin d'utiliser l'espace de stockage principal avec des fichiers rappelés uniquement pour satisfaire les demandes de lecture.</p>	<p>-is-passthrough -read-enabled {true</p>
---	--------	---	--

Condition pour les configurations de l'étendue FPolicy si la politique FPolicy utilise le moteur natif

Si vous configurez la règle FPolicy pour utiliser le moteur natif, il existe une condition spécifique à la définition du périmètre FPolicy configuré pour la règle.

Le périmètre FPolicy définit les limites de la règle FPolicy s'applique, par exemple, si la FPolicy s'applique à des volumes ou des partages spécifiés. Un certain nombre de paramètres limitent davantage l'étendue à laquelle la politique FPolicy s'applique. L'un de ces paramètres, `-is-file-extension-check-on-directories-enabled` indique s'il faut vérifier les extensions de fichier sur les répertoires. La valeur par défaut est `false`, ce qui signifie que les extensions de fichiers des répertoires ne sont pas vérifiées.

Lorsqu'une politique de FPolicy utilisant le moteur natif est activée sur un partage ou un volume et sur `-is-file-extension-check-on-directories-enabled` le paramètre est défini sur `false` pour le périmètre de la politique, l'accès au répertoire est refusé. Avec cette configuration, car les extensions de fichier ne sont pas vérifiées pour les répertoires, toute opération de répertoire est refusée si elle relève de la portée de la stratégie.

Pour vous assurer que l'accès au répertoire a réussi lors de l'utilisation du moteur natif, vous devez définir le `-is-file-extension-check-on-directories-enabled` paramètre à `true` lors de la création de la portée.

Avec ce paramètre défini sur `true`, Les contrôles d'extension se produisent pour les opérations d'annuaire et la décision d'autoriser ou de refuser l'accès est prise en fonction des extensions incluses ou exclues dans la configuration du périmètre FPolicy.

Remplissez la fiche de règles FPolicy

Vous pouvez utiliser cette fiche pour enregistrer les valeurs nécessaires lors du processus de configuration de la politique FPolicy. Il est important d'enregistrer si vous souhaitez inclure chaque paramètre dans la configuration de la règle FPolicy, puis d'enregistrer la valeur des paramètres à inclure.

Type d'information	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	
Nom de la règle	Oui.	
Noms des événements	Oui.	
Stockage persistant		
Nom du moteur externe		
Un screening obligatoire est-il requis ?		
Autoriser l'accès privilégié		

Nom d'utilisateur privilégié		
La lecture passthrough est-elle activée ?		

Planification de la configuration du cadre FPolicy

Planifier l'présentation de la configuration du cadre FPolicy

Avant de configurer le cadre FPolicy, vous devez comprendre ce qu'il signifie. Vous devez comprendre le contenu de la configuration du périmètre. Vous devez également comprendre les règles de priorité de la portée. Ces informations peuvent vous aider à planifier les valeurs que vous souhaitez définir.

Ce qu'il signifie pour créer une étendue FPolicy

La création du périmètre FPolicy consiste à définir les limites de la règle FPolicy. Le serveur virtuel de stockage (SVM) est la limite de base. Lorsque vous créez un cadre pour une politique FPolicy, vous devez définir la politique FPolicy à laquelle elle s'applique, et vous devez désigner la SVM à laquelle vous souhaitez appliquer le périmètre.

Un certain nombre de paramètres limitent davantage la portée au sein de la SVM spécifiée. Vous pouvez restreindre la portée en spécifiant ce qui doit être inclus dans la portée ou en spécifiant ce qui à exclure de la portée. Après avoir appliqué une portée à une stratégie activée, les vérifications d'événements de stratégie sont appliquées à la portée définie par cette commande.

Des notifications sont générées pour les événements d'accès aux fichiers où des correspondances sont trouvées dans les options « inclure ». Les notifications ne sont pas générées pour les événements d'accès aux fichiers où des correspondances sont trouvées dans les options « exclure ».

La configuration du périmètre FPolicy définit les informations de configuration suivantes :

- Nom du SVM
- Nom de la règle
- Les partages à inclure ou à exclure de ce qui est surveillé
- Les règles d'exportation à inclure ou à exclure de ce qui est surveillé
- Les volumes à inclure ou à exclure de ce qui est surveillé
- Les extensions de fichier à inclure ou exclure de ce qui est surveillé
- Vérification de l'extension de fichier sur les objets de répertoire



Il existe des considérations spéciales à prendre en compte pour ce qui est des règles FPolicy de cluster. La politique de FPolicy de cluster est une règle que l'administrateur du cluster crée pour le SVM d'admin. Si l'administrateur du cluster crée également le périmètre de cette politique FPolicy de cluster, l'administrateur du SVM ne peut pas créer de étendue pour cette même politique. Toutefois, si l'administrateur du cluster ne crée pas de périmètre pour la politique de FPolicy de cluster, tout administrateur du SVM peut créer le périmètre de cette politique. Si l'administrateur SVM crée un périmètre pour cette politique FPolicy de cluster, l'administrateur du cluster ne peut pas créer par la suite une étendue de cluster pour cette même policy de cluster. En effet, l'administrateur du cluster ne peut pas remplacer la portée de la même politique de cluster.

Les règles de priorité de la portée

Les règles de priorité suivantes s'appliquent aux configurations du périmètre :

- Lorsqu'un partage est inclus dans le `-shares-to-include` le paramètre et le volume parent du partage sont inclus dans le `-volumes-to-exclude` paramètre, `-volumes-to-exclude` a priorité sur `-shares-to-include`.
- Lorsqu'une export-policy est incluse dans le `-export-policies-to-include` et le volume parent de la export policy est inclus dans le `-volumes-to-exclude` paramètre, `-volumes-to-exclude` a priorité sur `-export-policies-to-include`.
- Un administrateur peut spécifier les deux `-file-extensions-to-include` et `-file-extensions-to-exclude` listes.

Le `-file-extensions-to-exclude` le paramètre est vérifié avant le `-file-extensions-to-include` le paramètre est vérifié.

Contenu de la configuration de l'étendue FPolicy

Pour planifier votre configuration, vous pouvez utiliser la liste suivante des paramètres de configuration du périmètre FPolicy disponibles :



Lors de la configuration des partages, des règles d'exportation, des volumes et des extensions de fichiers à inclure ou à exclure du périmètre, les paramètres d'inclusion et d'exclusion peuvent inclure des métacaractères tels que «`»?`» and «`»*`». L'utilisation d'expressions régulières n'est pas prise en charge.

Type d'information	Option
SVM Spécifie le nom du SVM sur lequel vous souhaitez créer une étendue FPolicy. Chaque configuration FPolicy est définie au sein d'un seul SVM. Le moteur externe, l'événement de politique, l'étendue des règles et la politique associés pour créer une configuration de politique FPolicy doivent tous être associés au même SVM.	<code>-vserver vserver_name</code>

<p><i>Nom de la politique</i></p> <p>Spécifie le nom de la politique FPolicy à laquelle vous souhaitez associer le périmètre. La politique FPolicy doit déjà exister.</p>	<p>-policy-name policy_name</p>
<p><i>Actions à inclure</i></p> <p>Spécifie une liste de partages délimitée par des virgules pour contrôler la politique FPolicy à laquelle le périmètre est appliqué.</p>	<p>-shares-to-include share_name, ...</p>
<p><i>Actions à exclure</i></p> <p>Spécifie une liste de partages délimitée par des virgules, à exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.</p>	<p>-shares-to-exclude share_name, ...</p>
<p><i>Volumes à inclure</i> Spécifie une liste de volumes séparés par des virgules à surveiller pour la politique FPolicy à laquelle le périmètre est appliqué.</p>	<p>-volumes-to-include volume_name, ...</p>
<p><i>Volumes à exclure</i></p> <p>Spécifie une liste de volumes séparés par des virgules à exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.</p>	<p>-volumes-to-exclude volume_name, ...</p>
<p><i>Exporter les stratégies à inclure</i></p> <p>Spécifie une liste des règles d'exportation séparées par des virgules pour surveiller la politique FPolicy à laquelle le périmètre est appliqué.</p>	<p>-export-policies-to -include export_policy_name, ...</p>
<p><i>Exporter des stratégies à exclure</i></p> <p>Spécifie une liste de règles d'exportation séparées par des virgules afin d'exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.</p>	<p>-export-policies-to -exclude export_policy_name, ...</p>
<p><i>Extensions de fichier à inclure</i></p> <p>Spécifie une liste d'extensions de fichiers délimitée par des virgules pour surveiller la politique FPolicy à laquelle le périmètre est appliqué.</p>	<p>-file-extensions-to -include file_extensions, ...</p>
<p><i>Extension de fichier à exclure</i></p> <p>Spécifie une liste d'extensions de fichiers délimitée par des virgules à exclure de la surveillance de la politique FPolicy à laquelle le périmètre est appliqué.</p>	<p>-file-extensions-to -exclude file_extensions, ...</p>

<p><i>La vérification de l'extension de fichier sur le répertoire est-elle activée ?</i></p> <p>Indique si les vérifications d'extension de nom de fichier s'appliquent également aux objets de répertoire. Si ce paramètre est défini sur <code>true</code>, les objets de répertoire sont soumis aux mêmes contrôles d'extension que les fichiers normaux. Si ce paramètre est défini sur <code>false</code>, les noms de répertoire ne correspondent pas pour les postes et les notifications sont envoyées pour les répertoires même si leurs extensions de nom ne correspondent pas.</p> <p>Si la politique FPolicy à laquelle l'étendue est affectée est configurée pour utiliser le moteur natif, ce paramètre doit être défini sur <code>true</code>.</p>	<pre>-is-file-extension -check-on-directories -enabled {true</pre>
<code>false</code>	<code>}</code>

Remplissez la fiche de l'étendue FPolicy

Vous pouvez utiliser cette fiche pour enregistrer les valeurs nécessaires lors du processus de configuration du périmètre FPolicy. Si une valeur de paramètre est requise, vous devez déterminer la valeur à utiliser pour ces paramètres avant de configurer l'étendue FPolicy.

Vous devez indiquer si vous souhaitez inclure chaque paramètre dans la configuration de l'étendue FPolicy, puis noter la valeur des paramètres que vous souhaitez inclure.

Type d'information	Obligatoire	Inclure	Vos valeurs
Nom de la machine virtuelle de stockage (SVM)	Oui.	Oui.	
Nom de la règle	Oui.	Oui.	
Partages à inclure	Non		
Partages à exclure	Non		
Volumes à inclure	Non		
Volumes à exclure	Non		
Export-policy à inclure	Non		
Exporter les règles à exclure	Non		
Extensions de fichier à inclure	Non		
Extension de fichier à exclure	Non		

La vérification de l'extension de fichier sur le répertoire est-elle activée ?	Non		
--	-----	--	--

Créer la configuration FPolicy

Créez le moteur externe FPolicy

Vous devez créer un moteur externe pour commencer à créer une configuration FPolicy. Le moteur externe définit la façon dont FPolicy établit et gère les connexions aux serveurs FPolicy externes. Si votre configuration utilise le moteur ONTAP interne (moteur externe natif) pour le blocage simple des fichiers, vous n'avez pas besoin de configurer un moteur externe FPolicy distinct et n'avez pas besoin de réaliser cette étape.

Ce dont vous avez besoin

Le "[moteur externe](#)" la fiche doit être remplie.

Description de la tâche

Si le moteur externe est utilisé dans une configuration MetroCluster, indiquez les adresses IP des serveurs FPolicy du site source en tant que serveurs primaires. Les adresses IP des serveurs FPolicy du site de destination doivent être spécifiées en tant que serveurs secondaires.

Étapes

1. Créez le moteur externe FPolicy à l'aide de `vserver fpolicy policy external-engine create` commande.

La commande suivante crée un moteur externe sur une machine virtuelle de stockage (SVM) vs1.example.com. Aucune authentification n'est requise pour les communications externes avec le serveur FPolicy.

```
vserver fpolicy policy external-engine create -vserver-name vs1.example.com
-engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
no-auth
```

2. Vérifiez la configuration du moteur externe FPolicy à l'aide du `vserver fpolicy policy external-engine show` commande.

Les informations d'affichage de la commande suivante concernant tous les moteurs externes configurés sur le SVM vs1.example.com :

```
vserver fpolicy policy external-engine show -vserver vs1.example.com
```

		Primary	Secondary	
External Vserver Type	Engine	Servers	Servers	Port Engine
-----	-----	-----	-----	-----
vs1.example.com synchronous	engine1	10.1.1.2, 10.1.1.3	-	6789

La commande suivante affiche des informations détaillées sur le moteur externe nommé « moteur1 » sur le SVM vs1.example.com :

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
-name engine1
```

```

Vserver: vs1.example.com
Engine: engine1
Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
Port Number of FPolicy Service: 6789
Secondary FPolicy Servers: -
External Engine Type: synchronous
SSL Option for External Communication: no-auth
FQDN or Custom Common Name: -
Serial Number of Certificate: -
Certificate Authority: -
```

Créez l'événement FPolicy

Dans le cadre de la configuration de règles FPolicy, vous devez créer un événement FPolicy. Lors de sa création, vous associez l'événement à la politique FPolicy. Un événement définit le protocole à surveiller et les événements d'accès aux fichiers à surveiller et à filtrer.

Avant de commencer

Vous devez terminer l'événement FPolicy ["feuille de calcul"](#).

Créez l'événement FPolicy

1. Créez l'événement FPolicy à l'aide de `vserver fpolicy policy event create` commande.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -file-operations open,close,read,write
```

2. Vérifiez la configuration d'événement FPolicy à l'aide de `vserver fpolicy policy event show`

commande.

```
vserver fpolicy policy event show -vserver vs1.example.com
```

Vserver	Event Name	Protocols	File Operations	Filters	Is Volume Operation
vs1.example.com	event1	cifs	open, close, read, write	-	false

Créez les événements de refus d'accès FPolicy

À partir de ONTAP 9.13.1, les utilisateurs peuvent recevoir des notifications en cas d'échec des opérations sur les fichiers en raison d'un manque d'autorisations. Ces notifications sont précieuses pour la sécurité, la protection contre les ransomware et la gouvernance.

1. Créez l'événement FPolicy à l'aide de `vserver fpolicy policy event create` commande.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

Créez des magasins persistants FPolicy

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. À partir de ONTAP 9.14.1, FPolicy vous permet de configurer votre système "[magasins persistants](#)" Pour capturer les événements d'accès aux fichiers pour les politiques asynchrones non obligatoires dans la SVM. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

À partir de ONTAP 9.15.1, la configuration du stockage persistant FPolicy est simplifiée. Le `persistent-store create` Automatise la création de volume pour le SVM et configure le volume pour le magasin persistant.

Selon la version ONTAP, il existe deux façons de créer un magasin persistant :

- ONTAP 9.15.1 ou version ultérieure : lorsque vous créez le magasin persistant, ONTAP crée et configure automatiquement son volume en même temps. Cela simplifie la configuration du magasin persistant FPolicy et met en œuvre toutes les bonnes pratiques.
- ONTAP 9.14.1 : créez et configurez manuellement un volume, puis créez un magasin persistant pour le volume qui vient d'être créé.

Il n'est possible de configurer qu'un seul magasin persistant sur chaque SVM. Ce magasin persistant unique doit être utilisé pour toutes les configurations FPolicy de cette SVM, même si les règles proviennent de différents partenaires.

Création d'un magasin persistant (ONTAP 9.15.1 ou version ultérieure)

À partir de ONTAP 9.15.1, utilisez le `fpolicy persistent-store create` Commande permettant de créer le stockage persistant FPolicy avec création et configuration de volumes en ligne. ONTAP bloque automatiquement le volume pour l'accès aux protocoles utilisateur externes (CIFS/NFS).

Avant de commencer

- La SVM sur laquelle vous souhaitez créer le magasin persistant doit avoir au moins un agrégat.
- Vous devez avoir accès aux agrégats disponibles pour la SVM et disposer des autorisations suffisantes pour créer des volumes.

Étapes

1. Créez le magasin persistant, qui crée et configure automatiquement le volume :

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store  
<name> -volume <volume_name> -size <size> -autosize-mode  
<off|grow|grow_shrink>
```

- Le `vserver` Paramètre est le nom du SVM.
- Le `persistent-store` paramètre est le nom du magasin persistant.
- Le `volume` paramètre est le nom du volume du magasin persistant.



Si vous souhaitez utiliser un volume existant vide, utilisez le `volume show` pour la rechercher et la spécifier dans le paramètre `volume`.

- Le `size` le paramètre est basé sur la durée pendant laquelle vous souhaitez conserver les événements qui ne sont pas transmis au serveur externe (application partenaire).

Par exemple, si vous souhaitez que 30 minutes d'événements se poursuivent dans un cluster avec une capacité de 30 000 notifications par seconde :

Taille du volume requis = $30000 \times 30 \times 60 \times 0,6$ Ko (taille moyenne des enregistrements de notification)
= 32400000 Ko = ~32 Go

Pour connaître le taux de notification approximatif, vous pouvez accéder à votre application partenaire FPolicy ou utiliser le compteur FPolicy `requests_dispatched_rate`.



Si vous utilisez un volume existant, le paramètre `size` est facultatif. Si vous indiquez une valeur pour le paramètre `size`, le volume sera modifié avec la taille que vous spécifiez.

- Le `autosize-mode` paramètre spécifie le mode de dimensionnement automatique du volume. Les modes de dimensionnement automatique pris en charge sont les suivants :
 - Désactivé : la taille du volume n'augmente pas ou ne diminue pas en fonction de la quantité d'espace utilisé.
 - Grow : le volume augmente automatiquement lorsque l'espace utilisé dans le volume dépasse le seuil Grow.
 - Grow_Grow - la taille du volume augmente ou diminue en fonction de la quantité d'espace utilisé.
2. Créez la règle FPolicy et ajoutez le nom du stockage persistant à cette règle. Pour plus d'informations, voir ["Créez la règle FPolicy"](#).

Création d'un magasin persistant (ONTAP 9.14.1)

Vous pouvez créer un volume, puis créer un magasin persistant pour utiliser ce volume. Vous pouvez ensuite bloquer le nouveau volume créé à partir de l'accès au protocole utilisateur externe (CIFS/NFS).

Étapes

1. Créer sur le SVM un volume vide pouvant être provisionné pour le magasin persistant :

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -policy  
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>  
-snapshot-policy <none>
```

Un utilisateur administrateur disposant de privilèges RBAC suffisants (pour créer un volume) crée un volume (à l'aide de la commande cli du volume ou de l'API REST) de la taille souhaitée et fournit le nom de ce volume en tant que `-volume`. Dans le magasin persistant, créez la commande CLI ou l'API REST.

- Le `vserver` Paramètre est le nom du SVM.
- Le `volume` paramètre est le nom du volume du magasin persistant.
- Le `state` le paramètre doit être défini sur `online` afin que le volume soit disponible.
- Le `policy` Le paramètre est défini sur la stratégie de service FPolicy, si vous en avez déjà un configuré. Si ce n'est pas le cas, vous pouvez utiliser le `volume modify` plus tard, pour ajouter la règle.
- Le `unix-permissions` le paramètre est facultatif.
- Le `size` le paramètre est basé sur la durée pendant laquelle vous souhaitez conserver les événements qui ne sont pas transmis au serveur externe (application partenaire).

Par exemple, si vous souhaitez que 30 minutes d'événements se poursuivent dans un cluster avec une capacité de 30 000 notifications par seconde :

Taille du volume requis = $30000 \times 30 \times 60 \times 0,6$ Ko (taille moyenne des enregistrements de notification)
= 32400000 Ko = ~32 Go

Pour connaître le taux de notification approximatif, vous pouvez accéder à votre application partenaire FPolicy ou utiliser le compteur `FPolicy requests_dispatched_rate`.

- Le paramètre `aggregate` est nécessaire pour les volumes FlexVol, sinon il n'est pas requis.
- Le `snapshot-policy` le paramètre doit être défini sur `none`. 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 empêche le traitement des événements en double.

Si vous souhaitez utiliser un volume existant vide, utilisez le `volume show` pour le trouver et le `volume modify` commande permettant d'apporter les modifications nécessaires. Assurez-vous que la stratégie, la taille et `snapshot-policy` les paramètres sont définis correctement pour le magasin persistant.

2. Créez le magasin persistant :

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store  
<PS_name> -volume <volume>
```

- Le `vserver` Paramètre est le nom du SVM.
 - Le `persistent-store` paramètre est le nom du magasin persistant.
 - Le `volume` paramètre est le nom du volume du magasin persistant.
3. Créez la règle FPolicy et ajoutez le nom du stockage persistant à cette règle. Pour plus d'informations, voir ["Créez la règle FPolicy"](#).

Créez la règle FPolicy

Lorsque vous créez la politique FPolicy, vous associez un moteur externe et un ou plusieurs événements à la règle. La politique spécifie également si un filtrage obligatoire est nécessaire, si les serveurs FPolicy ont un accès privilégié aux données sur la machine virtuelle de stockage (SVM) et si la lecture passe-automatique pour les fichiers hors ligne est activée.

Ce dont vous avez besoin

- La fiche de politique FPolicy doit être remplie.
- Si vous prévoyez de configurer la règle pour utiliser les serveurs FPolicy, le moteur externe doit exister.
- Il faut au moins un événement FPolicy que vous prévoyez d'associer à la règle FPolicy.
- Si vous souhaitez configurer l'accès aux données privilégié, un serveur SMB doit exister sur la SVM.
- Pour configurer un magasin persistant pour une stratégie, le type de moteur doit être **async** et la stratégie doit être **non obligatoire**.

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

Étapes

1. Créez la règle FPolicy :

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name
policy_name -engine engine_name -events event_name, [-persistent-store
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
privileged-user-name domain\user_name] [-is-passthrough-read-enabled
{true|false}]
```

- Vous pouvez ajouter un ou plusieurs événements à la règle FPolicy.
- Par défaut, le tramage obligatoire est activé.
- Si vous souhaitez autoriser l'accès privilégié en définissant l' `-allow-privileged-access` paramètre à `yes`, vous devez également configurer un nom d'utilisateur privilégié pour l'accès privilégié.
- Si vous souhaitez configurer Passthrough-read en définissant le paramètre `-is-passthrough-read-enabled` paramètre à `true`, vous devez également configurer l'accès privilégié aux données.

La commande suivante crée une politique nommée « politique 1 » qui est associée à l'événement « event1 » et au moteur externe « moteur1 ». Cette règle utilise des valeurs par défaut dans la configuration de la stratégie : `vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

La commande suivante crée une politique nommée « politique 2 » qui est associée à l'événement «

event2 » et au moteur externe « moteur2 ». Cette stratégie est configurée pour utiliser l'accès privilégié à l'aide du nom d'utilisateur spécifié. La lecture passe-système est activée :

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
-events event2 -engine engine2 -allow-privileged-access yes -privileged-
user-name example\archive_acct -is-passthrough-read-enabled true
```

La commande suivante crée une politique nommée ""native1"" qui est associée à l'événement ""event3"". Cette règle utilise le moteur natif et les valeurs par défaut dans la configuration de la règle :

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. Vérifiez la configuration de la politique FPolicy à l'aide de `vserver fpolicy policy show` commande.

La commande suivante affiche des informations sur les trois politiques FPolicy configurées, y compris les informations suivantes :

- SVM associé à la politique
- Moteur externe associé à la politique
- Événements associés à la politique
- Indique si un screening obligatoire est requis
- Si un accès privilégié est requis `vserver fpolicy policy show`

Vserver	Policy Name	Events	Engine	Is Mandatory	Privileged Access
-----	-----	-----	-----	-----	
vs1.example.com	policy1	event1	engine1	true	no
vs1.example.com	policy2	event2	engine2	true	yes
vs1.example.com	native1	event3	native	true	no

Créez le périmètre FPolicy

Après avoir créé la règle FPolicy, vous devez créer une étendue FPolicy. Lors de la création du périmètre, vous associez ce dernier à une règle FPolicy. Le périmètre définit les limites applicables à la politique FPolicy. Les portées peuvent inclure ou exclure des fichiers basés sur des partages, des règles d'exportation, des volumes et des extensions de fichier.

Ce dont vous avez besoin

La fiche de l'étendue de FPolicy doit être remplie. La politique FPolicy doit exister avec un moteur externe associé (si cette règle est configurée pour utiliser des serveurs FPolicy externes) et doit avoir au moins un événement FPolicy associé.

Étapes

1. Créez le cadre FPolicy à l'aide de `vserver fpolicy policy scope create` commande.

```
vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name policy1 -volumes-to-include datavol1,datavol2
```

2. Vérifiez la configuration du cadre FPolicy à l'aide du `vserver fpolicy policy scope show` commande.

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
Vserver: vs1.example.com
Policy: policy1
Shares to Include: -
Shares to Exclude: -
Volumes to Include: datavol1, datavol2
Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

Activez la règle FPolicy

Une fois que vous avez configuré une configuration de règles FPolicy, vous activez cette règle. L'activation de la stratégie définit sa priorité et lance la surveillance de l'accès aux fichiers pour la stratégie.

Ce dont vous avez besoin

La politique FPolicy doit exister avec un moteur externe associé (si cette règle est configurée pour utiliser des serveurs FPolicy externes) et doit avoir au moins un événement FPolicy associé. Le cadre de la politique FPolicy doit exister et doit être attribué à la politique FPolicy.

Description de la tâche

La priorité est utilisée lorsque plusieurs règles sont activées sur la machine virtuelle de stockage (SVM) et qu'une seule règle a souscrit au même événement d'accès aux fichiers. Les règles qui utilisent la configuration du moteur natif ont une priorité plus élevée que les règles pour tout autre moteur, quel que soit le numéro de séquence qui leur est attribué lors de l'activation de la stratégie.



Une policy ne peut pas être activée sur le SVM admin

Étapes

1. Activez la politique FPolicy à l'aide de `vserver fpolicy enable` commande.

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1 -sequence-number 1
```

2. Vérifiez que la politique FPolicy est activée à l'aide du `vserver fpolicy show` commande.

```
vserver fpolicy show -vserver vs1.example.com
```

		Sequence		
Vserver	Policy Name	Number	Status	Engine
-----	-----	-----	-----	-----
vs1.example.com	policy1	1	on	engine1

Gérer les configurations FPolicy

Modifier les configurations FPolicy

Commandes permettant de modifier les configurations FPolicy

Vous pouvez modifier les configurations FPolicy en modifiant les éléments de la configuration. Vous pouvez modifier les moteurs externes, les événements FPolicy, les étendues FPolicy, les magasins persistants FPolicy et les règles FPolicy. Vous pouvez également activer ou désactiver les règles FPolicy. Lorsque vous désactivez la règle FPolicy, la surveillance des fichiers est interrompue.

Vous devez désactiver une règle FPolicy avant de modifier sa configuration.

Si vous voulez modifier...	Utilisez cette commande...
Moteurs externes	<code>vserver fpolicy policy external-engine modify</code>
Événements	<code>vserver fpolicy policy event modify</code>
Étendues	<code>vserver fpolicy policy scope modify</code>
Stockage persistant	<code>vserver fpolicy persistent-store modify</code>
Stratégies	<code>vserver fpolicy policy modify</code>

Consultez les pages de manuels pour les commandes pour plus d'informations.

Activez ou désactivez les règles FPolicy

Vous pouvez activer les règles FPolicy une fois la configuration terminée. L'activation de la stratégie définit sa priorité et lance la surveillance de l'accès aux fichiers pour la stratégie. Vous pouvez désactiver les règles FPolicy pour arrêter la surveillance des accès aux fichiers correspondant à cette règle.

Ce dont vous avez besoin

La configuration FPolicy doit être réalisée avant l'activation des règles FPolicy.

Description de la tâche

- La priorité est utilisée lorsque plusieurs règles sont activées sur la machine virtuelle de stockage (SVM) et qu'une seule règle a souscrit au même événement d'accès aux fichiers.
- Les règles qui utilisent la configuration du moteur natif ont une priorité plus élevée que les règles pour tout autre moteur, quel que soit le numéro de séquence qui leur est attribué lors de l'activation de la stratégie.
- Pour modifier la priorité d'une règle FPolicy, vous devez la désactiver puis la réactiver à l'aide du nouveau numéro de séquence.

Étape

1. Effectuez l'action appropriée :

Les fonctions que vous recherchez...	Saisissez la commande suivante...
Activez une règle FPolicy	<code>vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer</code>
Désactiver une règle FPolicy	<code>vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name</code>

Affiche des informations sur les configurations FPolicy

Fonctionnement des commandes show

Il est utile lors de l'affichage d'informations sur la configuration FPolicy pour comprendre la `show` les commandes fonctionnent.

A `show` la commande sans paramètre supplémentaire affiche les informations sous forme récapitulative. De plus, chaque `show` la commande dispose des deux mêmes paramètres facultatifs mutuellement exclusifs. `-instance` et `-fields`.

Lorsque vous utilisez le `-instance` paramètre avec un `show` commande, la sortie de la commande affiche des informations détaillées au format de liste. Dans certains cas, le résultat détaillé peut être long et inclure plus d'informations que vous n'en avez besoin. Vous pouvez utiliser le `-fields fieldname[,fieldname...]` paramètre permettant de personnaliser la sortie afin qu'elle affiche les informations uniquement pour les champs que vous spécifiez. Vous pouvez définir les champs que vous pouvez spécifier en saisissant ? après le `-fields` paramètre.



La sortie d'un `show` commande avec `-fields` paramètre peut afficher d'autres champs pertinents et nécessaires associés aux champs demandés.

Toutes les `show` la commande comporte un ou plusieurs paramètres facultatifs qui filtrent la sortie et vous permettent de réduire la portée des informations affichées dans la sortie de la commande. Vous pouvez définir l'identité des paramètres facultatifs disponibles pour une commande en saisissant ? après le `show` commande.

Le `show` La commande prend en charge les motifs de style UNIX et les caractères génériques pour vous permettre de faire correspondre plusieurs valeurs dans les arguments de paramètres-commande. Par exemple, vous pouvez utiliser l'opérateur générique (*), L'opérateur NOT (!), l'opérateur OR (|), l'opérateur Range (integer...integer), l'opérateur moins-que (<), l'opérateur plus grand-que (>), l'opérateur MOINS-égal ou égal à (<=) et l'opérateur supérieur ou égal à (>=) lors de la spécification de valeurs.

Pour plus d'informations sur l'utilisation de modèles de style UNIX et de caractères génériques, reportez-vous au [Utilisation de l'interface de ligne de commandes ONTAP](#).

Commandes permettant d'afficher des informations sur les configurations FPolicy

Vous utilisez le `fpolicy show` Commandes permettant d'afficher des informations sur la configuration FPolicy, y compris les informations sur les moteurs, événements, étendues et règles FPolicy externes.

Pour afficher des informations sur FPolicy...	Utilisez cette commande...
Moteurs externes	<code>vserver fpolicy policy external-engine show</code>
Événements	<code>vserver fpolicy policy event show</code>
Étendues	<code>vserver fpolicy policy scope show</code>
Stratégies	<code>vserver fpolicy policy show</code>

Consultez les pages de manuels pour les commandes pour plus d'informations.

Affiche des informations sur l'état des règles FPolicy

Vous pouvez afficher des informations sur le statut des règles FPolicy pour déterminer si une règle est activée, le moteur externe qu'elle est configuré à utiliser, le numéro de séquence correspondant à la règle et à quel serveur virtuel de stockage (SVM) la politique FPolicy est associée.

Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom de la règle
- Numéro de séquence de police
- Statut de la stratégie

Outre l'affichage des informations sur l'état des règles de FPolicy configurées sur le cluster ou un SVM spécifique, vous pouvez utiliser les paramètres de la commande pour filtrer les résultats de la commande par d'autres critères.

Vous pouvez spécifier le `-instance` paramètre pour afficher des informations détaillées sur les règles répertoriées. Vous pouvez également utiliser le `-fields` paramètre pour afficher uniquement les champs indiqués dans la sortie de la commande, ou `-fields ?` pour déterminer les champs que vous pouvez utiliser.

Étape

1. Afficher des informations filtrées sur l'état des règles FPolicy à l'aide de la commande appropriée :

Pour afficher des informations d'état sur les stratégies...	Entrez la commande...
Sur le cluster	<code>vserver fpolicy show</code>
Dont le statut est spécifié	<code>`vserver fpolicy show -status {on</code>
<code>off}`</code>	Sur un SVM spécifié
<code>vserver fpolicy show -vserver vserver_name</code>	Avec le nom de la règle spécifiée
<code>vserver fpolicy show -policy-name policy_name</code>	Qui utilisent le moteur externe spécifié

Exemple

Les exemples suivants affichent les informations sur les règles FPolicy sur le cluster :

```
cluster1::> vserver fpolicy show
```

Vserver	Policy Name	Sequence Number	Status	Engine
FPolicy	cserver_policy	-	off	eng1
vs1.example.com	v1p1	-	off	eng2
vs1.example.com	v1p2	-	off	native
vs1.example.com	v1p3	-	off	native
vs1.example.com	cserver_policy	-	off	eng1
vs2.example.com	v1p1	3	on	native
vs2.example.com	v1p2	1	on	eng3
vs2.example.com	cserver_policy	2	on	eng1

Affiche des informations sur les règles FPolicy activées

Vous pouvez afficher des informations sur les règles FPolicy activées pour déterminer le moteur externe FPolicy à utiliser, la priorité de la règle et le SVM associé à la règle FPolicy.

Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom de la règle
- Priorité de la stratégie

Vous pouvez utiliser les paramètres de la commande pour filtrer la sortie de la commande par critères

spécifiés.

Étape

1. Afficher des informations sur les règles FPolicy activées à l'aide de la commande appropriée :

Si vous souhaitez afficher des informations sur les stratégies activées...	Entrez la commande...
Sur le cluster	<code>vserver fpolicy show-enabled</code>
Sur un SVM spécifié	<code>vserver fpolicy show-enabled -vserver vserver_name</code>
Avec le nom de la règle spécifiée	<code>vserver fpolicy show-enabled -policy-name policy_name</code>
Avec le numéro de séquence spécifié	<code>vserver fpolicy show-enabled -priority integer</code>

Exemple

Les exemples suivants affichent les informations sur les règles FPolicy activées sur le cluster :

```
cluster1::> vserver fpolicy show-enabled
Vserver                Policy Name                Priority
-----
vs1.example.com        pol_native                 native
vs1.example.com        pol_native2                native
vs1.example.com        pol1                       2
vs1.example.com        pol2                       4
```

Gérez les connexions du serveur FPolicy

Connectez-vous à des serveurs FPolicy externes

Pour activer le traitement de fichiers, vous devrez peut-être vous connecter manuellement à un serveur FPolicy externe si la connexion a déjà été interrompue. Une connexion est interrompue une fois le délai d'expiration du serveur atteint ou en raison d'une erreur. L'administrateur peut également mettre fin manuellement à une connexion.

Description de la tâche

En cas d'erreur fatale, la connexion au serveur FPolicy peut être interrompue. Après avoir résolu le problème à l'origine de l'erreur fatale, vous devez vous reconnecter manuellement au serveur FPolicy.

Étapes

1. Connectez-vous au serveur FPolicy externe à l'aide de `vserver fpolicy engine-connect`

commande.

Pour plus d'informations sur la commande, consultez les pages de manuels.

2. Vérifiez que le serveur FPolicy externe est connecté à l'aide du `vserver fpolicy show-engine` commande.

Pour plus d'informations sur la commande, consultez les pages de manuels.

Effectue la déconnexion des serveurs FPolicy externes

Vous devrez peut-être vous déconnecter manuellement d'un serveur FPolicy externe. Cette opération peut être utile si le serveur FPolicy présente des problèmes avec le traitement des demandes de notification ou si vous devez effectuer une maintenance sur le serveur FPolicy.

Étapes

1. Déconnectez-vous du serveur FPolicy externe à l'aide de `vserver fpolicy engine-disconnect` commande.

Pour plus d'informations sur la commande, consultez les pages de manuels.

2. Vérifiez que le serveur FPolicy externe est déconnecté à l'aide de `vserver fpolicy show-engine` commande.

Pour plus d'informations sur la commande, consultez les pages de manuels.

Affiche des informations sur les connexions aux serveurs FPolicy externes

Vous pouvez afficher les informations d'état des connexions aux serveurs FPolicy externes pour le cluster ou pour une machine virtuelle de stockage (SVM) spécifiée. Ces informations peuvent vous aider à déterminer quels serveurs FPolicy sont connectés.

Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom du nœud
- Nom de la règle FPolicy
- Adresse IP du serveur FPolicy
- État du serveur FPolicy
- Type de serveur FPolicy

En plus d'afficher les informations relatives aux connexions FPolicy sur le cluster ou un SVM spécifique, vous pouvez utiliser les paramètres de la commande pour filtrer les résultats de la commande par d'autres critères.

Vous pouvez spécifier le `-instance` paramètre pour afficher des informations détaillées sur les règles répertoriées. Vous pouvez également utiliser le `-fields` paramètre pour afficher uniquement les champs indiqués dans la sortie de la commande. Vous pouvez entrer ? après le `-fields` paramètre pour déterminer

les champs que vous pouvez utiliser.

Étape

1. Afficher des informations filtrées sur l'état de connexion entre le nœud et le serveur FPolicy à l'aide de la commande appropriée :

Pour afficher les informations sur l'état des connexions à propos des serveurs FPolicy...	Entrer...
Que vous spécifiez	<code>vserver fpolicy show-engine -server IP_address</code>
Pour un SVM spécifié	<code>vserver fpolicy show-engine -vserver vserver_name</code>
Associés à une politique spécifiée	<code>vserver fpolicy show-engine -policy-name policy_name</code>
Avec l'état du serveur que vous spécifiez	<code>vserver fpolicy show-engine -server-status status</code> La liste ci-dessous répertorie les différents États du serveur : <ul style="list-style-type: none">• connected• disconnected• connecting• disconnecting
Avec le type spécifié	<code>vserver fpolicy show-engine -server-type type</code> Le type de serveur FPolicy peut être l'un des suivants : <ul style="list-style-type: none">• primary• secondary

Qui ont été déconnectés avec la raison spécifiée	<pre>vserver fpolicy show-engine -disconnect-reason text</pre> <p>La déconnexion peut être due à plusieurs raisons. Les raisons courantes de la déconnexion sont les suivantes :</p> <ul style="list-style-type: none"> • Disconnect command received from CLI. • Error encountered while parsing notification response from FPolicy server. • FPolicy Handshake failed. • SSL handshake failed. • TCP Connection to FPolicy server failed. • The screen response message received from the FPolicy server is not valid.
--	--

Exemple

Cet exemple affiche des informations sur les connexions des moteurs externes aux serveurs FPolicy du SVM vs1.example.com :

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy
Vserver          Policy      Node          Server          Server-      Server-
-----          -
vs1.example.com policy1    node1         10.1.1.2        connected    primary
vs1.example.com policy1    node1         10.1.1.3        disconnected   primary
vs1.example.com policy1    node2         10.1.1.2        connected    primary
vs1.example.com policy1    node2         10.1.1.3        disconnected   primary
```

Cet exemple affiche des informations uniquement sur les serveurs FPolicy connectés :

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node          vserver          policy-name    server
-----
node1         vs1.example.com  policy1        10.1.1.2
node2         vs1.example.com  policy1        10.1.1.2
```

Affiche des informations sur l'état de la connexion de passerelle FPolicy

Vous pouvez afficher des informations sur l'état de la connexion de passage en lecture FPolicy à des serveurs FPolicy externes pour le cluster ou à un SVM spécifié. Ces

informations peuvent vous aider à identifier les serveurs FPolicy dotés de connexions de données de type « passthrough read » et pour lesquels les serveurs FPolicy sont déconnectés.

Description de la tâche

Si vous ne spécifiez aucun paramètre, la commande affiche les informations suivantes :

- Nom du SVM
- Nom de la règle FPolicy
- Nom du nœud
- Adresse IP du serveur FPolicy
- État de la connexion de lecture intermédiaire FPolicy

En plus d’afficher les informations relatives aux connexions FPolicy sur le cluster ou un SVM spécifique, vous pouvez utiliser les paramètres de la commande pour filtrer les résultats de la commande par d’autres critères.

Vous pouvez spécifier le `-instance` paramètre pour afficher des informations détaillées sur les règles répertoriées. Vous pouvez également utiliser le `-fields` paramètre pour afficher uniquement les champs indiqués dans la sortie de la commande. Vous pouvez entrer ? après le `-fields` paramètre pour déterminer les champs que vous pouvez utiliser.

Étape

1. Afficher des informations filtrées sur l’état de connexion entre le nœud et le serveur FPolicy à l’aide de la commande appropriée :

Pour afficher les informations sur l’état de la connexion...	Entrez la commande...
État de la connexion de lecture « pashrough FPolicy » pour le cluster	<code>vserver fpolicy show-passthrough-read-connection</code>
État de connexion de passerelle FPolicy pour un SVM spécifié	<code>vserver fpolicy show-passthrough-read-connection -vserver vserver_name</code>
État de la connexion de lecture intermédiaire FPolicy pour une règle spécifiée	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name</code>
État détaillé de la connexion de lecture intermédiaire FPolicy pour une règle spécifiée	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance</code>
État de la connexion de lecture intermédiaire FPolicy pour l’état que vous spécifiez	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status</code> La liste ci-dessous répertorie les différents États du serveur : <ul style="list-style-type: none">• <code>connected</code>• <code>disconnected</code>

Exemple

La commande suivante affiche des informations relatives aux connexions de lecture passerelle de tous les serveurs FPolicy du cluster :

```
cluster1::> vserver fpolicy show-passthrough-read-connection
```

Vserver	Policy Name	Node	FPolicy Server	Server Status
vs2.example.com	pol_cifs_2	FPolicy-01	2.2.2.2	disconnected
vs1.example.com	pol_cifs_1	FPolicy-01	1.1.1.1	connected

La commande suivante affiche des informations détaillées sur les connexions en lecture pasde serveurs FPolicy configurées dans la politique « Pol_cifs_1 » :

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name pol_cifs_1 -instance
```

```
Node: FPolicy-01
Vserver: vs1.example.com
Policy: pol_cifs_1
Server: 1.1.1.1
Session ID of the Control Channel: 8cef052e-2502-11e3-88d4-123478563412
Server Status: connected
Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

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.