Planifiez la configuration de la règle FPolicy

ONTAP 9

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/nas-audit/plan-fpolicy-policy-config-concept.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Planifiez la configuration de la règle FPolicy . . . 1
En savoir plus sur les configurations de stratégie ONTAP FPolicy . . . 1
Contenu de la configuration des règles FPolicy . . . 1
Exigence relative aux configurations de portée ONTAP FPolicy si la politique FPolicy utilise le moteur natif . . . 8
Feuilles de travail complètes sur la politique ONTAP FPolicy . . . 8

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.

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

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 ?		

Informations sur le copyright

Copyright © 2026 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 DÉLICTUELLE (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.