Planification de la configuration FPolicy

ONTAP 9

NetApp
February 13, 2026

Sommaire

Planification de la configuration FPolicy

Exigences, considérations et meilleures pratiques pour la configuration d'ONTAP 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 de stockage persistant se déplace d'un nœud à un autre dans la même SVM, les notifications qui doivent encore être traitées se déplacent également vers le nouveau nœud. Vous devez réexécuter le `fpolicy persistent-store create` commande sur l'un ou l'autre nœud après le déplacement du volume pour garantir que les notifications en attente sont transmises au serveur externe.

En savoir plus sur `fpolicy persistent-store create` dans le "Référence de commande ONTAP" .

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 :
   a. `statistics start -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics start -object fpolicy_policy -instance <instance_name> -sample-id <ID>`
2. Afficher les compteurs FPolicy :
   a. `statistics show -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `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
Latence maximale des demandes d'écran	demandes_en_attente
Nombre total de demandes d'écran en cours de traitement	requêtes_traitées

Compteurs	Description
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	**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

Pour en savoir plus sur `statistics start` et `statistics show` dans le "Référence de commande ONTAP".

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.

Informations associées

- "les statistiques montrent"
- "les statistiques commencent"

Configurer les configurations ONTAP 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

Planifier les configurations du moteur externe ONTAP 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
SVM Spécifie le nom du SVM que vous souhaitez associer à ce moteur externe. 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.	`-vserver vserver_name`
Nom du moteur 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. Le nom peut comporter jusqu'à 256 caractères. 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. Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants : • `a` à `z` • `A` à `Z` • `0` à `9` • «»_», «»-", `and` ".»	`-engine-name engine_name`

Serveurs FPolicy primaires 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. 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. 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.	`-primary-servers IP_address,...`
Numéro de port Spécifie le numéro de port du service FPolicy.	`-port integer`
Serveurs FPolicy secondaires 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. 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.	`-secondary-servers IP_address,...`
Type de moteur externe Indique si le moteur externe fonctionne en mode synchrone ou asynchrone. Par défaut, FPolicy fonctionne en mode synchrone. Lorsqu'il est réglé sur `synchronous`, 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. Lorsqu'il est réglé sur `asynchronous`, Le traitement des requêtes de fichier envoie une notification au serveur FPolicy, puis continue.	`-extern-engine-type external_engine_type` La valeur de ce paramètre peut être l'une des suivantes : • `synchronous` • `asynchronous`

Format de moteur externe Spécifiez si le format du moteur externe est xml ou protobuf. 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.	`- extern-engine-format` {`protobuf` ou `xml`}
Option *SSL pour la communication avec le serveur FPolicy* 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 : • Lorsqu'il est réglé sur `no-auth`, aucune authentification n'a lieu. La liaison de communication est établie sur TCP. • Lorsqu'il est réglé sur `server-auth`, Le SVM authentifie le serveur FPolicy à l'aide de l'authentification du serveur SSL. • Lorsqu'il est réglé sur `mutual-auth`, 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. Si vous choisissez de configurer l'authentification SSL mutuelle, vous devez également configurer l' `-certificate-common-name`, `-certificate-serial`, et `-certifcate-ca` paramètres.	`-ssl-option` {`no-auth`
`server-auth`	`mutual-auth`}
FQDN du certificat ou nom commun personnalisé 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. Si vous spécifiez `mutual-auth` pour le `-ssl-option` paramètre, vous devez spécifier une valeur pour le `-certificate-common-name` paramètre.	`-certificate-common -name` `text`
Numéro de série du certificat Spécifie le numéro de série du certificat utilisé pour l'authentification si l'authentification SSL entre le SVM et le serveur FPolicy est configurée. Si vous spécifiez `mutual-auth` pour le `-ssl-option` paramètre, vous devez spécifier une valeur pour le `-certificate-serial` paramètre.	`-certificate-serial` `text`

Autorité de certification 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. Si vous spécifiez `mutual-auth` pour le `-ssl-option` paramètre, vous devez spécifier une valeur pour le `-certificate-ca` paramètre.	`-certificate-ca text`

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
Délai d'annulation d'une demande Spécifie l'intervalle de temps en heures (`h`), minutes (`m`), ou secondes (`s`) Que le nœud attend une réponse du serveur FPolicy. 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. 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`.	`-reqs-cancel-timeout integer`[h
m	s]
Délai d'attente pour l'abandon d'une demande Spécifie le délai d'expiration en heures (`h`), minutes (`m`), ou secondes (`s`) pour l'abandon d'une demande. La plage de cette valeur est de `0` à `200`.	`-reqs-abort-timeout ` `integer`[h
m	s]

Intervalle pour l'envoi de demandes d'état Spécifie l'intervalle en heures (`h`), minutes (`m`), ou secondes (`s`) Après quoi une requête d'état est envoyée au serveur FPolicy. 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`.	`-status-req-interval integer`[h
m	s]
Nombre maximal de requêtes en attente sur le serveur FPolicy Spécifie le nombre maximal de requêtes en attente pouvant être mises en file d'attente sur le serveur FPolicy. La plage de cette valeur est de `1` à `10000`. La valeur par défaut est `500`.	`-max-server-reqs integer`
Timeout pour la déconnexion d'un serveur FPolicy non réactif Spécifie l'intervalle de temps en heures (`h`), minutes (`m`), ou secondes (`s`) Après quoi la connexion au serveur FPolicy est interrompue. 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 `max-server-reqs-` paramètre. La plage de cette valeur est de `1` à `100`. La valeur par défaut est `60s`.	`-server-progress -timeout integer`[h
m	s]
Intervalle d'envoi de messages de maintien de la disponibilité au serveur FPolicy 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. Les messages de maintien de la vie détectent les connexions à demi-ouverture. 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`.	`-keep-alive-interval-integer`[h
m	s]

Tentatives de reconnexion maximales Spécifie le nombre maximal de fois que le SVM tente de se reconnecter au serveur FPolicy une fois la connexion interrompue. La plage de cette valeur est de `0` à `20`. La valeur par défaut est `5`.	`-max-connection-retries integer`
Taille du tampon de réception Spécifie la taille du tampon de réception du socket connecté pour le serveur FPolicy. 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. 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.	`-recv-buffer-size integer`
Envoyer la taille du tampon Spécifie la taille du tampon d'envoi du socket connecté pour le serveur FPolicy. 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. 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.	`-send-buffer-size integer`
Délai de purge d'un ID de session pendant la reconnexion 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. Si la connexion entre le contrôleur de stockage et le serveur FPolicy est interrompue et la reconnexion est effectuée au sein du `-session -timeout` Intervalle, l'ancien ID de session est envoyé au serveur FPolicy pour qu'il puisse envoyer les réponses aux anciennes notifications. La valeur par défaut est définie sur 10 secondes.	`-session-timeout [integerh][integerm][integers]`

Informations supplémentaires sur la configuration des moteurs externes ONTAP FPolicy pour utiliser des 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. Ne supprimez pas ce certificat tant que les 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`.

Informations associées

- "installation du certificat de sécurité"

Les certificats ONTAP FPolicy ne se répliquent pas dans les relations de reprise après sinistre SVM avec une configuration sans préservation d'ID

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 `snapmirror 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).

Informations associées

- "création snapmirror"

Restrictions pour les moteurs externes ONTAP FPolicy à l'échelle du cluster avec les configurations de reprise après sinistre 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.

Fiches de configuration complètes du moteur externe ONTAP 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

Découvrez la configuration des événements ONTAP 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
SVM Spécifie le nom du SVM que vous souhaitez associer à cet événement 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.	`-vserver vserver_name`
Nom de l'événement 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. Le nom peut comporter jusqu'à 256 caractères. Le nom doit comporter jusqu'à 200 caractères si vous configurez l'évènement dans une configuration de reprise d'activité de MetroCluster ou de SVM. Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants : • `a à z` • `A à Z` • `0 à 9` • « `_` », `""-", and "`.»	`-event-name event_name`

Protocole Spécifie le protocole à configurer pour l'événement FPolicy. La liste pour `-protocol` peut inclure l'une des valeurs suivantes : • `cifs` • `nfsv3` • `nfsv4` Si vous spécifiez `-protocol`, vous devez alors spécifier une valeur valide dans l' `-file-operations` paramètre. Au fur et à mesure que la version du protocole change, les valeurs valides peuvent changer. À partir de ONTAP 9.15.1, nfsv4 vous permet de capturer les événements NFSv4.0 et NFSv4.1.	`-protocol protocol`

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 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	`-filters filter, ...`

Est une opération de volume requise Spécifie si une surveillance est requise pour les opérations de montage et de démontage de volumes. La valeur par défaut est `false`.	`-volume-operation {true`

`false}`
 	
`-filters filter, ...`
	Notifications 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. Des notifications seront générées pour l'opération de fichier ayant échoué en raison d'un manque d'autorisation, notamment :
	
	• Défaillances dues aux autorisations NTFS.
	• Échecs dus aux bits de mode Unix.
	• Défaillances dues à des ACL NFSv4.

`-monitor-fileop-failure {true`	`false}`

- `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.

Combinaisons d'opérations de fichiers et de filtres prises en charge par ONTAP FPolicy Monitors pour SMB

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

Combinaisons d'opérations de fichiers et de filtres prises en charge par ONTAP 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

Combinaisons d’opérations de fichiers et de filtres prises en charge par ONTAP FPolicy 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

Feuilles de calcul complètes de configuration des événements ONTAP 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

En savoir plus sur les configurations de stratégie ONTAP 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
Nom du SVM Spécifie le nom du SVM sur lequel vous souhaitez créer une politique FPolicy.	`-vserver vserver_name`	Oui.	Aucune
Nom de la politique Spécifie le nom de la politique FPolicy. Le nom peut comporter jusqu'à 256 caractères. ⓘ 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. Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants : • `a à z` • `A à Z` • `0 à 9` • «»_», «»-", and ".»	`-policy-name policy_name`	Oui.	Aucune

Noms d'événements Spécifie une liste d'événements séparés par des virgules à associer à la politique FPolicy. • 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.	`-events event_name, ...`	Oui.	Aucune
Magasin permanent 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.	`-persistent -store persistent_store_name`	Non	Aucune

Nom du moteur externe Spécifie le nom du moteur externe à associer à la politique FPolicy. • 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 `native` comme valeur. • Si vous souhaitez utiliser des serveurs FPolicy, la configuration du moteur externe doit déjà exister.	`-engine engine_name`	Oui (à moins que la politique n'utilise le moteur natif ONTAP interne)	`native`
Est un screening obligatoire Indique si un filtrage d'accès aux fichiers obligatoire est requis. • 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 `true`, les événements d'accès aux fichiers sont refusés. • Lorsqu'il est réglé sur `false`, les événements d'accès aux fichiers sont autorisés.	`-is-mandatory {true`	`false}`	Non

`true`	*Autoriser l'accès privilégié* 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. 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. 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 `cifs` comme l'un des protocoles autorisés. 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.	`-allow -privileged -access {yes`	`no}`

Non (sauf si la lecture passthrough est activée)	`no`	*Nom d'utilisateur privilégié* Spécifie le nom d'utilisateur du compte que les serveurs FPolicy utilisent pour l'accès aux données privilégié. • 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.	`-privileged -user-name user_name`

Non (sauf si l’accès privilégié est activé)	Aucune	*Autoriser la lecture_passthrough* 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 : • Passthrough-read est un moyen de lire les données pour les fichiers hors ligne sans restaurer les données dans le stockage primaire. 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.	`-is-passthrough -read-enabled {true`

Exigence relative aux configurations de portée ONTAP 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 parameter 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.

- Lorsqu'ils sont activés, les serveurs FPolicy traitent les données du fichier sur un canal de données privilégié distinct ouvert spécifiquement pour les lectures-passants
- Si vous souhaitez configurer passthrough-read, la stratégie doit également être configurée pour autoriser l'accès privilégié.

Feuilles de travail complètes sur la politique ONTAP 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

En savoir plus sur les configurations de portée ONTAP 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.	`-vserver vserver_name`

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

La vérification de l'extension de fichier sur le répertoire est-elle activée ? Indique si les vérifications d'extension de nom de fichier s'appliquent également aux objets de répertoire. Si ce paramètre est défini sur `true`, les objets de répertoire sont soumis aux mêmes contrôles d'extension que les fichiers normaux. Si ce paramètre est défini sur `false`, 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. Si la politique FPolicy à laquelle l'étendue est affectée est configurée pour utiliser le moteur natif, ce paramètre doit être défini sur `true`.	`-is-file-extension -check-on-directories -enabled {true`
`false`	}

Feuilles de travail complètes sur la portée de la politique ONTAP

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		

Informations sur le copyright

Informations sur les marques commerciales