Planification de la configuration du moteur externe FPolicy

ONTAP 9

NetApp
April 24, 2024

Sommaire

Planification de la configuration du moteur externe FPolicy

Planification de la configuration du moteur externe FPolicy

Avant de configurer le moteur externe FPolicy (moteur externe), vous devez comprendre les conséquences de cette opération pour créer 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 du moteur externe définit les informations dont FPolicy a besoin pour établir et gérer les connexions avec les serveurs FPolicy externes (serveurs FPolicy), notamment les informations suivantes :

- 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
- 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`
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` [`integer`h][`integer`m][`integer`s]

Informations supplémentaires sur la configuration des moteurs externes FPolicy pour utiliser les 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. Vous ne devez pas supprimer ce certificat lorsque des 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`.

Les certificats ne sont pas répliqués dans les relations de SVM de reprise après incident avec une configuration sans ID-preserve

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).

Restrictions liées aux moteurs externes FPolicy avec configurations de reprise après incident 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.

Remplir la fiche de configuration du moteur externe 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		