Fonctionnement de FPolicy avec des serveurs FPolicy externes

ONTAP 9

NetApp
April 01, 2023

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/nas-audit/fpolicy-external-fpolicy-servers-concept.html on April 01, 2023. Always check docs.netapp.com for the latest.

Table des matières

Fonctionnement de FPolicy avec des serveurs FPolicy externes

Fonctionnement de FPolicy avec les serveurs FPolicy externes

Une fois FPolicy configuré et activé sur le SVM, FPolicy s'exécute sur chaque nœud auquel le SVM participe. FPolicy est chargé de l'établissement et de la maintenance des connexions avec des serveurs FPolicy externes (serveurs FPolicy), pour le traitement des notifications, ainsi que pour la gestion des messages de notification vers et depuis des serveurs FPolicy.

Dans le cadre de la gestion des connexions, FPolicy possède également les responsabilités suivantes :

- Garantit que la notification des fichiers circule via le LIF correct vers le serveur FPolicy.
- Garantit que lorsque plusieurs serveurs FPolicy sont associés à une règle, l'équilibrage de la charge est réalisé lors de l'envoi de notifications aux serveurs FPolicy.
- Tentatives de rétablissement de la connexion en cas de panne de la connexion à un serveur FPolicy.
- Envoie les notifications aux serveurs FPolicy par le biais d'une session authentifiée.
- Gère la connexion de données de type passthrough établie par le serveur FPolicy pour le traitement des requêtes client lorsque la lecture-passe est activée.

Mode d'utilisation des canaux de contrôle pour les communications FPolicy

FPolicy initie une connexion du canal de contrôle à un serveur FPolicy externe à partir des LIFs de données de chaque nœud participant sur un SVM (Storage Virtual machine). FPolicy utilise des canaux de contrôle pour la transmission des notifications de fichiers. Par conséquent, un serveur FPolicy peut voir plusieurs connexions de canaux de contrôle basées sur la topologie SVM.

Utilisation des canaux privilégiés d'accès aux données pour la communication synchrone

Dans le cas d'une utilisation synchrone, le serveur FPolicy accède aux données résidant sur la machine virtuelle de stockage (SVM) via un chemin d'accès privilégié aux données. L'accès via le chemin privilégié expose l'ensemble du système de fichiers au serveur FPolicy. Elle peut accéder aux fichiers de données afin de collecter des informations, de scanner des fichiers, de lire des fichiers ou d'écrire dans des fichiers.

Étant donné que le serveur FPolicy externe peut accéder à l'intégralité du système de fichiers à partir de la racine de la SVM via le canal de données privilégié, la connexion de canal de données privilégié doit être sécurisée.

Comment les identifiants de connexion FPolicy sont utilisés avec les canaux d'accès aux données privilégiés

Le serveur FPolicy établit des connexions privilégiées aux données avec les nœuds du cluster grâce à des informations d'identification Windows spécifiques enregistrées avec la configuration FPolicy. SMB est le seul protocole pris en charge pour établir une connexion de canal avec accès aux données privilégié.

Si le serveur FPolicy nécessite un accès privilégié aux données, les conditions suivantes doivent être remplies :

- Une licence SMB doit être activée sur le cluster.
- Le serveur FPolicy doit fonctionner avec les identifiants configurés dans la configuration FPolicy.

Lors de la connexion à un canal de données, FPolicy utilise les informations d'identification du nom d'utilisateur Windows spécifié. Les données sont accessibles via le partage ONTAP_ADMIN$ par l'administrateur.

L'attribution d'informations d'identification de super utilisateur pour l'accès privilégié aux données signifie

ONTAP utilise la combinaison de l'adresse IP et des identifiants de l'utilisateur configurés dans la configuration FPolicy pour attribuer les identifiants des super utilisateurs au serveur FPolicy.

Lorsque le serveur FPolicy accède aux données, l'état du super utilisateur accorde les privilèges suivants :

- Évitez les contrôles d'autorisation

  L'utilisateur évite les vérifications de l'accès aux fichiers et aux répertoires.

- Privilèges de verrouillage spéciaux

  ONTAP permet l'accès en lecture, en écriture ou en modification à n'importe quel fichier, indépendamment des verrous existants. Si le serveur FPolicy possède des verrous de plage d'octets sur le fichier, il entraîne la suppression immédiate des verrouillages existants sur ce dernier.

- Évitez les vérifications FPolicy

  L'accès ne génère aucune notification FPolicy.

Gestion du traitement des règles par FPolicy

Il peut y avoir plusieurs règles FPolicy attribuées à votre SVM (Storage Virtual machine) ; chacune avec une priorité différente. Pour créer une configuration FPolicy appropriée sur le SVM, il est important de comprendre la façon dont FPolicy gère le traitement des règles.

Chaque requête d'accès aux fichiers est initialement évaluée afin de déterminer les règles qui surveillent cet

événement. S'il s'agit d'un événement surveillé, les informations relatives à l'événement surveillé et les politiques intéressées sont transmises à FPolicy où il est évalué. Chaque stratégie est évaluée par ordre de priorité attribuée.

Lors de la configuration des règles, vous devez tenir compte des recommandations suivantes :

- Lorsque vous voulez qu'une règle soit toujours évaluée avant d'autres règles, configurez-la avec une priorité plus élevée.
- Si le succès de l'opération d'accès aux fichiers demandée sur un événement contrôlé est une condition préalable à une demande de fichier évaluée par rapport à une autre stratégie, donnez à la stratégie qui contrôle le succès ou l'échec de l'opération de premier fichier une priorité plus élevée.

  Par exemple, si l'une des règles gère la fonctionnalité d'archivage et de restauration des fichiers FPolicy, et une seconde gère les opérations d'accès aux fichiers sur le fichier en ligne, la règle de gestion de la restauration des fichiers doit avoir une priorité plus élevée afin que le fichier soit restauré avant que l'opération gérée par la seconde stratégie puisse être autorisée.

- Si vous souhaitez évaluer toutes les règles pouvant s'appliquer à une opération d'accès aux fichiers, donnez une priorité inférieure aux règles synchrones.

Vous pouvez réorganiser les priorités de stratégie pour les stratégies existantes en modifiant le numéro de séquence de stratégie. Toutefois, pour que FPolicy évalue les règles en fonction de l'ordre de priorité modifié, vous devez désactiver et réactiver cette règle avec le numéro de séquence modifié.

Informations sur le copyright

Copyright © 2023 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.