



# **Planification de la configuration des événements FPolicy**

## **ONTAP 9**

NetApp  
September 12, 2024

# Sommaire

- Planification de la configuration des événements FPolicy ..... 1
  - Planifier l’présentation de la configuration des événements FPolicy ..... 1
  - Opérations de fichiers et combinaisons de filtres prises en charge que FPolicy peut surveiller pour SMB. . . 5
  - Opérations de fichiers et combinaisons de filtres prises en charge pouvant être moniteurs par FPolicy pour NFSv3 ..... 6
  - Opérations de fichiers et combinaisons de filtres prises en charge que FPolicy peut surveiller pour NFSv4 ..... 8
  - Remplissez la fiche de configuration des événements FPolicy ..... 10

# 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><b>SVM</b></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><b>Nom de l'événement</b></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>  <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> </div> <p>Le nom peut contenir n'importe quelle combinaison des caractères ASCII suivants :</p> <ul style="list-style-type: none"> <li>• a à z</li> <li>• A à Z</li> <li>• 0 à 9</li> <li>• « _ ", "' -, and ". »</li> </ul>	<p><code>-event-name event_name</code></p>
<p><b>Protocole</b></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"> <li>• cifs</li> <li>• nfsv3</li> <li>• nfsv4</li> </ul> <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> <div>  <p>À partir de ONTAP 9.15.1, nfsv4 vous permet de capturer les événements NFSv4.0 et NFSv4.1.</p> </div>	<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.

<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>	<p><code>-volume-operation {true</code></p>
<p><code>false}</code></p> <p><code>-filters filter, ...</code></p>	<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"> <li>• Défaillances dues aux autorisations NTFS.</li> <li>• Échecs dus aux bits de mode Unix.</li> <li>• Défaillances dues à des ACL NFSv4.</li> </ul>
<p><code>-monitor-fileop-failure {true</code></p>	<p><code>false}</code></p>

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

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		

## 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.