Créer la configuration FPolicy

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/nas-audit/create-fpolicy-external-engine-task.html on September 12, 2024. Always check docs.netapp.com for the latest.

Sommaire

Créer la configuration FPolicy 1
Créez le moteur externe FPolicy 1
Créez l’événement FPolicy 2
Créez des magasins persistants FPolicy 3
Créez la règle FPolicy 5
Créez le périmètre FPolicy 7
Activez la règle FPolicy 8

Créer la configuration FPolicy

Créez le moteur externe FPolicy

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

Ce dont vous avez besoin

Le "moteur externe" la fiche doit être remplie.

Description de la tâche

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

Étapes

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

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

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

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

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

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

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

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

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

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

Créez l'événement FPolicy

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

Avant de commencer

Vous devez terminer l'événement FPolicy "feuille de calcul".

Créez l'événement FPolicy

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

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

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

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

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

Créez les événements de refus d'accès FPolicy

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

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

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

Créez des magasins persistants FPolicy

Les magasins persistants peuvent aider à découpler le traitement des E/S client du traitement des notifications FPolicy afin de réduire la latence du client. À partir de ONTAP 9.14.1, FPolicy vous permet de configurer votre système "magasins persistants" Pour capturer les événements d'accès aux fichiers pour les politiques asynchrones non obligatoires dans la SVM. Les configurations obligatoires synchrones (obligatoires ou non) et asynchrones ne sont pas prises en charge.

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

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

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

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

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

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

Avant de commencer

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

Étapes

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

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

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

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

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

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

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

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

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

- Le `autosize-mode` paramètre spécifie le mode de dimensionnement automatique du volume. Les modes de dimensionnement automatique pris en charge sont les suivants :
  - Désactivé : la taille du volume n'augmente pas ou ne diminue pas en fonction de la quantité d'espace utilisé.
  - Grow : le volume augmente automatiquement lorsque l'espace utilisé dans le volume dépasse le seuil Grow.
  - Grow_Grow - la taille du volume augmente ou diminue en fonction de la quantité d'espace utilisé.

2. Créez la règle FPolicy et ajoutez le nom du stockage persistant à cette règle. Pour plus d'informations, voir "Créez la règle FPolicy".

Création d'un magasin persistant (ONTAP 9.14.1)

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

Étapes

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

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

   Un utilisateur administrateur disposant de privilèges RBAC suffisants (pour créer un volume) crée un volume (à l'aide de la commande cli du volume ou de l'API REST) de la taille souhaitée et fournit le nom de

ce volume en tant que `-volume` Dans le magasin persistant, créez la commande CLI ou l'API REST.

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

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

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

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

- Le paramètre aggregate est nécessaire pour les volumes FlexVol, sinon il n'est pas requis.
- Le `snapshot-policy` le paramètre doit être défini sur aucun. Cela permet de s'assurer qu'il n'y a pas de restauration accidentelle de l'instantané, ce qui entraîne la perte des événements actuels et empêche le traitement des événements en double.

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

2. Créez le magasin persistant :

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

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

3. Créez la règle FPolicy et ajoutez le nom du stockage persistant à cette règle. Pour plus d'informations, voir "Créez la règle FPolicy".

Créez la règle FPolicy

Lorsque vous créez la politique FPolicy, vous associez un moteur externe et un ou plusieurs événements à la règle. La politique spécifie également si un filtrage obligatoire est nécessaire, si les serveurs FPolicy ont un accès privilégié aux données sur la

machine virtuelle de stockage (SVM) et si la lecture passe-automatique pour les fichiers hors ligne est activée.

Ce dont vous avez besoin

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

  Pour plus d'informations, voir "Créez des magasins persistants".

Étapes

1. Créez la règle FPolicy :

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

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

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

     La commande suivante crée une politique nommée « politique 2 » qui est associée à l'événement « event2 » et au moteur externe « moteur2 ». Cette stratégie est configurée pour utiliser l'accès privilégié à l'aide du nom d'utilisateur spécifié. La lecture passe-système est activée :

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

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

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

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

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

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

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

Créez le périmètre FPolicy

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

Ce dont vous avez besoin

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

Étapes

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

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

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

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

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

Activez la règle FPolicy

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

Ce dont vous avez besoin

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

Description de la tâche

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

> Une policy ne peut pas être activée sur le SVM admin

Étapes

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

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

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

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

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

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 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.